

Second Edition

# GAS and OIL RELIABILITY ENGINEERING

Modeling and Analysis



Eduardo Calixto



# Gas and Oil Reliability Engineering

## Modeling and Analysis

Second Edition

**Dr. Eduardo Calixto**

*Federal Fluminense University - LATEC*



AMSTERDAM • BOSTON • HEIDELBERG • LONDON  
NEW YORK • OXFORD • PARIS • SAN DIEGO  
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO  
Gulf Professional Publishing is an imprint of Elsevier





Gulf Professional Publishing is an imprint of Elsevier  
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, USA  
The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1GB, UK

First Edition 2013

Second Edition 2016

Copyright © 2016, 2013 Elsevier Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: [www.elsevier.com/permissions](http://www.elsevier.com/permissions).

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

### Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

### British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library

### Library of Congress Cataloging-in-Publication Data

A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-805427-7

For information on all Gulf Professional Publishing  
visit our website at <https://www.elsevier.com/>



*Publisher:* Joe Hayton

*Acquisition Editor:* Katie Hammon

*Editorial Project Manager:* Kattie Washington

*Production Project Manager:* Sruthi Satheesh

*Designer:* Victoria Pearson

Typeset by TNQ Books and Journals

*To my parents,  
Jose de Arimatea and Maria Auxiliadora Calixto  
and to my son,  
Leonardo Calixto*

# Preface

The oil and gas industry is a competitive market that requires high-performance assets that can be translated into high operational availability, production efficiency, reliability, and maintainability of all assets. Nowadays, to achieve such high performance, it is necessary to extend this expectation to vendors. Therefore reliability engineering tools are very important to this industry and have contributed greatly to its success during the last several decades.

Reliability engineering should be applied systematically in the oil and gas industry to support the assets to achieve and maintain high performance. To meet this goal, it is necessary to establish the reliability management program, which must start at the very beginning of the asset life cycle phase and must be part of daily operations. The reliability management program includes the application of different qualitative and quantitative methods throughout the asset life cycle such as ALT (accelerated life test), HALT (high accelerated life test), RGA (reliability growth analysis), DFMEA (design failure mode and effects analysis), PFMEA (process failure mode and effects analysis), SFMEA (system failure mode and effects analysis), WA (warranty analysis), FRACAS (failure report analysis and correction actions system), PDA (probabilistic degradation analysis), RCM (reliability-centered maintenance), RBI (risk-based inspection), ReBI (reliability-based inspection), ReGBI (reliability growth-based inspection), ORT (optimum replacement time), RAM (reliability, availability, and maintainability) analysis, FTA (fault tree analysis), ETA (event tree analysis), LOPA (layers of protection analysis), SIL (safety integrity level) analysis, bow tie analysis, HRA (human reliability analysis), and APO (asset performance optimization).

Indeed, for companies with assets such as operational plants, platforms, and other facilities, quantitative and qualitative techniques are required during different phases of the life cycle. In project (concept, predesign, and design) and operational phases, DFMEA, SFMEA, RCM, RBI, WA, FRACAS, ReBI, ReGBI, ORT, RAM, APO, and HRA can be applied to support decisions for achieving and maintaining high performance in plant facilities and equipment. In addition, safety is one of the most important performance aspects of the oil and gas industry, and quantitative risk analysis methods, such as FTA, ETA, LOPA, SIL, and bow tie analysis, as well as qualitative risk analysis such as HAZOP, HAZID, PHA, and FMEA, can be implemented during the project (concept, predesign, and design) and operational phases.

Moreover, when equipment is being developed by vendors, ALT, HALT, RGA, and DFMEA are highly important for supporting product development and achieving the performance targets defined in WA by oil and gas companies.

This book discusses all of these techniques and includes examples applied to the oil and gas industry. In addition, reliability engineering program implementation as well as asset management is introduced with examples and case studies.

Asset management aims to drive action to achieve high-performance assets during the life cycle phases. Asset management is integrated with the company's strategy, business plan, and performance at all organization levels. Therefore reliability engineering plays an important role in an asset management program that encompasses asset integrity and integrated logistic support programs, as will be described in this book.

To present all reliability engineering methods as well as reliability engineering program and asset management concepts and applications, this book is organized into different chapters as follows.

Chapter 1: The main objective of lifetime data analysis (LDA) is to predict the reliability and failure rate for a specific period of time based on PDF (probability density function) parameters. Therefore the description of historical failure and repair data, the type of data (complete, censored, and interval), and how to obtain information from the specialists are relevant and will be discussed. Such PDF plots the reliability and failure rate function. However, the main issue when performing LDA is to define which PDF fits better with the historical data. Thus different goodness of fit methods, such as the plot, rank regression, maximum likelihood, chi square, Smirnov–Kolmogorov, and Cramér–von Mises are discussed in this chapter with examples applied to the oil and gas industry. In addition, the different types of PDFs, such as exponential, Weibull, lognormal, loglogistic, normal, logistic, Gumbel, gamma, and R, generalized Gama, Rayleigh, and their parameter characteristics, are also discussed including the importance of confidence limits based on the Fisher matrix concept. At the end of this chapter, LDA case studies applied to oil and gas equipment such as pumps, valves, compressors, heat exchangers, pipelines, and furnaces are presented to clarify the concept of LDA in real applications based on software tools.

Chapter 2: This chapter describes the importance of qualitative (HALT and HASS) and quantitative (ALT, RGA, and PDA) reliability engineering methods to understand product weakness under high operational stress and also to predict reliability concerning stress factors that influence equipment performance. During the design phase, ALT, HALT, HASS, and RGA are applied to predict asset failures and reliability in early design stages as well as to support equipment development and performance target achievement. The PDA is applied during the operation phase to predict equipment reliability based on equipment degradation caused by failure cumulative effects. The ALT methodology will be described based on different methods such as Arrhenius, Eyring, inverse power law, temperature–humidity, temperature–nonthermal, general loglinear, proportional hazard model, and the cumulative risk model. In addition, reliability growth analysis methodology will also be described based on different methods such as Duane, Crow–AMSAA (NHPP), Lloyd–Lipow, Gompertz, logistic, Crow extended, and power law. The PDA methodology will present different methods such as linear, exponential, power, logarithmic, and the phase exponential model. All these methods are described mathematically with examples and graphs applied to the oil and gas industry.

Chapter 3: This chapter begins with the concepts of failure and different FMEA examples. Furthermore, the qualitative approach to define critical equipment based on different criteria such as safety, environment, production, and cost will be discussed. To clarify the different maintenance strategies applied to RCM the concept of preventive maintenance as well as different types of predictive maintenance will be introduced with examples. The aim of this chapter is to introduce reliability engineering, qualitative methods related to maintenance such as FMEA, RCM, and RBI as well as quantitative methods such as ReBI, RGBI, and ORT. In addition, FRACAS and WA will be discussed as a baseline for a reliability database to enable the LDA discussed in Chapter 1. At the end of the chapter, several FMEA, RCM, and RBI case studies will be demonstrated related to the main critical equipment for the oil and gas industry such as pumps, valves, compressors, vessels, pipelines, tanks, and flexible risers.

Chapter 4: The aim of this chapter is to demonstrate the concept of sensors, performance indexes such as reliability, availability, and production efficiency as well as the approach to predict such performance indexes based on RAM methodology. Therefore RAM analysis is the basis of complex system performance analysis. To demonstrate such methodology, RAM analysis steps such as scope definition, LDA, modeling, simulation, critical analysis, sensitivity analysis, and conclusions will be discussed. In fact, RAM analysis simulates the system behavior in terms of subsystem and



equipment failures over the life cycle. To perform such simulation the reliability block diagram model is necessary, as will be demonstrated. In addition, rather than predicting the performance index the main object of RAM analysis is to analyze the influence of external factors on system performance, such as logistics, spare parts, redundancy configuration, as well as the effect of preventive maintenance in performance indexes. Each of such external factor influences will be demonstrated by example in this chapter. Moreover, to predict the necessary performance improvement, improvement allocation and optimization concepts will be discussed. The chapter will present 10 different case studies applied to oil and gas onshore and offshore assets during projects and the operation phase.

Chapter 5: This chapter aims to present different HRAs to model human error during the different asset life cycles, such as design, manufacturing, commissioning, operation, as well as transportation and maintenance. In addition to human error probability assessment, the human performance factors will be analyzed to minimize the factors that influence human error such as internal (psychological, social, physical, and mental) and external (technology, procedures, ergonomic, and layout). HRA can be performed by different methods such as THERP (technique for human error rate prediction), OAT (operator action tree), ASEP (accident sequence evaluation program), HEART (human error assessment reduction technique), STAHR (social technical analysis of human reliability), SPAR-H (standardized plant analysis risk human reliability), SLIM (success likelihood index method), SHERPA (systematic human error reduction and prediction approach), and Bayesian networks. The advantages and disadvantages of implementing each HRA method will also be discussed. In addition, case studies applied to safety, operational, and maintenance related to the oil and gas industry will be presented.

Chapter 6: This chapter aims to present the concept of risk management over the asset life cycle based on hazard identification, risk analysis, risk evaluation, and risk mitigation. To proceed with the risk analysis, different qualitative and quantitative methods will be presented with examples applied to the oil and gas industry. Qualitative risk methods such as HAZOP, HAZID, PHA, and FMEA will demonstrate examples applied to the oil and gas industry to identify different types of hazard and analyze the risk qualitatively. In addition, quantitative risk analysis methods applied to predict the risk, such as FTA, ETA, LOPA, SIL, and bow tie analysis, will be presented with oil and gas examples. At the end, case studies will demonstrate the different combinations of qualitative and quantitative risk methods as well as the combination of risk analysis with other methods such as RAM analysis and HRA.

Chapter 7: The aim of this chapter is to discuss the process of building up a successful reliability engineering program in the oil and gas industry. In this way, the first step will be to understand the competitiveness of the oil and gas industry based on different factors such as customers, suppliers, competitors, regulators, and substitute products. A further step will be to understand the application of different reliability methods over enterprises' life cycles. Once the importance of each method application is understood, the successful factors that influence reliability engineering programs, such as culture, organizational framework, resource, and work routine, will be presented. In addition, 10 reliability engineering pitfalls will be presented to avoid common mistakes that have been made for different organizations around the world. Despite these important factors, there are many barriers to implementing reliability engineering programs in many organizations, such as leader profile, fast food culture, and a standard approach. Finally, successful cases of reliability engineering organizations as well as organizations that promote reliability engineering around the world, including Bayer, USNRC, ESRA, ESReDA, SINTEF, Karlsruhe Institute Technology, Indian Institute of Technology

Kharagpur, University of Strathclyde Business School, and University of Stavanger, will be presented.

Chapter 8: The aim of this chapter is to introduce the concept of asset management by including reliability engineering, asset integrity management, and integrated logistics support programs. Asset management has the main objective of supporting the assets to achieve high performance. Therefore different methods based on reliability engineering, risk management, human reliability, as well as life cycle cost must be performed in a different asset life cycle as defined by the asset management plan. The chapter also presents standards such as PAS 55 and ISO 5500 and additional references such as KP3 asset integrity program and the concepts of JP 886 standards related to ILS. Moreover, the chapter proposes the quantitative asset management evaluation methodology based on ISO 55000 and quality award methodology. To clarify the asset management concepts, four case studies related to asset management are presented. The first one describes asset integrity management during the design phase applied to a subsea asset. The second case study describes the recovery sulfur plant asset integrity implementation during the predesign phase. The third case study describes the integrated logistics support program applied during the design phase for subsea assets. The fourth case study describes an asset management program applied to an integrated offshore system.

The benefits of this book include:

- Understanding how to use failure and repair historical data to predict reliability based on examples and case studies;
- Understanding how to predict reliability during the design phase, considering stressor factors as well as how to improve such reliability;
- Predicting reliability based on the cumulative effect of failures;
- Understanding the concept of different methods applied to repairable equipment and systems with several examples of FMEA, RCM, and RBI applied to the oil and gas industry;
- Predicting and optimizing complex asset performance, such as refinery plants, utility facilities, subsea, and platform, considering different factors such as reliability, maintainability, preventive maintenance, spare parts, logistics, and life cycle cost;
- Understanding the application of HRA by considering the influence of human error on asset safety, operation, and maintenance task performance;
- Understanding the effect of safety on asset performance by considering the relation between safety, reliability, and maintenance;
- Understanding the importance of a reliability program over the asset life cycle as well as the application of different reliability engineering methods in different asset phases: the 10 reliability pitfalls as well as the reliability program barriers will also be clearly understood;
- Understanding the asset management program concepts and the relation of asset management to other important programs such as reliability engineering, asset integrity, and integrated logistic support.

The new edition of this book is based on the author's knowledge and experience over the past 13 years as a reliability engineer in the oil and gas industry by applying consultant services and proposing solutions for different oil and gas companies from the United States, South America, Europe, Asia, Africa, Australia, and the Middle East.

# Acknowledgment

Thank you to my masters from Fluminense Federal University, Gilson Brito Alves Lima and Oswaldo Luiz Gonçalves Quelhas, for supporting and sponsoring my engineering career.

I also thank the following teammates: Joao Marcus Sampaio Gueiros, Jr., Carlos Daniel, Wilson Alves dos Santos, Geraldo Alves, Cid Atusi, Darlene Paulo Barbosa, Leonardo Muniz Carneiro, Aneil Souza, Michael Sabat, Carlos Hanriot, Willyane Castro, Paulo Ricardo, Ronaldo Priante, Oswaldo Martins, Istone R., Alexandre Nunes, Milton Iginio, Jose Luiz Nunes, Fernando Sigilliao, Joao Eustaquio, Carlos Eustaquio Soukef, Fabio Franca, Nelmo Furtado, Carlos Andre, Delton Correa, Miguel Ricardo, Rafael Ribeiro, Marcio Bonfa, Jorge Fernandes, Claudio Garcia, Joseane Garcia, Paulo Rijo, Manoel Coelho, Antônio Ribeiro Louzana, Wilson Antunes, Jr., Marco Evangelista, Mariano Pacholok, Mauricio Requiao, Ricardo Alexandre, Amauri dos Santos Cardoso, Helio Goes, Manoel Jose Gomez, Romeu Wachburger, Gustavo de Carvalho, Jorge Luiz Ventura, Douglas Tirapani, Borges Ezequiel, Adelci Menezes, Aldo Silvestre, Tony Lisias, Frederico Vieira, Mario Barros, Paulo Rosemberg, Francisco Bezerra, Eduardo Guerra, William Frederic Schmitt, Antonio Carlos Freitas Araujo, Luiz Eduardo Lopes, Gustavo Furtado, Emerson Vilela, Carlos Frederico Eira, Marcelo Ramos, Atila R., and Professor Carlos Amadeu Palerosi for supporting my reliability analysis over the years.

For contributing to this book and to my reliability engineering career, I thank Joao Marcus Sampaio Gueiros, Jr. from Petrobras, Claudio Spano from Reliasoft Brazil, Cid Augusto from Reliasoft Brazil, Pauli Adriano de Amada Garcia from Fluminense Federal University, and Paulo Renato Alves Firmino from UFRPE.

I have also to thank Stephen Laurie from Frontica Business Solutions (UK), David Thompson from RAMsoft Ltd. (UK), Doug Ogden from Reliasoft Corporation (USA), Yzak Bot from BQR Reliability Ltd. (Israel), and Andrzej Kozak from UDT, Safety Inspection Office (Poland) for all their support on my international career as a reliability engineer.

To my wife Isabel Katrin Calixto: thank you for all your support during this time.

## LIFETIME DATA ANALYSIS

**CHAPTER OUTLINE**

<b>1.1 Quantitative Failure Data Analysis .....</b>	<b>2</b>
<b>1.2 Probability Density Functions .....</b>	<b>11</b>
1.2.1 Exponential Probability Density Function.....	17
1.2.2 Normal Probability Density Function .....	20
1.2.3 Logistic Probability Density Function .....	23
1.2.4 Lognormal Probability Density Function.....	25
1.2.5 Loglogistic Probability Density Function .....	27
1.2.6 Gumbel Probability Density Function .....	29
1.2.7 Weibull Probability Density Function.....	31
<i>Mixed Weibull Probability Density Function.....</i>	<i>33</i>
1.2.8 Gamma Probability Density Function.....	35
1.2.9 Generalized Gamma Probability Density Function.....	37
1.2.10 Rayleigh Probability Density Function .....	39
<b>1.3 Goodness of Fit Methods: How to Define PDF Parameters and Choose PDF that Fits Better in Failures Data .....</b>	<b>41</b>
1.3.1 Plot Method.....	42
1.3.2 Rank Regression .....	47
1.3.3 Maximum Likelihood Methods .....	50
1.3.4 Chi Square Methods .....	52
1.3.5 Kolmogorov–Smirnov Method.....	54
1.3.6 Cramer–von Mises Tests.....	57
<b>1.4 How Reliable is Reliability: Confidence Bound Will Tell You About !!! .....</b>	<b>59</b>
<b>1.5 Lifetime Data Analysis Cases .....</b>	<b>64</b>
1.5.1 Pump Lifetime Data Analysis.....	64
1.5.2 Screw Compressor Lifetime Data Analysis Case.....	67
1.5.3 Valve Lifetime Data Analysis Case.....	75
1.5.4 Sensor Lifetime Data Analysis Case .....	76
1.5.5 Heat Exchanger Lifetime Data Analysis Cases .....	80
1.5.6 Pipeline Lifetime Data Analysis Cases.....	83
1.5.7 Furnace Lifetime Data Analysis Cases .....	87
<b>References .....</b>	<b>92</b>



---

## 1.1 QUANTITATIVE FAILURE DATA ANALYSIS

The reliability concept is the probability a piece of equipment, product, or service being successful until a specific time. To define equipment, product, and service reliability it is necessary to collect historical failure data.

Therefore the first step in the life cycle analysis study is to know how failures occur over time, which is critical to defining an index like failure rate, reliability, availability, and mean time to failure (MTTF) to support decisions in defining the best time for inspection, maintenance, to check if the equipment has achieved a reliability requirement, and to supply information to new projects.

To conduct lifetime data analysis it is necessary to have historical data about failure modes. The failure mode is the way that a piece of equipment or product loses part or all of its capacity to conduct its function.

Many companies in the oil and gas and other industries do not have historical data for their equipment, and a number of equipment suppliers have no historical failure data for their products. Therefore the first step in lifetime data analysis is to collect data, but in many cases the engineer who needs data for lifetime data analysis is not the same person who fixes or performs maintenance on the equipment and collects the data. In summary, some companies have historical failure data and others do not.

An environment for assessing root cause analysis and solving problem as well as making decisions based on reliable information makes the data collection process and the creation of historical data reports very important.

For companies that do not have data to make decisions, the first step is to create a historical data report before carrying out lifetime data analysis. When doing so, managers must be aware of the importance of collecting equipment failure data and also introducing and supporting employees to do so. Moreover, employees must be trained in collecting data and take decisions based on reliable data. This is a big challenge for most companies, because even when procedures and programs are established, it is necessary to collect, assess, and store failure data in files and reports for access later.

Depending on the system, collecting failure data depends on maintenance and inspection routines, and this data collection process often competes with other activities. In the oil and gas industry, equipment generally does not have a high frequency of failure, which enables employees to more easily collect and work with equipment failure data.

For many reliability professionals, historical failure data means a reliability index, which includes failure rate, reliability, availability, efficiency, MTTF, or probability density function (PDF) parameters. For inspection and maintenance professionals, historical failure data means files with services described by type of failure of occurrence, time to repair data, and recommendations. In fact, if there are no reliability index and PDF parameters for conducting lifetime data analysis, this data must be created by reliability specialists based on available data. In reality, creating the data is the first step of lifetime data analysis, and then defining the reliability index based on this data. The best scenario, of course, is that there is a reliability index and PDF parameters available for reliability professionals, but this is not usually the case. Thus two points of view among reliability professionals are discussed all over the world: the reliability index and PDF parameters must be defined in a report to make analysis easier, or index and PDF parameters must be calculated and updated for the specialist. When reliability professionals assess PDF parameters from reports, the chance of error is greater than when comparing

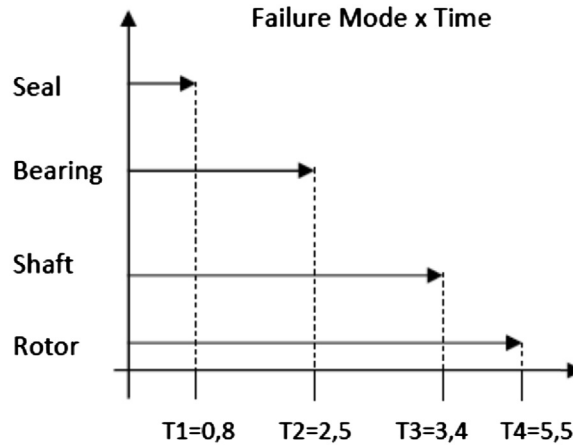
them with defined parameters based on historical data. Despite the time required to assess files, creating historical data reports before and then creating the PDF parameters, reliability index, lifetime data analysis based on historical data, and failure root cause analysis are more reliable because they are better understood and updated more frequently.

Another important point is that equipment PDF characteristics change over time and PDFs must be assessed whenever a failure occurs, even though there is a reliability index. Thus the failure data reports must be updated from time to time. Additionally, new equipment has different lifetime data cycles over time, and this information needs updating, which makes the reliability index cumbersome. To conduct life cycle analysis the following data, classified by configuration, is required:

- Individual or grouped data;
- Complete data;
- Right suspension data;
- Left suspension data;
- Data in interval.

Individual data is data from one piece of equipment only and grouped historical data comes from more than one piece of similar equipment. In the first case the main objective is to assess equipment for lifetime data analysis, and historical failure data from one piece of equipment is enough, but such equipment should have a certain quantity of data for reliable lifetime data analysis. In some cases there is not enough historical data and it is necessary to look at a similar piece of equipment with a similar function and operational condition to create the historical failure data. In real life, it is not always easy to find similar equipment because in many cases, maintenance operations, and process conditions interfere with the equipment life cycle. In cases where reliability analysis is conducted during the project phase, similarity is easier to obtain because operational conditions, processes, and maintenance procedures are similar to project requirements. However, to increase the reliability of lifetime data analysis historical grouped data must be used and in this case requires considering more than one piece of similar equipment to create PDFs for the equipment being assessed. It is also necessary to validate equipment similarities and in projects this is also easier.

When historical data is defined when the failure occurs, the data is called complete and in this case it is necessary to establish a time measure (hours, days, months, years). It is essential to know the initial operation time, that is, when the equipment life cycle began. Caution must be used when defining the initial operation time because in some equipment there is a different start time because it has changed over time. Maintenance and operational data in many cases help to validate the initial operation time. In some cases, equipment has no failure data reports and it appears that the first failure occurred after 5 or 10 years, but in reality no failures have been reported. Fig. 1.1 shows different failure mode data for pumps. Such information is assessed from failure data reports, which include root cause of failure, repair time, and recommendations, as shown in Fig. 1.2. There are many types of reports, but when failure modes are defined it is easier for everyone to understand what happened, why it happened, and to assess if the recommendations conducted solved the failures. When defining failure modes, all employees should understand what each of the failure modes means otherwise some failure modes will be described incorrectly. Sometimes it is difficult to define the failure mode, and in this case it is easier to put the general failure mode as “other” for the classification. However, this must be avoided whenever possible because it does not help identify and solve problems or improve equipment.



**FIGURE 1.1**

Pump complete data failure modes.

The other possibility is to use electronic failure reports, which have the following advantages:

- Can be consulted for different sites;
- Can be updated automatically;
- Support life cycle analysis automatically;
- Save maintenance and reliability specialists time in life cycle analysis.

Despite those advantages it is necessary to train people to input data in electronic reports. Additionally, electronic reports often do not have the same details as paper reports and in some cases this can influence important decisions. Information security is another concern because electronic reports are easier to access and copy than paper reports.

The disadvantages of using electronic reports include:

- They have fewer details;
- May have errors because in some cases the person who inputs the data is not the one who assesses the equipment failure;
- If there is an electronic system failure the electronic report cannot be accessed;
- Depending on the particular case, if there is an error in the index, such as failure rate or reliability, it is necessary to check the mathematics used to compile the report.

For data configuration, in some cases, when some of the equipment used to create the PDFs has not failed in the observed time, it is considered right censored data and must be considered in the analysis. In real life, in many cases, this data is often not taken into account, but it can influence the reliability index.

The other type of data configuration is when there is some data that failure occurred before a specific time, and there is no information about when such failure occurred. This happens most often when failure reports are configured after equipment operation start time. While it may seem that the

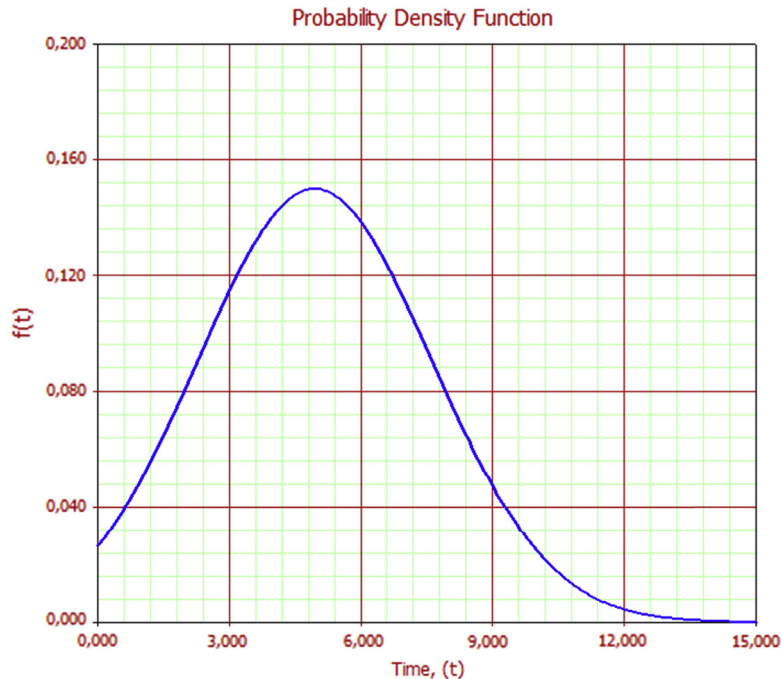
Data: 10/12/2004		Equip Tag: B-114001A		Managment: Dinamic Maintanance	
Ref: R033		Professional : Alexandre Nunes			
Type of intervention:	Inspection	Corretive Maintanance	Programmed Maintanance	Predictive Maintanance	
		x			
Data of itervention :	10/12/2004	Time of itervention :	8h		
Data of start service :	10/12/2004	Time of start service :	9h		
Data of Finish service :	12/12/2004	Time of Finish service :	10h		
Failure Mode Types					
Item		Root Cause			
x	1 - Seal leakage	<b>Pump operation over than specified in procedure</b>			
	2 - Bearing				
	3 - Shaft				
	4 - Rotor				
	5 - Eletric Motor				
	6 - Vibration				
	7 - Impeller				
	8 - Rings suction				
	9 - Gaskets				
	10 - Specify other				
Pump Draw					
Signature :					

**FIGURE 1.2**

Equipment failure reports.

equipment had high reliability, in reality there were unreported failures at the beginning of the equipment life cycle. A good example is what happens in one critical equipment life cycle analysis, for example, coke formation in a furnace is expected to happen every 6 months. After looking at the failure report, the PDF that indicates frequency of failures over time was concentrated in 4 years; totally different from what project engineers expected. After consulting the operator it was confirmed





**FIGURE 1.3**

Furnace PDF (coke formation).

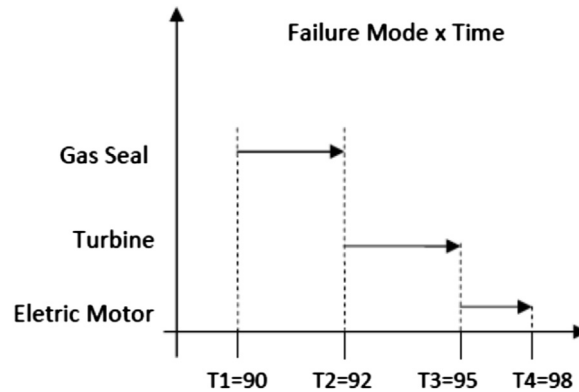
that the equipment failed every 6 months, but the failures were not reported at the beginning of the life cycle. Fig. 1.3 shows different PDFs from reported failures data and real data. The PDF characteristic will be discussed in the following sections, but looking at Fig. 1.3 it is possible to see how different the PDF is and how it cannot be used to make decisions.

Another historical data configuration is when there is no exact information about when equipment failure occurred but the interval of failure time and this type of data is called interval data. In many cases this is considered enough information to do life cycle analysis, but in some other cases it is not. Fig. 1.4 shows equipment failure occurrences in different intervals over time.

In many cases this kind of failure data configuration can be obtained from maintenance and operation specialist opinions even when data is not reported. This is most often the case when equipment failures are not reported, but when they occur the impact on the system is great.

The big challenge in life cycle analysis is working with data when there is not much available, or the data available is not reliable enough to be considered. In this case, specialist opinion can be used to define the PDF parameters, and there are some techniques to estimate the variable values from specialist opinion:

- Aggregated individual method: In this method, experts do not meet but make estimates individually. These estimates are then aggregated statistically by taking the geometric mean of all the individual estimates for each task.
- Delphi method: In this method, experts make their assessments individually and then all the assessments are shown to all the experts and then the parameter values are defined for the group.



**FIGURE 1.4**

Turbine failures in interval data.

- Nominal group technique: This method is similar to the Delphi method, but after the group discussion, each expert makes his or her own assessment. These assessments are then statistically aggregated.
- Consensus group method: In this method, each member contributes to the discussion, but the group as a whole must then arrive at an estimate upon which all members of the group agree.
- Bayesian inference methodology: This method is a mathematical approach applied to estimating variable values (a posteriori variable values) based on prior knowledge (ie, taking into account all specialist opinions and prior knowledge to estimate variable values as explained next).

The aggregated individual method requires mathematic treatment using the geometric mean to define the final variable value. In this way the weight of each individual opinion will highly influence the results. Such an approach is indicated when there is heterogeneous knowledge among specialists about the estimated variable value. This approach is helpful when it is difficult to get a value consensus of the specialist group, but caution is required when defining specialist opinion weight.

The Delphi method requires that specialists know other specialists' opinions and assess until the discussed point is agreed upon (in this case a variable value). With this approach, files are sent to specialists in different places to get opinions, and this process is repeated until consensus is achieved. This approach can be difficult because there is no discussion about conflicting opinions, and it is not always clear why a specialist defines a different value. Despite this, this method is a good option when it is not possible for all specialists to meet. In some cases, for example, specialists send back the questionnaires after the third sequence, and it is necessary to take into account their opinion and decide the value of the variable.

The nominal group technique is similar to the Delphi method but after a group discussion specialists give their own opinions about variable values and then those values are statistically assessed. Depending on the variance between variable values there might be a higher or lower error expectation. When specialists have similar opinions, there is not significant variance in the variable value result.

The consensus group method requires that specialists discuss the values (after their own individual analyses) with other specialists and then come to a conclusion about ideal parameter values. This approach is helpful because all specialists are given the opportunity to discuss their opinion and details

can be discussed. This approach is most common when there is known equipment but no failure data analysis. In such an approach it is necessary to pay attention to the operational and maintenance conditions the specialist is basing his or her opinion on. A good example is when one specialist states his opinion about heat exchanger incrustation and says it happens in 3 years with half-year deviation. In an effort to better understand his opinion, other specialists ask about which period of time he was taking into account, and he describes what he saw in the last 5–10 years. But this equipment had been in use for 20 years. Fig. 1.5 shows the difference of specialist opinions in terms of frequency of incrustation in the heat exchanger. The difference in these results is very influential.

Bayesian inference methodology is a mathematical approach applied to defining variable values based on a priori knowledge to estimate a posteriori variable values (ie, all specialist opinions are considered and prior knowledge is used to estimate variable values). This state is represented by the Bayes equation, as follows:

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{P(B|A) \times P(A)}{P(B)}$$

This equation can be represented also like:

$$\pi(\theta|E) = \frac{P(\theta \cap E)}{P(E)} = \frac{P(E|\phi) \times \pi_0(\phi)}{\int P(E|\phi) \times \pi_0(\phi)}$$

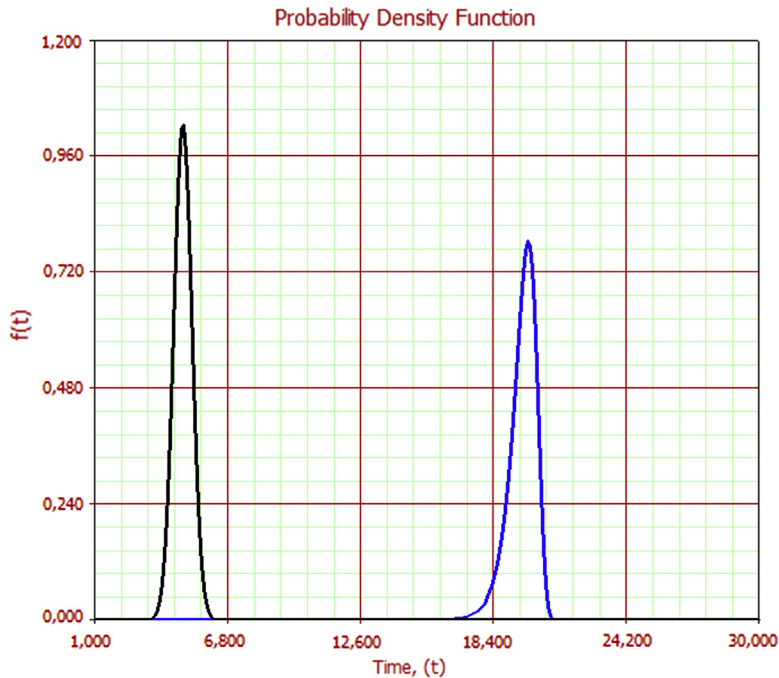


FIGURE 1.5

Specialist A (normal— $\mu = 5$ ;  $\sigma = 0.5$ ) and other specialists' opinion (Gumbel— $\mu = 20$ ;  $\sigma = 0.5$ ).

where  $\pi(\theta|E)$  = a posteriori knowledge, which represents uncertainty about  $\theta$  after knowing the value of  $E$ ;  $\pi_0(\theta)$  = is prior knowledge, before knowing the value of  $E$ ; and  $P(E|\theta)$  = is maximum likelihood of specialist opinion.

Applying specialist opinion it is possible to estimate the value of  $\theta$ . Such an approach is often used in drilling projects in Brazil to define the probability of an event when risk analysis is being conducted. In this case, that approach is adequate because historical failure data from other drills is not reliable because of the existing different conditions for each drill.

After looking at different types of data configuration and specialist opinion techniques the next step is to create the PDFs and assess the data characteristics.

Thus data characteristics can be individual, grouped, complete, right suspension, left suspension, at interval, or a combination of these configurations. In addition, data can also be multicensored. This happens when because of any reason a component or piece of equipment under life cycle analysis is censored (maintenance, change in policy, energy breakdown, etc.) without the necessary analysis time. This type of data is common for standby equipment where the main equipment is operated for a period of time and then the standby equipment is substituted for operation. Consequently, there will be a failure and suspense data for different periods of time.

Another important difference in data characteristics is between repairable and nonrepairable equipment. When we are considering nonrepairable equipment or components, when such a failure occurs, a new piece of equipment is introduced and a new initial time has to be established to calculate failure time. This happens only when a component or piece of equipment is considered as good as new. Such an assumption is hard to do in real life, even though a component is new, because the processes, maintenance, and operational actions still affect the equipment life cycle. When a human error in component assembly occurs, for example, it is common to have a failure in a couple of hours after replacement even when failure, based on historical data, is expected after some years. Such failure times cannot be considered in life cycle analysis, but when a “good as new” assumption is taken into account, such data will influence PDF shape. In some cases, equipment that would be represented for a PDF shape with failure at the end of the life cycle will be represented by a PDF shape with failure at the beginning of the life cycle.

For repairable equipment or components common in the oil and gas industry, each failure must consider the initial time ( $T_0$ ) when the equipment began operation to calculate time to failure, as shown in Fig. 1.1. When repairable equipment or components replace old ones, a new initial time will be defined.

The Laplace test, also known as the centroid test, is a measure that compares the centroid of the observed arrival times with the midpoint of the period of observation. Such a method determines whether discrete events in a process have a trend. In this way the Laplace score can be mathematically calculated by:

$$L_s = \frac{\frac{\sum_{i=0}^N T_i}{N} - \frac{T_n}{2}}{T_n \sqrt{\frac{1}{12N}}}$$

where  $L_s$  = Laplace score;  $T_n$  = period of failure of initial time;  $T$  = observation period; and  $N$  = number of failure time data.



When the last event occurs at the end of the observation period ( $T_n = T$ ), use  $N - 1$  despite  $N$ , so the formula will be:

$$L_s = \frac{\frac{\sum_{i=1}^{N-1} T_i}{N-1} - \frac{T}{2}}{T \sqrt{\frac{1}{12(N-1)}}}$$

A Laplace score greater than zero means that there is an increasing trend, and a score less than zero means there is a decreasing trend. When the Laplace score is zero, there is no trend, and in this case it is stationary.

When determining the reliability of a repairable system under life cycle analysis, the Laplace test can be used to check failure trends. Table 1.1 shows an example of a seal pump failure over a long period. The first column shows the time when the seal leakage occurred. The second column shows the time between seal leakage, and if this time is used, the seal is considered to be as good as new after repair. This is similar to having an initial time after any seal repair. The last column gives the time between failures, from smallest to highest value.

To prove that data cannot be treated as good as new because there is an increase trend in failure, the Laplace test is applied as follows:

$$L_s = \frac{\frac{\sum_{i=1}^{N-1} T_i}{N-1} - \frac{T}{2}}{T \sqrt{\frac{1}{12(N-1)}}}$$

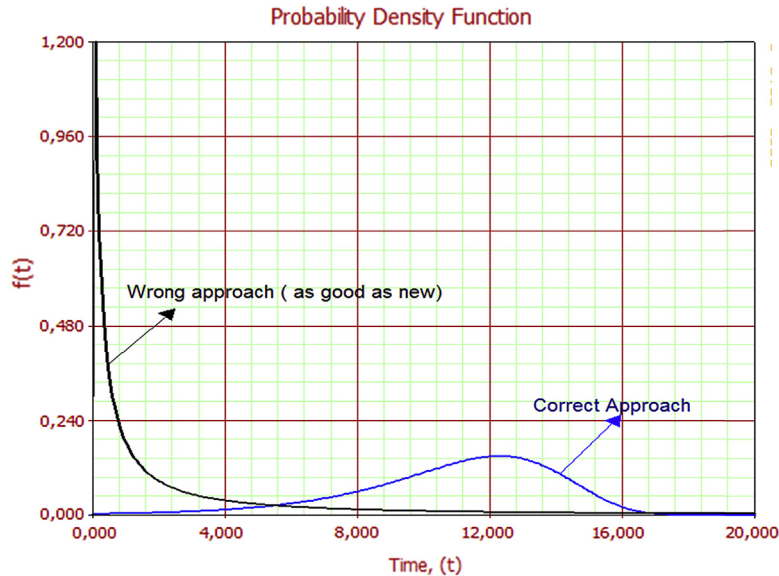
$$L_s = \frac{\frac{\sum_{i=0}^{5-1} T_i}{5-1} - \frac{T}{2}}{T \sqrt{\frac{1}{12(5-1)}}} = \frac{\frac{42.58}{4} - \frac{12.92}{2}}{12.92 \sqrt{\frac{1}{12(5-1)}}} = 2.24$$

If there is an increase in failure rate, this means wear on the seal. Thus failure data has to be fitted in the first column of the table, and it is not correct to consider that after seal repair the seal is as good as new. Fig. 1.6 shows the big difference between the data from the first column and third column of Table 1.1.

The PDF on the left shows that most failures occur at the beginning of the life cycle (data from the third column of Table 1.1) and the gray PDF on the right shows that most failures occurs at the end of

<b><i>T</i></b>	<b>TBF</b>	<b>TBF Sequence</b>
6.42	6.42	0.08
10.67	4.25	0.17
12.67	2	2
12.83	0.17	4.25
12.92	0.08	6.42

TBF, *Time between failures.*



**FIGURE 1.6**

Wrong versus correct approach PDF (seal leakage failures).

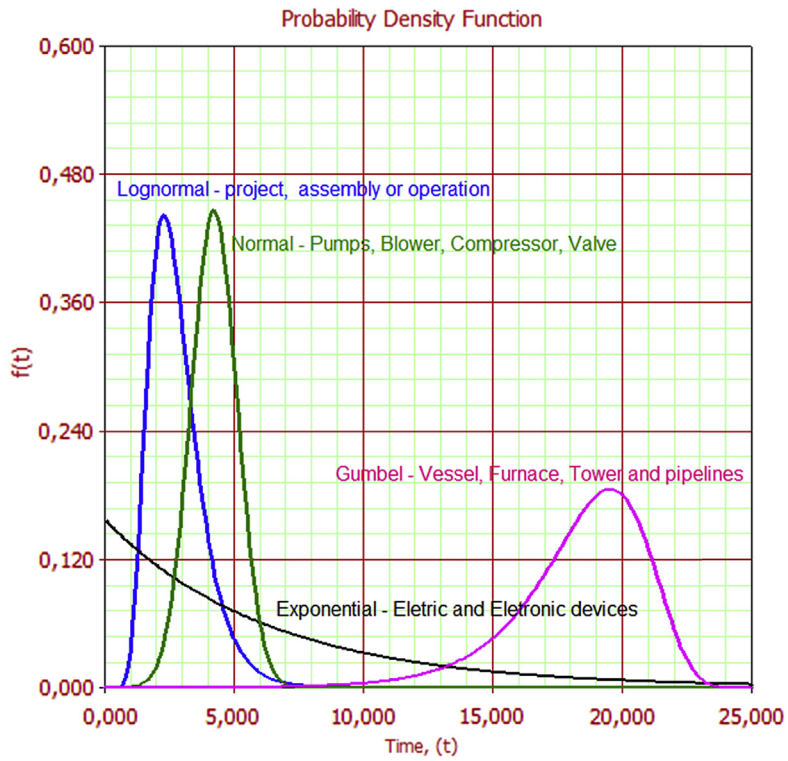
the life cycle (data from the first column of [Table 1.1](#)). The next section describes the types of PDFs and other reliability parameters.

## 1.2 PROBABILITY DENSITY FUNCTIONS

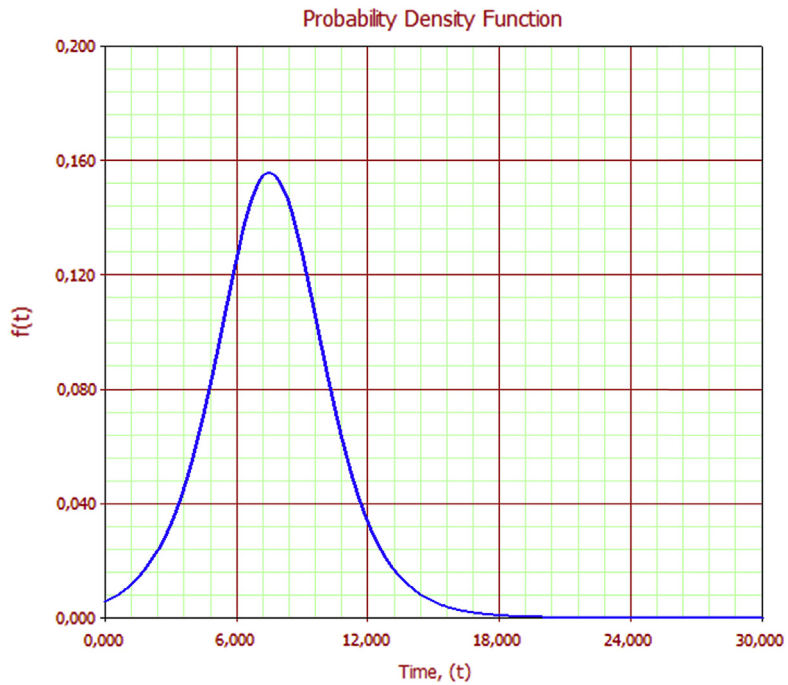
The PDFs describe graphically the possibility of events occurring over time; in equipment life cycle analysis, this means failure or repair time occurrence over time. This allows maintenance and reliability professionals to make decisions about maintenance policies, inspection policies, and failure behavior. Actually, another index is necessary, such as failure rate or reliability function to make these decisions, but PDFs are the first step to better understanding how failures occur over time. [Fig. 1.7](#) shows different shapes of PDFs that represent different types of equipment in the oil and gas industry.

In fact, failures have a greater chance of occurring at the beginning, during a specific period of time, at the end, or randomly during the equipment life cycle. In some cases, equipment has an expected behavior in terms of failure. Electrical devices have expected constant failure rate and mechanical components have expected increasing failure rate. Sometimes, process conditions or even human actions change failure equipment's behavior. This is what happens, for example, with an electronic actuator valve that, despite random failure over time, is suspected of failure, because of the effects of water whenever it rains, of having a normal PDF despite exponential PDF behavior on it, as shown in [Fig. 1.8](#). In doing so, equipment PDF behavior is only an expectation of occurrence, because the only way to find out the equipment PDF is to conduct life cycle analysis.

It must be noted that no matter what the PDF shape is, it is important to try to understand clearly why the equipment PDF has such a shape. It is also important to validate this information with



**FIGURE 1.7**  
PDFs and equipment.



**FIGURE 1.8**  
Pressure swing adsorption system valve actuator PDF.

maintenance professionals and operators who know the equipment. In some cases, some data may be missed or not reported in the historical data.

PDFs for reliability engineering are represented mathematically in most cases for the following functions:

- Exponential
- Normal
- Logistic
- Lognormal
- Loglogistic
- Weibull

The exponential PDF describes random behavior over time and fits well to electrical and electronic equipment best. The normal PDF describes some dynamic equipment failures or failures that occur in specific periods of time with some deviation. The logistic PDF is similar in shape to the normal PDF. The lognormal PDF best describes failure that occurs at the beginning of the life cycle that mostly represents failure in a project, startup, installation, or operation. The loglogistic PDF is similar in shape to lognormal. The Weibull PDF is a generic function and depends on parameters that represent exponential, lognormal, or normal PDFs. The gamma and generalized gamma are also generic PDFs but can represent exponential, lognormal, normal, and Gumbel PDFs, depending on parameter characteristics. Gumbel PDFs represent equipment failures that occur at the end of the life cycle such as in a pipeline, vessel, and towers, and in some cases before the end of the life cycle because a process or facility has influenced the failure mechanism.

Despite being used intensively to describe failure over time, PDFs may also describe repair time, costs, or other variables. For repair time, the lognormal and normal PDFs are most often used by reliability professionals. For lognormal PDFs most of the repairs are made for short periods of time when performed by experienced employees and take considerably more time when repair is carried out by an inexperienced employee or logistic issues cause repair delays. A normal PDF is used to represent repair failure for a repair that is made mostly in one period of time with a deviation. The following section explains each PDF mathematically to best illustrate reliability concepts.

The PDF shows the behavior of the variable in a time interval, in other words the chance of such an event occurring in a time interval. So a PDF is mathematically represented as follows:

$$P(a \leq x \leq b) = \int_a^b f(x)dx$$

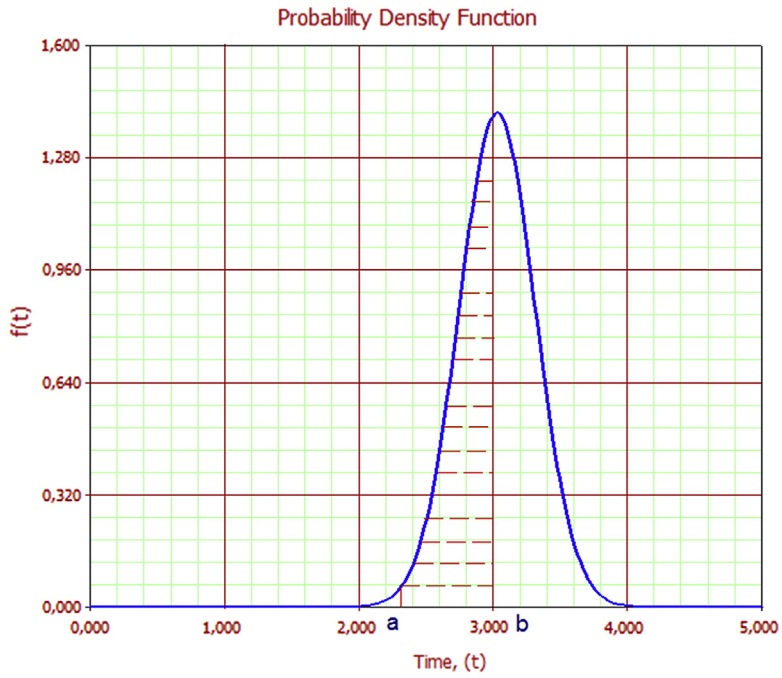
This is represented graphically by [Fig. 1.9](#), which is the area between interval  $a$  and  $b$ .

The probability cumulative is PDF integration that represents the chance to failure occurring until time  $t$  and is represented by the equation:

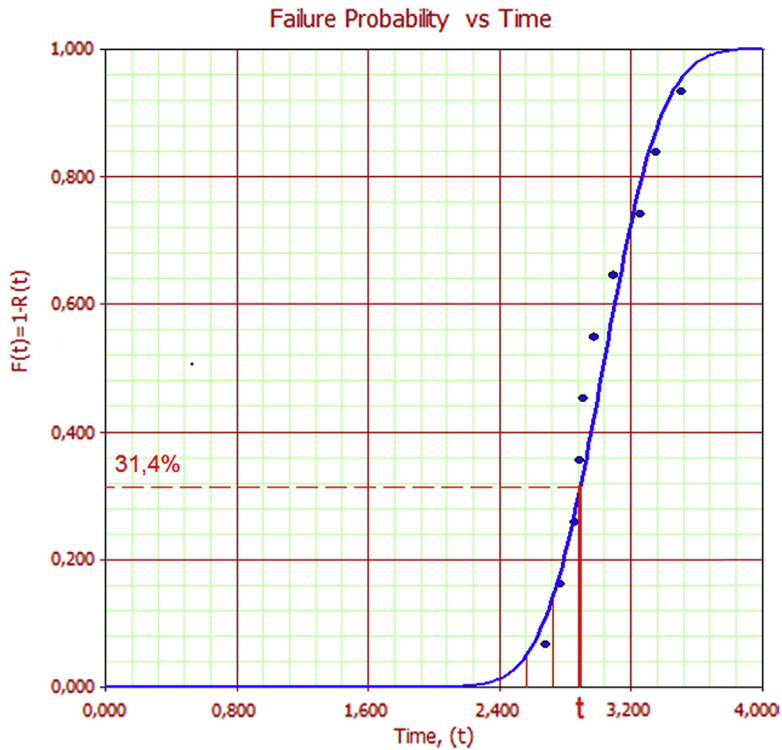
$$P(x \leq t) = \int_0^t f(x)dx = F(t)$$

The cumulative probability of failure is represented by [Fig. 1.10](#).

As discussed, reliability is the probability of a piece of equipment, product, or service operating successfully until a specific period of time, and is mathematically complementary of cumulative



**FIGURE 1.9**  
Probability density function.



**FIGURE 1.10**  
Cumulative density function. Probability of failure (from 0 to  $t = 2.9$ ).

failure probability. Thus the following equation represents the relation between cumulative failure and reliability (if the two values are added, the result is 100% or 1):

$$R(t) + F(t) = 1$$

$$R(t) = 1 - F(t)$$

$$R(t) = 1 - \int_0^t f(x)dx$$

This equation shows that failure rate varies over time. To have a constant value the relation between the PDF and reliability must be constant. Failure rate function analysis is a very important tool for maintenance and reliability professionals because it provides good information about how failure rates change over time. The classic failure rate representation is the bathtub curve, as shown in Fig. 1.11.

In fact, equipment failure rate is represented for one or two bathtub curve periods. When three periods of equipment-life shapes exist, such as the bathtub curve, Weibull 3P is being represented. In Weibull 3P (three parameters), three pieces of equipment form a common system or three components form one piece of equipment. Thus the bathtub curve is represented for mixed Weibull, which comprises more than one population; in this case the data of three components. In Fig. 1.12, early life ( $\beta = 0.45; \eta = 2.45; \gamma = 0.45$ ) occurs from 0 to 3.8 years, useful life ( $\beta = 1.06; \eta = 0.063; \gamma = 0.39$ )

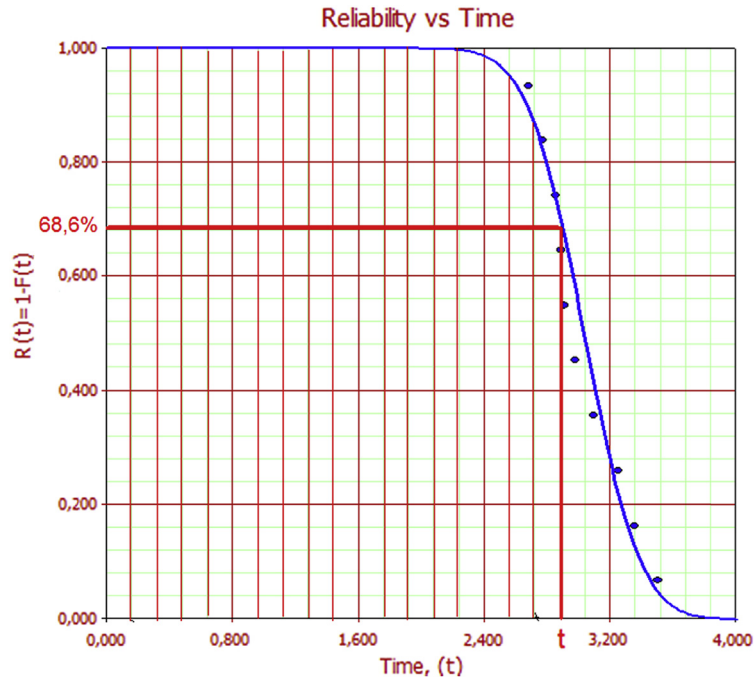


FIGURE 1.11

Cumulative density function. Reliability (from 0 to  $t = 2.9$ ).

occurs from 3.8 to 7.9 years, and wear-out ( $\beta = 49.95; \eta = 8.92; \gamma = 0.14$ ) occurs from 7.9 years on. Generally, lognormal or loglogistic PDF represents well early failures. The exponential PDF represents well random failures. The normal or logistic PDF represents well wear-out failures. The Weibull 3P may be performing different bathtub curve characteristics. Therefore, if equipment, component, or product failure rate shapes the early life characteristic, in most cases, this means failure caused by a design or manufacturing error, installation error, or even human error during operation. Whether the failure rate shapes as a constant line, it's means that the failures occur randomly. Finally, if the failure rate shapes such as an increasing failure rate, that means wear-out.

The other important concept in reliability engineering is MTTF, which means the expected time to failure, represented by:

$$MTTF = \int_0^{\infty} t \cdot f(t) dt$$

In many cases, MTTF is calculated as an arithmetic average, which is correct only for normal, logistic, or PDFs with such normal characteristics, because in this case mean, mode, and expected time are all the same. Another important concept is the mean time between failure (MTBF) value, which is similar to the MTTF value, but repair time is included in the MTBF case. In many cases in the oil and gas industry, expected time to failure is represented in years and expected time to repair is represented in hours. Sometimes repair time is less than 1 day and in most cases less than 1 month. In some cases it takes more than a month to repair a piece of equipment, but in these cases there is mostly a logistical delay issue, such as purchase or delivery delay. In these cases logistical delays are included in the MTBF calculation. The MTBF function can be represented as follows:

$$MTBF = MTTF + MTTR$$

$$MTBF = \int_0^T T \cdot f(x) dx + \int_0^t t \cdot f(y) dy$$

where  $T$  is time to failure and  $t$  is time to repair. When time to repair is too small compared to time to failure, the MTBF is approximately the MTTF as follows:

$$MTTF \gggg MTTR$$

$$MTBF \approx MTTF$$

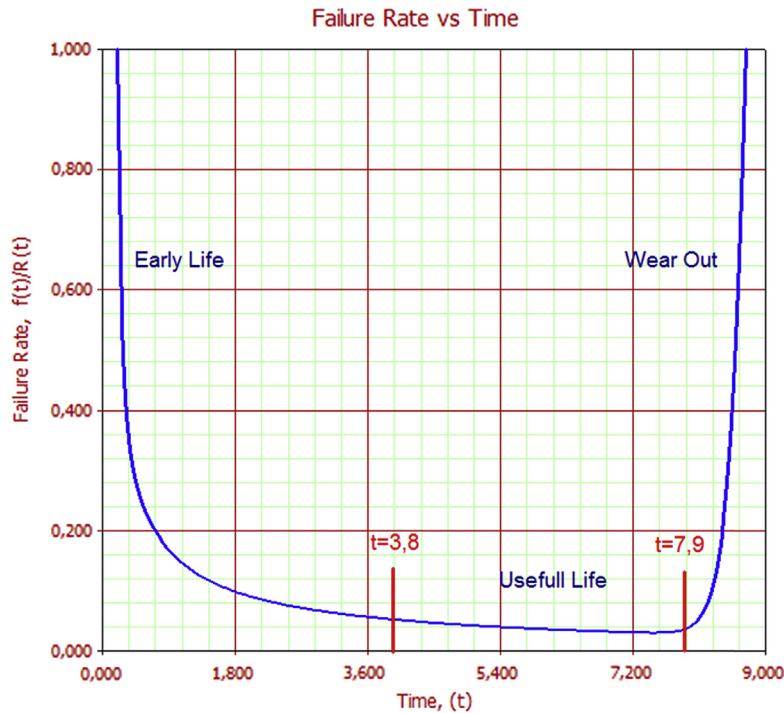
$$MTBF \approx \int_0^T T \cdot f(x) dx$$

Another important index is failure rate, which is defined by relations between PDF and reliability functions, as shown in the equation:

$$\lambda(t) = \frac{f(t)}{R(t)}$$

This represents that the failure rate varies over time. To have a constant value the relation between PDF and reliability must be constant. Failure rate function analysis is a very important tool for maintenance and reliability professionals because it gives reliable information as to how the failure rate behaves over time. The classic failure rate representation is a bathtub curve, as shown in Fig. 1.12.





**FIGURE 1.12**

Bathtub curve.

### 1.2.1 EXPONENTIAL PROBABILITY DENSITY FUNCTION

To further explain reliability engineering concepts we will begin with the exponential PDF because of its simple mathematics compared to other PDFs. The exponential PDF represents a random occurrence over time and best represents electronic, electrical, or random events. However, in some cases, electrical and electronic equipment does not have random failure occurrences over time. The exponential PDF equation is:

$$f(t) = \lambda e^{-\lambda t}$$

Fig. 1.13 shows the exponential PDF ( $\lambda = 1.68$ ;  $\gamma = 0.46$ ), which represents a failure in the temperature alarm.

Notice that in the figure the curve begins with a range at 0.46. This means the position parameter ( $\gamma$ ) represents how long one piece of equipment operates without failure; in other words, how long one piece of equipment has 100% reliability. This means that before parameter position value ( $\gamma$ ), equipment has 100% reliability. In this case,  $\gamma = 0.46$  (year).

When there is a position parameter, it is represented in the PDF equation by:

$$f(t) = \lambda e^{\lambda(t-\gamma)}$$

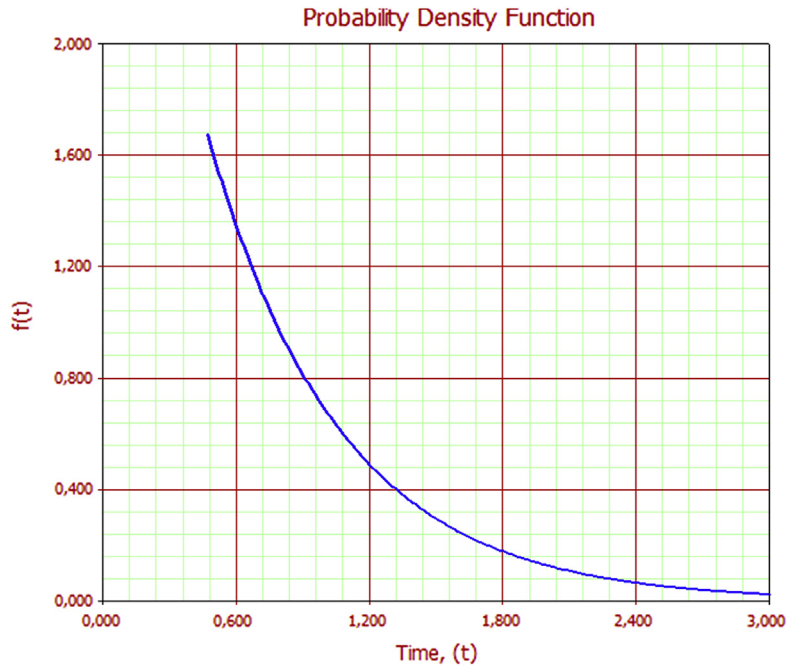


FIGURE 1.13

Exponential PDF.

This means that failure occurs randomly after a period of time and that it is observed in some electrical equipment. In some cases, parameter position ( $\gamma$ ) may represent a guaranteed time during which no equipment failures are expected; in other words, 100% reliability until time  $t = \gamma$ .

After understanding the exponential PDF it is necessary to define the reliability function, the cumulative density function (CDF), and then the failure rate and MTTF as follows:

$$R(t) + F(t) = 1$$

$$F(t) = \int_0^t f(x)dx = \int_0^t \lambda e^{-\lambda x} dx = 1 - \frac{\lambda}{\lambda} e^{-\lambda t} = 1 - e^{-\lambda t}$$

$$R(t) = 1 - F(t) = 1 - (1 - e^{-\lambda t}) = e^{-\lambda t}$$

The exponential reliability function depends only on the failure rate parameter, therefore the equation is simple. Whenever the exponential reliability function is applied to calculate equipment, product, service, or event reliability, the main assumption is that events occur randomly over time; otherwise it makes no sense to use it. Another important index is failure rate, which is obtained by dividing the PDF and reliability functions to define the failure rate, as follows:

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda$$

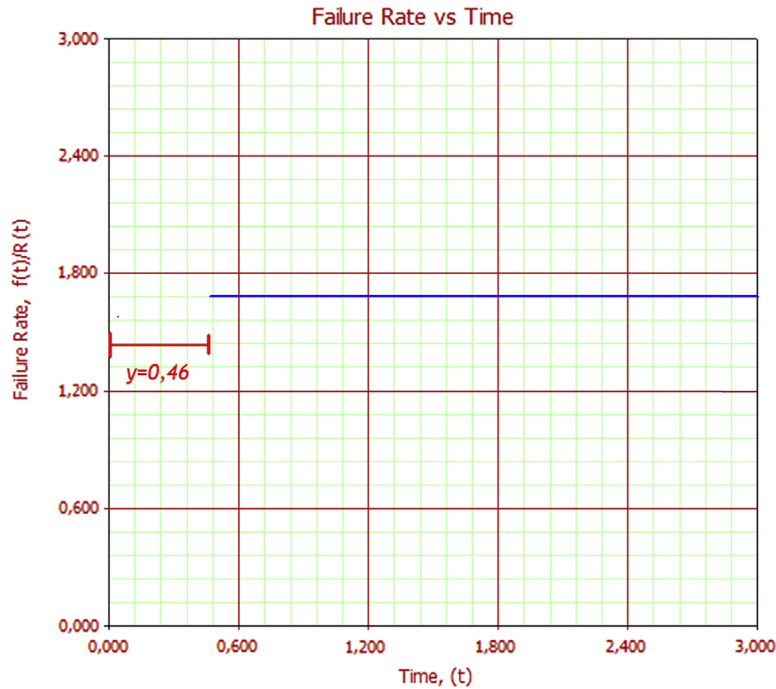
The failure rate is constant over time, as shown in Fig. 1.11. The failure rate was calculated based on the PDF and reliability function of Fig. 1.14. In doing so it is possible to see the range of time without value, which represents the position parameter ( $\gamma = 0.46$ ).

The failure rate is constant if events occur randomly over time. To calculate the MTTF applying the following equation, it is possible to see that the MTTF is the inverse of the failure rate in the exponential PDF case:

$$MTTF = \int_0^t t \cdot f(x) dx = t \int_0^t \lambda e^{-\lambda t} dt$$

$$MTTF = t \cdot \frac{\lambda}{\lambda^2 t} = \frac{1}{\lambda}$$

This happens only for the exponential PDF. Many reliability and maintenance professionals incorrectly consider the MTTF the inverse of the failure rate when the PDF is not exponential. This fact influences decisions because the MTTF cannot be constant over time if failure is not represented by the exponential PDF, which means failures are not random. In wear-out failure phases, the MTTF is lower than the previous phase, and if it has been considered constant, failure will likely occur before the time expected.



**FIGURE 1.14**  
Failure rate ( $\gamma = 0.46$ ).

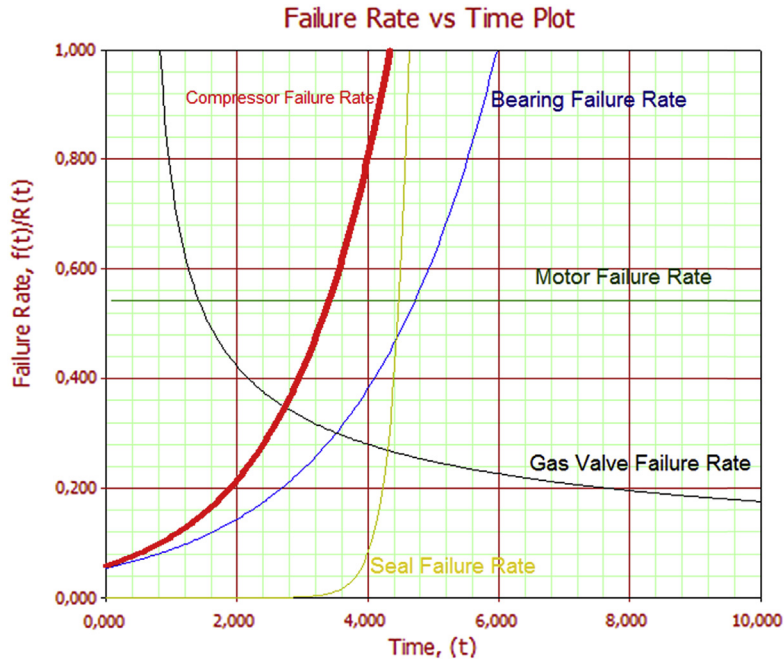


FIGURE 1.15

Gas compressor and component failure rates.

Many specialists consider the system PDF as exponential because they believe that by regarding different PDFs for each component and equipment, the system PDF shape will be exponential. In fact, this does not always happen, because depending on the life cycle time assessed, it will have different PDF configurations for the system's equipment. For example, a gas compressor with many components (eg, electric motor, bearing, valve, and seal) with a compressor failure rate is comprised of different component failure rates and will result in an increased compressor failure rate and not a constant failure rate shape, as shown in Fig. 1.15.

In a gas compressor there are components with increased failure rates, such as the seal and bearing, constant failure rates, such as the electric motor, and decreased failure rates, such as the gas valve. Including all the data to define the gas compressor failure rate the result is an increased failure rate, as shown in red in Fig. 1.15. The following section describes the normal PDF, which is used in many cases by maintenance and reliability specialists.

### 1.2.2 NORMAL PROBABILITY DENSITY FUNCTION

The normal PDF is a frequently used function because it describes the process under control, which means the variable values occur around the mean with deviation. In fact, many variables from many analyses are treated like normal distributions, but are not always well represented. Once there exists a higher deviation it is harder to predict the variable value; in the reliability case it is either failure time or repair time. In other

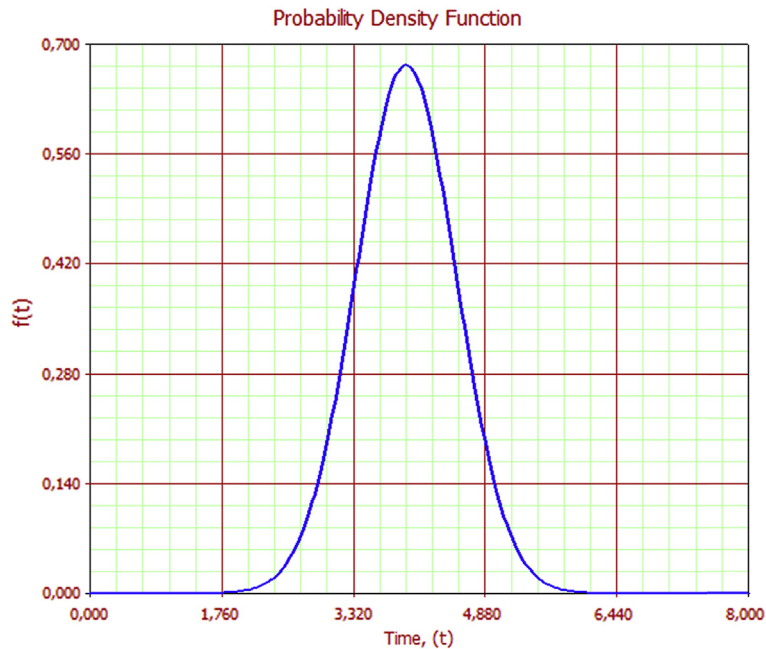
words, the less reliable the variable prediction, the less accurate the failure time or repair time value will be. Different from the usual exponential PDF, the normal PDF has two parameters: average ( $\mu$ ) and deviation ( $\sigma$ ). These are called position and scale parameters, respectively. It is important to notice that whenever  $\sigma$  decreases, the PDF is pushed toward the mean, which means it becomes narrower and taller. In contrast, whenever  $\sigma$  increases, the PDF spreads out away from the mean, which means it becomes broader and shallower. The normal PDF is represented mathematically by:

$$f(T) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{T-\mu}{\sigma}\right)^2}$$

Fig. 1.16 shows the PDF configuration in a pump seal leakage failure. As discussed, failure time averages around ( $\mu = 3.94$ ) with deviation ( $\sigma = 0.59$ ). The whole figure area represents a 100% chance of failure, and there will always be more chance of seal leakage occurring around the average. The normal reliability function is represented by:

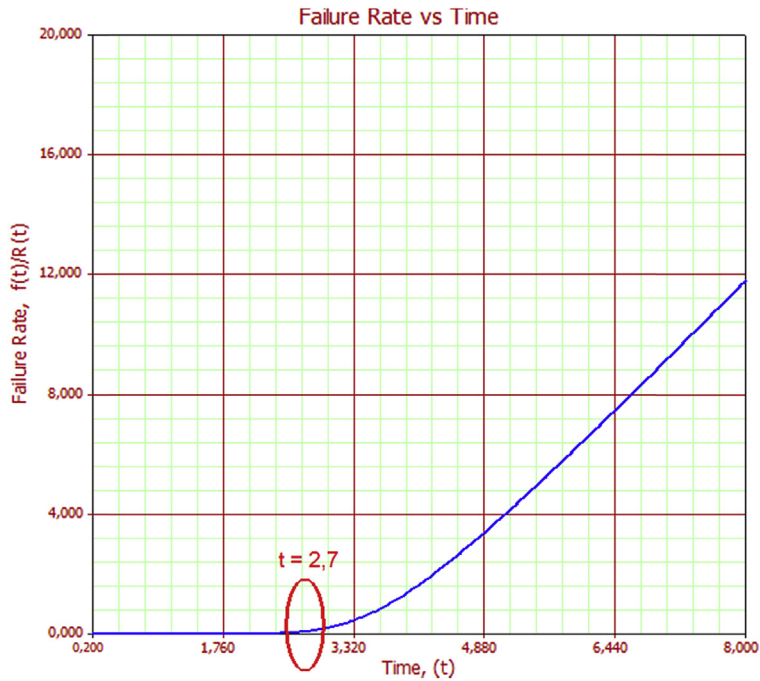
$$R(T) = \int_T^{\infty} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt$$

There are two remarkable characteristics in the normal PDF. First, the failure rate increases from one specific period of time, which represents the wear-out life characteristic in the bathtub curve. Fig. 1.17 shows an example seal leakage increased failure rate over time. In fact, there will be a constant failure rate during part of the life cycle, and such a constant failure rate before an increase in



**FIGURE 1.16**

Pump seal leakage (normal PDF).



**FIGURE 1.17**

Seal pump failure rate.

failure rate is the main objective of preventive maintenance. This means that by applying preventive maintenance it is possible to avoid increased failure rate or wear-out for a period of the equipment life cycle. To prevent the wear-out life cycle, inspections and preventive maintenance must be conducted before the increased failure rate time begins, and that is a good contribution the reliability engineer can give to maintenance equipment policies. The second remarkable point is that in the normal PDF the MTTF is similar to the mean. Only in this case, the mean average is similar to the expected number of failures.

The pump seal leakage failure rate is increased, which represents the wear-out life cycle. Nevertheless, the wear-out life cycle does not mean the equipment has to be replaced. In fact, after repair, depending on equipment degradation and maintenance efficiency, most equipment can recover to almost 100% of initial reliability. To define inspection and maintenance periods of time, the failure rate must be assessed, and in the seal leakage example, 2.7 years is the time during which the failure rate starts to increase, so a specific time must be defined before 2.7 years to perform an inspection of the seal, and if necessary conduct preventive maintenance. In fact, inspection and maintenance will be conducted for different component failure rates and such data will provide input information for maintenance professionals to plan their inspection and maintenance routines over time. In addition to recovering reliability in equipment, there will be one period of time during which operational costs will increase, and in this case such equipment must be replaced. This is the replacement optimum time approach, explained in Chapter 6.

### 1.2.3 LOGISTIC PROBABILITY DENSITY FUNCTION

The logistic PDF is very similar to the normal PDF in shape and also describes the process under control, with a simple mathematical concept. The logistic parameters are mean ( $\mu$ ) and deviation ( $\sigma$ ), and the variable values, failure, or repair time, for example, vary around deviation. Despite having a similar shape the logistic PDF shape looks like a normal PDF. As in the normal PDF case, the less reliable the variable prediction is, the less reliable the failure time or repair time value will be. Similar to the normal PDF the logistic PDF has two parameters: mean ( $\mu$ ) and deviation ( $\sigma$ ), which are also called position and scale parameters, respectively. It is important to notice that whenever  $\sigma$  decreases, the PDF is pushed toward the mean, which means it becomes narrower and taller. In contrast, whenever  $\sigma$  increases, the PDF spreads out away from the mean, which means it becomes broader and shallower.

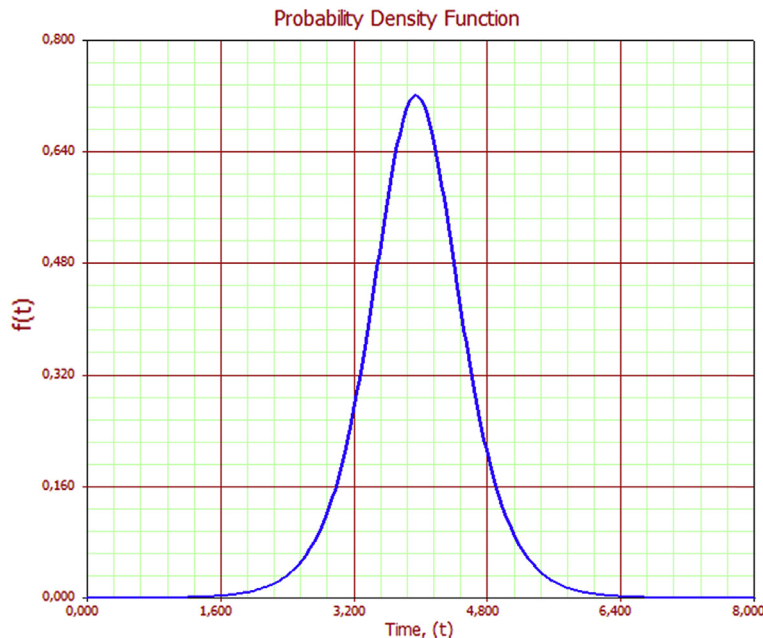
The logistic PDF is represented mathematically by the equation:

$$f(t) = \frac{e^z}{\sigma(1 + e^z)^2}$$

where:

$$z = \frac{t - \mu}{\sigma}$$

Fig. 1.18 shows the PDF configuration, for example, in seal pump leakage failure data, this time using the logistic PDF ( $\mu = 3.94$ ;  $\sigma = 0.347$ ). As discussed, failure varies around the average. The



**FIGURE 1.18**

Pump seal leakage (logistic PDF).

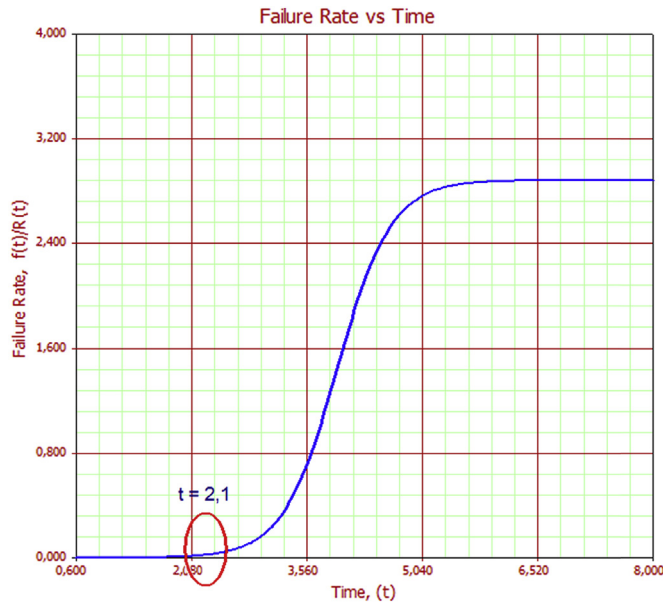


whole figure area represents 100% chance of failure, and there will always be more chance of seal leakage occurring around the average. The reliability logistic PDF is represented by:

$$R(t) = \frac{1}{1 + e^z}$$

Similar to the normal PDF the failure rate increases from one specific period of time  $t$ , which represents the wear-out life characteristic bathtub curve. In fact, there will be part constant failure rate, and this is better than an increased failure rate, and preventive maintenance tries to keep equipment in useful life and avoid wear-out. To prevent the wear-out life cycle, inspection and preventive maintenance must be conducted beforehand, and this is a good way reliability engineers can enhance maintenance policies. As before, the MTTF is similar to the mean. Only in this case the mean average is similar to the expected number of failures. Fig. 1.19 shows the pump seal failure rate as an example increasing over time from 2.1 to 5.6 years and then staying constant.

Despite the similarity in the PDF shapes presented in Figs. 1.16 and 1.18, the failure rate presented in Fig. 1.17 is different from the failure rate presented in Fig. 1.19. In the logistic case the point to expect inspection and maintenance is 2.1 years, earlier than the 2.7 years presented in the normal failure rate figure. Despite the same failure data there are some differences between the results that can influence decisions when different PDFs are taken into account, even when they are very similar, as with the normal and logistic PDFs.



**FIGURE 1.19**

Pump seal failure rate (logistic PDF).

### 1.2.4 LOGNORMAL PROBABILITY DENSITY FUNCTION

The lognormal PDF shapes tell us that most failures occur at the beginning of the life cycle and happen most often because the project was not good, the startup equipment was incorrect, operation of the equipment capacity was poor, or the equipment was built incorrectly. All this has great influence on equipment failure occurring at the beginning of a piece of equipment's life cycle. The lognormal PDF has two parameters: average ( $\mu$ ) and deviation ( $\sigma$ ), which are called position and scale parameters, respectively. It is important to notice that whenever  $\sigma$  decreases, the PDF is pushed toward the mean, which means it becomes narrower and taller. In contrast, whenever  $\sigma$  increases, the PDF spreads out away from the mean, which means it becomes broader and shallower. Different from normal and logistic distribution the lognormal PDF is skewed to the right, and because of the effect of scale parameters, equipment has more of a chance of failing at the beginning of the life cycle. Mathematically, the lognormal PDF is represented by the function:

$$f(T') = \frac{1}{\sigma_{T'}} e^{-\frac{1}{2} \left( \frac{T' - \mu'}{\sigma_{T'}} \right)^2}$$

where:  $\sigma_{T'} = Ln\sigma_T$ ;  $T' = LnT$ ;  $\mu' = \mu$ .

The lognormal reliability function is represented by the equation:

$$R(T') = \int_T^{\infty} \frac{1}{\sigma' \sqrt{2\pi}} e^{-\frac{1}{2} \left( \frac{t' - \mu'}{\sigma'} \right)^2} dt$$

A real example of lognormal can be applied to repair time. In fact, using lognormal to represent repair time suggests that repair is most often performed for a shorter period of time by experienced employees and takes longer for inexperienced employees. Fig. 1.20 shows valve repair time represented by the lognormal PDF. In fact, in many cases a valve is repaired in a warehouse and replaced with a new one so as to not shut down any process.

The lognormal PDF describes well the repair time because represent that most of repairs are done in a short period of time and a small number of repair takes a longer time. Even though, it is also possible to describe repair time based on another PDF functions.

The repair time can be represented by the normal PDF for example. That means, the repair time is always done during an average time with a standard deviation. In this case, the employees take a similar amount of time to repair equipment.

As discussed the lognormal PDF best represents failures at the beginning of the life cycle and those that occur, for example, in tower distillation in refinery plants when oil specification has changed. In this case the lognormal PDF represents the corrosion in the tower, as shown in Fig. 1.21.

This is why it is so important to understand exactly why failures occur. In this example the failure occurred before the expected time because of a bad decision to accept a different oil specification in the distillation plant. The expected PDF for corrosion is Gumbel, which means that such a failure mode would happen only in a wear-out life cycle, or in other words at the end of equipment life.

Another important point to understand is failure rate behavior over time. The lognormal failure rate increases over time, and after a specific period of time decreases, as shown in Fig. 1.22. That time represents control time and it reduces failures at the beginning of the equipment life cycle. The best way to stop failures is to use proper startup equipment and keep a quality procedure in place to detect quality failure.

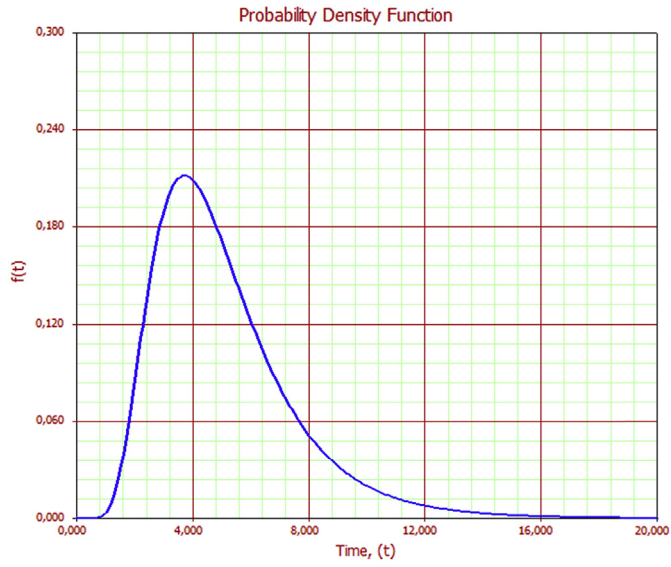


FIGURE 1.20

Valve repair time PDF.

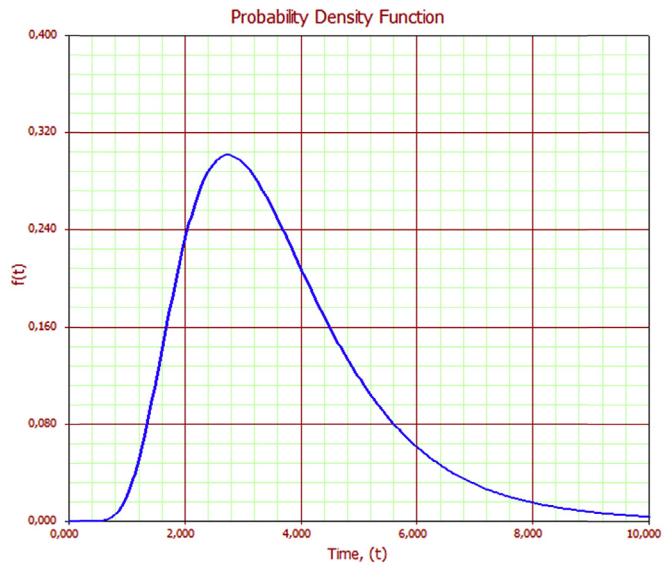
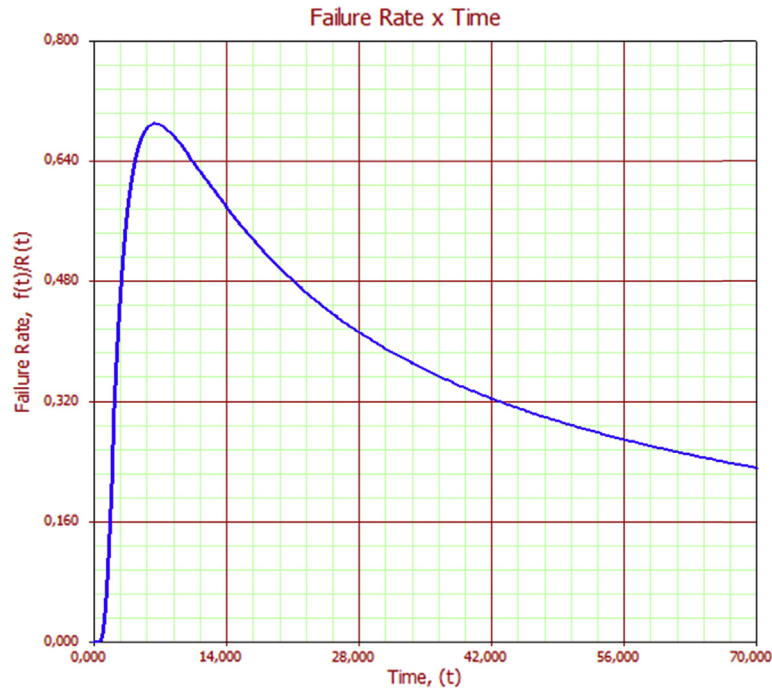


FIGURE 1.21

Furnace corrosion lognormal PDF.

**FIGURE 1.22**

Furnace corrosion failure rate  $\times$  time (lognormal).

The lognormal distribution is unwanted in all systems because it means equipment failure at the beginning of the life cycle. To avoid this it is necessary to be careful in assembly and startup, and operate and perform maintenance at the beginning of the equipment life cycle. Some equipment has lower reliability than expected and has lognormal distribution. In many cases, when this happens there is not enough time to perform maintenance. In other situations, to save money and reduce costs, maintenance and operation services from suppliers are not taken into account in purchase orders, even when the maintenance team is not familiar with new equipment; consequently repair quality is poor and longer shutdown as well as equipment failing come sooner than expected.

### 1.2.5 LOGLOGISTIC PROBABILITY DENSITY FUNCTION

The loglogistic PDF, like the lognormal PDF shape, shows that most failures occur at the beginning of the life cycle and happen for the same reasons discussed before. The loglogistic PDF has two parameters: average ( $\mu$ ) and deviation ( $\sigma$ ), which are called position and scale parameters, respectively. Again, whenever  $\sigma$  decreases, the PDF is pushed toward the mean, which means it becomes narrower and taller. And again, in contrast, whenever  $\sigma$  increases, the PDF spreads out away from the mean,

which means it becomes broader and shallower. The loglogistic PDF is also skewed to the right, and because of this, equipment will often fail at the beginning of the life cycle, as in the lognormal PDF case. Mathematically, loglogistic PDFs are represented by:

$$f(t) = \frac{e^z}{\sigma t(1 + e^z)^2}$$

where:

$$z = \frac{\ln t - \mu}{\sigma}$$

and  $t$  = life cycle time.

The loglogistic reliability function is represented by the equation:

$$R(T) = \frac{1}{1 + e^z}$$

For example, Fig. 1.23 shows the loglogistic PDF that also represents corrosion in a furnace. Note that there is little difference between the lognormal PDF (gray) and the loglogistic PDF (black).

Also note the loglogistic failure rate and its behavior over time. The loglogistic failure rate as well as the lognormal failure rate increase over time, and after specific periods of time decrease, as shown in Fig. 1.24. Comparing the loglogistic failure rate (black line) with the lognormal failure rate (gray line) it is possible to see in Fig. 1.24 that the loglogistic failure rate decreases faster than the logistic failure

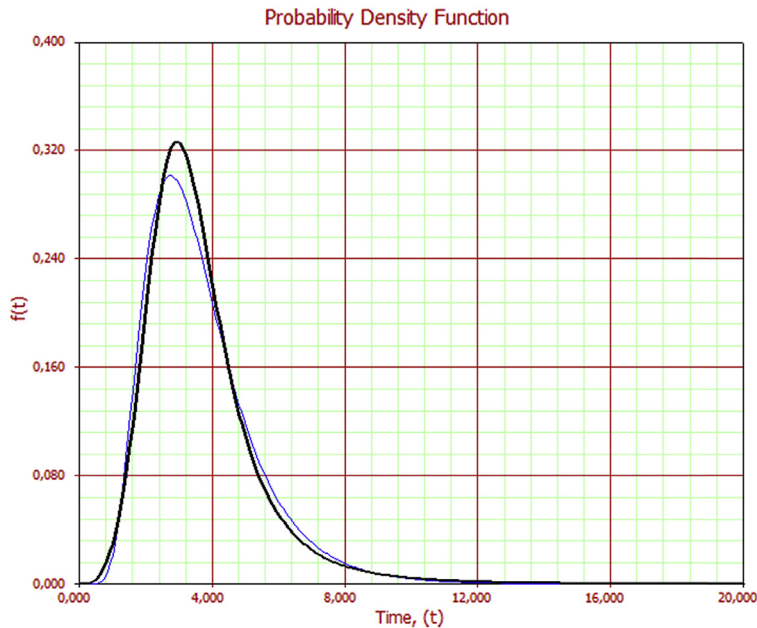
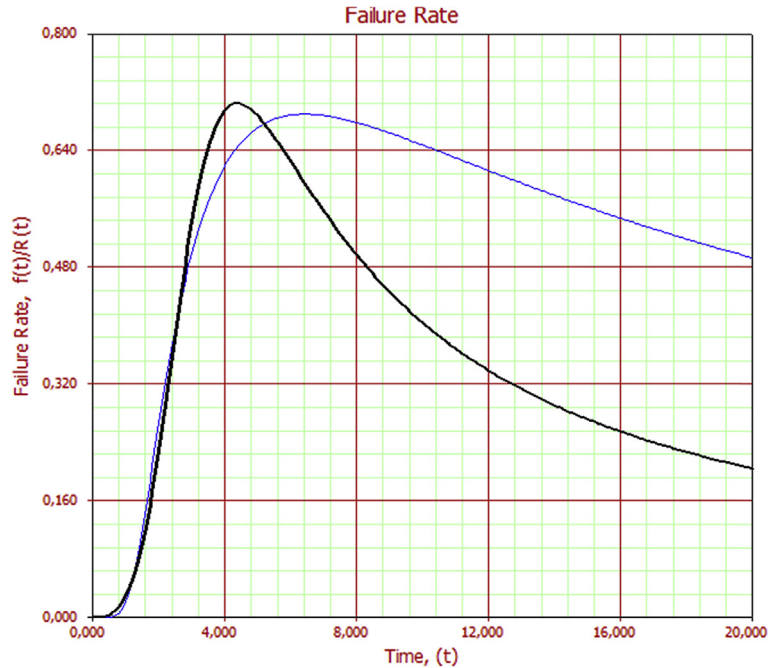


FIGURE 1.23

Furnace corrosion loglogistic PDF.



**FIGURE 1.24**

Furnace corrosion failure rate  $\times$  time (loglogistic—black line).

rate, even using the same historical failure data. Thus it is important to pay attention and choose the PDF that fits the historical failure data better to make the best decisions. We will now discuss the Gumbel PDF, which is skewed to the left, having the opposite mean of the lognormal and loglogistic distributions.

### 1.2.6 GUMBEL PROBABILITY DENSITY FUNCTION

The Gumbel, or smallest extreme value, PDF is the opposite of the lognormal PDF in terms of shape. The curve shape is skewed to the left because most of the failures occur at the end of the life cycle, which represents the robustness of equipment such as vessels and tanks.

The Gumbel PDF has two parameters: average ( $\mu$ ) and deviation ( $\sigma$ ), which are called position and scale parameters, respectively. Whenever  $\sigma$  decreases, the PDF is pushed toward the mean and becomes narrower and taller. Whenever  $\sigma$  increases, the PDF spreads out away from the mean and becomes broader and shallower. Different from the lognormal and loglogistic distributions, the Gumbel PDF is skewed to the left and scale parameters are on the right, so the equipment has a higher chance of failing at the end of the life cycle. Mathematically, the Gumbel PDF is represented by:

$$f(t) = \frac{1}{\sigma} e^{-e^{\frac{t-\mu}{\sigma}}}$$

where:

$$z = \frac{T - \mu}{\sigma}$$

The Gumbel reliability function is represented by:

$$R(T) = e^{-e^z}$$

An example of a Gumbel failure is when a tower in a hydrogen generation unit has external corrosion. Such failures occur around 18 years of operation, despite maintenance during the life cycle. Fig. 1.25 shows corrosion in the tower.

The failure rate behavior over time has some similarity to the normal and logistic PDFs because after constant value the failure rate starts to increase in a specific period of time. Despite the similarity, in the Gumbel failure rate function, when the failure rate starts to increase it is mostly during the wear-out period. In other words, in normal and logistic PDFs, if maintenance was conducted before the increased failure rate period, the equipment will recover some reliability. That does not usually occur in the Gumbel PDF, mainly for vase and tank failure modes. Some pumps and compressors have component failures skewed to the left, and they are well represented by the Gumbel PDF. It is possible to perform maintenance in such equipment and recover part of its reliability.

The Gumbel failure rate is constant most of time, and after a specific period of time increases, as shown in the example of external corrosion in the tower of the hydrogen generation plant in Fig. 1.26.

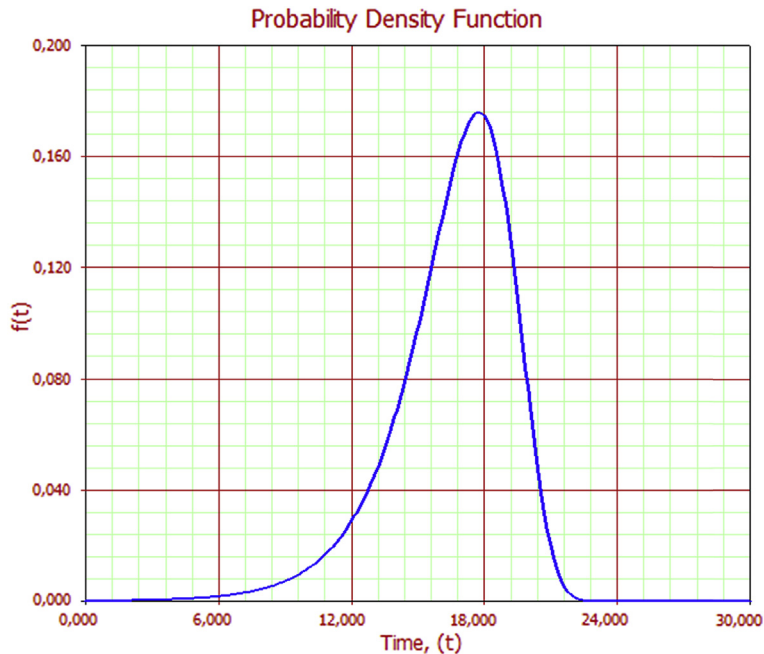
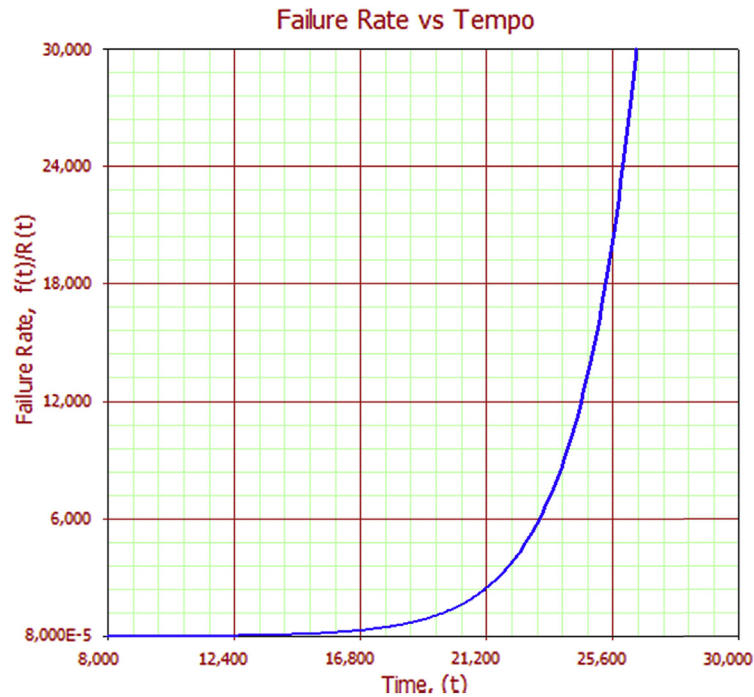


FIGURE 1.25

Furnace external corrosion Gumbel PDF.





**FIGURE 1.26**

Furnace corrosion failure rate  $\times$  time (Gumbel).

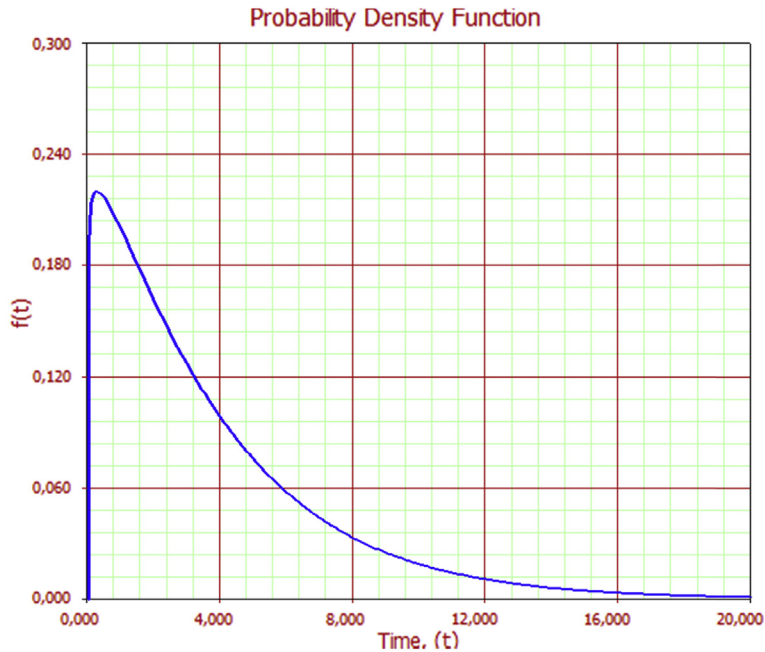
The following PDFs are generic, which means such functions can represent different PDFs depending on the characteristic and combination parameters. The generic PDFs are Weibull, gamma, and generalized gamma. The first one is more predicabile than the last two, as will be shown.

### 1.2.7 WEIBULL PROBABILITY DENSITY FUNCTION

The first generic PDF to be discussed is the Weibull function, which can represent exponential, lognormal, or normal shape characteristics. The Weibull PDF can have any of those characteristics, which means a random failure occurrence over the life cycle, or failure occurrence at the beginning of the life cycle with failure time skewed to the right on average with deviation or failure occurrence around a specific period of time centralized in the average with deviation. The Weibull PDF shape behavior depends on the shape parameter ( $\beta$ ), which can be:

- $0 < \beta < 1$  (asymptotic shape)
- $\beta = 1$  (exponential asymptotic shape)
- $1 < \beta < 2$  (lognormal shape)
- $\beta > 2$  (normal shape)

Regarding shape parameter, as the beta value becomes higher, the PDF shape starts to change from normal shape to Gumbel shape. Fig. 1.27 shows the lognormal PDF characteristic when failures



**FIGURE 1.27**

Furnace burner damage (Weibull PDF).

occur at the beginning of the life cycle. In this case, furnace burner damage may occur, as it did in the distillation furnace after 2 years of operation because of high temperatures in the furnace operation. This is another example of why it is so important to know exactly why a failure is occurring. In this case the failure occurred before the expected time because a different oil specification was used in the distillation plant. The expected PDF for burner damage is Gumbel, which means that such a failure would happen only in the wear-out life cycle, or in other words at the end of a piece of equipment's life.

The Weibull PDF has three parameters: a shape parameter ( $\beta$ ), a characteristic life parameter ( $\eta$ ), and a position parameter ( $\gamma$ ). If the position parameter is zero, the Weibull PDF has two parameters. The characteristic life or scale parameter means that 63.2% of failures will occur until the  $\eta$  value, that is, a period of time. The position parameter represents how long equipment has 100% reliability; in other words there will be no failure until the  $\gamma$  value, which is a certain period of time. In doing so the Weibull PDF is represented by:

$$f(t) = \frac{\beta}{\eta} \left( \frac{T - \gamma}{\eta} \right)^{\beta-1} e^{-\left( \frac{T-\gamma}{\eta} \right)^{\beta-1}}$$

where  $\beta > 0$ ,  $\eta > 0$ , and  $\gamma > 0$ .

The Weibull reliability function is represented by the equation:

$$R(T) = e^{-\left(\frac{T-\gamma}{\eta}\right)^\beta}$$

The Weibull failure rate function is represented by the equation:

$$\lambda(T) = \frac{\beta}{\eta} \left(\frac{T-\gamma}{\eta}\right)^{\beta-1}$$

The Weibull two-parameter PDF in Fig. 1.27 has parameter values  $\beta = 1.06$  and  $\eta = 3.87$ . Look at the shape parameter. When  $1 < \beta < 2$  the PDF shape looks like the lognormal PDF and the characteristic life is  $\eta = 3.87$ , which means that until 3.87 years 63% failure will occur.

The failure rate shape in the Weibull function depends on the shape parameter ( $\beta$ ), which can be constant over time, constant part of the time, and increasing from a specific time ( $t$ ), or decreasing part of the time and after a specific time ( $t$ ) to be constant; that is, respectively, exponential, normal, and lognormal behavior.

The advantage of Weibull over other generic PDFs such as gamma and generalized gamma is that by looking at the parameters it is easy to have a clear idea about the shapes.

Despite this it represents different PDFs well, but that is not to say that Weibull distributions are best in all cases. In some cases, despite the similarity with other PDFs, it would be better to use other PDFs that best fit the data. This will be discussed in the next section.

**Mixed Weibull Probability Density Function**

The mixed Weibull density function has the special characteristic to provide information of different subpopulations inside the sample data assessed. In other words, if equipment historical data is assessed for lifetime data analysis, different subpopulations, such as components, can be characterized based on Weibull parameters. Therefore depending on the  $K$  number of subpopulations, there will be a  $K$  number of parameters as follows:

The  $K$  subpopulation is represented by:

$$N_1, N_2, N_3, \dots, N_K$$

The Weibull parameters for  $K$  subpopulations are represented by:

$$(\beta_1, \eta_1, \gamma_1), (\beta_2, \eta_2, \gamma_2), (\beta_3, \eta_3, \gamma_3), \dots, (\beta_K, \eta_K, \gamma_K)$$

In doing so the Weibull density function is represented by the equation:

$$f(t) = \sum_{i=1}^K \frac{N_i \beta_i}{N \eta_i} \left(\frac{T-\gamma_i}{\eta_i}\right)^{\beta_i-1} e^{-\left(\frac{T-\gamma_i}{\eta_i}\right)^{\beta_i-1}}$$

where  $\beta > 0$ ,  $\eta > 0$ , and  $\gamma > 0$ .

The Weibull reliability function is represented by the equation:

$$R(T) = \sum_{i=1}^K \frac{N_i}{N} e^{-\left(\frac{T-\gamma_i}{\eta_i}\right)^{\beta_i}}$$

The Weibull failure rate function is represented by the equation:

$$\lambda(T) = \frac{f_{1,2,3...K}(T)}{R_{1,2,3...K}(T)}$$

$$\lambda(T) = \frac{\frac{N_1}{N}f_1(T) + \frac{N_2}{N}f_2(T) + \frac{N_3}{N}f_3(T) + \dots + \frac{N_K}{N}f_K(T)}{\frac{N_1}{N}R_1(T) + \frac{N_2}{N}R_2(T) + \frac{N_3}{N}R_3(T) + \dots + \frac{N_K}{N}R_K(T)}$$

An example of mixed Weibull analysis is demonstrated in Fig. 1.28, when a lifetime data analysis was performed for a refinery pump that shows three subpopulations represented by black, red, and green colors plotted on an unreliability × time function.

The parameters for each population are, respectively:

- Population 1 ( $\beta = 1, \eta = 1, \gamma = 1$ )
- Population 2 ( $\beta = 2, \eta = 2, \gamma = 2$ )
- Population 3 ( $\beta = 3, \eta = 3, \gamma = 1$ )

The population 1 parameters define the early life failure based on a  $\beta$  value lower than 1 ( $\beta = 0.85$ ). In addition, it is possible to define 24.5% of the chance that failure will happen in years based on the  $\eta$  value ( $\eta = 45.43$ ).

The population 2 parameters define the wear out failure pattern based on a  $\beta$  value lower than 1 ( $\beta = 5.1$ ). In addition, it is possible to define 36.73% of the chance that failure will happen in years based on the  $\eta$  value ( $\eta = 315.14$ ).

The population 3 parameters define the early life failure based on a  $\beta$  value lower than 1 ( $\beta = 0.72$ ). In addition, it is possible to define 38.77% of the chance that failure will happen in years based on the  $\eta$  value ( $\eta = 4100.8$ ).

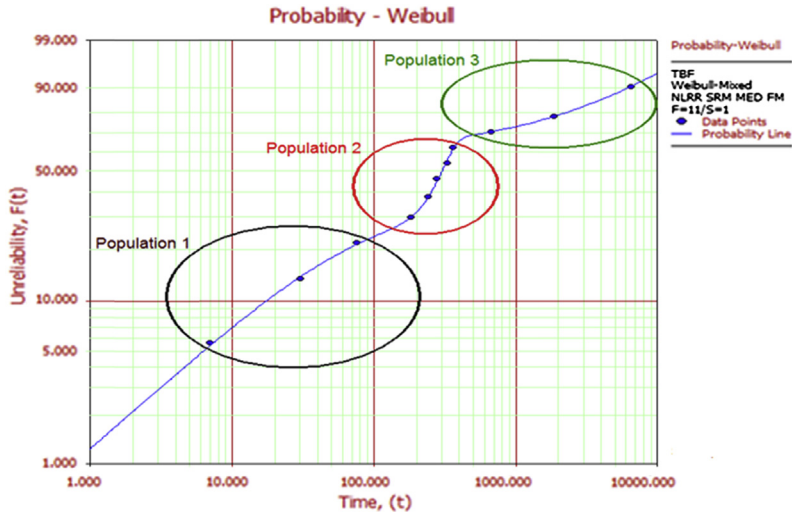


FIGURE 1.28

Pump mixed Weibull PDF.

### 1.2.8 GAMMA PROBABILITY DENSITY FUNCTION

The second generic PDF is the gamma, which, like the Weibull distribution, can represent exponential, lognormal, or normal shape characteristics. The gamma PDF can have any of those characteristics, which means random failure occurrence over the life cycle, or failure occurrence at the beginning of the life cycle with failure time skewed to the right on average with deviation or failure occurrence around a specific period of time centralized in the average with deviation. The gamma PDF shape behavior depends on the shape parameter ( $k$ ), which can be:

- $k < 1$  (asymptotic shape)
- $k = 1$  (exponential asymptotic shape)
- $k > 1$  (lognormal shape)

Fig. 1.29 shows different PDF shapes for the gamma PDF depending on shape parameters. From top to bottom, the first line shape looks like an asymptotic shape compared to the Weibull PDF ( $0 < \beta < 1$ ), and in this case the shape parameter of the gamma PDF is  $k = 0.2$ . The second line shape looks like the exponential PDF shape compared to the exponential or Weibull PDF ( $\beta = 1$ ), and in this case the shape parameter of the gamma PDF is  $k = 0.98 (\cong 1)$ . The third line shape looks like lognormal, and in this case the shape parameter of the gamma PDF is  $k = 1.2$ . In all three cases the location parameter is  $\mu = 3.8$ .

As with other functions, the gamma PDF has the scale parameter and the highest of such parameters in the PDF is stretched out to the right and its height decreases. In contrast a lower value of

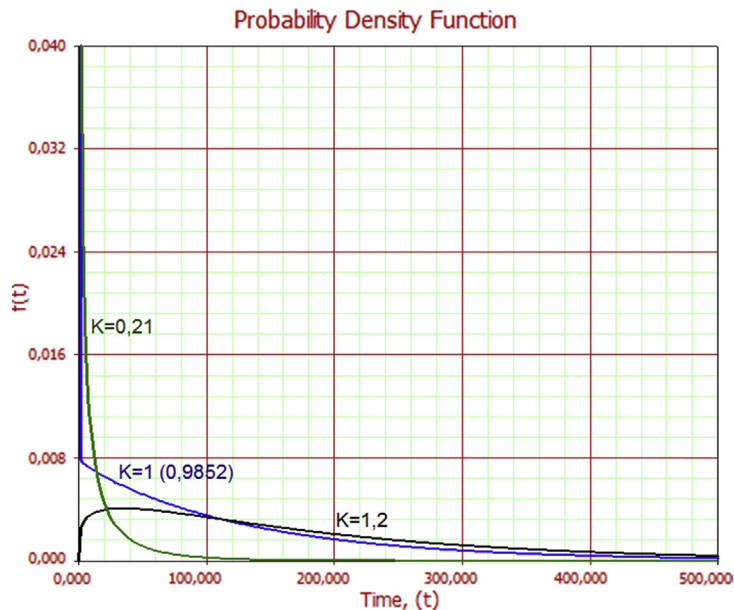


FIGURE 1.29

Gamma PDF with different shape.

the scale parameter PDF is stretched out to the left and its height increases. The gamma PDF is represented by:

$$f(t) = \frac{e^{kz - e^z}}{\Gamma(k)}$$

where  $z = Lnt - \mu$ ;  $e^\mu$  = scale parameter; and  $k$  = shape parameter.

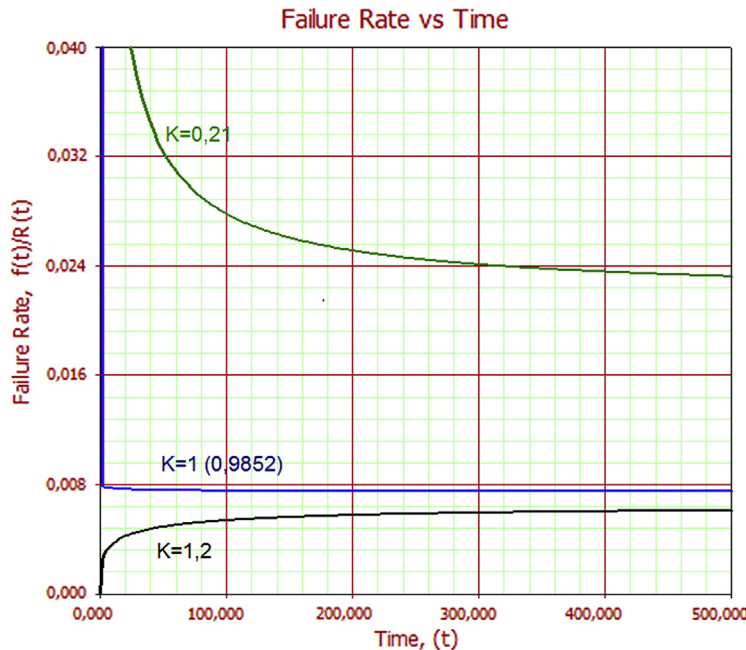
The reliability function is represented by the equation:

$$R(t) = 1 - \Gamma_1(k, e^z)$$

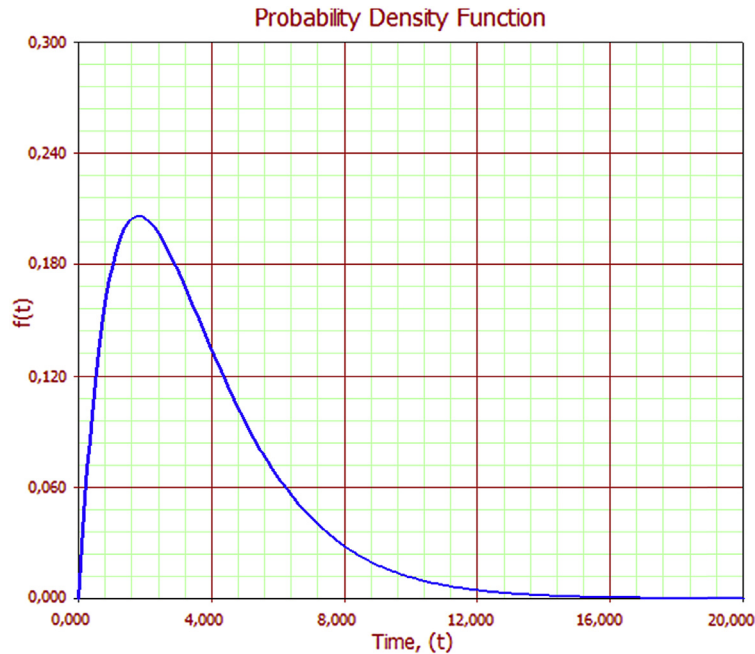
The failure rate shape in the gamma PDF also depends on the shape parameter ( $k$ ), and it can be constant over time ( $k = 0.9852$ ) (Fig. 1.29), decreasing part of the time, and constant from a specific time ( $k = 0.21$ ) (Fig. 1.29), or increasing part of the time and then being constant ( $k = 1.2$ ) (Fig. 1.29). This means, respectively, exponential, asymptotic, and lognormal behavior.

Fig. 1.30 shows different failure rate shapes, which depend on the shape parameter ( $k$ ) value. This means, respectively, exponential, asymptotic, and lognormal behavior.

A good example of the gamma PDF ( $k = 2$  and  $\mu = 0.57$ ) is a compressor in a propylene plant that fails during the first 2 years because of an incorrect startup procedure after energy shutdown. Despite energy shutdown downtime, the compressor downtime was critical because of the increased total downtime, and the situation only improved after the maintenance manager hired supplier compressor operation services. Fig. 1.31 shows the compressor failure PDF, which means energy shutdown and



**FIGURE 1.30**  
Failure rate  $\times$  time (gamma).



**FIGURE 1.31**

Energy shutdown in the compressor (gamma PDF).

human error in the startup compressor. After 3 years the startup compressor procedure conducted properly reduced downtime in energy shutdown cases. After 8 years, cogeneration energy started to supply energy to the propylene plant and energy shutdown slowed down over the years.

The next PDF is generalized gamma, which represents different PDFs; however, it is complex, and the shape depends on parameter combinations.

### 1.2.9 GENERALIZED GAMMA PROBABILITY DENSITY FUNCTION

The third generic PDF to be discussed is the generalized gamma function, which can represent different PDF distributions such as exponential, lognormal, normal, or Gumbel shape characteristics; random failures occurring over the life cycle; failures occurring at the beginning of the life cycle with the shape skewed to the right with average and deviation; failures occurring around the specific period of time centralized in the average with deviation; as well as failures occurring at the end of the life cycle with the shape skewed to the left with average and deviation, respectively. The gamma PDF shape behavior depends not only on the shape parameter ( $k$ ) value, but on a combination of shape parameters and scale parameters ( $\theta$ ), including:

- $\lambda = 1$  and  $\sigma = 1$  (exponential asymptotic shape)
- $\lambda = 0$  (lognormal shape)

When  $\lambda = \sigma$  is approximately the gamma distribution shape, it can be the exponential, lognormal, or normal shape (Pallerosi, 2007). In fact, the combination stated previously is very rare when working with data to create a gamma PDF and this makes the generalized gamma hard to predict looking at only parameter values, so it is better to look at the PDF shape by itself. Fig. 1.32 shows the generalized gamma PDF ( $\mu = 1.52$ ;  $\sigma = 0.58$ ;  $\lambda = 0.116$ ), which represents turbine blade damage failure caused by a component from a cracking catalyst plant.

The gamma PDF is represented by:

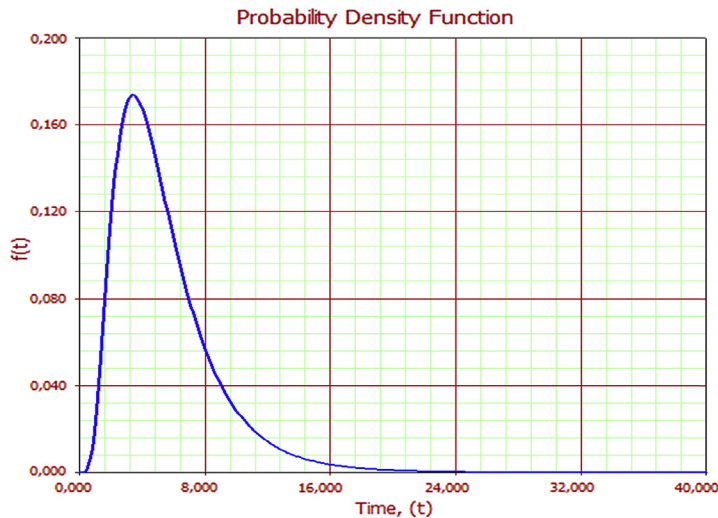
$$f(t) = \frac{\beta}{\Gamma(k) \cdot \theta} \cdot \left(\frac{t}{\theta}\right)^{k\beta-1} \cdot e^{-\left(\frac{t}{\theta}\right)^\beta}$$

where  $\theta$  = scale parameter;  $k$  = shape parameter;  $\beta$  = shape parameter;  
 and  
 $\theta, k, \beta > 0$ .  
 If:

$$\mu = Ln\theta + \frac{1}{\beta} \cdot Ln\left(\frac{1}{\lambda^2}\right)$$

$$\sigma = \frac{1}{\beta\sqrt{k}}$$

$$\lambda = \frac{1}{\sqrt{k}}$$



**FIGURE 1.32**  
 Turbine blade damage PDF (generalized gamma).



To  $\lambda \neq 0$ ,  $f(t)$  is:

$$f(t) = \frac{|\lambda|}{\sigma \cdot t} \cdot \frac{1}{\Gamma\left(\frac{1}{\lambda^2}\right)} \cdot e^{\left[ \frac{\lambda \frac{\ln t - \mu}{\sigma} + \ln\left(\frac{1}{\lambda^2}\right) - e^{\lambda \frac{\ln t - \mu}{\sigma}}}{\lambda^2} \right]}$$

To  $\lambda = 0$ ,  $f(t)$  is:

$$f(t) = \frac{1}{\sigma \cdot t \sqrt{2\pi}} \cdot e^{-\frac{1}{2} \left(\frac{\ln t - \mu}{\sigma}\right)^2}$$

The generalized gamma reliability function is represented by the following equations:

If  $\lambda < 0$ :

$$R(t) = \Gamma_I \left( \frac{e^{\lambda \left(\frac{\ln t - \mu}{\sigma}\right)}}{\lambda^2}, \frac{1}{\lambda^2} \right)$$

If  $\lambda = 0$ :

$$R(t) = 1 - \Theta \left( \frac{\ln t - \mu}{\sigma} \right)$$

If  $\lambda > 0$ :

$$R(t) = 1 - \Gamma_I \left( \frac{e^{\lambda \left(\frac{\ln t - \mu}{\sigma}\right)}}{\lambda^2}, \frac{1}{\lambda^2} \right)$$

The failure rate shape in the gamma function depends on shape parameter ( $\lambda$ ) and other parameters. Fig. 1.33 shows the compressor blade failure rate function shape, which increases at the beginning and decreases after a specific period of time ( $t = 7$ ).

After discussing the main PDF, which describes equipment failure over time and repair time, it is necessary to know how to define PDF parameters and which is the better PDF for failure or repair data, that is, the PDF that best fits the data.

### 1.2.10 RAYLEIGH PROBABILITY DENSITY FUNCTION

The fourth generic PDF function to be presented is the Rayleigh function, which may also represent different PDF distributions like exponential, lognormal, normal, or Gumbel shape characteristics. The Rayleigh probability density function is represented by the equation:

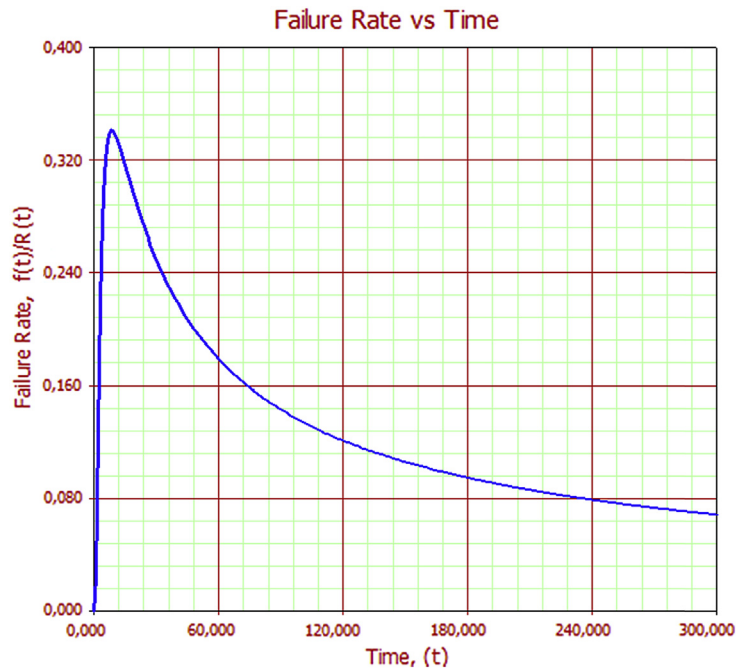
$$f(t) = \frac{t}{\sigma^2} e^{-\frac{t^2}{2\sigma^2}}$$

$$t \geq 0$$

where  $\sigma$  = scale parameter and  $X$  = location parameter.

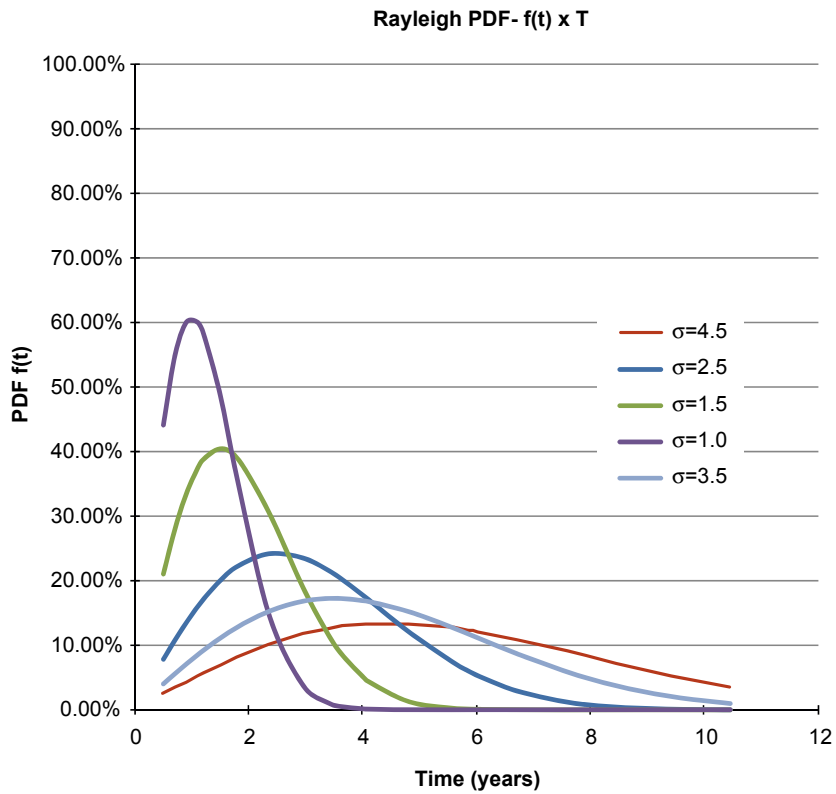
The Rayleigh CDF function is described by the equation:

$$F(t) = 1 - e^{-\frac{t^2}{2\sigma^2}}$$



**FIGURE 1.33**

Turbine blade damage failure rate function (generalized gamma).



**FIGURE 1.34**

Probability density function  $f(t)$ .

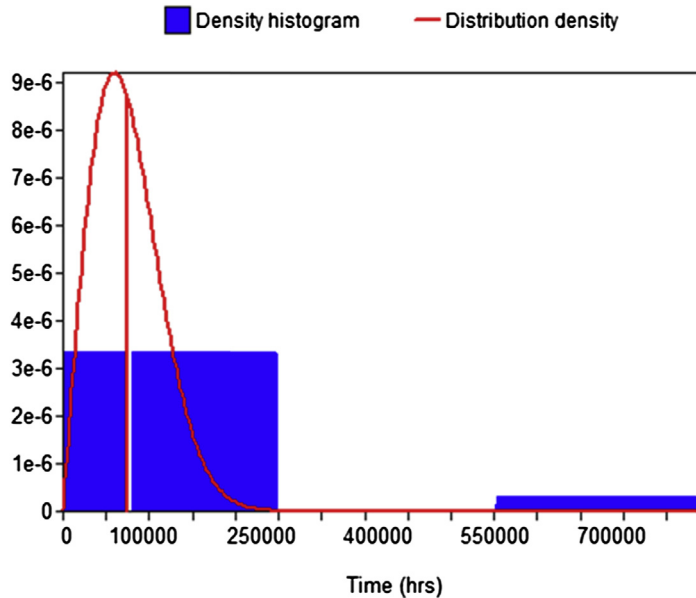


FIGURE 1.35

Pump PDF (Rayleigh).

Therefore:

$$F(t) + R(t) = 1$$

$$R(t) = 1 - F(t)$$

$$R(t) = 1 - \left(1 - e^{-\frac{t^2}{2\sigma^2}}\right)$$

$$R(t) = e^{-\frac{t^2}{2\sigma^2}}$$

The Rayleigh CDF shape behavior depends on the scale parameter ( $\sigma$ ), as shown in Fig. 1.34.

Fig. 1.34 shows Rayleigh PDF ( $\sigma = 65,927$  hours (7.5 years)) plotted on CAFDE software from BQR Reliability Engineering Consultant Ltd, which represents pump failures that happen because of bearing and seal failures. Section 1.5 will demonstrate several case studies to show how to perform lifetime data analysis. Case 1.5.1 will describe the components PDF of the pump related to Fig. 1.35.

### 1.3 GOODNESS OF FIT METHODS: HOW TO DEFINE PDF PARAMETERS AND CHOOSE PDF THAT FITS BETTER IN FAILURES DATA

After understanding the different PDF types that represent repair time or failure time, some main questions arise, such as:

- After collecting data, how do you create the PDF? How do you define the PDF parameters?
- If you have PDF parameters, how do you determine the best PDF for the failure data?
- How do you compare two or more PDFs to determine the best one for the failure or repair data?

The first question is answered with different methodologies and the most known are the plot method, the minimum quadratic approach, and the maximum likelihood method. Thus before choosing one method to define the best PDF that fits better on failure or repair data, it is necessary to define PDF parameters. There are two strategies for choosing the best PDF: the first one is to choose the PDF that best fits your data, and the second strategy is to choose the generic PDF (eg, Weibull 2P) and then look into the parameter characteristics and compare them with similar PDFs.

When using the first strategy, choosing the correct PDF depends on failure or repair data frequency over the life cycle. So the best PDF will be:

- At the beginning of the life cycle: lognormal or loglogistic;
- During a specific period of time with some equal variance on both sides: normal or logistic;
- At the end of the life cycle: Gumbel;
- Randomly occurring over the life cycle: exponential.

Generic PDFs, such as Weibull, gamma, and the generalized gamma, may also be chosen. Indeed, the strategy for choosing the PDF that best fits the frequency occurrence may be limited because the specialist may have to choose the PDF based on the equipment or component characteristics. A reliability engineer, for example, assessing the electrical equipment may be likely to choose the exponential PDF based on experience that such equipment has random failures over time or from knowledge gained from literature.

The second strategy is to define a generic PDF and look into PDF parameter characteristics; then it is possible to compare it to a similar PDF to find the one that fits better, but this is the second step after defining the PDF parameters. If a generic PDF is chosen, it is important to remember the limitations it represents for other PDFs. For example, Weibull and gamma represent the exponential PDF well, as well as the normal and lognormal PDFs, but not the Gumbel PDF very well. The generalized gamma PDF represents most PDF distributions well, but it is mathematically difficult to work with.

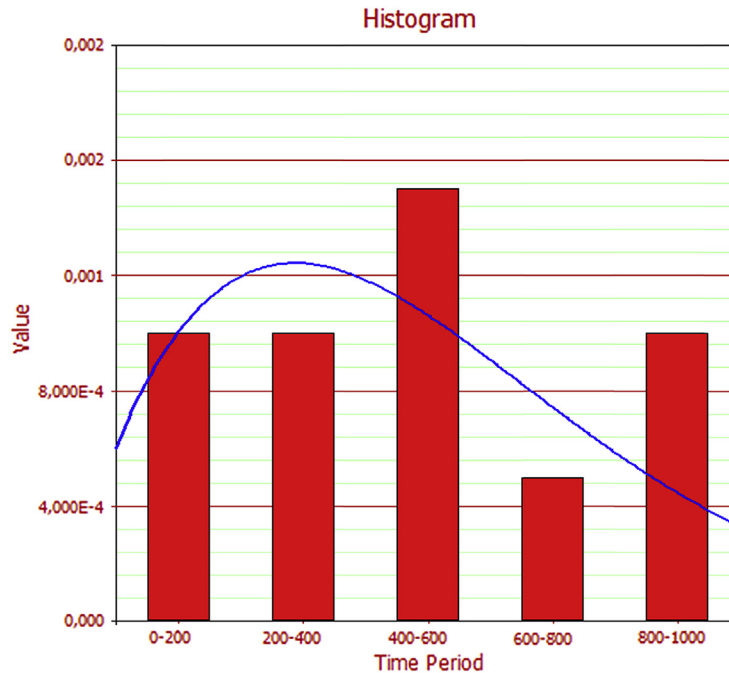
To give an example of how to approach PDF parameters, we discuss an electric compressor motor that operates in a drill facility. The electric motor historical failure data does not have exponential shape characteristics, as shown in Fig. 1.36, but the Weibull PDF is used to define parameters. So the next step is to apply the plot method, rank regression method, or the maximum likelihood method.

The electric motor histogram gives an idea of the PDF shape, but when a specialist does not have software available or has to make a fast decision, he or she will go with the generic PDF.

### 1.3.1 PLOT METHOD

The first method to define PDF parameters is the plot method, and the first step is to define the rank of the failure. Then it is necessary to define the cumulative probability of failure values for each failure time, and with plotting functions, it is possible to define the PDF parameter values. To define the cumulative probability of failure values for each failure time it is necessary to apply a median rank method with 50% confidence. The median rank equation is:

$$\sum_{k=i}^n \binom{n}{k} (MR)^k (1 - MR)^{n-k} = 0.5$$



**FIGURE 1.36**

Electric motor failure histogram.

The Bernard equation gives approximately the same values as the median rank method, and the equation is:

$$F(t_i) = \frac{i - 0.3}{n + 0.4}$$

Using data from Fig. 1.36 and applying the Bernard equation, the probability of failure in each time is given in Fig. 1.37.

Using data from Fig. 1.33 and applying the Bernard equation, the probability of failure in each time is given in Fig. 1.37.

The next step is to plot data on Weibull probability paper, for example, to obtain Weibull parameters. In doing so we are assuming that Weibull distribution will be used like PDFs and the further step is to find out which PDF fits better to the electric motor failure data. Consequently, when plotting cumulative probability failure values on Weibull paper it is possible to define the PDF parameters, as shown in Fig. 1.37. The Weibull paper is obtained by applying Log on X values and LogLog on Y values Y and X axes.

The shape parameter ( $\beta$ ) is a slope of linear function. The scale parameter, or characteristic life ( $\eta$ ), is defined when it goes to 63% of failure and graphically when the Y axis meets the function with a direct line from 63% in the Y axis and then meets the value in the X axis, which is the life characteristic

Time to Failure ( <i>h</i> )	Failure Order	<i>F</i> ( <i>t</i> )
58	1	6.7%
180	2	16.3%
216	3	26%
252	4	35.6%
421	5	45.2%
515	6	54.8%
571	7	64.4%
777	8	74%
817	9	83.7%
923	10	93.3%

FIGURE 1.37

Cumulative probability of failure (Bernard equation).

parameter value ( $\eta$ ). The position parameter is defined by the difference of the first *X* value from the first curve (*X*1) and the first *X* value from the adjusted curve (*X*2), as shown in Fig. 1.38. If the adjusted line is on the right, the position value is negative, and if it is on the left, the position parameter value is positive.

The plotted methodology can be applied for all PDFs; it depends on the strategy used to define the PDF that best fits the failure or repair data. As discussed, when a generic PDF such as Weibull is

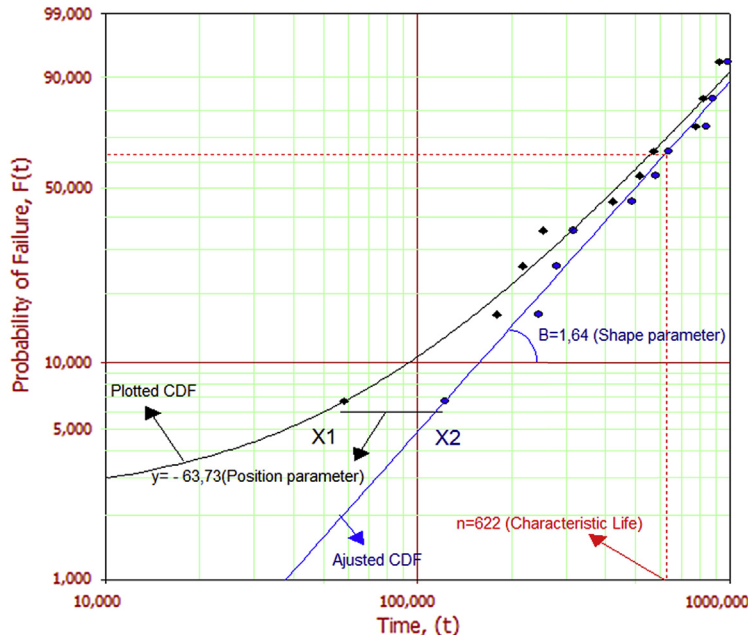


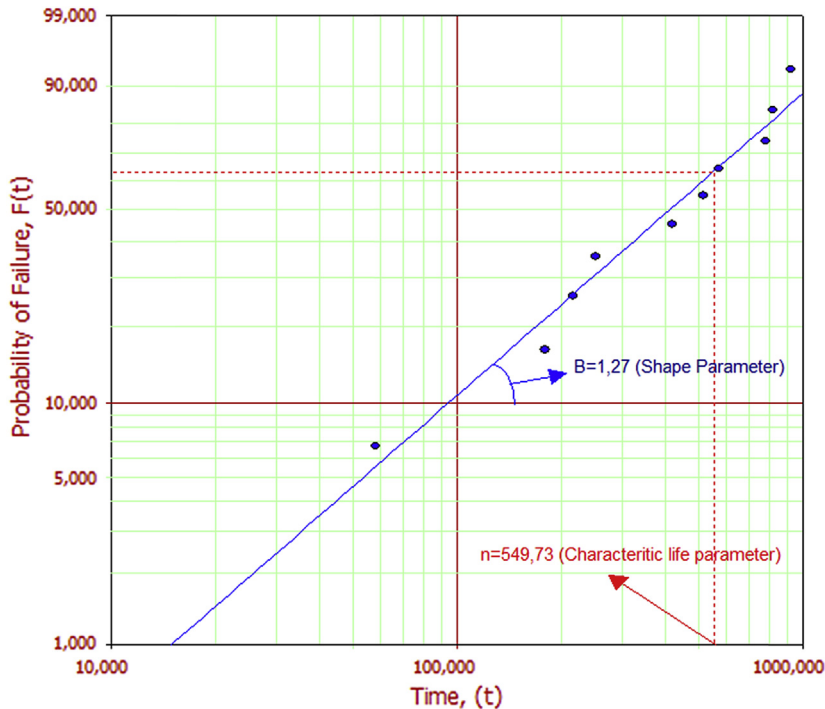
FIGURE 1.38

Plotted Weibull 3P CFD and parameters.

chosen, look at the parameter characteristics to more easily identify the PDF shape. In the electric motor case the three Weibull parameters are  $\beta = 1.64$ ,  $\eta = 622$ , and  $\gamma = -63.73$ . This means the PDF shape looks like a lognormal PDF ( $1 \leq \beta \leq 2$ ). The characteristic parameter ( $\eta$ ) means that 63% of failure will occur until 622 h, and the position parameter ( $\gamma$ ) means that at 63.73 in the time period the equipment starts to degrade. Because it is a negative value, degradation will begin before equipment starts to work. In real life, this means degradation will occur while equipment is in stock or transported to the warehouse.

If we do not consider Weibull 3P, it means we are considering Weibull 2P, the shape parameter. ( $\beta$ ) will be 1.27 and the characteristic life ( $\eta$ ) parameter will be 549. In this case the Weibull 2P parameters are  $\beta = 1.27$  and  $\eta = 549$ . This means the PDF shape also looks like the lognormal PDF ( $1.2 \leq \beta \leq 2.5$ ). The characteristic parameter ( $\eta$ ) means that 63% of failures will occur until 549 hours. The Weibull 2P parameter value is very similar to the Weibull 3P parameter value. Fig. 1.39 shows the Weibull 2P plotted.

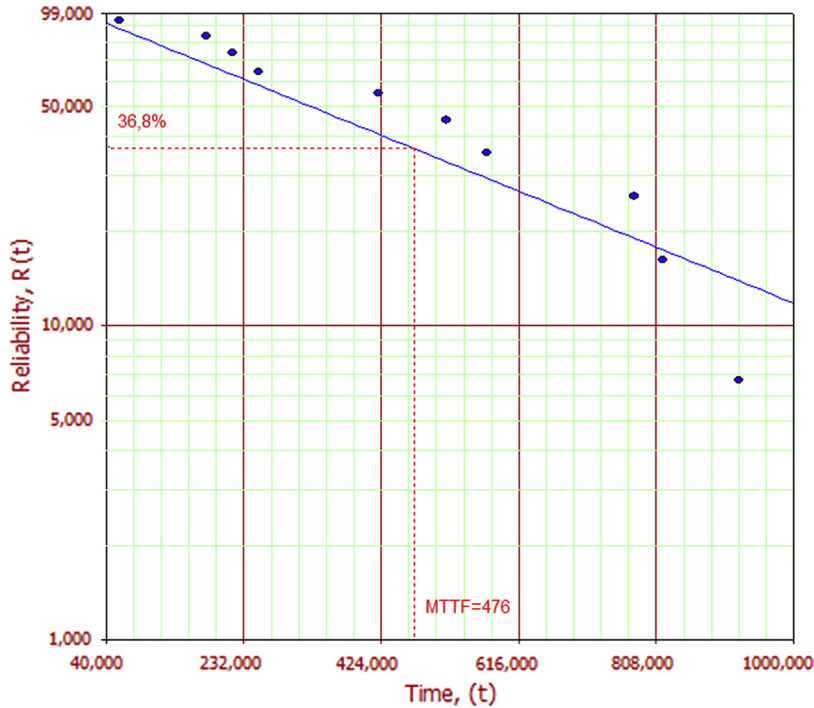
In the end, because it is electrical equipment, it would be helpful to think in regard to exponential distribution, so in this case there is only one parameter to estimate when the CDF is plotted, and that is MTTF. To define the MTTF value it is necessary to define the value of  $R(t)$ . So regarding  $t = \text{MTTF}$  it is possible to define  $R(t)$  when substituting  $t$  in the reliability equation. Further, looking at the graph shown in Fig. 1.39 and regarding such an  $R(t)$  value, then dropping down to the X scale in the



**FIGURE 1.39**

Plotted Weibull 2P CFD and parameters.

reliability curve on the graph, it is possible to define the MTTF, which is a time value, as shown in Fig. 1.40. So when  $t = \text{MTTF}$ :



**FIGURE 1.40**  
Plotted exponential CDF and parameter.

In fact, because it is electrical equipment, it feasible to regard to exponential distribution to represents this equipment. Therefore, in this case, there is only one parameter to estimate when the CDF is plotted, and that is MTTF. To define the MTTF value plotted in the exponential CDF it is necessary to define the value of  $F(t)$ . Drawing a line from such value to meet the CDF equation and then dropping down to the X scale results in MTTF, as shown in Fig. 1.40. So when  $t = \text{MTTF}$ :

$$R(t) = e^{-\lambda t}$$

$$\lambda = \frac{1}{\text{MTTF}}$$

If  $t = \text{MTTF}$ :

$$R(t) = e^{-\frac{1}{\text{MTTF}}t} = e^{-\frac{1}{\text{MTTF}}\text{MTTF}} = e^{-1} = 0.368$$

The MTTF value is 476 hours. To define the parameter in the normal and logistic PDFs after plotting the CDF, it is necessary to go to the Y axis line in 50% of failure probabilities and when the line drops down to the X axis in the X scale. That is, the average ( $\mu$ ) in the normal distribution meets the CDF line and drops down until meeting the X-valued average ( $\mu$ ) in the normal distribution. In the lognormal distribution it is necessary to apply  $\ln$  in such a value.



The plot method is a good first step, because it is not possible to compare two or more PDFs to know which one best fits the failure or repair data. That is only possible using the following methods, because the plot method is only a visual representation of how well data is adjusted to linear functions and gives PDF parameters.

### 1.3.2 RANK REGRESSION

Rank regression is often used instead of least squares or linear regression because values of Y come from median rank regression in the Y scale. The rank regression method defines the best straight line that has the best distance between the setup point and the line (function) having the Y or X scale as a reference. This methodology is not applied to Weibull 3P, gamma, and generalized gamma, because in those cases it is not possible to use linear regression. The first step of the rank regression method is to create a linear function applying ln on both the CDF equation sides and then to define the linear parameters for the Y (or X) value. The rank regression equations are:

$$\sum_{i=1}^N (A + Bx_i - y_i)^2 = \min(a, b) \sum_{i=1}^N (a + bx_i + y_i)$$

where A and B are the estimation of the a and b values based on the following equations:

$$A = \frac{\sum_{i=1}^N y_i}{N} + B \frac{\sum_{i=1}^N x_i}{N} = Y - BX$$

$$B = \frac{\sum_{i=1}^N x_i y_i - \frac{\sum_{i=1}^N x_i \sum_{i=1}^N y_i}{N}}{\sum_{i=1}^N x_i^2 - \frac{(\sum_{i=1}^N x_i)^2}{N}}$$

Applying such an equation to Weibull 2P, as discussed previously, the first step is to turn the Weibull 2P into a linear equation, so:

$$F(T) = 1 - e^{-\left(\frac{T}{\eta}\right)^\beta}$$

$$1 - F(T) = e^{-\left(\frac{T}{\eta}\right)^\beta}$$

$$\ln(1 - F(T)) = \ln\left(e^{-\left(\frac{T}{\eta}\right)^\beta}\right)$$

$$\ln(1 - F(T)) = \ln e^{-\left(\frac{T}{\eta}\right)^\beta}$$

$$\ln(1 - F(T)) = -\left(\frac{T}{\eta}\right)^\beta$$

$$\ln(-\ln(1 - F(T))) = \ln\left(\frac{T}{\eta}\right)^\beta$$

$$n(-\ln(1 - F(T))) = \beta \ln\left(\frac{T}{\eta}\right)$$

$$\ln(-\ln(1 - F(T))) = \beta \ln T - \beta \ln \eta$$

By applying CDF values of the electric motor in rank regression methodology it is possible to estimate the Weibull 2P parameters. Table 1.2 makes obtaining such parameters easy.

So turns out in linear equation the linear function parameters are:

$$Y = \ln(-\ln(1 - F(T)))$$

$$A = -\beta \ln \eta$$

$$B = \beta$$

In doing so, applying CDF values of the electric motor in rank regression methodology it is possible to estimate Weibull 2P parameters. Table 1.2 allows obtaining such parameters easily.

Observing the values in Table 1.2 and substituting in the following equations, the parameters are:

$$B = \frac{\sum_{i=1}^N x_i y_i - \frac{\sum_{i=1}^N x_i \sum_{i=1}^N y_i}{N}}{\left(\frac{\sum_{i=1}^N x_i}{N}\right)^2} \quad A = \frac{\sum_{i=1}^N y_i}{N} - B \frac{\sum_{i=1}^N x_i}{N} = Y - BX$$

$$B = \frac{-22.31 - \frac{58.98(-5.23)}{10}}{354.61 - \frac{(58.98)^2}{10}} = \frac{-22.31 + 30.84}{354.61 - 347.86} = \frac{8.53}{6.75} = 1.26$$

and:

$$A = \frac{-5.23}{10} - 1.26 \cdot \frac{58.98}{10} = -0.523 - 7.42 = -7.94$$

$$A = -\beta \ln \eta$$

$$\eta = e^{\frac{-A}{\beta}} = e^{-\frac{(-7.94)}{1.26}} = e^{6.30} = 544$$

N	t <sub>i</sub>	ln(t <sub>i</sub> )	F(t <sub>i</sub> )	V <sub>i</sub>	(ln t <sub>i</sub> ) <sup>2</sup>	V <sub>i</sub> <sup>2</sup>	(ln t <sub>i</sub> )V <sub>i</sub>
1	58	4.060443	0.07	2.66384	16.4872	7.09606	10.8164
2	180	5.1911196	0.16	1.72326	26.94772	2.969636	8.94567
3	216	5.3754988	0.26	1.20202	28.89599	1.44486	6.46147
4	252	5.5299484	0.36	0.82167	30.58033	0.675136	4.54377
5	421	6.0419514	0.45	0.5086	36.50518	0.258669	3.07291
6	515	6.2450896	0.55	0.23037	39.00114	0.053068	1.43865
7	571	6.348131	0.64	0.032925	40.29877	0.001084	0.209012
8	777	6.6559322	0.74	0.299033	44.30143	0.089421	1.990343
9	817	6.7060262	0.84	0.593977	44.97079	0.352809	3.983227
10	923	6.828099	0.93	0.992689	46.62294	0.985431	6.778178
S	4731.5927	58.982239	5	5.23113	354.6115	13.92617	22.3181

To know and understand how well data fits in the Weibull 2P function the correlation defined by the following equation will give absolute values between zero and one, and in this case, no matter if the value is positive or negative, how close the correlation value is to one the better the correlation it is. Whenever the correlation is positive, when one variable value increases or decreases, the other variable value increases or decreases as well. Whenever the correlation is negative, when one variable value increases, the other variable value decreases and vice versa. Positive correlation means that two variables are directly correlated; in other words, if one variable value increases, the other variable will increase too. Negative correlation means that variables have inverse correlation, so while one variable value increases, the other variable value will decrease. The correlations coefficient is calculated by the following equation (electric motor):

$$\rho = \frac{\sum_{i=1}^N x_i y_i - \frac{\sum_{i=1}^N x_i \sum_{i=1}^N y_i}{N}}{\sqrt{\left(\sum_{i=1}^N x_i^2 - \frac{\left(\sum_{i=1}^N x_i\right)^2}{N}\right) \cdot \left(\sum_{i=1}^N y_i^2 - \frac{\left(\sum_{i=1}^N y_i\right)^2}{N}\right)}}$$

$$\rho = \frac{-22.31 - \frac{(58.98 \cdot (-5.23))}{10}}{\sqrt{\left(354.61 - \frac{3478}{10}\right) \cdot \left(13.92 - \frac{27.36}{10}\right)}} = \frac{-22.31 + 30.84}{\sqrt{(6.81) \cdot (11.18)}} = \frac{8.53}{8.72} = 0.98$$

Applying the rank regression method in an exponential PDF using the failure data from the last example (electric motor) we have:

$$F(T) = 1 - e^{-\lambda t}$$

$$1 - F(T) = e^{-\lambda t}$$

$$\ln(1 - F(T)) = \ln(e^{-\lambda t})$$

$$\ln(1 - F(T)) = -\lambda t$$

$$Y = A + Bx$$

$$Y = \ln(1 - F(T))$$

$$B = -\lambda$$

$$A = 0$$

In doing so, applying the values of [Table 1.3](#) in the equation allows us to obtain such an exponential parameter ( $\lambda$ ).

Observing the values in [Table 1.3](#) and substituting in the following equations:

$$B = \frac{\sum_{i=1}^N x_i y_i}{\sum_{i=1}^N x_i^2} = \frac{-59.95}{354.61} = -0.169$$

$$\lambda = -B = -(-0.17) = 0.17$$

**Table 1.3 Rank Regression to Electric Motor Failure Data (Exponential PDF)**

$N$	$t_i$	$\ln(t_i)$	$F(t_i)$	$V_i$	$(\ln t_i)^2$	$V_i^2$	$(\ln t_i)V_i$
1	58	4.060443	0.07	0.06968	16.4872	0.004855	0.28293
2	180	5.1911196	0.16	0.17848	26.94772	0.031856	0.92653
3	216	5.3754988	0.26	0.30059	28.89599	0.090352	1.6158
4	252	5.5299484	0.36	0.4397	30.58033	0.193335	2.43151
5	421	6.0419514	0.45	0.60134	36.50518	0.361609	3.63326
6	515	6.2450896	0.55	0.79424	39.00114	0.630822	4.96012
7	571	6.348131	0.64	1.03347	40.29877	1.068066	6.56062
8	777	6.6559322	0.74	1.34855	44.30143	1.818598	8.97588
9	817	6.7060262	0.84	1.81118	44.97079	3.280364	12.1458
10	923	6.828099	0.93	2.69848	46.62294	7.281798	18.4255
S	4731.5927	58.982239	5	9.27571	354.6115	14.76166	59.958

To check the correlation of failure data to the exponential PDF the correlation coefficient equation is applied:

$$\rho = \frac{\sum_{i=1}^N x_i y_i - \frac{\sum_{i=1}^N x_i \sum_{i=1}^N y_i}{N}}{\sqrt{\left( \sum_{i=1}^N x_i^2 - \frac{\left( \sum_{i=1}^N x_i \right)^2}{N} \right) \cdot \left( \sum_{i=1}^N y_i^2 - \frac{\left( \sum_{i=1}^N y_i \right)^2}{N} \right)}}$$

$$\rho = \frac{-59.95 - \frac{(58.98 \cdot (-9.27))}{10}}{\sqrt{\left( 354.61 - \frac{3478}{10} \right) \cdot \left( 14.76 - \frac{86.03}{10} \right)}} = \frac{-59.95 + 54.67}{\sqrt{(6.81) \cdot (6.15)}} = \frac{-5.28}{6.47} = -0.81$$

Comparing both results, in exponential PDF  $\rho = 0.81$  is obtained, which is less than  $\rho = 0.98$  from Weibull 2P. This means failure data fits better in Weibull 2P PDF than in exponential PDF.

### 1.3.3 MAXIMUM LIKELIHOOD METHODS

The maximum likelihood method is another approach used to define PDF parameters and understand how historical failure data fits PDFs. To define parameters by this method it is necessary to define the maximum likelihood estimation (MLE) function that defines the main variable based on several values related to such a variable. This method can be applied to all PDFs, and, depending on the number of variables, may be easier or harder to work with. The MLE function is:

$$L(\theta_1, \theta_2, \theta_3 \dots \theta_n / x_1, x_2, x_3 \dots x_n) = \prod_{i=1}^n f(\theta_1, \theta_2, \theta_3 \dots \theta_k; x_i)$$

$$i = 1, 2, 3 \dots n$$

To find the variable value it is necessary to find the maximum value related to one parameter and that is achieved by performing partial derivation of the equation as follows:

$$\frac{\partial(\wedge)}{\partial(\theta_j)} = 0$$

$$j = 1, 2, 3, 4 \dots n$$

where:

$$\wedge = \ln L$$

$$L = \prod_{i=1}^n f(\theta_1, \theta_2, \theta_3 \dots \theta_k; x_i)$$

$$\ln L = \ln \left( \prod_{i=1}^n f(\theta_1, \theta_2, \theta_3 \dots \theta_k; x_i) \right)$$

$$\ln L = \sum_{i=1}^n f(\theta_1, \theta_2, \theta_3 \dots \theta_k; x_i)$$

$$\wedge = \sum_{i=1}^n f(\theta_1, \theta_2, \theta_3 \dots \theta_k; x_i)$$

To illustrate this method the electric motor failure data will be used to estimate the exponential PDF. In the exponential PDF case there is only one variable to be estimated, which is  $\lambda$ . In doing so, perform the preceding equation steps:

$$\wedge = \ln L$$

$$L = \prod_{i=1}^n \lambda e^{-\lambda t_i} = \lambda^n e^{-\lambda \sum_{i=1}^n t_i}$$

$$\ln L = \ln \left( \lambda^n e^{-\lambda \sum_{i=1}^n t_i} \right)$$

$$\ln L = n \ln(\lambda) - \lambda \sum_{i=1}^n t_i$$

$$\wedge = n \ln(\lambda) - \lambda \sum_{i=1}^n t_i$$

$$\frac{\partial(\wedge)}{\partial(\lambda)} = \frac{n}{\lambda} - \sum_{i=1}^n t_i$$

$$\frac{\partial(\wedge)}{\partial(\lambda)} = 0$$

$$\frac{n}{\lambda} - \sum_{i=1}^n t_i = 0$$

$$\lambda = \frac{n}{\sum_{i=1}^n t_i} = \frac{10}{(58 + 180 + 216 + 252 + 421 + 515 + 571 + 777 + 817 + 923)} = 0.0021$$

This means 0.0021 failures per hour, or MTTF = 4731 hours.

$$\hat{\Lambda} = n \ln(\lambda) - \lambda \sum_{i=1}^n t_i = (10 \cdot \ln(0.0021) - (0.0021)(4731)) = -61.65 - 9.93 = -71.59$$

If we need to compare two or more PDFs to decide which one best fits the failure data we only look at the MLE value. In this case, if the other PDFs have an MLE higher than  $-71.59$ , such PDF is a better fit to the electric motor failure data.

Currently, reliability professionals have software to perform life cycle analysis, and they can easily define the better PDF for failure or repair data.

### 1.3.4 CHI SQUARE METHODS

The chi square method is one more possibility to assess the data goodness of fit and find out if such data fits the expected PDF or not. Such assessment is based on comparing the real data values and predicted values. The parameter used is frequency, which is a measure of goodness of fit and accounts for the difference between expected and observed frequencies each squared and divided by the expectation, as shown in the equation:

$$\chi^2 = \sum_{i=1}^n \frac{(O_i - E_i)^2}{E_i}$$

where  $\chi^2$  = chi square value;  $O_i$  = observed frequency; and  $E_i$  = expected frequency.

The expected value is calculated by the equation:

$$E_i = \left( \frac{F(UL_i) - F(LL_i)}{N} \right)$$

where  $F$  = the cumulative distribution function for the distribution being tested;  $UL_i$  = the upper limit for class  $i$ ;  $LL_i$  = the lower limit for class  $i$ ; and  $N$  = the sample size.

The chi square value ( $\chi^2$ ) represents the discrepancy between the observed value and the expected value. Thus the higher the chi square value, the higher will be a chance to reject the PDF tested.

The second step of chi square is to proceed with the hypothesis test based on an acceptable error, which is defined as the risk that is considered accept to face to take the final decision related to accepting or rejecting the PDF.

The additional parameter is the number of degrees of freedom “ $\alpha$ ,” usually given by  $(N - n - 1)$ , where “ $N$ ” is the number of observations and “ $n$ ” is the number of fitted parameters. The chi square value related to degree of freedom ( $\alpha$ ) must be defined based on the values in [Table 1.4](#).

**Table 1.4 Chi Square Critical Values**

		Chi Square Values				
	$\alpha$	0.100	0.050	0.025	0.010	0.005
→	1	0.1000	0.0500	0.0250	0.0100	0.0050
	2	2.7055	3.8415	5.0239	6.6349	7.8794
	3	4.6052	5.9915	7.3778	9.2103	10.5966
	4	6.2514	7.8147	9.3484	11.3449	12.8382
	5	7.7794	9.4877	11.1433	13.2767	14.8603
	6	9.2364	11.0705	12.8325	15.0863	16.7496
	7	10.6446	12.5916	14.4494	16.8119	18.5476
	8	12.0170	14.0671	16.0128	18.4753	20.2777
	9	13.3616	15.5073	17.5345	20.0902	21.9550
	10	14.6837	16.9190	19.0228	21.6660	23.5894

Based on Table 1.4, the value of  $\chi^2 = 0.1$ , considering  $\alpha = 1$  and a 90% confidence level. The degree of freedom ( $\alpha$ ) depends on the number of observations and fitted characteristic as discussed previously.

The last step is to apply the hypothesis null test ( $H_0$ ) to decide if the data (PDF) is accepted or rejected. Therefore if:

$$H_0: \chi^2 < \chi^2_{\alpha}$$

The hypothesis is accepted and the PDF has a goodness of fit to the historical data collected.

To have a better understanding about the chi square test, let us consider the following historical failure data collected from a compressor’s sensor, as shown in Table 1.5.

Based on chi square methodology the following steps are summarized in Table 1.6 such as:

- First: It is necessary to define different classes of interval for the historical data (column 2).
- Second: Calculate the exponential PDF parameters based on historical data (MTTF = 7.37).
- Third: For each class of interval (column 2) it is necessary to predict the CDF (column 3) and PDF values (column 4).

**Table 1.5 Compressor’s Sensor Observed Data**

Observed Data							
0.52	1.65	1.73	1.85	2.45	2.56	2.59	2.95
3.25	3.54	3.56	4.18	4.25	4.38	4.61	4.99
5.23	5.56	6.02	7.33	7.56	7.65		9.45
10.23	11.01		11.8	12.13		12.78	16.92
17.11	20.23	21.2	21.32	22.34	22.56		34.49

Row	Interval End Value	CDF	PDF	Expected	Observed	Chi Square
1	3	0.277704398	0.2777044	9.997358	8	0.3990494
2	5	0.418533162	0.1408288	5.069836	8	1.6935192
3	9.5	0.643058202	0.224525	8.082901	7	0.145081
4	17	0.841735018	0.1986768	7.152365	6	0.1856653
5	35	0.977526296	0.1357913	4.888486	7	0.9120393
					<b>Sum</b>	<b>3.3353542</b>

PDF, Probability density function; CDF, cumulative density function.

- Fourth: Calculate the expected values (column 4  $\times$  total number of data).
- Fifth: Define the number of observed values for each interval (column 6).
- Sixth: Calculate the chi square value (column 7).

The final step is to compare the calculated value with the value defined in Table 1.7. Therefore, considering 95% of confidence and 3 degrees of freedom ( $N - n - 1 = 3 - 1 - 1$ ). The value defined in Table 1.7 is 5.9915.

The final step is now complete when performing the null hypothesis:

$$H_0: \chi^2 < \chi_\alpha^2$$

$$H_0: 3.23 < 5.9$$

The conclusion is that the sensor failure historical data has a goodness of fit for exponential PDF. In fact, different PDFs would be assumed in this example; in this case the same methodology would be applied to check the null hypothesis.

### 1.3.5 KOLMOGOROV—SMIRNOV METHOD

The Kolmogorov—Smirnov method (K—S test) is also another goodness of fit method that compares the maximum distance between the experimental cumulative distribution function and the theoretical cumulative distribution function. The maximum discrepancy is defined by the equation:

$$D_{n,n^r} = \sup_x |F_{1,n}(x) - F_{2,n^r}(x)|$$

where  $F_{1,n}$  = experimental distribution;  $F_{2,n^r}$  = theoretical distribution; and  $\sup$  = supremum function.

The graphical representation that describes the K—S test is demonstrated in Fig. 1.41, which demonstrates the maximum discrepancy  $D$ .

To perform the goodness of fit test, similar to the other methods, the null hypothesis must be applied. Therefore whenever the maximum discrepancy between the experimental and theoretical CDF is smaller than normally expected for a given sample, the theoretical distribution is acceptable for



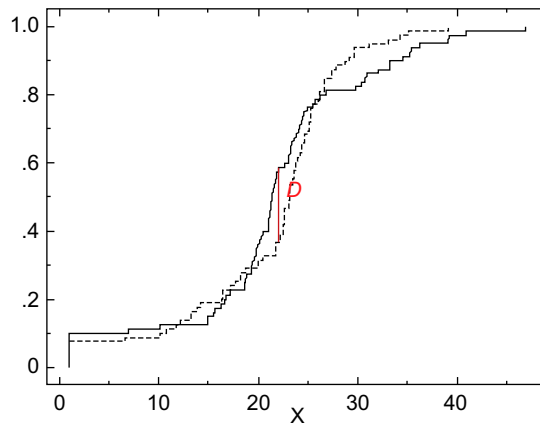
**Table 1.7 Chi Square Critical Value**

		Chi Square Values				
		↓				
	$\alpha$	0.100	0.050	0.025	0.010	0.005
→	1	0.1000	0.0500	0.0250	0.0100	0.0050
	2	2.7055	3.8415	5.0239	6.6349	7.8794
	3	4.6052	5.9915	7.3778	9.2103	10.5966
	4	6.2514	7.8147	9.3484	11.3449	12.8382
	5	7.7794	9.4877	11.1433	13.2767	14.8603
	6	9.2364	11.0705	12.8325	15.0863	16.7496
	7	10.6446	12.5916	14.4494	16.8119	18.5476
	8	12.0170	14.0671	16.0128	18.4753	20.2777
	9	13.3616	15.5073	17.5345	20.0902	21.9550
	10	14.6837	16.9190	19.0228	21.6660	23.5894

modeling the underlying population considering a certain confidence level.  $H_0$  is accepted at level  $\alpha$  as described in the equation:

$$D_{n,n^\tau} < C(\alpha) \sqrt{\frac{n + n^\tau}{nn^\tau}}$$

where  $D_{n,n^\tau}$  = maximum discrepancy;  $C(\alpha)$  = critical value of  $N$  sample size and ( $\alpha$ ) confidence level;  $n$  = number of elements on theoretical sample; and  $n^\tau$  = number of elements on experimental sample.



**FIGURE 1.41**

Kolmogorov–Smirnov method (K–S test) comparison cumulative plot.

The  $C(\alpha)$  is defined for different confidence level ( $\alpha$ ) and sample size element, as shown in Table 1.8.

Table 1.8 shows that  $C(\alpha) = 0.9$ , considering the sample of 1 and  $\alpha = 0.20$ .

To understand the K–S test the sample of pump electrical motor failures, which is assumed to have a goodness of fit in an exponential PDF with MTTF = 2.5 years, is tested based on the K–S test, as demonstrated in Table 1.9.

Column 1 demonstrates the time in years and column 2 shows the theoretical unreliability based on exponential CDF for each interval of time. Column 3 shows the experimental unreliability and column 4 shows the difference between the values in columns 2 and 3. Fig. 1.42 shows the graphical representation of the K–S test applied to calculate the maximum discrepancy.

The last step is to perform the null hypothesis test based on the following equation. Considering  $n = 6$  and  $\alpha = 0.05$ , the critical value is  $C(\alpha) = 0.521$ :

$$D_{n,n^c} < C(\alpha) \sqrt{\frac{n + n^c}{nn^c}}$$

$$0.285 < 0.521 \sqrt{\frac{6 + 6}{6 \times 6}}$$

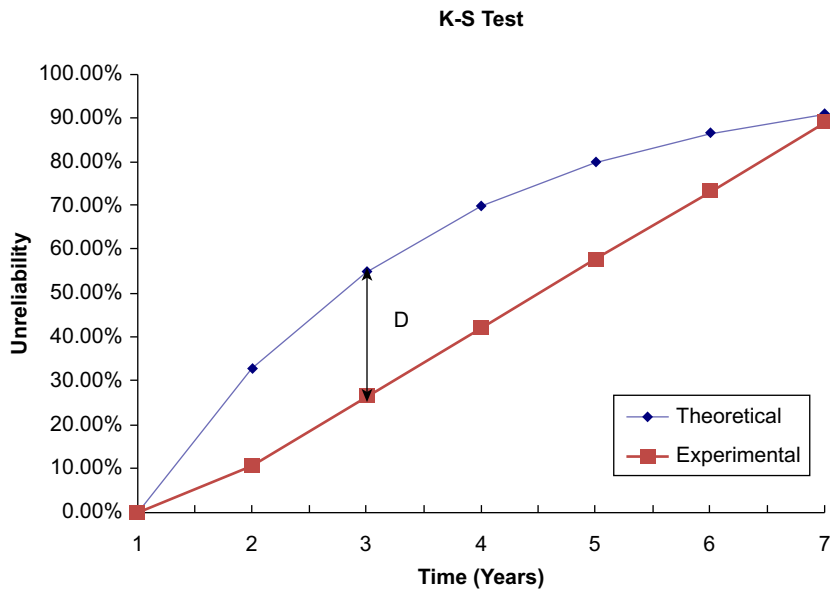
$$0.285 < 0.3007$$

The final result means that the null hypothesis is accepted; in other words, the exponential PDF fits well for the pump electrical motor failure data with 95% of confidence.

	Sample Size $N$	Significance Level $\alpha$				
		0.20	0.15	0.10	0.05	0.01
→	1	0.900	0.925	0.950	0.975	0.995
	2	0.684	0.726	0.776	0.842	0.929
	3	0.565	0.597	0.642	0.708	0.829
	4	0.494	0.525	0.564	0.624	0.734
	5	0.446	0.474	0.510	0.563	0.669
	6	0.410	0.436	0.470	0.521	0.618
	7	0.381	0.405	0.438	0.486	0.577
	8	0.358	0.381	0.411	0.457	0.543
	9	0.339	0.360	0.388	0.432	0.514
	10	0.322	0.342	0.369	0.409	0.489

Time	CDF		Difference
	$F(T)$ Theoretical	$F(T)$ Experimental	
0	0.000	0.000	0.000
1	0.330	0.109	0.220
<b>2</b>	<b>0.551</b>	<b>0.266</b>	<b>0.285</b>
3	0.699	0.422	0.277
4	0.798	0.578	0.220
5	0.865	0.734	0.130
6	0.909	0.891	0.019

CDF, Cumulative density function.



**FIGURE 1.42**

K–S test graphical representation.

### 1.3.6 CRAMER–VON MISES TESTS

The Cramer–von Mises tests are the last goodness of fit methods demonstrated in this chapter. Such a method has a more direct approach by applying the null test ( $H_0$ ). Therefore the  $T$  value defined in the

following equation is compared with the critical value defined for the Cramer–von Mises method in Table 1.10. The  $T$  statistic is defined by the equation:

$$T = \frac{1}{12n} + \sum_{i=1}^n \left[ \frac{2i-1}{2n} - F(x_i) \right]^2$$

where  $F(x_i)$  = experimental cumulative distribution and  $n$  = number of elements in the sample.

$H_0$  (null hypothesis) is represented by the following equations, whether the acceptance of the theoretical PDF if:

$$T < n\omega^2$$

The critical values ( $n\omega^2$ ) are defined based on the confidence level ( $\alpha$ ), as shown in Table 1.10. Concerning an instance  $\alpha = 0.05$ , the  $n\omega^2 = 0.462$ .

Let us take into account the similar pump’s electric motor failure data described in Section 1.3.5. Therefore Table 1.11 shows the calculation of “ $T$ ” as described previously.

Table 1.11 shows the  $T$  statistic calculation. The first column shows the time and the second column shows the unreliability values for an exponential PDF with MTTF = 2.5 years.

To simplify the calculation the equation applied in column 3 is:

$$T = \frac{1}{12n} + t$$


where:

$$t = \sum_{i=1}^n \left[ \frac{2i-1}{2n} - F(x_i) \right]^2$$

The null test shows that null hypothesis accepted the goodness fitness for the exponential PDF as demonstrated in the equation:

$$T < n\omega^2$$

$$0.311 < 0.462$$

	Significance Level $\alpha$	Critical $n\omega^2$
	0.5	0.120
	0.4	0.148
	0.3	0.184
	0.25	0.210
	0.2	0.241
	0.1	0.348
	0.05	0.462
	0.025	0.581
	0.01	0.744
	0.005	0.870

**Table 1.11 Cramer—von Mises  $H_0$  Test**

Time	CDF		Critical Values ( $\alpha = 0.05$ )
	$F(T)$ Theoretical	$t$	
0	0.000	0.007	
1	0.330	0.061	
<b>2</b>	<b>0.551</b>	0.090	
3	0.699	0.080	
4	0.798	0.046	
5	0.865	0.013	
6	0.909	0.000	
	$\Sigma$	0.297	
	$T$	<b>0.311</b>	
		0.462	

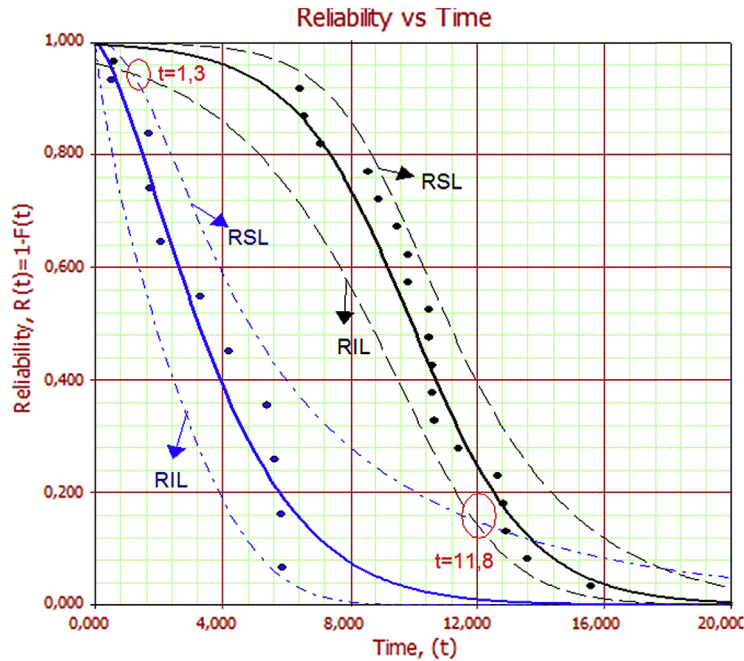
CDF, Cumulative density function.

## 1.4 HOW RELIABLE IS RELIABILITY: CONFIDENCE BOUND WILL TELL YOU ABOUT !!!

To understand how reliable reliability prediction is, it is necessary to explain the confidence bound that can be defined by one or both confidence-bound sides. This means there is an error whenever reliability is defined and it is important, for example, when making some decisions, such as when comparing different equipment chains to see if one is better in terms of reliability than the other. In some cases, only one confidence-bound side (superior or inferior) takes place, and in this case it is necessary to define only one value as the limit. This is usual for process variables control (eg, temperature, pressure, levels, etc.). For example, a burner in a furnace will not have a lower temperature limit inside, but there is a higher temperature limit because damage in the burner will affect its performance. In a hydrogen generation plant, damage in the burner inside the furnace occurs whenever a high temperature (over project specifications) occurs over time. In this case it is necessary to define only a superior confidence bound to a control process to avoid the higher temperature specified.

But in other cases it is necessary to know both confidence bounds. For example, in a coke plant, if the furnace shuts down and the oil temperature cools down lower than the specified temperature limit, such oil may clog the pipeline. But if the temperature goes higher than specified, there will be coke formation in the furnace tubes, which will shut down the plant. To make such decisions when comparing the reliability of two different equipment chains it is necessary to look at confidence bounds, as shown in Fig. 1.43.

Fig. 1.43 shows two seals from different chains. From top to bottom of the graph, the first three lines are reliability superior limit (RSL), reliability, and reliability inferior limit (RIL) of the best seal (A). The next three lines are RSL, reliability, and RIL of seal B. In the worse situation, seal pump A (RIL) is better than seal pump B (RSL) between 1.3 and 11.8 years with 90% confidence. Reliable assumptions about confidence bounds depend on data, and whenever there is a high quantity of data available to estimate confidence bounds, it is better to make decisions because there will not be a high range between the superior and inferior limits around the average. In fact, oil and gas equipment usually have high reliability and most of the time there is not much failure data available to perform



**FIGURE 1.43**  
Seal pump reliability (confidence bound).

reliability analysis. In this case, it is hard to make decisions with high confidence bound limits such as 90%, 95%, or 99% with a low range of values between confidence limits. In other words, if a high confidence bound is required and there is not much data available, there will be a high range between superior and inferior limits around the average. The lower the number of data to predict reliability with certain confidence limits, the higher the range between superior and inferior confidence bounds. This means low confidence in supporting decisions, but each company or industry has their own standards, and in some cases 60% of confidence, for example, might be high enough. Actually, confidence depends on the particular case that is being assessed. If the variable assessed is well described as the normal distribution, for example, the expected value of variable  $T$  (time to repair) with confidence limits will be:

$$T = \mu \pm z \frac{\partial}{\sqrt{n}}$$

where  $Z$  is a variable established and depends on how much confidence bound is required;  $n$  = number of elements assessed;  $\mu$  = average mean;  $\partial$  = deviation:

$$\partial = \frac{1}{n-1} \sum_{i=1}^n (T' - t)^2$$

$T'$  = population mean; and  $t$  = values.

Confidence Bound	“Z”	Equation	Confidence Limits
90%	1.64	$T_1 = \mu \pm 1.64 \frac{\hat{\sigma}}{\sqrt{n}}$	$T_1 = 35.6 \pm 1.64 \frac{2}{\sqrt{100}} = 35.6 \pm 0.328$
95%	1.96	$T_2 = \mu \pm 1.98 \frac{\hat{\sigma}}{\sqrt{n}}$	$T_2 = 35.6 \pm 1.98 \frac{2}{\sqrt{100}} = 35.6 \pm 0.392$
99%	2.58	$T_3 = \mu \pm 2.58 \frac{\hat{\sigma}}{\sqrt{n}}$	$T_3 = 35.6 \pm 2.58 \frac{2}{\sqrt{100}} = 35.6 \pm 0.516$

A good example of a real application of confidence bound limits is to define equipment repair time, which managers are required to estimate to make decisions and plan maintenance service time and to inform others about how long the plant will be shut down. For example, a maintenance team predicted 35 hours to repair a gas compressor. But how reliable is the predicted repair time? To come up with this estimate, the maintenance team assessed 100 similar maintenance repair times performed on similar compressors and had 35.6 hours repair time on average, and, regarding 90%, 95%, and 99% confidence values, the following results were achieved: there is a 90% confidence of the repair being done between 35.272 and 35.928 hours, a 95% confidence of the repair being done between 35.208 and 35.992 hours, and a 99% confidence of the repair being done between 35.084 and 36.116 hours, as shown in [Table 1.12](#).

In doing so, there is a 90% chance of the repair being done between 35.272 and 35.928 h, a 95% chance of the repair being done between 35.28 and 35.992 hours, and a 99% chance of the repair being done between 35.084 and 36.116 hours.

$$\begin{aligned}
 P(35.272 \leq T_1 \leq 35.928) &= 90\% \\
 P(35.208 \leq T_2 \leq 35.992) &= 95\% \\
 P(35.084 \leq T_3 \leq 36.116) &= 99\%
 \end{aligned}$$

In this case the industrial manager estimated 36 hours to perform the seal repair in the compressor with 99% confidence and informed the CEO that the plant would be shut down for 36 hours. The main assumption in this case is that the repair is well represented by normal distribution and the gas compressor repair is standardized for the maintenance team, or, in other words, all maintenance teams that perform seal gas compressor repairs take on average 35.6 hours.

In some cases, other methodologies such as the Fisher matrix can define variation parameter estimation, that is, using one parameter estimation such as the exponential PDF represented by a general function,  $F$ , which is a function of one parameter estimator, say  $F(\lambda)$ . For example, the mean of the exponential methodologies such as the Fisher matrix will define variation parameter estimation. Thus regarding some probability density function with one parameters such as exponential PDF represented by a general function,  $F$ , which is a function of one parameter estimator, say  $F(\hat{\theta})$ . For example, the mean of the exponential distribution is a function of the parameter  $\lambda$ :  $F(\lambda) = 1/\lambda = \mu$ . Then, in general, the expected value of  $E(F(\hat{\theta}))$  can be found by:

$$E(F(\bar{\lambda})) = F(\lambda) + e\left(\frac{1}{n}\right)$$

where  $F(\lambda)$  is some function of  $\lambda$ , such as the mean value, and  $\lambda$  is the population parameter where:

$$E(\bar{\lambda}) = \lambda$$

when:

$$n \rightarrow \infty$$

If:

$$\bar{\lambda} = \frac{1}{MTTF} \quad \text{and} \quad F(\lambda) = \frac{1}{\lambda}$$

then:

$$E(F(\bar{\lambda})) = F(\lambda) + e\left(\frac{1}{n}\right) \quad \text{and} \quad e\left(\frac{1}{n}\right) = \frac{\sigma^2}{n}$$

Thus when:

$$n \rightarrow \infty,$$

$$E(F(\bar{\lambda})) = \mu$$

The variance for a function can be estimated by the equation:

$$Var(E(F(\bar{\lambda}))) = \left(\frac{\sigma F}{\sigma \bar{\lambda}}\right)_{\bar{\lambda}=\lambda}^2 Var(\bar{\lambda}) + o\left(\frac{1}{n^{\frac{3}{2}}}\right)$$

So the confidence bound is:

$$E(F(\bar{\lambda})) \pm z_{\alpha} \sqrt{Var(E(F(\bar{\lambda})))}$$

In case of two variables like Weibull 2P, variance can be estimated by:

$$E(F(\bar{\beta}, \bar{\eta})) = F(\beta, \eta) + e\left(\frac{1}{n}\right)$$

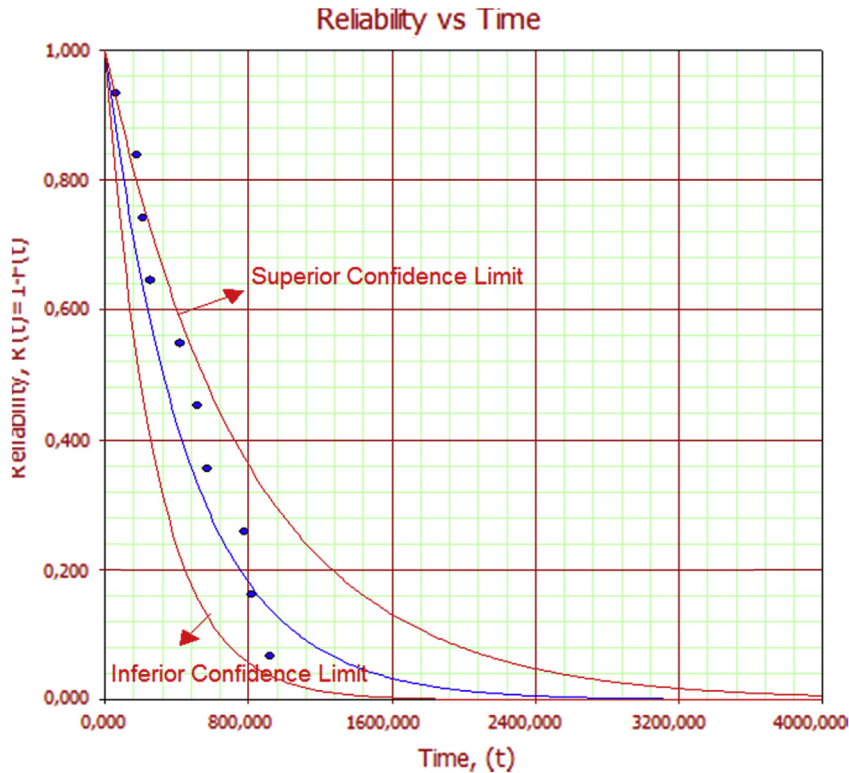
where:

$$\begin{aligned} Var(E(F(\bar{\beta}, \bar{\eta}))) &= \left(\frac{\sigma F}{\sigma \bar{\beta}}\right)_{\bar{\beta}=\beta}^2 Var(\bar{\beta}) + \left(\frac{\sigma F}{\sigma \bar{\eta}}\right)_{\bar{\eta}=\eta}^2 Var(\bar{\eta}) \\ &+ 2 \left(\frac{\sigma F}{\sigma \bar{\beta}}\right)_{\bar{\beta}=\beta} \left(\frac{\sigma F}{\sigma \bar{\eta}}\right)_{\bar{\eta}=\eta} Cov(\bar{\beta}, \bar{\eta}) + e\left(\frac{1}{n^{\frac{3}{2}}}\right) \end{aligned}$$

Using the previous equation to find the variance and estimate the confidence bound, it is possible to define the confidence bound for reliability, failure rate,  $MTTF$ , and other functions, as shown in Fig. 1.39, which is an example of the exponential reliability function, with  $\lambda = 0.0021$ . For the 90% confidence bound, the superior failure per rate is  $\lambda = 0.0036$  and the inferior failure per rate is  $\lambda = 0.0013$  (Fig.1.44).

A remarkable point in life cycle analysis is that whenever historical data is collected to make up the PDF, the maintenance effect is not being considered. Or, in other words, for repairable components the repair is able to reestablish component reliability as good as new or the component is replaced.





**FIGURE 1.44**

Confident limits to reliability function.

In Chapter 4, the general renovation process will be shown to clear up other methodology to consider maintenance or other effects when the component is not as good as new.

In addition to specialist elicitation, in some cases, the equipment supplier needs to obtain a reliability function to check if the equipment achieves the reliability target defined by the client. Therefore, to get such an estimation in a shorter period of time during the design, the accelerated life test is performed. Such tests force failure occurrence in a shorter time when equipment is submitted to harder operational conditions during laboratory tests. Thus, with failure data obtained from the accelerated test it is possible to estimate reliability function in usual operation conditions. In some cases, even when equipment accelerated tests are not carried out, the similar mathematical methods can be implemented when the failure data are provided based on equipment which works in harder operational conditions to predict the reliability function of similar equipment in softer operational conditions.

By the other hand, in some cases when developing an equipment or components and performing accelerated tests, companies find out that their products are not as robust as they suppose to be under harder operation conditions.

Therefore, it is necessary to make some improvements. In these cases, the reliability growth program is carried out to achieve product reliability target and improve the product robustness. Furthermore, another reliability growth application is to check the effect of maintenance and operation conditions in equipment reliability.

In fact, all these issues will be discussed in the next chapter.

## 1.5 LIFETIME DATA ANALYSIS CASES

The final item in this chapter has the main objective of demonstrating the real cases of lifetime data analysis applied in the oil and gas industry. Such analysis is one of the most important analyses performed by reliability engineers, which support important decisions such as:

- To compare different equipment's vendor performance;
- To define the best vendor to be an equipment supplier;
- To define equipment warranty requirements;
- To follow up equipment performance along the life cycle;
- To be an input in reliability, availability, maintainability (RAM) analysis;
- To support the time to perform preventive maintenance and inspection;
- To be an input in quantitative risk analysis such as fault tree analysis.

To perform lifetime data analysis, it is necessary to have a reliable historical failure database. It is also important to be aware that the lifetime data analysis can be performed on equipment or component level that depends on the historical data detail level. In fact, in some cases the historical failure data is new and does not have all the information about the whole equipment's component failures. In addition, different equipment and components have a different life cycle duration. Usually, rotating equipment has a shorter life cycle when compared with static equipment. Moreover, when considering rotating equipment such as pumps and compressors, different components like seals and bearings fail earlier than others such as impellers and shafts. Therefore whenever the historical failure database has a small number of years like 5 years or fewer, there will not be failure historical data about all components available.

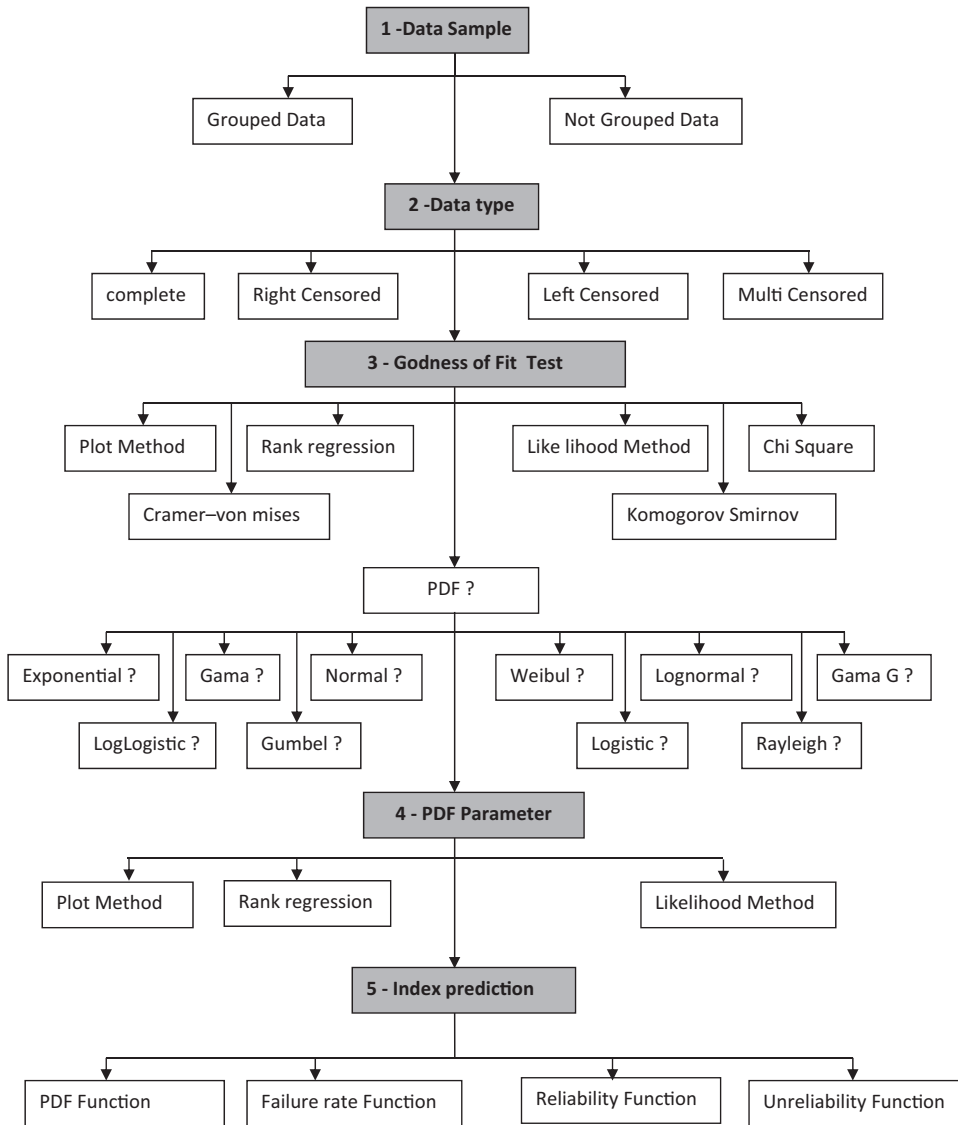
The final condition about the database is that many professionals expect to acquire a huge number of failures to perform the lifetime data analysis, but this is not happening in most cases for oil and gas equipment because this is high-performance equipment. The important point is to have reliable data. The lack of data related to high reliability is always good news and not a bad news when it shows that such equipment has a high reliability.

To obtain a higher number of failures from specific equipment many analysts try to collect historical failure data from similar equipment. Be careful when doing this because it is necessary to take into account operational condition, the type of product, and equipment function when considering two or more similar pieces of equipment.

The case studies will demonstrate different equipment from different types of plant in the oil and gas industry. In general terms, the lifetime data analysis follows the five steps demonstrated in Fig. 1.45 and discussed previously, such as select the sample, define the type of sample, define the type of data, perform the goodness of fit test, define the PDF parameter, and predict the performance index.

### 1.5.1 PUMP LIFETIME DATA ANALYSIS

The first case study describes the lifetime data analysis of a propylene plant pump, the feed pump, and concerns the component failures described in the historical database. Therefore because in refinery plants each process plant has different operational conditions, products, configurations, and design setups such as pressure, temperature, and flow, the pump is considered not a grouped sample.



**FIGURE 1.45**

Lifetime data analysis steps.

Based on failure historical database, the data is complete, which means that all failures available have a defined date and the pump failed during the period assessed. Table 1.13 shows the failure historical database.

Table 1.13 shows data from two main pump components, which presents the lowest reliability. The pump reliability is greatly affected by these two components, but in some intervals of time some other

**Table 1.13 Pump Failure Historical Data**

Equipment	Component	Failure	Repair Start	Repair Finish	Maintenance Type	Cause	Consequence	Solution
B-31005 B	Bearing	25/02/1994	26/02/1994	03/03/1994	Corrective	Wear out	High vibration	Replace
B-31005 B	Bearing	09/11/1998	09/11/1998	17/11/1998	Corrective	Wear out	High vibration	Replace
B-31005 B	Bearing	21/12/1998	22/12/1998	22/12/1998	Predictive	Wrong design	High vibration	Redesign
B-31005 B	Bearing	02/03/2001	02/03/2001	14/03/2002	Corrective	Installation error	High vibration	Replace
B-31005 B	Bearing	04/09/2002	06/09/2002	16/09/2002	Predictive	Wrong design	Loss of performance	Redesign
B-31005 B	Seal	07/01/2003	08/01/2003	17/01/2003	Corrective	Wear out	Leakage	Replace
B-31005 B	Seal	25/01/2003	25/01/2003	27/01/2003	Corrective	Installation error	Leakage	Replace
B-31005 B	Seal	17/06/2003	18/06/2003	20/06/2003	Corrective	Operation error	Leakage	Replace
B-31005 B	Seal	25/07/2003	25/07/2003	26/07/2003	Corrective	Installation error	Leakage	Replace
B-31005 B	Seal	23/08/2003	24/08/2003	29/09/2003	Corrective	Installation error	Leakage	Replace
B-31005 B	Bearing	25/10/2004	26/10/2004	28/11/2004	Corrective	Wear out	Loss of performance	Replace
B-31005 B	Seal	10/01/2005	10/01/2005	11/01/2005	Corrective	Wear out	Leakage	Replace

components were replaced as part of the maintenance plan. The additional important information on the database regards maintenance, cause of failure, the consequence, and solution. In fact, to perform a reliable lifetime data analysis, it is necessary to have a clear and reliable database as well as such additional information to prevent failures in the future.

The next step is to perform the goodness of fit test and in most cases software is the most indicated solution to support such analysis because it has a faster and more reliable result.

Therefore CAFDE software from BQR Reliability Engineering Ltd was applied. CAFDE software has the chi square methods to perform the goodness of fit test and the likelihood method to predict the PDF parameters. Before performing such tests, it is necessary to organize the information collected on the failure historical database in Excel format to export directly to CAFDE. Table 1.14 shows the data organized in Excel format to import directly to CAFDE. A further step is to perform the goodness of fit test and predict the PDF parameter, as shown in Fig. 1.46.

Fig. 1.46 shows the possible type of PDFs such as normal, lognormal, exponential, Weibull, uniform, Pareto, and Rayleigh.

Figs. 1.47 and 1.48 show the final PDF parameter estimation for the two most critical components such as bearing and seal, respectively. On the left of Figs. 1.47 and 1.48 it is possible to observe the level of significance of the chi square test for each type of PDF. On the bottom of Figs. 1.47 and 1.48 are the parameter  $\alpha$  values.

After the PDF parameter estimation the final step is to predict the reliability and failure rate function, as shown in Figs. 1.49 and 1.50, respectively.

## 1.5.2 SCREW COMPRESSOR LIFETIME DATA ANALYSIS CASE

The second case study describes the lifetime data analysis of a fluid catalytic cracking plant compressor, the export screw compressor, and concerns the component failures described in the historical database. The screw compressor is the only one in the fluid catalytic cracking plant, therefore the failure data is considered not a grouped sample.

Based on the failure historical database, the data is complete, which means that the failure has a defined date and the screw compressor failed during the period assessed. Table 1.15 shows the failure historical database in CAFDE template format. The historical failure database has no additional information about the cause of failure, the type of maintenance, consequence, and solution. In this case, to improve the equipment performance it will be necessary to identify the critical component cause of failures. Therefore root cause analysis must be implemented to define the cause of component failures and propose solutions. Chapter 3 will describe the root cause analysis method as well as FRACAS (failure reporting, analysis, and corrective action system) analysis to support the complete failure database.

The goodness of fit test is the next step to proceed with the screw compressor lifetime data analysis. Fig. 1.51 shows the screw compressor and the different components' lifetime data analysis result concerning the PDF for each one, such as bearing, seal, shaft, and cylinder valve.

Figs. 1.52 and 1.53 show the final PDF parameter estimation for the two most critical components, such as bearing and seal, respectively. Fig. 1.54 shows the compressor parameter estimation considering all components. In Figs. 1.52–1.54 on the left it is possible to observe the level of significance of the chi square test for each type of PDF. In Fig. 1.52, for example, the Rayleigh PDF is the most significant (48.42%). On the bottom of Figs. 1.52–1.54 are the PDF parameter values.

**Table 1.14 Pump Failure Historical Data—CAFDE Template**

Data Start Date												
01/01/1990												
Off Date	Off Type	Off Description	System Serial Number	System Location	Maintenance Start Date	Maintenance Finish Date	On Date	LRU Name	LRU Serial Number	SRU Name	SRU Serial Number	Component Name
25/02/1994	Failure	Description 1	A3	1401	25/02/1994	03/03/1994	03/03/1994	Bearing	B-31005 B	Bearing	2	Bearing
09/11/1998	Failure	Description 2	A3	1401	09/11/1998	17/11/1998	17/11/1998	Bearing	B-31005 B	Bearing	2	Bearing
21/12/1998	Failure	Description 3	A3	1401	21/12/1998	22/12/1998	22/12/1998	Bearing	B-31005 B	Bearing	2	Bearing
02/03/2001	Failure	Description 4	A3	1401	02/03/2001	14/03/2002	14/03/2002	Bearing	B-31005 B	Bearing	2	Bearing
04/09/2002	Failure	Description 5	A3	1401	04/09/2002	16/09/2002	16/09/2002	Bearing	B-31005 B	Bearing	2	Bearing
07/01/2003	Failure	Description 6	A3	1401	07/01/2003	17/01/2003	17/01/2003	Seal	B-31005 B	Seal	1	Seal
25/01/2003	Failure	Description 7	A3	1401	25/01/2003	27/01/2003	27/01/2003	Seal	B-31005 B	Seal	1	Seal
17/06/2003	Failure	Description 8	A3	1401	17/06/2003	20/06/2003	20/06/2003	Seal	B-31005 B	Seal	1	Seal
25/07/2003	Failure	Description 9	A3	1401	25/07/2003	26/07/2003	26/07/2003	Seal	B-31005 B	Seal	1	Seal
23/08/2003	Failure	Description 10	A3	1401	23/08/2003	29/09/2003	29/09/2003	Seal	B-31005 B	Seal	1	Seal
25/10/2004	Failure	Description 11	A3	1401	25/10/2004	28/11/2004	28/11/2004	Bearing	B-31005 B	Bearing	2	Bearing
10/01/2005	Failure	Description 12	A3	1401	10/01/2005	11/01/2005	11/01/2005	Seal	B-31005 B	Seal	1	Seal

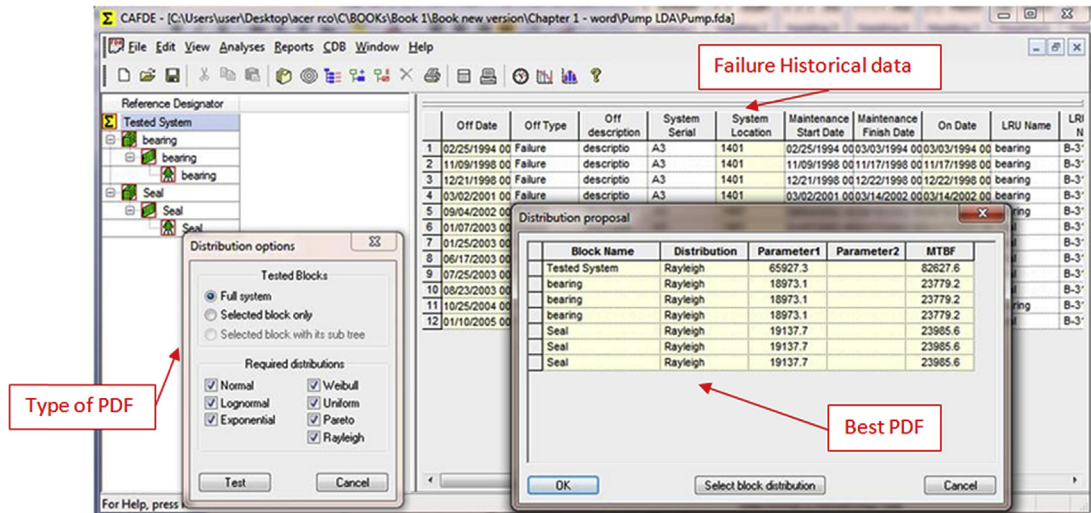


FIGURE 1.46 Pump failure historical data—CAFDE lifetime data analysis.

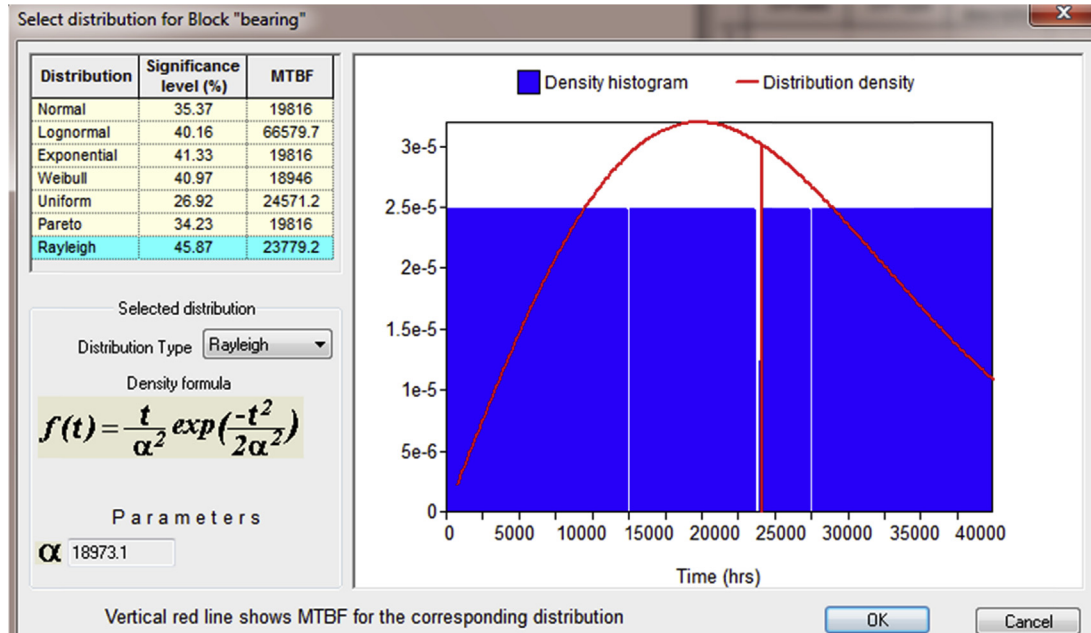


FIGURE 1.47 Pump bearing lifetime data analysis—CAFDE template.

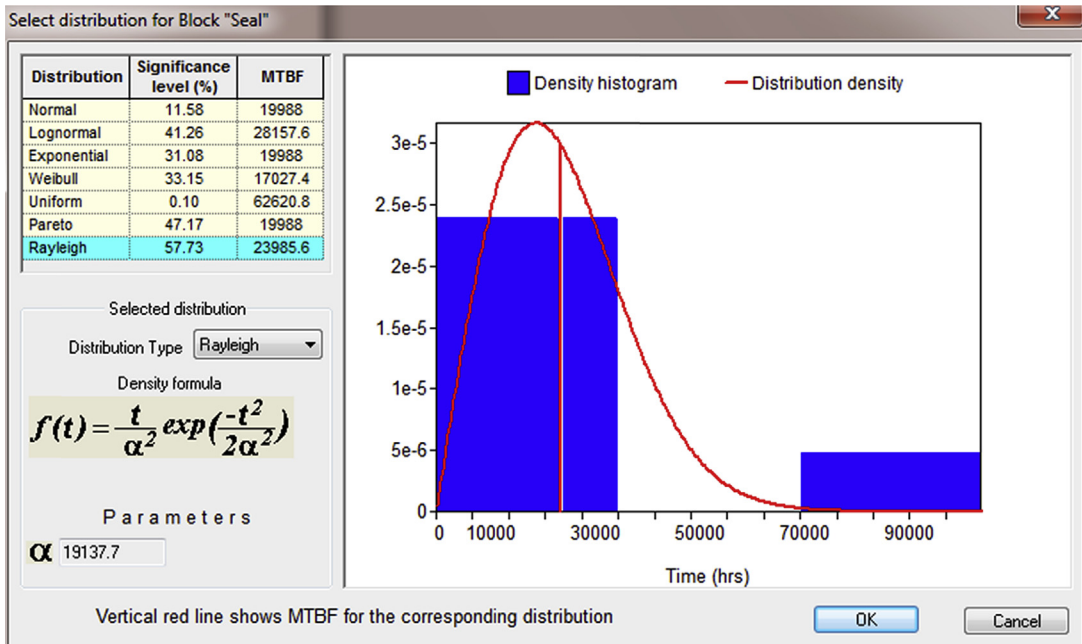


FIGURE 1.48

Pump seal lifetime data analysis—CAFDE template.

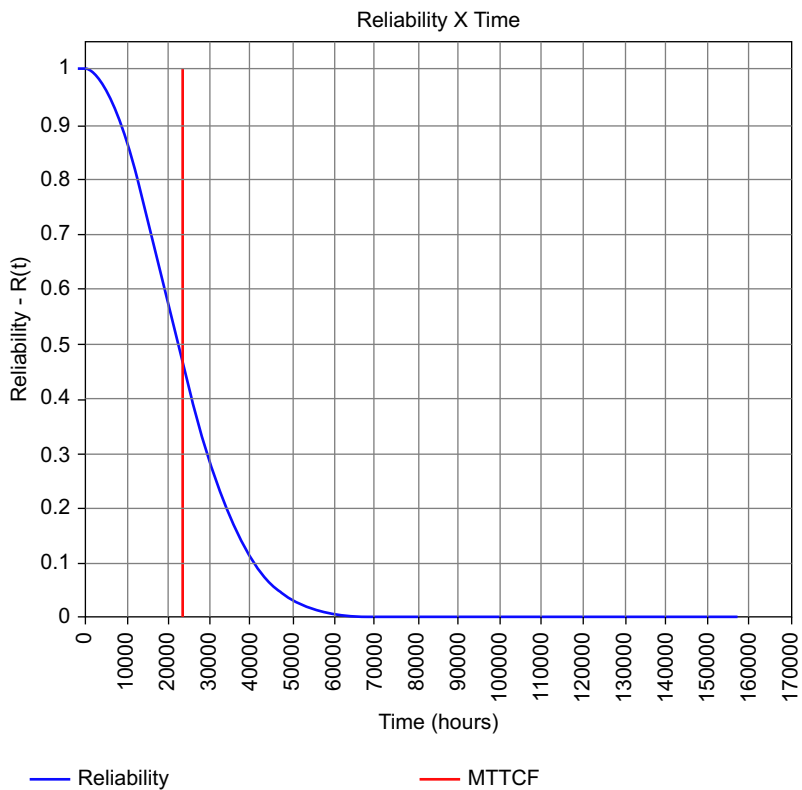
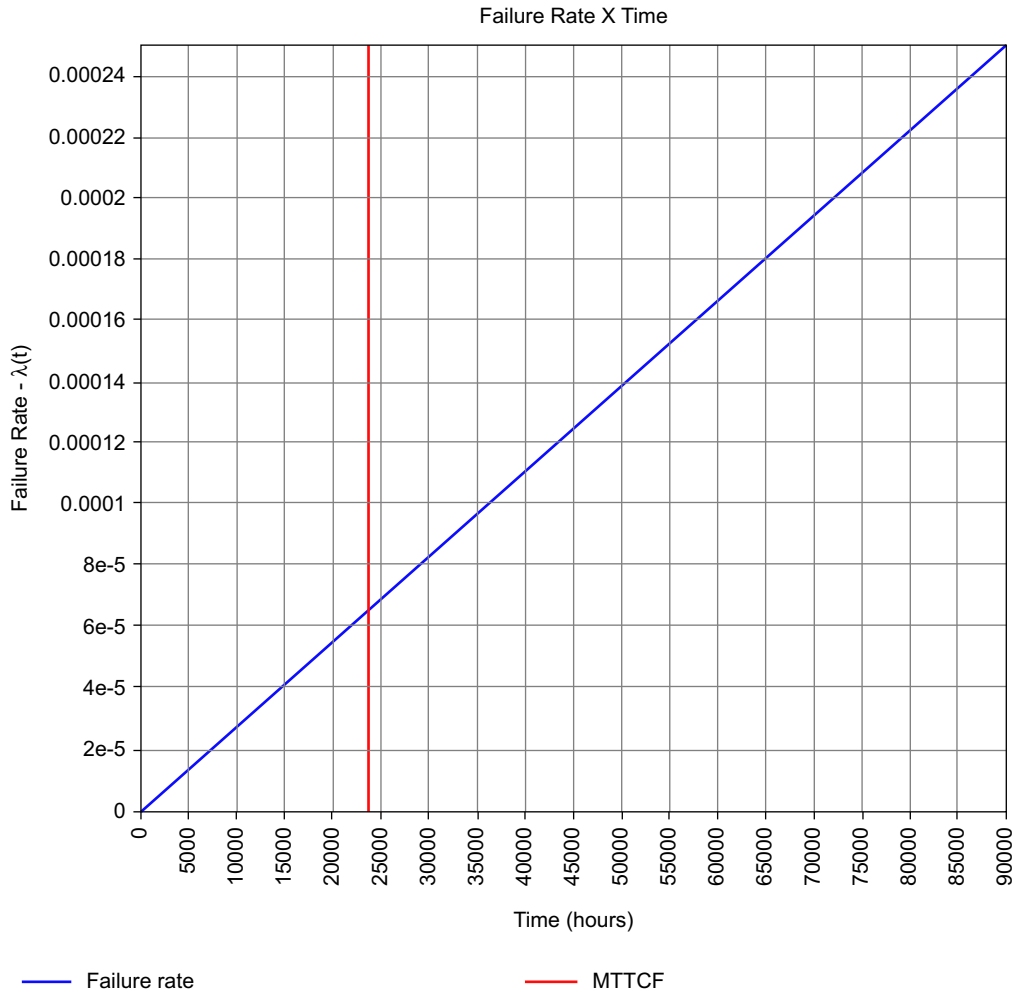


FIGURE 1.49

Bearing reliability function.





**FIGURE 1.50**

Bearing failure rate function.

The final step is to predict the reliability and failure rate functions, as shown in Figs. 1.55 and 1.56. Despite a constant failure rate demonstrated in Fig. 1.56 for the screw compressor, different components require different strategy actions in terms of maintenance and spare parts. Chapter 8 will define the integrated logistics support method concerning the maintenance and spare part optimization, which will be applied in these similar cases to achieve the asset performance optimization.

**Table 1.15 Screw Compressor—CAFDE Template**

Data Start Date													
01/01/2004													
Off Date	Off Type	Off Description	System Serial Number	System Location	Maintenance Start Date	Maintenance Finish Date	On Date	LRU Name	LRU Serial Number	SRU Name	SRU Serial Number	Component Name	Component Serial Number
10/05/2005	Failure	Description 1	K15	2001	10/05/2005	11/05/2005	11/05/2005	Seal	K-002	Seal	6	Seal	61
09/08/2005	Failure	Description 2	K7	2001	09/08/2005	10/08/2005	10/08/2005	Cylinder valve	K-001	Cylinder valve	4	Cylinder valve	41
26/09/2005	Failure	Description 3	K8	2001	26/09/2005	26/09/2005	26/09/2005	Cylinder valve	K-001	Cylinder valve	4	Cylinder valve	41
11/11/2005	Failure	Description 4	K11	2001	11/11/2005	11/11/2005	11/11/2005	Cylinder valve	K-001	Cylinder valve	4	Cylinder valve	41
14/12/2005	Failure	Description 5	K2	2001	14/12/2005	16/12/2005	16/12/2005	Bearing	K-001	Bearing	3	Bearing	31
30/12/2005	Failure	Description 6	K1	2001	30/12/2005	31/12/2005	31/12/2005	Bearing	K-001	Bearing	3	Bearing	31
12/01/2006	Failure	Description 7	K9	2001	12/01/2006	13/01/2006	13/01/2006	Cylinder valve	K-001	Cylinder valve	4	Cylinder valve	41
25/11/2008	Failure	Description 8	K3	2001	25/11/2008	27/11/2008	27/11/2008	Bearing	K-001	Bearing	3	Bearing	31
21/01/2009	Failure	Description 9	K16	2001	21/01/2009	22/01/2009	22/01/2009	Seal	K-003	Seal	6	Seal	61
06/02/2009	Failure	Description 10	K4	2001	06/02/2009	09/02/2009	09/02/2009	Bearing	K-001	Bearing	3	Bearing	31
07/05/2009	Failure	Description 11	K17	2001	07/05/2009	08/05/2009	08/05/2009	Seal	K-004	Seal	6	Seal	61
10/08/2009	Failure	Description 12	K12	2001	10/08/2009	11/08/2009	11/08/2009	Shaft	K-001	Shaft	5	Shaft	51
04/09/2009	Failure	Description 13	K6	2001	04/09/2009	06/09/2009	06/09/2009	Bearing	K-001	Bearing	3	Bearing	31
13/10/2009	Failure	Description 14	K10	2001	13/10/2009	14/10/2009	14/10/2009	Cylinder valve	K-001	Cylinder valve	4	Cylinder valve	41
17/11/2009	Failure	Description 15	K13	2001	17/11/2009	18/11/2009	18/11/2009	Shaft	K-001	Shaft	5	Shaft	51
01/02/2010	Failure	Description 16	K14	2001	01/02/2010	03/02/2010	03/02/2010	Shaft	K-001	Shaft	5	Shaft	51
11/02/2010	Failure	Description 17	K5	2001	11/02/2010	13/02/2010	13/02/2010	Bearing	K-001	Bearing	3	Bearing	31
04/05/2010	Failure	Description 18	K18	2001	04/05/2010	05/05/2010	05/05/2010	Seal	K-005	Seal	6	Seal	61

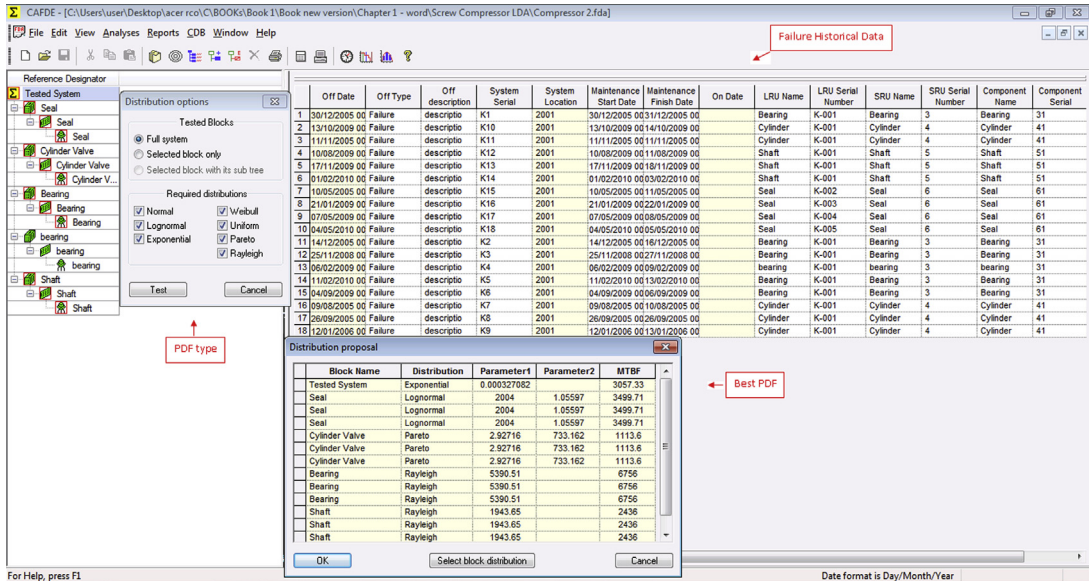


FIGURE 1.51

Screw compressor failure historical data—CAFDE lifetime data analysis.

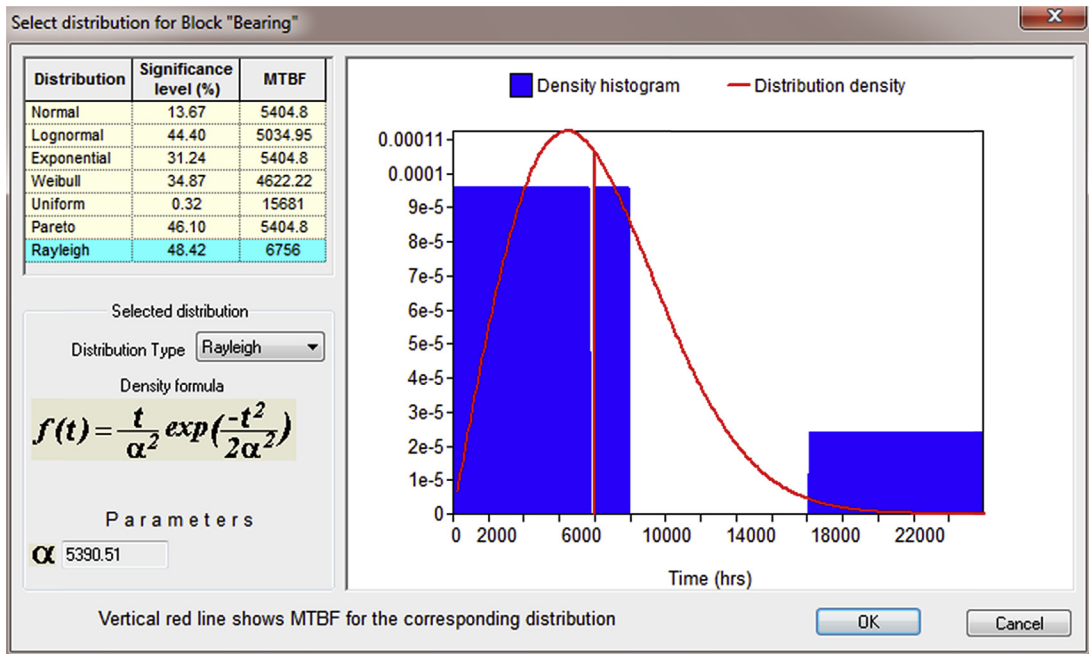


FIGURE 1.52

Screw compressor bearing lifetime data analysis—CAFDE template.

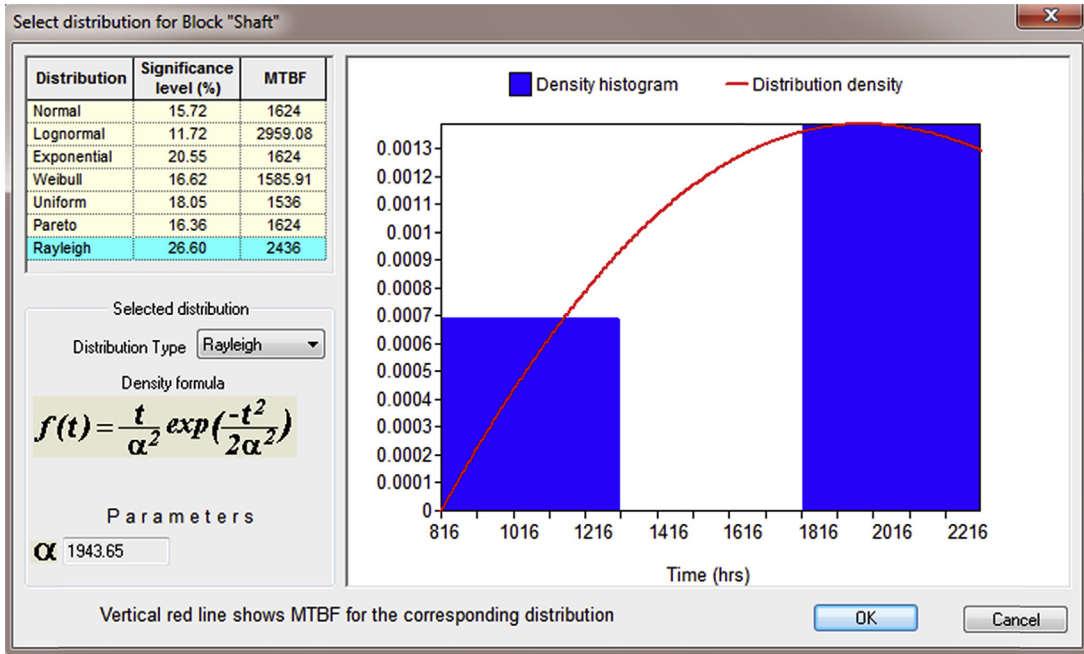


FIGURE 1.53 Screw compressor seal lifetime data analysis—CAFDE template.

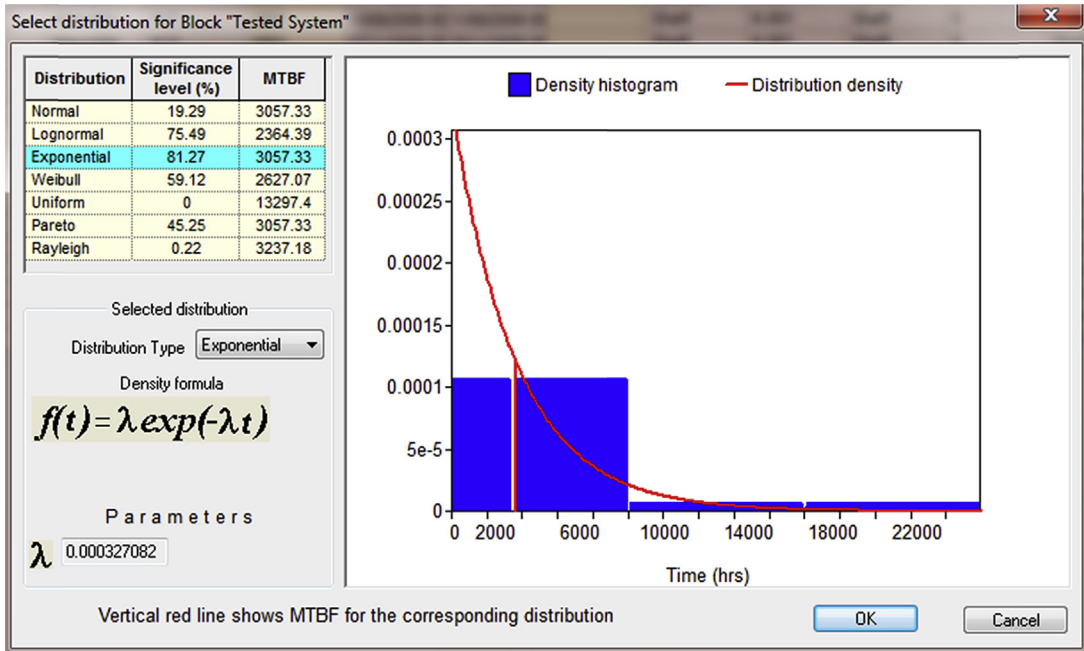
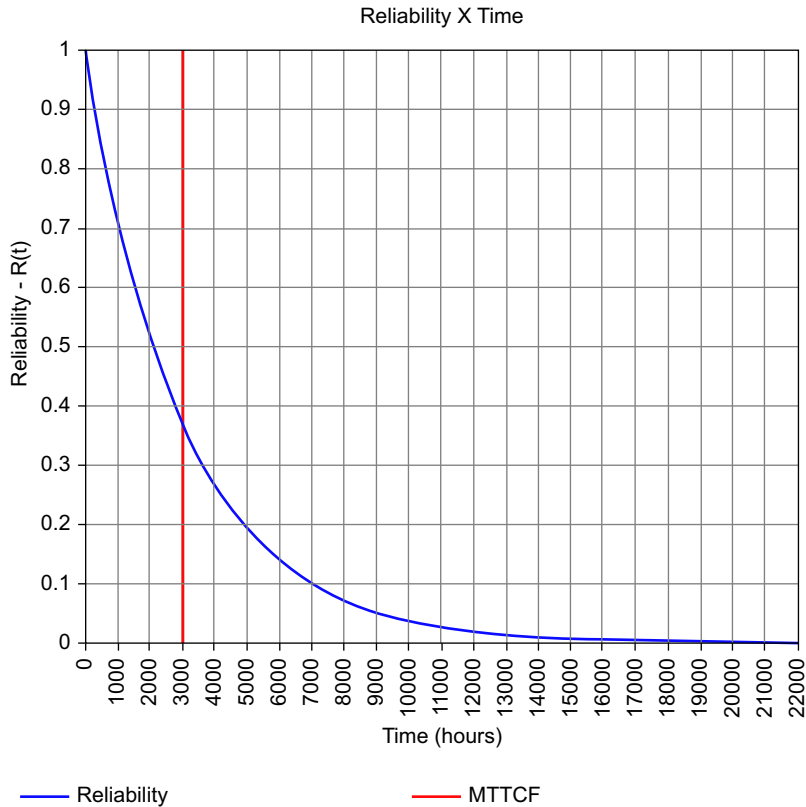


FIGURE 1.54 Screw compressor lifetime data analysis—CAFDE template.



**FIGURE 1.55**

Screw compressor reliability function—CAFDE template.

### 1.5.3 VALVE LIFETIME DATA ANALYSIS CASE

The third case study describes the lifetime data analysis of a pressure swing adsorption valve, XV valve, and concerns the main component failures described in the historical database. In fact, four XV valves are installed for each of five vessels. These valves have different cycles. Concerning the different XV valves, the critical one that will be assessed is installed on the top of the vessels. The XV valves are similar in terms of function and perform different on/off cycles inside the five vessels (XV-2001 A–D). In addition, the XV valves with similar functions have also similar operational conditions. Because of this, the XV valve is considered a grouped sample.

Based on the failure historical database, the data is complete, which means that the failure dates available are defined and the XV valves failed during the period assessed. Table 1.16 shows the historical failure database in a CAFDE template format. The historical failure database has no additional information about the cause of failure, the type of maintenance, consequence, and solution. In this case, root cause analysis was performed to solve the problem in the most critical component, the actuator.

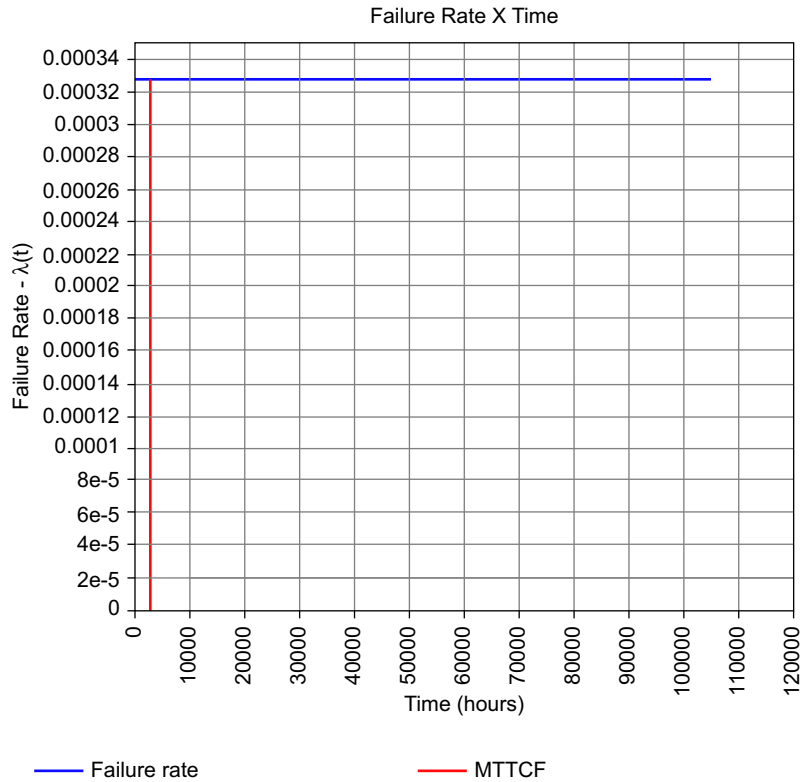


FIGURE 1.56

Screw compressor failure rate function—CAFDE template.

The goodness of fit test is the next step to proceed with the XV valve lifetime data analysis. Fig. 1.57 shows the different XV valve components such as actuator, gasket, and diaphragm. Because the number of failures of gasket and diaphragm is very low, lifetime data analysis was performed at equipment level. In fact, the actuator is responsible for 77.27% of failures based on the failure historical database.

Fig. 1.58 shows the final PDF parameter estimation for the XV valve concerning all components defined on the failure historical database. On the left of Fig. 1.58 it is possible to observe the level of significance of the chi square test for each type of PDF. The Rayleigh PDF is the most significant (89.41%). On the bottom of Fig. 1.58 is the PDF parameter value ( $\alpha = 2573.29$ ).

The final step is to predict the reliability and failure rate functions, as shown in Figs. 1.59 and 1.60.

#### 1.5.4 SENSOR LIFETIME DATA ANALYSIS CASE

The fourth case study describes the lifetime data analysis of a safety integrity function sensor, which shuts down the centrifugal compressor in case of spurious failure.

**Table 1.16 XV Valve—CAFDE Template**

Data Start Date													
01/01/2000													
Off Date	Off Type	Off Description	System Serial Number	System Location	Maintenance Start Date	Maintenance Finish Date	On Date	LRU Name	LRU Serial Number	SRU Name	SRU Serial Number	Component Name	Component Serial Number
18/02/2000	Failure	Description	V01	2001	18/02/2000	18/02/2000	18/02/2000	Diaphragm	XV-2001 D	Diaphragm	1D	Diaphragm	111
14/12/2001	Failure	Description	V01	2001	14/12/2001	14/12/2001	14/12/2001	Actuator	XV-2001 C	Actuator	1C	Actuator	111
25/09/2002	Failure	Description	V01	2001	25/09/2002	25/09/2002	25/09/2002	Actuator	XV-2001 B	Actuator	1B	Actuator	111
28/11/2002	Failure	Description	V01	2001	28/11/2002	28/11/2002	28/11/2002	Actuator	XV-2001 A	Actuator	1A	Actuator	111
11/12/2002	Failure	Description	V01	2001	11/12/2002	11/12/2002	11/12/2002	Actuator	XV-2001 D	Actuator	1D	Actuator	111
21/01/2003	Failure	Description	V01	2001	21/01/2003	21/01/2003	21/01/2003	Actuator	XV-2001 C	Actuator	1C	Actuator	111
13/01/2004	Failure	Description	V01	2001	13/01/2004	13/01/2004	13/01/2004	Diaphragm	XV-2001 A	Diaphragm	1A	Diaphragm	111
11/03/2004	Failure	Description	V01	2001	11/03/2004	11/03/2004	11/03/2004	Actuator	XV-2001 B	Actuator	1B	Actuator	111
13/04/2004	Failure	Description	V01	2001	13/04/2004	13/04/2004	13/04/2004	Actuator	XV-2001 C	Actuator	1C	Actuator	111
28/04/2004	Failure	Description	V01	2001	28/04/2004	28/04/2004	28/04/2004	Actuator	XV-2001 A	Actuator	1A	Actuator	111
29/04/2004	Failure	Description	V01	2001	29/04/2004	29/04/2004	29/04/2004	Diaphragm	XV-2001 D	Diaphragm	1D	Diaphragm	111
06/09/2004	Failure	Description	V01	2001	06/09/2004	06/09/2004	06/09/2004	Actuator	XV-2001 A	Actuator	1A	Actuator	111
28/01/2005	Failure	Description	V01	2001	28/01/2005	28/01/2005	28/01/2005	Actuator	XV-2001 C	Actuator	1C	Actuator	111
25/05/2005	Failure	Description	V01	2001	25/05/2005	25/05/2005	25/05/2005	Actuator	XV-2001 A	Actuator	1A	Actuator	111
25/05/2005	Failure	Description	V01	2001	25/05/2005	25/05/2005	25/05/2005	Actuator	XV-2001 B	Actuator	1B	Actuator	111
27/05/2005	Failure	Description	V01	2001	27/05/2005	27/05/2005	27/05/2005	Actuator	XV-2001 D	Actuator	1D	Actuator	111
31/05/2005	Failure	Description	V01	2001	31/05/2005	01/06/2005	01/06/2005	Gasket	XV-2001 C	Gasket	1C	Gasket	111
15/12/2005	Failure	Description	V01	2001	15/12/2005	15/12/2005	15/12/2005	Actuator	XV-2001 A	Actuator	1A	Actuator	111
30/06/2006	Failure	Description	V01	2001	30/06/2006	30/06/2006	30/06/2006	Actuator	XV-2001 D	Actuator	1D	Actuator	111
20/07/2006	Failure	Description	V01	2001	20/07/2006	21/07/2006	21/07/2006	Gasket	XV-2001 B	Gasket	1B	Gasket	111
11/09/2007	Failure	Description	V01	2001	11/09/2007	11/09/2007	11/09/2007	Actuator	XV-2001 A	Actuator	1A	Actuator	111
25/09/2007	Failure	Description	V01	2001	25/09/2007	25/09/2007	25/09/2007	Actuator	XV-2001 C	Actuator	1C	Actuator	111

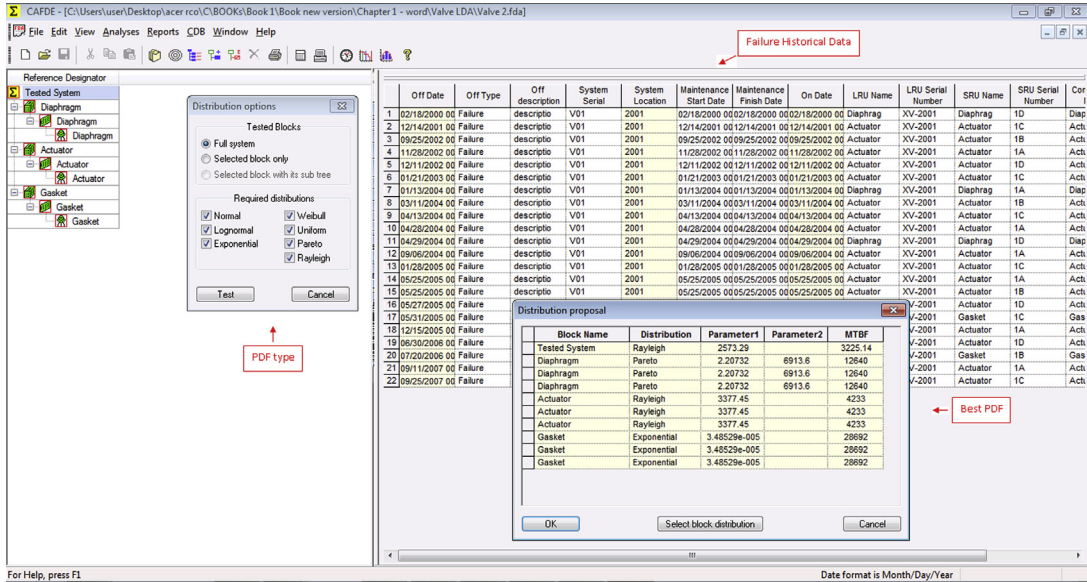


FIGURE 1.57

XV valve failure historical data—CAFDE template.

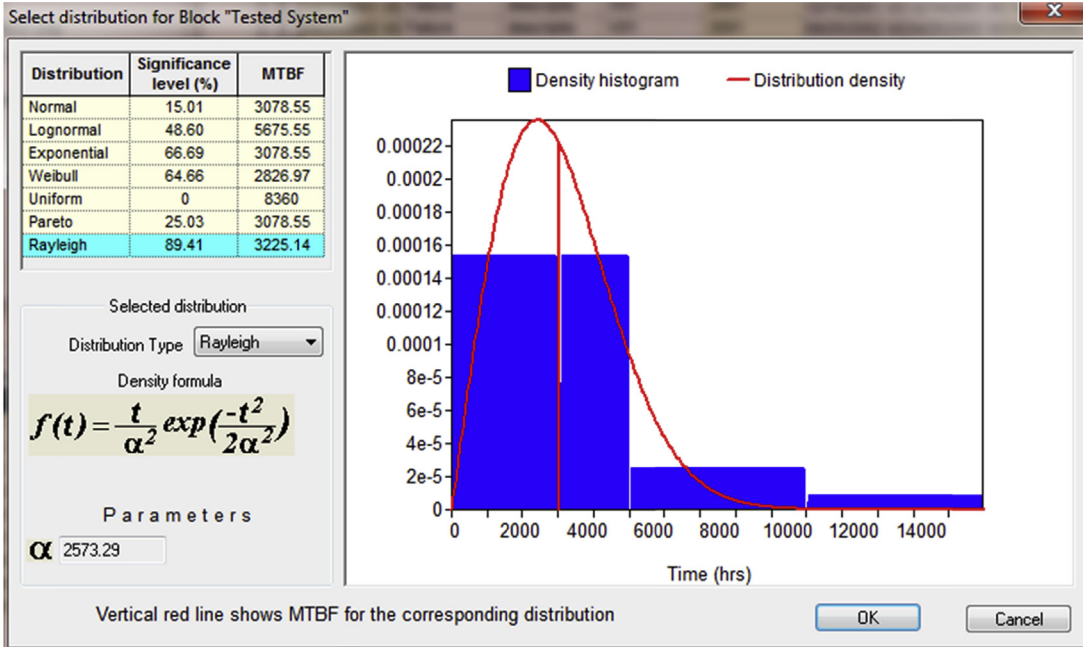
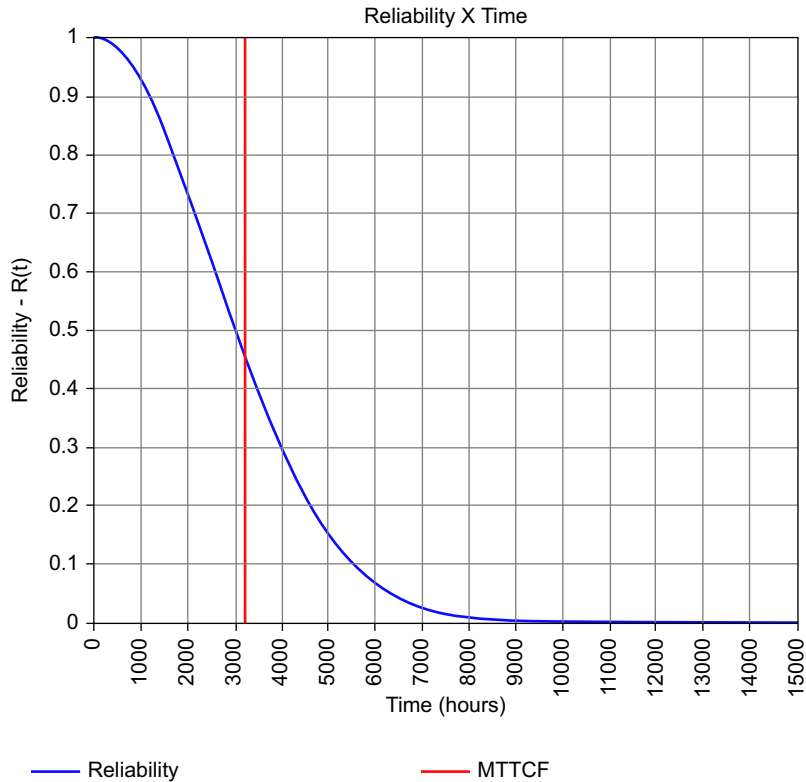


FIGURE 1.58

XV valve lifetime data analysis—CAFDE template.





**FIGURE 1.59**

XV valve reliability function—CAFDE template.

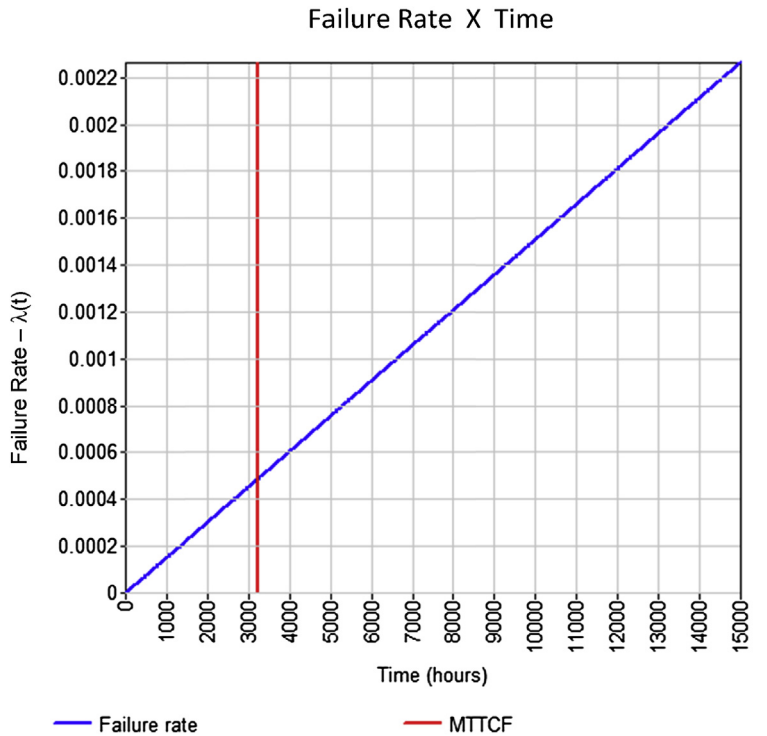
Based on the failure historical database, the data is complete, which means that the failure dates available are defined for the sensor during the period assessed. In addition, only one single sensor was assessed, therefore the sample is considered not a group sample.

Table 1.17 shows the historical failure database in a CAFDE template format. The type of failure mode was not defined in the historical failure database. In this case the failures are related to a sensor, which is replaced whenever the failures happen. Despite of the replacement, the failure mode and root cause must be defined. In this case, the spurious failure was related mainly to wrong design. Such information was defined in another database and not in the historical failure database. The importance to include the failure mode and root causes in failure historical databases will be discussed in the Chapter 3.

Fig. 1.61 shows the final PDF parameter estimation for the sensor based on a failure historical database. On the left of Fig. 1.61 it is possible to observe the level of significance of the chi square test for each type of PDF. The Rayleigh PDF is the most significant (61.42%). At the bottom are the parameter  $\alpha$  values.

The final step is to predict the reliability and failure rate functions, as shown in Figs. 1.62 and 1.63.

The sensors are a type of equipment that can be tested in the laboratory to predict the reliability during the design phase, test the sensor robustness, and if necessary implement improvement actions to increase the reliability. Such methods are known as ALT (accelerated life test),



**FIGURE 1.60**

XV valve failure rate function—CAFDE template.

HALT (high accelerated test), and RGA (reliability growth analysis) and will be demonstrated in Chapter 2.

### 1.5.5 HEAT EXCHANGER LIFETIME DATA ANALYSIS CASES

The fifth case study describes the lifetime data analysis of a heat exchanger (shell and tube) placed on a fluid catalytic cracking plant. Based on the failure historical database, the data is complete, which means that all failure dates available are defined for the heat exchanger during the period assessed. In addition, only one single heat exchanger was assessed, therefore the sample is considered not a grouped sample. Despite such an assumption, more than one tube was taken into account inside the heat exchanger to provide the failure historical database. Table 1.18 shows the historical failure database in a CAFDE template format. The historical failure database shows only the component tube; the main problem is tube incrustation caused by bad water quality.

The goodness of fit test is the next step to proceed with the heat exchanger lifetime data analysis. After importing the Excel template to the CAFDE software, the test was performed. Fig. 1.64 shows the level of significance of the chi square test for each type of PDF. The Rayleigh PDF is the most significant (61.42%). At the bottom is the parameter value ( $\alpha = 16,433.9$ ).

**Table 1.17 Safety Instrumented Function—CAFDE Template**

Data Start Date													
01/01/2001													
Off Date	Off Type	Off Description	System Serial Number	System Location	Maintenance Start Date	Maintenance Finish Date	On Date	LRU Name	LRU Serial Number	SRU Name	SRU Serial Number	Component Name	Component Serial Number
11/01/2002	Failure	Description 1	S1	2101	11/01/2002	11/01/2002	11/01/2002	Safety instrumented function	B-31005 B	Safety instrumented function	10	Sensor	101
12/04/2002	Failure	Description 2	S2	2101	12/04/2002	12/04/2002	12/04/2002	Safety instrumented function	B-31005 B	Safety instrumented function	10	Sensor	101
23/03/2005	Failure	Description 3	S3	2101	23/03/2005	23/03/2005	23/03/2005	Safety instrumented function	B-31005 B	Safety instrumented function	10	Sensor	101
12/05/2005	Failure	Description 4	S4	2101	12/05/2005	12/05/2005	12/05/2005	Safety instrumented function	B-31005 B	Safety instrumented function	10	Sensor	101
04/06/2005	Failure	Description 5	S5	2101	04/06/2005	04/06/2005	04/06/2005	Safety instrumented function	B-31005 B	Safety instrumented function	10	Sensor	101
26/05/2006	Failure	Description 6	S6	2101	26/05/2006	26/05/2006	26/05/2006	Safety instrumented function	B-31005 B	Safety instrumented function	10	Sensor	101
27/05/2006	Failure	Description 7	S7	2101	27/05/2006	27/05/2006	27/05/2006	Safety instrumented function	B-31005 B	Safety instrumented function	10	Sensor	101
22/02/2009	Failure	Description 8	S8	2101	22/02/2009	22/02/2009	22/02/2009	Safety instrumented function	B-31005 B	Safety instrumented function	10	Sensor	101
05/01/2010	Failure	Description 9	S9	2101	05/01/2010	05/01/2010	05/01/2010	Safety instrumented function	B-31005 B	Safety instrumented function	10	Sensor	101
13/03/2010	Failure	Description 10	S10	2101	13/03/2010	13/03/2010	13/03/2010	Safety instrumented function	B-31005 B	Safety instrumented function	10	Sensor	101
16/04/2011	Failure	Description 11	S11	2101	16/04/2011	16/04/2011	16/04/2011	Safety instrumented function	B-31005 B	Safety instrumented function	10	Sensor	101

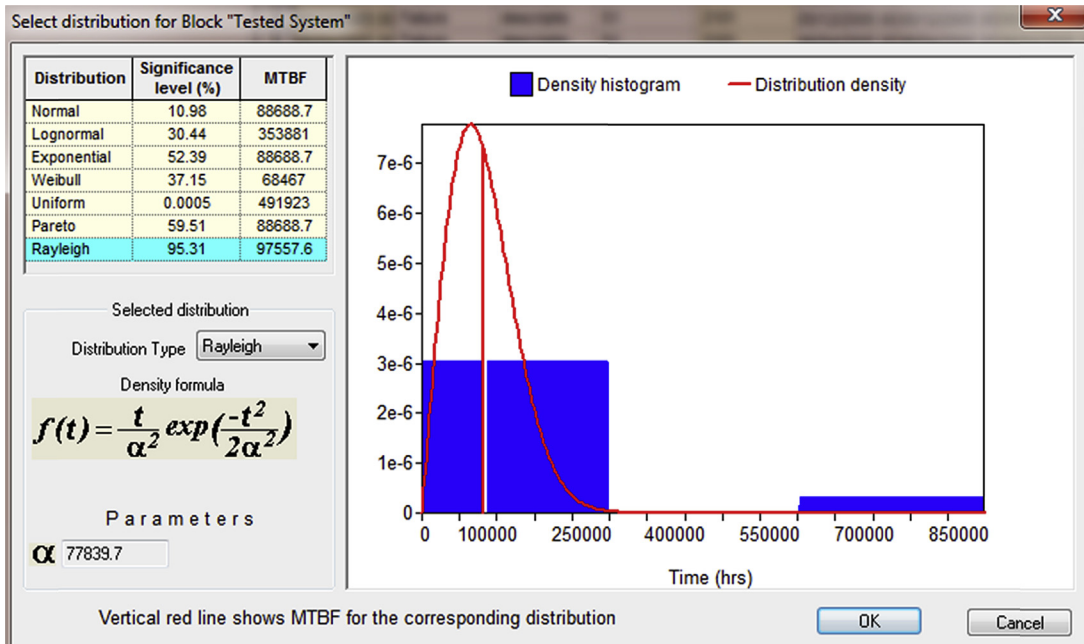


FIGURE 1.61

Sensor lifetime data analysis—CAFDE template.

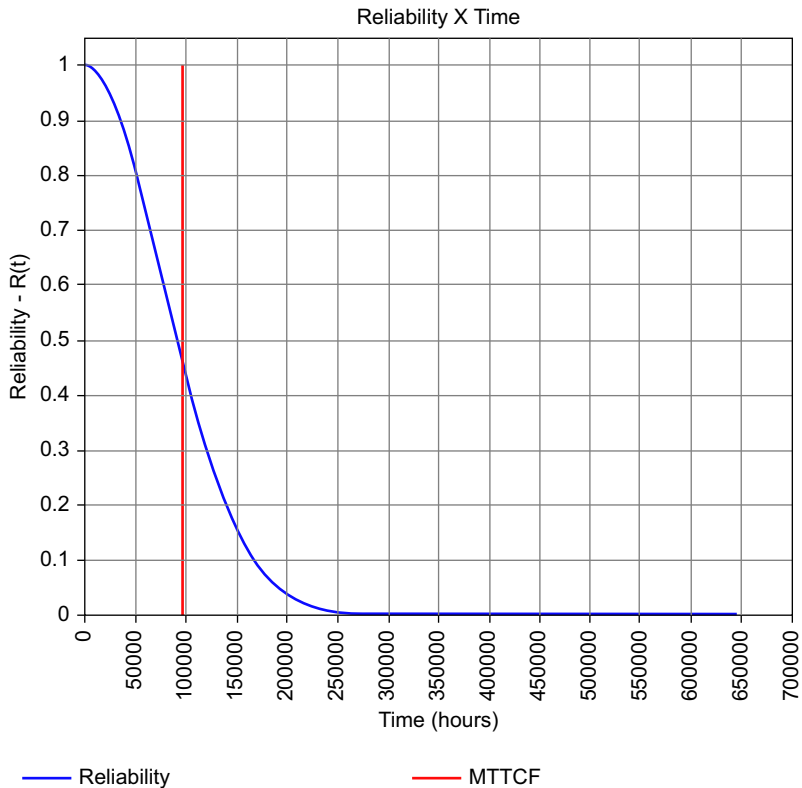


FIGURE 1.62

Sensor reliability function—CAFDE template.

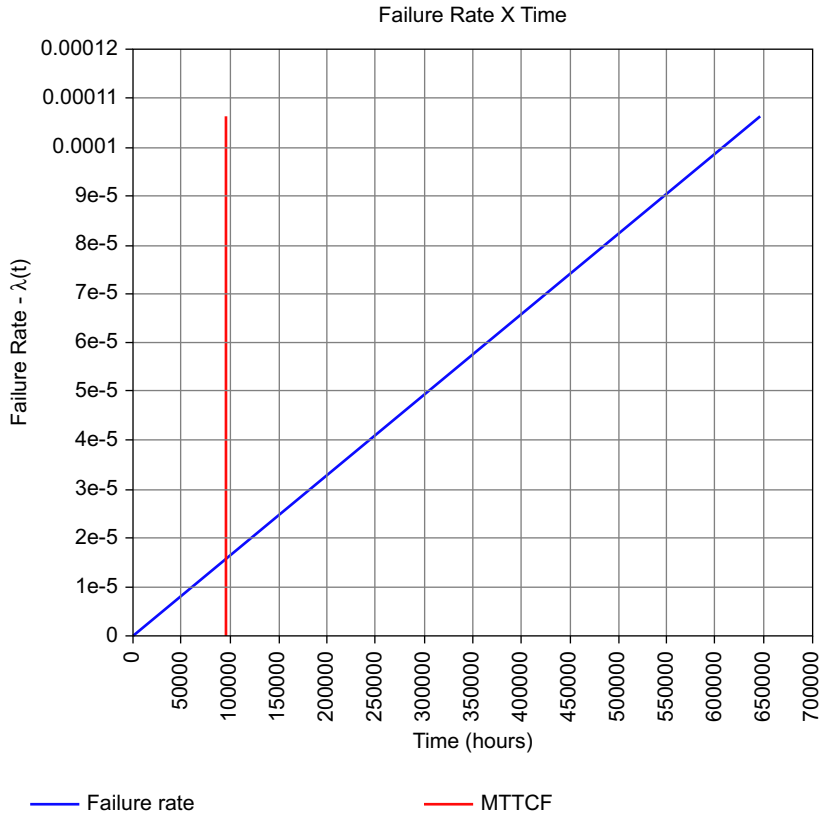


FIGURE 1.63

Sensor failure rate function.

The final step is to predict the reliability and failure rate functions, as shown in Figs. 1.65 and 1.66.

### 1.5.6 PIPELINE LIFETIME DATA ANALYSIS CASES

The sixth case study describes the lifetime data analysis of a pipeline. Based on the failure historical database, the data is complete, which means that all failure dates available are defined for the pipeline during the period assessed. In addition, more than one pipeline (P2201 A–D) was taken into account to collect the failure historical data. All these pipelines have similar function, design, and operational condition, therefore the sample is considered a grouped sample. Table 1.19 shows the historical failure database. The historical failure database is related to pipe corrosion.

Table 1.20 shows the historical failure database in Reliability Workbench template format. The information came from the seventh column of Table 1.19. In this case, more than one similar pipe (P2201 A–D) in terms of function and operational condition was used to perform the lifetime data analysis, therefore the pipeline sample is considered a grouped sample.

**Table 1.18 Heat Exchanger—CAFDE Template**

Data Start Date													
11/02/1997													
Off Date	Off Type	Off Description	System Serial Number	System Location	Maintenance Start Date	Maintenance Finish Date	On Date	LRU Name	LRU Serial Number	SRU Name	SRU Serial Number	Component Name	Component Serial Number
11/11/1999	Failure	Description 1	HE03	1302	11/11/1999	14/11/1999	14/11/1999	Heat exchanger	E-13002	Tubes	7	Tubes	72
13/01/2001	Failure	Description 2	HE03	1302	13/01/2001	13/01/2001	13/01/2001	Heat exchanger	E-13002	Tubes	7	Tubes	72
21/10/2002	Failure	Description 3	HE03	1302	21/10/2002	24/10/2002	24/10/2002	Heat exchanger	E-13002	Tubes	7	Tubes	72
29/02/2004	Failure	Description 4	HE03	1302	29/02/2004	01/03/2004	01/03/2004	Heat exchanger	E-13002	Tubes	7	Tubes	72
07/04/2006	Failure	Description 5	HE03	1302	07/04/2006	11/04/2006	11/04/2006	Heat exchanger	E-13002	Tubes	7	Tubes	72
22/11/2008	Failure	Description 6	HE03	1302	22/11/2008	25/11/2008	25/11/2008	Heat exchanger	E-13002	Tubes	7	Tubes	72

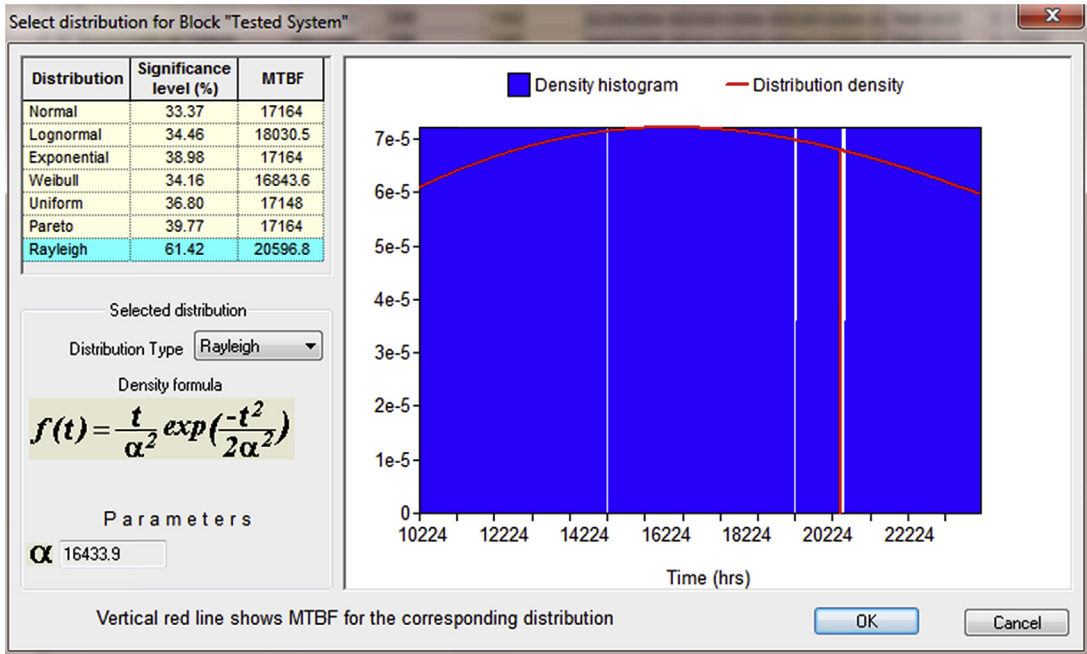


FIGURE 1.64

Heat exchanger PDF—CAFDE template.

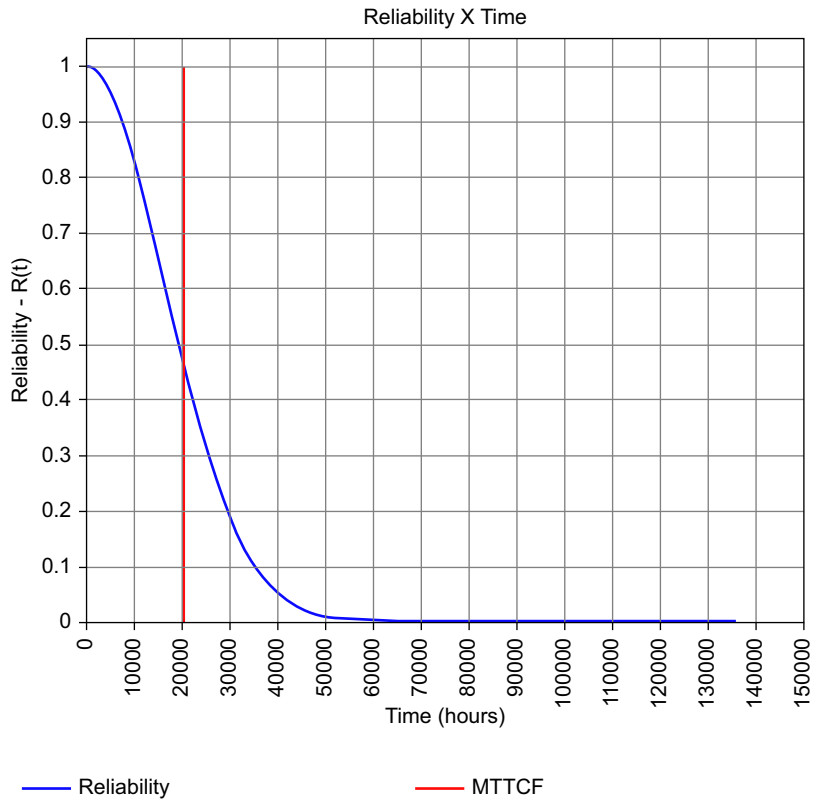
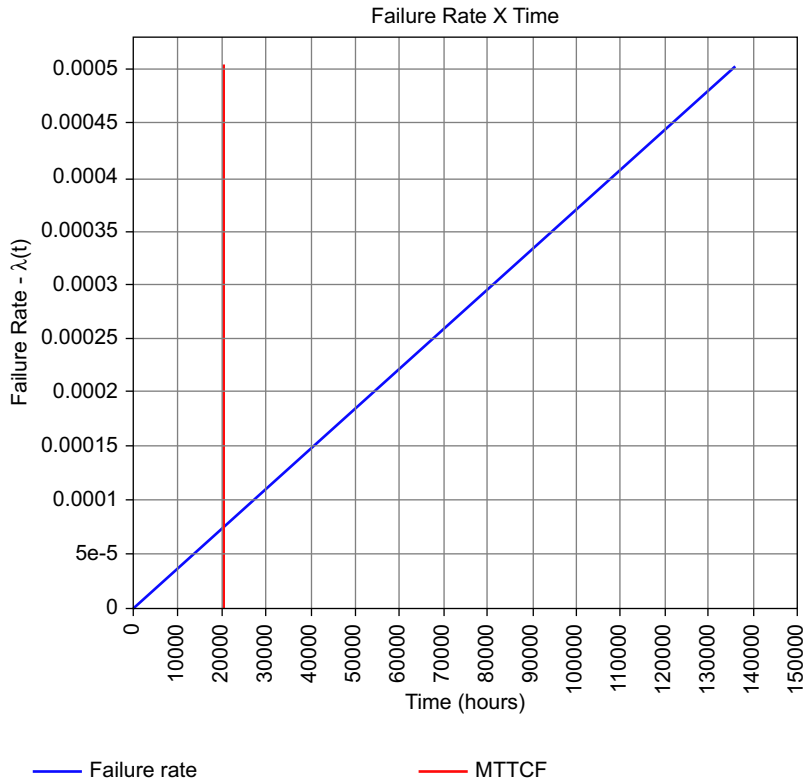


FIGURE 1.65

Heat exchanger reliability function—CAFDE template.



**FIGURE 1.66**

Heat exchanger failure rate function—CAFDE template.

<b>Table 1.19 Pipeline Failure Historical Database</b>							
<b>Start Date:</b>	<b>11/02/1980</b>						
<b>Equipment</b>		<b>Failure Mode</b>	<b>Data</b>	<b>Year</b>	<b>Month</b>	<b>Days</b>	<b>Time (Years)</b>
Pipeline	P-2201 A	External corrosion	31/08/2003	23	5	20	23.47
Pipeline	P-2201 D	External corrosion	01/10/2003	23	7	20	23.64
Pipeline	P-2201 B	External corrosion	07/11/2003	24	8	26	24.74
Pipeline	P-2201 C	External corrosion	06/12/2003	24	9	25	24.82
Pipeline	P-2201 B	External corrosion	06/08/2005	25	5	27	25.49
Pipeline	P-2201 A	External corrosion	17/09/2005	25	6	36	25.60
Pipeline	P-2201 D	External corrosion	18/10/2006	26	8	7	26.69
Pipeline	P-2201 B	External corrosion	11/09/2007	27	7	0	27.58
Pipeline	P-2201 C	External corrosion	09/10/2008	28	7	28	28.66
Pipeline	P-2201 A	External corrosion	04/12/2008	28	9	23	28.81
Pipeline	P-2201 B	External corrosion	13/12/2008	28	10	2	28.84
Pipeline	P-2201 C	External corrosion	29/09/2009	29	7	18	29.63
Pipeline	P-2201 A	External corrosion	01/01/2010	30	11	11	30.95
Pipeline	P-2201 B	External corrosion	03/02/2011	30	11	24	33.98



It is important to realize that in this case, the failures happen at the end of the life cycle and the cumulative time to failure is more appropriate than the interval between failures as performed in previous case studies. The software Reliability Workbench has only the Weibull PDF to perform the lifetime data analysis. In fact, it is not a problem at all because as a generic function, the Weibull PDF can represent different PDFs such as exponential, normal, lognormal, and Gumbel. In the pipeline case, the Weibull has the Gumbel PDF shape, as shown in Fig. 1.67. To predict the Weibull parameter the Reliability Workbench software applies the rank and plot methods.

The final step is to predict the reliability and failure rate functions. In the case of Reliability Workbench, only the failure rate is plotted, as shown in Fig. 1.68.

To model the failure impact at the end of pipeline life cycle, it is necessary to apply the RAM model. In some cases, the same equipment presents consecutive failures as a consequence of the degradation process. In this case, additional methods such as Kijima factor must be taken into account in RAM analysis. In addition, the failure as a consequence of the degradation process can also be predicted based on statistic degradation, which will be presented in Chapter 2.

In the other case studies, where the component is considered new after replacement or repair, the time is accountable for zero after such a repair or replacement, therefore the time between failures would be applied in the software Reliability Workbench to perform the lifetime data analysis.

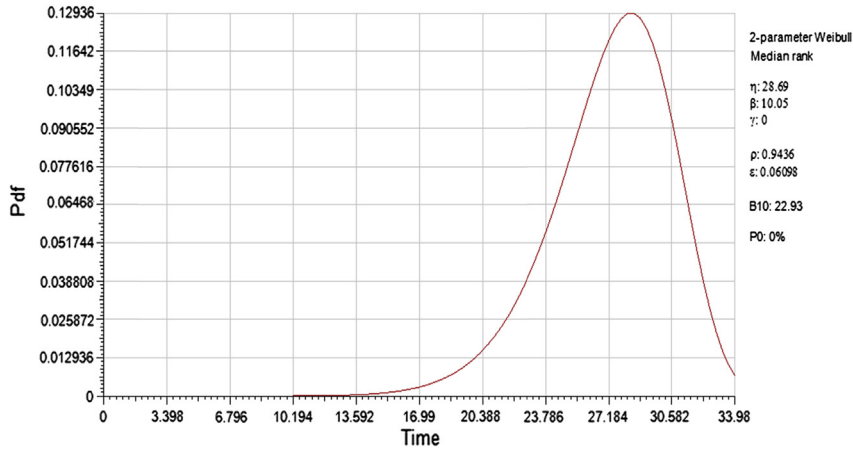
### 1.5.7 FURNACE LIFETIME DATA ANALYSIS CASES

The final case study describes the lifetime data analysis of a furnace from a distillation plant.

Based on the failure historical database, the data is complete, which means that all failure dates available are defined for the furnace during the period assessed. In addition, only one furnace (F-3100)

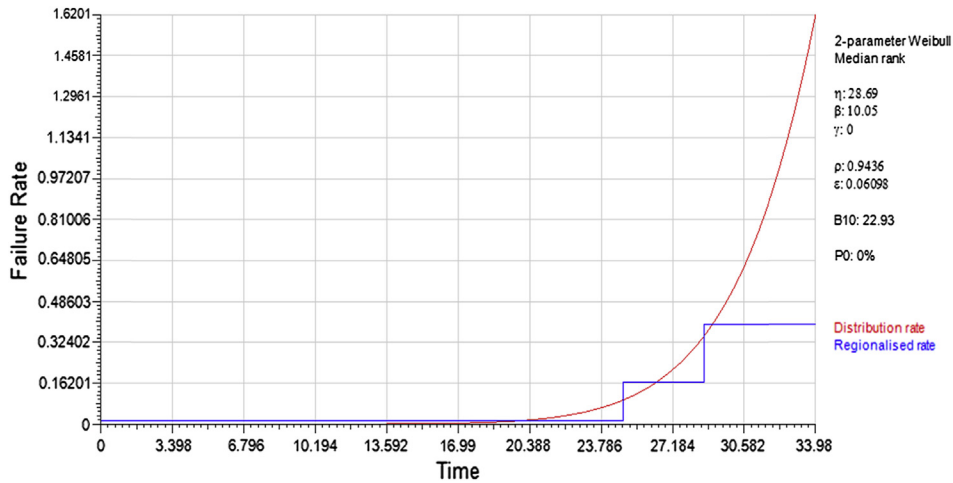
**Table 1.20 Pipeline—Weibull Reliability Workbench Template**

Time	Suspended	Disabled	Quantity	Reference ID
23.47	<input type="checkbox"/>	<input type="checkbox"/>	1	
23.64	<input type="checkbox"/>	<input type="checkbox"/>	1	
24.74	<input type="checkbox"/>	<input type="checkbox"/>	1	
24.82	<input type="checkbox"/>	<input type="checkbox"/>	1	
25.49	<input type="checkbox"/>	<input type="checkbox"/>	1	
25.6	<input type="checkbox"/>	<input type="checkbox"/>	1	
26.69	<input type="checkbox"/>	<input type="checkbox"/>	1	
27.58	<input type="checkbox"/>	<input type="checkbox"/>	1	



**FIGURE 1.67**  
Pipeline PDF—Reliability Workbench template.

was taken into account to collect the failure historical data. Therefore the sample is considered not a grouped sample. Table 1.21 shows the historical failure database. The historical failure database describes component failures, but not the cause of failures. In fact, after root cause analysis, the furnace component failure mode causes were corrosion in the joint and internal wall as well as joint leakage. The internal corrosion was caused by oil out of project specification throughout the distillation plant and the leakage was a consequence of such corrosion in the joint.



**FIGURE 1.68**  
Pipeline failure rate function—Reliability Workbench template.

**Table 1.21 Furnace Failure Historical Data—CAFDE Template**

Data start Date													
01/01/1990													
Off Date	Off Type	Off Description	System Serial Number	System Location	Maintenance Start Date	Maintenance Finish Date	On Date	LRU Name	LRU Serial Number	SRU Name	SRU Serial Number	Component Name	Component Serial Number
31/07/1990	Failure	Description	F02	3100	31/07/1990	05/08/1990	05/08/1990	Burner	F-3100	Burner	1	Burner	11
01/08/1992	Failure	Description	F02	3100	01/08/1992	06/08/1992	06/08/1992	Internal wall	F-3100	Internal wall	2	Internal wall	12
10/10/1995	Failure	Description	F02	3100	10/10/1995	15/10/1995	15/10/1995	Internal wall	F-3100	Internal wall	2	Internal wall	12
05/08/1998	Failure	Description	F02	3100	05/08/1998	10/08/1998	10/08/1998	Burner	F-3100	Burner	1	Burner	11
12/05/2004	Failure	Description	F02	3100	12/05/2004	17/05/2004	17/05/2004	Joint	F-3100	Joint	3	Joint	13
24/07/2004	Failure	Description	F02	3100	24/07/2004	28/07/2004	28/07/2004	Joint	F-3100	Joint	3	Joint	13
16/02/2005	Failure	Description	F02	3100	16/02/2005	21/02/2005	21/02/2005	Joint	F-3100	Joint	3	Joint	13
18/08/2005	Failure	Description	F02	3100	18/08/2005	22/08/2005	22/08/2005	Joint	F-3100	Joint	3	Joint	13

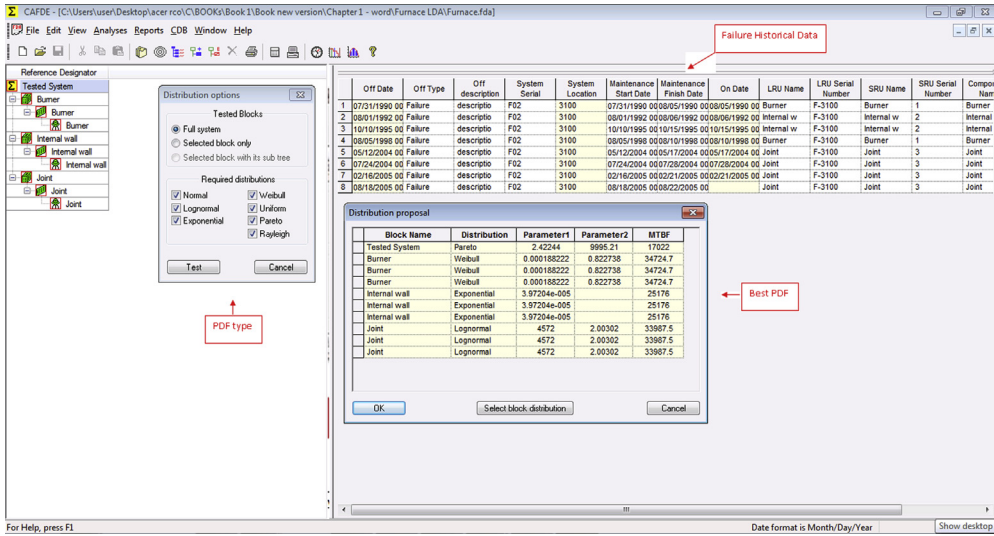


FIGURE 1.69 Furnace failure historical data—CAFDE template.

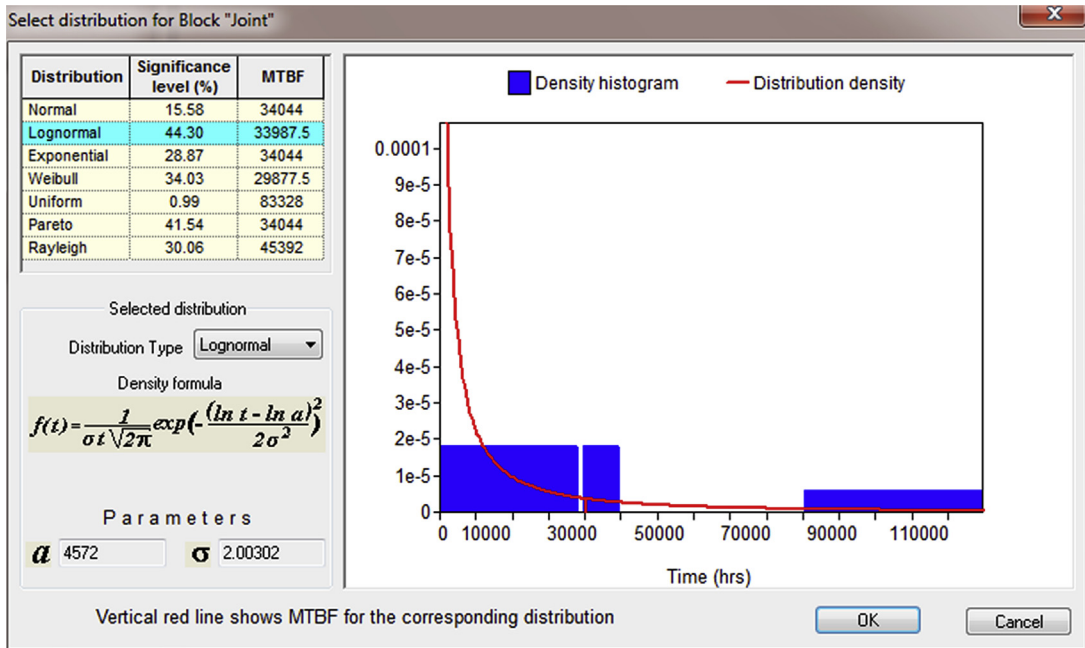


FIGURE 1.70 Joint failure PDF—CAFDE graphic.

The goodness of fit test is the next step to proceed with the furnace lifetime data analysis. Fig. 1.69 shows the different furnace component failures such as joint, internal wall, and burner.

The goodness of fit test is the next step to proceed with the furnace lifetime data analysis. Fig. 1.70 shows the level of significance of the chi square test for each type of PDF. The lognormal PDF is the most significant (44.30%) of the joint (leakage). At the bottom are the parameter values ( $\alpha = 4572$  and  $\sigma = 2.00302$ ).

The final step is to predict the reliability and failure rate functions, as shown in Figs. 1.71 and 1.72.

It is important to understand that the early life failure observed in this case is related to a human error to pass oil with a high sulfur component level, which caused the internal corrosion. The furnace is reliable equipment and is not expected to have such failures at the beginning of the life cycle. In spite of not accepting such early life failures, such information can be used to convince managers to implement the modification because of the high impact on operational availability during the distillation plant’s long life cycle. To do this, it is necessary to input the component’s PDF parameter in the reliability block diagram model and apply Monte Carlo simulation as part of RAM analysis. This will be discussed in Chapter 4.

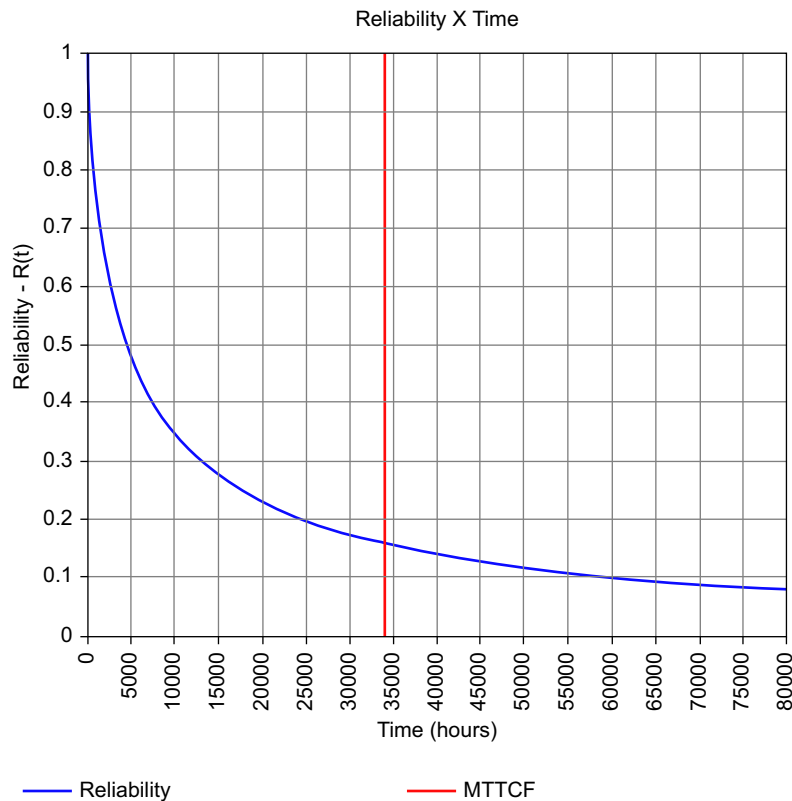
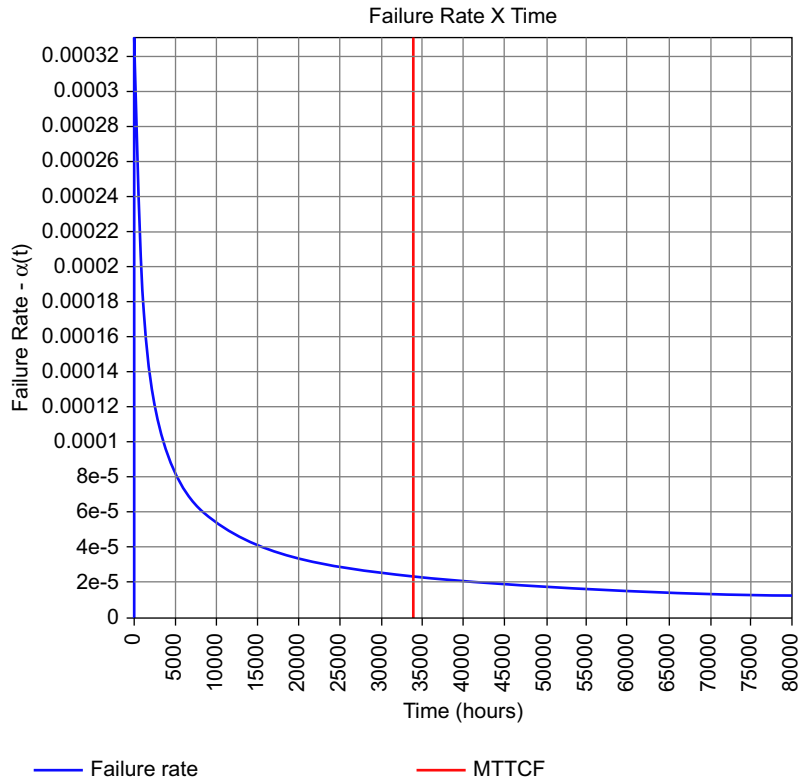


FIGURE 1.71

Joint reliability function—CAFDE graphic.

**FIGURE 1.72**

Joint failure rate function—CAFDE graphic.

## REFERENCES

Pallerosi, A.C., 2007. Confiabilidade, A quarta dimensão da qualidade. Conceitos básicos e métodos de cálculo. Reliasoft, Brasil.

To practice the case studies use the link <http://www.bqr.com/new-edition-of-the-book-gas-and-oil-reliability-engineering-modeling-and-analysis/>

# ACCELERATED LIFE TEST, RELIABILITY GROWTH ANALYSIS, AND PROBABILISTIC DEGRADATION ANALYSIS

## CHAPTER OUTLINE

<b>2.1</b>	<b>Introduction</b> .....	<b>94</b>
<b>2.2</b>	<b>Quantitative Accelerated Test</b> .....	<b>94</b>
2.2.1	Arrhenius Life–Stress Model .....	97
2.2.2	Eyring Life–Stress Model .....	101
2.2.3	Inverse Power Law Life–Stress Model .....	103
2.2.4	Temperature–Humidity Stress Model .....	104
2.2.5	Thermal–Nonthermal Stress Model.....	109
2.2.6	General Loglinear Life–Stress Model .....	110
2.2.7	Proportional Hazard Model .....	113
2.2.8	Cumulative Risk Model .....	116
<b>2.3</b>	<b>Qualitative Accelerated Test (HALT and HASS)</b> .....	<b>119</b>
<b>2.4</b>	<b>Reliability Growth Analysis</b> .....	<b>122</b>
2.4.1	Duane Model .....	123
2.4.2	Crow–AMSAA Model (NHPP) .....	124
2.4.3	Lloyd–Lipow.....	131
2.4.4	Gompertz Model .....	133
2.4.5	Logistic Model .....	136
2.4.6	Crow Extended Model .....	138
2.4.7	Power Law .....	141
<b>2.5</b>	<b>Probabilistic Degradation Analysis (PDA)</b> .....	<b>143</b>
2.5.1	Linear .....	145
2.5.2	Exponential .....	148
2.5.3	Power.....	150
2.5.4	Logarithmic .....	151
2.5.5	Phase Exponential Model .....	156
	<b>References</b> .....	<b>158</b>

---

## 2.1 INTRODUCTION

Chapter 1 showed how engineers collect historical failure data to conduct life cycle analysis to support decisions about maintenance policies, equipment, and system performance. Most often such analysis is performed on systems during the operation phase or when the system is in the project phase and has operational plant equipment as a reference for historical failure data.

In the oil and gas industry, most of the time the operational plant's equipment (refinery, drill facilities, and platform) will supply the failure data to perform reliability analysis.

In this chapter, accelerated test analysis, conducted mostly in the product development project phase, will be discussed. This is an important approach for companies that supply equipment to the oil and gas industry and need to meet reliability requirements. For oil and gas companies that have process plants, accelerated tests provide information and help make decisions about which equipment to buy based on test performance. In addition, the accelerated testing approach can be used in some cases to supply failure and reliability information about equipment based on reliability prediction or other similar equipment working under harder conditions.

Accelerated tests are used to predict equipment reliability and failures in a short period of time, and most often this approach is conducted during the project development phase. These tests are called "accelerated" because they are performed under harder conditions than usual to force equipment failures faster than usual and predict equipment reliability and failures. In the product development project phase this information is crucial to reducing product development time. Thus there are two types of accelerated tests used, depending on the circumstances:

- Quantitative accelerated life test
- Qualitative accelerated life test

The quantitative accelerated life test is used to predict equipment reliability and understand failure modes, and to test stress conditions used to force such failures to happen in a short period of time.

The qualitative accelerated life test or the highly accelerated life test (HALT) is used to find out a piece of equipment's failure modes and stress conditions, and is conducted to force such failures to happen in a shorter period of time. This kind of accelerated test is most often performed when it is necessary to know equipment failure modes to develop products in a short period of time, and there is not enough time to perform a quantitative accelerated test.

In the product development project phase, when the reliability of a product is not enough and improvements are needed to achieve reliability targets, reliability growth analysis is conducted to see if the modifications of products are resulting in reliability improvements and are achieving reliability targets.

Many issues such as stressor variables, stress levels, periods of testing, and conditions of the test influence the test results. All of these issues will be discussed in this chapter with specific examples from the oil and gas industry. At the end of the chapter it will be easy to see how product development phases and reliability approaches applied in such phases give oil and gas companies the information they need to make decisions about equipment life cycles, many of which greatly influence systems performance.

---

## 2.2 QUANTITATIVE ACCELERATED TEST

As defined, quantitative accelerated tests are used to predict product reliability and to better understand failure modes. The main advantages here are that decisions are made fast and do not impact the product



development phase, and customers can certify that reliability requirements will be achieved or have a high chance of being achieved.

But despite the advantages, quantitative accelerated tests can be expensive and in some cases take longer than expected because test conditions are not easy to define and can give unreliable results. In fact, many things influence quantitative accelerated tests, including:

- Type of stress factor
- Test duration
- Test conditions

To define the type of stress factor it is necessary to know product failures and product weaknesses under certain stress conditions. The usual stressors are temperature, pressure, humidity, tension, vibration, or a combination of these stressors.

Depending on the equipment, such stressors are more applicable than others, such as high temperature in electronic sensors or low temperature in an aerospace product. Many products such as electronic devices have standards to support their tests, but in some cases, especially for new products with unknown behavior failures or even known products with different applications, it is harder to define stressors or a combination of stressors to apply in accelerated tests for reliable results. In all cases the experience of product developers, operators, and maintenance professionals helps when defining stressors and test conditions. In some cases, design failure mode and effects analysis (DFMEA) is conducted to help define product weaknesses, as will be discussed in Chapter 3.

Test duration also highly influences test results, and time is also considered as a stressor when applied during a test period. Thus, regarding stressor level variation over test time, it is possible to have different levels of variation from constant stress level to increasing stress level over all test times. When a stressor value remains constant over test time duration it is called independent. For example, when testing lubricant effects in bearing performance, temperature can be constant over time, so in this case duration is independent because the stressor does not vary over test time.

When the stressor value varies minimally over test time with a defined value and period of time to change duration it is called almost independent, and when the stressor value varies over all test time it is called dependent. For example, in a sensor that operates in a drill, pressure and temperature are two important stressors to be tested, and both stressors will vary during the specific period of time and remain constant until the next stressor level. Thus, in this case, duration is dependent because stressors vary over test time.

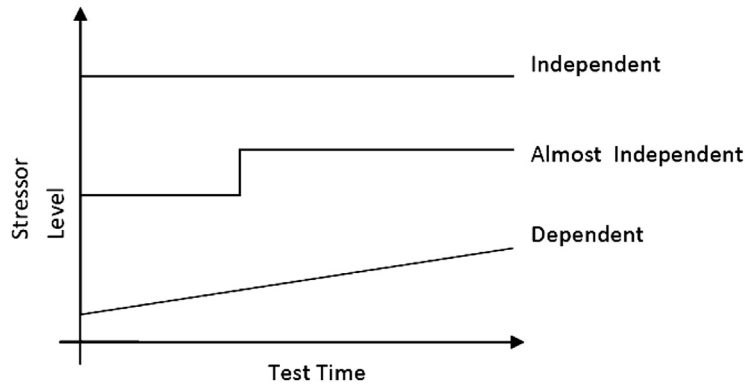
Fig. 2.1 shows the different types of approaches applied in testing for the duration of stresses over test time.

Obviously, test conditions are an important consideration when accelerated tests are being conducted, because reliable test conditions are needed for reliable test results and for reliable equipment, controls, and even the people involved in conducting the test.

Whenever accelerated tests are conducted, some failure is expected with stressors such as high temperature, humidity, voltage, electrical current, vibration, and fatigue.

With high temperature, expected failures include corrosion, creep, electromigration, and interdiffusion.

- Corrosion is the disintegration of a material into its constituent atoms caused by chemical reactions, that is, electrochemical oxidation of metals in reaction to an oxidant such as oxygen that is accelerated by temperature.



**FIGURE 2.1**

Stressor level duration over test time.

- Creep is the tendency of a solid material to deform permanently under the influence of mechanical stresses and temperature. Creep is more severe in materials that are subjected to heat for long periods and close to the melting point. Creep always increases with higher temperatures.
- Electromigration is the transport of material caused by the gradual movement of the ions in a conductor caused by the momentum transfer between conducting electrons and diffusing metal atoms. Such movement is accelerated by high temperature and consequently results in mass transfer and vacancies created where microcracks occur.
- Interdiffusion occurs when two materials are in contact at the surface and molecules can migrate to other material. When subjected to high temperature this process is intensified but is not similar in both materials.

The other stressor is humidity, which influences failures such as corrosion and short circuiting. In the first case, when the metal is in a humid environment it yields electrons that become positively charged ions and consequently cause an electrochemical process that causes fatigue. In the second case, moisture condenses onto surfaces when the temperature is below the dew point, and thus liquid water that deposits on surfaces may coat circuit boards and other insulators, leading to short circuiting inside the equipment.

The high voltage is also used as a stressor in accelerated tests and causes failure on insulators. The insulator loses its function, which is to support or separate electrical conductors without allowing current through.

Electrical current becomes higher when temperature increases and consequently causes component degradation. Such temperature increases corrosion because of increased electrochemical processes.

Higher vibration is also used as a stressor in accelerated tests. Higher vibration is accomplished by introducing a forcing function into a structure, usually with some type of shaker. Two typical types of vibration tests performed are random (all frequencies at once) and sine (one frequency at a time). Sine tests are performed to survey the structural response of the device being tested. A random test is generally considered more closely to replicate a real world environment, such as road inputs to a moving automobile.

Fatigue is also used as a stressor. There are two general types of fatigue tests conducted: the cyclic stress-controlled test and the cyclic strain-controlled test. In the first case the test focuses on the nominal stress required to cause a fatigue failure in a number of cycles. In the second case the strain amplitude is held constant during cycling. Strain-controlled cyclic loading is more representative of the loading found in thermal cycling, where a component expands and contracts in response to fluctuations in the operating temperature.

Whenever a test condition is defined as well as a stressor it is necessary to deal mathematically with data to predict reliability, and there are some models to apply depending on the type of data, type of stressor, and the number of stressors involved in the test. The mathematic life—stress models include:

- Arrhenius
- Eyring
- Inverse power law
- Temperature—humidity (T—H)
- Thermal—nonthermal (T—NT)
- General loglinear (GLL)
- Proportional hazard
- Cumulative risk

### 2.2.1 ARRHENIUS LIFE—STRESS MODEL

The Arrhenius life—stress model has been widely used when the stressor is thermal and is probably the most common life—stress relationship utilized in accelerated life testing. Such a model is used to test electrical and electronic equipment, and whatever product in which reliability is highly influenced by temperature. The following equation describes the thermal effect on equipment or product life:

$$t_v = C \times e^{\frac{E}{kV}}$$

$$B = \frac{E_A}{k}$$

$$t_v = C \times e^{\frac{B}{V}}$$

where  $t_v$  = life under stress conditions;  $C$  = unknown nonthermal constant, which depends on test conditions;  $E_A$  = activation energy, which is the quantity of energy required for a reaction to take place that produces the failure mechanism;  $K$  = Boltzmann's constant ( $8.617 \times 10^{-5}$  eV/K); and  $V$  = stress level, mostly in temperature (kelvin).

To estimate how much equipment is degraded under test conditions when compared with usual conditions it is necessary to know what is called the accelerator factor, that is, the relation between normal life and life under stress, which can be represented mathematically by:

$$AF = \frac{t_{v_u}}{t_{v_A}} = \frac{C \times e^{\frac{B}{v_u}}}{C \times e^{\frac{B}{v_A}}} = e^{\left(\frac{B}{v_u} - \frac{B}{v_A}\right)}$$

To estimate equipment probability density function (PDF) parameters tested under higher temperatures in normal conditions it is necessary to substitute  $t_v$  for the life characteristic parameter, as shown in the next equation.

First, it is necessary to define the PDF that best represents the data tested and substitute its life parameter with the life parameter that represents the equipment under the test condition. For example, the exponential PDF can be used and substitutes the mean time to failure (MTTF) for the life characteristic parameter under stress level; the reliability equation under the stress condition will be:

$$R(t) = e^{-\lambda t} = e^{-\frac{t}{MTTF}}$$

$$t_v = C \times e^{\frac{B}{v}} = MTTF$$

$$R(t, v) = e^{-\frac{t}{t_v}} = e^{-\frac{t}{C \times e^{\frac{B}{v}}}}$$

where  $R(t, v)$  is reliability under test condition  $v$ .

In Weibull PDF, reliability under test condition is:

$$R(t) = e^{\left(-\frac{t}{\eta}\right)^\beta}$$

$$t_v = C \times e^{\frac{B}{v}} = \eta$$

$$R(t, v) = e^{\left(-\frac{t}{C \times e^{\frac{B}{v}}}\right)^\beta}$$

To illustrate the Arrhenius life–stress model, an example of a vibration compressor sensor accelerated life test is given where three groups of sensors are submitted to a temperature stress test. The sensor operational temperature is 120°C (323K), and to define reliability under such conditions the specialist defines three different stress temperatures: 150°C (423K), 200°C (473K), and 250°C (523K). In each temperature a group of similar sensors will be tested. Table 2.1 shows the times of failures in hours when the sensor is under different temperatures. The test result helps to decide if 100% of reliability in 1 year is achieved as a customer requirement.

The Arrhenius model parameters are:

- $B = 1711.6$
- $v_u = 120^\circ\text{C}$  (323K)
- $v_A = 250^\circ\text{C}$  (523K)

Time to Failure— $T$ (K)		
423K	473K	523K
7.884	3.504	2.628
15.768	7.008	5.256
22.776	11.388	7.008
29.784	14.016	8.76
35.916	16.644	11.388
	18.396	13.14
		14.892
		17.52

Applying the accelerated factor (AF) equation, we have:

$$AF = \frac{t_{V_u}}{t_{V_A}} = e^{\left(\frac{1711.6}{323} - \frac{1711.6}{523}\right)} = 7.58$$

The *AF* means that at 523K (250°C) the sensor is degraded 7.58 times more than at 323K (120°C), its usual temperature. Such information also indicates how high the temperature must be to force failure in a short time. The most important information from the test is predicting sensor reliability under usual conditions, shown mathematically as follows:

$$R(t, v) = e^{\left(-\frac{t}{C \times e^{\frac{v}{k}}}\right)^\beta}$$

$$R(t, v) = e^{\left(-\frac{t}{411.39 \times e^{\frac{1711.6}{v}}}\right)^{2.3113}}$$

$$R(8760, 323) = e^{\left(-\frac{8760}{411.39 \times e^{\frac{1711.6}{323}}}\right)^{2.31136}} = 99.44\%$$

The reliability in 1 year (8760 hours) at 120°C is 99.44%, and there is less than a 1% chance of sensor failure in 1 year. The test guarantees the sensor and 100% reliability is proven if the sensor supplier is willing to accept less than 1% of the risk of not achieving the sensor reliability requirement. Fig. 2.2 shows reliability time. The Weibull 2P parameters are  $\beta = 2.3113$  and  $\eta = 82,400$ .

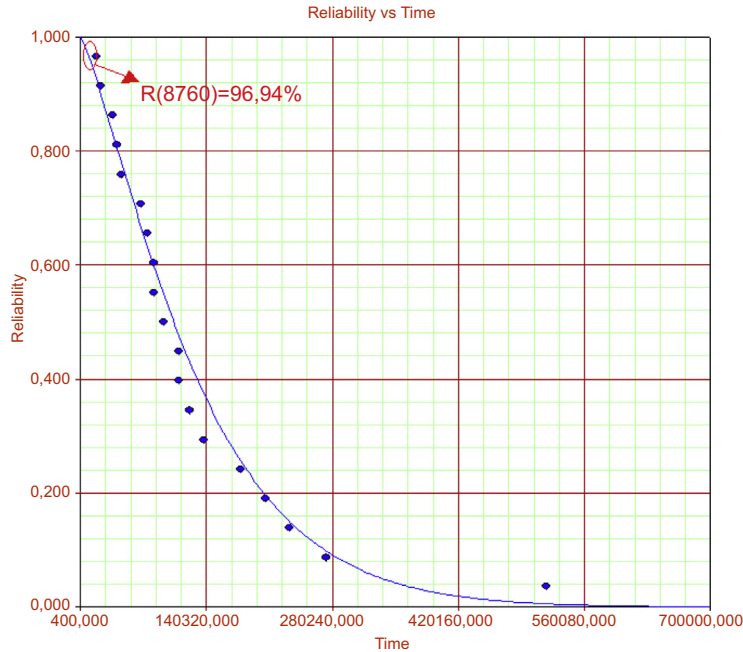


FIGURE 2.2

Sensor reliability curve under usual conditions.

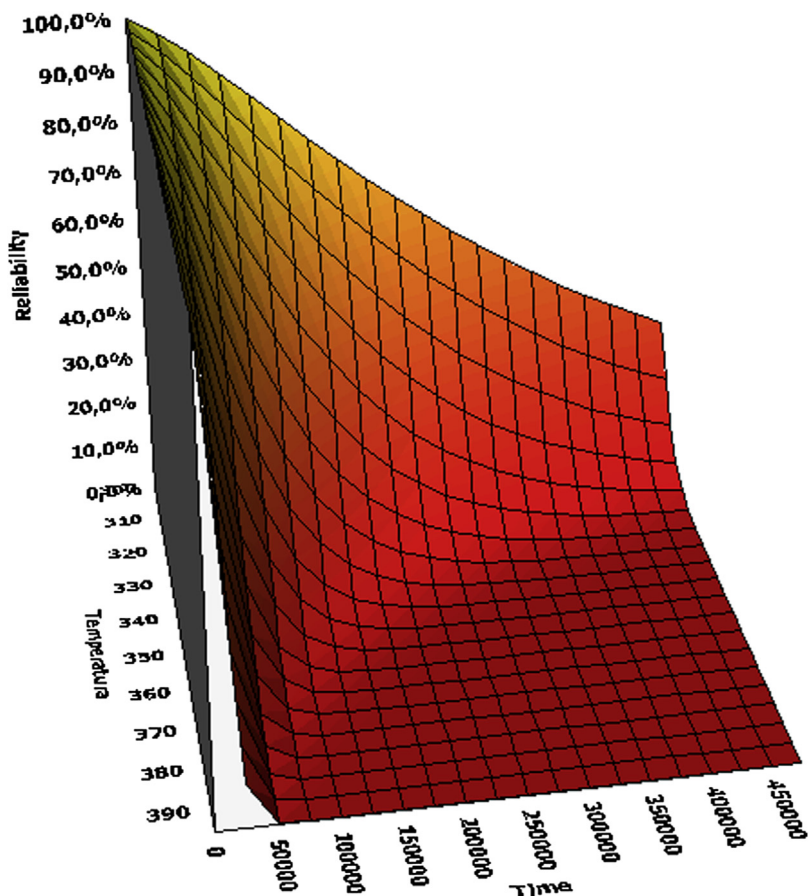


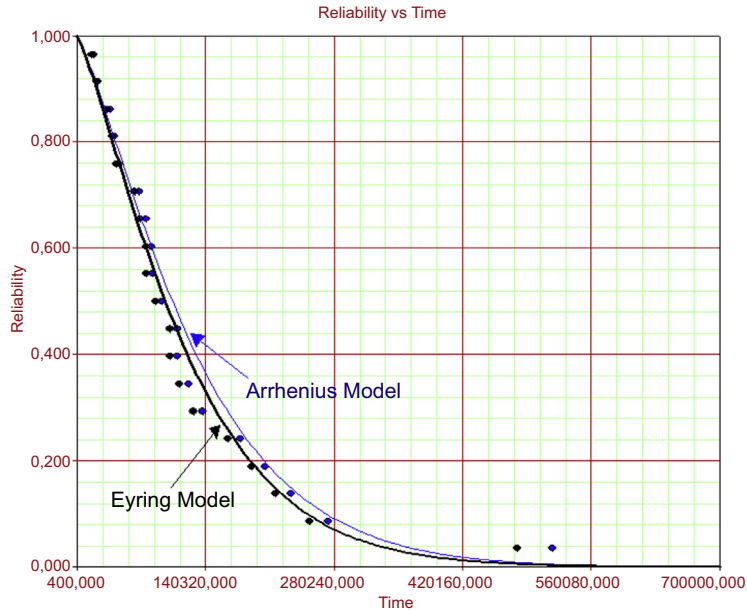
FIGURE 2.3

Sensor reliability curve under different temperature conditions.

Using software such as ALTA PRO (Reliasoft) to assess accelerated test data enables faster conclusions, and it is easier to understand final test results. In fact, reliability decisions are supported by software that enables complex mathematical solutions that were until now difficult to perform. Figs. 2.3 and 2.4 shows a 3D graph of reliability time and temperature, which shows a different reliability curve per time and per temperature. Thus the higher the temperature, the worse the reliability over time.

In addition, there is also a life cycle thermal model that is applied to devices submitted to cycle temperatures. Such a model is well applied in aeronautic equipment, and the number of cycles until failure is defined mathematically by an inverse power equation known as the Coffin–Manson relationship, described by:

$$N = \frac{A}{(\Delta t)^\beta}$$



**FIGURE 2.4**

Reliability  $\times$  time (Eyring and Arrhenius models).

where  $N$  = number of cycles;  $A$  and  $\beta$  = constants characteristic of material property and product design ( $\beta > 0$ ); and  $\Delta t$  = range of temperature.

### 2.2.2 EYRING LIFE—STRESS MODEL

The Eyring life—stress model is used when the stressor is thermal, such as in the Arrhenius life—stress model. Such a model is used to test electrical and electronic equipment and any product where reliability is highly influenced by temperature or humidity. The following equation describes the thermal effect on equipment or product life of the Eyring model:

$$t_v = \frac{1}{V} \times e^{-\left(A - \frac{E_A}{kV}\right)}$$

$$B = \frac{E_A}{k}$$

$$t_v = \frac{1}{V} \times e^{-\left(A - \frac{B}{V}\right)}$$

where  $t_v$  = life under stress conditions;  $A$  = unknown nonthermal constant, which depends on test conditions;  $E_A$  = activation energy, which is the quantity of energy required for a reaction to take place that produces the failure mechanism;  $K$  = Boltzmann's constant ( $8.617 \times 10^{-5}$  eV/K); and  $V$  = stress level, mostly in temperature (kelvin).

In the Arrhenius model, the accelerator factor is represented by:

$$AF = \frac{t_{v_u}}{t_{v_A}} = \frac{\frac{1}{V_u} \times e^{-\left(A - \frac{B}{V_u}\right)}}{\frac{1}{V_A} \times e^{-\left(A - \frac{B}{V_A}\right)}} = \frac{V_A}{V_u} e^{\left(\frac{B}{V_u} - \frac{B}{V_A}\right)}$$

In addition, a characteristic life parameter such as  $\mu$  or  $\eta$  is needed to take the place of  $t_v$ . First, it is necessary to define the PDF that best represents the data tested and substitute its life parameter with the life parameter that represents the equipment under the test condition. For example, with the Weibull PDF, the reliability under the test condition is:

$$R(t) = e^{\left(-\frac{t}{\eta}\right)^\beta}$$

$$t_v = \frac{1}{V} \times e^{-\left(A - \frac{B}{V}\right)} = \eta$$

$$R(t, v) = e^{\left(-\frac{t}{\frac{1}{V} \times e^{-\left(A - \frac{B}{V}\right)}}\right)^\beta}$$

Applying the same data from the compressor sensor vibration accelerated test used with the Eyring model the parameters are:

- $B = 1241.56$
- $A = -13.1765$
- $v_u = 120^\circ\text{C}$  (323K)
- $v_A = 250^\circ\text{C}$  (523K)

Applying the  $AF$  as follows we have:

$$AF = \frac{V_A}{V_u} e^{\left(\frac{B}{V_u} - \frac{B}{V_A}\right)} = \frac{523}{323} e^{\left(\frac{1241.56}{323} - \frac{1241.56}{523}\right)} = 7.04$$

The  $AF$  means that at 523K (250°C) the sensor is degraded 7.04 times more than at 323K (120°C), its usual temperature. The  $AF$  in the Eyring model (7.04) has almost the same value as the  $AF$  in the Arrhenius model (7.58). The other important information found is the sensor reliability under usual conditions, expressed mathematically as:

$$R(t, v) = e^{\left(-\frac{t}{\frac{1}{V} \times e^{-\left(A - \frac{B}{V}\right)}}\right)^\beta}$$

$$R(8760, 323) = e^{\left(-\frac{8760}{\frac{1}{323} \times e^{-\left(-13.1765 - \frac{1241.56}{323}\right)}}\right)^{2.3075}} = 99.33\%$$

The reliability in 1 year (8760 hours) at 120°C is 99.33%, very close to the reliability of the Arrhenius model (99.44%). Thus there is less than 1% (0.67%) of chance that sensor fails in 1 year. The accelerated test Eyring model enable to predict the sensor reliability and shows similar results when compared with the Arrhenius model results. The Weibull 2P parameters in the Eyring model are  $\beta = 2.3075$  and  $\eta = 76,300$  and in the Arrhenius model  $\beta = 2.1331$  and  $\eta = 82,400$ . The reliability curve in both cases is very similar under such test conditions.



### 2.2.3 INVERSE POWER LAW LIFE—STRESS MODEL

The inverse power law life—stress model is more appropriate when the stressor is nonthermal, such as in tension, vibration, fatigue, etc. Such a model is used to test electrical, electronic, and mechanical equipment and whatever product where reliability is well represented for the inverse power equation when it is under accelerated test conditions. The equation that describes the nonthermal effect on equipment or product life is:

$$t_V = \frac{1}{k \times V^n}$$

where  $t_V$  = life under stress conditions;  $n$  = stress factor that describes load stress effect on equipment life;  $K$  = constant that depends on test conditions; and  $V$  = stress level.

In the inverse power law model the  $AF$  is represented by:

$$AF = \frac{t_{V_U}}{t_{V_A}} = \frac{\frac{1}{k \times V_U^n}}{\frac{1}{k \times V_A^n}} = \left( \frac{V_A}{V_U} \right)^n$$

In addition, the characteristic life parameter concerning accelerated test conditions, ( $t_V$ ) have to replace the characteristic life parameter such as  $\mu$ ,  $MTTF$ , or  $\eta$  to estimate PDF or reliability under test conditions. For the Weibull 2P the reliability under the test condition is:

$$R(t, V) = e^{-\left(\frac{t}{\eta}\right)^\beta}$$

$$t_V = \frac{1}{k \times V^n}$$

$$R(t, V) = e^{-\left(\frac{t}{\frac{1}{k \times V^n}}\right)^\beta} = e^{-(k \times V^n \times t)^\beta}$$

To illustrate the inverse power law model, a bearing pump test was conducted to improve its reliability performance required for refinery maintenance management. In this accelerated test, three different levels of rotation (rpm) were tested to test three similar groups of bearings: 3000, 3500, and 4000 rpm. Table 2.2 shows the bearing failures in time (hours) under test conditions. The test results help to decide if bearing reliability under usual conditions is acceptable. The target is 99.99% in 3 years (26.28 hours) under 1200 rpm.

The inverse power law model parameters are:

$$\beta = 2.42$$

$$k = 3.87E - 25$$

$$n = 6.2732$$

Applying the  $AF$  equation we have:

$$AF = \left( \frac{V_A}{V_U} \right)^n$$

$$AF = \left( \frac{4000}{1200} \right)^{6.2732} = 1906$$

<b>Time to Failure (hours)</b>	<b>Rotation (rpm)</b>
320.52	3000
346.36	3000
350.19	3000
401.26	3000
111.34	3500
146.67	3500
152.01	3500
154.51	3500
254.85	3500
10.17	4000
11.33	4000
33.5	4000
66	4000
83.34	4000
84.84	4000

The  $AF$  means that at 4000 rpm the bearing is degraded 1906 times more than at 1200 rpm, its usual rotation. The test can also help predict bearing reliability (3 years) under usual conditions (1200 rpm), mathematically expressed as:

$$R(t, V) = e^{-(k \times V^n \times t)^\beta}$$

$$R(26, 280, 1200) = e^{-(3.87E-25 \times (1200)^{6.2732} \times 26,280)^{2.4258}}$$

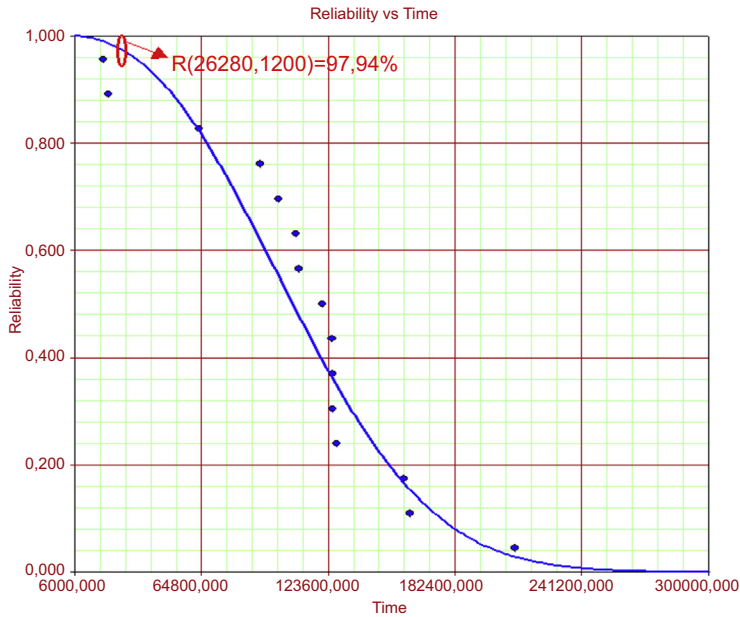
$$R(26, 280, 1200) = 97.74\%$$

The reliability in 3 years (26,280 hours) at 1200 rpm is 97.74%, less than expected. In this case, some bearing improvement is required to achieve customer reliability requirements. Fig. 2.5 shows the reliability time graph. The Weibull 2P parameters are  $\beta = 2.42$  and  $\eta = 124,700$ . In the next section we will present reliability growth analysis methodology, which is used to assess whether products are achieving reliability targets after reliability improvement actions are performed during the development phase.

Fig. 2.6 shows the 3D reliability time rotation graph, which shows the different reliability curves per time and per rotation. Thus the higher the rotation, the worse the reliability is over time.

#### 2.2.4 TEMPERATURE—HUMIDITY STRESS MODEL

The T–H life–stress model is appropriate when temperature and humidity greatly influence equipment such as sensors and other electronic devices. Such a model is used to test electrical, electronic, and mechanical equipment and other products in which reliability is represented well for the



**FIGURE 2.5**

Bearing reliability × time under operational conditions.

exponential equation under accelerated testing conditions. The equation that describes thermal effects on equipment or product life is:

$$t_{V,U} = A \times e^{\left(\frac{\varphi}{V} + \frac{b}{U}\right)}$$

where  $t_{V,U}$  = life under stress conditions;  $\varphi$  = factor that influences temperature stress;  $b$  = factor that influences humidity stress;  $A$  = constant that depends on test conditions;  $V$  = stress level in temperature (kelvin); and  $U$  = stress level of humidity (%).

In the T–H model the  $AF$  is defined by:

$$AF = \frac{t_{V_U, U_U}}{t_{V_A, U_A}} = e^{\left[\varphi \times \left(\frac{1}{V_U} - \frac{1}{V_A}\right) + b \times \left(\frac{1}{U_U} - \frac{1}{U_A}\right)\right]}$$

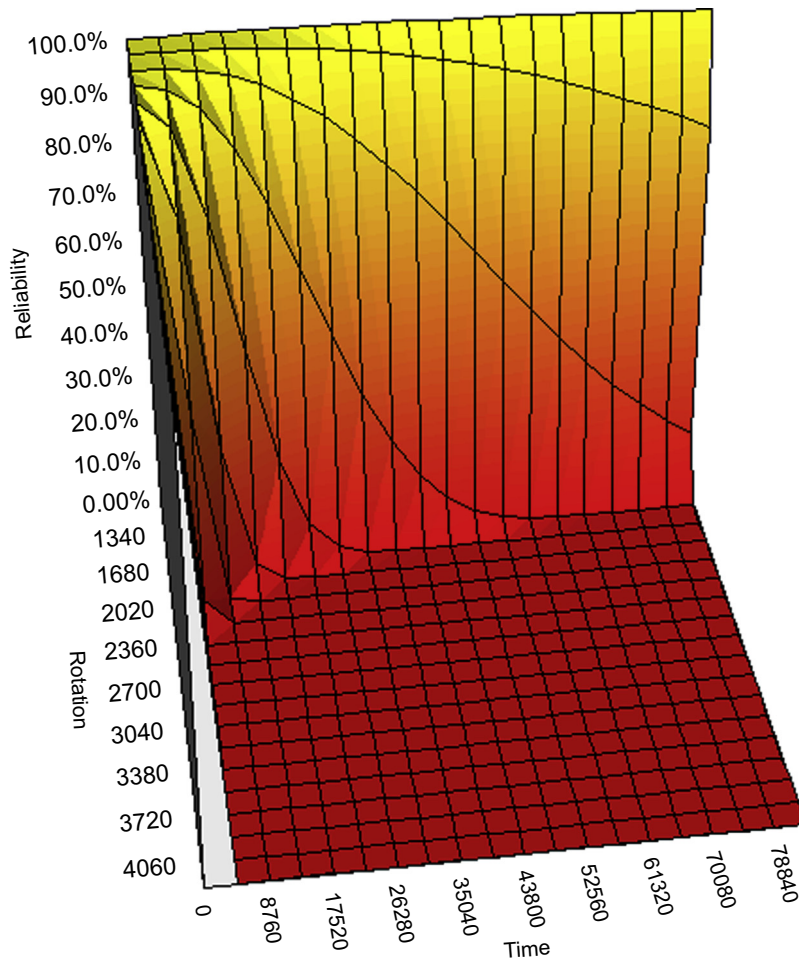
In addition, to estimate reliability under stress conditions (humidity and temperature), a characteristic life parameter such as  $\eta$  is substituted for  $t_{V_A}$ . For Weibull 2P, for example, the reliability under test conditions is:

$$R(t, V, U) = e^{-\left(\frac{t}{\eta}\right)^\beta}$$

$$t_{V,U} = A \times e^{\left(\frac{\varphi}{V} + \frac{b}{U}\right)}$$

$$R(t, V, U) = e^{-\left(\frac{t}{A \times e^{\left(\frac{\varphi}{V} + \frac{b}{U}\right)}}\right)^\beta}$$

$$R(t, V, U) = e^{-\left(\frac{t}{A} \times e^{-\left(\frac{\varphi}{V} + \frac{b}{U}\right)}\right)^\beta}$$



**FIGURE 2.6**

Bearing reliability curve under different rotation conditions.

To clarify the T–H model, a logic element example in safety instrumented function configuration is given as follows, where temperature and humidity are tested to predict reliability under operational conditions: 25°C and 15% humidity. Under test conditions the temperature is stated in two levels: 120°C (373K) and 150°C (393K) as well as humidity: 35% and 75%. Such conditions test two groups of similar logic elements. Table 2.3 shows the logic element failures in time (hours) under test conditions. This test helps determine gas detector reliability.

The T–H model parameters are:

$$\varphi = 5827.31$$

$$b = 0.0464$$

Time to Failure	Temperature (K)	Humidity (%)
305	373	0.35
311	373	0.35
325	373	0.35
401	373	0.35
275	373	0.75
293	373	0.75
315	373	0.75
370	373	0.75
105	393	0.35
115	393	0.35
116	393	0.35
195	393	0.35

$A = 4.98 \times 10^{-5}$   
 $V = 373 \text{ and } 393\text{K}$   
 $U = 35\% \text{ and } 75\%$

Applying the  $AF$  we have:

$$AF = \frac{t_{V_U, U_U}}{t_{V_A, U_A}} = e^{\left[ \varphi \times \left( \frac{1}{V_U} - \frac{1}{V_A} \right) + b \times \left( \frac{1}{U_U} - \frac{1}{U_A} \right) \right]}$$

Applying parameter factors the  $AF$  is:

$$AF = e^{\left[ \varphi \times \left( \frac{1}{V_U} - \frac{1}{V_A} \right) + b \times \left( \frac{1}{U_U} - \frac{1}{U_A} \right) \right]}$$

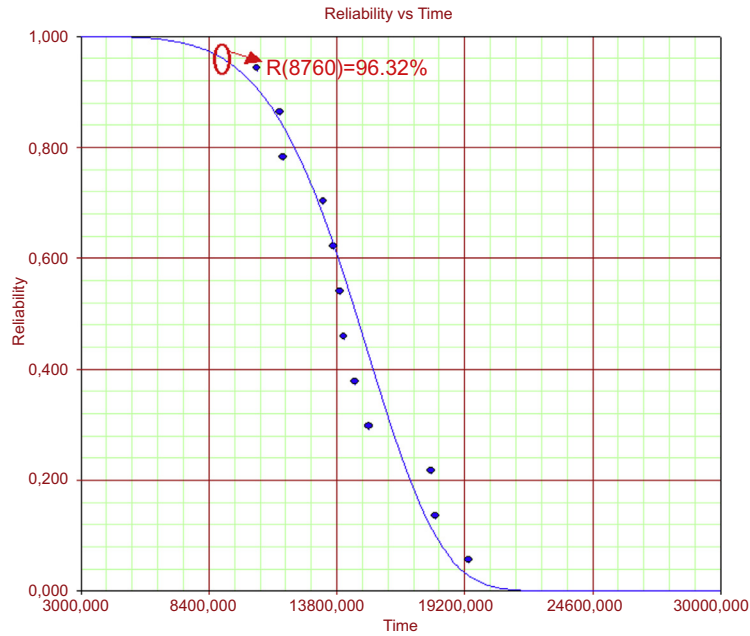
$$AF = e^{\left[ 5827.31 \times \left( \frac{1}{298} - \frac{1}{393} \right) + 0.0464 \times \left( \frac{1}{15} - \frac{1}{75} \right) \right]} = 112.16$$

The  $AF$  means that at 393K (120°C) and 75% humidity the detector degraded 112 times more than at 298K (25°C) and 15% humidity, the usual temperature and humidity operational conditions. This test can also help predict logic element reliability under usual conditions, expressed mathematically as:

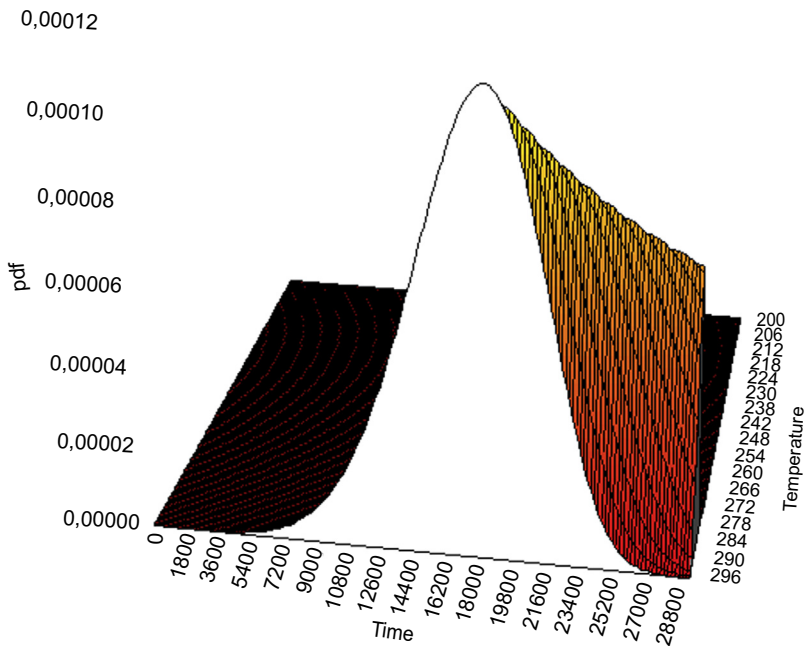
$$R(8760, 298, 15\%) = e^{-\left( \frac{8760}{4.98 \times 10^{-5}} e^{-\left( \frac{5827.31}{298} + \frac{0.0464}{15} \right)} \right)^{5.81}} = 96.32\%$$

The reliability in 1 year (8760 hours) at 25°C and 15% humidity is 96.32%, and there is a more than 3% chance of logic element failure in 1 year. Fig. 2.7 shows reliability time. The Weibull 2P parameters are  $\beta = 5815$  and  $\eta = 15,540$ .

Fig. 2.8 shows the PDF dislocation to the right when temperature decreases, which means failure probability is lower under operational conditions than in stress temperature conditions.



**FIGURE 2.7**  
Logic element reliability curve under operational conditions.



**FIGURE 2.8**  
Logic element PDF curve under temperature conditions.

### 2.2.5 THERMAL–NONTHERMAL STRESS MODEL

The T–NT life–stress model is comprised of two other models: the Arrhenius model and the inverse power law model. The T–NT model is appropriate when temperature and other nonthermal stressors affect equipment such as electronic devices. This type of test is applied to understand how temperature and tension affect electronic devices. The following equation represents life under stress conditions for both stressors (temperature and tension):

$$t_{V,U} = \left[ A \times e^{\frac{B}{V}} \right] \left[ \frac{1}{k \times U^n} \right]$$

$$C = \frac{A}{K}$$

$$t_{V,U} = \frac{A \times e^{\frac{B}{V}}}{k \times U^n} = \frac{C}{U^n \times e^{-\frac{B}{V}}}$$

where  $t_{V,U}$  = life under stress conditions;  $C$  = unknown nonthermal constant that depends on test conditions;  $B$  = factor that influences temperature stress;  $n$  = factor related to nonthermal stress;  $A$  = unknown nonthermal constant that depends on test conditions;  $K$  = Boltzmann's constant ( $8.617 \times 10^{-5}$  eV/K);  $V$  = stress level, mostly in temperature (kelvin); and  $U$  = nonthermal stress level.

In the T–NT model, the  $AF$  equation is represented by:

$$AF = \frac{t_{V_U, U_U}}{t_{V_A, U_A}} = \frac{\frac{C}{U_u^n \times e^{-\frac{B}{V_u}}}}{\frac{C}{U_A^n \times e^{-\frac{B}{V_A}}}} = \frac{C}{U_u^n \times e^{-\frac{B}{V_u}}} \times \frac{U_A^n \times e^{-\frac{B}{V_A}}}{C} = \left( \frac{U_A}{U_U} \right)^n \times \left( \frac{e^{-\frac{B}{V_A}}}{e^{-\frac{B}{V_U}}} \right) = \left( \frac{U_A}{U_U} \right)^n \times e^{B \left( \frac{1}{V_U} - \frac{1}{V_A} \right)}$$

Additionally, a characteristic life parameter under stress conditions such as  $t_{V,U}$  must to replace the Weibull characteristic life parameter  $n$  to estimate reliability under test conditions. For the Weibull 2P, the reliability under test conditions is:

$$R(t, V, U) = e^{-\left(\frac{t}{n}\right)^\beta}$$

$$R(t, V, U) = e^{-\left(\frac{\frac{t}{C}}{U^n \times e^{-\frac{B}{V}}}\right)^\beta}$$

$$R(t, V, U) = e^{-\left(\frac{t \times U^n \times e^{-\frac{B}{V}}}{C}\right)^\beta}$$

To illustrate the T–NT model, a vessel temperature sensor in a refinery plant was tested to estimate reliability under operational conditions. In this case, temperature and voltage are the stresses and vary from 100°C (373K) to 120°C (393K) and from 8 V to 12 V, respectively. Operational conditions are 30°C (303 V) and 2 V. Table 2.4 shows sensor failure in time (hours) under test conditions.

The T–NT model parameters are:

$$C = 42.26$$

$$B = 2057.74$$

**Table 2.4 Time to Failures in Accelerated Test (Thermal–Nonthermal)**

Time to Failure	Temperature (K)	Voltage (V)
780	373	8
812	373	8
818	373	8
982	373	8
540	373	12
576	373	12
373	393	12
598	393	8
620	393	8
756	393	8

$n = 1.26$   
 $V = 393 \text{ K}$   
 $U = 12 \text{ V}$

Applying the  $AF$  equation we have:

$$AF = \frac{t_{V_U, U_U}}{t_{V_A, U_A}} = \left(\frac{U_A}{U_U}\right)^n \times e^{B\left(\frac{1}{V_U} - \frac{1}{V_A}\right)} = \left(\frac{12}{2}\right)^{1.24} \times e^{2057.74\left(\frac{1}{303} - \frac{1}{393}\right)} = 43.53$$

The  $AF$  means that at 393K (120°C) and 12 V the sensor degraded 44 times more than at 303K (30°C) and 2 V, the operational conditions. This test can also help predict logic element reliability under usual conditions, expressed mathematically as this equation:

$$R(t, V, U) = e^{-\left(\frac{t \times U^n \times e^{-\frac{B}{V}}}{C}\right)^\beta}$$

$$R(8760, 303, 2) = e^{-\left(\frac{8760 \times 2^{1.24} \times e^{-\frac{2057.74}{303}}}{48.26}\right)^{11.28}} = 99.97\%$$

The reliability in 1 year (8760 hours) at 30°C and 2 V is 99.97%. Fig. 2.9 shows reliability time. The Weibull 2P parameters are  $\beta = 11.28$  and  $\eta = 18,120$ .

Fig. 2.10 shows the failure rate under different temperature conditions. With higher temperatures, the failure rate increases sooner.

### 2.2.6 GENERAL LOGLINEAR LIFE–STRESS MODEL

The GLL life–stress model is well represented by the exponential function, which comprises several stressor effects that are described by vectors, as shown in the following equation:

$$t(\underline{X}) = e^{\alpha_0 + \sum_{j=1}^n \alpha_j X_j}$$

where  $\alpha_j$  = model parameters and  $\underline{X}$  = vector with  $n$  stressors.





FIGURE 2.9

Sensor reliability curve under operational conditions.

Other models such as the Arrhenius or inverse power law models, for example, can be used to represent stressor effects, and, for example, the equation for two thermal stressors and one nonthermal stressor factor is:

$$t_{V_1, V_2, U} = e^{\alpha_0 + \alpha_1 \times \frac{1}{V_1} + \alpha_2 \times \frac{1}{V_2} + \alpha_3 \times \ln(U)}$$

Applying the AF equation we have:

$$AF = \frac{t_{V_{U_1}, V_{U_2}, U_U}}{t_{V_{A_1}, V_{A_2}, U_A}} = \frac{e^{\alpha_0 + \frac{\alpha_1}{V_{U_1}} + \frac{\alpha_2}{V_{U_2}} + \alpha_3 \times \ln(U_U)}}{e^{\alpha_0 + \frac{\alpha_1}{V_{A_1}} + \frac{\alpha_2}{V_{A_2}} + \alpha_3 \times \ln(U_A)}}$$

$$AF = e^{\left[ \left( \alpha_0 + \frac{\alpha_1}{V_{U_1}} + \frac{\alpha_2}{V_{U_2}} + \alpha_3 \times \ln(U_U) \right) - \left( \alpha_0 + \frac{\alpha_1}{V_{A_1}} + \frac{\alpha_2}{V_{A_2}} + \alpha_3 \times \ln(U_A) \right) \right]}$$

A characteristic life parameter under stress conditions such as  $t_{V_1, V_2, U}$  must to replace the Weibull characteristic life parameter  $n$  to estimate reliability under test conditions. For the Weibull 2P, reliability under test conditions is:

$$R(t, V_1, V_2, U) = e^{-\left(\frac{t}{n}\right)^\beta}$$

$$R(t, V_1, V_2, U) = e^{-\left(\frac{t}{e^{\alpha_0 + \frac{\alpha_1}{V_1} + \frac{\alpha_2}{V_2} + \alpha_3 \times \ln(U)}}\right)^\beta}$$

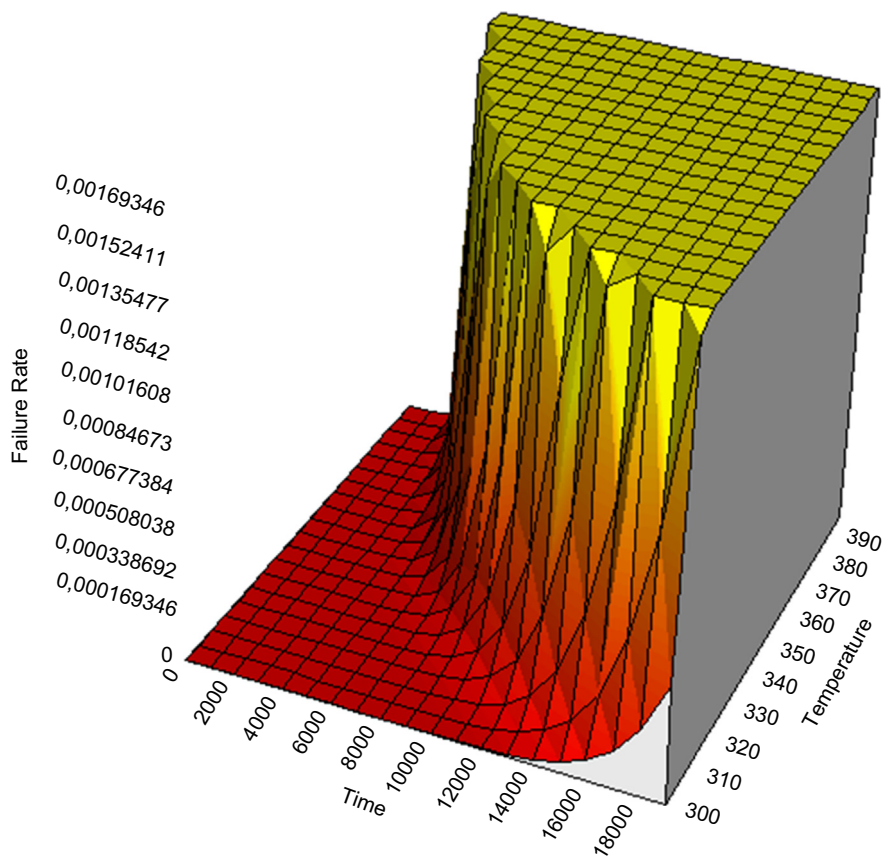


FIGURE 2.10

Failure rate under temperature conditions.

To illustrate the GLL model, a vessel temperature sensor at a refinery plant is shown as an example. Thus in this case temperature, humidity, and voltage are the stressors, which vary from 100°C (373K) to 120°C (393K), from 70% to 90%, and from 8 V to 12 V, respectively, and the operational conditions are 30°C (303K), 15%, and 2 V. Table 2.5 shows the sensor failures in time (hours) under test conditions.

The T–NT model parameters are:

$$\beta = 11.88$$

$$\alpha_0 = 14.48$$

$$\alpha_1 = -0.186$$

$$\alpha_2 = -0.1375$$

$$\alpha_3 = 0.50$$

**Table 2.5 Time to Failures in Accelerated Test (General Loglinear Model)**

Time to Failure	Temperature (K)	Voltage (V)	Humidity (%)
780	373	8	0.7
812	373	8	0.7
818	373	8	0.7
982	373	8	0.7
540	373	12	0.7
576	373	12	0.9
373	393	12	0.9
598	393	8	0.9
620	393	8	0.9
756	393	8	0.9

Applying the *AF* equation we have:

$$AF = e^{\left[ \left( \alpha_0 + \frac{\alpha_1}{V_{U1}} + \frac{\alpha_2}{V_{U2}} + \alpha_3 \times \ln(U_U) \right) - \left( \alpha_0 + \frac{\alpha_1}{V_{A1}} + \frac{\alpha_2}{V_{A2}} + \alpha_3 \times \ln(U_A) \right) \right]}$$

$$AF = e^{\left[ \left( 14.48 + \frac{-0.186}{303} + \frac{-0.1375}{15} + 0.5 \times \ln(2) \right) - \left( 14.48 + \frac{-0.186}{393} + \frac{-0.1375}{90} + 0.5 \times \ln(12) \right) \right]}$$

$$AF = 0.4031$$

The *AF* means that at 393K (120°C), 90% humidity, and 12 V, the sensor degraded 45.83 times more than at 303K (30°C), 15% humidity, and 2 V, its operational condition.

Applying the reliability function under usual conditions we see the sensor achieves 100% reliability in 1 year (8760 hours), as shown in the following equation. This test can also be used to predict sensor reliability under usual conditions, expressed mathematically as:

$$R(t, V_1, V_2, U) = e^{-\left( \frac{t}{e^{\left( \alpha_0 + \frac{\alpha_1}{V_1} + \frac{\alpha_2}{V_2} + \alpha_3 \ln(U) \right)}} \right)^\beta}$$

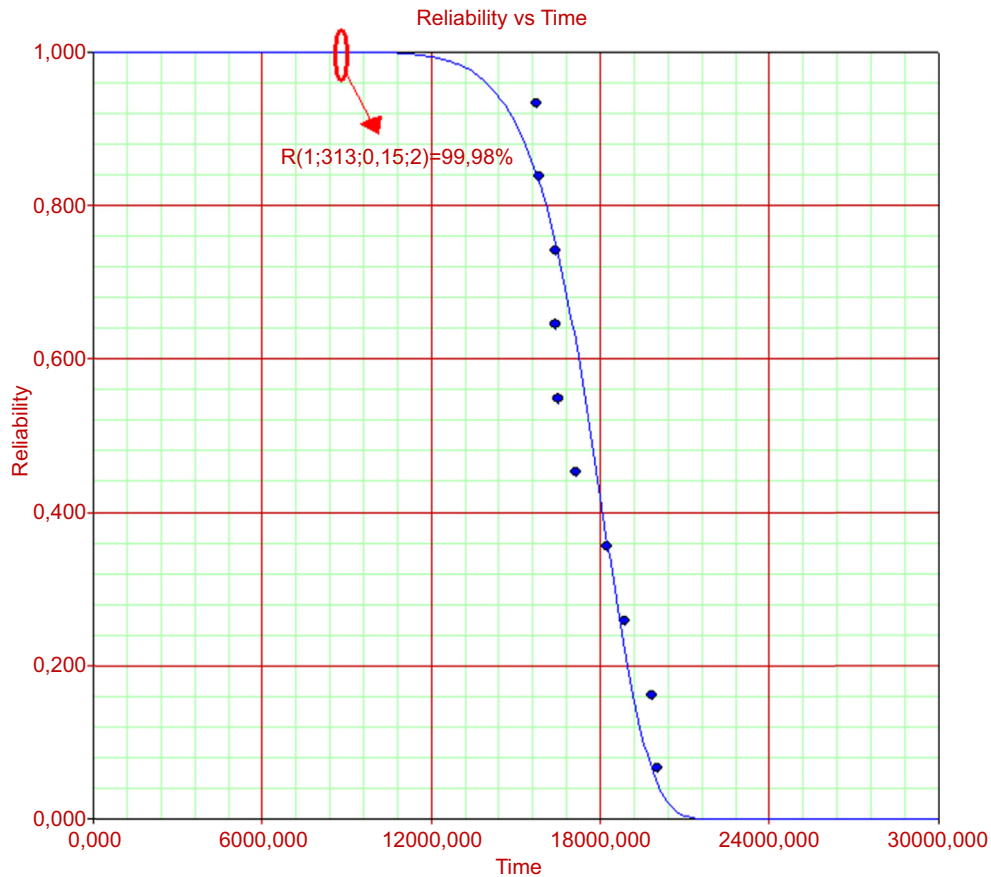
$$R(1, 303, 0.15, 2) = e^{-\left( \frac{1}{e^{\left( 14.48 + \frac{-0.186}{303} + \frac{-0.1375}{0.15} + 0.5 \times \ln(2) \right)}} \right)^{11.88}} = 100\%$$

The reliability at 30°C, 15% humidity, and 2 V is 100% in 1 year (8760 hours). Fig. 2.11 shows reliability time under operational conditions predicted from the accelerated test conditions. The Weibull 2P parameters are  $\beta = 11.88$  and  $\eta = 9,710,000$ .

Fig. 2.12 shows reliability, temperature, and voltage under operational conditions predicted from the accelerated test conditions. As we can see, the higher the temperature, the lower the reliability over time.

### 2.2.7 PROPORTIONAL HAZARD MODEL

The proportional hazard life—stress model developed by Dr D.R. Cox uses several stressor effects in failure rate function, with a specific function to describe covariance between variables such as



**FIGURE 2.11**  
Sensor reliability curve under operational conditions.

temperature, humidity, voltage, etc. The proportional hazard model has been most widely used in the medical field in applications such as survival times of cancer patients. In recent years, the model has received attention from researchers in reliability studies. This is not surprising in view of the direct analogy between human mortality and equipment failure. The failure rate is usually defined as:

$$\lambda(t) = \frac{f(t)}{R(t)}$$

where  $f(t)$  = PDF function and  $R(t)$  = reliability function.

When stressor covariance is taken into account the failure rate function is defined as:

$$g(\underline{x}, \underline{A}) = e^{\sum_{j=1}^m A_j x_j}$$

$$\lambda(t, \underline{x}) = \lambda_0(t) \times e^{\sum_{j=1}^m A_j x_j}$$

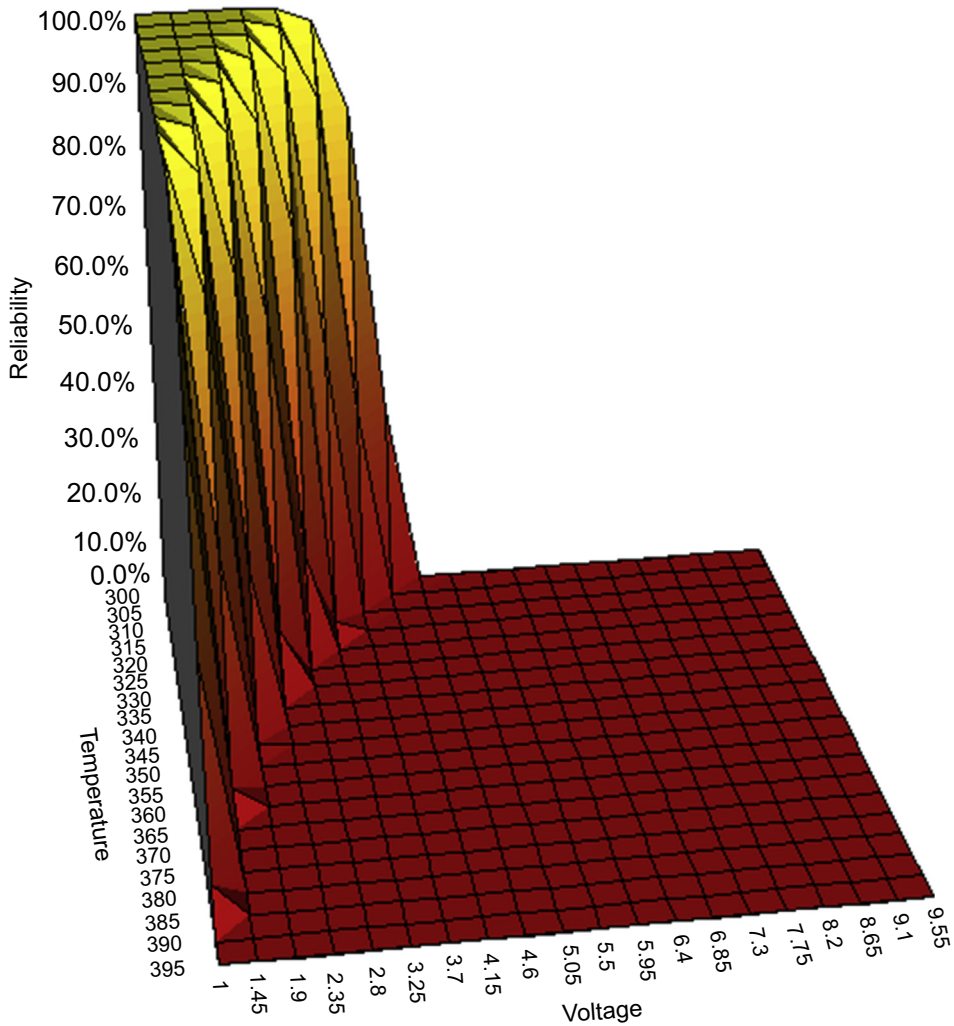


FIGURE 2.12

Reliability × temperature × voltage (logic element).

where  $\lambda_0(t)$  = failure rate function;  $g(\underline{x}, \underline{A})$  = a function that takes into account covariance between stressors;  $\underline{x} = (x_1, x_2, \dots, x_n)$ ;  $\underline{A} = (A_1, A_2, \dots, A_n)^T$ ;  $\underline{x}$  = row vector with covariance values; and  $\underline{A}$  = column vector with unknown parameters.

In Weibull distribution the failure rate is:

$$\lambda(t, \underline{x}) = \frac{\beta}{\eta} \left(\frac{t}{\eta}\right)^{\beta-1} \times e^{\sum_{j=1}^m A_j x_j}$$

Time to Failure	Temperature (K)
788.4	423
1576.8	423
2978.4	423
3591.6	423
22,776	423
262.8	523
525.6	523
700.8	523
876	523
1138.8	523
1314	523
1489.2	523
1752	523

To illustrate the proportional hazard model, a vessel temperature sensor similar to the one applied in the T–NT model (Section 2.2.5) will be considered here. Table 2.6 shows temperature sensor failures in time (hours) under test conditions.

Fig. 2.13 shows the failure rate for different temperature cycles, and for 8760 hours the failure rate is 0.845. A variation of the proportional hazard model is the nonproportional hazard model in which covariates vary over time. The other important issue to be regarded in this test is the cumulative effect of stressor factors. The next section will introduce the cumulative risk model, which considers the cumulative effects of stress.

## 2.2.8 CUMULATIVE RISK MODEL

To have test results sooner, in some cases the stressor is varied over time, and to model cumulative stressor effects on the component the cumulative risk life–stress model is proposed. Thus it is necessary to define the cumulative effects of stress and regard such effects on the reliability function under test conditions. So to represent the stressor effects for the inverse power law model, for example, we have:

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^\beta}$$

$$R(t, V) = e^{-\left(\frac{t}{t_V}\right)^\beta}$$

$$t_V = \frac{1}{K \times V^n} = \eta$$

$$R(t, V) = e^{-\left(\frac{t}{\frac{1}{K \times V^n}}\right)^\beta} = e^{-(K \times V^n)^\beta}$$

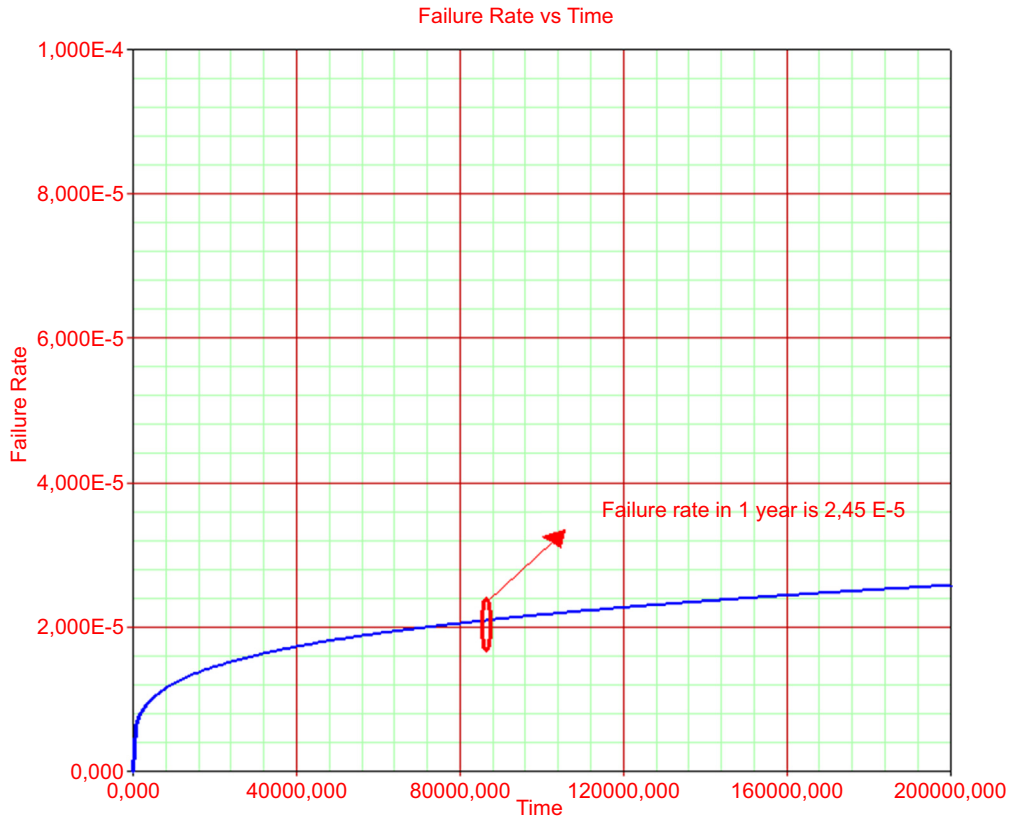


FIGURE 2.13

Failure rate under operational conditions (40°C = 313K).

For different stressor levels there will be different reliability equations, so for the three different stress levels we have levels 1, 2, and 3 and the equations are:

$$R(t, V_1) = e^{-(K \times V_1^n \times t)^\beta}$$

$$R(t, V_2) = e^{-(K \times V_2^n \times t)^\beta}$$

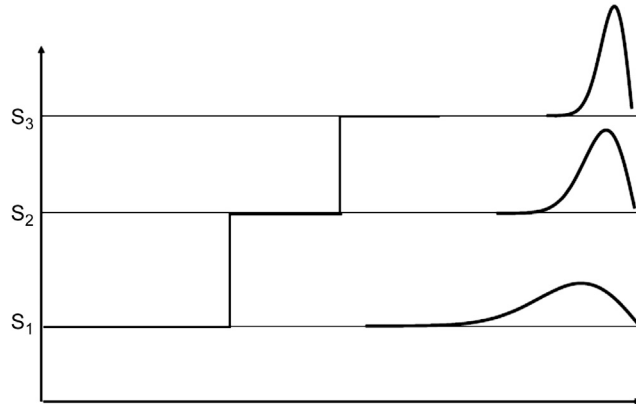
$$R(t, V_3) = e^{-(K \times V_3^n \times t)^\beta}$$

Fig. 2.14 shows the different stress levels over time, and such a configuration depends on the test being conducted.

Despite the importance of assessing stressor effects in each stress level the most important assessment is the cumulative effect during the whole test time, and in this case it is necessary to assess the stress level effects of period T1 in period T2, and so on. To assess such cumulative effects it is

FIGURE 2.14

Stress level over test time.



necessary to take into account damage caused in testing components in failure time and to include the time the test began. The cumulative effects are represented by:

$$R(t, V_2) = e^{-(K \times V_2^n((t-t_1)+\epsilon_1))^\beta}$$

where  $\epsilon_1$  = accumulate age from first stress level and  $t - t_1$  = period of failure under stress level 2.

The general reliability equation regarding different stress levels is:

$$R(t, V_i) = e^{-(K \times V_i^n((t-t_{i-1})+\epsilon_{i-1}))^\beta}$$

where:

$$\epsilon_{i-1} = (t_{i-1} - t_{i-2}) \left( \frac{V_{i-1}}{V_{i-2}} \right)^n + \epsilon_{i-2}$$

The following example illustrates the different stress levels and will use two stress levels of voltage (8 V and 12 V) on the vessel temperature sensor to define reliability in the operational condition (2 V). Table 2.7 shows failure in two stress levels. Under such operational stress conditions (2 V), the sensor has 99.9% reliability in 8 years (70,080 hours), as shown in Fig. 2.15.

Other important information about the range of stressor variation in the test is shown in Fig. 2.16. Thus it is possible to know which range of stress components is being tested. In the sensor case the two voltage ranges of stress are 8 V and 12 V.

Time to Failure	Voltage (V) Level 1	Time to Failure	Voltage (V) Level 2
740	8	980	12
820	8	1012	12
930	8	1018	12
		1182	12
		1202	12



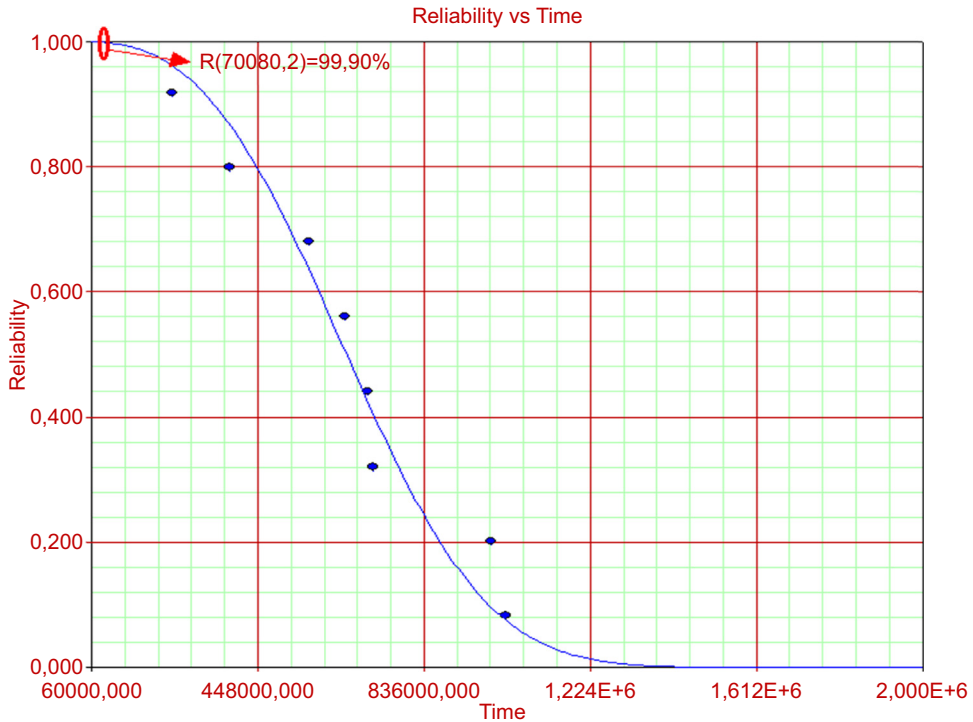


FIGURE 2.15

Reliability  $\times$  time  $\times$  voltage.

## 2.3 QUALITATIVE ACCELERATED TEST (HALT AND HASS)

After looking at different quantitative accelerated test models it is important to discuss qualitative accelerated tests because of the advantages of such an approach in developing product phases despite not predicting reliability under operational conditions. There are two types of qualitative accelerated test: HALT and HASS. HALT (highly accelerated life test), as called by Gregg K. Hobbs in 1988, is a development test, an enhanced form of step stress testing. It is used to identify design weaknesses and manufacturing process problems and to increase the margin of strength of the design but does not predict quantitative life or reliability of the product. HASS (highly accelerated stress screening test) is another type of qualitative accelerated test that presents the most intense environment seen by the product, but it is typically of a very limited duration. HASS is designed to go to “the fundamental limits of the technology” (Koeche, 2010). This is defined as the stress level at which a small increase in stress causes a large increase in the number of failures. In qualitative testing, both HALT and HASS go over operation limits and closer to destruction limits to force failure occurrences sooner. Fig. 2.17 shows different stress limits that accelerated stress tests achieve to force product failure in less time. Most quantitative accelerated tests work between the operating limits and destruction limits, but qualitative accelerated tests work closer to the destruct limitation to force product failure faster.

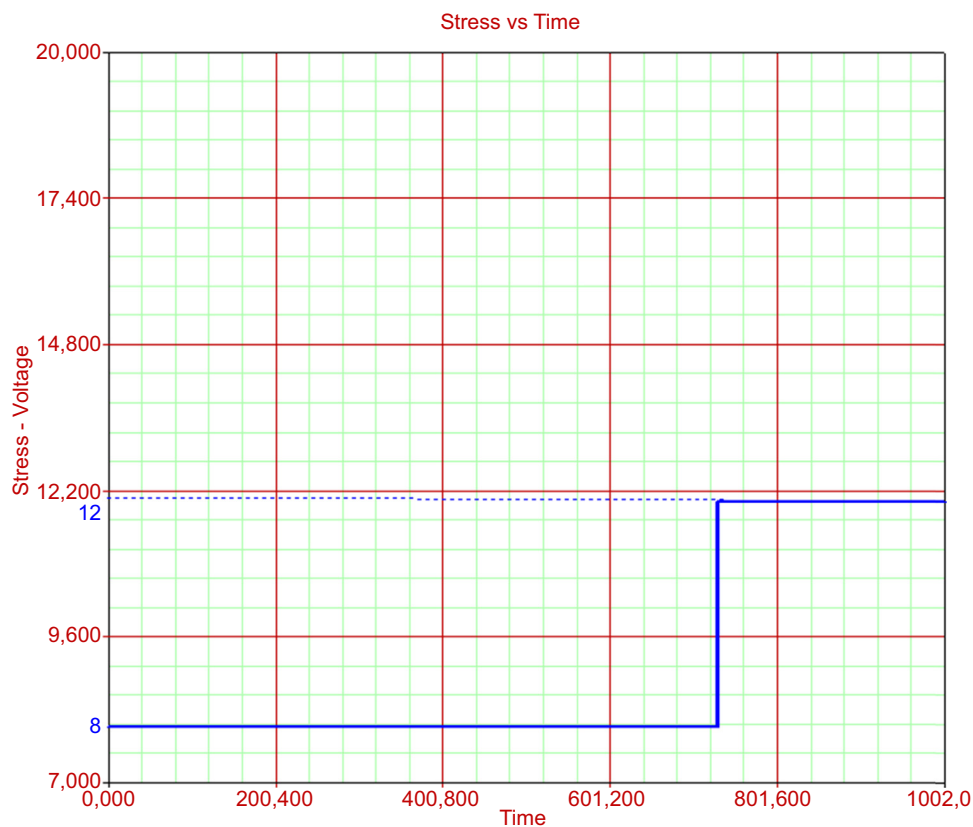


FIGURE 2.16

Varying stress levels.

To achieve stress levels some variables such as temperature and vibration or a combination of both variables are applied in the test at varying stress levels. It is important to know destruction limits and to be able to detect failure occurrences in the test and their causes. In many cases, stress levels start closer to the operating limits and then go up to a point closer to the destruction limits. In any case, the more knowledge known about the product and failure modes, the more time is saved during testing. Fig. 2.18 shows an example of temperature and vibration stressors in a HALT test. In 150 min it was possible to detect a failure in the electronic component that in a normal quantitative accelerated test would take much longer. As discussed, qualitative and quantitative tests have different objectives, and both help in product development.

When the temperature is being tested in a HALT test, temperatures mostly vary from 100°C to 200°C, using to slow down the temperature. Vibration generally varies from 1 to 100 g or from 10 to 10,000 Hz (Koeche, 2009). To implement such a test, equipment, such as a temperature chamber, is needed to test temperature, vibration, and other variables. The temperature chamber used in the test laboratory in Brazil is shown in Fig. 2.19.

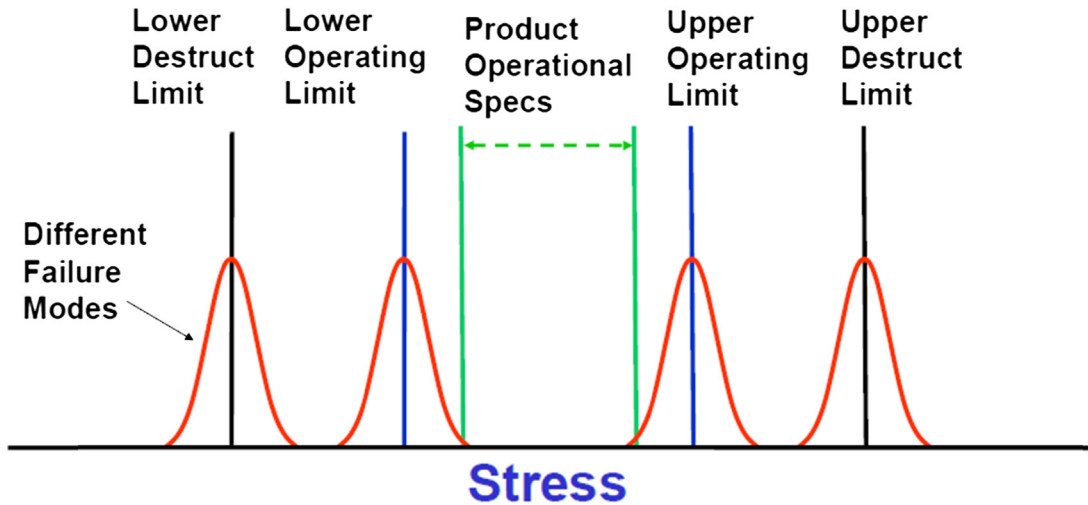


FIGURE 2.17

Stress limits.

Source: Regis, SIC2009.

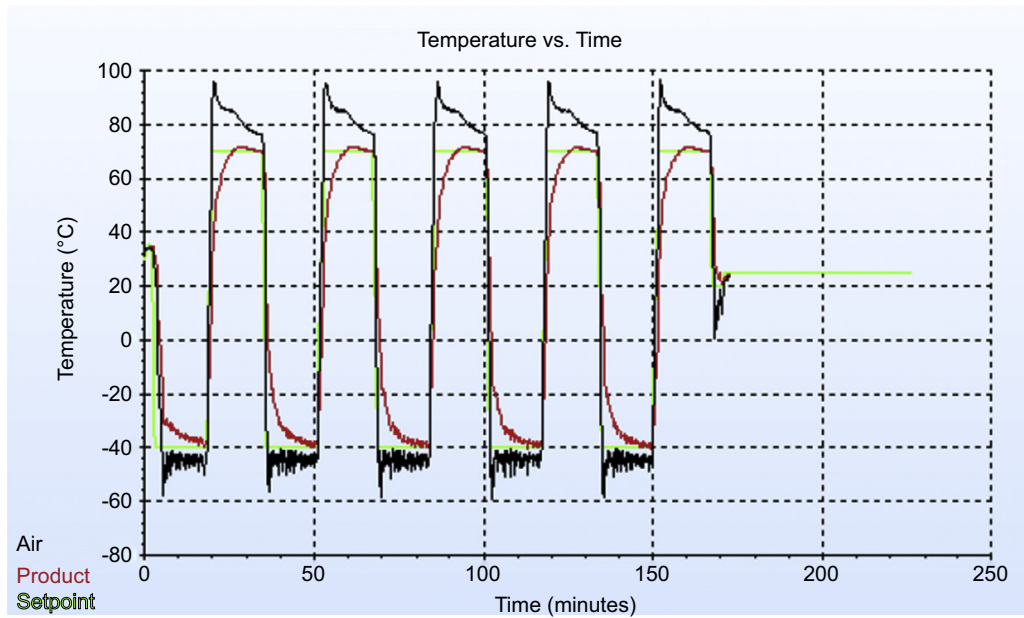


FIGURE 2.18

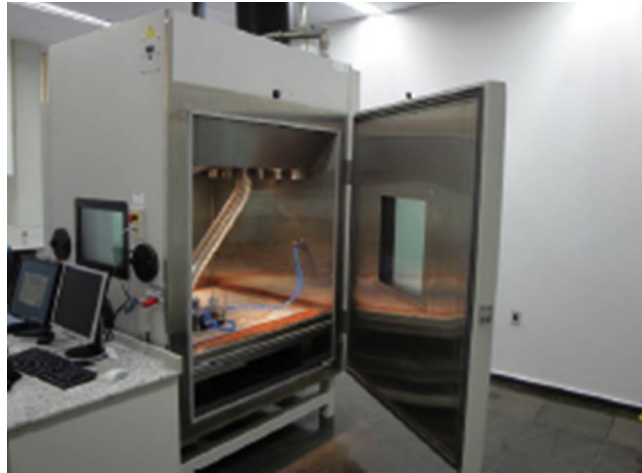
Temperature × vibration × time.

Source: Regis, SIC2009.

**FIGURE 2.19**

Temperature chamber.

*Source: Regis, SIC2009.*



While not a focus of this text, qualitative accelerated tests are important for defining failure modes and are most applicable in projects that involve new technologies, for example, drills in deep water that work under harder conditions and require robust equipment. In these cases, HALT would be very applicable for developing the equipment process and can be considered as a good alternative for understanding equipment weaknesses in operation in the oil and gas industry.

Despite not being the main focus of this book, it is very important to be aware of how important is the qualitative accelerated test (HALT and HASS) to define equipment weakness when such equipment face extreme operating conditions and also demonstrate latent failure modes.

Such methods enable to improve the product robustness during the design phase in a short period of time and support the product design.

An example applied to oil and gas industry is drill equipment which operates in deep water working under harder operation conditions, which requires a high robustness level.

In this case, HALT would be very applicable for developing the equipment based on HALT process. Additional equipments such as sensors, actuators, valves can be considered by the oil and gas industry as a good opportunity to apply HALT process to improve such equipment robustness.

---

## 2.4 RELIABILITY GROWTH ANALYSIS

Accelerated tests predict reliability under usual conditions, and when the results are not good, products need to be improved to meet reliability requirements and safety standards. In some cases, poor reliability results can lead to unsafe failures or loss of production. So to achieve product reliability targets, reliability growth analysis is conducted.

Reliability growth analysis consists of improving products whenever a failure shows up during testing, called the test—fix—test approach, or after the test, the test—find—test approach. Depending on the product characteristics, both corrective actions would be conducted using the test—fix—find test approach, which means improving the product when failure is detected or postponed improvement,

depending on the case. Testing continues until the reliability target is achieved. The term reliability growth is used because improvement in product development is expected after the corrective actions. However, in practice, no growth or negative growth may occur.

In some cases, a well-defined reliability growth program is required to manage product improvement during the development phase based on the corrective actions needed for the failures detected. The main objective in a reliability growth program is achieving the reliability target, monitoring improvements, learning to avoid future mistakes, and reducing the product development phase time. Such programs include a planning test, failure mode identification, corrective actions, and valid reliability assessment. In a reliability growth program, failure and root cause analysis support product improvements, and effective corrective action and understanding root causes help to achieve reliability targets.

Reliability growth methodology may also be used to assess a repairable system and corrective maintenance, and it is possible to predict the reliability growth or nongrowth and number of failures over time. In some cases, equipment requires modifications to improve performance, and when these improvements are made, the equipment must be assessed with the reliability growth analysis approach. Depending on the type of data, there are different reliability growth models like:

- Duane
- Crow—AMSAA (NHPP)
- Lloyd—Lipow
- Gompertz
- Logistic
- Crow Extended
- Power Law

### 2.4.1 DUANE MODEL

The Duane model is empirical and shows linear relations between accumulated mean time between failure (MTBF) and time (T) when the natural logarithm (ln) function is applied to both variables MTBF and T. This approach is applied in reliability growth analysis to show the effects of corrective actions on reliability. After accelerated testing it is possible to estimate the MTBF, which is considered the initial MTBF in the Duane model. The equation that describes the reliability growth in the Duane model is:

$$MTBF_a = MTBF_i \times \left( \frac{t_a}{t_i} \right)^\alpha$$

where  $MTBF_a$  = accumulated mean time to failure;  $MTBF_i$  = initial mean time to failure;  $t_a$  = accumulated time;  $t_i$  = initial time; and  $\alpha$  = reliability growth.

If:

$$MTBF_a = \frac{1}{\lambda_a}$$

and:

$$MTBF_i = \frac{1}{\lambda_i}$$

thus:

$$\lambda_a = \lambda_i \times \left(\frac{t_a}{t_i}\right)^{-\alpha}$$

In practice, accelerated testing is performed and the duration time in such testing will be the initial time in the reliability growth analysis. The MTBF predicted in the test will be the initial mean time to failure in the Duane model. When reliability growth analysis ends, the total time will be the accumulated time and the accumulated mean time to failure will be defined.

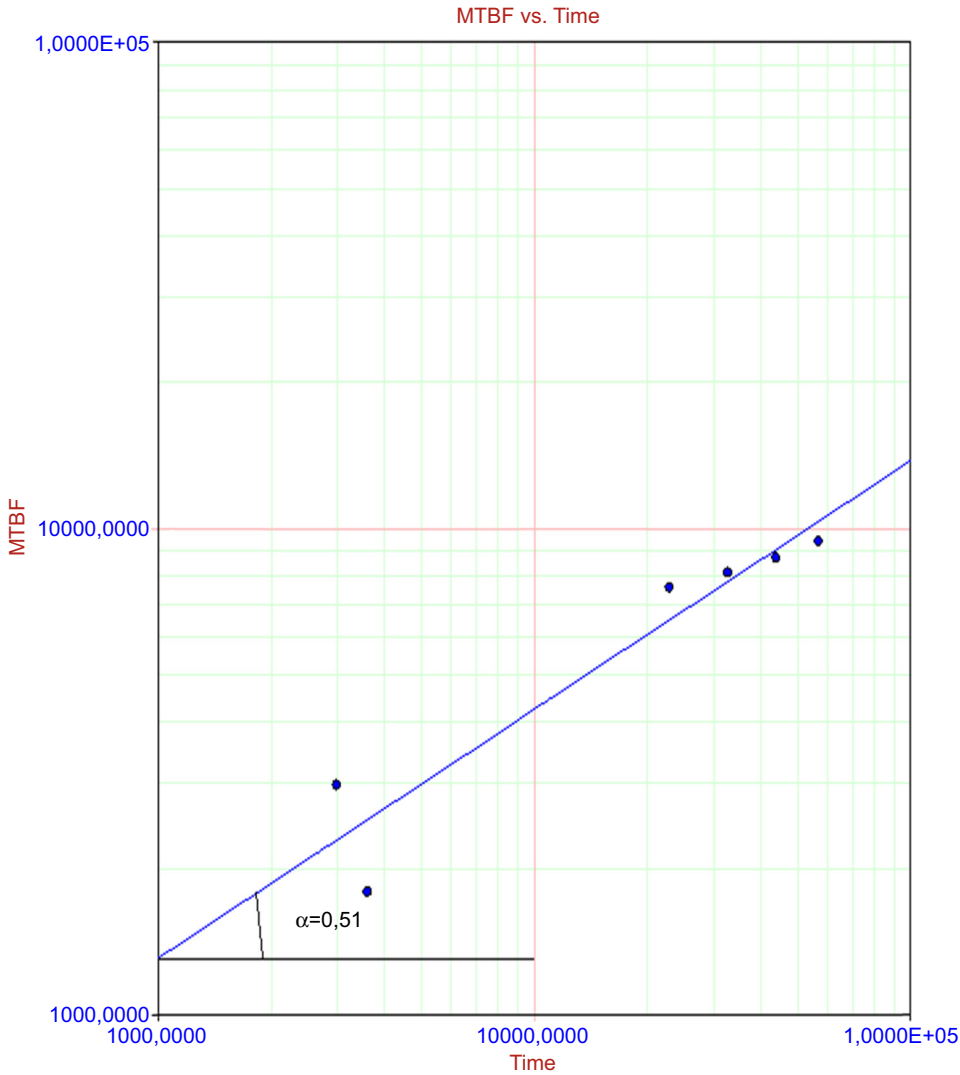
To illustrate the Duane model the sensor in the accelerated test in Section 2.2.1 must be improved. The sensor MTBF is 2300 hours, and to achieve a higher MTBF the sensor material was changed to make the sensor more robust to higher temperatures. In this way the testing sensors with new material failures over time were 3592, 22,776, 32,566, 43,666, and 56,700 hours. Such improved sensors were tested under harder operational conditions over 6 years. Thus applying the Duane equation we have:

$$\begin{aligned} \text{MTBF}_a &= \text{MTBF}_i \times \left(\frac{t_a}{t_i}\right)^\alpha \\ \ln(\text{MTBF}_a) &= \ln\left[\text{MTBF}_i \times \left(\frac{t_a}{t_i}\right)^\alpha\right] \\ \ln(\text{MTBF}_a) &= \ln(\text{MTBF}_i) + \alpha \ln\left(\frac{t_a}{t_i}\right) \\ \alpha \ln\left(\frac{t_a}{t_i}\right) &= \ln(\text{MTBF}_a) - \ln(\text{MTBF}_i) \\ \alpha \ln\left(\frac{t_a}{t_i}\right) &= \ln\left(\frac{\text{MTBF}_a}{\text{MTBF}_i}\right) \\ \alpha &= \frac{\ln\left(\frac{\text{MTBF}_a}{\text{MTBF}_i}\right)}{\ln\left(\frac{t_a}{t_i}\right)} = \frac{\ln\left(\frac{10,343}{2300}\right)}{\ln\left(\frac{5700}{2978}\right)} = 0.51 \end{aligned}$$

Fig. 2.20 shows the accumulated MTBF  $T$  where reliability growth is the angular coefficient ( $\alpha = 0.51$ ). Whenever the MTBF increases over time, it means improvement on sensor reliability. If the MTBF decreases over time, reliability is decreasing. In these cases, as  $\alpha < 1$ , there is reliability growth and the MTBF increases after improvement. The final MTBF (10,343 hours) is higher than the initial MTBF (2300 hours).

#### 2.4.2 CROW—AMSAA MODEL (NHPP)

The Crow—AMSAA model, introduced by Dr Larry H. Crow in 1974, is a statistical model that uses the Weibull distribution parameter to describe the relationship between accumulated time between



**FIGURE 2.20**  
Accumulated MTBF  $\times$  time.

failure and test time. This approach is applied in reliability growth analysis to show the effect of corrective actions on reliability when a product is being developed or even in repairable systems during the operation phase. Thus whenever improvements are implemented during testing (test-fix-test), the Crow-AMSAA model is used to predict reliability growth and the expected cumulative number of failures.

The expected cumulative number of failures is represented mathematically by:

$$E(N_i) = \int_0^T \rho(t) dt$$

The Crow–AMSAA model assumes that intensity failure is approximately the Weibull failure rate, thus intensity of failure on time is:

$$\rho(t) = \frac{\beta}{\eta^\beta} T^{\beta-1}$$

Using the initial failure rate as:

$$\lambda_i = \frac{1}{\eta^\beta}$$

if the cumulative failure rate is approximately the failure intensity we have:

$$\lambda_c = \beta \lambda_i T^{\beta-1}$$

The preceding equation describes failure intensity during testing and depends on whether the  $\beta$  value increases/decreases or remains constant over time. In fact,  $\beta$  is a shape parameter of the intensity failure function in the Crow–AMSAA model. Thus in this model when  $\beta > 1$  the reliability is decreasing over time because failure intensity is increasing, or, in other words, the corrective product actions are not improving the product. When  $\beta < 1$ , the intensity of failure is decreasing over time, or, in other words, the corrective product actions are improving product reliability. When  $\beta = 1$ , the product behaves as if no corrective action has taken place and intensity failure is constant over time. It is important to keep in mind that the  $\beta$  in the Crow–AMSAA model describes intensity failure behavior and has no relation to the Weibull distribution shape parameter. The growth rate in the Crow–AMSAA model is  $1 - \beta$ .

To define the failure intensity parameters in the Crow–AMSAA model the maximum likelihood method may be used, as introduced in Chapter 1. Thus we have:

$$L(\theta_1, \theta_2, \theta_3 \dots \theta_n / x_1, x_2, x_3 \dots x_n) = \prod_{i=1}^n f(\theta_1, \theta_2, \theta_3 \dots \theta_k; x_i) \quad i = 1, 2, 3 \dots n$$

To find the variable value it is necessary to find the maximum value related to one parameter and that is achieved by performing partial derivation of the equation as follows:

$$\frac{\partial(\Lambda)}{\partial(\theta_j)} = 0 \quad j = 1, 2, 3, 4 \dots n$$

Applying the maximum likelihood method we have:

$$f(t) = \frac{\beta}{\eta} \left(\frac{T_i}{\eta}\right)^{\beta-1} e^{-\lambda_i T_i^\beta} = \beta \frac{1}{\eta^\beta} T_i^{\beta-1} e^{-\lambda_i T_i^\beta} = \beta \lambda_i T_i^{\beta-1} e^{-\lambda_i T_i^\beta}$$



$$L = \prod_{i=0}^N f(t) = \prod_{i=0}^N \beta \lambda_i T_i^{\beta-1} e^{-\lambda_i T_i^\beta} = \beta^N \lambda_i^N e^{-\lambda_i T_i^\beta} (\beta - 1) \prod_{i=0}^N T_i$$

$$\Lambda = LnL$$

$$LnL = Ln \left( \beta^N \lambda_i^N e^{-\lambda_i T_i^\beta} (\beta - 1) \prod_{i=0}^N T_i \right)$$

$$\Lambda = NLn\beta + NLn\lambda_i - \lambda_i T_i^\beta + (\beta - 1) \sum_{i=0}^N LnT_i$$

$$\frac{\partial(\Lambda)}{\partial(\lambda_i)} = 0$$

$$\frac{\partial(\Lambda)}{\partial(\lambda_i)} = \frac{N}{\lambda_i} - T_i^\beta = 0$$

$$\lambda_i = \frac{N}{T_i^\beta}$$

$$\frac{\partial(\Lambda)}{\partial(\beta)} = 0$$

$$\frac{\partial(\Lambda)}{\partial(\beta)} = \frac{1}{\beta} - \lambda T^\beta LnT + \sum_{i=0}^N LnT_i = 0$$

$$\beta = \frac{N}{NLnT - \sum_{i=0}^N LnT_i}$$

To clarify the Crow-AMSAA model, the same example used for the Duane model will be used here. Thus the failures on time for the testing sensor with new material were 3592 hours, 22,776 hours, 32,566 hours, 43,666 hours, and 56,700 hours. The parameters are:

$$\beta = \frac{N}{NLnT - \sum_{i=0}^N LnT_i} = \frac{6}{(6 \times Ln(56,700) - (7.9 + 8.2 + 10 + 10.3 + 10.6 + 10.9))}$$

$$\beta = 0.807$$

and

$$\lambda_i = \frac{N}{T_i^\beta} = \frac{6}{56,700^{0.8075}} = 0.00087 \approx 0.0009$$

Thus applying the parameter in the failure intensity equation we have:

$$\lambda_c = 0.807 \times 0.0009 T^{0.807-1} = 0.0007263 T^{-0.193}$$

Thus at the end of testing (56,700 hours):

$$\lambda_c = 0.0001$$

Fig. 2.21 shows failure intensity time, and it is clear that when there is reliability growth, failure intensity is decreasing over time.

One interesting and very important Crow–AMSAA model application is to repairable systems when it is necessary to assess if repairs and turnout are performing as good as expected or to predict the future number of failures. In the latter it is possible to plan future inspections and maintenance, which are topics discussed in Chapter 3.

Thus Fig. 2.22 shows the expected number of failures of different pumps from different tower distillation plants having pumps with the same function. Such pumps were assessed to support decisions to project pumps with lower rotation to have higher reliability because of lesser seal leakage failures over time. The pump seals were repaired over time and some of them with reliability growth had improved during turnout. The seal pump Crow–AMSAA parameters are presented in Table 2.8. It is clear that pumps P-2A (S-B) and P-1A (S-F) had reliability growth because  $\beta < 1$ . Despite reliability growth, pumps P-1A (S-F) have more failures in 20 years than pumps that had no reliability growth, such as P-7A (S-F).

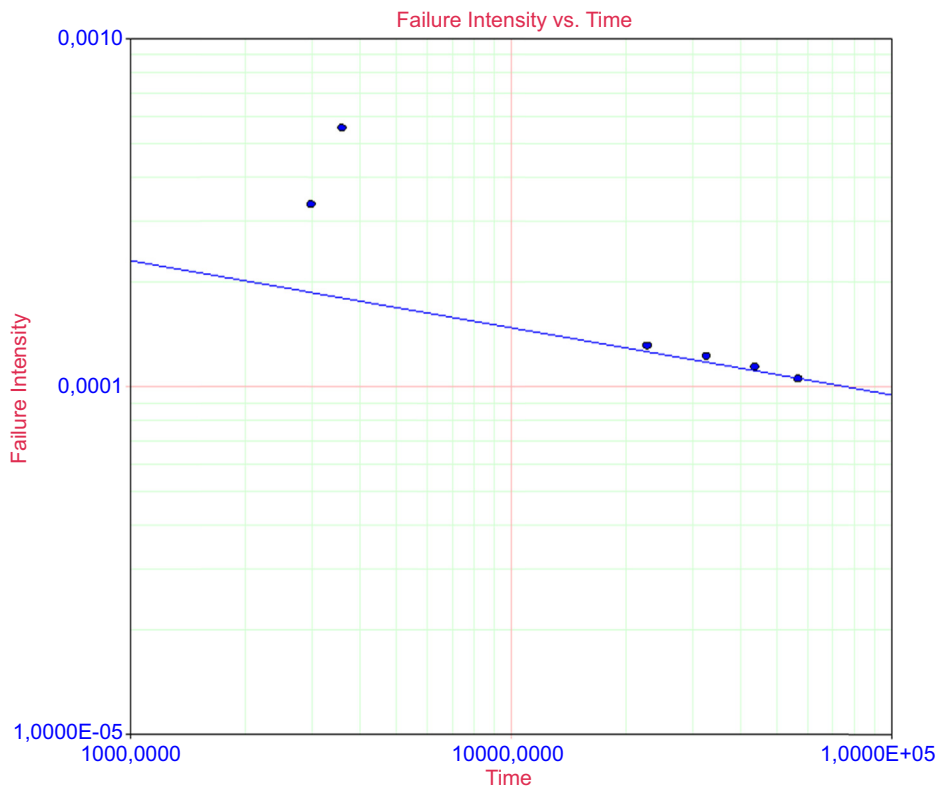


FIGURE 2.21

Failure intensity  $\times$  time.

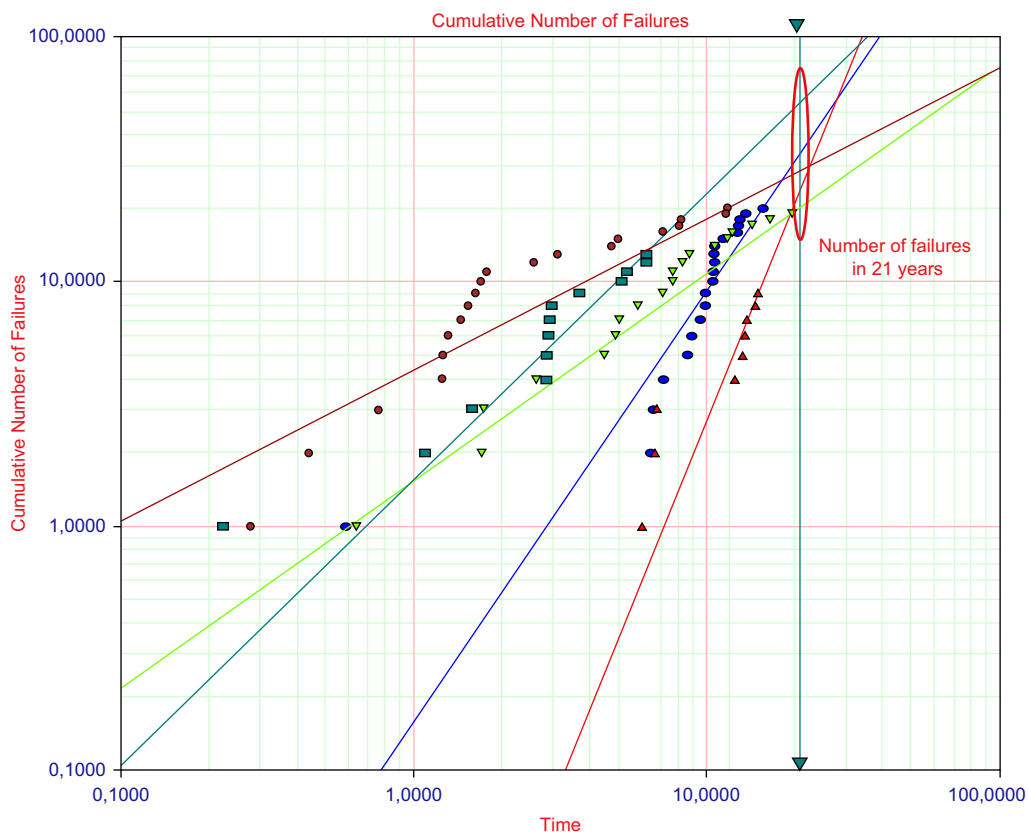


FIGURE 2.22

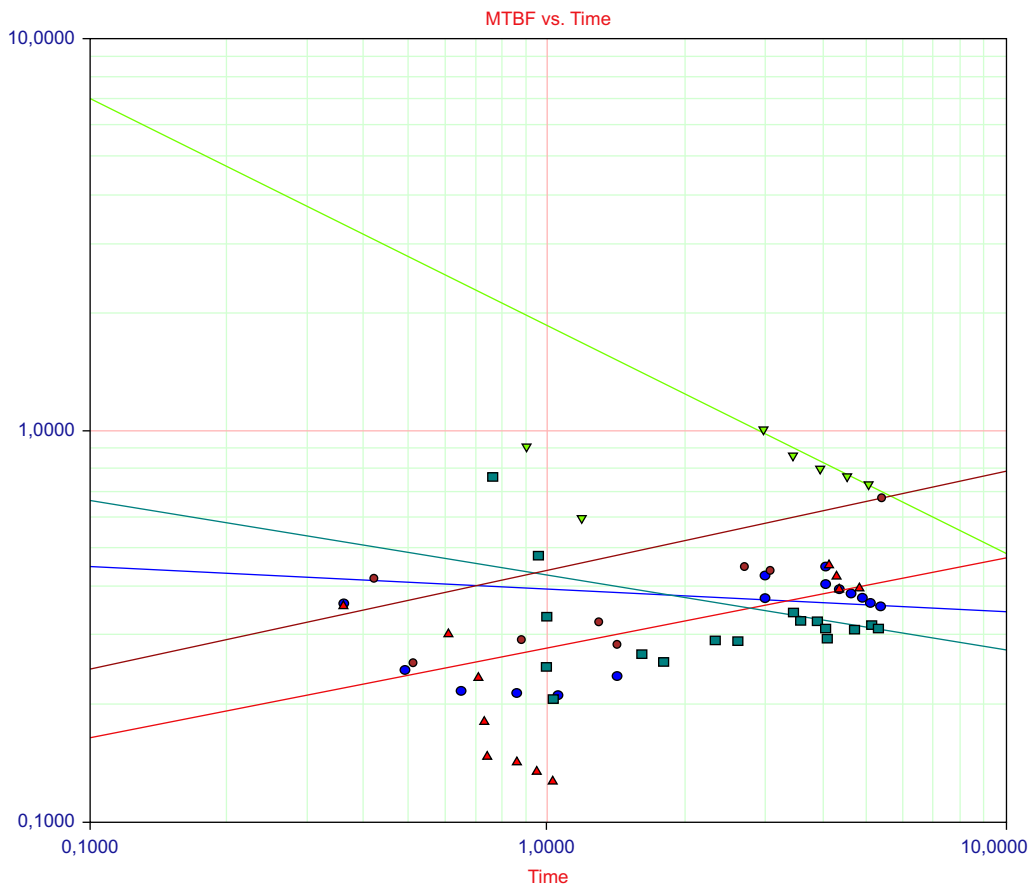
Seal pump failure intensity  $\times$  time. *Red line* (dark gray in print version), P-7A(S-F); *blue line* (darkest gray print version), P-1A(S-F); *green line* (gray in print version), P-2A(S-D); *dark green line* (light gray in print version), P-1A(S-B); *dark red line* (darker gray in print version), P-1A(S-B). P, pump; S, supplier.

Table 2.8 Pumps Crow–AMSAA Parameters					
	P-01 A (S-F)	P-07 A (S-F)	P-03 A (S-B)	P-02 A (S-B)	P-01 A (S-F)
$\beta$	1.7585	2.94	1.1705	0.8474	0.6185
Growth rate	-0.7585	-1.94	-0.1705	0.1526	0.3815
Cumulative number of failures (20 years)	31	21	51	19	28

Depending on time, some seal pumps may have a higher cumulative number of failures as shown in Fig. 2.20. The line slope shows the number of failures over time.

The other example is made for the compressor from the catalyst cracking plant. In this case, despite redundancy configuration, compressor failures impact plant availability. Actually, some years ago, such a compressor had more than 20 years and some turnout and modifications were made to increase compressor reliability. Therefore, after turnout, reliability growth analysis was performed to assess if the MTBF was increasing or decreasing over time. Fig. 2.23 shows the MTBF over time for each compressor.

As shown in Fig. 2.23, compressors with  $\beta > 1$ , such as C-1A, C-2A, and C-1C, have reliability decreasing, and the MTBF line has a negative slope. In contrast, compressors with  $\beta < 1$ , such as C-1B and C-2B, have reliability increasing, and the MTBF line has a positive slope. Actually, in addition to



**FIGURE 2.23**

Compressor MTBF  $\times$  time.

reliability growth analysis, compressor RAM analysis (reliability, availability, and maintainability) was conducted to measure compressor availability over time and its impact on the plant. The Crow–AMSAA model is a good tool for assessing reliability growth in product improvements in development phases and to assess repairable systems such as pumps and compressors.

### 2.4.3 LLOYD–LIPOW

The Lloyd–Lipow model was created by Lloyd and Lipow in 1962 to be applied in reliability growth programs that have different stages. In each stage, improvement actions are implemented for similar products to improve reliability, and the results are recorded as success or failure. The reliability in the  $k$  test stage is described as:

$$R_k = R_\infty - \frac{\alpha}{k}$$

where  $R_k$  = reliability in  $k$  test stage;  $R_\infty$  = reliability of actual stage after improvement implemented in previous test stages;  $\alpha$  = reliability growth index; and  $k$  = test stage.

The reliability in the  $k$  stage may be also described as:

$$R_k = \frac{S_k}{n_k}$$

where  $n_k$  = number of tested components in stage  $k$  and  $S_k$  = number of successes.

To obtain reliability in stage  $k$  it is necessary first to define the reliability growth index. Thus the following equation defines the reliability growth index ( $\alpha$ ):

$$\alpha = \frac{\sum_{k=1}^N \frac{1}{k} \times \sum_{k=1}^N \frac{S_k}{n_k} - N \times \sum_{k=1}^N \frac{S_k}{k \times n_k}}{N \times \sum_{k=1}^N \frac{1}{k^2} - \left( \sum_{k=1}^N \frac{1}{k} \right)^2}$$

And the reliability actual stage is given as:

$$R_\infty = \frac{\sum_{k=1}^N \frac{1}{k^2} \times \sum_{k=1}^N \frac{S_k}{n_k} - \sum_{k=1}^N \frac{1}{k} \times \sum_{k=1}^N \frac{S_k}{k \times n_k}}{N \times \sum_{k=1}^N \frac{1}{k^2} - \left( \sum_{k=1}^N \frac{1}{k} \right)^2}$$

To clarify the Lloyd–Lipow model a bearing development test was presented as follows. The bearing test was performed using the test–fix–test concept, and a group of pump bearings was tested at different stages ( $k = 10$ ), implementing improvements in materials. Table 2.9 shows the success in each group of pump bearings at different stages. Each stage is 7 days.

Regarding the test results from Table 2.9 the reliability growth is:

$$\alpha = \frac{\sum_{k=1}^N \frac{1}{k} \times \sum_{k=1}^N \frac{S_k}{n_k} - N \times \sum_{k=1}^N \frac{S_k}{k \times n_k}}{N \times \sum_{k=1}^N \frac{1}{k^2} - \left( \sum_{k=1}^N \frac{1}{k} \right)^2}$$

Stage	Number of Bearings Tested	Number of Failures
1	12	5
2	12	6
3	11	3
4	13	6
5	12	4
6	13	4
7	13	5
8	13	6
9	14	6
10	14	4

$$\sum_{k=1}^N \frac{1}{K} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{10} = 2.92$$

$$\left( \sum_{k=1}^N \frac{1}{K} \right)^2 = (2.92)^2 = 8.52$$

$$\sum_{k=1}^N \frac{1}{K^2} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{10^2} = 1.54$$

$$\sum_{k=1}^N \frac{S_k}{n_k} = \frac{7}{12} + \frac{6}{12} + \frac{8}{11} + \dots + \frac{10}{14} = 7.03$$

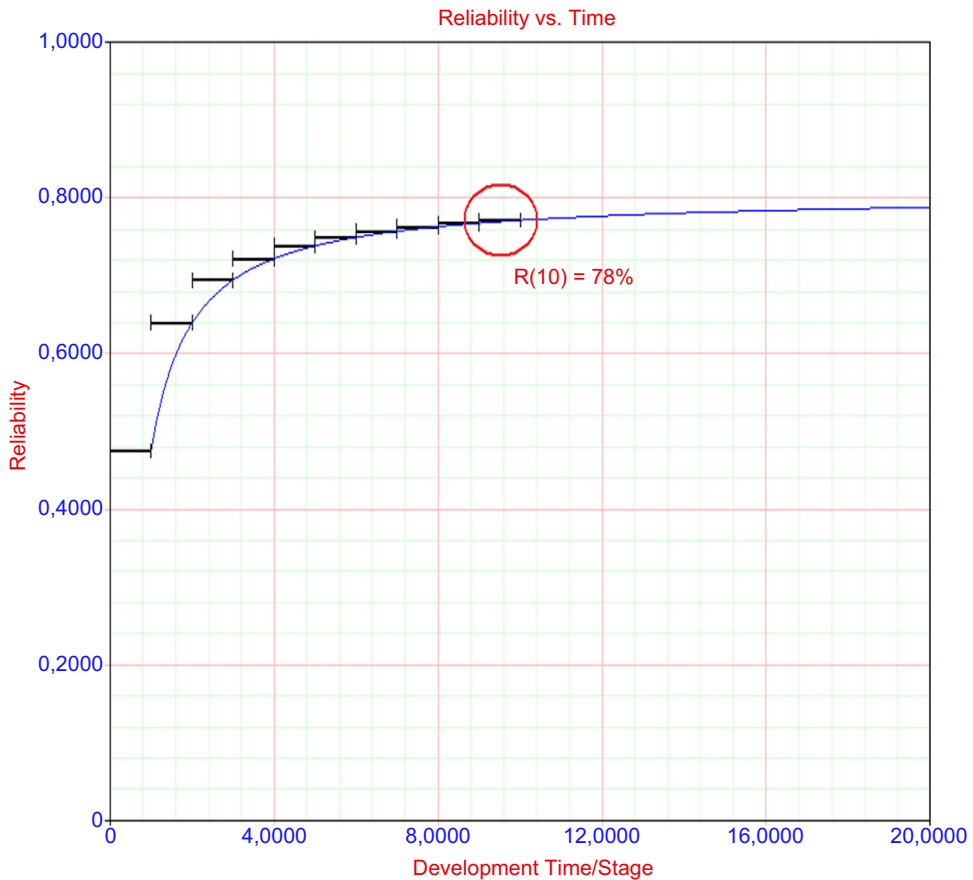
$$\sum_{k=1}^N \frac{S_k}{k \times n_k} = \frac{7}{1 \times 12} + \frac{6}{2 \times 12} + \frac{8}{3 \times 11} + \dots + \frac{10}{10 \times 14} = 1.85$$

$$\alpha = \frac{(2.92 \times 7.03) - (10 \times 1.85)}{(10 \times 1.54) - (8.52)} = \frac{(20.59) - (18.5)}{(15.4 - 8.52)} = \frac{2.02}{6.88} = 0.3197$$

The reliability of the 10th stage is:

$$R_{\infty} = \frac{(1.54 \times 7.03) - (2.92 \times 1.85)}{(10 \times 1.54) - (8.52)} = \frac{(10.82) - (5.4)}{(15.4 - 8.52)} = \frac{5.42}{6.88} = 78\%$$

Fig. 2.24 shows reliability growth in 10 test stages, and in the 10th stage the bearing achieved 78% reliability. The reliability achieved is under test conditions, thus predicting reliability under operational conditions is 95%, the reliability requirement for 3 years. In the following section, we will discuss the Gompertz model.

**FIGURE 2.24**

Reliability  $\times$  time stages (Lloyd–Lipow model).

### 2.4.4 GOMPERTZ MODEL

The Gompertz model is similar to the Lloyd–Lipow model and uses reliability results over different test stages. Again at each stage, improvements are implemented for similar products to improve reliability, and the results are recorded for reliability. The Gompertz model also uses reliability targets expressed mathematically as:

$$R(t) = ab^{c^t}$$

where  $a$  = reliability target ( $0 < a \leq 1$ );  $b$  = reference parameter ( $0 < b < 1$ );  $ab$  = initial reliability;  $c$  = reliability growth ( $0 < c < 1$ ); and  $T$  = stage time ( $T > 0$ ).

To define Gompertz model parameters, take the following steps:

1. Define the stage intervals during testing;
2. Divide the total stages into three groups with a similar number of stages;
3. Define  $S_1$ ,  $S_2$ , and  $S_3$  based on the sums of LnRn in each stage.

After defining  $S_1$ ,  $S_2$ , and  $S_3$ , the Gompertz model parameters are defined by: Reliability growth ( $c$ ):

$$c = \left( \frac{S_3 - S_2}{S_2 - S_1} \right)^{\frac{1}{n}}$$

Reliability target ( $a$ ):

$$a = e^{\left[ \frac{1}{n} \left( S_1 + \frac{S_2 - S_1}{1 - c^n} \right) \right]}$$

Reference parameter ( $b$ ):

$$b = e^{\left[ \frac{(S_2 - S_1) \times (c - 1)}{(1 - c^n)^2} \right]}$$

To illustrate the Gompertz model, the example (bearing) used for the Lloyd–Lipow model will be used here. The bearing tests were performed based on the test–fix–test concept, and a group of pump bearings was tested at different stages ( $k = 10$ ), implementing improvements in materials. To conduct the methodology proposed by the Gompertz model there will be nine stages ( $K = 9$ ) and three groups, as shown in Table 2.10.

In doing so, applying the following equations we have Gompertz model parameters:

$$c = \left( \frac{S_3 - S_2}{S_2 - S_1} \right)^{\frac{1}{n}} = \left( \frac{13 - 12.9}{12.9 - 12.26} \right)^{\frac{1}{3}} = 0.5473$$

$$a = e^{\left[ \frac{1}{n} \left( S_1 + \frac{S_2 - S_1}{1 - c^n} \right) \right]} = e^{\left[ \frac{1}{3} \left( 12.26 + \frac{12.9 - 12.26}{1 - 0.5473^3} \right) \right]} = 0.7678$$

Group	Stage	Reliability	LnR(t)	Sn
1	1	47.47	3.86	12.26
	2	63.95	4.16	
	3	69.45	4.24	
2	4	72.19	4.28	12.90
	5	73.84	4.30	
	6	74.94	4.32	
3	7	75.72	4.33	13.00
	8	76.31	4.33	
	9	76.77	4.34	

*Ln, natural logarithm.*



$$b = e^{\left[ \frac{(s_2 - s_1) \times (c-1)}{(1-e^c)^2} \right]} = e^{\left[ \frac{(12.9-12.26) \times (0.54-1)}{(1-0.54^3)^2} \right]} = 0.66$$

Thus the reliability growth in stage 10 will be:

$$R(10) = ab^{c^T} = 0.7678 \times 0.66^{0.54^{10}} = 0.7671$$

Fig. 2.25 shows the reliability during the test stages, and it is possible to see reliability increasing during testing after improvement actions were implemented. In the 10th stage the predictable reliability is 76.71%.

In the S-curve shape reliability growth, the modified Gompertz model is more appropriate and uses position parameter  $d$ . In this case, the reliability in stage  $T$  will be:

$$R(t) = d + ab^{c^T}$$

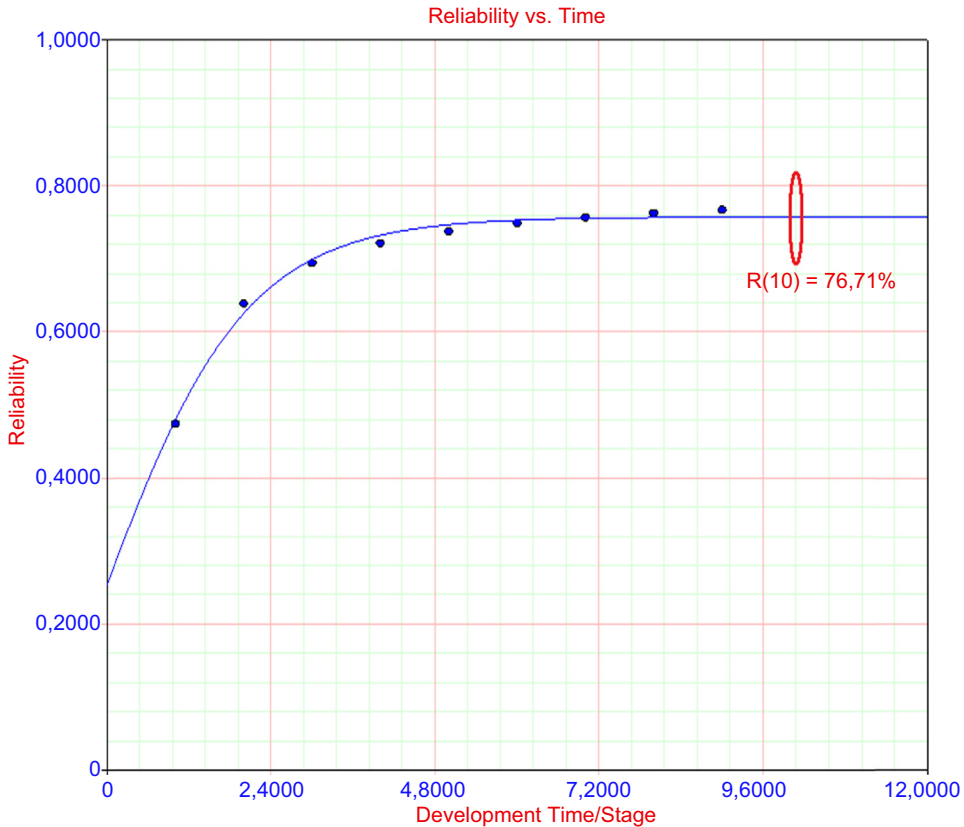


FIGURE 2.25

Reliability time stages (Gompertz model).

where  $d$  = position parameter;  $a + d$  = reliability target ( $0 < a \leq 1$ );  $b$  = reference parameter ( $0 < b < 1$ );  $d + ab$  = initial reliability;  $c$  = reliability growth ( $0 < c < 1$ ); and  $T$  = stage time ( $T > 0$ ).

Because the data assessed in the Gompertz model has no S-curve characteristics, such data is not assessed in the modified Gompertz model. In the next section, the logistic model will be discussed. It represents better reliability growth with an S-curve shape.

### 2.4.5 LOGISTIC MODEL

The logistic model also works with reliability results during different test stages, and in most of the stages some improvements are implemented to similar products to improve reliability. The results are recorded as for reliability. The logistic model describes the reliability growth S-shape curve very well and is described by:

$$R(t) = \frac{1}{1 + be^{-kT}}$$

where  $b$  = position parameter ( $b > 0$ ), because the higher the “ $b$ ” value, the lesser is reliability;  $k$  = shape parameter ( $k > 0$ ), because the lower the “ $k$ ” value, the lesser is reliability; and  $T$  = stage time ( $T > 0$ ).

To define the logistic model equation parameter the following equations are applied based on the least squares method, which will not be discussed in this section:

$$\begin{aligned}\bar{b} &= e^{\bar{b}_0} \\ \bar{k} &= -\bar{b}_1 \\ \bar{b}_1 &= \frac{\sum_{i=0}^{N-1} T_i Y_i - N \cdot \bar{T} \cdot \bar{Y}}{\sum_{i=0}^{N-1} T_i^2 - N \cdot \bar{T}^2} \\ \bar{b}_0 &= \bar{Y} - \bar{b}_1 \cdot \bar{T} \\ Y_i &= Ln\left(\frac{1}{R_i} - 1\right) \\ \bar{Y} &= \frac{1}{N} \cdot \sum_{i=0}^{N-1} Y_i \\ \bar{T} &= \frac{1}{N} \cdot \sum_{i=0}^{N-1} T_i\end{aligned}$$

To illustrate the logistic model a shaft reliability growth test is implemented to achieve higher reliability, and the improvements are conducted over 11 stages. [Table 2.11](#) shows reliability during the stage phases.

$$Y_i = Ln\left(\frac{1}{R_i} - 1\right)$$

$$\bar{Y} = \frac{1}{N} \cdot \sum_{i=0}^{N-1} Y_i = \frac{1}{11} [(-0.49) + (-0.55) + \dots + (-1.94)] = -0.99$$

$$\bar{T} = \frac{1}{N} \cdot \sum_{i=0}^{N-1} T_i = \frac{1}{11} [(1) + (2) + \dots + (10)] = 5$$

$$\sum_{i=0}^{N-1} T_i^2 = 385$$

$$\sum_{i=0}^{N-1} T_i Y_i = -74.76$$

$$\bar{b}_1 = \frac{\sum_{i=0}^{N-1} T_i Y_i - N \cdot \bar{T} \cdot \bar{Y}}{\sum_{i=0}^{N-1} T_i^2 - N \cdot \bar{T}^2} = \frac{(-74.76) - (11 \times 5 \times -0.99)}{385 - (11 \times 5^2)} = -18.46$$

$$\bar{b}_0 = \bar{Y} - \bar{b}_1 \cdot \bar{T} = -0.99 - (-18.46) \times 5 = -0.06682$$

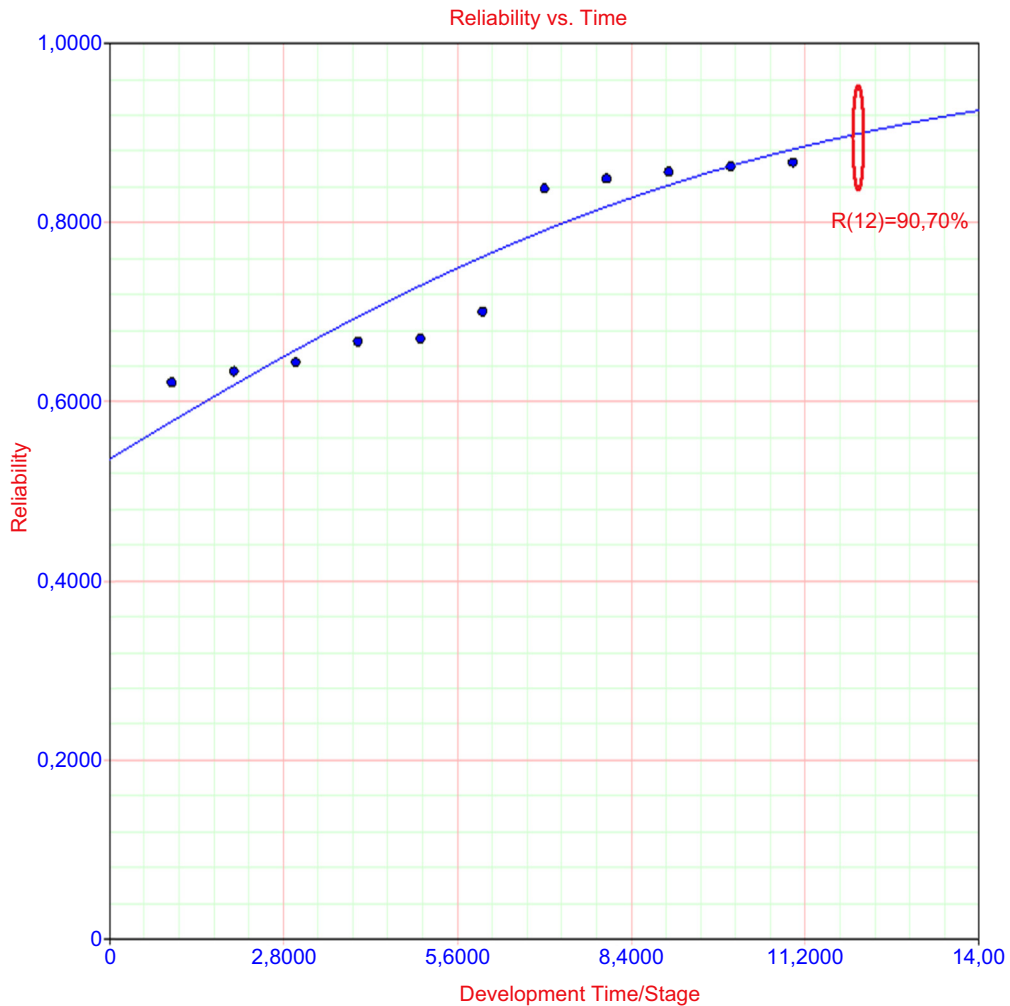
$$\bar{k} = -\bar{b}_1 = 18.46$$

$$\bar{b} = e^{\bar{b}_0} = e^{-0.06682} = 0.9395$$

$$R(12) = \frac{1}{1 + b e^{-kT}} = \frac{1}{1 + 0.9395 e^{-18.46 \times 12}} = 0.9070$$

Fig. 2.26 shows reliability during the test stage, and it is possible to see that reliability increases during the test after improvements. In the 12th stage the predicted reliability is 90.7%.

Test Stage	Reliability
1	0.6219
2	0.6345
3	0.6444
4	0.6677
5	0.6711
6	0.7011
7	0.8384
8	0.8494
9	0.8572
10	0.8631
11	0.8677



**FIGURE 2.26**  
Reliability × time stages (logistic model).

### 2.4.6 CROW EXTENDED MODEL

The Crow extended model is a more complete model compared to the Crow–AMSAA model because it works with improvement actions during the test stage and delayed improvement actions to be implemented having a predictable reliability for two situations. Thus two reliability estimates can be defined. The first one arises from test–fix–test where corrective action is implemented over testing, and in this case we have demonstrated reliability. The second one arises from test–find–test, and in this case corrective actions are not implemented during the test and improvements are made at the end

of the test. Therefore we have projected reliability. In reliability growth model it's also possible to have a combination of both situations, that means, test—fix—find test. In this case, the Crow Extended Model will handle this complexity of data combination. The main difference between this model and the previous one is the possibility of predicting the reliability values based on the index which regards the effect of delayed improvement in product. In order to simplify the mathematical representation of the Crow extended model the following codes are defined for each type of action such as:

- NF: No fixed action is performed;
- FI: Fixed action implemented during test (test—fix—test);
- FD: Fixed action delayed to be implemented when test is completed (test—find—test).

To represent reliability growth the intensity failure function may be more appropriate and such a function includes all types of actions performed during testing. Thus we have:

$$\lambda(t) = \lambda_{NF} + \lambda_{FI} + \lambda_{FD}$$

$$\lambda_{FD} = \sum_{i=1}^n \lambda_{FD_i}$$

where  $i = 1, 2, 3, \dots, n$  and  $n$  is the number of failures related to delayed improvement action.

The other important parameter is  $d$ , which represents the effectiveness factor of the improvement in reducing failure intensity, or, in other words, in increasing reliability. Such a factor is put into the failure intensity equation as  $(1 - d)$ . Thus, for improvement effectiveness during testing, the failure intensity function is:

$$\lambda(t) = \lambda_{NF} + \sum_{i=1}^n (1 - d_i) \lambda_{FI_i} + \left( \lambda_{FD_i} - \sum_{i=1}^n \lambda_{FI_i} \right)$$

where:

- $\sum_{i=1}^n (1 - d_i) \lambda_{FI_i}$  = failure intensity after improvement action;
- $\lambda_{FD_i} - \sum_{i=1}^n \lambda_{FI_i}$  = remaining failure intensity for all FD failures.

The other important parameter is the potential reliability growth, expressed mathematically as:

$$R_G = \lambda_{NF} + \sum_{i=1}^n (1 - d_i) \lambda_{FI_i} = \frac{N_{NF}}{T} + \sum_{i=1}^n (1 - d_i) \frac{N_{FI_i}}{T}$$

where  $N_{NF}$  = number of not fixed action;  $N_{FI_i}$  = number of fixed action implemented; and  $MTBF_{RG} = \frac{1}{R_G}$ .

To estimate the Crow extended parameters the following equations, which arise from maximum likelihood, are necessary:

$$\overline{\beta_{FD}} = \frac{n}{\sum_{i=1}^N Ln\left(\frac{T}{t_i}\right)}$$

$$\overline{\lambda_{FD}} = \frac{n}{T^{\overline{\beta_{FD}}}}$$

Time	Action in Test	Failure Mode	Effectiveness
2978.4	NF	1	
3591.6	FD	2	0.8
22,776	NF	1	
32,566	FD	2	0.8
43,666	FD	3	0.85
56,700	FD	4	0.9

$$\bar{d} = \frac{1}{n} \sum_{i=1}^N d_i$$

$$\overline{\lambda(t)} = \left[ \frac{n_{FI}}{T} + \sum_{i=1}^N (i - d_i) \frac{n_i}{T} \right] + \bar{d} \left[ \frac{N}{T} \overline{B_{FD}} \right]$$

where  $n$  = number of failure modes;  $T$  = total test time; and  $d$  = effectiveness index.

To illustrate the Crow extended model, the same example applied in the Crow–AMSAA model will be used here, but some improvement actions were not implemented during the test. The results are shown in Table 2.12.

Applying data from Table 2.12 on the Crow extended model equation we have:

$$\overline{\beta_{FD}} = \frac{N}{\sum_{i=1}^N \text{Ln}\left(\frac{T}{t_i}\right)} = \frac{3}{(2.75) + (0.55) + (0.26) + (0)} = \frac{3}{3.57} = 0.83$$

$$\overline{\lambda_{FD}} = \frac{N}{T \overline{\beta_{FD}}} = \frac{3}{56,700^{0.83}} = \frac{3}{8820} = 3.4 \times 10^{-4}$$

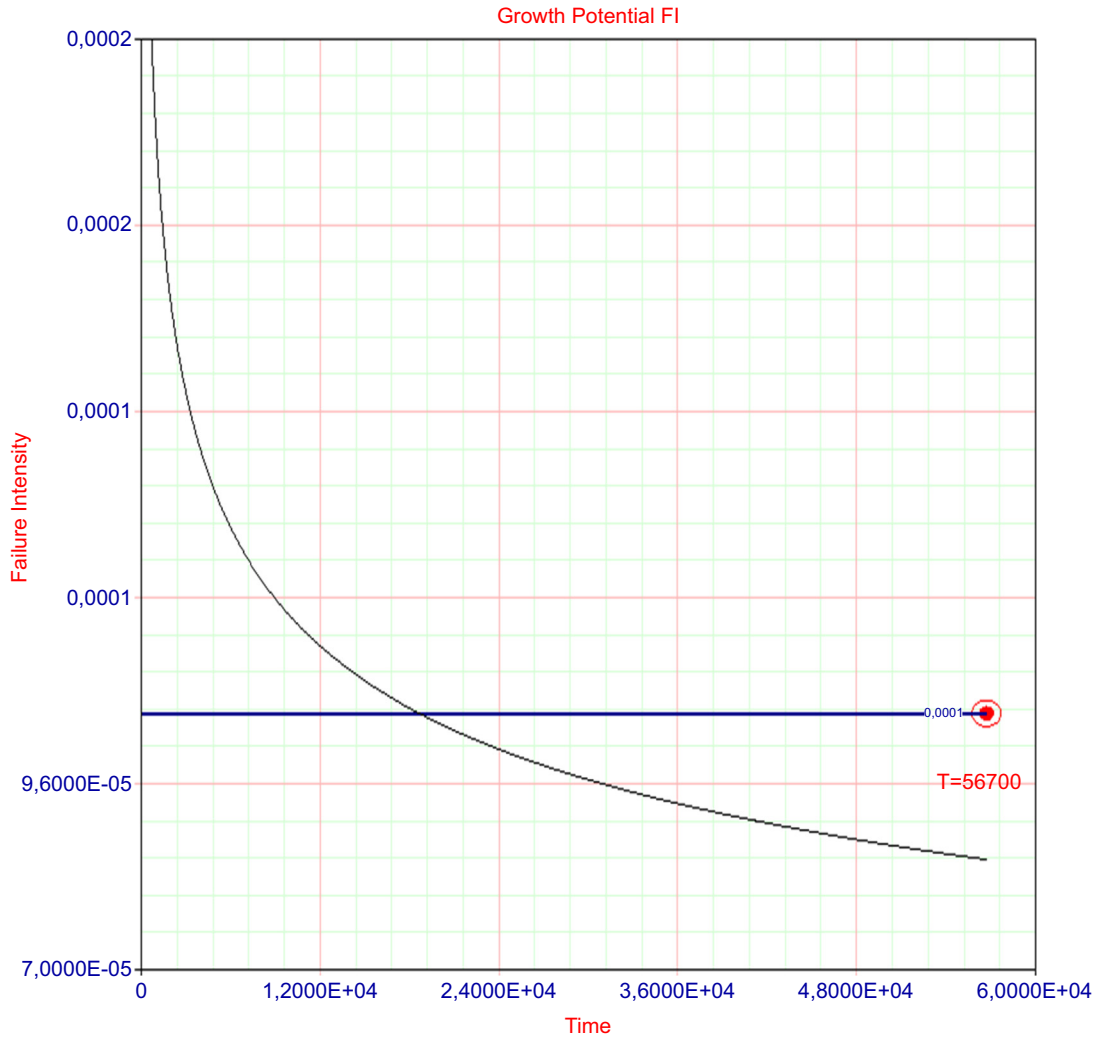
$$\bar{d} = \frac{1}{n} \sum_{i=1}^N d_i = \frac{1}{3}(0.8 + 0.85 + 0.9) = 0.85$$

$$\overline{\lambda(t)} = \left[ \frac{n_{FI}}{T} + \sum_{i=1}^N (i - d_i) \frac{n_i}{T} \right] + \bar{d} \left[ \frac{N}{T} \overline{B_{FD}} \right]$$

$$\overline{\lambda(t)} = \left[ \frac{2}{56,700} + \sum_{i=1}^3 (1 - d_i) \frac{n_i}{56,700} \right] + 0.85 \left[ \frac{3}{56,700} \times 0.83 \right]$$

$$\overline{\lambda(t)} = 1 \times 10^{-4}$$

Fig. 2.27 shows failure intensity at 56,700 hours (0.0001). It also shows the instantaneous intensity failure during test time.



**FIGURE 2.27**

Reliability × time stages (Crow extended model).

### 2.4.7 POWER LAW

The power law model is addressed for repairable systems. The expected cumulative number of failures is expressed mathematically as:

$$E(N_i) = \int_0^T \rho(t) dt$$

The power law model assumes that intensity failure is the Weibull failure rate, thus the intensity of failure over time is:

$$\rho(t) = \frac{\beta}{\eta^\beta} T^{\beta-1}$$

With the initial failure rate as:

$$\lambda_i = \frac{1}{\eta^\beta}$$

the cumulative failure rate is:

$$\lambda_c = \beta \lambda_i T^{\beta-1}$$

The intensity of failure equation describes failure intensity over operating time, and depending on the  $\beta$  value the failure intensity will increase, decrease, or keep constant over time. Keep in mind that in the power law model,  $\beta$  describes intensity failure behavior and has no relation to the Weibull distribution shape parameter. In fact,  $\beta$  is a shape parameter of the intensity failure function in the power law model. Thus in this model when  $\beta > 1$ , reliability is decreasing over time because failure intensity is increasing, or, in other words, the corrective actions are not improving the system. When  $\beta < 1$ , the intensity of failure is decreasing over time, which means reliability growth, or, in other words, the corrective actions are improving system reliability. Actually, the corrective action is more than corrective maintenance to have reliability growth in equipment. In this case, overhauling or modification is required to do so. When  $\beta = 1$ , reliability has been reestablished and the system is considered as good as new.

Using a repairable system as an example, let us consider a diesel pump at a drilling facility with failure times in years (1.07, 1.22, 1.4, 1.63, 3.12, 3.8, 5.34, 7.34, 7.4). For parameters, using equations similar to the Crow-AMSAA model, we have:

$$\beta = \frac{N}{N \ln T - \sum_{i=0}^N \ln T_i}$$

$$\beta = \frac{N}{N \ln T_i - \sum_{i=0}^N \ln T_i}$$

$$\beta = \frac{9}{(9 \times \ln(7.4) - (0.07 + 0.2 + 0.34 + 0.49 + 1.14 + 1.34 + 1.68 + 1.99 + 2))}$$

$$\beta = 1.025$$

$\beta \cong 1$ , which means no reliability growth or degradation.

$$\lambda_i = \frac{N}{T^\beta}$$

$$\lambda_i = \frac{N}{T^\beta} = \frac{9}{7.4^{1.025}} = 1.156$$



$$\text{MTBF}_i = \frac{1}{\lambda_i} = \frac{1}{1.156} = 0.865$$

$$\lambda_c = \beta \lambda_i T^{\beta-1}$$

$$\lambda_c = 1.025 \times 1.156 \times 7.4^{0.025} = 1.245$$

$$\text{MTBF}_a = \frac{1}{\lambda_a} = \frac{1}{1.245} = 0.8026$$

When comparing the accumulated MTBF with the initial MTBF and there are no significant variations, the MTBF as well as the failure rate tend to be constant over time, which makes sense if we look at the  $\beta$  (1.025) value. Fig. 2.28 shows the MTBF time, which is almost constant.

After studying the examples in this chapter, it is easy to see how accelerated testing and reliability growth analysis support oil and gas companies in their efforts to find better equipment suppliers and to make sure equipment is measuring up to quality and reliability expectations.

Many reliability requirements arise during system RAM analysis in projects or during the operational phase or even when comparing equipment performance in life cycle analysis. No matter the case, the second step after defining system availability, critical equipment, and reliability targets is to make sure critical equipment is achieving those reliability targets.

In cases when equipment in an operational system has the same technology as equipment in a project it is possible to access historical data to perform life cycle analysis. In contrast, in some cases new technology is evolved in a project and failure historical data is not reliable enough to predict new equipment reliability.

In these cases, accelerated testing is necessary to discuss more than the usual possible weaknesses and failures. Even in unusual equipment an experienced professional familiar with similar equipment would provide information to improve the product or implement actions to avoid failures that cause loss of production, accidents, or environmental impacts.

After working with the quantitative and qualitative models applied in accelerated testing and the quantitative model applied in reliability growth analysis, the next step is to access failure mode qualitatively as well as maintenance and inspection. Even if equipment and systems have high reliability, when they fail it is necessary to substitute or carry on effective maintenance. Depending on the system, maintenance may be more necessary to keep system available.

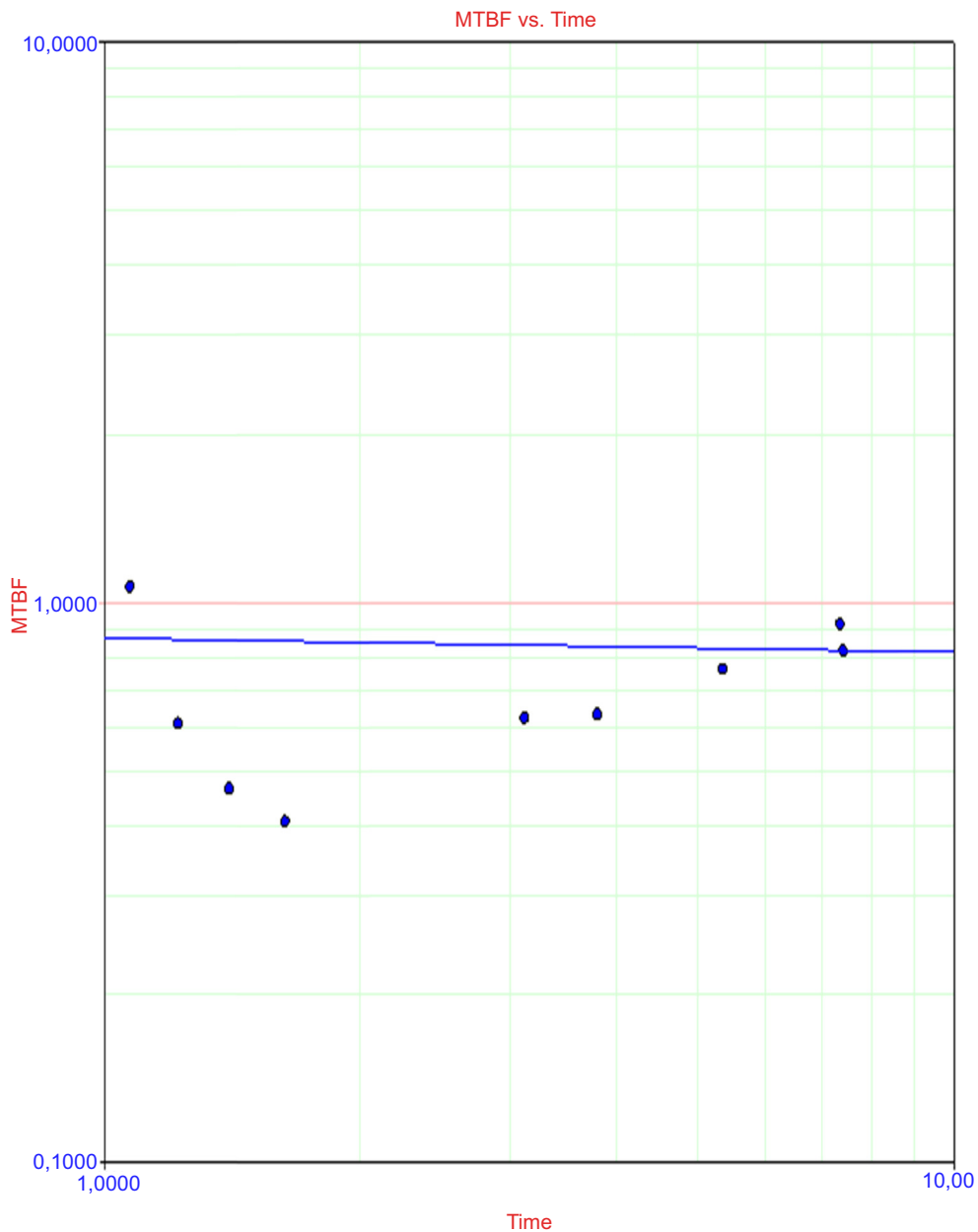
In Chapter 3, reliability will be discussed with a focus on maintenance by qualitative tools, such as DFMEA, FMEA, FMECA, RCM, RBI, REBI and RGBI as well as quantitative tools, such as optimum replacement time. All methods will be discussed with many examples to illustrate how important such methodology is and how much it can help to keep a repairable system with high availability.

---

## 2.5 PROBABILISTIC DEGRADATION ANALYSIS (PDA)

The probabilistic degradation method has the main objective of predicting the failure caused by a degradation process based on historical data. Degradation can be understood as a cumulative process of loss of function, which is caused by external factors.

Degradation refers to a specific type of failure, the effect of which is cumulative over time; in other words, it does not have an instantaneous effect on equipment or component performance. The usual



**FIGURE 2.28**  
MTBF  $\times$  time (power law).

type of degradation failure is crack, corrosion, and erosion, which are common in static equipment such as pipelines, heat exchanger tubes, furnace walls, and external equipment parts.

Therefore in order to perform the PDA, two parameters are necessary to be measured such as the degradation and the time of measurement.

In the first case, to measure the degradation process it is necessary to apply certain technology by predictive maintenance methods such as infrared and thermography, which measures the thickness of corrosion in a pipeline, for example. In addition, the time of measurement is also necessary. Therefore, as part of predictive maintenance, a report with the thickness measured and the date and operating conditions must be included to support the PDA.

The first step in the PDA is to define measurements that are considered a failure; in other words, the minimum thickness allowed. In the case of corrosion, for example, it will be the thickness caused by corrosion that leads to a loss of function. In fact, to define the limit that is considered a failure, it is necessary to take into account the time to perform the inspection and repair of the equipment.

In many cases such degradation limit is defined based on procedures or vendors' specifications, but equipment replacement time is also based on qualitative methods such as risk-based inspection, which will be demonstrated in Chapter 3.

Despite a very good approach and considering specialist opinion, the best solution is a combination of different approaches. Therefore it is interesting to implement the predictive maintenance methods and finally implement the quantitative methods such as the PDA, which will be exemplified in the next item.

The thickness measurement is very necessary because with a certain number of measurements it is possible to forecast when the limit degradation value will be achieved on time. To do this, different mathematical methods can be applied such as:

- Linear
- Exponential
- Power
- Logarithmic
- Gompertz
- Lloyd–Lipow

Additional information is the time that such measurement took place to obtain a probabilistic time to failure. In fact, in this case the probabilistic time to failure will follow the lifetime data analysis methodology described in Chapter 1. Therefore a specific PDF such as exponential, lognormal, normal, logistic, loglogistic, Gumbel, Weibull, gamma, generalized gamma, and Rayleigh will be applied to predict the probability of having a failure at the time predicted by the degradation effect.

### 2.5.1 LINEAR

The linear model describes the degradation failure process based on a linear function such as:

$$Y = AT + B$$

where  $Y$  = degradation;  $T$  = time; and  $A$  and  $B$  = parameters to be estimated.

To exemplify the linear model, cumulative pitting in a tank wall will be demonstrated based on pitting thickness measurements of six different critical points over 13 months, as shown in [Table 2.13](#).

**Table 2.13 Tank Pitting Degradation Over Time**

Measurement	Tank Wall 1 Pitting Thickness (mm per year)	Tank Wall 2 Pitting Thickness (mm per year)	Tank Wall 3 Pitting Thickness (mm per year)	Tank Wall 4 Pitting Thickness (mm per year)	Tank Wall 5 Pitting Thickness (mm per year)	Tank Wall 6 Pitting Thickness (mm per year)	Maximum Pitting Thickness (mm)	Months
1	0.12	0.12	0.14	0.07	0.13	0.06	1.0	1.0
2	0.17	0.18	0.18	0.13	0.18	0.11	1.0	2.0
3	0.19	0.21	0.23	0.16	0.20	0.13	1.0	3.0
4	0.24	0.26	0.28	0.21	0.26	0.19	1.0	4.0
5	0.31	0.32	0.33	0.30	0.33	0.26	1.0	5.0
6	0.36	0.38	0.39	0.36	0.38	0.37	1.0	6.0
7	0.43	0.41	0.44	0.39	0.45	0.44	1.0	7.0
8	0.53	0.55	0.51	0.53	0.55	0.53	1.0	8.0
9	0.60	0.62	0.63	0.60	0.62	0.60	1.0	9.0
10	0.68	0.67	0.66	0.65	0.70	0.68	1.0	10.0
11	0.73	0.70	0.74	0.68	0.74	0.72	1.0	11.0
12	0.79	0.81	0.83	0.80	0.80	0.78	1.0	12.0
13	0.87	0.90	0.88	0.89	0.88	0.86	1.0	13.0

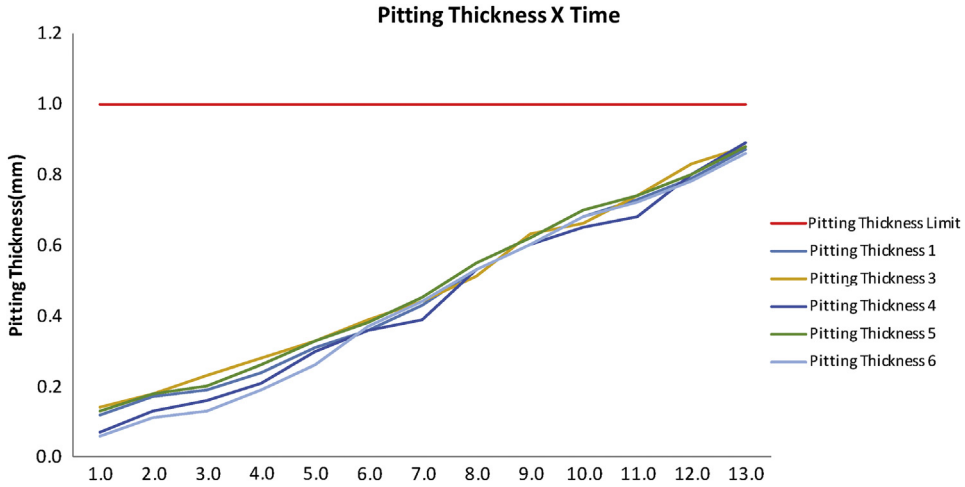


FIGURE 2.29

Tank pitting thickness degradation.

Based on the information described in Table 2.13, the linear model is the one that fits better on pitting thickness over time with high correlation ( $\sigma = 0.97$ ) for different points in the tank wall. Fig. 2.29 shows the forecast of pitting thickness for the six points in the tank wall.

Table 2.14 shows the linear equation for each measurement point and also the prediction of failure time concerning the maximum pitting thickness (1 mm) that is input in each equation.

Based on the results of Table 2.14, the lifetime data analysis prediction takes place to define the PDF, which forecasts the probability of failure. Therefore, based on lifetime data analysis, it will be possible to define the reliability for the next year to support the decision about inspection in the tank. To perform such analysis, Reliability Workbench was used, as shown in Fig. 2.30.

The Weibull PDF ( $\beta = 13.87, \eta = 15.55$ ) shows the expected profile of pitting in the tank wall that happens at the end of the life cycle. Based on Weibull 2P the reliability in the 14th year is 79.33%, which is a low value when associated with the consequence of pitting in the tank wall.

Table 2.14 Tank Pitting Thickness Degradation Prediction		
Measurement (mm per year)	Linear Model Equation	Corrosion Failure Time (years)
Pitting thickness 1	$Y_1 = 0.065T + 0.0081$	15.26
Pitting thickness 2	$Y_2 = 0.0648T + 0.0181$	15.15
Pitting thickness 3	$Y_3 = 0.0637T + 0.0342$	15.16
Pitting thickness 4	$Y_4 = 0.0684T + 0.0346$	14.11
Pitting thickness 5	$Y_5 = 0.065T + 0.0235$	15.02
Pitting thickness 6	$Y_6 = 0.0704T + 0.0523$	13.46

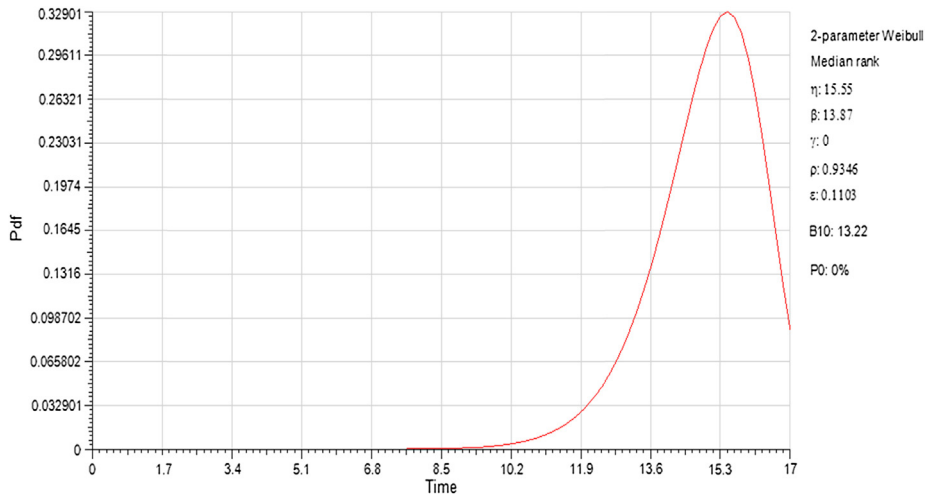


FIGURE 2.30

Tank pitting thickness failure PDF.

## 2.5.2 EXPONENTIAL

The exponential model describes the degradation failure process based on an equation such as:

$$Y = B \cdot e^{AT}$$

where  $Y$  = degradation;  $T$  = time; and  $A$  and  $B$  = parameters to be estimated by the regression method based on historical data.

To exemplify the exponential model the cumulative corrosion in a vessel will be demonstrated based on thickness measurements of seven different critical points over the next 10 years of this life cycle, as shown in [Table 2.15](#).

Based on the information described in [Table 2.15](#), the exponential model is the one that fits better on corrosion thickness over time with high correlation ( $\sigma = 0.97$ ) for different points in the vessel. [Fig. 2.31](#) shows the forecast of corrosion thickness for the six points in the vessel.

[Table 2.16](#) shows the exponential equation for each measurement point and also the prediction of failure time concerning the minimum corrosion thickness (0.12 mm), which is input in each equation.

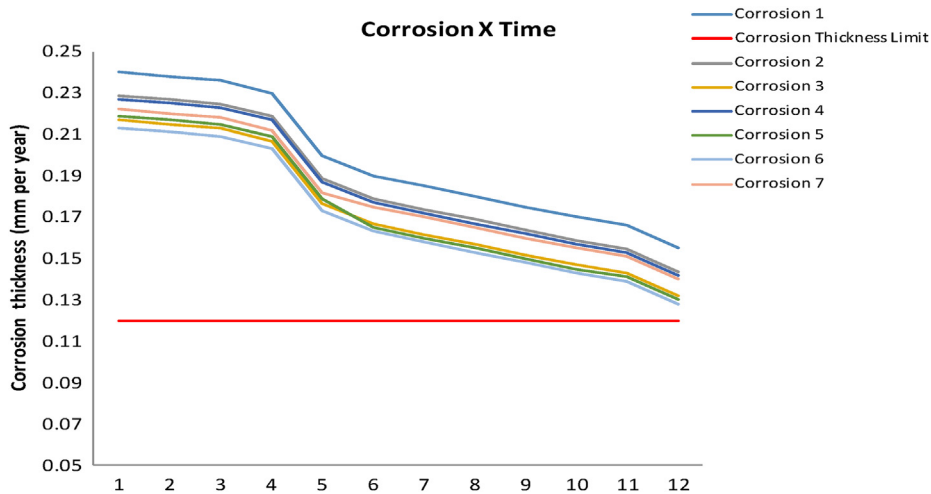
Based on the result of [Table 2.16](#), the lifetime data analysis, prediction takes place to define the PDF, which forecasts the probability of failure. Therefore, based on lifetime data analysis, it will be possible to define the reliability for the next year to support the decision about inspection in the vessel. To perform such analysis, Reliability Workbench was used, as shown in [Fig. 2.32](#).

The Weibull PDF ( $\beta = 20.13$ ,  $\eta = 16.97$ ) shows the expected profile of corrosion in a vessel that happens at the end of the life cycle. In this case, the life cycle lasts 20 years.

Based on Weibull 2P the reliability in January 2011 was 67%, which is a low value when associated with the consequence of leakage in this vessel. Therefore the final decision was to perform a repair in this vessel.

**Table 2.15 Vessel Degradation Over Time**

Measurement	Corrosion Thickness Measurement 1 (mm per year)	Corrosion Thickness Measurement 2 (mm per year)	Corrosion Thickness Measurement 3 (mm per year)	Corrosion Thickness Measurement 4 (mm per year)	Corrosion Thickness Measurement 5 (mm per year)	Corrosion Thickness Measurement 6 (mm per year)	Corrosion Thickness Measurement 7 (mm per year)	Minimum Corrosion Thickness (mm)	Time (years)
1	0.24	0.229	0.217	0.227	0.219	0.213	0.222	0.12	14/06/2002
2	0.238	0.227	0.215	0.225	0.217	0.211	0.22	0.12	21/10/2003
3	0.236	0.225	0.213	0.223	0.215	0.209	0.218	0.12	01/11/2003
4	0.23	0.219	0.207	0.217	0.209	0.203	0.212	0.12	03/01/2004
5	0.2	0.189	0.177	0.187	0.179	0.173	0.182	0.12	14/04/2004
6	0.19	0.179	0.167	0.177	0.165	0.163	0.175	0.12	27/06/2004
7	0.185	0.174	0.162	0.172	0.16	0.158	0.17	0.12	07/03/2005
8	0.18	0.169	0.157	0.167	0.155	0.153	0.165	0.12	09/01/2006
9	0.175	0.164	0.152	0.162	0.15	0.148	0.16	0.12	12/02/2007
10	0.17	0.159	0.147	0.157	0.145	0.143	0.155	0.12	10/08/2007
11	0.166	0.155	0.143	0.153	0.141	0.139	0.151	0.12	03/03/2008
12	0.155	0.144	0.132	0.142	0.13	0.128	0.14	0.12	01/01/2010



**FIGURE 2.31**  
Vessel degradation prediction.

Measurement (mm per year)	Exponential Model Equation	Corrosion Failure Time (years)
Corrosion thickness 1	$Y_1 = 0.2563 \cdot e^{-0.042T}$	18.06
Corrosion thickness 2	$Y_2 = 0.2455 \cdot e^{-0.045T}$	17.04
Corrosion thickness 3	$Y_3 = 0.2339 \cdot e^{-0.048T}$	15.89
Corrosion thickness 4	$Y_4 = 0.2438 \cdot e^{-0.045T}$	16.88
Corrosion thickness 5	$Y_5 = 0.2377 \cdot e^{-0.051T}$	16.27
Corrosion thickness 6	$Y_6 = 0.2303 \cdot e^{-0.049T}$	15.52
Corrosion thickness 7	$Y_7 = 0.2378 \cdot e^{-0.044T}$	16.28

### 2.5.3 POWER

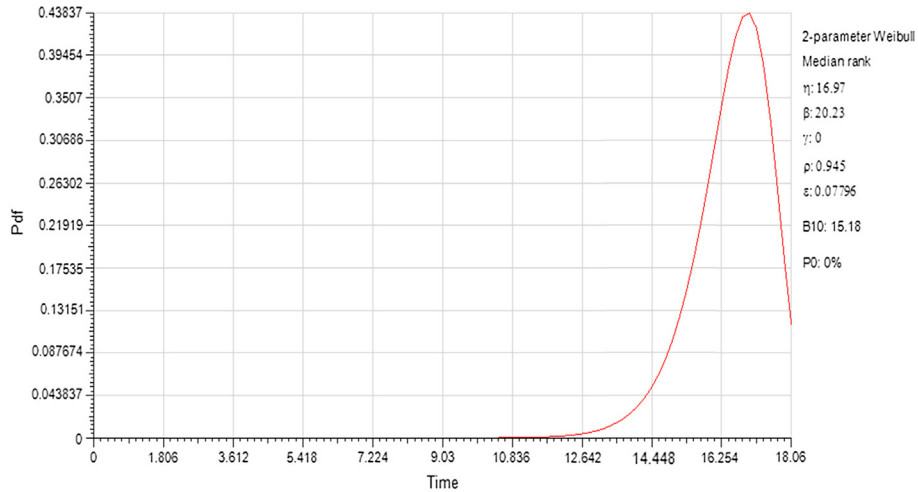
The power model describes the degradation failure process based on a power function such as:

$$Y = B \cdot T^A$$

where  $Y$  = degradation;  $T$  = time; and  $A$  and  $B$  = parameters to be estimated by the regression method based on historical data.

To exemplify the power model the cumulative crack length in a turbine blade will be demonstrated based on the measurement of six different critical points over the 6 years of the turbine life cycle, as shown in [Table 2.17](#).





**FIGURE 2.32**  
Vessel corrosion PDF.

Based on the information described in [Table 2.17](#), the power model is the one that fits better on crack failure over time with high correlation ( $\sigma = 0.92$ ) for different points in the turbine blade. [Fig. 2.33](#) shows the forecast of blade crack length for the six points in the turbine blade.

[Table 2.18](#) shows the power equation for each measurement point and also the prediction of failure time concerning the maximum crack length (20 mm), which is input in each equation.

Based on the result of [Table 2.18](#), the lifetime data analysis, prediction takes place to define the PDF that forecasts the probability of crack failure. Therefore, based on lifetime data analysis, it will be possible to define the reliability for the next year to support the decision about predictive maintenance. To perform such analysis, Reliability Workbench was used, as shown in [Fig. 2.34](#).

The Weibull PDF ( $\beta = 10.18, \eta = 7.797$ ) shows the expected profile of the crack turbine blade that happens at the end of the life cycle. In this case, the life cycle lasts 20 years.

Based on Weibull 2P the turbine blade reliability 1 year after the sixth inspection is 71%, which is a high value. Therefore the decision is to perform more than one ultrasonic predictive maintenance at the end of the seventh year.

### 2.5.4 LOGARITHMIC

The logarithmic model describes the degradation failure process based on a mathematic function such as:

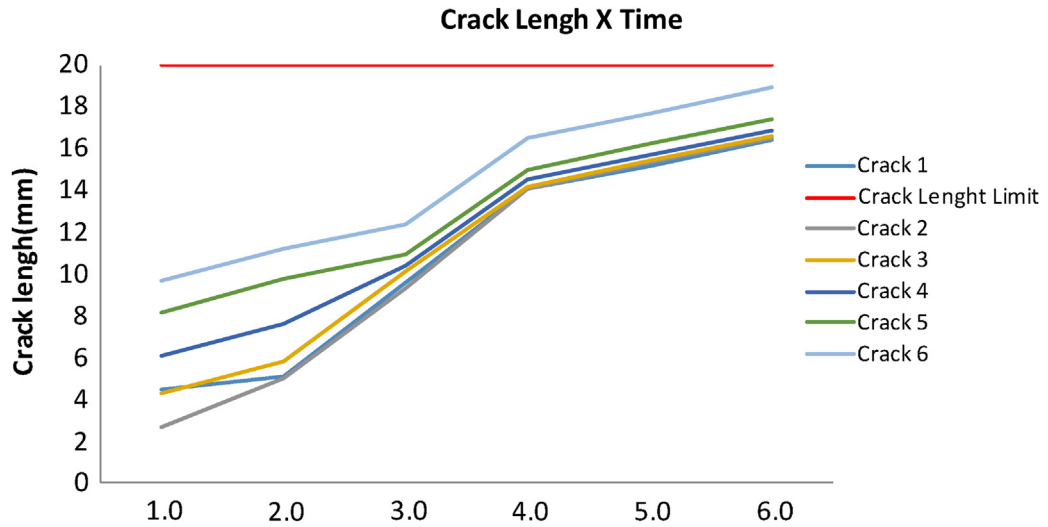
$$Y = A \cdot \ln(T) + B$$

where  $Y$  = degradation;  $T$  = time; and  $A$  and  $B$  = parameters to be estimated by the regression method based on historical data.

To exemplify the logarithmic model the cumulative erosion thickness in heat exchanger tubes will be demonstrated based on measurements of six different critical tubes of the heat exchanger over 5 years, as shown in [Table 2.19](#).

**Table 2.17 Turbine Blade Crack Degradation Over Time**

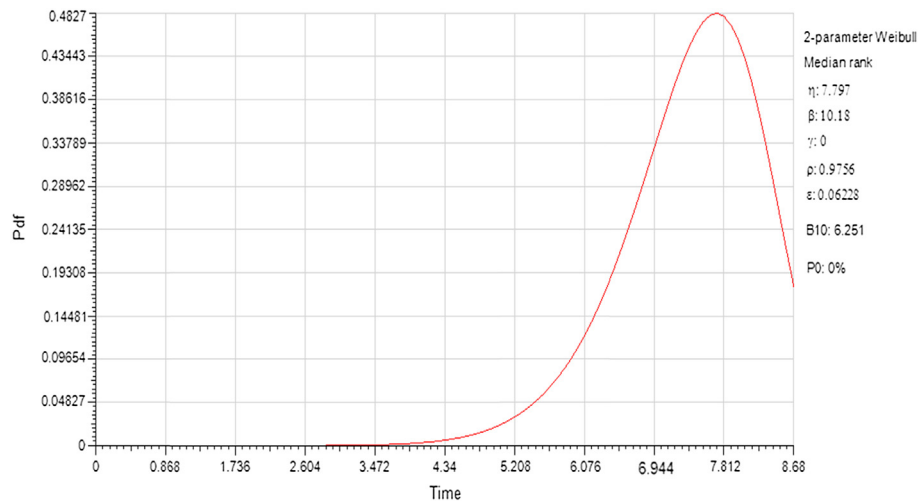
Measurement	Cracking Length 1 (mm per cycle)	Cracking Length 2 (mm per cycle)	Cracking Length 3 (mm per cycle)	Cracking Length 4 (mm per cycle)	Cracking Length 5 (mm per cycle)	Cracking Length 6 (mm per cycle)	Maximum Cracking Length (mm)	Years Cycles	Cycles ( $\times 1000$ )
1	4.47	2.67	4.27	6.07	8.17	9.67	20	1.0	150
2	5.13	5.03	5.83	7.63	9.73	11.23	20	2.0	300
3	9.6	9.3	10.1	10.4	10.9	12.4	20	3.0	450
4	14.1	14.1	14.2	14.5	15	16.5	20	4.0	600
5	15.2	15.3	15.4	15.7	16.2	17.7	20	5.0	750
6	16.4	16.5	16.6	16.9	17.4	18.9	20	6.0	900



**FIGURE 2.33**

Turbine blade crack prediction.

Measurement (mm per year)	Power Model Equation	Crack Failure Time (years)
Crack length 1	$Y_1 = 3.8793 \cdot X^{0.8246}$	7.31
Crack length 2	$Y_2 = 2.6468 \cdot X^{1.089}$	6.41
Crack length 3	$Y_3 = 3.9561 \cdot X^{0.8318}$	7.02
Crack length 4	$Y_4 = 5.6177 \cdot X^{0.6197}$	7.76
Crack length 5	$Y_5 = 7.5997 \cdot X^{0.4477}$	8.68
Crack length 6	$Y_6 = 9.0421 \cdot X^{0.3927}$	7.55

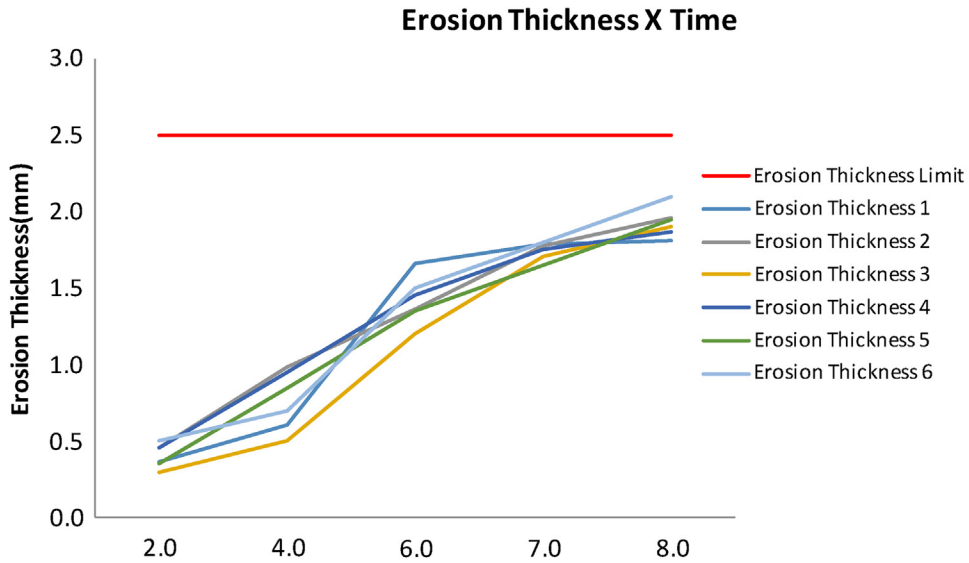


**FIGURE 2.34**

Turbine blade crack PDF.

**Table 2.19 Heat Exchanger Erosion Degradation Over Time**

Measurement	Tube 1 Erosion Thickness (mm per year)	Tube 2 Erosion Thickness (mm per year)	Tube 3 Erosion Thickness (mm per year)	Tube 4 Erosion Thickness (mm per year)	Tube 5 Erosion Thickness (mm per year)	Tube 6 Erosion Thickness (mm per year)	Maximum Erosion Thickness (mm)	Years
1	0.36	0.46	0.3	0.45	0.35	0.5	2.5	2.0
2	0.6	0.98	0.5	0.95	0.85	0.7	2.5	4.0
3	1.66	1.36	1.2	1.45	1.35	1.5	2.5	6.0
4	1.78	1.77	1.7	1.75	1.65	1.8	2.5	7.0
5	1.81	1.96	1.9	1.87	1.95	2.1	2.5	8.0



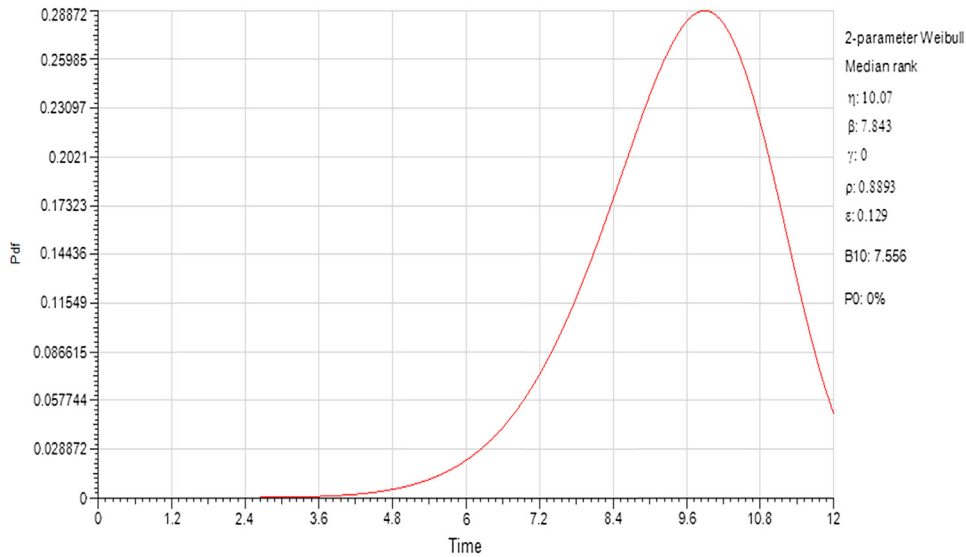
**FIGURE 2.35**  
Tube heat exchanger erosion thickness.

Based on the information described in Table 2.19, the logarithmic model is the one that fits better on erosion failure over time with high correlation ( $\sigma = 0.93$ ) for different tubes in the heat exchanger. Fig. 2.35 shows the forecast of tube erosion thickness for the six tubes.

Table 2.20 shows the logarithmic equation for each measurement point and also the prediction of failure time concerning the maximum erosion thickness (3.0 mm), which is input in each equation to forecast the time of erosion failure.

Based on the result of Table 2.20, the lifetime data analysis, prediction takes place to define the PDF, which forecasts the probability of erosion failure. Therefore, based on lifetime data analysis, it will be possible to define the reliability for the next year to support the decision about predictive maintenance. To perform such analysis, Reliability Workbench used, as shown in Fig. 2.36.

Table 2.20 Heat Exchanger Tube Erosion Prediction		
Heat Exchanger Tubes	Logarithmic Model Equation	Erosion Failure Time (years)
Tube 1—Erosion thickness	$Y_1 = 1.0363 \cdot \ln(x) + 0.2497$	8.77
Tube 2—Erosion thickness	$Y_2 = 0.9466 \cdot \ln(x) + 0.3997$	9.20
Tube 3—Erosion thickness	$Y_3 = 1.0632 \cdot \ln(x) + 0.102$	9.54
Tube 4—Erosion thickness	$Y_4 = 0.9236 \cdot \ln(x) + 0.4096$	9.61
Tube 5—Erosion thickness	$Y_5 = 0.9963 \cdot \ln(x) + 0.2761$	9.32
Tube 6—Erosion thickness	$Y_6 = 1.04543 \cdot \ln(x) + 0.3191$	8.05



**FIGURE 2.36**

Heat exchanger tubes erosion PDF.

The Weibull PDF ( $\beta = 10.07$ ,  $\eta = 7.843$ ) shows the expected profile of the tube erosion that happens at the end of the life cycle. In this case, the life cycle lasts 20 years.

Based on Weibull 2P the tube reliability 1 year after the eighth inspection is 52%, which is a high value. Therefore the decision is to replace the damaged tubes.

### 2.5.5 PHASE EXPONENTIAL MODEL

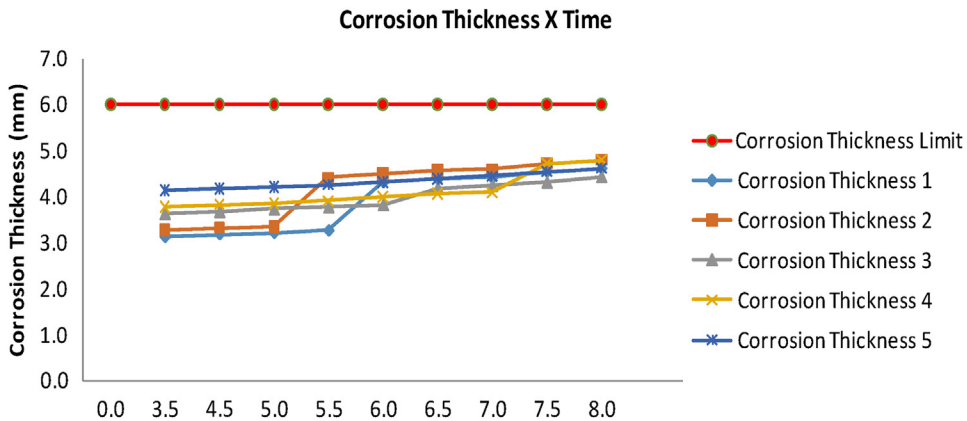
The phase exponential model developed by C. Guedes Soares and Y. Garbatov describes the degradation failure process based on an exponential function concerning a period after loss of corrosion protection. In fact, in the first phase it is assumed that there is no corrosion because the corrosion protection system is elective. Failure of the protection system will occur at a random point in time and the corrosion wastage will start a nonlinear growing process with time (Soares and Garbatov, 1999). Such phase degradation is represented by the equation:

$$Y = 1 - e^{-\left(\frac{T-\tau_c}{\tau_t}\right)}$$

where  $Y$  = degradation;  $T$  = time;  $\tau_c$  = time without degradation; and  $\tau_t$  = transition time.

To exemplify the phase model the cumulative corrosion thickness in a tank bottom will be demonstrated based on measurements of five different measurement points on the bottom floor over 8 years, as shown in Table 2.21.

Table 2.21 Tank Floor Corrosion Failure Prediction		
Tank Floor Points	Phase Model Equation	Corrosion Failure Time (years)
Point 1—Corrosion thickness	$Y_1 = 1 - e^{-\left(\frac{T-3.5}{5}\right)}$	11.5
Point 2—Corrosion thickness	$Y_2 = 1 - e^{-\left(\frac{T-3.5}{4.5}\right)}$	10.7
Point 3—Corrosion thickness	$Y_3 = 1 - e^{-\left(\frac{T-3.5}{4.75}\right)}$	11.1
Point 4—Corrosion thickness	$Y_4 = 1 - e^{-\left(\frac{T-3.5}{4.6}\right)}$	10.86
Point 5—Corrosion thickness	$Y_5 = 1 - e^{-\left(\frac{T-3.5}{5.1}\right)}$	12.66

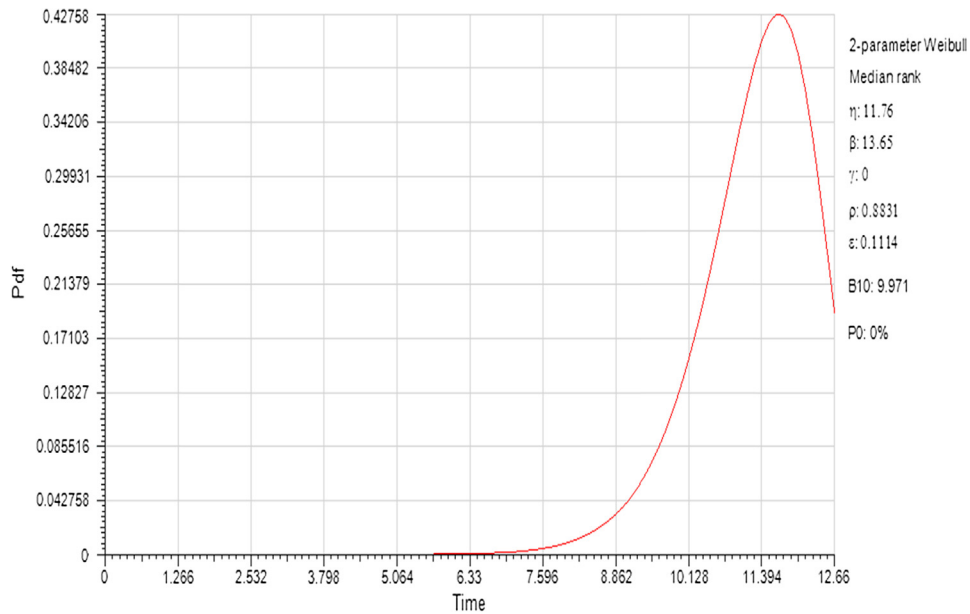


**FIGURE 2.37**  
Tank corrosion thickness.

Based on the information described in Table 2.21, the model is the one that fits better on corrosion failure over time. Fig. 2.37 shows the forecast of corrosion thickness for the different measurement points.

Table 2.21 shows the model equation for each measurement point and also the prediction of failure time concerning the maximum erosion thickness (6.0 mm), which is input in each equation to forecast the time of corrosion failure.

Based on the result of Table 2.21, the lifetime data analysis, prediction takes place to define the PDF, which forecasts the probability of corrosion failure. Therefore, based on lifetime data analysis, it will be possible to define the reliability for the next year to support the decision about predictive maintenance. To perform such analysis, Reliability Workbench was used, as shown in Fig. 2.38.



**FIGURE 2.38**

Tank floor corrosion PDF.

The Weibull PDF ( $\beta = 13.75$ ,  $\eta = 11.76$ ) shows the expected profile of the tank floor corrosion that happens after 3.5 years caused by a high level of corrosive acid in the tank product.

Based on Weibull 2P the tank corrosion reliability 1 year after the last inspection measurement is predicted to be 97.5%, which is a low chance of failure. Therefore the decision is not to replace the damaged floor and wait for the result of the next inspection.

## REFERENCES

- Crow, L.H., 1974. Reliability analysis for complex repairable systems. In: Proschan, F., Senffing, R.J. (Eds.), *Reliability and Biometry*. SIAM, Philadelphia, p. 379.
- Guedes Soares, C., Garbatov, Y., 1999. Reliability of maintained, corrosion protected plates subjected to non-linear corrosion and compressive loads. *Elsevier Marine Structures* 12, 425–445.
- Koeche, A.R., 2009. Crescimento da confiabilidade em produtos para automação bancária. SIC, Reliasoft Brasil.
- Koeche, A.R., 2010. O desenvolvimento de produtos usando técnica HALT e RGA. SIC, Reliasoft Brasil.
- ReliaSoft Corporation. Altapro Software Package, Tucson, AZ. [www.Weibull.com](http://www.Weibull.com).
- ReliaSoft Corporation. RGA++ 7.0 Software Package, Tucson, AZ. [www.Weibull.com](http://www.Weibull.com).



# RELIABILITY AND MAINTENANCE

## CHAPTER OUTLINE

<b>3.1 Introduction</b> .....	<b>159</b>
3.1.1 FMEA Introduction .....	160
<i>Design Failure Mode Effects Analysis</i> .....	163
<i>Failure Mode Analysis: Process and Operational Applications</i> .....	167
<i>Criticality Analysis to Define the Critical Equipment List</i> .....	174
<b>3.2 Maintenance Strategy</b> .....	<b>179</b>
<b>3.3 RCM Analysis</b> .....	<b>189</b>
<b>3.4 RBI Analysis</b> .....	<b>193</b>
<b>3.5 ReBI Analysis (Reliability Based Inspection)</b> .....	<b>199</b>
<b>3.6 ReGBI Analysis (Reliability Growth Based Inspection)</b> .....	<b>202</b>
<b>3.7 Optimum Replacement Time Analysis</b> .....	<b>204</b>
<b>3.8 FRACAS Analysis</b> .....	<b>207</b>
3.8.1 Warranty Analysis .....	212
<b>References</b> .....	<b>219</b>
<b>Appendix</b> .....	<b>221</b>
<b>3.9 FMEA, RCM, and RBI Case Studies</b> .....	<b>221</b>
3.9.1 Centrifugal Pump FMEA/RCM .....	225
3.9.2 Valve FMEA/RCM .....	226
3.9.3 Pipeline FMEA/RBI .....	233
3.9.4 Tank FMEA/RBI .....	233
3.9.5 Centrifugal Compressor FMEA/RCM .....	238
3.9.6 Flowline FMEA/RBI .....	248

## 3.1 INTRODUCTION

Chapters 1 and 2 dealt with quantitative approaches and methodologies to assess failure data to predict reliability. Such approaches are very appropriate mainly when known equipment is being assessed, and even in a test it is not hard to form conclusions with respect to equipment reliability. However, when there is no historical data available or very little information about a product in the development phase, qualitative analysis may help to make decisions about equipment failures and what must be done to

avoid such failures or reduce their impact. In addition, in development, test qualitative analysis would help to define products' weakness, which must be used to obtain reliable test results.

### 3.1.1 FMEA INTRODUCTION

Failure mode and effects analysis (FMEA) is a qualitative approach proposed to clear up equipment failure modes in equipment analysis or development products to support decisions when there is insufficient information and data to carry out quantitative analysis.

The FMEA was carried out first by US Army. In the 1950s the MIL-P-1629 procedure was developed and in following decades the aerospace and other industries started to apply FMEA in their processes to better understand equipment failures. Thus FMEA can be applied in the product development phase to support decisions and obtain information from experienced manufacturers and operators who operate, fix, and perform maintenance of such equipment. In the development product phase, FMEA is called DFMEA, which means design failure mode effects analysis, and it will be described in more detail in the next section.

FMEA can also be applied to operational plant equipment to support reliability, availability, and maintainability (RAM) analysis, risk analysis, reliability centered maintenance (RCM), and maintenance policy.

Indeed, FMEA's focus is equipment failure modes and it is possible to divide plants into systems and subsystems to assess each piece of equipment and its failure mode. Such analysis may focus on safety, environment, or operational effects, in case of equipment failures. Thus, depending on the objective, FMEA may have a different focus. One remarkable point is that FMEA supports RAM analysis. Typically in this case the system analyzed in the RAM analysis is unknown, and FMEA will clear up equipment failure modes in each system assessed in RAM analysis. When a reliability professional does not know too much about the equipment, this is a good approach before starting RAM analysis because FMEA will give a good idea and precise information about what kind of failure each equipment is experiencing, which failures must be in historical data, and which failures impact system availability. Despite the advantage of clearing up equipment failure modes and their impacts, whenever FMEA is performed before RAM analysis, more time is required and in some cases its impact on analysis time should be known. When there is historical failure data available to perform the RAM analysis and it is clear which failure mode impacts on system availability it is not necessary to perform FMEA. In Chapter 4 there will be examples of RAM analysis with and without FMEA.

Based on FMEA results it is possible to perform RCM. RCM analysis has as its main objective to define equipment maintenance policies and in some cases failure historical data and life cycle analysis can support RCM as well as FMEA. However, is always ideal to perform RCM analysis supported by lifetime data analysis results as input to have a more reliable definition about when the failures might occur in order to define the preventive maintenance and inspection task schedule to be carried out along asset life cycle. Essentially, RCM analysis may be carried out also based on equipment and components failure modes defined by FMEA analysis. Such approach enables to be more specific about the preventive maintenance and inspections task which must prevent the failure modes which occur during operational life cycle phase.

Depending on the failure mode, in some cases equipment failures may cause accidents and have an effect on health or the environment. In this way, FMEA is carried out as risk analysis and in this case the consequences may be damaging to employees' health or to the environment. A failure that may cause damage to employees' health is called unsafe failure, for example, pipeline corrosion that may cause a toxic product spill.

As risk analysis tools, traditionally it is necessary to define the frequency and consequence for each failure mode, but in many cases this is not done, despite being a risk analysis. This happens because mostly all recommendations will be implemented no matter how bad the consequences are. In fact, there is a variation of FMEA that regards frequency, consequence, and detection using a qualitative qualification approach based on safe policies. In doing so, this approach is called FMECA, which means failure mode, effects, and criticality analysis. The criticality is an index that defines failure cause frequency, failure consequence, and failure detection. Examples of FMECA will be given in the next section in detail and the advantages and drawbacks of performing such a methodology will be made clearer. Essentially, the advantages of applying FMECA are to have, at the end of the analysis, a hierarchy of failure modes ranging from the highest critical to the least critical. In a project this is a very good approach because it is easier to prioritize which recommendation will be implemented first.

Before describing FMEA applications it is very important to have in mind the different types of failure that will be used in an FMEA:

- Failure on demand;
- Occult failure;
- Common cause failure;
- Unsafe failure.

*Failure on demand* occurs when equipment is required to operate and fail. A good example is a standby pump that fails when it is required to operate. Most of the time such a standby pump is not operating because a similar pump is operating, but when this main pump fails, a standby pump is required to operate to avoid system shutdown. The maintenance professional has a very important responsibility in establishing inspection routines in standby equipment to avoid failures on demands. In the case of pumps, a number of maintenance professionals suggest occasionally putting the standby equipment into operation to guarantee that failure on demand will not occur. Thus when one piece of equipment is operating, the other piece of equipment will be inspected and if necessary perform preventive maintenance.

*Occult failure* occurs when equipment fails and nobody is aware. This is where there is a typical failure of safety equipment like safety instrumented function (SIF) where, for example, more than one sensor to trigger a logic element to a final element (valve) is activated. In some cases, for example, there must be two or three signals (2oo3) or, in other words, architecture two out of three. In this case if one initial element fails, there will be another two, and even with occult failure the equipment is still working. If there is one sensor failure on an SIF, such a failure is occult because the sensor failure will only be identified when unsafe conditions occur and the SIF is needed. In some cases even when failures occur it is hard to identify occult failure because the equipment does not lose its function. Some occult failure occurs in other types of equipment in the oil and gas industry such as in tube and shell heat exchangers. In such equipment obstructions occur in some tubes because of bad water quality, for example, but the equipment keeps its heat exchange performance. During preventive maintenance, when the maintenance team opens the heat exchanger they may find that some tubes are obstructed and it is necessary to clear or change the tubes for good equipment.

*Common cause failure* is when two different failures have one common cause. The best example is an energy system shutdown, which shuts down the whole plant. In this case, there are many types of equipment in the plant that can fail after the plant returns to operation and these failures would not happen if the plant were not shut down by the energy system shutdown. In this case the equipment failure cause is the same: the system energy shutdown.

*Unsafe failure* makes equipment unsafe, which may cause harm to employees or have an environmental impact. An example of unsafe failure is when the relief valve in a furnace fails to close. Considering the furnace as a piece of equipment and a relief valve as a furnace component, such failure is unsafe because even if it is possible to operate the furnace without a relief valve if the pressure goes higher than usual, it will not happen because the relief valve is a closed failure in unsafe conditions. It is very important to state that equipment does not impact system availability when an unsafe failure occurs, but depending on safety policies in each company, such equipment may be kept in operation. Many accidents happen in the gas and oil industry all over the world because of unsafe failure and attention must be given to this type of failure.

For FMEA to be effective it is necessary to observe four main stages during analysis: planning, effectiveness, review, and recommendations implementation at the correct time. Therefore, FMEA can be divided into four stages with 10 steps (Carson, 2005), which may make FMEA application easier with more chance of success, as shown in Fig. 3.1. The first FMEA phase is the planning stage and it includes a planning strategy to develop FMEA and planning resources steps.

The planning strategy includes the steps needed to get the professional and physical resources and management support in place. Without planning, the chance of success decreases.

The second important step is planning resources. Actually, the most important resource in FMEA are the experienced professionals who contribute their knowledge, but it is important to remember that in most companies such professions are working on other services at the same time. In some cases, it is better to postpone FMEA to have the most experienced professionals take part than to improvise or

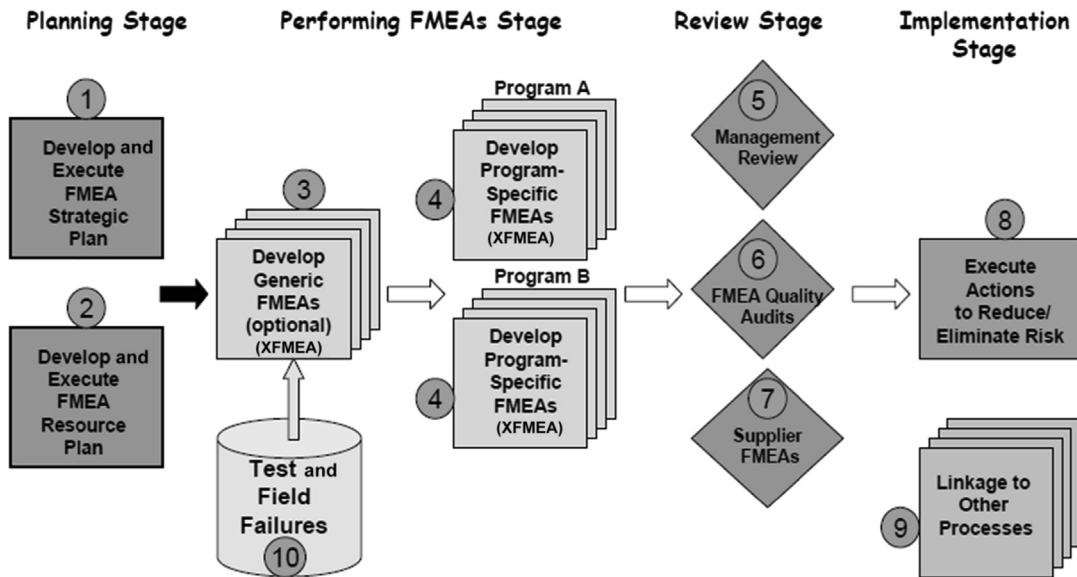


FIGURE 3.1

Effective FMEA process (adapted).

Source: Carson, C.S., 2005. *Fazendo da FMEA uma ferramenta de Confiabilidade Poderosa*. SIC.

perform analysis without this knowledge and experience. In addition professionals, local and visual resources and data are also important to have a more successful FMEA analysis.

The third stage is performing FMEA, and after all the necessary resources have been found, it is necessary to define the objectives and boundaries of analysis. While this may seem obvious, in some cases it is not, because different specialists that take part in an FMEA analysis group have different objectives. Because of this it is very important to have a good FMEA leader to clarify the main FMEA objectives and maintain FMEA focus.

The fourth stage is the review, which ensures that all recommendations of the FMEA are implemented to achieve the FMEA main objective. Basically, the review stage comprises management review, quality audit, and supplier FMEA. Management review and support are essential to implement recommendation because management is responsible for economics and making decisions, and if they are not convinced of the importance of the recommendations, they will likely not be implemented. In some cases, an FMEA quality audit is needed, usually when FMEA is performed in the project phase to check the consistency of the recommendations. Such an audit is not necessarily a formal audit, but someone or a group of specialists with experience to critically analyze the FMEA. While audits are common in some companies, in others such critical analyses are not well accepted. In these cases, it is because some believe that the main objective of the FMEA audit is to find errors and not to improve the process.

In some cases, the root cause of equipment and component failures must be supplied to the FMEA. But in other cases it is hard to define the root cause of equipment failure because it is related to component quality and such issues must be addressed to suppliers.

The last and final stage is implementation where recommendations discussed in FMEA are implemented and linked with other processes that influence the effectiveness of the recommendation. [Fig. 3.1](#) illustrates all these aspects.

All 10 steps are equally important for a successful FMEA. In case of any mistakes along the way efficacy may be lost and more resources may be necessary. When time is restricted, a delay in FMEA can mean not implementing a recommendation, which can be critical to a project or process in terms of mitigating risk or increasing availability.

### ***Design Failure Mode Effects Analysis***

During the product development phase DFMEA is applied with the potential to prevent failures in equipment and save time during the development phase. Whenever failure modes are detected, in time the DFMEA recommendations enable product improvement and supply testing with information for testing product weakness. DFMEA has a qualitative prioritization criterion called RPN (risk priority number), which includes frequency of failure occurrence, consequence severity, and detection. When FMEA is applied during the operation phase, in some cases, the RPN prioritization criterion is also applied, and this approach is called FMECA, as will be explained in the following section. No matter the phase, in an RPN, the higher the consequence severity, the higher the probability, and the harder it is to detect a failure mode, the more critical the failure mode will be. These three variables may have different combinations and for each one there are qualitative criteria. Each criterion has a qualitative explanation related to a specific number, and when probability, consequence, and detection are assessed, this qualitative state is chosen and a number is defined for each variable. In the end the product of these three numbers defines the RPN values. An example of probability criterion is shown in [Table 3.1](#).

<b>Frequency Qualification</b>	<b>Frequency</b>	<b>Ranking</b>
<b>Very high: failure is almost inevitable</b>	>1 in 2	<b>10</b>
	1 in 3	<b>9</b>
<b>High: repeated failures</b>	1 in 8	<b>8</b>
	1 in 20	<b>7</b>
<b>Moderate: occasional failures</b>	1 in 80	<b>6</b>
	1 in 400	<b>5</b>
	1 in 2,000	<b>4</b>
<b>Low: relatively few failures</b>	1 in 15,000	<b>3</b>
	1 in 150,000	<b>2</b>
<b>Remote: failure is unlikely</b>	<1 in 1,500,000	<b>1</b>

In [Table 3.1](#), 1 in 2, for example, means one failure in 2 years. In some cases, despite frequency failure, the values in the table represent probability and are also used to calculate the RPN value.

Thus, depending on the expected occurrence of failure frequency, a ranking number will be defined and included in the DFMEA file. As discussed, the higher the frequency failure ranking, the worse the situation and the greater the influence on the RPN value.

Similar to failure frequency, severity has a ranking related to the severity effect of the failure, which is described in [Table 3.2](#). The higher the severity ranking, the higher the RPN value. The severity criteria given in [Table 3.2](#) are adequate for operational and safety effects. Such concepts can also be applied when the failure affects the environment.

The third criterion is detection and it is necessary to be cautious here because in many cases detection looks easy, but it is not. If detection is underestimated, the RPN will be lower and the failure will not be prioritized over other failures modes. In detection ranking, the higher the rank, the harder is to detect the failure mode and the more impact the detection criterion has on the RPN value.

In some cases, inspection devices are recommended to detect failures before they occur. These are most often useful when failure effects have high consequence severity. Detection can be visual, auditive, manual, or automatic. In some cases, to reduce failure occurrences, more than one detection is used for equipment or for a process. [Table 3.3](#) shows an example of detection classification.

RPN parameters in the DFMEA file have blanks to define failure modes, causes, consequences, and recommendation.

System or equipment characteristics, draw numbers, data, people involved in the analysis, and other important references are generally included.

[Table 3.4](#) shows an example DFMEA of a seal pump during the development phases when DFMEA was performed. It is interesting to observe that most failures are related to the material used in the product (seal), assembly configuration, and other failures in the product development phase.

As discussed, DFMEA is a good tool for finding out the probable weakness of a product and to supply an accelerated testing and reliability growth program with such information.

In [Table 3.4](#), there are three failure modes detected in DFMEA. The first one is the sensor seal with internal or external damage or loosened during assembly because of compression. The effects are that

**Table 3.2 Severity Effect**

Severity Level	Severity Description	Ranking
Hazardous without warning	Very high severity ranking when a potential failure mode affects safe system operation without warning	10
Hazardous with warning	Very high severity ranking when a potential failure mode affects safe system operation with warning	9
Very high	System inoperable with destructive failure without compromising safety	8
High	System inoperable with equipment damage	7
Moderate	System inoperable with minor damage	6
Low	System inoperable without damage	5
Very low	System operable with significant degradation of performance	4
Minor	System operable with some degradation of performance	3
Very minor	System operable with minimal interference	2
None	No effect	1

**Table 3.3 Detection**

Detection	Likelihood of Detection by Design Control	Ranking
Absolute uncertainty	Design control <b>cannot</b> detect potential cause/mechanism and subsequent failure mode	10
Very remote	<b>Very remote</b> chance the design control will detect potential cause/mechanism and subsequent failure mode	9
Remote	<b>Remote</b> chance the design control will detect potential cause/mechanism and subsequent failure mode	8
Very low	<b>Very low</b> chance the design control will detect potential cause/mechanism and subsequent failure mode	7
Low	<b>Low</b> chance the design control will detect potential cause/mechanism and subsequent failure mode	6
Moderate	<b>Moderate</b> chance the design control will detect potential cause/mechanism and subsequent failure mode	5
Moderately high	<b>Moderately high</b> chance the design control will detect potential cause/mechanism and subsequent failure mode	4
High	<b>High</b> chance the design control will detect potential cause/mechanism and subsequent failure mode	3
Very high	<b>Very high</b> chance the design control will detect potential cause/mechanism and subsequent failure mode	2
Almost certain	Design control <b>will</b> detect potential cause/mechanism and subsequent failure mode	1

**Table 3.4 Seal Pump DFMEA**

Item/ Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	S e v	Potential Cause(s)/ Mechanism(s) of Failure	F r e q	Current Design Controls	D e t	R P N	Recommended Action(s)	Responsibility and Target Completion Date
Seals										
Sensor mount. seal	Loosen during sensor assembly/service	Leakage	6	Fitting not held in place	1		1	6	New fitting design. Prototype validation	Reliability engineer
	Damaged internal thread	Cannot install sensor	6	Damaged during installation or transportation	1		1	6	Quality control in installation and transportation	Quality supervisor
	Damaged external thread	Cannot install wire nut	3	Damaged during shipment to customer	2		1	6	Quality control in shipment	Logistic supervisor
Hose connection	Crack/break burst. Bad seal poor hose quality	Leak	7	Over pressure	7	Burst, validation pressure cycle	1	49	Test included in prototype and production validation testing	Reliability engineer
		Failed mount	4	Vibration	8	Vibration w/road tapes	3	96	Obtain vibration road tape	Quality supervisor
		Hose leak	6	Overpressure	5	Burst, validation pressure cycle with clamps	2	60	Obtain clamps and clamping specification	Quality supervisor
Heat transfer structure	Stress crack	Leak. Loss of heat transfer	7	Wicking. Material strength	6	Thermal cycle	1	42	Included in product specification	Quality supervisor
	Corrosion	Leak. Loss of heat transfer	7	Coolant quality. Contamination. Environment— int/ext	6	Service simulation coolant evaluation	5	210	Supplier coolant to be evaluated	Reliability engineer
	Seam fail	Leak. Loss of heat transfer	4	Environment— int/ext	1	Service simulation	1	4	Included in product specification	Quality supervisor

the sensor cannot be installed and there is leakage. The recommendation is quality control in assembling a new design prototype.

The second failure mode is related to a hose connection with a crack, break, or burst caused by vibration and overpressure. The main recommendation is performing a validating test.

The third failure mode is for the heat transfer structure where leakage occurs because of loss of heat transfer mainly because of material quality. The main recommendation is to verify product specifications.



There are additional types of FMEA such as process FMEA (PFMEA) and system FMEA (SFMEA). PFMEA is dedicated to identifying failure during the production and assembly phase after the design. SFMEA is dedicated to assessing the consequence of failures at the system level considering the effects on other systems. SFMEA can be carried out on equipment and component levels as well as on other systems. Moreover, during SFMEA analysis, different phases can be taken into account, which are related to the causes of the failure modes. [Section 3.8](#) demonstrates several examples of FMEA that encompass different phases such as design, manufacturing, transportation, commissioning, operation, and decommissioning. Such an approach is appropriate when certain equipment or systems are assessed. In the case of new equipment, different applications, or environmental conditions, it is also necessary to apply specific FMEAs such as DFMEA, PFMEA, and SFMEA to different phases.

### ***Failure Mode Analysis: Process and Operational Applications***

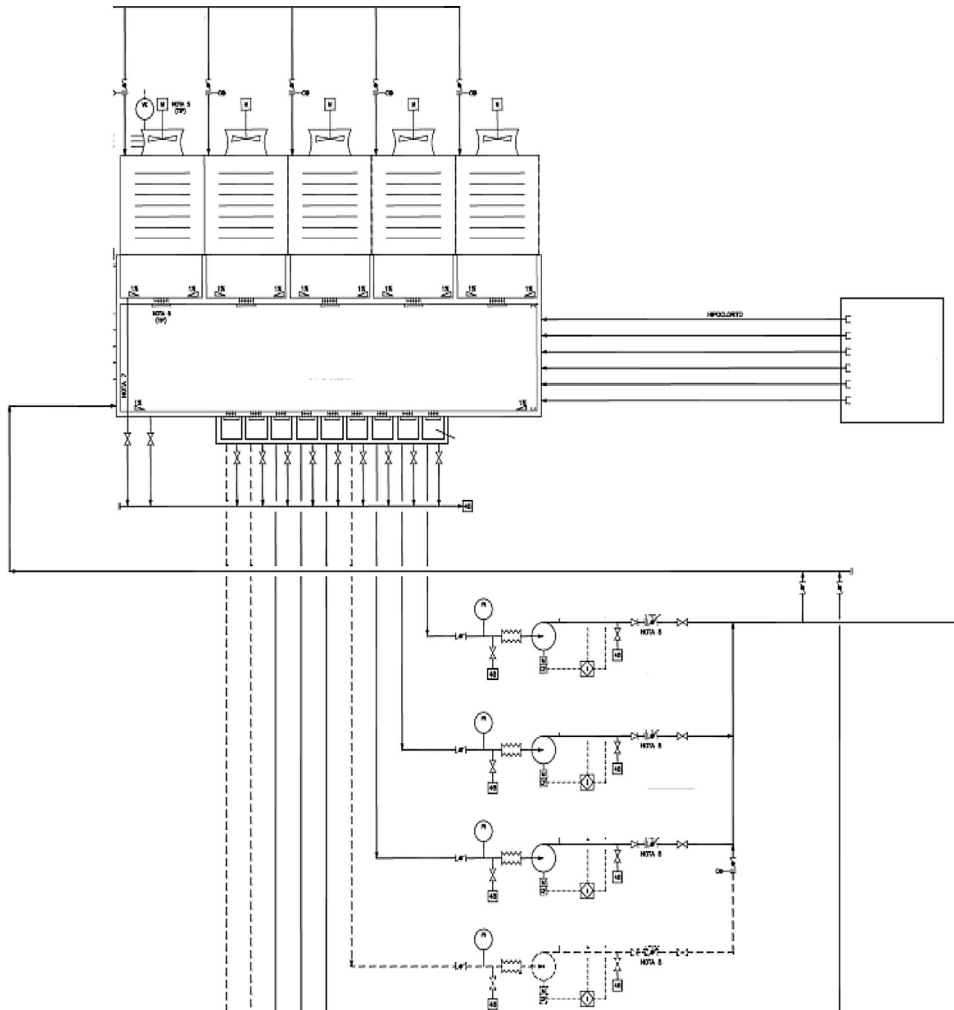
Failure mode analysis has many applications for assessing equipment in a project phase or operational phase. In fact, FMEA can be carried out for single piece of equipment or for all equipment in a whole plant. As discussed, the main objective is to describe the types of failures for each piece of equipment and component, the causes, effects, and necessary recommendations. Failure can be understood as the way that equipment or components lose their function, which partially or totally affects performance. When applied to understanding and avoiding failure modes in equipment, FMEA is not used to describe unsafe failure, unless it affects system or equipment availability. Thus whenever FMEA is carried out with an operational focus it must be clear that some unsafe failure modes exist, and performing FMEA do not mean that it is not necessary to perform other risk analysis. Unfortunately, most of the time FMEA is carried out with one specific focus, which means operational and safety issues uncovered in the analysis. This happens because of reduced time to perform FMEA, different objectives, and sometimes because a safety specialist is not involved. Addressing FMEA and operational and safety issues at the same time is not a problem, but it involves more resources, which may or may not be available.

To illustrate this point, this section provides FMEA examples with operational focus and safety focus.

The following examples include a water facility, electrical system facility, load movement drill subsystem, and a diethylamine treatment system, which are facilities and equipment used in upstream and downstream operations all over the world.

#### **Water Supply System**

The first example is a water supply system, which provides water to cool down other systems. Such a system usually includes pumps, valves, and cooling towers. The cooling towers have fans that are connected to electric motors. The water is pumped in through towers passing below fans when it is cooling down and pumped out by pumps. In this case the whole system includes all equipment and is called a cooling system. [Fig. 3.2](#) shows a water supply system. Above the towers the water is pumped by pumps that are not shown in the figure. There are four towers where at least one must be available to supply their main customer. The flow of water is regulated by valves (on/off) and after passing by the towers there is one huge water collector, then more valves to control flow to the pumps. There are four pumps to pump water out of the system and at least one is required to supply water to the cooling



**FIGURE 3.2**

Water supply system.

system. Despite only one tower and only one pump to supply the cooling system to keep the main customer system available, the other towers and pumps are required for other systems.

Table 3.5 represents the FMEA data and the failures modes, causes, effects, and recommendations necessary to fill out the draw number, system name, analyst team names, and date.

In this way it is possible to understand the equipment failure modes. The following step is an additional recommendation. In water system draw there is a chemical product tank that supplies the water collector. In case of failure in the chemical tank such as corrosion, chemical product may leak to

**Table 3.5 FMEA (Water System)**

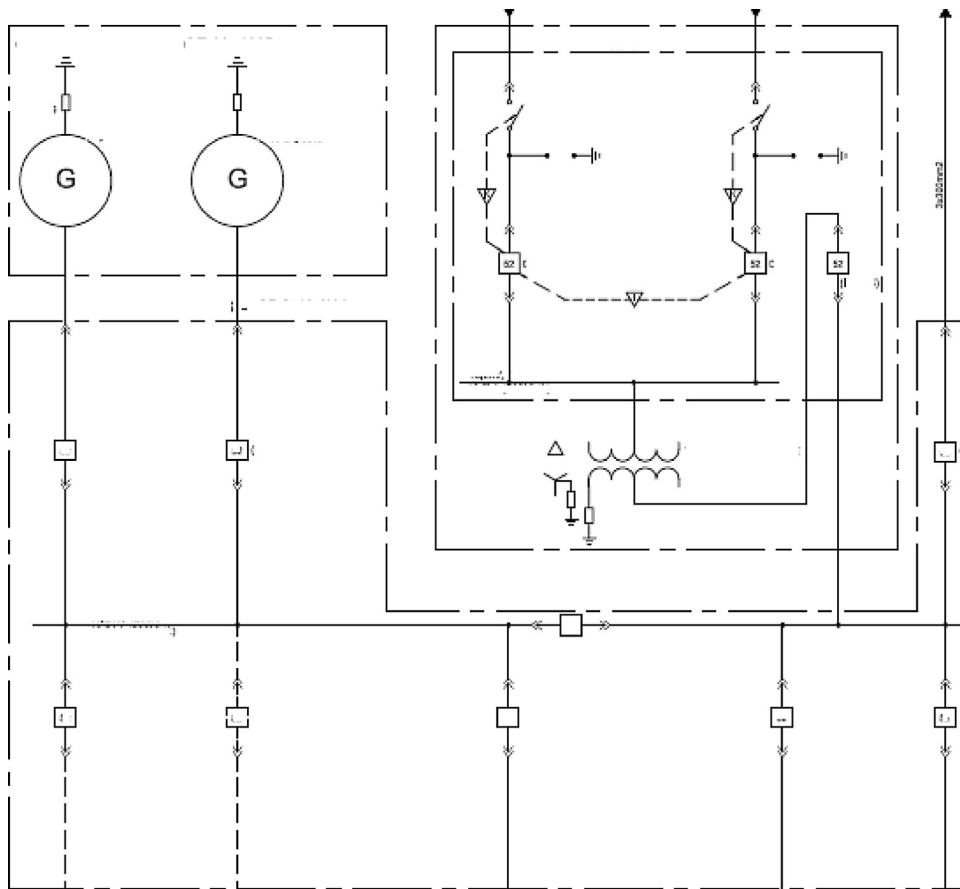
Gas and Oil Company		FMEA (Failure Mode Analysis)		Management: Project Engineer		
System: Cooling Water		Subsystem: Water Supply		Date: 16/07/2011		
Draw Number: DE-16444-56		Team: xxx				
Component	Failure Mode	Causes	Effect to System	Effect in Other Components	Detection	Recommendation
Valve	Fail total open	Diaphragm damaged	Waste of water	No	Waste of water	R001—Perform inspection periodically based on a maintenance plan. Action by: maintenance management
	Fail total closed	Human failure	Water not supplied	No	Unavailability in cooling system or other system	R002—Define a procedure to close the valve and use adequate equipment. Action by: operational management
Pumps	Seal leakage	Rotation higher than specified	Water not supplied	No	Reduced performance in cooling system or other system	R003—Follow the procedure to operate pumps inadequate rotation. Action by: operational management
	Bearing damaged	Higher vibration	Water not supplied	No	Reduced performance in cooling system or other system	R004—Follow the procedure to operate pumps inadequate rotation. Action by: operational management
	Rotor broken	Higher vibration	Water not supplied	No	Reduced performance in cooling system or other system	R005—Detect high vibration by predictive maintenance to avoid rotor damage. Action by: maintenance management
	Shaft broken	High vibration	Water not supplied	No	Reduced performance in cooling system or other system	Similar to R005
Fan (tower)	Bearing damaged	Low quality	Water temperature not cool down	No	Increase water temperature in cooling system	R006—Perform inspection periodically based in maintenance plan. Action by: maintenance management
	Chain broken	Not changed on time	Water temperature not cool down	No	Increase water temperature in cooling system	R006—Perform change of chain periodically based in maintenance plan. Action by: maintenance management
Motor (tower)	Short circuit		Water temperature not cool down	No	Increase water temperature in cooling system	No recommendation

the environment or cause harm to maintenance employees. In this case, such failures are unsafe failures and not taken into account in the FMEA. There are unsafe failures even in a water system.

### Electrical System

The following FMEA example is an electrical system comprised of a motor generator, transformers, wires, substation, and barr. Fig. 3.3 shows the system described in the FMEA with all the equipment. In such a system there are two diesel generators linked to the barr on the left. On the right there are other supply options also linked to the same barr.

Table 3.6 shows the electrical system FMEA and includes failure modes, causes, consequences, effects on the system, effects on other equipment, detection, and recommendations.



**FIGURE 3.3**

Electrical system.



### Load Movement System

In offshore drilling, the drill is a very important part of the system and as an example we will discuss the load movement system, the equipment that allows drilling movement during different phases. The load movement system is comprised of a cathead, drawwork, mast, traveling block, swivel, crown block, and easy torque. Fig. 3.4 shows the load movement system.

In Table 3.7 the load movement system is assessed by FMEA with main failures, effects, and recommendations.

The remarkable characteristic in a load movement system is the influence of human operation and maintenance. Additionally, some onshore drills have to be moved to drill another well, which causes damage to equipment.

### Diethylamine Treatment System

The following system is a diethylamine treatment system comprised of a pipeline, vases, SIF, pumps, and heat exchangers. To focus on unsafe failure, this example will consider the pipeline, vase, and reactor as the more critical equipment. Fig. 3.5 shows the most critical equipment in terms of safety, which means, in the case of unsafe failure, the consequences can be catastrophic.

Diethylamine is produced on the top of the system in the gas treatment unit, and there's an option to burn gas in the flare in the upper line. Acid water is produced on the bottom. Table 3.8 shows the FMEA of the main equipment of Fig. 3.5. The unsafe failures are also highlighted in Table 3.8.



**FIGURE 3.4**

Load movement system.

**Table 3.7 Load Movement System**

Gas and Oil Company		FMEA (Failure Mode Analysis)		Management: Project Engineer		
System: Drill		Subsystem: Load Movement		Date: 30/09/2010		
Draw Number: DE-17333-57		Team: xxx				
Component	Failure Mode	Causes	Effect to System	Effect on Equipmenor Other Components	Detection	Recommendation
Drawwork	Wearing chain	Overloading	Subsystem shutdown	Damaged in traveling block, swivel in case of a fall	Low lift load performance	R001—Perform inspection periodically based on a maintenance plan and change hook as planned. Action by: maintenance team
	Drawwork motor shutdown	Short circuit				
Mast	Corrosion or fatigue	Shock when reallocated and transported	Subsystem shutdown	Damaged in traveling block, swivel in case of a fall Accident with serious damage	Visual	
Travelling block	Corrosion or fatigue	Shock when reallocated and transported	Subsystem shutdown	Accident with serious damage in case of fall	Accident with serious damage	
Swivel	Leakage	Swivel overwork	Subsystem shutdown	No	Low lift load performance	
	Wearing	Overload and wearing during transportation	Subsystem shutdown			
Crown block	Bearing wear	Overload during operation	Subsystem shutdown	No	Low lift load performance	
Easy torq	Cylinder leakage	Human failure in operation	Subsystem shutdown	No	Low lift load performance	
Cathead	Bearing damaged Transmission chain wears	Human failure in operation	Subsystem shutdown	No	Low lift load performance	

After studying these examples, it is easy to see how the focus and recommendations of DMEA and FMEA differ. Most failure causes and recommendation in DFMEA are related to supplier material quality or components and the recommendation is to test and have procedures to check supplier quality. However, in FMEA most failure modes are related to operation conditions and product reliability and the recommendations are usually preventive maintenance and inspections. In FMEA,

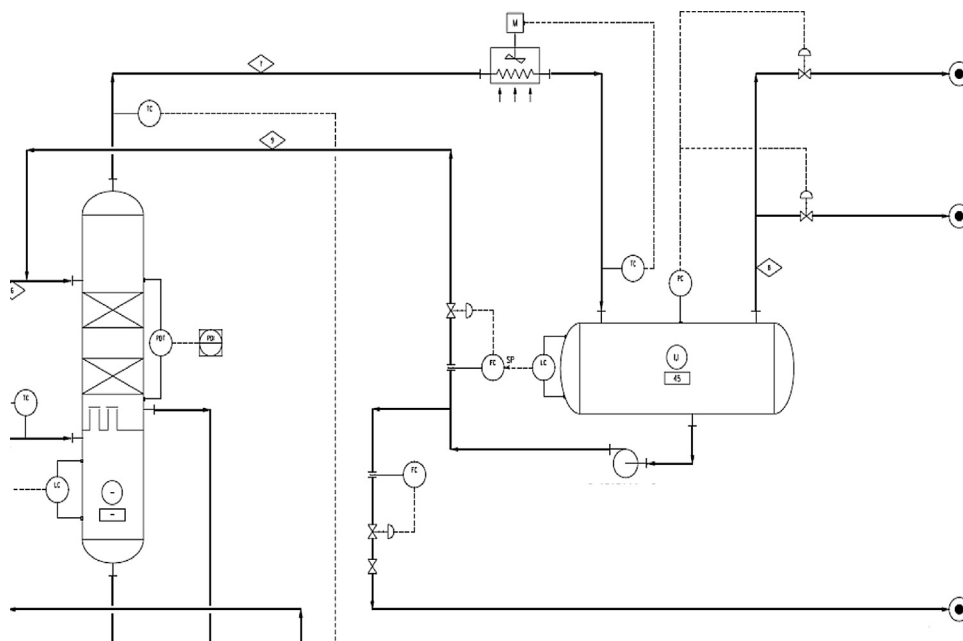


FIGURE 3.5

Diethylamine treatment system.

recommending a maintenance routine is not enough. The type of maintenance and when it should be performed is also necessary. It is better to apply RCM analysis to define the best maintenance policy qualitatively, which is discussed in the next section.

### ***Criticality Analysis to Define the Critical Equipment List***

In many cases, it is necessary to prioritize the most critical equipment in a refinery plant or on a platform to prevent critical failures and define a maintenance program. Therefore the main objective of criticality analysis is to define the critical equipment based on the worst failure consequences regarding aspects such as safety, the environment, production, and cost. Based on this, the classification system presented in Table 3.9, which ranges from 1 to 6, assesses and scores each aspect. In fact, the table can be adjusted based on different risk matrix values and procedures.

To define the equipment criticality score, the highest score will be applied concerning all aspects.

Based on criticality assessment, it will be possible to define three different criticality levels. The most critical levels are 5 and 6, the level below is between 4 and 3. Therefore, the highest numbers means that such equipments must be a priority in terms of improvement actions and implementation of assessment.

The ideal situation is to perform the FMEA and RCM for all equipment, but the reality is that most of organizations have limited resources such as money, time, and people to perform such analysis. Therefore the criticality criterion must be to prioritize the most critical items of equipment. Indeed, based on asset management methodology, which will be described in Chapter 7, reliability engineering methods must be addressed for all assets in a specific life cycle. However, during the operational



**Table 3.8 Load Movement System**

Gas and Oil Company		FMEA (Failure Mode Analysis)		Management: Project Engineer		
System: Diethylamine System		Subsystem: DEA Regenerator		Date: 30/09/2010		
Draw Number: DE-22343-58		Team: xxx				
Component	Failure Mode	Causes	Effect to System	Other Effects	Detection	Recommendation
Tube and shell heat exchanger	Tube incrustation	Bad water quality	Heat low performance		Low heat exchange performance	R001—Treat water system and keep it under specification. Action by: water facility operator
	Internal corrosion	Material out of specification	Product contamination		Low heat exchange performance	R002—Control product specification. Action by: operator
	External corrosion		Toxic product spills	Harm to employee health	Low heat exchange performance	R003—Perform preventive maintenance and change material whenever necessary. Action by: operator
DEA regenerator tower	Internal corrosion	Material out of specification	Loss of performance in tower		Process control	R004—Perform preventive maintenance and change component whenever necessary. Action by: maintenance
	External corrosion		Toxic product spills	Harm to employee health	Process control	
Pump	Seal leakage	Pump working over specified conditions	If the standby pump is not available system will shut down	Low quantity of toxic product spills with harm to employee health	Process control	R005—Perform preventive maintenance. Action by: maintenance
	Shaft wearing	Higher vibration				
Vessel	Internal corrosion	Material out of specification	Loss of performance in tower		Process control	R006—Perform preventive maintenance. Action by: maintenance
	External corrosion	Material out of specification	Toxic product spills	Harm to employee health		
Pipelines (overhead vessel)	External corrosion	Material out of specification	Toxic product spills	Harm to employee health	Process control	

**Table 3.9 Criticality Matrix**

			Aspects			
			Safety	Environment	Production	Cost
Consequences of severities	6	Catastrophic	Catastrophic injures with multiples deaths and effect on people outside	Catastrophic environmental impact without environmental recovery	More than one plant shutdown	>US\$ 500,000.00
	5	Severe	Severe injures with death, it is possible to affect people outside	Severe environmental impact with long-term environmental recovery	Plant shutdown	Between US\$100,000.00 and US\$500,000.00
	4	Critical	Critical injures, employees stay a period of time out of workplace	Critical effect on environment with medium-term environmental recovery	High production reduction (50% or higher)	Between US\$50,000.00 and US\$100,000.00
	3	Moderate	Moderate injures with first aid assistance required	Moderate effect on environment with short-term environmental recovery	Medium production reduction (between 20% and 30%)	Between US\$10,000.00 and US\$50,000.00
	2	Minor	Minor injures with minimum first aid assistance required	Minor effect on environment with fast environmental recovery	Low production reduction (lower than 20%)	Between US\$1000.00 and US\$10,000.00
	1	Insignificant	No effect	No effect	No effect	Lower than US\$ 1000.00

phases, different factors such as operation condition, maintenance, and human error can result in poorly performing equipment and it is necessary to analyze this equipment to prevent failure.

The alternative to this approach is to perform RAM Analysis, which will be described in Chapter 4, but this method requires extensive information regarding historical failure data, maintenance, and system configuration, and requires medium- or long-term investment ranging from 1 to 2 months.

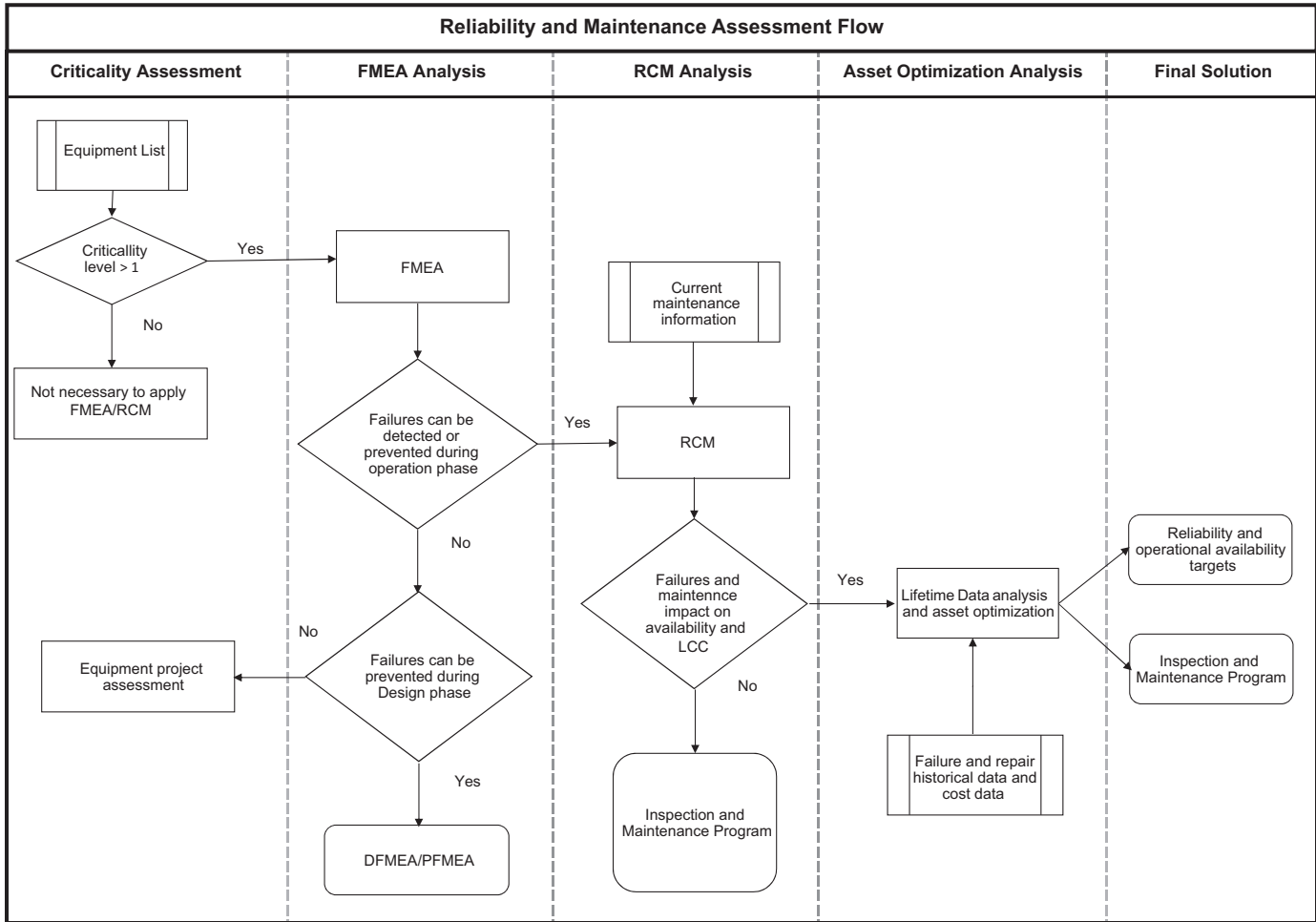
Despite this being a much better approach to defining critical equipment, in many cases low performance requires immediate action to improve critical equipment performance, and in this case it will be necessary to define the most critical equipment, perform individual analysis ,and check the positive impact on system performance.

An additional classification, called “priority rank,” groups the priority list of equipment at the same criticality level as FMEA and RCM analysis. The priority rank is a result of each aspect’s score multiplication. **Table 3.10** shows an example of criticality analysis. Based on the criticality and priority rank the items that must be assessed by FMEA and RCM are separation vessels (V-001 A and V-002 A), compressors (K-001 A and K-002 B), feed pumps (B-001 A/B), ESD valves (ESD-001 and ESD-002), cooler (E-001), and reboilers (E-003 A and E-003 B).

The general critical equipment assessment methodology is demonstrated in **Fig. 3.6**. The main objective of this analysis is to define the critical items and propose a maintenance program, including

**Table 3.10 Equipment Criticality Assessment**

Equipment Criticality Assessment								
Item	Equipment	Function	Safety	Environment	Production	Cost	Criticality Score	Priority Rank
1	E-001	Cooler (separation treatment 1)	4	2	3	2	4	48
2	E-003 A	Reboiler (separation train 1)	4	2	1	2	4	16
3	E-003 B	Reboiler (separation train 2)	4	2	1	2	4	16
4	B-001 A/B	Feed pump (feed system)	3	2	5	2	5	60
5	ESD-01	ESD valve (compression line 2)	4	3	3	2	4	72
6	ESD-02	ESD valve (compression line 1)	4	3	3	2	4	72
7	V-001 A	Separation vessel (separation line 1)	6	5	3	4	6	360
8	V-002 A	Separation vessel (separation line 1)	6	5	3	4	6	360
9	K-001 A	MP Gas compressor (compression line 1)	5	4	3	3	5	180
10	K-001 B	Export gas compression (compression line 2)	5	4	3	3	5	180



**FIGURE 3.6**

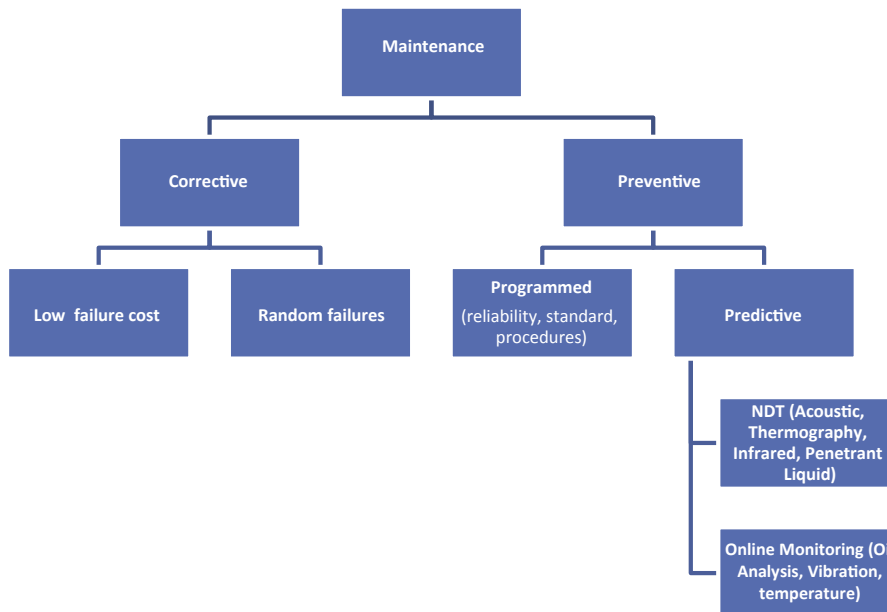
Preventive maintenance and inspection asset optimization flow.

all tasks defined during the RCM analysis. A further step is to perform lifetime data analysis and asset performance, maintenance, and spare part optimization (optional). Such additional steps are explained in Chapter 4.

## 3.2 MAINTENANCE STRATEGY

Maintenance strategy is the type of maintenance applied to assets concerning different phases of asset life cycles. In fact, asset means different physical assets such as equipment and components. In some cases it is also important to realize that maintenance will not reestablish asset operational availability and reliability or the increasing operational cost over time that is required to replace the equipment. Section 3.6 will discuss optimum replace time (ORT), which is the time needed to replace an asset based on increasing operational cost.

There are two types of maintenance: corrective and preventive. Corrective maintenance occurs after equipment fails and preventive maintenance occurs before equipment fails. The objective of performing maintenance before equipment failure is to reduce time between failures and cost. It is difficult to define the best moment to perform preventive maintenance even when there is quantitative data available such as probability density function (PDF) and failure rate function. It is also not possible to reestablish reliability in equipment such as electrical and electronic devices in which failures occur randomly. The best time to perform inspection and maintenance will be discussed in Section 3.6, where maintenance based on reliability and reliability growth will be introduced. Fig. 3.7 summarizes the maintenance strategy types.



**FIGURE 3.7**

Maintenance strategies.

Nowadays, considerable focus on preventive maintenance approaches has been given by maintenance groups to prevent equipment failure rather than allow failure to happen and then correct it. Therefore the main objective is to detect failure before it happens based on physical equipment symptoms such as excessive vibration and high temperature as well as initial degradation. The availability of different nondestructive test (NDT) technologies, which apply methods to detect failures in their early stages, has created the “potential failure phase.” In fact, when failure is detected in the potential phase, there will be more time to plan and prepare the necessary action to repair or replace such failed components, which can reduce the impact on system availability, costs and in some cases avoid accidents. Fig. 3.8 illustrates the concept of the potential—functional interval.

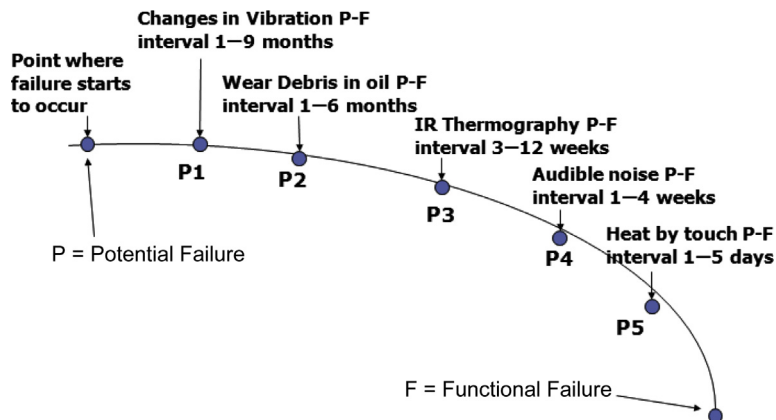
Preventive maintenance can be predictive (PdM) and programmed. Predictive maintenance is based on NDT, the main objective of which is to detection variables that predict equipment failures and help to decide when repair must be performed before failure occurs. In fact, there are different prediction methods, known as NDT and online monitoring, that can predict equipment conditions or parameters, which may influence equipment failure. The most applied NDTs are:

- Infrared
- Acoustic
- Radiography
- Penetrant liquid

In addition, monitoring methods can also be applied as predictive methods such as:

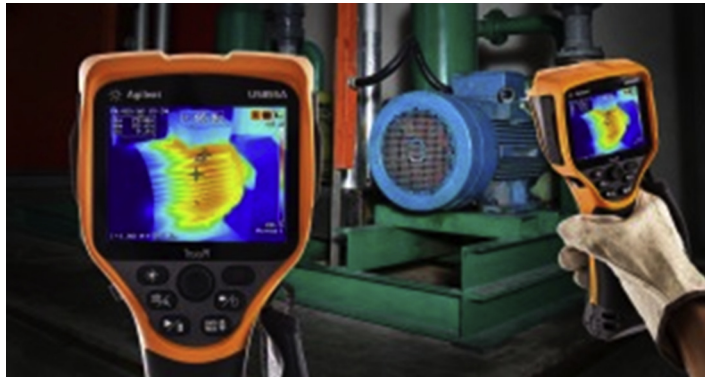
- Vibration
- Oil analysis
- Temperature

*Infrared methods* detect the emission of radiant energy in the infrared wavelength to define equipment condition. Therefore it is possible to check temperature changes. The infrared method can check conditions such as overheated bearings, spindles and motors, loose electrical power connections,



**FIGURE 3.8**

Potential—functional interval.



**FIGURE 3.9**

SDT infrared detector.

Source: <http://electronicsmaker.com/agilent-technologies-announces-new-handheld-thermal-imager-and-insulation-resistance-testers>.

steam/refrigerant leaks, insulation damage, moisture problems, roof leaks and damage, and defective steam traps. To perform infrared thermography the infrared detector is applied as shown in Fig. 3.9.

The infrared test has advantages and disadvantages such as:

Advantages:

- Measurements can be taken from a distance for hot surfaces or equipment that cannot be touched or contaminated.
- Measurements can also be taken of moving parts.
- Memory and advanced measurement functionality are available.
- It is easy to use.

Disadvantages:

- Infrared thermometers cannot take measurements of gas or liquids.
- The environment needs to be clean, without dust, high humidity, or similar.
- Specialty meters can be very expensive.

The *acoustic method* detects equipment friction and stress waves by producing distinctive sounds in the upper ultrasonic range. Therefore the modification of such waves can suggest deteriorating conditions. The acoustic method can also detect the friction and stress in the sonic range, but in this case application is limited to mechanical equipment. The detected failures by the acoustic methods are corrosion, erosion, pitting, leakage in pressurized systems, and arcing in electrical systems. Acoustic measurement is performed by using a detector, as shown in Fig. 3.10.

The acoustic test has advantages and disadvantages such as:

Advantages:

- Requires only one side accessibility.
- Capable of detecting internal defects.
- Not hazardous.



**FIGURE 3.10**

SDT ultrasound detector.

Source: <http://www.sdt.eu/index.php?page=products-unuipm-sdt270-overview>.

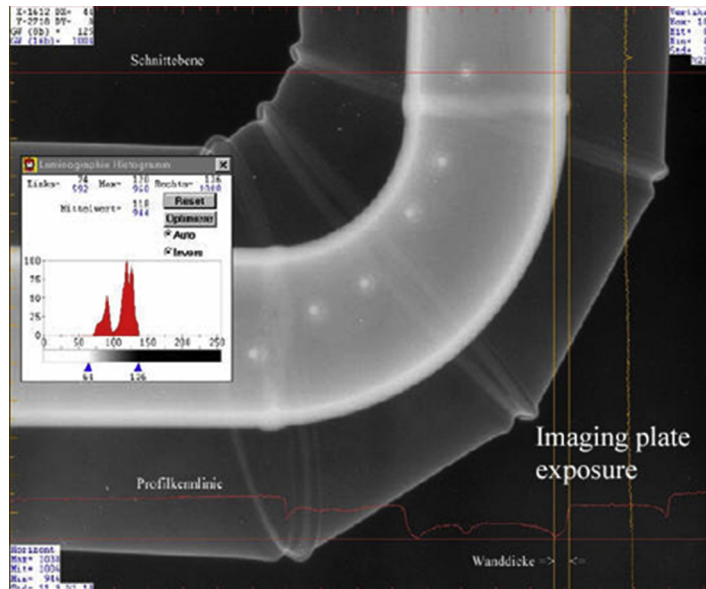
- Applicable for thickness measurement, detection of discontinuity, and determination of material properties.
- Can provide the size of the discontinuity detected.
- Very sensitive to planar type discontinuity.
- Suitable for automation.
- Equipment is mostly portable and suitable for field inspection.
- Applicable for thick materials.

Disadvantages:

- Not capable of detecting defects whose plane is parallel to the direction of the sound beam.
- Requires the use of a couplant to enhance sound transmission.
- Requires calibration blocks and reference standards.
- Requires highly skilled and experienced operators.
- Not so reliable for surface and subsurface discontinuity because of interference between initial pulse and signal caused by discontinuity.

The *radiography method* applies gamma or X radiation to examine the imperfection of equipment parts. Therefore an X-ray generator source is used as a source of radiation, which goes directly through an equipment part, resulting in a typical radiographic film. When the film is processed, a dark image will show the homogeneity of the material tested. In general, the absorption of radiation by a material depends on the effective thickness through which the radiations penetrate. Fig. 3.11 shows the result of a radiography test applied in a furnace tube.





**FIGURE 3.11**

Radiograph test result.

Source: <http://www.ndt.net/article/ecndt02/414/414.htm>.

The radiography test has advantages and disadvantages such as:

Advantages:

- Applies to almost all materials.
- Produces permanent images that are readily retrievable for future reference.
- Capable of detecting surface, subsurface, and internal discontinuities.
- Capable of exposing fabrication errors at different stages of fabrication.
- Most equipment is portable.

Disadvantages:

- Radiation used is hazardous to workers and members of the public.
- Expensive method (cost of equipment and other accessories related to radiation safety are relatively expensive).
- Incapable of detecting laminar discontinuities.
- Some equipment is bulky.
- For X-ray radiography, it needs electricity.
- Requires two-side accessibility (film side and source side).
- Results are not instantaneous. It requires film processing, interpretation, and evaluation.

The *penetrant liquid* test is a predictive method that applies a liquid to the equipment surface to detect surface discontinuity. The liquid's physical properties allow deep penetration into extremely fine cracks or pitting to demonstrate failures. This approach requires different phases such as pre-cleaning, penetrated application, removal of excess applicants, application of the developer, and postcleaning. First, the surface is cleaned, then the dye or fluorescence penetrant is applied, the excess penetrant liquid is then removed, next, the dry powder or wet developer draws penetrant out of the discontinuity, and finally, postcleaning is performed to remove the material, which can be corrosive.

Fig. 3.12 shows the penetrant test results.

The penetrant liquid test has advantages and disadvantages such as:

Advantages:

- High sensitivity to small surface discontinuities.
- Easy inspection of parts with complex shapes.
- Quick and inexpensive inspection of large areas and large volumes of parts/materials.
- Few material limitations.
- A visual representation of the flaw is indicated directly on the part's surface.
- Aerosol spray cans make the process portable, convenient, and inexpensive.
- Indications can reveal relative size, shape, and depth of the flaw.
- It is easy and requires a minimal amount of training.

Disadvantages:

- Detects flaws only open to the surface.
- Materials with porous surfaces cannot be examined using this process.
- Only clean, smooth surfaces can be inspected. (Rust, dirt, paint, oil, and grease must be removed.)
- Metal smearing from power wire brushing, shot blasting, or grit blasting must be removed prior to liquid penetrant examination.



**FIGURE 3.12**

Penetrant liquid test results.

Source: <http://www.ndt.net/article/ecndt02/414/414.htm>.

- The examiner must have direct access to the surface being examined.
- Surface finish and roughness can affect examination sensitivity. (It may be necessary to grind surfaces before penetrant liquid test (PT).)
- Multiple process steps must be performed and controlled.
- Postcleaning of parts and material is required, especially if welding is to be performed.
- Proper handling and disposal of chemicals is required.
- Fumes can be hazardous and flammable without proper ventilation.

*Vibration analysis* is applied to rotating equipment and evaluates the condition of equipment components such as bearings, shafts, and couplings to avoid failures caused by misalignment, looseness, and imbalance. Therefore a sensor is placed at different equipment points to predict the vibration waves. Depending on the amplitude and frequency of vibration waves, it is possible to identify unusual vibration conditions.

In fact, when performing vibration analysis, different approaches such as high-frequency detection and phase analysis can be applied. In the first case, low amplitude and high frequency characterize the failures in bearings based on unusual peaks, as shown [Fig. 3.13A and B](#).

The Vibration monitoring has advantages and disadvantages such as:

Advantages:

- Allows the maintenance team time to schedule the necessary repairs on damaged parts.
- Avoids failures happening under unsafe conditions.
- Reduces corrective maintenance once the component part's defects are identified and anticipated.

Disadvantages:

- Requires extensive knowledge and experience regarding vibration interpretation.
- In many cases, equipment shutdown is unnecessary, caused by wrong vibration analysis.

*Oil lubricant analysis* consists of quality degradation measurement. The techniques performed on oil samples can be classified in two categories: used oil analysis and wear particle analysis. Used oil analysis determines the condition of the lubricant itself, defines the quality of the lubricant, and checks its suitability for continued use. Used oil analysis is performed in laboratories that are equipped to run complete oil lubricant diagnostics. In some cases laboratory analyses can take up to several days or even weeks to obtain the results.

Wear particle analysis determines the mechanical condition of machines by testing the oil features. Wear particle analysis can identify parts undergoing sliding, fatigue, or creep; pieces of metal will begin to break off the components and result in wear debris in the lubricant.

There are three main wear debris monitoring techniques such as offline monitoring, wear online, and wear inline monitoring. Offline monitoring requires a sample that can be assessed either in an on-site or off-site laboratory. Wear online and inline monitoring are performed by collecting samples constantly in the oil flow. The three wear monitoring types are shown in [Fig. 3.14](#).

Oil lubricant analysis has advantages and disadvantages such as:

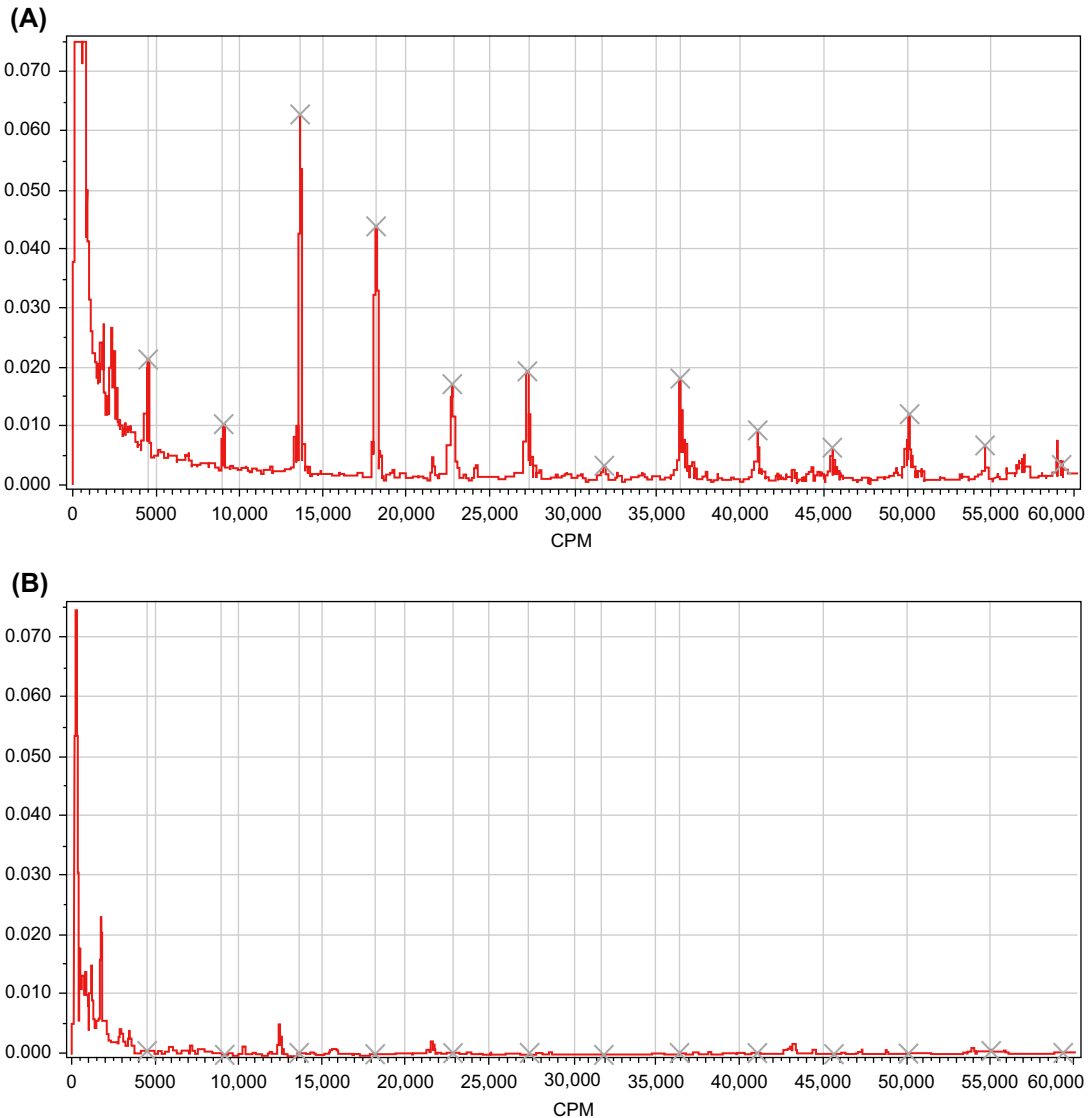
Advantages:

- Allows the maintenance team time to schedule the necessary repair on damaged parts.
- Avoid failures happening under unsafe conditions.
- Reduces corrective maintenance costs in degraded components.

Disadvantages:

- Requires a extensive knowledge and experience regarding oil analysis interpretation.
- In the case of laboratory analysis, it takes a considerable time to show the final results.

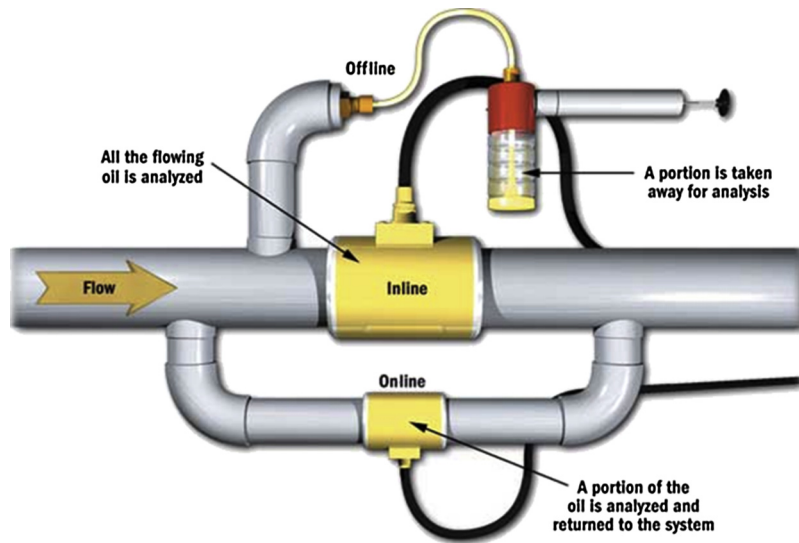
Programmed or scheduled maintenance is performed based on predictive maintenance results or in specific times based on reliability, standards, or procedures. Time in many cases is defined by



**FIGURE 3.13**

(A) Bearing vibration before repair and (B) Bearing vibration after repair.

Source: <http://www.prognost.com/casestudies>.



**FIGURE 3.14**

Oil wear online and inline monitoring.

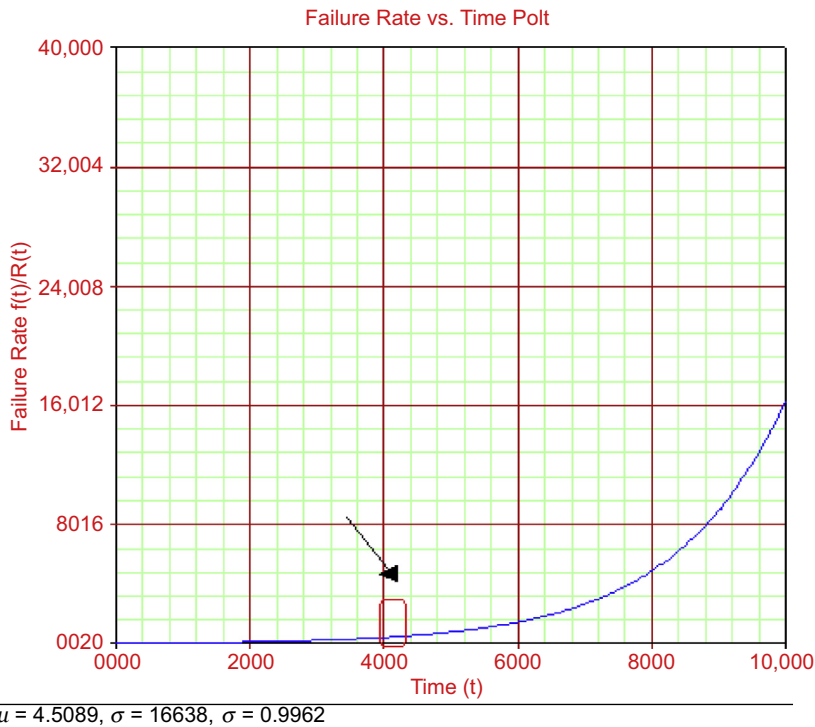
Source: <http://www.machinerylubrication.com/Read/521/in-line-wear-debris-detectors>.

equipment suppliers and regulators such as the aeronautic industry or by the experience of maintenance professionals. Whenever sufficient data is available, reliability analysis results in a prediction of time to failure. Therefore preventive maintenance can be carried out before the expected time to failure, as shown in Fig. 3.15. After defining the PDF parameter during lifetime data analysis, the failure rate function can be plotted and will show the time when the failure rate started to increase. Preventive maintenance must be performed before this time. In fact, whenever a warranty is accomplished and the equipment does not fail before the expected time, such a concept can be implemented. The problem is that many factors such as operation, maintenance, installation, and even design will influence equipment reliability performance, which can trigger a failure during the warranty period. Therefore NDT is vital because in many cases it will be possible to detect the failure and define the time to perform a preventive action. Indeed, whenever preventive action is performed, equipment reliability is reestablished at certain levels, unless in random failure occurs. The concept of the maintenance impact on reliability will be presented in Chapter 4.

Despite the preventive maintenance concept being the most modern and effective way to avoid equipment failures, critical decision factors such as consequences and frequency of failures must be taken into account to make a decision regarding maintenance strategy.

Predictive maintenance methods require investment in technology and training, which defines to which type of equipment and component such methods will be applied.

When considering a plant or a group of plants, for example, a refinery or an industrial complex, it is necessary to define the priority of equipment when using predictive methods. In fact, when considering equipment failure that does not affect the safety, environment, quality of product, or system availability, the operate to failure (OTF) approach is the best solution. Examples of OTF application are

**FIGURE 3.15**

Programmed/schedule maintenance based on reliability.

sensors, specific filters, and valves. The opposite is predictive maintenance or condition-based monitoring (CBM), which must be applied to avoid unwanted consequences such as high failure cost caused by corrective actions and downtime. The worst case is when failures result in high consequence and high frequency that cannot be detected in time to benefit from preventive action. In this case, redesign out maintenance (ROM) is a better option to perform a design assessment to avoid early failures with high consequence.

When early failures do not result in high consequence, such equipment must be assessed to find out if there is an error in installation, operation, or design. The intermediate situation is failures with medium consequence and frequency, which must be allocated a preventive programmed strategy whenever failure is predictable and the application of predictive maintenance does not have a good cost/benefit ratio.

Equipment such as vessels benefit from periodic inspection (5 years), as defined by law in many countries throughout the world. In this case, inspection must be implemented independently of the maintenance strategy. Such criteria focus on safety and not cost/benefit ratios. Indeed, many organizations take advantage of periodic inspection to perform maintenance on degraded equipment that needs preventive action.

To define the best maintenance strategy and the specific maintenance tasks to be carried out during the asset life cycle, RCM and RBI analysis are the most common methods applied. These methods will be described in the next section.

### 3.3 RCM ANALYSIS

RCM was developed first by the aeronautic during the 1960s. The main objective of RCM is to define an equipment component maintenance policy based on several criteria, including failure, cost, reliability, and safety. RCM is actually a guide to support maintenance managers in making decisions about maintenance based on planning developed during RCM analysis. Despite being good maintenance management tool, RCM must be updated with new information as needed. The technical standard SAE JA1011, *Evaluation Criteria for RCM Processes*, sets out the minimum criteria that any process should meet before starting RCM:

- What is the item supposed to do and what are its associated performance standards?
- In what ways can it fail to provide the required functions?
- What are the events that cause each failure?
- What happens when each failure occurs?
- In what way does each failure matter?
- What systematic task can be performed proactively to prevent, or to reduce to a satisfactory degree, the consequences of the failure?
- What must be done if a suitable preventive task cannot be found?

To understand what RCM proposes it is necessary to define different types of maintenance and in which situation each type of maintenance would be applied based on the maintenance strategy discussed on [Section 3.3](#).

In some cases, before performing maintenance, inspections are required to best define when or which type of maintenance must be performed on equipment. Inspections are used to check equipment conditions and if possible detect potential failures. Maintenance is used to reestablish equipment reliability or part of such reliability. Whenever possible, maintenance tries to reestablish 100% reliability, but in most cases, because of equipment wear over time or even because of human error in maintenance, that is not possible. To illustrate the RCM approach, the water supply system and load movement system and their equipment will be assessed. Equipment features and reliability parameters will be analyzed to define the type of and time to perform each equipment maintenance procedure in both systems. [Table 3.11](#) shows the water supply system RCM and part of the data provided from the FMEA ([Table 3.3](#)). It is possible to recognize that recommendation is related to the period and maintenance type. In a valve, for example, a PDF failure (closed or open) is normal and the parameters are  $\mu = 6$  and  $\sigma = 1$ . The proposed schedule maintenance is every 5 years because in 6 years there is a greater chance of failure occurring. The same idea was applied to other equipment. For pumps, in addition to preventive maintenance, a predictive NDT or visual inspection would have been carried out to check pump component conditions. In some cases, NDT is biannual but schedule maintenance is performed if necessary every 4 years (bearing) and 3 years (chain). The electrical motor has random failures, and because of that no schedule maintenance will be carried out, but it is necessary to require 1 year of 100% reliability from the supplier ( $\gamma = 1$ ). In addition, an annual infrared test will be performed to detect the component condition of the motor.

The next RCM covers the load movement system, as shown in [Table 3.12](#) based on the FMEA of [Table 3.7](#).

In the load movement system RCM analysis, the same logic used in previous example is applied, so drawwork will have preventive maintenance every 2.5 years, regarding that is necessary 6 months to carry on inspection and additional actions. In doing so, all equipment with normal or Gumbel PDFs was considered for the preventive maintenance time, the difference between average and deviation.

<b>Table 3.11 RCM (Water Supply)</b>						
<b>Gas and Oil Company</b>		<b>FMEA (Failure Mode Analysis)</b>		<b>Management: Project Engineer</b>		
<b>System: Cooling Water</b>		<b>Subsystem: Water Supply</b>		<b>Date: 16/07/2011</b>		
<b>Draw Number: DE-16444-56</b>		<b>Team: xx</b>				
<b>Component</b>	<b>Failure Mode</b>	<b>Causes</b>	<b>Effect</b>	<b>Reliability</b>	<b>Maintenance</b>	<b>Recommendation</b>
Valve	Fail total open	Diaphragm damaged	Waste of water	Normal $\mu = 6$ $\sigma = 1$	Preventive	R001—Perform preventive maintenance in 5 years. Action by: maintenance management
	Fail total closed	Human failure	Water not supplied	Normal $\mu = 6$ $\sigma = 1$	Corrective	R002—Perform corrective maintenance whenever a human error cause valve failed total closed. Action by: maintenance management
Pumps	Seal leakage	Rotation higher than specified	Water not supplied	Normal $\mu = 5$ $\sigma = 0.5$	Preventive	R003—Perform annual inspection and preventive maintenance in 4 years. Action by: maintenance management
	Bearing damaged	Higher vibration	Water not supplied	Normal $\mu = 6$ $\sigma = 1$	Preventive	R004—Monitor vibration based on sensor constantly and if necessary schedule maintenance in 5 years. Action by: maintenance management
	Rotor broken	Higher vibration	Water not supplied	Gumbel $\mu = 9$ $\sigma = 2$	Preventive	R005—Monitor vibration based on sensor constantly and preventive maintenance in 7 years if necessary. Action by: maintenance management
	Shaft broken	Higher vibration	Water not supplied	Gumbel $\mu = 8$ $\sigma = 1$	Predictive	R006—Monitor vibration based on sensor constantly and perform inspections and program schedule if necessary in 7 years. Action by: maintenance management
Fan (tower)	Bearing damaged	Low quality	Water temperature does not cool down	Normal $\mu = 6$ $\sigma = 2$	Preventive	R007— Perform biannual predictive vibration analysis and schedule maintenance in 4 years if necessary. Action by: maintenance management
	Broken chain	Not changed with time	Water temperature does not cool down	Normal $\mu = 4$ $\sigma = 1$	Preventive	R008—Perform annual inspection and preventive maintenance in 3 years. Action by: maintenance management
Motor (tower)	Short circuit		Water temperature does not cool down	Exponential MTTF = 6 $\gamma = 1$	Corrective	R009—Require 1 year of guarantee from the motor supplier. R010—Perform annual predictive infrared test Action by: maintenance management



Gas and Oil Company		RCM (Reliability centered maintenance)		Management: Project Engineer		
System: Drill		Subsystem: Load Movement		Date: 30/09/2010		
Draw Number: DE-17333-57		Team: xxx				
Component	Failure Mode	Causes	Reliability	Maintenance	Recommendation	Cost
Drawwork	Wearing chain	Overloading	Normal $\mu = 3$ $\sigma = 0.5$	Preventive	R001—Perform annual inspection and preventive maintenance in 2.5 years. Action by: maintenance management – Team A	USX.00
	Drawwork motor shutdown	Short circuit	Normal $\mu = 3$ $\sigma = 0.5$	Preventive		USX.00
Mast	Corrosion or fatigue	Shock when reallocated and transported	Gumbel $\mu = 30$ $\sigma = 2$	Preventive	R002—Perform annual predictive ultrasound test and preventive maintenance in 28 years. Action by: maintenance management – Team A	USX.00
Traveling block	Corrosion or fatigue	Shock when reallocated and transported	Normal $\mu = 1$ $\sigma = 0.5$	Preventive	R003—Perform monthly predictive ultrasound test and programmed maintenance in 6 months. Action by: maintenance management – Team B	USX.00
Swivel	Leakage	Swivel overwork	Normal $\mu = 1$ $\sigma = 0.1$	Preventive	R004—Perform monthly inspections and preventive maintenance in 6 months. Action by: maintenance management – Team A	USX.00
	Wearing	Overload and wearing during transportation	Normal $\mu = 1$ $\sigma = 0.1$			
Crown block	Bearing wear	Overload during operation	Gumbel $\mu = 24$ $\sigma = 2$	Preventive	R005—Perform annual predictive vibration analysis and scheduled maintenance in 22 years. Action by: maintenance management – Team B	USX.00
Ease torq	Cylinder leakage	Human failure in operation	Exponential MTTF = 0.5	Corrective	R005—Require high reliability from suppliers based on others easy torq. Action by: maintenance management – Team A	USX.00
Cathead	Bearing damaged Transmission chain wears	Human failure in operation	Normal $\mu = 1$ $\sigma = 0.1$	Preventive	R003—Perform monthly predictive vibration analysis and preventive maintenance in 9 months. Action by: maintenance management – Team B	USX.00

The other important difference from the first RCM analysis is that this second example defines the team responsible for apply maintenance over time as well as the estimated cost of maintenance.

In many cases, RCM analysis focuses too much on maintenance policies without making sure there will be money and people available to perform such maintenance plans.

These are very important issues to be considered in RCM analysis because in some cases there is not money enough to perform such recommendations and some modifications are needed. However, resources must be allocated prior to RCM analysis to fulfill recommendations.

The third and important step is how to update and check the RCM plan over time, and that can influence RCM recommendations. This recommendation is applied to a simple file that must be updated using suitable software. Fig. 3.16 shows an example of the water system RCM analysis applied by RCM++ software.

The screenshot shows the RCM++ software interface. The main window is titled 'Water System' and displays a 'System Hierarchy' tree. The tree structure is as follows:

- Water System
  - Valve
  - Tower
    - Bearing
    - Chain
  - Pumps
    - Seal
    - Bearing
    - Rotor
    - Shaft
  - Motor

An 'Item Reliability' dialog box is open, showing the 'Define Item Reliability' section. The 'Data Source' is set to 'Pump File'. The 'Time Dependent Life Distribution' radio button is selected. The 'Distribution and Parameters' section shows a dropdown menu set to 'Normal', with 'Mean' set to 5 and 'Std' set to 0,5.

The 'Item Properties' panel on the right shows the following details for the selected 'Seal' component:

Property Name	Value
Item Name	Seal
Reference Number	230501
Part Number	P-230501-09
Alternate Part Number	P-230401-05
Item Description	Seal pump
Remarks	leakage
Qty per System	10
Qty per Assembly	
Supplier	Workington S.A
Similar To	Flex S.A
Environmental Conditions	Tolerable
Last Updated	15/08/2011 15:54
Last Updated By	Eduardo Calixto

The 'Reliability' section shows:

- Type: Time-Dependent Distribution
- Distribution: Normal
- Parameters: Mean = 5; Std = 0,5
- Data Source: Pump File
- Last Updated: 15/08/2011 15:55
- Last Updated By: Eduardo Calixto

The 'Maintainability' section shows:

- Operating Time: 35040 Hour
- Downtime Rate: 0,00068 per Hour

FIGURE 3.16

Water system RCM (RCM++—Reliasoft).

Source: Reliasoft Corporation, RCM++ 7.0.

Fig. 3.16 shows the water system in RCM software where it is possible to work with information and develop maintenance plans and tasks easily.

Thus comparing the two alternatives, the first option, performing RCM analysis in a simple office file, has the advantage of cost because with low cost it is possible to perform RCM analysis. On the other hand, there is a risk of losing the RCM file or it may not be updated. In fact, the RCM software has the main advantage of saving different RCM plans with diverse information and links to other software; it can also receive information from other software.

---

### 3.4 RBI ANALYSIS

Inspections are usually part of an integrated integrity management strategy for managing the risk of failure. Other control measures may be included as appropriate, such as routine inspection and preventive maintenance. Inspection and maintenance functions are increasingly linked within a common framework. Although there are usually fewer high-risk items in operating plants than low-risk items, not paying attention in the inspection and maintenance of high-risk equipment may produce catastrophic results.

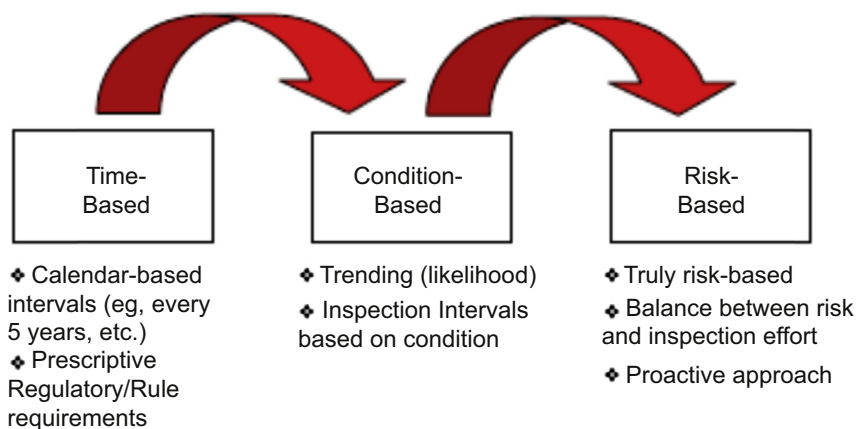
The American Petroleum Institute (API) initiated a project called Risk-Based Inspection (RBI) in 1983. As a risk methodology, RBI is used as the basis for prioritizing and managing the efforts of an inspection program (American Petroleum Institute, 2002). An RBI program allows inspection and maintenance resources to be shifted to provide a higher level of coverage to high-risk items while maintaining an adequate effort on lower-risk equipment. The main goal of RBI is to increase equipment availability while improving or maintaining the same level of risk (Sobral and Ferreira, 2010).

RBI provides a methodology for the prudent assignment of resources to assess and maintain equipment integrity based on their risk levels (Jenny, 2007).

Traditional practices, as exemplified by prescriptive rules and standard methods, lack the flexibility to respond to these demands. Risk- and reliability-based methodologies allow the development of systematic and rational methods of dealing with variations from the “standard” approach. This strategy of developing more advanced methods of maintenance and inspection follows an evolutionary continuum (Lee et al., 2006) that other industries are also following, as shown in Fig. 3.17.

Risk-based inspection involves the planning of an inspection on the basis of information obtained from a risk analysis of the equipment. The purpose of the risk analysis is to identify potential degradation mechanisms and threats to the integrity of the equipment and to assess the consequences and risks of failure. An inspection plan can then be designed to target high-risk equipment and detect potential degradation before fitness-for-service is threatened. Sometimes, the term “risk-informed inspection” is used. This was first introduced by the US Nuclear Regulatory Commission to emphasize that there is a link, although not a direct correlation, between risk and inspection. If “risk-based inspection” is understood as inspection planned on the basis of information obtained regarding risk, then the two terms are synonymous.

An inspection provides new information regarding the condition of equipment, which may be better, worse, or the same as previously estimated. However, the effect is to reduce uncertainty. New information can therefore change the estimated probability of failure. An impending failure and its consequences are not prevented or changed by risk-based inspection unless additional, mitigating actions are taken. Inspection is an initiator of actions such as the repair or replacement of deteriorating

**FIGURE 3.17**

Evolution of inspection and maintenance plan strategies.

*Source: Lee, A.K., Serratella, C., Wang, G., Basu, R.A.B.S., Spong, R., 2006. Flexible approaches to risk-based inspection of FPSOs. In: 2006 Offshore Technology Conference Held in Houston, Texas, U.S.A., May 1–4, 2006. Energo Engineering Inc. OTC 18364.*

equipment or a change in operating conditions. By identifying potential problems, risk-based inspection increases the chances that mitigating actions will be taken and thereby reduces the frequency of failure.

Depending on the particular piece of equipment, unsafe failures may occur, meaning that catastrophic consequences such as the release of stored energy and/or hazardous contents from a pressurized system could occur. Failure under such circumstances usually involves a breach of the containment boundary and the release of the contents into the environment. In extreme cases, stored energy may be released as high-pressure jets, missiles, structural collapse, or pipe whip, and the contents may be flammable and/or toxic. The Control of Major Accident Hazards (COMAH) system regulates the control of major accident hazards at installations as a whole. Such installations may include atmospheric storage tanks, process, pipeline, and other equipment containing flammable, toxic, or otherwise hazardous materials.

The probability of failure is the chance a failure event would occur in a given period of time.

The consequence of failure through the unintentional release of stored energy and hazardous material is the potential for harm. Duty holders have a responsibility to assess potential harm to the health and safety of employees and/or the public and to the environment from pollution and other causes. They may also legitimately consider the consequences of failure in their business, such as the costs of lost production, repair, and replacement of equipment and damage to the reputation of the company.

The risk of failure combines the frequency of failure with a measure of the consequences of that failure. If these are evaluated numerically, then the risk is defined as the product of the frequency and the measured consequence. Different measures of consequence can have different risks. Despite this definition, risk is often assessed qualitatively without this formal factoring. In this situation, the risk is

the combination of qualitatively assessed likelihood and consequence of failure and is often presented as an element within a likelihood–consequence matrix (Jenny, 2007). Figs. 3.18–3.20 show an example of a risk matrix, frequency, and severity rank used in RBI analysis.

- Red (dark gray in print versions) color → high risk (priority 1–5)
- Pink (gray in print versions) color → medium high risk (priority 6–12)
- Yellow (light gray in print versions) color → medium risk (priority 13–19)
- Green (darkest gray in print versions) color → low risk (priority 20–25)

The reasons to adopt a risk-based approach to the management of plants can be varied. It is generally agreed that one of the main drivers is to optimize the costs of complying with statutory obligations regarding health and safety. The main aim and benefit of RBI, when properly carried out, must always be to manage the likelihood and consequences of plant failure at an acceptable level and thereby avoid unreasonable risks of harm to people and the environment. Failures almost always have a direct or indirect effect that is harmful to the business, for example:

- Lost production
- Costs of follow-up to an incident, replacement of equipment, etc.
- Loss of any public image the user may have established within the community
- Increased insurance premiums
- Costs of legal action

		INSPECTION PRIORITY CATEGORY				
PROBABILITY CATEGORY	1	11	7	4	2	1
	2	16	13	8	6	3
	3	20	19	14	9	5
	4	23	21	18	15	10
	5	25	24	22	19	12
		E	D	C	B	A
		SEVERITY CATEGORY				

FIGURE 3.18

RBI risk matrix.

Source: Jenny (2007).

Frequency Qualification	Frequency	Ranking
Very high: failure is almost inevitable	1 in 3	1
High: repeated failures	1 in 20	2
Moderate: occasional failures	1 in 400	3
Low: relatively few failures	1 in 15,000	4
Remote: failure is unlikely	<1 in 1,500,000	5

FIGURE 3.19

Frequency rank.

Severity Level	Severity Description	Ranking
Very high	Very high severity ranking when a potential failure mode affects safe system operation without warning	A
High	Very high severity ranking when a potential failure mode affects safe system operation with warning	B
Moderate	System inoperable with destructive failure without compromising safety	C
Low	System inoperable without damage	D
Very minor	System operable with minimal interference	E

FIGURE 3.20

Severity rank.

Different consequences arise from plant failure depending on the type of risk involved. These include potential financial consequences and health and safety consequences. The RBI team should ensure that financial considerations and broader company concerns do not distort or reduce the importance of personal safety. In well-managed businesses, these are indistinguishable. The RBI team should ensure that the attention, resources, and scrutiny that the six items will receive do not compromise inspection of the two medium-risk health and safety items.

Inspection bodies have traditionally followed a prescriptive inspection philosophy. This has often been criticized for causing excessive plant downtime leading to unnecessary loss of production and operating revenue. In addition, inspection has the potential to cause the plant to return to service in a less safe condition.

For example, some equipment only suffers degradation when opened up for visual examination. In other equipment, the most onerous conditions are experienced either during start-up or shutdown. In these cases, there are strong arguments for the inspection being carried out less often or nonintrusively. Equipment is shut down not only for inspection, but also for maintenance purposes. These may be driven by a process or by energy efficiency requirements, for example, removal and replenishment of catalysts and removal of fouling in process plants. Plant operators often seek to increase the flexibility of inspection scheduling to allow plant shutdowns to be governed by maintenance needs.

An RBI example can be applied to the diethylamine system in Figs. 3.18–3.20. For each failure mode causes one specific probability rank, and for each failure mode effect one severity rank is selected. Combining probability with severity will result in risk based on the risk matrix in Fig. 3.18. The lower the number, the greater the importance of inspection to avoid unsafe failure. Risk analysis is risk policy based on risk level, and some actions are based on risk level, including:

Red (dark gray in print versions) color → high risk (priority 1–5)—intolerable = advisable to reduce risk

Pink (gray in print versions) color → medium high risk (priority 1–5)—tolerable = advisable to reduce risk if possible

Yellow (light gray in print versions) color → medium risk (priority 13–19)—tolerable = maintain risk level

Green (darkest gray in print versions) color → low risk (priority 20–25)—minor = monitor risk

RBI defines which failure is more critical, but also the lowest risk value must be prioritized during inspections to avoid failure. Fig. 3.21 shows the diethylamine system RBI.

Gas and Oil Company		RBI (Risk based Inspection)			Management: Project Engineer		
System: Deethanamine System		Subsystem: DEA Regenerator			Date: 30/09/2010		
Draw Number: DE-22343-58		Team: xxx					
Component	Failure Mode	Causes	F	Effect to System	S	R	Recommendation
Tube and shell heat exchanger	Tube incrustation	Bad water quality	3	Heat low performance	E	20	R001—Treat water system and keep it under specification. Action by: water facility operator
	Internal corrosion	Material out of specification	4	Product Contamination	C	18	R002—Control product specification. To perform NDT (ultrasound test) every 5 years Action by: operator
	External corrosion		4	Toxic product spill Damage to employee health	B	16	R003—Perform annual inspection and schedule maintenance each 5 years and change material whenever is necessary: Action by: operator
DEA regenerator Tower	Internal corrosion	Material out of specification	5	Loss of performance in Tower	D	24	R004—To perform NDT - ultrasound test and infrared test every 2 years and schedule maintenance every 5 years Action by: maintenance
	External corrosion		5	Toxic product spills Damage to employee health	B	24	
Vessel	Internal corrosion	Material out of specification	5	Loss of performance in Tower	C	22	R006—To perform NDT - ultrasound test every 2 years and schedule maintenance every 5 years Action by: maintenance
	External corrosion	Material out of specification	5	Toxic product spills Damage to employee health	A	12	R006—Perform inspection and preventive maintenance Action by: maintenance
Pipelines (overhead vessel)	External corrosion	Material out of specification	5	Toxic product spills Damage to employee health	A	12	R006—To perform NDT - ultrasound test and radiography test every 2 years and schedule maintenance every 5 years Action by: maintenance

**FIGURE 3.21**

Diethylamine system RBI.

As Fig. 3.21 shows, RBI is mainly applied to static equipment but this is not always so.

To perform the RBI it is necessary for the number of people on the team and its composition to vary depending on the complexity of the installation (three might be a minimum), but the team should be able to demonstrate adequate technical knowledge and experience in the following areas:

- Risk assessment
- Production process hazards and the consequences of failure
- Plant safety and integrity management
- Mechanical engineering, including materials chemistry and plant design
- Plant-specific operation, maintenance, and inspection history
- Inspection methods and the effectiveness of Non Destructive Examination (NDE) techniques and procedures

Team members should have a breadth of knowledge and experience from working at other plants and sites. Sometimes, particular specialists (eg, corrosion chemists, dispersion analysts, and statisticians) may need to be consulted. Because there are significant health and safety implications arising from equipment failure, the qualifications and competence of the individuals in the team need to be of a professionally recognized level.

After performing an analysis it is necessary to implement recommendations. Thus RBI teams need to have leaders who have the authority to manage their teams and the responsibility of ensuring that appropriate RBI plans are developed. For pressure systems and other regulated equipment, a designated competent person will normally be included in the team to fulfill statutory responsibilities.

The trend toward a risk-based approach is being supported by extensive plant operating experience, improved understanding of material degradation mechanisms, and the availability of fitness-for-service assessment procedures.

The industry is recognizing that benefits may be gained from more informed inspections. Certain sectors of industry, particularly the refining and petrochemicals sectors, are now setting inspection priorities on the basis of the specific risk of failure. Improved targeting and timing of inspection offers industry the potential benefits of:

- Improved management of health and safety and other risks of plant failure.
- Timely identification and repair or replacement of deteriorating equipment.
- Cost savings by eliminating ineffective inspections, extending inspection intervals, and greater plant availability.

To achieve such results, the RBI must be performed at the correct time, and this is one of the vulnerabilities of this methodology, because in most cases inspection time is defined qualitatively. To support such a methodology, the three methods of inspection based on PDF reliability, and reliability growth will be discussed using examples from drilling facility systems.

Despite being a good approach, the RBI defines probability qualitatively and depends on team opinion. In some cases the team will manipulate the numbers to prioritize what is more important in terms of inspection. A solution to this problem is to calculate probability or inspection time quantitatively as is proposed by the ReBI (reliability-based inspection) and RGI (reliability growth-based inspection) methods, as discussed in the next two sections.



### 3.5 ReBI ANALYSIS (RELIABILITY BASED INSPECTION)

The previous approaches mostly considered probability of failure qualitatively. Even when PDF failure is taken into account, equipment degradation over time is not considered, and the same inspection or maintenance period of time (interval) is established. In fact, in these cases, the second, third, and following inspections and maintenance will be in the same time interval, and as equipment degrades over time, the chance of equipment failure before inspection or maintenance also increases. This affects system availability. Thus to avoid impact on system availability targets it is necessary to conduct maintenance and inspection before failures occur. This requires setting inspection time, based on reliability targets or probability of failure targets.

The ideal situation is that the reliability level remains approximately the same between two inspections (Sobral and Ferreira, 2010). In this case, equation 1 represents the reliability at a given time after the first inspection.

Equation 1

$$\begin{aligned} R(t + \Delta t) &= R(t) \\ R(t + \Delta t) &= R(t^n) \end{aligned}$$

where  $n$ , inspection time period;  $R(t)$ , reliability on time  $t$ ; and  $R(t + \Delta t)$ , reliability on time  $t + \Delta t$ .

Depending on the PDF, different equations are used to define inspection based on the reliability level and time  $t$ . For example, equation 2 uses the Weibull PDF.

Equation 2

$$\begin{aligned} R(t^n) &= e^{-\left(\frac{t^n}{\eta}\right)^\beta} \\ \ln(R(t^n)) &= \ln\left(e^{-\left(\frac{t^n}{\eta}\right)^\beta}\right) \\ \ln(R(t^n)) &= -\left(\frac{t^n}{\eta}\right)^\beta \\ \ln(R(t^n)) &= -\left(\frac{(t^n)^\beta}{\eta^\beta}\right) \\ (t^n)^\beta &= -\eta^\beta (\ln R(t^n)) \\ t^n &= \left[-\eta^\beta (\ln R(t^n))\right]^{\frac{1}{\beta}} \\ t^n &= -\eta (\ln R(t^n))^{\frac{1}{\beta}} \end{aligned}$$

An illustration of the application of equation (2) is shown in Table 3.13, an example of a crown block from a drilling system using the Weibull PDF (parameters:  $\beta = 3.97$  and  $\eta = 1.22$ ) with failure time, reliability, probability of failure, inspection sequence, inspection period, and inspection intervals.

In the first column, the failure time is given; in the second column the reliability over time; in the third column the probability of failure; and in the fourth the inspection sequence. In the fifth column,

Failure Time	Reliability (%)	Probability of Failure (%)	Inspection	Inspection Time (year)	Inspection Moment (year)
$t$	$R(t)$	$F(t)$	$n$	$T_n$	$T_n - T_{n-1}$
0.77	84	16	1	0.78	0.78
1.07	61	39	2	1.02	0.23
1.22	39	61	3	1.20	0.18
1.4	16	84	4	1.42	0.22

the maximum time during which inspection based on reliability must be done is given, which is associated with failure time and reliability. Thus a first inspection must be done in 0.78 years (9.4 months), the second one must be done in 1.02 years and must be following the third (1.2 years) and fourth (1.4 years) until the maintenance team defines the preventive maintenance.

However, it is possible to state a reliability target to perform inspections, for example, 61%, and in doing so before 1.02 years an inspection will be performed, which will define if it is necessary to perform preventive maintenance. Another option is to define inspection (or preventive maintenance) based on failure time and in this case inspection periods will be carried out over time as defined in column 5 until preventive maintenance is performed.

The third column where the stated probability of failure would be used as input for RBI analysis, and depending on time assessed, there will be different risks that influence inspection plans.

In some cases we have a Weibull 3P (Weibull PDF with three parameters, which means including a position parameter) and it is necessary to apply equation 3.

Equation 3

$$R(t^n) = e^{-\left(\frac{t^n - \gamma}{\eta}\right)^\beta}$$

$$\ln(R(t^n)) = \ln\left(e^{-\left(\frac{t^n - \gamma}{\eta}\right)^\beta}\right)$$

$$\ln(R(t^n)) = -\left(\frac{t^n - \gamma}{\eta}\right)^\beta$$

$$t^n - \gamma = \varphi$$

$$\ln(R(t^n)) = -\left(\frac{\varphi}{\eta}\right)^\beta$$

$$\varphi^\beta = \eta^\beta(-\ln(R(t^n)))$$

$$\varphi = [\eta^\beta(-\ln(R(t^n)))]^{\frac{1}{\beta}}$$

$$\varphi = \eta[(-\ln(R(t^n)))]^{\frac{1}{\beta}}$$

$$t^n - \gamma = \varphi$$

$$t^n - \gamma = \eta[(-\ln(R(t^n)))]^{\frac{1}{\beta}}$$

$$t^n = \eta[(-\ln(R(t^n)))]^{\frac{1}{\beta}} + \gamma$$

Failure Time	Reliability (%)	Probability of Failure (%)	Inspection	Inspection Time (year)	Inspection Moment (year)
$t$	$R(t)$	$F(t)$	$n$	$T_n$	$T_n - T_{n-1}$
1.07	93	8	1	0.73	0.735
1.22	82	18	2	1.26	0.522
1.4	72	28	3	1.78	0.518
1.63	61	39	4	2.37	0.598
3.12	49	51	5	3.06	0.691
3.8	39	61	6	3.80	0.736
5.34	29	72	7	4.79	0.988
7.39	18	82	8	6.12	1.331
7.4	7	93	9	8.59	2.472

An example of Weibull 3P is a diesel motor of a drilling system with PDF parameters:  $\beta = 1.18$ ,  $\eta = 3.70$ , and  $\gamma = 0.30$ . Applying equation 3 results in the inspection time given in Table 3.14.

Similar to the previous example, the failure time is given in the first column; in the second column the reliability over time; in the third column the probability of failure; in the fourth the inspection sequence; and in the fifth the inspection period, which is associated with failure time and reliability. In the sixth column the inspection interval is given. Thus a first inspection must be made before 0.73 years, the second before 1.26 years, and further as stated in the fifth column in Table 3.14. In some cases, inspection time is higher than failure time, but this is only an estimate. It is expected that inspection time is less than failure time but when this is not possible failure time can be used as inspection time.

In Weibull PDF distribution, depending on the  $\beta$  value, the inspection interval has a tendency to remain constant, increase, or decrease. In the first example (crown block) with  $\beta = 3.7$  (wear-out phase— $\beta > 2.5$ ), the inspection time interval (sixth column) decreases over time. This means that equipment is in a wear-out phase (bathtub curve) and failure rate increases over time. This means inspection is required in a shorter period of time.

In the second example, the diesel motor has an early life characteristic (bathtub curve) with  $\beta = 1.18$ . In this case the inspection time interval tendency increases over time as shown in the sixth column in Table 3.14. In this case, failure rates decrease over time. This means inspection is required after a longer period of time. The inspection time can be defined by other PDFs, and in this case it is necessary to define an equation based on reliability time. In general, PDFs with early life phase characteristics (lognormal) will have inspection time intervals increasing over time. The PDFs with useful life characteristics (exponential) will have inspection time intervals constant over time, and PDFs with wear-out phase life characteristics (normal, logistic, Gumbel) will have inspection time intervals decreasing over time.

Despite a good methodology for defining inspection time, the values based on reliability do not take into account reliability degradation after maintenance. In these cases, the same inspection time values will be used unless a new PDF substitutes the previous one.

The next section will discuss inspection based on reliability growth, and in this case reliability degradation effects will be considered over time.

### 3.6 ReGBI ANALYSIS (RELIABILITY GROWTH BASED INSPECTION)

The reliability growth approach is applied to product development and supports decisions for achieving reliability targets after improvements have been implemented (Crow, 2008).

Various mathematical models may be applied in reliability growth analysis depending on how the test is carried out, as stated in Chapter 2. The mathematical models include:

- Duane
- Crow-AMSAA
- Crow extended
- Lloyd–Lipow
- Gompertz
- Logistic
- Power law

The ReGBI method uses power law analysis methodology to assess repairable systems that are also applied to estimate future inspections. The expected cumulative number of failures is mathematically represented by equation 1:

Equation 1

$$E(N_i) = \int_0^T \rho(t) dt$$

The expected cumulative number of failures can also be described by equation 2:

Equation 2

$$E(N(t)) = \lambda T^\beta$$

To determine the inspection time, it is necessary to use the cumulative number of failures function and, based on equipment failure data, to define the following accumulative failure number. Based on this number, it is necessary to reduce the time to inspection and maintenance to anticipate corrective maintenance.

Applying such methodology to the drilling diesel motor it is possible to predict when the next failure will occur, and based on such prediction, to define inspection time. The cumulative number of failures is 10. Therefore substituting the expected cumulative number of failures and using the power law function parameters ( $\lambda = 1.15$  and  $\beta = 1.02$ ) in equation 3, the next failure is expected to occur in 8.32 years, as shown in equation 1.

Equation 3

$$E(N(t)) = \lambda T^\beta$$

$$T = \left( \frac{E(N(t))}{\lambda} \right)^{\frac{1}{\beta}}$$

$$T = \left( \frac{10}{1.15} \right)^{\frac{1}{1.02}} = 8.32$$

The same approach is used to define the following failure using equation 4, in which 11 is used as the expected accumulated number of failures.

Equation 4

$$E(N(t)) = \lambda T^\beta$$

$$T = \left( \frac{E(N(t))}{\lambda} \right)^{\frac{1}{\beta}}$$

$$T = \left( \frac{11}{1.15} \right)^{\frac{1}{1.02}} = 9.15$$

In equation 5, the expected number of failures used is 12, so the expected time to failure will be:  
Equation 5

$$E(N(t)) = \lambda T^\beta$$

$$T = \left( \frac{E(N(t))}{\lambda} \right)^{\frac{1}{\beta}}$$

$$T = \left( \frac{12}{1.15} \right)^{\frac{1}{1.02}} = 9.96$$

After defining the expected time of the next failures, it is possible to define the appropriate inspection periods of time. If we consider 1 month (0.083 years) as an adequate time to perform inspection, the following inspection time after the ninth, tenth, and eleventh expected failure will be:

- First inspection: 8.23 years (8.32–0.083)
- Second inspection: 9.07 years (9.15–0.083)
- Third inspection: 9.87 years (8.32–0.083)

The remarkable point is in regard to reliability growth and previewing the following failures over time, whereas the other model makes inspection decisions assuming that PDF failure will be similar to the previous analysis. In the ReGBI method, whenever new failures occur, it is possible to update the model and get more accurate values of the cumulative expected number of failures.

An example of cumulative failure plotted against time for a diesel motor is presented in [Fig. 3.22](#), using the cumulative failure function parameters  $\beta = 1.02$  and  $\lambda = 1.15$ . Based on such analysis, it is possible to observe that the next failures (failures 10th, 11th, and 12th) will occur after 8.32, 9.15, and 9.96 years, respectively.

Despite its simple application, ReGBI analysis first requires power law parameters and then to calculate expected cumulative number of failures. As discussed in Chapter 2, such parameters can be estimated by applying the maximum likelihood method, but this method requires time, and the higher the number of failure, the more complex they are to calculate. When possible it is advisable to use software to directly plot the expected number of failures graphs. In this case, it is possible to update historical data with new data and plot expected future failures directly.

The next section discusses ORT (optimum replacement time). Actually, even applying the best practice to assess failure and anticipate it with inspections and maintenance when equipment achieves

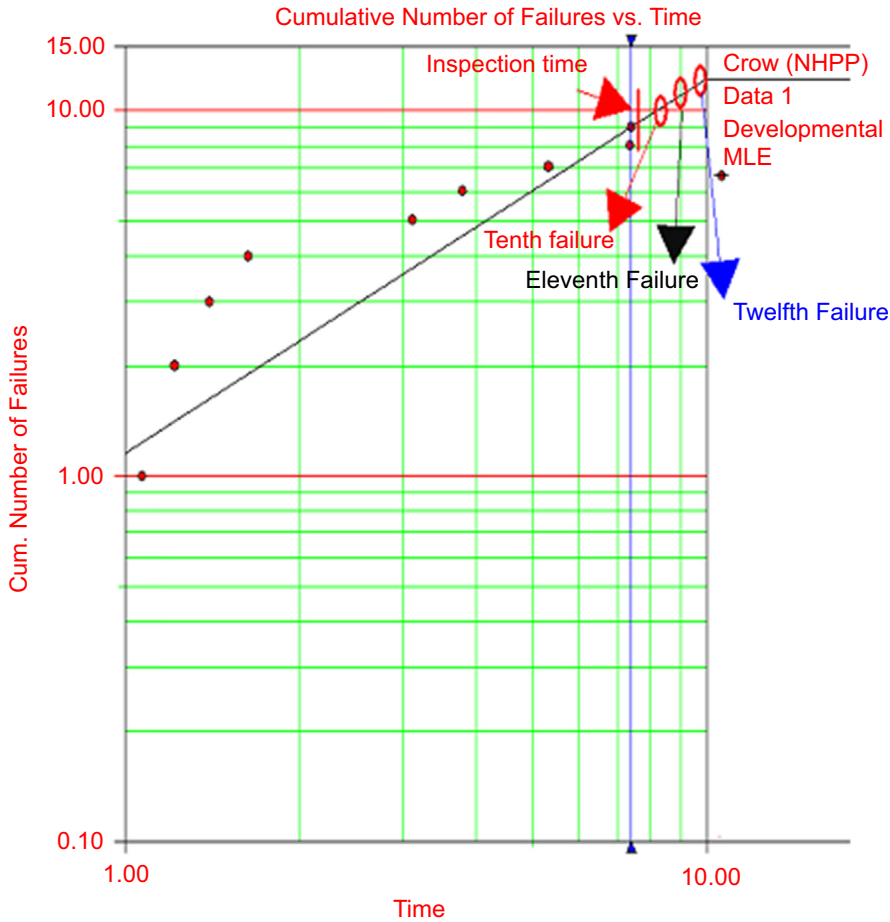


FIGURE 3.22

Inspection based on reliability growth (ReGBI).

wear-out, a very important question still arises: “Is the best decision to overhaul the equipment or replace it?”

To answer this question, operational costs must be considered, the topic of the next section.

### 3.7 OPTIMUM REPLACEMENT TIME ANALYSIS

One of the most important decisions for reliability engineers and maintenance professionals to make is the *best time to replace equipment*, which requires life cycle analysis as well as operational cost analysis. The operational costs include all direct and indirect costs needed to keep equipment working properly, such as inspections, maintenance, stocking components, energy, and human hours. So for operational costs over time it is possible to define the optimum time when operational costs per time

achieve the minimum value and then start to increase (Jardine, 2006). The generic operational cost function over time is defined in equation 1.

Equation 1

$$C(t_r) = \frac{\int_0^{t_r} C(t)dt + c_r}{t_r + T_r}$$

where  $C(t)$ , total operational cost;  $C(t_r)$ , operational cost of time;  $c_r$ , residual cost;  $T_r$ , optimum replacement time; and  $t_r$ , operational time.

The residual cost is related to the cost of not replacing equipment in optimum time, and assuming that equipment will be replaced at optimum time, equation 1 can be simplified by equation 2.

Equation 2

$$C(t_r) = \frac{\int_0^{t_r} C(t)dt}{t_r}$$

The optimum replacement time is defined when the partial derivative of operational cost per time is equal to zero, as shown in equation 3.

Equation 3

$$\frac{\partial'' C(t_r)}{\partial t_r} = 0$$

The operational cost function can be described by acquisition cost, which is a constant value, and operational cost, which varies over time, as shown in equation 4. In some cases and when equipment is in the wear-out phase, the maintenance cost is the most relevant cost, because equation 4 regards operational cost equal to maintenance cost.

Equation 4

$$C(t_r) = C(Acq) + \int_0^{t_r} Ce(M_t)$$

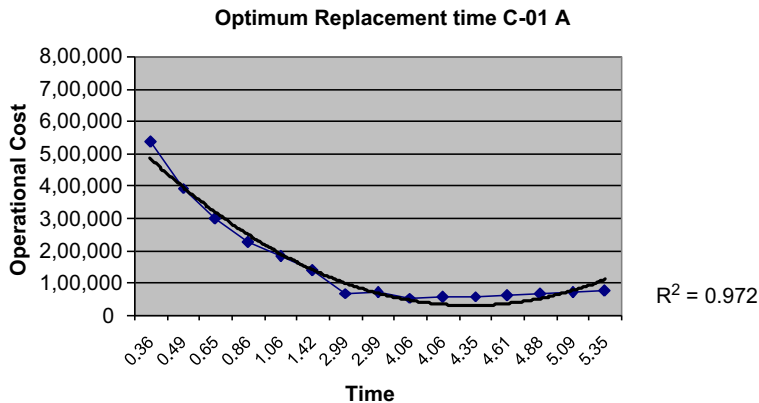
where  $Ce(M_t) = (1 - R(t)) \times C(M_t) = F(t) \times C(M_t)$ ;  $Ce(M_t)$ , maintenance cost expected on time  $t$ ;  $C(M_t)$ , maintenance cost of time  $t$ ;  $R(t)$ , reliability on time  $t$ ;  $F(t) = (1 - R(t))$ , probability of failure on time  $t$ ; and  $C(Aq)$ , acquisition cost.

An example of ORT methodology is a compressor that operates in a refinery plant over 20 years (Calixto and Michael, 2011). The acquisition cost is \$10,000,000.00. After operating for 20 years and after many corrective and preventive maintenance actions and an overhauling of the compressor after 5 years, the compressor had some failures, as shown in Table 3.15. The question arises: What is better: replace the equipment or perform maintenance over 5 years?

In the first column of Table 3.15 is the stated failure time, in second column the failure probability; in third column the maintenance cost; in the fourth column the expected maintenance cost resulting from multiplying the values from the second and third columns. In the fifth column the accumulated maintenance cost is given, and in the sixth the operational costs, which consider per time the annual acquisition costs and accumulated maintenance costs. Plotting operational costs per time as shown in Fig. 3.23, it is possible to see that the optimum replacement time is 4.06 years. After this time, operational costs increase over time.

**Table 3.15 Compressor Operational Cost on Time**

Failure Time C-01 A	Failure Probability	Maintenance Cost	Expected Maintenance Cost	Accumulated Cost	Operational Cost per Time
0.36	0.092367559	370	34.17599701	34.17599701	534,284
0.49	0.104214914	840	87.5405275	121.7165245	392,714
0.65	0.120260768	2012	241.9646662	363.6811907	296,418
0.86	0.143855177	2531	364.097452	727.7786427	224,460
1.06	0.16905792	2738	462.8805859	1190.659229	182,546
1.42	0.221118538	5195	1148.710807	2339.370036	137,076
2.99	0.523083762	10,362	5420.193945	7759.56398	66,912
2.99	0.523083762	11,042	5775.890903	13,535.45488	68,844
4.06	0.732717503	13,643	9996.464891	23,531.91977	53,163
4.06	0.732717503	14,783	10,831.76284	34,363.68262	55,830
4.35	0.78044122	29,104	22,713.96127	57,077.64389	57,330
4.61	0.818727495	37,129	30,398.53316	87,476.17706	60,691
4.88	0.853745061	37,129	31,698.70037	119,174.8774	63,828
5.09	0.877617277	43,083	37,810.38514	156,985.2626	68,623
5.35	0.903199515	52,112	47,067.53315	204,052.7957	74,086

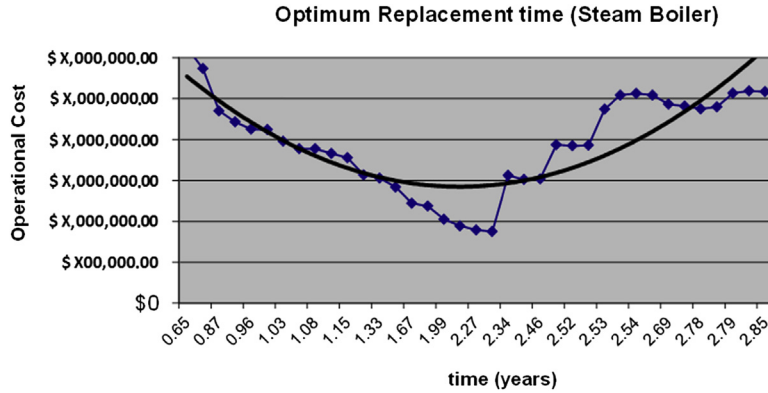


**FIGURE 3.23**

Optimum replacement time.

In fact, after overhauling, the equipment is considered as good as new. If compressor reliability is not as good as new and failures are worse than expected, the optimum replace point will be earlier than expected (4.06 years). In doing so, because the compressor is operating for 5 years until preventive maintenance, the decision is to replace the compressor at 4.06 years.



**FIGURE 3.24**

Boiler optimum replacement time.

It is possible to predict future failures using the power law model and replace the failure time in Table 3.15 in column 1. Such a method is more accurate for predicting future failures and timing inspections, but the best time to replace the compressor will be estimated and operational costs also have to be considered.

An additional example is a boiler that after an overhaul demonstrates increasing failure rate and operational costs. Because such a boiler operates for more than 20 years without a proper preventive maintenance policy, the components degrade faster than usual. In this particular case, there is a standby boiler and therefore there is no impact on boiler system operational availability. Nonetheless, based on increasing operational costs, as shown in Fig. 3.24, the boiler must be replaced.

### 3.8 FRACAS ANALYSIS

The failure report analysis and corrective action system (FRACAS) has the main objective of supporting the asset manager's decisions and assesses equipment performance based on a failure report, which provides the background for lifetime data analysis, reliability growth analysis, as well as implementing corrective actions.

The FRACAS methodology must be defined during the design phase based on FMEA and RCM analysis, and also based on the vendors' performance contract or warranty contract.

In the first case, the DFMEA, PFMEA, and SFMEA will provide the baseline to identify each component failure mode and causes to create a codification for the failure report. In addition, the root cause analysis linked to the failure report will clarify if the recommendations defined during the FMEA to avoid failures were implemented or not.

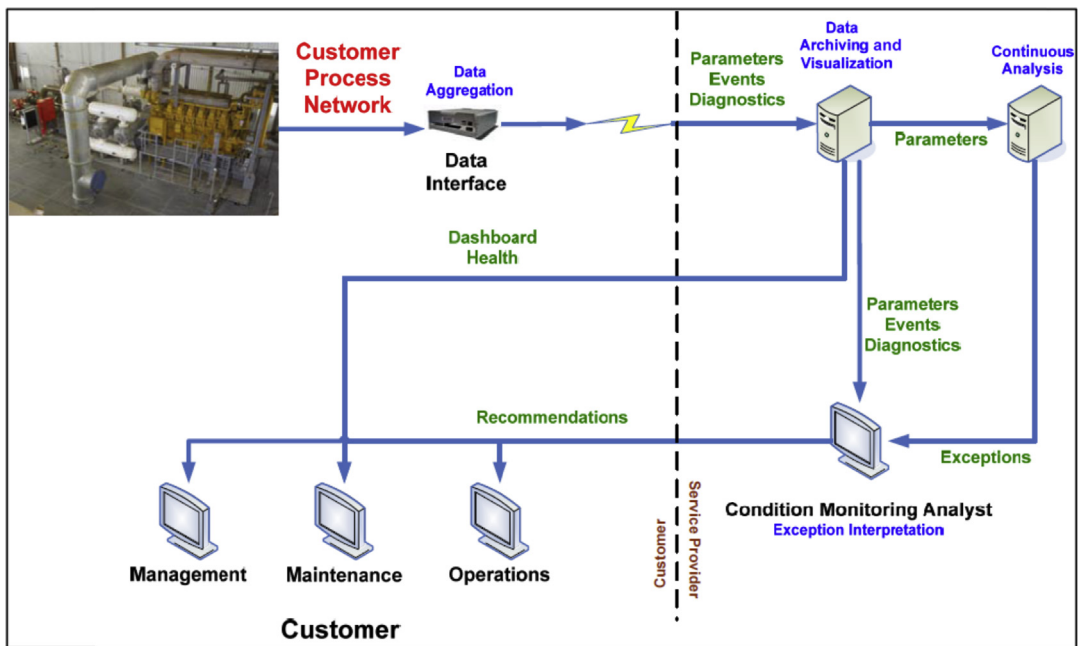
The failure report, which is a FRACAS module, provides information to the historical failure data based on component failure modes and cause codes. Such information will be stored in a database such as a System Application Product (SAP) software. Therefore such information can be exported from FRACAS to an Excel sheet and imported into lifetime data analysis software such as the CAFDE, as demonstrated in Chapter 1. Lifetime data analysis is a method that provides a background check if the warranty reliability index is not achieved.

RCM and RBI are also important to identify which type of maintenance and inspection is performed for each piece of equipment and components and to check the effectiveness of such tasks to prevent failures. In fact, the type of predictive monitoring and NDT must be defined in the warranty contract to establish the method of detecting the failure during the warranty time.

Vendor equipment performance, which must be defined in the warranty contract, is the most important piece of information for the FRACAS, because it is a criterion to analyze the vendors' equipment performance. Therefore for all failures, storage on the FRACAS database will then be input to lifetime data analysis to assess vendor performance based on the warranty contract.

In fact, in many cases, if vendors' equipment performs poorly, the root cause may not be associated with faulty design, but error during installation, operation, and maintenance, or even sabotage. Therefore root cause analysis is a very important assessment when a failure occurs during the warranty period.

Unfortunately, root cause analysis also has limitations and in many cases these are not conclusive. As a result, many vendors decided to monitor their assets during the warranty period to gather evidence regarding their assets' performance and the possible cause of failures, as shown in Fig. 3.25.



**FIGURE 3.25**  
Data monitoring.

Source: Mark, W., Russel, W.B., David, K., 2012. Utilizing Equipment Data for proactive asset management. In: Gas Machinery Conference, Austin, Texas.

In general terms, the FRACAS must achieve three main objectives:

1. To supply and create an effective failure report database of equipment and components including the failures and causes based on specific codes and standards.
2. To create a platform to perform a root cause analysis for each equipment failure, which must be easy to access and use on a daily basis.
3. To create a baseline to monitor the equipment reliability performance index to support asset managers' decisions.

In the first case, the failure database is created based on FMEA analysis. [Table 3.16](#) shows an example of the type of information that is implemented on FRACAS to store failures. Therefore whenever a failure happens, the analyst who input the information on the FRACAS system needs to identify which code must be applied.

In the second case, for each failure reported on FRACAS, a root cause analysis must be carried out using fault tree analysis. A fault tree analysis diagram identifies different combinations of failures or causes that can trigger one failure. In fact, in many cases this is only the first step because further laboratory tests are needed to prove that it was a material failure or that the material is out of specification based on a sample of the real equipment. [Fig. 3.26](#) shows fault tree analysis applied to root cause analysis.

One of the most important rules in fault tree analyses is not to repeat events. In [Fig. 3.26](#), despite the root causes such as RC1 applied to different gates, each RC1 frequency that leads to different failure modes will have different frequencies. Therefore despite a similar code, the RC1 applied to different failure modes have different events.

The advantages of fault tree analysis applied to root cause analysis are easy visualization and the important information stored in a FRACAS database to support future root cause analysis.

In many cases it is necessary to perform laboratory tests to confirm the root cause such as material quality, wrong material specification, operation conditions, and robustness. Such laboratory tests are carried out mainly by independent organizations because it is necessary to demonstrate if the failures are caused by the company or the supplier.

In root cause analysis, failure evidence is very important. Therefore the failure mode investigation that provides the operation conditions, design specification, procedures, and training list is very important in understanding and defining the root cause of the failure. The “5 Why Test” may also be applied to confirm the final decision. The FRACAS system may also have the “5 Why Test,” which also supports future analysis. [Fig. 3.27](#) shows an example of the “5 Why Test” applied to bearing wear (FM1) caused by overload (RC2).

The second part of FRACAS analysis is the important corrective actions system, which ensures that such failures do not occur in the future. The corrective actions system must support the managers by following up the corrective action implementation and also managing the teams and budget to implement such actions. Thus it is very important that the corrective actions system has the equipment and component identification and also the failure modes, root cause, and consequences to clarify and reinforce such corrective actions. The action plan is also part of this module, which includes “Who,” “When,” “Frequency,” “How Much,” and “Status.” The corrective implementation status must connect the FRACAS with other managers' information systems such as SAP and Lotus Note, for example. [Fig. 3.28](#) shows the corrective actions system, which supports managers when following up recommendations.

**Table 3.16 Failure Report Analysis**

Failure Reporting Analysis and Corrective Action System (FRACAS)											
Specialist Name: Dr. Eduardo Calixto			ID: 0234056		Specialist Function: Principal Reliability Engine				Management Group: Industrial		
FRACAS Database											
Equipment Start Date: 02/01/1990											
LRU Serial Number	Off Date	Off Type	System Location Code	Maintenance Start Date	Maintenance Finish Date	On Date	LRU Name	Failure Mode	Root Cause	Consequence	Detection
B-31005 B	17/06/1991	Failure	1401— Distillation plant	17/06/1991	20/06/1991	20/06/1991	1—Seal	FM1—Worn	RC 1—Wrong design	C1—External leak	D1—Visual inspection
B-31005 B	25/07/1992	Failure	1401— Distillation plant	25/07/1992	26/07/1992	27/07/1992	1—Seal	FM1—Worn	RC 2— Incorrect installation	C1—External leak	D1—Visual inspection
B-31005 B	25/02/1994	Failure	1401— Distillation plant	25/02/1994	03/03/1994	03/03/1994	2—Bearing	FM1—Worn	RC1— Insufficient or lack of lubrication	C1—High vibration	D2— Monitoring on line
B-31005 B	25/10/1995	Failure	1401— Distillation plant	25/10/1995	28/11/1995	28/11/1995	2—Bearing	FM1—Worn	RC2— Overload that causes high vibration	C2—Pump low performance	D2— Monitoring on line
B-31005 B	23/08/1997	Failure	1401— Distillation plant	23/08/1997	29/09/1997	29/09/1997	1—Seal	FM4—Corrosion	RC 6— Chemical attack caused by wrong material selection	C1—External leak	D1—Visual inspection
B-31005 B	09/11/1998	Failure	1401— Distillation plant	09/11/1998	17/11/1998	17/11/1998	2—Bearing	FM1—Worn	RC1— Insufficient or lack of lubrication	C1—High vibration	D1— Vibration analysis
B-31005 B	21/12/1998	Failure	1401— Distillation plant	21/12/1998	22/12/1998	22/12/1998	2—Bearing	FM2— Deformation	RC3— Misaligned caused by wrong assembly	C1—High vibration	D1— Vibration analysis
B-31005 B	02/03/2001	Failure	1401— Distillation plant	02/03/2001	14/03/2002	14/03/2002	2—Bearing	FM1—Worn	RC2— Overload that causes high vibration	C2—Pump low performance	D2— Monitoring on line
B-31005 B	04/09/2002	Failure	1401— Distillation plant	04/09/2002	04/09/2002	04/09/2002	2—Bearing	FM2— Deformation	RC3— Misaligned caused by wrong assembly	C1—High vibration	D1— Vibration analysis
B-31005 B	07/01/2003	Failure	1401— Distillation plant	07/01/2003	07/01/2003	07/01/2003	1—Seal	FM3—Cracking	RC5—High friction heat at the seal faces caused by excessive pressures or velocity	C1—External leak	D1—Visual inspection
B-31005 B	25/01/2003	Failure	1401— Distillation plant	25/01/2003	27/02/2003	27/02/2003	1—Seal	FM2—Face deflexion	RC4— Improper stationary seal face	C1—External leak	D1—Visual inspection
B-31005 B	10/01/2005	Failure	1401— Distillation plant	10/01/2005	11/01/2005	11/01/2005	1—Seal	FM1—Worn	RC3— Overload that causes high vibration	C1—External leak	D1—Visual inspection

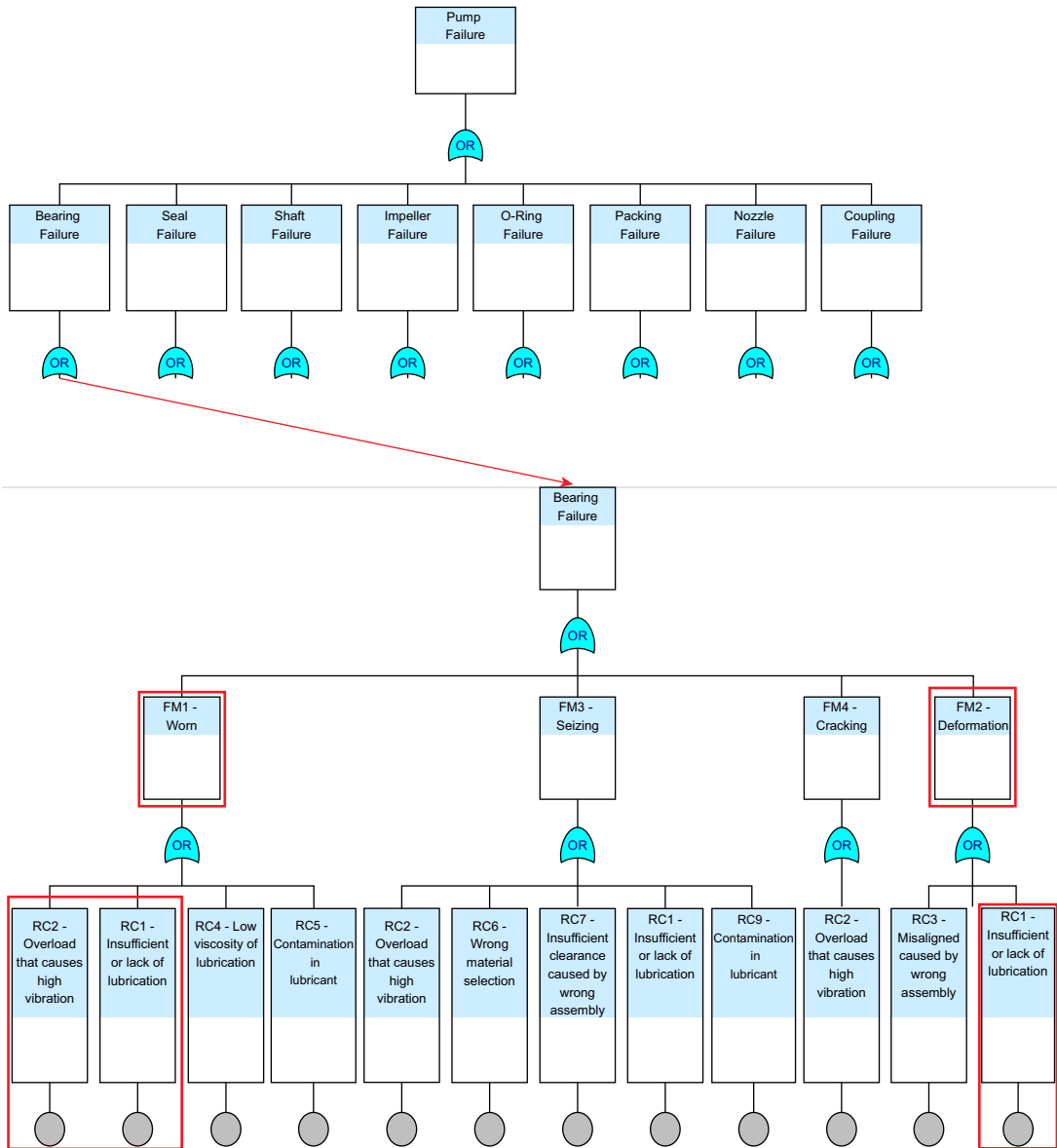


FIGURE 3.26

Fault tree analysis applied to root cause analysis.

Failure Reporting Analysis and Corrective Actions System (FRACAS)	
FRACAS module: 5 WHY TEST	Equipment: Pump      Component: Bearing
Failure Mode: FM1—worn	Root Cause: RC2—Overload that causes high vibration
FIRST WHY	The historical database shows that overload is the most probable cause of bearing wear.
SECOND WHY	The operation records show high flow several times in different shifts.
THIRD WHY	The overload was higher than design specification.
FOURTH WHY	The operator was not aware of the design specification.
FIFTH WHY	The operator had no training in new procedures, including the pumps.

**FIGURE 3.27**

5 WHY Test.

The final FRACAS step is to create a performance index platform to be followed up during the operation phase. In fact, the warranty analysis must be the baseline to analyze equipment performance, in addition to a general overview of equipment component performance. Thus the basic information that the FRACAS system must contain is the percentage of failures, root causes, and consequences, as shown in Fig. 3.29.

Once the critical components are identified, the failure mode effect must be revealed, as shown in Fig. 3.30. Such types of information help to analyze if the corrective actions are being successful in preventing failure modes occurring in the future. Based on Fig. 3.30, wear-out and deformation are the two most common failure modes registered on the FRACAS database.

It is important to bear in mind that the FRACAS performance report changes over time depending on the equipment that is taken into account. This is a further step to identify the root causes that influence such failure modes. Therefore, based on Fig. 3.31, the RC1, RC2, and RC3 are the most critical which cause more failure mode. The conclusion is that the human error (RC2 and RC3) is responsible for 66% of the root causes that affected the bearing or seal pump. In this case, the bearing and seal design is not the main root cause for low asset performance but the human error. Chapter 5 will demonstrate different human reliability analysis methods.

The additional performance analysis that must be assessed based on the FRACAS database is reliability, which will be discussed in the next section.

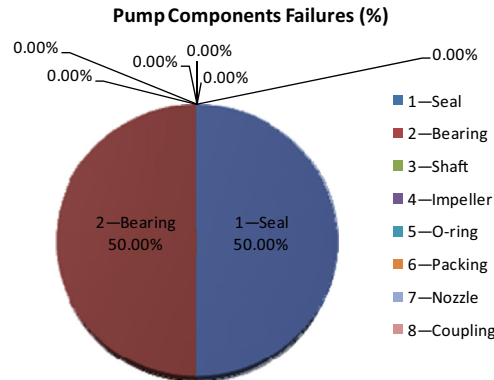
### 3.8.1 WARRANTY ANALYSIS

The main objective of warranty analysis is to measure equipment performance to check that what the vendor is committed to is delivered in terms of performance achieved during a specific period of time, operational hours, or other utilization factor. In fact, vendor equipment performance must be measured in terms of reliability during a specific period of time, for example, and such an index must be defined on the warranty contract.

Failure Reporting Analysis and Corrective Action System (FRACAS)										
Specialist name: Dr. Eduardo Calixto			Specialist Function: Principal Reliability Engineer				Management Group: Industrial			
FRACAS Database										
Equipment Start Date: 02/01/1990										
LRU Serial Number	SRU Name	Failure Mode	Root Cause	Consequence	Corrective action	Who?	When?	Frequency	How Much?	Status
B-31005 B	1—Seal	FM1—worn	RC 1—wrong design	C1—External leak	Change the Seal design based on DFMEA	Maintenance/Project Group	20/06/1991	Every new project specification	\$	OK
B-31005 B	1—Seal	FM1—worn	RC 2—Incorrect installation	C1—External leak	Implement inspection and test during installation	Maintenance Group	27/07/1992	Every installation	\$	OK
B-31005 B	2—bearing	FM1—worn	RC 1—Insufficient or lack of lubrication	C1—High vibration	Implement Oil quality test	Maintenance Group	01/04/1994	Every 6 months	\$	OK
B-31005 B	2—bearing	FM1—worn	RC2—Overload that causes high vibration	C2—Pump Low performance	Implement vibration analysis	Maintenance Group	01/01/1996	Every 3 months	\$	OK
B-31005 B	1—Seal	FM4—corrosion	RC 6—Chemical attack caused by wrong material selection	C1—External leak	Change the Seal design based on DFMEA	Maintenance/Project Group	23/08/1997	Every new specification	\$	OK
B-31005 B	2—bearing	FM1—worn	RC1—Insufficient or lack of lubrication	C1—High vibration	Implement monitoring inline oil quality	Maintenance Group	17/11/1998	Inline	\$	OK
B-31005 B	2—bearing	FM2—deformation	RC3—Misaligned caused by wrong assembly	C1—High vibration	Implement inspection and vibration analysis test during installation	Maintenance Group	22/12/1998	Every installation	\$	OK
B-31005 B	2—bearing	FM1—worn	RC2—Overload that causes high vibration	C2—Pump Low performance	Maintain vibration analysis and review operation procedure	Maintenance Group	14/03/2002	Every 3 months	\$	Not attend
B-31005 B	2—bearing	FM2—deformation	RC3—Misaligned caused by wrong assembly	C1—High vibration	Maintain vibration analysis and review operation procedure and training of operators	Maintenance Group	04/10/2002	Every 3 months	\$	Not attend
B-31005 B	1—Seal	FM3—cracking	RC5—High friction heat at the seal faces caused by excessive pressures or velocity	C1—External leak	Review operation procedure and training of operators	Maintenance Group	07/02/2003	Every Year	\$	OK
B-31005 B	1—Seal	FM2—face deflexion	RC4—Improper stationary seal face support	C1—External leak	Change the Stationary Seal design based on DFMEA	Maintenance/Project Group	25/01/2003	Every new specification	\$	OK
B-31005 B	1—Seal	FM1—worn	RC3—Overload that causes high vibration	C1—External leak	Review operation procedure and training of operators	Maintenance Group	11/02/2005	Every Year	\$	OK

FIGURE 3.28

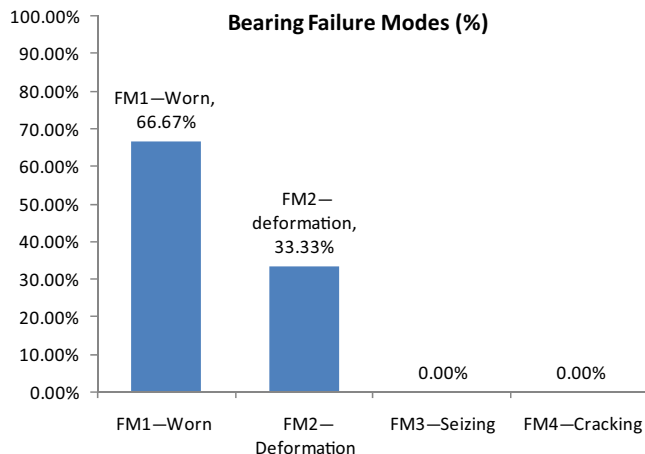
Corrective actions system.



**FIGURE 3.29**  
Pump critical component failure (%).

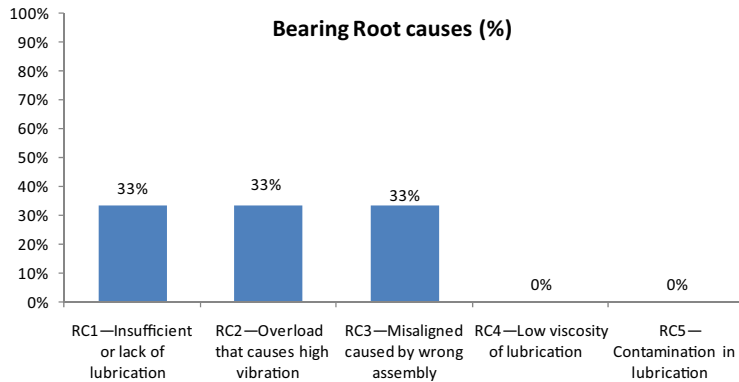
In addition, the turnout, or total repair time may also be defined as a target when the vendor is responsible for repairing the equipment during the warranty time. Turnout is the total time since equipment shutdown until such equipment is ready to start up. Such time encompasses repair or replacement time and also logistic time, which includes team dislocation and spare parts delivery. Therefore a stock policy must be defined to avoid unnecessary impact on system operational availability. The spare parts policy will be discussed in detail in Chapter 4. But now, let us focus on the reliability performance index.

To measure the reliability index during the warranty time it is necessary to collect the failure time of equipment and also the cause and consequence of failures. Such data is stored in the FRACAS database as discussed previously. To calculate reliability performance, lifetime data analysis must be carried out, as explained in Chapter 1. In addition, “reliability function  $\times$  time” must be compared with the reliability function target, as shown in Fig. 3.32, which compares two reliability functions of a centrifugal pump. The reliability target is 100% in 2 years; in other words, 2 years without defect.



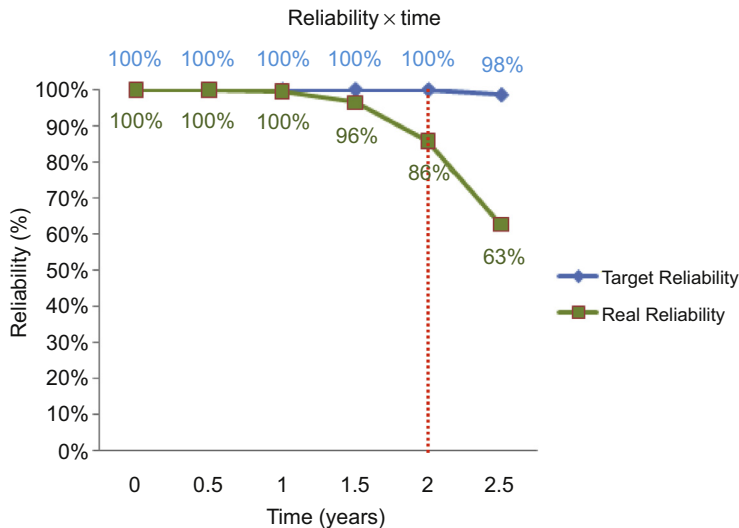
**FIGURE 3.30**  
Critical failure modes (%).



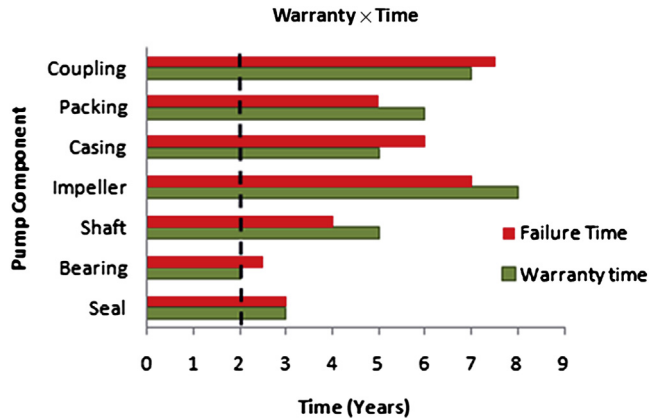


**FIGURE 3.31**  
Critical root causes (%).

Fig. 3.32 shows that the equipment reliability target is not achieved because the target is 100% in 2 years and the reliability achieved was 86% in 2 years. The additional issue when defining warranty performance is also defining the reliability index for the main components because each component has a different expected time to fail. Whenever the warranty is defined for equipment, the critical components are taken into account. In reality, other components have higher expected times to fail. Therefore it is important to define such a reliability performance index at the component level whenever possible. Fig. 3.32 shows the warranty defined for a pump, but the best approach is to define a reliability target for the main components such as coupling, packing, casing, shaft, bearing, and seal, as shown in Fig. 3.33.



**FIGURE 3.32**  
Real reliability × target reliability.



**FIGURE 3.33**

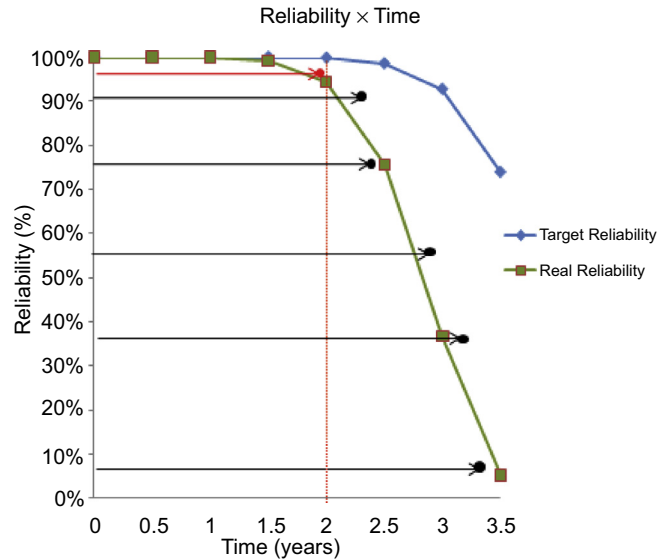
Warranty  $\times$  time.

If we assume 100% reliability in 2 years for the pump demonstrated in Fig. 3.32, the warranty is achieved because the first failure will happen in 2.5 years, but if we consider the warranty for the main components, which means the time to first failure, the warranty is not achieved for packing, impeller, and shaft components. Such an individual target is very important because of the focus on equipment life cycle time. This results in better equipment performance and reduction in the number of spare parts.

There is a different case where the reliability target is measured concerning equipment already installed. Whenever the reliability performance is measured to verify the warranty achievement, it is important to take into account that the operating environment conditions of such equipment because it take influence in equipment reliability performance. In other words, to consider a sample of equipment, it is necessary that such equipment operates in similar conditions and has a similar maintenance policy. Fig. 3.34 shows an example of reliability warranty based on the sample of a bearing installed in similar pumps. In this case, the bearing operates under similar operational conditions and maintenance policy. Fig. 3.34 shows that the reliability target has achieved 95% in 2 years.

Whenever the warranty is established for equipment or a sample of equipment it is important to define the duration of such required performance. In some cases, the operational time is more effective because equipment such as standby pumps does not operate 24 h per day. Therefore the general rule is that whenever equipment utilization is very high, time is a good parameter to establish the reliability target. However, when equipment has minimal utilization, the operation time or the parameter must be established.

Additional information on a warranty contract shows how equipment will be monitored and how failure will be detected. In many cases, equipment performance can be monitored online based on parameters such as flow, temperature, and vibration. In other cases, it is necessary to perform a predictive test (NDT) to gain a better assessment of equipment conditions. The most important thing is to establish all such methods and measurements on a warranty contract.



**FIGURE 3.34**

Real reliability  $\times$  target reliability (sample).

An additional item that must be established on a warranty contract is the action and compensation that the vendor will provide for the client in case of equipment failure during warranty time. In a case where equipment failure leads to plant shutdown, the cost of failure is much higher than the repair cost and a price penalty must be established in the warranty contract. The warranty contract must have three parts dedicated to reliability, maintainability, and operational availability. Each part must define the performance index, penalties, performance achieved index, performance benchmarking, measurement, and monitoring. Table 3.17 shows an example of a warranty performance index.

As shown in the tables, reliability is defined as a performance index rather than mean time between failure (MTBF) and failure rate. In fact, whenever a decision is taken we are dealing with risk and probabilistic chances that some event will occur or not on time. The huge advantages of reliability are the possibility of comparing similar equipment based on reliability performance before and after the warranty period. Such advantages do not exist when the MTBF or mean time to failure (MTTF) is established as the performance index. In fact, two or more similar pieces of equipment can have similar MTBFs but different reliability, as proved in the case of a sensor lifetime data analysis when three sensors were compared by Dr. Andrzej (2014) from the Office of Technical Inspection (UDT—Poland), as shown in Fig. 3.35, which demonstrates three different equipment reliability functions. This case describes three equipment reliabilities with similar MTTF; their PDF parameters and performance index are:

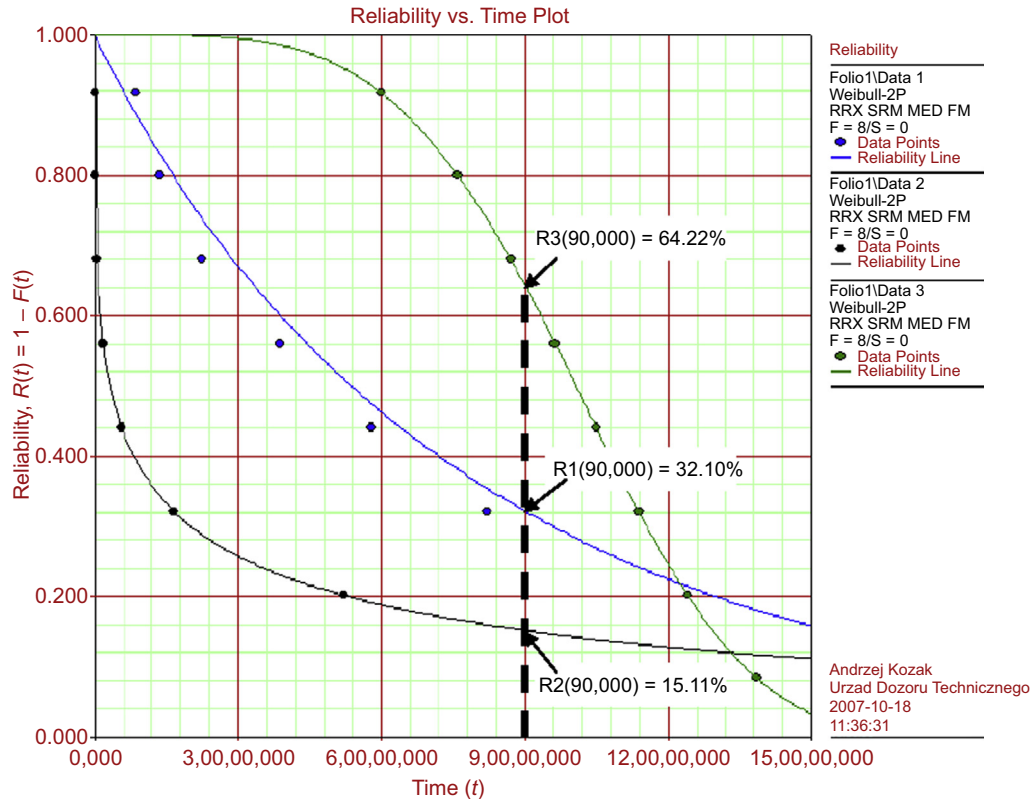
Equipment 1:  $\eta_1 = 78,705$  h,  $\beta_1 = 0.95$ ,  $MTTF_1 = 80,437.8$  h,  $R_1(90.000) = 32.10\%$

Equipment 2:  $\eta_2 = 10,797$  h,  $\beta_2 = 0.3$ ,  $MTTF_2 = 99,985.9$  h,  $R_2(90.000) = 15.11\%$

Equipment 3:  $\eta_3 = 110,330$  h,  $\beta_3 = 4.0$ ,  $MTTF_3 = 10,0003$  h,  $R_3(90.000) = 64.22\%$

**Table 3.17 Warranty Performance Index**

Warranty Performance Index Contract				
	<b>Equipment: Centrifugal Pump</b> Code: P-101 A	<b>Component: Seal</b> Code: SP-101 A	<b>Supplier: Flowsever</b>	<b>Commercial Contractor:</b> David Thompson
	<b>Summarized Customer Requirements</b>	<b>Summarized Supplier Achievement</b>	<b>Reference and Benchmarks</b>	<b>Measurement and Monitoring</b>
<b>Reliability</b>	<p><b>Performance Requirements:</b></p> <p><b>Index 1:</b> 100% reliability in 2.5 years</p> <p><b>Index 2:</b> Zero failures in 2 years</p> <p><b>Penalty regime:</b> Replace seal without any cost and pay for loss of production hours caused by component failure</p>	<p><b>Performance Achievement:</b></p> <p><b>Index 1:</b> 100% reliability in 2.5 years</p> <p><b>Index 2:</b> Zero failures in 3 years</p> <p><b>Penalty regime:</b> No penalty</p>	<p><b>Performance Reference:</b></p> <p><b>Index 1:</b> 100% reliability in 2.5 years based on historical best seal performance of this pump function</p> <p><b>Index 2:</b> Zero failures in 2.5 years based on historical best seal performance of this pump function</p> <p><b>Penalty regime:</b> Based on last contracts</p>	<p><b>Measurement Method:</b> Reliability must be measured based on lifetime data analysis method by applying the CAFDE reliability software from BQR</p> <p><b>Monitoring Method:</b> Monitoring failure based on FRACAS database</p>
<b>Availability</b>	<p><b>Performance Requirements:</b></p> <p><b>Index 1:</b> 99.99% of operational availability in 3 years</p> <p><b>Index 2:</b> Three failures in 10 years</p> <p><b>Penalty regime:</b> Replace seal without any cost and pay for loss of production hours caused by component failure</p>	<p><b>Performance Achievement:</b></p> <p><b>Index 1:</b> 99.99% of operational availability in 3 years</p> <p><b>Index 2:</b> One failure in 3 years</p> <p><b>Penalty regime:</b> No penalty</p>	<p><b>Performance Reference:</b></p> <p><b>Index 1:</b> 99.9% of operational availability based on historical best seal performance of this pump function</p> <p><b>Index 2:</b> Three failures in 10 years</p> <p><b>Penalty regime:</b> Based on last contracts</p>	<p><b>Measurement Method:</b> Operational availability (OA) defined as the fraction between uptime and total time OA=uptime/total time</p> <p><b>Monitoring Method:</b> Monitoring failure based on FRACAS database</p>
<b>Maintainability</b>	<p><b>Performance Requirements:</b></p> <p><b>Index 1:</b> 8 hours of maximum turnout</p> <p><b>Index 2:</b> One seal spare part for both active and standby pumps. The minimum spare level must be maintained during the time</p> <p><b>Penalty regime:</b> If the extra hour affects the plant operational availability the loss of production must be paid by the vendor. If the extra hour does not affect the plant operational availability the vendor will lose one level of the vendor qualification system</p>	<p><b>Performance Achievement:</b></p> <p><b>Index 1:</b> 6 hours of turnout</p> <p><b>Index 2:</b> One seal spare part for both pumps in stock</p> <p><b>Penalty regime:</b> No penalty</p>	<p><b>Performance Reference:</b></p> <p><b>Index 1:</b> 8 hours of maximum turnout based on vendor's average time</p> <p><b>Index 2:</b> One seal spare part for both active and standby pumps. Based on spare part utilization</p> <p><b>Penalty regime:</b> Based on last contracts</p>	<p><b>Measurement Method:</b> Turnout is then calculated based on the sum of hours between the repair order release until the time of equipment acceptance by operator</p> <p><b>Monitoring Method:</b> Monitoring failure based on FRACAS database. The visual inspection and monitoring online are the methods to detect the seal failure</p>

**FIGURE 3.35**

Reliability is better than MTTF.

Based on Fig. 3.35, the MTTF is quite similar but the reliability is very different. When comparing equipment 1 and 2,  $MTTF_2 > MTTF_1$ ; however,  $R(t)_2 < R(t)_1$ , which proves to be the best performance index. Whether the PDF parameters of equipment 2 are input in the diagram block and Monte Carlo simulation is carried out, the number of failures of equipment 2 will happen earlier than equipment 1, as will be demonstrated in Chapter 4. MTTF performance index additional limitations will be discussed in Chapter 4.

The next section provides case studies to help the reader learn more about the FMEA, RCM, and RBI methods.

## REFERENCES

- American Petroleum Institute, May 2002. API Recommended Practice 580, first ed. Risk-based Inspection.
- Andrzej, K., 2014. Why to Use the Consulting Services in Safety. III Forum on Functional Safety. Office of Technical Inspection, Poland, Warsaw.

- Calixto, E., Michael, S.S., 2011. The Optimum Replacement Time Considering Reliability Growth, Life Cycle and Operational Costs. ARS, Amsterdam.
- Carson, C.S., 2005. Fazendo da FMEA uma ferramenta de Confiabilidade Poderosa. SIC.
- Crow, L.H., 2008. A methodology for managing reliability growth during operational mission profile testing. Proceedings of the 2008 Annual Reliability and Maintainability Symposium, pp. 48–53.
- Jardine, A.K.S., 2006. Maintenance, Replacement, and Reliability. Theory and Applications. Taylor & Francis.
- Jenny, S., 2007. The application of risk based inspection to pressure vessels and aboveground storage tanks in petroleum fuel refineries. In: 5th Australasian Congress on Applied Mechanics (ACAM 2007), December 10–12, 2007, Brisbane, Australia.
- Lee, A.K., Serratella, C., Wang, G., Basu, R.A.B.S., Spong, R., 2006. Flexible approaches to risk-based inspection of FPSOs. In: 2006 Offshore Technology Conference Held in Houston, Texas, U.S.A., May 1–4, 2006. Energo Engineering Inc. OTC 18364.
- Mark, W., Russel, W.B., David, K., 2012. Utilizing equipment data for proactive asset management. In: Gas Machinery Conference, Austin, Texas.
- ReliaSoft Corporation, RCM++ 7.0 Software Package, Tucson, AZ, [www.Weibull.com](http://www.Weibull.com)
- Risk Based Inspection Base Resource Document, May 2000. API Publication 581, Preliminary Draft. American Petroleum Institute.
- Sobral, M.J., Ferreira, L.A., 2010. Development of a new approach to establish inspection frequency in a RBI assessment. In: Papazoglou, A., Zio (Eds.), Reliability, Risk and Safety. Taylor & Francis Group, London, ISBN 978-0-415-60427-7. Esrel 2010, Rhodos.

## APPENDIX

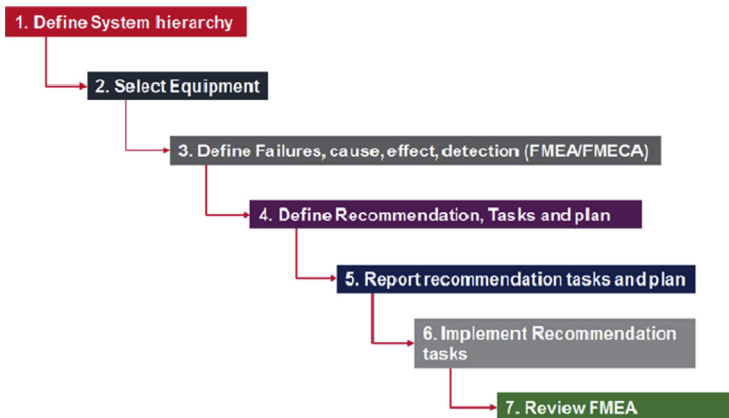
### 3.9 FMEA, RCM, AND RBI CASE STUDIES

The FMEA as described in this chapter is a qualitative reliability engineering method for systematically analyzing the possible failure mode of each equipment component, and identifying the possible failure cause, how such a cause can be detected, as well as the resulting consequence of the effect on safety, health, the environment, and assets.

During the FMEA, risk assessment is a qualitative analysis of each failure mode, likelihood, and the failure mode effect and consequence based on a specific risk matrix. According to the risk criterion, risk evaluation is performed and recommendations are proposed, whenever necessary, to mitigate risk. This section will provide examples of FMEA, which follows the steps described in Fig. 3.36.

In general, FMEA is presented as a worksheet. The spreadsheet is divided into 15 main sections:

- Equipment description
- Equipment configuration
- Equipment function
- Component
- Component function
- Failure modes
- Failure causes
- Phase
- Likelihood
- Detection
- Effect
- Consequence



**FIGURE 3.36**

FMEA steps.

- Risk assessment
- Risk evaluation
- Recommendation

*Equipment description* describes the type of equipment, supplier, operation conditions, and design specification.

*Equipment configuration* describes the number of equipment components to clarify if there is redundancy or not.

*Equipment function* describes the equipment objective.

*Component* describes the type of components used in the equipment.

*Component function* describes the objective of the components.

*Failure modes* describes the way such components lose their function.

*Failure mode causes* describes why failure mode happens.

*Phase* describes each phase of an asset when the failure mode happens, based on its cause. The asset phases are described in the FMEA sheet as: De (design), Mo (Montage), Tra (Transportation), Ins (Installation), Prec (Pre-Commissioning), Op (Operation).

*Risk assessment* in the FMEA is the combination of the likelihood of failure mode with the consequence of failure mode effect. To analyze the risk, qualitative risk assessment was carried out based on specialist opinion, concerning a risk matrix with the likelihood and consequence criteria established.

*Likelihood assessment* is the frequency of failure modes occurring for each system analyzed.

The RCM processes set out the minimum criteria that any process should meet before starting RCM and should answer the following questions:

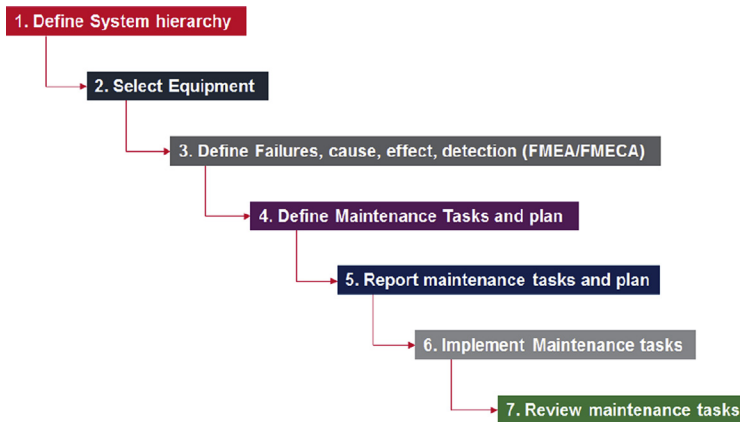
- What is the item supposed to do and what are its associated performance standards?
- In what ways can it fail to provide the required functions?
- What are the events that cause each failure?
- What happens when each failure occurs?
- In what way does each failure matter?
- What systematic task can be performed proactively to prevent, or to reduce to a satisfactory degree, the consequences of the failure?
- What must be done if a suitable preventive task cannot be found?

Based on such questions, the RCM steps are defined in [Fig. 3.37](#).

In general, RCM analysis is also presented in a worksheet format. The spreadsheet includes the FMEA template and also additional main sections such as:

- Maintenance task
- Type
- Frequency
- Maintenance cost
- Spare part
- Spare part cost
- Total cost
- Responsible
- Status





**FIGURE 3.37**

RCM steps.

*Maintenance task* describes the type of maintenance task defined during the RCM workshop.

*Type* describes the type of maintenance such as Co (corrective), Sch (schedule), PdM (predictive), and On-line (on-line monitoring).

*Frequency* describes the frequency of maintenance tasks in hours, days, weeks, months, or years.

*Maintenance cost* describes the total maintenance cost including the direct cost of the activity per year.

*Spare part* describes the number of equipment or component spare parts.

*Spare part cost* describes the cost of equipment or component spare parts per year.

*Total cost* describes the sum of maintenance cost and spare part cost.

*Responsible* describes the team leader responsible for implementing the maintenance task.

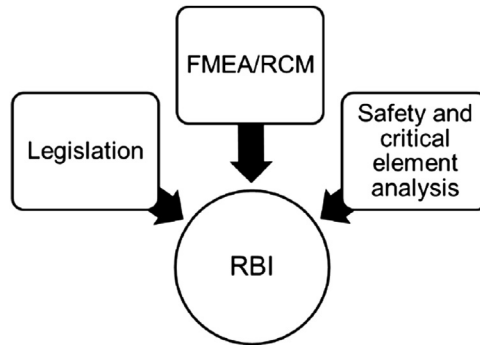
*Status* describes the status of the maintenance task per year.

The final method described in the case studies is the RBI, which is different from the RCM because it focuses on risk mitigation of unsafe failure and hazard events based on inspection and NDT. RBI input information as shown in Fig. 3.38 and comes from different types of analysis such as FMEA, RCM, legislation, and safety critical element, which are defined in risk analysis as preliminary hazard analysis (PHA), hazard and operability (HAZOP), hazard identification (HAZID), and quantitative risk analysis.

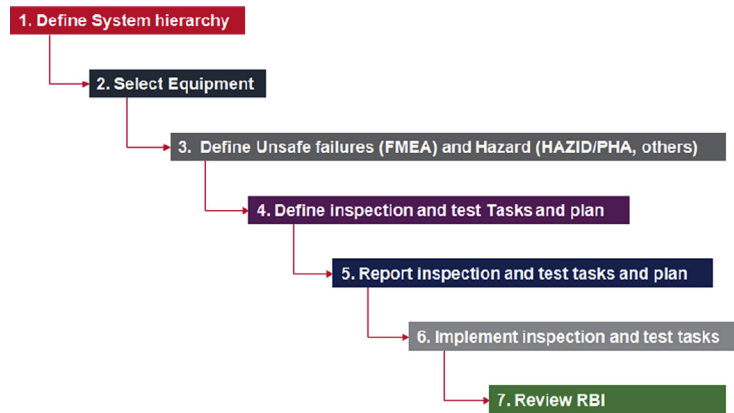
In general terms, the RBI steps are described in Fig. 3.39.

In general, RCM analysis is also presented in a worksheet format. The spreadsheet includes the FMEA template and additional hazards as well as additional main sections such as:

- Inspection task
- Type
- Frequency
- Inspection cost
- Spare part
- Inspection part cost



**FIGURE 3.38**  
RBI input information.



**FIGURE 3.39**  
RBI steps.

- Total cost
- Responsible
- Status

*Inspection task* describes the type of inspection and test task defined during the RBI workshop.  
*Type* describes the type of inspection and test such as PdM (predictive) and On-line (online monitoring).

*Frequency* describes the frequency of inspection and test task in hours, days, weeks, months, or years.

*Inspection cost* describes the total inspection or test cost, including the direct cost of the activity per year.

*Spare part* describes the number of equipment or component spare parts.

*Spare part cost* describes the cost of equipment or component spare parts per year.

*Total cost* describes the sum of inspection and test cost and spare part cost.

*Responsible* describes the team leader responsible for implementing the inspection and task.

*Status* describes the status of the maintenance task per year.

The following section will demonstrate the FMEA, RCM, and RBI case studies by applying the steps described previously.

### 3.9.1 CENTRIFUGAL PUMP FMEA/RCM

The centrifugal pump is one of the most used pumps in the gas and oil industry, therefore this case study will describe the main component failure modes and maintenance tasks. The first step in FMEA is to define the equipment and the components list. The main component of a centrifugal pump can be described on the equipment hierarchy as shown in Fig. 3.40.

The next step is to define the equipment and component function, which is described in Table 3.18.

The next step is to define the component failure modes, cause, and consequences, which are defined in Tables 3.19–3.23.

There are different configurations of the risk matrix and such configurations must reflect the law and companies' risk policies. Fig. 3.41 shows an example of a risk matrix with four severity categories and six frequency categories.

In addition, severity classification must describe all parties affected in case of an accident involving employees, the community, and the environment as well as company installation costs. Fig. 3.42 shows an example of the severity category.

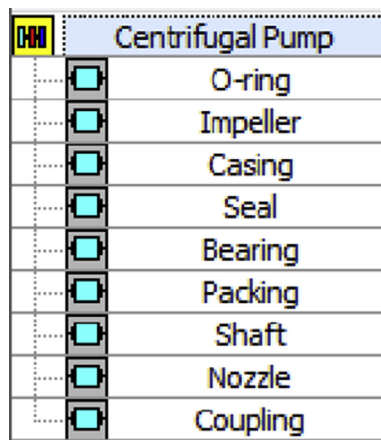


FIGURE 3.40

Centrifugal pump hierarchy.

**Table 3.18 Equipment and Component Function (FMEA)**

Failure Mode and Effect Analysis (FMEA)						
FMEA Leader: Dr. Eduardo Calixto			Document: DE-12456-001 Rev01		Date: 15-02-2014	
System: Distillation Plant			Subsystem: Vacuum Distillation		Equipment: P101 A/B	
No.	Equipment Number	Equipment Description	Equipment Configuration	Equipment Function	Component	Component Function
1	P-101 A/B	Centrifugal pump	2 × 100%	This pump is used to increase the pressure flow in train 1. It transfers fluids, enough to deliver to the main export pumps	O-ring	Avoid fluid turbulence
2					Casing	Protect the impeller and create a chamber for the fluid to be pumped through
3					Coupling	Transmit torque to impeller
4					Impeller	Spin the fluid inside the pump chamber
5					Shaft	Transmit mechanical energy
6					Seal	Prevent external leakage
7					Bearing	Ensure shaft alignment
8					Packing	Control leakage
9					Nozzle	Avoid fluid turbulence

### 3.9.2 VALVE FMEA/RCM

The valve is one of the most important pieces of equipment in the gas and oil industry, therefore this case study will describe the main component failure modes and maintenance tasks. The first step in FMEA is to define the equipment and the components list. The main component of the valve can be described on the equipment hierarchy as shown in Fig. 3.43.

The next step is to define the component failure modes, cause and consequences as shows Table 3.24 and finally, to define the preventive maintenance task based on RCM analysis as defined in Table 3.25.

**Table 3.19 O-Ring, Casing, and Coupling Risk Assessment (FMEA/RCM)**

Failure Mode and Effect Analysis (FMEA)												Reliability Centered Maintenance (RCM)									
FMEA Leader: Dr. Eduardo Calixto				Document: DE-12456-001 Rev01		Date: 15-02-2014				FMEA Leader: Dr. Eduardo Calixto		Date:16-02-2014									
System: Distillation Plant				Subsystem: Vacuum Distillation		Equipment: P101 A/B			Component: O-Ring, Casing and Coupling			Equipment: P101 A/B		Component: O-Ring, Casing and Coupling							
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S	Risk (Pri)	Mitigate Action	O	S	Risk (Post)	Task	Type	Frequency	Cost	Status				
1	O-ring	Worn out	Op	Normal wear	E	Low flow (pumps less than the required flow rate of 'X' or pressure of 'Y')	I	EI	N/A												
2			Op	Excessive solids in fluid causing premature wear	E			EI	N/A												
3			Ins	Impeller misaligned	E			EI	N/A												
4			Brittle	Overheat caused by lack of cooling or adequate liquid flow	Op			E	EI	N/A											
5			Deformation	Excessive temperature, pressure or chemical attack	OP			E	EI	N/A											
6	Casing	Worn out	Op	Normal wear	D	Low flow (pumps less than the required flow rate of 'X' or pressure of 'Y')	I	DI	N/A												
			Op	Excessive solids in fluid causing premature wear	D			DI	N/A												
7	Distorted	Op	Excessive pipe strain caused by overload	D	DI			N/A													
8	Coupling	Worn out	Op	Vibration caused by improper shaft alignment	D		II	DII	N/A												
			Op	Improper lubrication	D			DII	N/A												
			Op	Normal wear	D			DII	N/A												

**Table 3.20 Impeller and Shaft (FMEA/RCM)**

Failure Mode and Effect Analysis (FMEA)													Reliability Centered Maintenance (RCM)						
FMEA Leader: Dr. Eduardo Calixto			Document: DE-12456-001 Rev01			Date: 15-02-2014			RCM Leader: Dr. Eduardo Calixto			Date: 16-02-2014							
System: Distillation Plant			Subsystem: Vacuum Distillation			Equipment: P101 A/B			Component: Impeller and Shaft			Equipment: P101 A/B		Component: Impeller and Shaft					
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S	R	Mitigate Action	O	S	Risk (Post)	Task	Type	Frequency	Cost	Status		
1	Impeller	Worn out	Op	Normal wear	D	High operation cost and low flow (pumps less than the required flow rate of 'X' or pressure of 'Y')	II	DII	N/A										
2			Op	Excessive solids in fluid causing premature wear	D		III	DIII	Define preventive maintenance	B	III	BIII	Sample fluid analysis	Pdm	Yearly	\$	OK		
3			Op	Pump cavitation	D		Damage to pump bearings	I	DI	N/A									
4			Plugged	Op	Foreign material in process		D	Low flow (pumps less than the required flow rate of 'X' or pressure of 'Y')	II	DII	N/A								
5	Impeller	Loose	Op	Excessive backow	D	Low flow (pumps less than the required flow rate of 'X' or pressure of 'Y')	II	DII	N/A				N/A						
			Op	Incorrect installation	D	Damage to pump bearings and process impact—low flow (pumps less than the required flow rate of 'X' or pressure of 'Y')	II	DII	N/A				N/A						
6	Shaft	Worn out	Op	Excessive solids in fluid causing premature wear	D	Low flow (pumps less than the required flow rate of 'X' or pressure of 'Y')	III	DIII	Define preventive maintenance	B	III	BIII	Sample fluid analysis	Pdm	Yearly	\$	OK		
			Ins	Incorrect installation	D		II	DIII	Installation procedure	B	III	BIII	Vibration test	Pdf	After installation	\$	OK		
			Op	Normal wear	D		II	DII	N/A				N/A						
7	Shaft	Fracture	Op	Excessive vibration	D	Low flow (pumps less than the required flow rate of 'X' or pressure of 'Y')	III	DIII	Define preventive maintenance	B	III	BIII	Monitoring vibration analysis	Pdm	Online	\$	OK		
Corrosion		De	Chemical attacks caused by wrong specification	D	III		DIII	Review the design specification: <b>Action:</b> <b>Design Group</b>	D	II	DII	N/A							

**Table 3.21 Seal (FMEA/RCM)**

Failure Mode and Effect Analysis (FMEA)											Reliability Centered Maintenance (RCM)								
FMEA Leader: Dr. Eduardo Calixto			Document: DE-12456-001 Rev01			Date: 15-02-2014					RCM Leader: Dr. Eduardo Calixto		Date: 16-02-2014						
System: Distillation Plant			Subsystem: Vacuum Distillation			Equipment: P101 A/B			Component: Seal			Equipment: P101 A/B		Component: Seal					
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S	R	Mitigate Action	O	S	Risk (Post)	Task	Type	Freq uency	Cost	Status		
1	Seal	Worn out	Op	Spring fatigue	E	External leak rate is above the acceptable rate that causes consequent loss of fluid to the ground	II	EII	N/A				N/A						
2			Op	Incorrect installation	E		III	EIII	Installation procedure	B	III	BIII	N/A						
3			Op	Normal wear (abrasive process fluid with no seal in water system)	E		II	EII	N/A					N/A					
4			Corrosion	De	Chemical attacks caused by wrong material selection		D	III	DIII	Review the design specification: <b>Action: Design Group</b>	B	III	BIII	N/A					
5			Fretting corrosion	Op	Constant back and forth movement of seal over shaft sleeve		E	II	EII	N/A					N/A				
				Op	Higher vibration		E	II	EII	N/A					N/A				
6		Spit and sputters	Op	The product is vaporizing and flashing across the seal face	D		II	DII	N/A					N/A					
7		Squeals	Op	Inadequate amount of liquid at sealing faces	D		II	DII	N/A										
8		Distortion	Op	Improper assembly	E		II	EII	N/A										
			De	Improper cooling liquid	D		II	DII	N/A										
9		Erosion	Op	Excessive flush rate	D		II	DII	N/A										
10			Op	Flush fluid contaminated with abrasive particles	D		II	DIII	Define preventive maintenance	B	III	BIII	Sample fluid analysis	Pdm	Yearly	\$	OK		
11	Op		High friction, heat at the seal faces caused by lack of lubrication	E	II	EII	N/A												
12	Cracking	Op	High friction, heat at the seal faces caused by vaporization at the seal face	D	II	DII	N/A												

Continued





**Table 3.22 Bearing (FMEA/RCM)**

Failure Mode and Effect Analysis (FMEA)													Reliability Centered Maintenance (RCM)					
FMEA Leader: Dr. Eduardo Calixto			Document: DE-12456-001 Rev01			Date: 15-02-2014			RCM Leader: Dr. Eduardo Calixto			Date: 16-02-2014						
System: Distillation Plant			Subsystem: Vacuum Distillation			Equipment: P101 A/B			Component: Bearing			Equipment: P101 A/B		Component: Bearing				
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S	R	Mitigate Action	O	S	Risk Post	Task	Type	Freq uency	Cost	Status	
1	Bearing	Deformation	Ins	Misaligned caused by wrong assembly	E	Low flow (pumps less than the required flow rate of 'X' or pressure of 'Y')	II	EII	N/A									
2			Op	Insufficient or lack of lubrication	D		II	DII	N/A									
3		Seizing	Op	Overload that causes high vibration	E		III	EIII	Define preventive maintenance	B	II	BII	Monitoring vibration analysis	Pdm	Online	\$	OK	
4			De	Wrong bearing material selection	D		II	DII	N/A									
5			Ins	Insufficient clearance caused by wrong assembly	D		II	DII	N/A									
6			Op	Insufficient or lack of lubrication	D		II	DII	N/A									
7			Op	Contamination in lubricant	D		II	DII	N/A									
8			Cracking	Op	High vibration caused by overload		E	High cost and low flow	III	EIII	Define preventive maintenance	B	II	BII	Monitoring vibration analysis	Pdm	Online	\$
9		Worn out	Op	Overload that causes high vibration	D		Low flow	II	DII	N/A								
10			Op	Lack of lubrication	D		II	DII	N/A									
12			Op	Contamination in lubricant	D		High cost and low flow	III	EIII	Define preventive maintenance	B	II	BII	Monitoring iubrificant quality	Pdm	Online	\$	OK



		FREQUENCY CATEGORY					
		A (extremely remote)	B (remote)	C (Little frequency)	D (Frequent)	E (Very frequent)	F (Extremely frequent)
		At least 1 between 1000 and 100,000 years	At least 1 between 50 and 1000 years	At least 1 between 30 and 50 years	At least 1 between 5 and 30 years	At least 1 in 5 years	At least 1 in 1 year
SEVERITY CATEGORY	IV	M	NT	NT	NT	NT	NT
	III	M	M	NT	NT	NT	NT
	II	T	T	M	M	M	M
	I	T	T	T	M	M	M

FIGURE 3.41

Risk matrix.

### 3.9.3 PIPELINE FMEA/RBI

The pipeline has an additional impact on production in case of failure and can also trigger an accident scenario. Therefore the RBI method is more appropriate and will focus on inspection an NDT to prevent unsafe failure, such as corrosion, which can lead to toxic leakage, jet fire, fireball, boiling liquid expanding vapor explosion (BLEVE), and explosion.

Concerning RBI methodology, all unsafe failures will be assessed based on FMEA analysis and the risk matrix demonstrated in Fig. 3.41 in will be applied.

Because of the impact on the environment and safety in case of unsafe failure, severity and risk will take into account the four classifications described in the risk matrix. Fig. 3.44 and Table 3.26 show the pipeline components list and the FMEA function, respectively.

Based on the previous description, Tables 3.27 and 3.28 show the FMEA and RBI, respectively.

### 3.9.4 TANK FMEA/RBI

The tank is an important piece of equipment for the oil and gas industry. Its main function is to store product and reduce the impact of production loss when a shutdown occurs. Concerning unsafe failures, leakage from tanks can also cause a serious accident and environmental impact, therefore it is necessary to define preventive maintenance, inspection, and NDT to prevent such failures. Consequently, the RBI method is more appropriate and will focus on inspection and NDT to prevent unsafe failure, such as corrosion, which can lead to toxic leakage, jet fire, fireball, BLEVE, and explosion.

Concerning RBI methodology, all unsafe failures will be assessed based on FMEA in this case, and a similar risk matrix applied to another case study will be considered here.










Because of the impact on the environment and safety in case of unsafe failure, severity and risk will take into account the four classifications described in the risk matrix. Fig. 3.45 and Table 3.29 show the tank components list and the FMEA function, respectively.

Once the valves, sensor, alarms, and controls are assessed in another case study, the tank FMEA will focus on tank, joint, gasket, and nozzle. It is important to highlight if the vent and the Pressure

			Description and characteristic			
			PERSONAL SAFETY	INSTALLATION	ENVIRONMENT AND IMAGE	SOCIAL
<b>SEVERITY CATEGORY</b>	IV	Catastrophic	Catastrophic injuries with death, it is possible to affect people outside	Losses in equipment and plant with high cost to buy new one	Loss of ecosystem with bad national and international company reputation	Economic effects on local activities, health costs to local population, economic losses in tourism, ecosystem local losses and quality of life losses (Between R\$101,000,000.00 and R\$336,000,000.00)
	III	Critical	Critical injuries. Employees stay a period of time out of workplace	Serious damage to equipment with high cost to repair	Critical effects to the environment being hard to improve the condition of the ecosystem even with human actions. Bad national and international company reputation	Economic effects on local activities, health costs to local population, economic losses in tourism, ecosystem local losses (Between R\$2,500,000.00 and R\$101,000,000.00)
	II	Marginal	Moderate injuries with first aid assistance	Low equipment damage with low repair cost	Not serious environmental effects but it is necessary for human intervention and actions to improve environment. Bad national company reputation	Economic effects on local activities, health costs to local population, economic losses in tourism, fishing and other areas (From R\$0.00 to R\$2,500,000.00)
	I	No effect	There are no injuries or damage to health	There is no damage to equipment and plant	Insignificant environmental effects. No improvement necessary to ecosystem. National company image not affected	There are no economic effects on local activities, health costs to local population

**FIGURE 3.42**

Severity classification.

Ref.Des.	
<b>HH</b>	Plug Valve
	Seat
	Plug
	Stem
	Diaphragm
	Gasket
	Hand Wheel
	Packing
	Disk
	Body

**FIGURE 3.43**

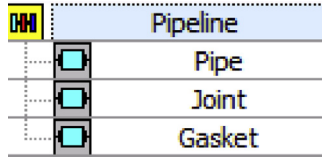
Globe valve hierarchy.

**Table 3.24 Equipment and Component Function (FMEA)**

Failure Mode and Effect Analysis (FMEA)						
FMEA Leader: Dr. Eduardo Calixto			Document: DE-210116-002 Rev03		Date: 10-08-2011	
System:			Subsystem:		Equipment: V 01	
No.	Equipment Number	Equipment Description	Equipment Configuration	Equipment Function	Component	Component Function
1	V-01	Plug valve	1 × 100%	Control the product flow	Seat	Release heat in the valve and prevent valve
2					Globe plug	Helps to shut off mechanism
3					Stem	Connect the actuator inside the valve
4					Diaphragm	Support the actuator movement
5					Gasket	Avoid leakage
6					Handwheel	Regulate the valve position
7					Packing	Avoid leakage
8					Disk	Reduce the flow
9					Body	Protect valve components







**FIGURE 3.44**  
Pipeline equipment list hierarchy.

Table 3.26 Pipeline Equipment FMEA Function						
Failure Mode and Effect Analysis (FMEA)						
FMEA Leader: Dr. Eduardo Calixto			Document: DE-100110-001 Rev01		Date: 20-03-2007	
System: Hydrogen Plant			Subsystem: PSA		Equipment: PL- 001	
No.	Equipment Number	Equipment Description	Equipment Configuration	Equipment Function	Component	Component Function
1	PL-01	Pipeline	1 × 100%	Transport product from point x to point y	Pipe	Transport product from point x to point y
2					Joint	Absorb the heat and vibration, to hold the parts together and to allow movement
3					Gasket	Avoid leakage

Safety Valve (PSV) valve fail to open, the pressure inside the tank increases, which can trigger an accident. Therefore it is necessary to constantly inspect such valves.

Based on the previous description Tables 3.30 and 3.31 show the FMEA and Tables 3.32 and 3.33 show the RBI, respectively.

### 3.9.5 CENTRIFUGAL COMPRESSOR FMEA/RCM

The centrifugal compressor is one of the most important types of compressor used in the gas and oil industry, therefore this case study will describe the main component failure modes and maintenance tasks of such equipment. The first step in FMEA is to define the equipment and the components list. The main component of the centrifugal compressor is described on the equipment hierarchy list, as shown in Fig. 3.46.

Based on the another FMEA/RCM/RBI analysis carried out in this section, the pumps, valves, pipes, and tanks will not be considered in this case study. Therefore the centrifugal gas compressor will encompass the following equipment and components described in Fig. 3.47.

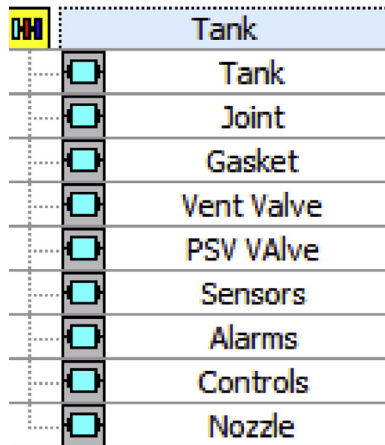


**Table 3.27 Pipeline FMEA**

Failure Mode and Effect Analysis (FMEA)																										
FMEA Leader: Dr. Eduardo Calixto			Document: DE-100110-001 Rev01				Date: 20-03-2007																			
System: Hydrogen Plant			Subsystem: PSA				Equipment: PL-01				Component: Pipe, Joint, Gasket															
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S P	S I	S E	S S	R P	R I	R E	R S	Mitigate Action	O	S P	S I	S E	S S	R P	R I	R E	R S		
1	Pipe	Weld fatigue	De	Inferior weld	D	Process impact	I	II	I	I	DI	DI	DI	DI	N/A											
2			Op	Fatigue caused by high vibration	D		I	II	I	I	DI	DI	DI	DI	N/A											
3		Corrosion	Op	Chemical attacks	C	Leakage with safety, environment, social and process impact	III	III	IV	IV	CIII	CIII	CIV	CIV	Define preventive maintenance	A	III	III	IV	IV	AIII	AIII	AIV	AIV		
4		Erosion	Op	High flow velocity	D		III	III	IV	IV	DIII	DIII	DIV	DIV	Define preventive maintenance	A	III	III	IV	IV	AIII	AIII	AIV	AIV		
5	Joint	Worn out	Op	Normal wear	D	Leakage with safety, environment, social and process impact	II	III	II	II	DII	DIII	DII	DII	Define preventive maintenance	B	II	III	II	II	BII	BIII	BII	BII		
6			Ins	Incorrect installation	D		II	III	II	II	DII	DIII	DII	DII	N/A	B	II	III	II	II	BII	BIII	BII	BII		
7		Looseness	Op	High vibration	D		II	III	II	II	DII	DIII	DII	DII	Define preventive maintenance	B	II	III	II	II	BII	BIII	BII	BII		
8			Op	Physical damage	C		II	III	II	II	CII	CIII	CII	CII	N/A	B	II	III	II	II	BII	BIII	BII	BII		
9	Gasket	Worn out	Ins	Incorrect installation	D	Leakage with safety, environment, social and process impact	II	III	II	II	DII	DIII	DII	DII	Define preventive maintenance	B	II	III	II	II	BII	BIII	BII	BII		
10			Op	Chemical degradation	D		II	III	II	II	DII	DIII	DII	DII	Define preventive maintenance	B	II	III	II	II	BII	BIII	BII	BII		
11			Op	Age-related degradation	D		II	III	II	II	DII	DIII	DII	DII	N/A	B	II	III	II	II	BII	BIII	BII	BII		

**Table 3.28 Pipeline RBI**

Risk Based Inspection (RBI)												
FMEA Leader: Dr. Eduardo Calixto			Document: DE-100110-001 Rev01				Date: 20-03-2007					
System: Hydrogen Plant			Subsystem: PSA				Equipment: PL-01			Component: Pipe, joint, gasket		
No.	Component	Failure Mode	Phase	Cause	O	Consequence	Mitigate Action	Inspection and Test Task	Type	Frequency	Cost	Status
1	Pipe	Weld fatigue	De	Inferior weld	D	Process impact	N/A					
2			Op	Fatigue caused by high vibration	D		N/A					
3		Corrosion	Op	Chemical attacks	C	Leakage with safety, environment, social and process impact	Define preventive maintenance	NDT (ultrasound test) and probabilistic degradation analysis after corrosion detection	Pdm	3 years	\$	OK
4		Erosion	Op	High flow velocity	D	Leakage with safety, environment, social and process impact	Define preventive maintenance	NDT (radiograph test)	Pdm	3 years	\$	OK
5	Joint	Worn out	Op	Normal wear	D	Leakage with safety, environment, social and process impact	Define preventive maintenance	NDT (radiograph test)	Pdm	3 years	\$	OK
6			Ins	Incorrect installation	D		N/A					
7		Looseness	Op	High vibration	D		Define preventive maintenance	Monitoring vibration analysis	Pdm	Online	\$	OK
8			Op	Physical damage	C		N/A					
9	Gasket	Worn out	Ins	Incorrect installation	D	Leakage with safety, environment, social and process impact	Define preventive maintenance	NDT (radiograph test)	Pdm	After installation and maintenance		
10			Op	Chemical degradation	D	Define preventive maintenance	NDT (radiograph test)	Pdm	3 years	\$	OK	
11			Op	Age-related degradation	D	N/A						



**FIGURE 3.45**

Tank equipment list hierarchy.

**Table 3.29 Tank Equipment FMEA Function**

Failure Mode and Effect Analysis (FMEA)						
FMEA Leader: Dr. Eduardo Calixto			Document: DE-100210-001 Rev01		Date: 25-05-2008	
System: Distillation			Subsystem: Vacuum Distillation		Equipment: TQ - 001	
No.	Equipment Number	Equipment Description	Equipment Configuration	Equipment Function	Component	Component Function
1	TQ-01	Product Tank	1 × 100%	Storage product	Tank	Storage product
2					Joint	Absorb the heat and vibration, to hold the parts together and to allow movement
3					PSV	Release the excess pressure
4					Vent	Release the internal vapor formation
5					Control	Detect process and equipment operational condition based on physical parameters
6					Sensors	Trigger the alarms and actuator in case of unsafe condition
7					Alarms	Alert the unwanted and unsafe process conditions
9					Gasket	Avoid leakage
10					Nozzle	Avoid fluid turbulence

Table 3.30 Tank FMEA

Failure Mode and Effect Analysis (FMEA)																										
FMEA Leader: Dr. Eduardo Calixto		Document: DE-100210-001 Rev01				Date: 25-05-2008																				
System: Distillation		Subsystem: Vacuum Distillation				Equipment: TQ-01								Component: Tank												
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S P	S I	S E	S S	R P	R I	R E	R S	Mitigate Action	O	S P	S I	S E	S S	R P	R I	R E	R S		
1	Tank	Weld fatigue	De	Inferior weld	D	Process impact	I	II	I	I	DI	DI	DI	DI	N/A											
2			Op	Fatigue caused by high vibration	D		I	II	I	I	DI	DI	DI	DI	N/A											
3		Corrosion	Op	Chemical attacks	C	Leakage with safety, environment, social and process impact	III	III	IV	IV	CIII	CIII	CIV	CIV	Define preventive maintenance	A	III	III	IV	IV	AIII	AIII	AIV	AIV		
4		Erosion	Op	High flow velocity	D		III	III	IV	IV	DIII	DIII	DIV	DIV	Define preventive maintenance	A	III	III	IV	IV	AIII	AIII	AIV	AIV		
5		Loss of insulation	Op	Age-related degradation	D	Process impact	I	II	I	I	DI	DII	DI	DI	N/A											
6			Ins	Wrong installation	D		I	II	I	I	DI	DII	DI	DI	N/A											
7		Brittle	De	Wrong material selection	C	Process impact	I	II	I	I	CI	CII	CI	CI	N/A											
			OP	Temperature out of specification	D		I	II	I	I	DI	DI	DI	DI	N/A											
8	Bottom leakage	Op	Chemical attacks	D	Leakage with safety, environment, social and process impact	III	III	IV	IV	DIII	DIII	DIV	DIV	Define preventive maintenance	A	III	III	IV	IV	AIII	AIII	AIV	AIV			

**Table 3.31 Tank FMEA**

Failure Mode and Effect Analysis (FMEA)																								
FMEA Leader: Dr. Eduardo Calixto			Document: DE-100210-001 Rev01					Date: 25-05-2008																
System: Distillation			Subsystem: Vacuum Distillation					Equipment: TQ-01							Component: Joint, Gasket, Nozzle, Vent Valve and PSV Valve									
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S P	S I	S E	S S	R P	R I	R E	R S	Mitigate Action	O	S P	S I	S E	S S	R P	R I	R E	R S
1	Joint	Worn out	Op	Normal wear	D	Leakage with safety, environment, social and process impact	II	III	II	II	DII	DIII	DII	DII	Define preventive maintenance	B	II	III	II	II	BII	BIII	BII	BII
2			Ins	Incorrect installation	D		II	III	II	II	DII	DIII	DII	DII	Installation procedure	B	II	III	II	II	BII	BIII	BII	BII
3		Looseness	Op	High vibration	D		II	III	II	II	DII	DIII	DII	DII	Define preventive maintenance	B	II	III	II	II	BII	BIII	BII	BII
4			Op	Physical damage	C		II	III	II	II	CII	CIII	CII	CII	Monitoring and prevent physical damage	B	II	III	II	II	BII	BIII	BII	BII
5	Gasket	Worn out	Ins	Incorrect installation	D	Leakage with safety, environment, social and process impact	II	III	II	II	DII	DIII	DII	DII	Define preventive maintenance	B	II	III	II	II	BII	BIII	BII	BII
6			Op	Chemical degradation	D		II	III	II	II	DII	DIII	DII	DII	Define preventive maintenance	B	II	III	II	II	BII	BIII	BII	BII
7			Op	Age-related degradation	D		II	III	II	II	DII	DIII	DII	DII	Define preventive maintenance	B	II	III	II	II	BII	BIII	BII	BII
8	Nozzle	Nozzle spanned	Op	Overload during operation	D	Process impact	I	II	I	I	DI	DII	DI	DI	N/A									
9			Op	Support is elevated above usual conditions	D		I	II	I	I	DI	DII	DI	DI	N/A									
10	Vent valve	Fail to open	Op	Internal component damage	D	Safety and process impact	III	III	II	I	DIII	DIII	DII	DI	Define preventive maintenance	B	III	III	II	II	BIII	BIII	BII	BII
11	PSV valve	Fail to open	Op		D		III	III	II	I	DIII	DIII	DII	DI		B	III	III	II	II	BIII	BIII	BII	BII

**Table 3.32 Tank RBI**

Risk Based Inspection (RBI)												
FMEA Leader: Dr. Eduardo Calixto			Document: DE-100210-001 Rev01				Date: 26-05-2008					
System: Distillation			Subsystem: Vacuum Distillation				Equipment: TQ-01			Component: Tank		
No.	Component	Failure Mode	Phase	Cause	O	Consequence	Mitigate Action	Inspection and Test Task	Type	Frequency	Cost	Status
1	Tank	Weld fatigue	De	Inferior weld	D	Process impact	N/A					
2			Op	Fatigue caused by high vibration	D		N/A					
3		Corrosion	Op	Chemical attacks	C	Leakage with safety, environment, social and process impact	Define preventive maintenance	NDT (ultrasound test) and probabilistic degradation analysis after corrosion detection	Pdm	1 year	\$	OK
								Visual inspection	Visual	5 years	\$	OK
								Hydrostatic test	NDT	5 years	\$	OK
4		Erosion	Op	High flow velocity	D	Process impact	Define preventive maintenance	NDT (radiograph test)	Pdm	1 year	\$	OK
5		Loss of insulation	Op	Age-related degradation	D		Define preventive maintenance	NDT (radiograph test)	Pdm	1 year	\$	OK
6			Ins	Wrong installation	D	N/A						
7		Brittle	Op	Wrong material selection	C	Process impact	N/A					
8	Op		Temperature out of specification	D	N/A							
9	Bottom leakage	Op	Chemical attacks	D	Leakage with safety, environment, social and process impact	Define preventive maintenance	Visual inspection	Visual	5 years	\$	OK	
							Magnetic flux leakage test	NDT	5 years	\$	OK	

**Table 3.33 Joint, Gasket, Nozzle, Vent Valve, and PSV Valve RBI**

Risk Based Inspection (RBI)												
FMEA Leader: Dr. Eduardo Calixto			Document: DE-100210-001 Rev01				Date: 26-05-2008					
System: Distillation			Subsystem: Vacuum Distillation				Equipment: TQ-01			Component: Joint, Gasket, Nozzle, Vent Valve and PSV Valve		
No.	Component	Failure Mode	Phase	Cause	O	Consequence	Mitigate Action	Inspection and Test Task	Type	Frequency	Cost	Status
1	Joint	Worn out	Op	Normal wear	D	Leakage with safety, environment, social and process impact	Define preventive inspection and NDT	NDT (radiograph test)	Pdm	3 years	\$	OK
2			Ins	Incorrect installation	D		N/A					
3		Looseness	Op	High vibration	D		Define preventive inspection and NDT	Monitoring vibration analysis	Pdm	Online	\$	OK
4			Op	Physical damage	C		N/A					
5	Gasket	Worn out	Ins	Incorrect installation	D	Leakage with safety, environment, social and process impact	Define preventive inspection and NDT	NDT (radiograph test)	Pdm	After installation and maintenance		
6			Op	Chemical degradation	D		Define preventive inspection and NDT	NDT (radiograph test)	Pdm	3 years	\$	OK
7			Op	Age-related degradation	D		N/A					
8	Nozzle	Nozzle spanned	Op	Overload during operation	D	Process impact	N/A					
9			Op	Support is elevated above usual conditions	D		N/A					
10	Vent valve	Fail to open	Op	Internal component damage	D	Safety and process impact	Define preventive inspection and NDT	NDT (radiograph test)	Pdm	1 year	\$	OK
11	PSV valve	Fail to open	Op		D		D	Define preventive inspection and NDT	Visual inspection and clean	Insp	1 year	\$
				Online test		Pdm			6 months	\$	OK	
				NDT (radiograph test)		Pdm			1 year	\$	OK	
				Visual inspection		Insp			1 year	\$	OK	

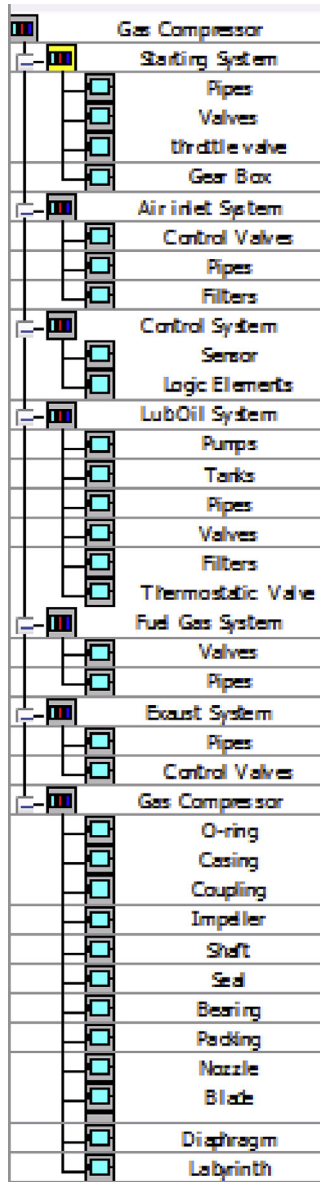
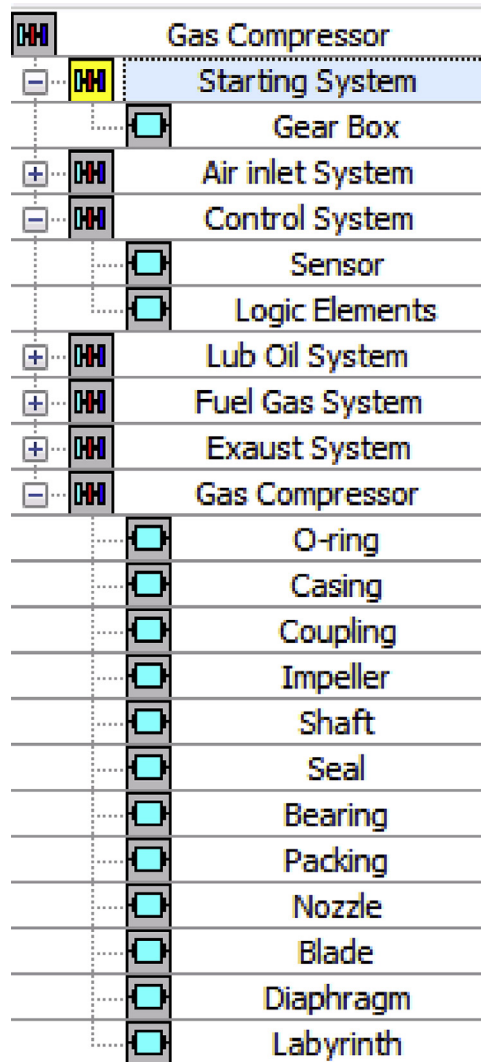


FIGURE 3.46 Centrifugal compressor hierarchy list.





**FIGURE 3.47**  
Centrifugal compressor hierarchy final list.

**Table 3.34 Compressor System Equipment (FMEA Function)**

Failure Mode and Effect Analysis (FMEA)						
FMEA Leader: Dr. Eduardo Calixto			Document: DE-10301-001 Rev02		Date: 11-12-2010	
System: Platform			Subsystem: Compression		Equipment: G-301 A/B, FT-301A/B	
No.	Equipment Number	Equipment Description	Equipment Configuration	Equipment Function	Component	Component Function
1	Gearbox	G-301	1 × 100%	Transmit 'X' horsepower, while reducing the rotational speed from 'Y' to 'Z' RPM	N/A	
2	Filters	FT-301 A/B	2 × 100%	Filter ambient air at 'X' to remove particulate greater than 'Y' at a maximum pressure drop of 'Z'	N/A	Eliminate unwanted solid elements from the main product
3	Sensors	N/A	N/A	Detect different process parameters such as level, vibration, temperature pressure	N/A	Detect process and equipment operational condition based on physical parameters
4	Logic elements	N/A	N/A	Trigger the safety final element in case of unsafe condition	N/A	Trigger the alarms and actuator in case of unsafe condition

The next step is to define the equipment and component functions, which are described in [Tables 3.34 and 3.35](#). Despite many similar components compared to the pump, the causes of failures are different in some cases, as shown in [Tables 3.36–3.46](#).

### 3.9.6 FLOWLINE FMEA/RBI

The flowline is an important piece of equipment for subsea oil production. Its main function is the transportation of production or injection fluids and linking a subsea structure to another structure or to

**Table 3.35 Compressor Equipment (FMEA Function)**

Failure Mode and Effect Analysis (FMEA)						
FMEA Leader: Dr. Eduardo Calixto			Document: DE-10301-001 Rev02		Date: 13-12-2010	
System: Platform			Subsystem: Compression		Equipment: K301 A/B	
No.	Equipment Number	Equipment Description	Equipment Configuration	Equipment Function	Component	Component Function
1	K-301 A/B	Centrifugal compressor	2 × 100%	Compress a given vapor at a system required rate of 'X' and a differential pressure of 'Y'	O-ring	Avoid fluid turbulence
2					Casing	Protect the impeller and create a chamber for the fluid to be pumped through
3					Coupling	Transmit torque to impeller
4					Impeller	Spin the fluid inside the pump chamber
5					Shaft	Transmit mechanical energy
6					Seal	Prevent external leakage
7					Bearing	Ensure shaft alignment
8					Packing	Control leakage
9					Nozzle	Avoid fluid turbulence
	Blade	Control the inlet air throughout the compressor				
	Diaphragms	Create a barrier between fluids and gases				
	Labyrinth	Prevent external leakage				

**Table 3.36 Compressor System—Gearbox (FMEA/RCM)**

Failure Mode and Effect Analysis (FMEA)													Reliability Centered Maintenance (RCM)					
FMEA Leader: Dr. Eduardo Calixto			Document: DE-10301-001 Rev02			Date: 11-12-2010			RCM Leader: Dr. Eduardo Calixto			Date: 12-12-2010						
System: Platform			Subsystem: Compression – Starting System			Equipment: Gearbox			Component:			Equipment: GA -301		Component:				
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S	R	Mitigate Action	O	S	Risk Post	Task	Type	Frequ ency	Cost	Status	
1	Gearbox (teeth)	Worn out	OP	Improper lubrication	D	High repair cost and process impact (reduced flow)	III	DIII	Preventive maintenance	B	III	BIII	Visual inspection	Sch	3 years	\$	OK	
2			Op	Improper shaft alignment	C		II	CII					N/A	N/A				
3			Op	Normal wear	D	II	DII	N/A	N/A									
4		Fracture	Op	Overload	D	Process impact (reduced flow)	II	DII	N/A					N/A				
5			Man	Wrong manufacture	D		II	DII	N/A	N/A								
6			Abrasive wear	Op	Presence of solid in lubricant		D	II	DII	N/A	N/A							
7	Gearbox (flank)	Worn out	Op	Improper lubrication	D	High repair cost and process impact (reduced flow)	II	DIII	Preventive maintenance	B	III	BIII	Visual inspection	Sch	3 years	\$	OK	
8			Op	Overload	D		II	DII					N/A	N/A				
9	Gear (coupling)	Worn out	OP	Improper shaft alignment	D	Process impact (reduced flow)	II	DII	N/A				N/A					
10			Op	Improper lubrication	D		High repair cost and process impact (reduced flow)	II		DIII	Preventive maintenance	B	III	BIII	Visual inspection	Sch	3 years	\$
																		Sample oil analysis

**Table 3.37 Compressor System—Filter (FMEA/RCM)**

Failure Mode and Effect Analysis (FMEA)													Reliability Centered Maintenance (RCM)					
FMEA Leader: Dr. Eduardo Calixto			Document: DE-10301-001 Rev02			Date: 11-12-2010			RCM Leader: Dr. Eduardo Calixto			Date: 12-12-2010						
System: Platform			Subsystem: Compression – Air Inlet			Equipment: Filters			Component: N/A			Equipment: FT-301 A/B		Component:				
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S	R	Mitigate Action	O	S	Risk Post	Task	Type	Freq uency	Cost	Status	
1	Filter	Worn out	Op	Product out of specification	D	Process impact (reduced flow)	II	DII	N/A									
2			Ins	Wrong installation	C		II	CII	N/A				N/A					
3			Op	Normal wear	D		II	DII	N/A					N/A				
4		Blockage	Op	Overload	D	High internal pressure with equipment damage and process impact (reduced flow)	II	DIII	Define preventive maintenance	B	III	BIII	Monitoring pressure online	Pdm	On-line	\$	OK	
		Abrasive wear	Op	Presence of solid in product	D	Process impact (reduced flow)	II	DII	N/A				N/A					
7		Corrosion	Op	Chemical attacks	D	Air leakage and process impact (reduced flow)	II	DIII	Define preventive maintenance	B	III	BIII	Sample product analysis	Pdm	In-line	\$	OK	
8		Disconnection	Ins	Wrong installation	D		III	DIII	Define procedure to install equipment and perform inspection after installation and maintenance	B	III	BIII	N/A					

**Table 3.38 Compressor System—Control System—Sensor and Controls (FMEA/RCM)**

Failure Mode and Effect Analysis (FMEA)													Reliability Centered Maintenance (RCM)						
FMEA Leader: Dr. Eduardo Calixto			Document: DE-10301-001 Rev02			Date: 13-12-2010			RCM Leader: Dr. Eduardo Calixto			Date: 14-12-2010							
System: Platform			Subsystem: Compression – Control System			Equipment: Sensor and Controls			Component: N/A			Equipment Sensor and controls		Component: N/A					
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S	R	Mitigate Action	O	S	Risk Post	Task	Type	Frequ ency	Cost	Status		
1	Sensor	Lack of signal	OP	External damage	D	Loss of control and possible process impact (reduced flow)	II	DII	N/A				N/A						
2			Ins	Wrong installation	E		II	EII	N/A				N/A						
3			OP	Presence of dust and external element	E		II	EII	N/A					N/A					
4			Op	Overvoltage or temperature			II	DII	N/A						N/A				
5			OP	High vibration	E		II	EII	N/A						N/A				
6			De	Wrong configuration	D		II	DIII	Perform HALT test	B	III	BIII			N/A				
	Disconnection	Ins	Wrong installation	D	II	DII						BIII	N/A						
7	Control	Lack of signal	Op	External damage	D	Loss of control and possible process impact (reduced flow)	II	DII	N/A				N/A						
8			Op	Overvoltage or temperature	D		II	DII	N/A					N/A					
9			OP	High vibration	E		II	EII	N/A					N/A					
10			Op	Wrong signal input	E		II	DII	N/A						N/A				
11		Continuous signal	De	Wrong configuration	D		II	DIII	Perform software test during design	B	III	BIII		N/A					
12		Disconnection	Ins	Wrong installation	D		II	DII	N/A						N/A				

**Table 3.39 O-Ring (FMEA/RCM)**

Failure Mode and Effect Analysis (FMEA)											Reliability Centered Maintenance (RCM)								
FMEA Leader: Dr. Eduardo Calixto				Document: DE-10301- 01 Rev01		Date: 13-12-2010					FMEA Leader: Dr. Eduardo Calixto		Date: 14-12-2010						
System: Platform				Subsystem: Compression		Equipment: K-101 A/B			Component: Casing and Coupling		Equipment: K-101 A/B			Component: O-Ring					
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S	Risk (Pri)	Mitigate Action	O	S	Risk (Post)	Task	Type	Freq uency	Cost	Status		
1	O-ring	Worn out	Op	Normal wear	D	Low flow (compressor less than the required flow rate of 'X' or pressure of 'Y')	I	DI	N/A				N/A						
2			Op	Excessive solids in fluid causing premature wear	D		DI	N/A						N/A					
3			Ins	Impeller misaligned	D		DI	N/A						N/A					
4			Brittle	Overheat caused by lack of cooling or adequate liquid flow	D		DI	N/A						N/A					
5			Deformation	OP	Excessive temperature, pressure or chemical attack		D	DI	N/A					N/A					

**Table 3.40 Casing and Coupling (FMEA/RCM)**

Failure Mode and Effect Analysis (FMEA)												Reliability Centered Maintenance (RCM)						
FMEA Leader: Dr. Eduardo Calixto				Document: DE-10301- 01 Rev01		Date: 13-12-2010				RCM Leader: Dr. Eduardo Calixto		Date: 14-12-2010						
System: Platform				Subsystem: Compression		Equipment: K-101 A/B			Component: Casing and Coupling		Equipment: K-101 A/B		Component: Casing and Coupling					
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S	Risk (Pri)	Mitigate Action	O	S	Risk (Post)	Task	Type	Freq uency	Cost	Status	
6	Casing	Worn out	Op	Normal wear	D	Low flow (compressor less than the required flow rate of 'X' or pressure of 'Y')	I	DI	N/A				N/A					
			Op	Excessive solids in fluid causing premature wear	D			DI	N/A				N/A					
7		Distorted	Op	Excessive pipe strain caused by overload	D					DI	N/A				N/A			
8	Coupling	Worn out	Op	Vibration caused by improper shaft alignment	D	High maintenance cost and low flow (compressors less than the required flow rate of 'X' or pressure of 'Y')	III	DIII	Define preventive maintenance	B	III	BIII	Monitoring vibration analysis	Pdm	On line	\$	Ok	
			Op	Improper lubrication	D	Low flow (compressor less than the required flow rate of 'X' or pressure of 'Y')	II	DII	N/A					N/A				
			Op	Normal wear	D		II	DII	N/A						N/A			



**Table 3.41 Impeller and Shaft (FMEA/RCM)**

Failure Mode and Effect Analysis (FMEA)													Reliability Centered Maintenance (RCM)					
FMEA Leader: Dr. Eduardo Calixto			Document: DE-10301- 01 Rev01			Date: 13-12-2010			RCM Leader: Dr. Eduardo Calixto			Date: 14-12-2010						
System: Platform			Subsystem: Vacuum Distillation			Equipment: P101 A/B			Component: Impeller and Shaft			Equipment: P101 A/B		Component: Impeller				
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S	R	Mitigate Action	O	S	Risk (Post)	Task	Type	Frequency	Cost	Status	
1	Impeller	Worn out	Op	Normal wear	D	High maintenance cost and low flow (compressors less than the required flow rate of 'X' or pressure of 'Y')	II	DII	N/A									
2			Op	Excessive solids in fluid causing premature wear	D		III	DIII	Define preventive maintenance	B	III	BIII	Monitoring product online	Pdm	Online	\$	OK	
3			Op	Higher vibration	D		I	DIII	Define preventive maintenance	B	III	BIII	Monitoring vibration analysis	Pdm	Online	\$	OK	
4		Plugged	Op	Foreign material in process	D		II	DII	N/A				N/A					
5	Impeller	Loose	Op	Excessive backflow	D	Low flow (compressor less than the required flow rate of 'X' or pressure of 'Y')	II	DII	N/A				N/A					
			Op	Incorrect installation	D	Damage to compressor bearings and process impact - low flow (pumps less than the required flow rate of 'X' or pressure of 'Y')	II	DII	N/A				N/A					
6	Shaft	Worn out	Op	Excessive solids in fluid causing premature wear	D	Low flow (pumps less than the required flow rate of 'X' or pressure of 'Y')	III	DIII	Define preventive maintenance	B	III	BIII	Sample fluid analysis	Pdm	Yearly	\$	OK	
			Ins	Incorrect installation	D		II	DIII	Installation procedure	B	III	BIII	Vibration test	Pdm	After installation	\$	OK	
7		Fracture	Op	Normal wear	D		II	DII	N/A				N/A					
		Corrosion	De	Excessive vibration	D	III	DIII	Define preventive maintenance	B	III	BIII	Monitoring vibration analysis	Pdm	Onlin	\$	OK		
				Chemical attacks caused by wrong specification	D	III	DIII	Review the design specification: <b>Action: Design Group</b>	D	II	DII	N/A						



13	Seal	Cracking	De	High friction, heat at the seal faces caused by lack of proper cooling	D	External leakage	II	DII	N/A									
14			Op	High friction, heat at the seal faces caused by excessive pressures or velocity	D		II	DII	N/A									
15		Seal faces deflection	Op	Improper stationary seal face support	D		II	DII	N/A									
16			Op	Operation beyond the pressure limits of seals	D		II	DII	N/A									
17			Op	Inadequate balancing of hydraulic and mechanical load on seal face	D		II	DII	N/A									

**Table 3.43 Bearing (FMEA/RCM)**

Failure Mode and Effect Analysis (FMEA)													Reliability Centered Maintenance (RCM)					
FMEA Leader: Dr. Eduardo Calixto			Document: DE-10301- 01 Rev01			Date: 13-12-2010			RCM Leader: Dr. Eduardo Calixto			Date: 14-12-2010						
System: Distillation Plant			Subsystem: Vacuum Distillation			Equipment: P101 A/B			Component: Bearing			Equipment: P101 A/B		Component: Bearing				
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S	R	Mitigate Action	O	S	Risk Post	Task	Type	Freq uency	Cost	Status	
1	Bearing	Deformation	Ins	Misaligned caused by wrong assembly	E	Low flow (compressor less than the required flow rate of 'X' or pressure of 'Y')	II	EII	N/A									
2			Op	Insufficient or lack of lubrication	D		II	DII	N/A									
3			Op	Overload that causes high vibration	E		III	EIII	Define preventive maintenance	B	II	BII	Monitoring vibration analysis	Pdm	Online	\$	OK	
4		Seizing	De	Wrong bearing material selection	D		II	DII	N/A									
5			Ins	Insufficient clearance caused by wrong assembly	D		II	DII	N/A									
6			Op	Insufficient or lack of lubrication	D		II	DII	N/A									
7			Op	Contamination in lubricant	D		II	DII	N/A									
8			Op	High vibration caused by overload	E		High cost and low flow	III	EIII	Define preventive maintenance	B	II	BII	Monitoring vibration analysis	Pdm	Online	\$	OK
9		Worn out	Op	Overload that causes high vibration	D		Low flow	II	DII	N/A								
10			Op	Lack of lubrication	D		II	DII	N/A									
12			Op	Contamination in lubricant	D		High cost and low flow	III	EIII	Define preventive maintenance	B	II	BII	Monitoring lubricant quality	Pdm	Online	\$	OK

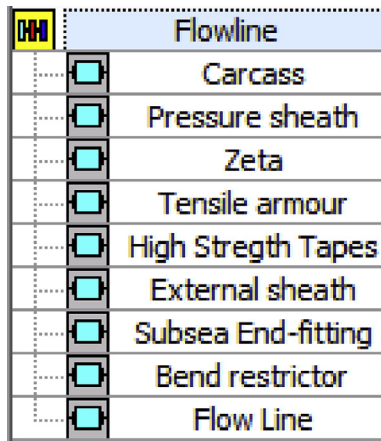


**Table 3.45 Blade (FMEA/RCM)**

Failure Mode and Effect Analysis (FMEA)												Reliability Centered Maintenance (RCM)					
FMEA Leader: Dr. Eduardo Calixto			Document: DE-10301- 01 Rev01			Date: 13-12-2010			RCM Leader: Dr. Eduardo Calixto			Date: 14-12-2010					
System: Platform			Subsystem: Compression			Equipment: K-101 A/B			Component: Packing and Nozzle			Equipment: K-101 A/B		Component: Packing and Nozzle			
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S	R	Mitigate Action	O	S	Risk Post	Task	Type	Freq uency	Cost	Status
1	Blade	Worn out	Ins	Incorrect installation	D	High cost and low flow (compressor less than the required flow rate of 'X' or pressure of 'Y')	II	DII	N/A								
2			Op	Excessive solids in fluid causing premature wear	D		III	DIII	Define preventive maintenance	B	II	BII	Monitoring product quality	Pdm	Online	\$	OK
3			Op	Normal wear	D		II	DII	N/A								
4		Corrosion	Op	Contaminated fluid	D	III	DIII	Define preventive maintenance	B	III	BIII	Monitoring vibration analysis	Pdm	Online	\$	OK	
5		Erosion	Op	High flow velocity	D	II	DII	N/A									
6		Cracking	Op	High vibration caused by overload	D	II	DIII	Define preventive maintenance	B	III	BIII	Monitoring vibration analysis	Pdm	Online	\$	OK	
6	Diaphragm	Fretting wear	Op	Insufficient or lack of lubrication	C	Low flow (compressor less than the required flow rate of 'X' or pressure of 'Y')	II	DII	N/A								
7	Labyrinth	Corrosion	Oü	Contaminated fluid	C		II	DII	N/A								

**Table 3.46 Flowline Equipment FMEA Function**

Failure Mode and Effect Analysis (FMEA)						
FMEA Leader: Dr. Eduardo Calixto			Document: DE-500510-001 Rev01		Date: 30-01-2006	
System: Subsea			Subsystem: Subsea Flowline		Equipment: FL - 002	
No.	Equipment Number	Equipment Description	Equipment Configuration	Equipment Function	Component	Component Function
1	FL-02	Flowline	10 × 100%	Transportation of production or injection fluids and linking a subsea structure to another structure or to a production facility	Carcass	Provide strength against external hydrostatic pressure and mechanical protection
2					Pressure sheath	Provide internal leak proofs
3					Zeta	To sustain the radial load caused by internal pressure and to protect against hydrostatic collapse
4					Tensile armour	Withstand axial load
5					High strength tapes	Resist reverse end cap effect
6					External sheath	Isolate and protect internal layers from the external environment
7					Bend restrictor	Prevent overbend on flexible flowline near tie in location
8					Flowline	Transportation of production or injection fluids and linking a subsea structure to another structure or to a production facility



**FIGURE 3.48**

Flowline equipment list hierarchy.

a production facility. Concerning unsafe failures, rather than cost, external leakage may cause a serious environmental impact, therefore it is necessary to define preventive maintenance, inspection, and NDT to prevent such failures. Therefore the RBI method is more appropriate and will focus on defining inspection and NDT to prevent unsafe failures, such as corrosion, which can lead to an oil spill on the water.

Concerning the RBI methodology, all unsafe failures will be assessed based on FMEA in this case, and a similar risk matrix applied to another case study will be considered here.

Because of the impact on the environment and safety in case of unsafe failure, severity and risk will take into account the four classifications described in the risk matrix. Fig. 3.48 and Table 3.46 show the flowline components list and the FMEA function, respectively.

Based on the previous description, Tables 3.47 and 3.48 show the FMEA and Tables 3.49 and 3.50 show the RBI, respectively.

The next chapter will discuss RAM analysis methodology with several examples and applications. To predict system operational availability and define the critical equipment it is recommended that RAM analysis be performed, which asks questions such as:

- What is system, subsystem, and equipment availability?
- What is system, subsystem, and equipment reliability?
- What is system, subsystem, and equipment maintainability?
- Which subsystem and equipment impacts more on system availability?
- Which subsystem and equipment impacts more in system reliability?
- How much do stock policies impact on system availability?
- How much do maintenance and inspection policies impact on system availability?
- What is the impact of redundancy on system availability?
- What impact does equipment reliability have on system availability?



**Table 3.47 Flowline Equipment FMEA Function**

Failure Mode and Effect Analysis (FMEA)																									
FMEA Leader: Dr. Eduardo Calixto			Document: DE-500510-001 Rev01				Date: 30-01-2006																		
System: Subsea			Subsystem: Subsea Flowline				Equipment: FL-01							Component: Carcass, Pressure Sheath, Zeta, Tensile Armor, High Strength Tapes											
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S P	S I	S E	S S	R P	R I	R E	R S	Mitigate Action	O	S P	S I	S E	S S	R P	R I	R E	R S	
1	Carcass	Corrosion	Op	Presence of H2S and high temperature	D	Reduction in carcass thickness	I	III	I	I	DI	DIII	DI	DI	Define preventive maintenance										
2		Erosion	Op	High flow velocity	D		I	III	I	I	DI	DIII	DI	DI	Process control	B	I	III	I	I	BI	BIII	BI	BI	
3	Pressure sheath	Blistering	Op	High temperature and pressure	D	Collapse and leakage	I	II	I	I	DI	DII	DI	DI	N/A	B	I	III	I	I	BI	BIII	BI	BI	
4	Zeta	Annulus corrosion	OP	Presence of H2S	D	Hydrostatic collapse	I	III	I	I	DI	DIII	DI	DI	Define preventive maintenance	B	I	III	I	I	BI	BIII	BI	BI	
5		Overbending	Ins	Human error during installation	E	Unlocking and bursting of pipe	I	III	II	I	EI	EIII	EI	EI	Define installation procedure	B	I	III	I	I	BI	BIII	BI	BI	
6	Tensile armor	Annulus corrosion	Op	Presence of H2S and high temperature	D	Reduction in thickness	I	III	I	I	DI	DIII	DI	DI	Define preventive maintenance	B	I	III	I	I	BI	BIII	BI	BI	
7	High strength tapes	Annulus corrosion	Op	Presence of H2S and high temperature	D	Early wear-out	I	III	I	I	DI	DIII	DI	DI	Define preventive maintenance	B	I	III	I	I	BI	BIII	BI	BI	

**Table 3.48 Flowline Equipment FMEA—cont'd**

Failure Mode and Effect Analysis (FMEA)																								
FMEA Leader: Dr. Eduardo Calixto			Document: DE-100210-001 Rev01					Date: 25-05-2008																
System: Subsea			Subsystem: Subsea Flowline					Equipment: FL-01					Component: External Sheath, Subsea End Fitting, Bend Restrictor, Flowline											
No.	Component	Failure Mode	Phase	Cause	O	Consequence	S P	S I	S E	S S	R P	R I	R E	R S	Mitigate Action	O	S P	S I	S E	S S	R P	R I	R E	R S
1	External sheath	Tear	Op	Dropped objects	D	Ingress of seawater in annulus	I	III	I	I	DI	DIII	DI	DI	Define preventive maintenance	B	I	III	I	I	BI	BIII	BI	BI
2			Op	Human error during installation	E		I	III	II	I	EI	EIII	EI	EI	Define installation procedure	B	I	III	I	I	BI	BIII	BI	BI
3		Overbending	Ins	Human error during installation	E	Damage to external sheath	I	III	II	I	EI	EIII	EI	EI	Define installation procedure	B	I	III	I	I	BI	BIII	BI	BI
4		Rupture	Op	Barge impact	E		I	III	II	I	EI	EIII	EI	EI	Monitoring vessel	B	I	III	I	I	BI	BIII	BI	BI
5	Subsea end fitting	Leakage	Ins	Human error during installation	E	Loss of containment	I	III	II	I	EI	EIII	EIII	Define installation procedure	B	I	III	I	I	BI	BIII	BIII	BIII	
6		External corrosion	Op	Damage to coating	D	End fitting	I	III	I	I	DI	DIII	DI	DI	Define preventive maintenance	B	I	III	I	I	BI	BIII	BI	BI
7	Bend restrictor	Early wear our	De/Ma	Material defect or design flaw	D	Low flow and high pressure	I	II	I	I	DI	DII	DI	DI	N/A									
8	Flowline	Blockage	Op	Formation of hydrates, wax, gel, asphaltene		Low flow and high pressure	I	III	I	I	DI	DIII	DI	DI	Define preventive maintenance	B	I	III	I	I	BI	BIII	BI	BI

**Table 3.49 Flowline Equipment RBI**

Risk Based Inspection (RBI)												
RBI Leader: Dr. Eduardo Calixto		Document: DE-500510-001 Rev01				Date: 31-01-2006						
System: Subsea			Subsystem: Subsea Flowline			Equipment: FL-01			Component: Carcass, Pressure Sheath, Zeta, Tensile Armor, High Strength Tapes			
No.	Component	Failure Mode	Phase	Cause	O	Consequence	Mitigate Action	Inspection and Test Task	Type	Frequency	Cost	Status
1	Carcass	Corrosion	Op	Presence of H2S and high temperature	D	Reduction in carcass thickness	Define preventive inspection and NDT	Monitoring of gas temperature	Pdm	Online	\$	OK
		Erosion	Op	High flow velocity	D			Process control	N/A	OR	1 year	\$
2												
3	Pressure sheath	Blistering	Op	High temperature and pressure	D	Collapse and leakage	N/A	N/A				
4	Zeta	Annulus corrosion	OP	Presence of H2S	D	Hydrostatic collapse	Define preventive inspection and NDT	Monitoring of gas temperature	Pdm	Online	\$	OK
		Overbending	Ins	Human error during installation	E	Unlocking and bursting of pipe		Define installation procedure	N/A	OR	1 year	\$
5												
6	Tensile armor	Annulus corrosion	Op	Presence of H2S and high temperature	D	Reduction in thickness	Define preventive inspection and NDT	Monitoring of gas temperature	Pdm	Online	\$	OK
								Gas sampling for CO2	OR	1 year	\$	OK
7	High strength tapes	Annulus corrosion	Op	Presence of H2S and high temperature	D	Early wear-out	Define preventive inspection and NDT	Monitoring of gas temperature	Pdm	Online	\$	OK
								Gas sampling for CO2	OR	1 year	\$	OK

**Table 3.50 Flowline Equipment RBI**

Risk Based Inspection (RBI)												
RBI Leader: Dr. Eduardo Calixto			Document: DE-500510-001 Rev01				Date: 31-01-2006					
System: Subsea			Subsystem: Subsea Flowline				Equipment: FL-01			Component: Carcass, Pressure Sheath, Zeta, Tensile Armor, High Strength Tapes		
No.	Component	Failure Mode	Phase	Cause	O	Consequence	Mitigate Action	Inspection and Test Task	Type	Frequency	Cost	Status
1	External sheath	Tear	Op	Dropped objects	D	Ingress of seawater in annulus	Define preventive maintenance	ROV inspection	Pdm	6 months	\$	OK
2			Op	Human error during installation	E		Define installation procedure	N/A				
3		Overbending	Ins	Human error during installation	E	Damage to external sheath	Define installation procedure	N/A				
4		Rupture	Op	Barge impact	E		Monitoring vessel	N/A				
5	Subsea end fitting	Leakage	Ins	Human error during installation	E	Loss of containment	Define installation procedure	N/A				
6		External corrosion	Op	Damage to coating	D	End fitting	Define preventive maintenance	ROV inspection	Pdm	6 months	\$	OK
7	Bend restrictor	Early wear-out	De/Ma	Material defect or design flaw	D	Low flow and high pressure	N/A					
8	Flowline	Blockage	Op	Formation of hydrates, wax, gel, asphaltene	D	Low flow and high pressure	Define preventive maintenance	Monitoring of operating temperature and pressure in flow	OR	Daily	\$	OK

- Which equipment must be improved to improve system availability?
- How is it possible to optimize system operational availability and minimize life cycle cost based on optimal preventive maintenance and inspection interval as well as optimal spare part level?

When RAM analysis is performed first, then other methods such as FMEA, RCM, ReBI, and ReGBI provide the opportunity to reliability engineers and maintenance professionals to focus on the real problem. In other words, to focus on more critical subsystems and equipment. This saves time, which is a critical resource for maintenance, operation, and reliability professionals.

# RELIABILITY, AVAILABILITY, AND MAINTAINABILITY (RAM ANALYSIS)

## CHAPTER OUTLINE

<b>4.1 RAM Analysis Introduction .....</b>	<b>272</b>
4.1.1 Scope Definition.....	274
4.1.2 Data Failure and Repair Analysis .....	275
4.1.3 Modeling and Simulation .....	277
4.1.4 Sensitivity Analysis.....	280
4.1.5 Conclusion and Reports .....	281
<b>4.2 Modeling and Simulation .....</b>	<b>283</b>
4.2.1 Reliability Block Diagram.....	283
<i>DEA (Diethylamine) System—Assumption List to RBD Model.....</i>	<i>287</i>
4.2.2 Markov Chain Methodology.....	288
4.2.3 Simulation.....	291
<i>Case 1.....</i>	<i>293</i>
<i>Case 2.....</i>	<i>294</i>
<i>Case 3.....</i>	<i>295</i>
4.2.4 Reliability and Availability Performance Index.....	299
<i>Percentage Losses Index .....</i>	<i>299</i>
<i>Failure Rank Index .....</i>	<i>300</i>
<i>Downtime Event Critical Index.....</i>	<i>301</i>
<i>Availability Rank Index.....</i>	<i>302</i>
<i>Reliability Importance Index.....</i>	<i>303</i>
<i>Availability Importance Index.....</i>	<i>304</i>
<i>Utilization Index.....</i>	<i>305</i>
<b>4.3 Sensitivity Analysis: Redundancy Policies, Maintenance Policies, Stock Policies, and Logistics .....</b>	<b>305</b>
4.3.1 Redundancy Policies .....	306
4.3.2 Maintenance Policies.....	309
4.3.3 A General Renovation Process: Kijima Models I and II.....	313
4.3.4 Stock Policy.....	318
4.3.5 Logistics.....	320
<b>4.4 Improvement Allocation Based on Availability .....</b>	<b>324</b>
<b>4.5 Performance Optimization .....</b>	<b>328</b>

<b>4.6 Case Studies.....</b>	<b>333</b>
4.6.1 Sensibility Analysis in Critical Equipment: The Distillation Plant Study Case in the Brazilian Oil and Gas Industry .....	334
<i>Failure and Repair Data Analysis</i> .....	335
<i>Modeling</i> .....	335
<i>Simulation Subsystem</i> .....	344
<i>Critical Analysis</i> .....	345
<i>Sensitivity Analysis</i> .....	347
<i>Conclusion</i> .....	348
4.6.2 Systems Availability Enhancement Methodology: A Refinery Hydrotreating Unit Case Study.....	348
<i>Failure and Repair Data Analysis</i> .....	349
<i>Optimization (Minimum Availability Target)</i> .....	349
<i>The Hydrodesulfurization Process</i> .....	350
<i>Modeling</i> .....	350
<i>Simulation and Optimization</i> .....	351
<i>Optimization of HDT</i> .....	357
<i>Conclusions</i> .....	357
4.6.3 The Nonlinear Optimization Methodology Model: The Refinery Plant Availability Optimization Case Study .....	359
<i>Failure and Repair Data Analysis</i> .....	359
<i>Modeling</i> .....	359
<i>Simulation</i> .....	363
<i>Critical Analysis</i> .....	363
<i>Optimization</i> .....	365
<i>Conclusion</i> .....	371
4.6.4 CENPES II Project Reliability Analysis Case Study .....	372
<i>System Characteristics</i> .....	372
<i>Data Analysis</i> .....	373
<i>System Modeling and Simulation</i> .....	375
<i>Optimization</i> .....	379
<i>Efficiency Cost Analysis</i> .....	384
<i>Conclusions</i> .....	384
4.6.5 The Operational Effects in Availability: Thermal Cracking Plant RAM Analysis Case Study .....	385
<i>Failure and Repair Data Analysis</i> .....	385
<i>Modeling</i> .....	386
<i>Simulation</i> .....	392
<i>Critical Analysis</i> .....	392
<i>Sensibility Analysis</i> .....	397
<i>Conclusion</i> .....	398
4.6.6 Partial Availability Based on System Age: The Drill Facility System Case Study.....	399
<i>Introduction</i> .....	399

<i>Partial Availability</i> .....	399
<i>Partial Availability Case Study</i> .....	404
<i>Conclusions</i> .....	415
4.6.7 High-Performance System Requires Improvements? The Compressor's Optimum Replacement Time Case Study.....	416
<i>Failure and Repair Data Analysis</i> .....	416
<i>Modeling</i> .....	416
<i>Simulation</i> .....	421
<i>Critical Analysis</i> .....	421
<i>Sensitivity Analysis</i> .....	422
<i>Conclusion</i> .....	426
4.6.8 RAM + L Analysis: Refinery Case Study.....	427
<i>Failure and Repair Data Analysis</i> .....	428
<i>System Modeling</i> .....	429
<i>Logistic Resources</i> .....	436
<i>Systems Simulation</i> .....	439
<i>Critical Analysis and Improvement Actions</i> .....	441
<i>RAM + L Simulation</i> .....	443
<i>Conclusions</i> .....	443
4.6.9 RAM Analysis Applied to Decommissioning Phase: Comparison and Assessment of Different Methods to Predict Future Failures.....	445
<i>Introduction</i> .....	445
<i>RAM Analysis in Decommissioning Phase</i> .....	446
<i>Reliability Growth Analysis</i> .....	448
<i>General Renewal Process</i> .....	449
<i>Lifetime Data Analysis</i> .....	450
<i>Comparing Different Methods</i> .....	453
<i>RAM Analysis in the Decommissioning Phase Case Study</i> .....	454
<i>Conclusion</i> .....	457
4.6.10 RAM Analysis During the Design Phase: The Best Platform Offshore Configuration Case Study.....	460
<i>Introduction</i> .....	460
<i>Methodology</i> .....	461
<i>Lifetime Data Analysis</i> .....	461
<i>Modeling</i> .....	462
<i>Simulation</i> .....	465
<i>Criticality Analysis</i> .....	465
<i>Sensitivity Analysis</i> .....	465
<i>Conclusion</i> .....	469
<b>References</b> .....	<b>469</b>
<b>Bibliography</b> .....	<b>470</b>



## 4.1 RAM ANALYSIS INTRODUCTION

We have discussed many approaches to working with failure data and making decisions based on qualitative or quantitative reliability engineering methodologies. In Chapter 3 the examples showed how it is possible to assess the whole system by failure mode and effects analysis (FMEA) or reliability-centered maintenance (RCM) methodologies. However, even in these cases, it is not possible to define which system, subsystems, and equipment impacts system availability. However, reliability, availability, and maintainability (RAM) analysis enables you to quantitatively define:

- System availability and reliability;
- Subsystem and equipment, which impact more on system availability;
- Stock policy impact on system availability;
- Maintenance policy impact on system availability;
- Logistic impact on system availability;
- Redundancy impact on system availability;
- Maintenance, inspection, and spare part optimization.

Applying RAM analysis it is possible to find out quantitatively system availability, reliability, and equipment maintainability and which critical subsystems and equipment influence system performance the most. RAM analysis can be performed for a single piece of equipment with several components or for a complex system with several pieces of equipment.

In this way, if a system is not achieving the availability target, the critical equipment will be identified and improvement recommendations can be tested by simulation to predict system availability. This is a remarkable point in RAM analysis results because in many cases RAM analysis shows that it is not necessary to improve all equipment availability to achieve the system availability target, only the most critical equipment.

As discussed, reliability is the probability of one piece of equipment, product, or service being successful until a specific time. Maintainability is the probability of equipment being repaired in a specific period of time.

In addition to reliability and maintainability, availability also includes:

- Punctual availability;
- Average availability;
- Permanent regime availability;
- Inherent availability;
- Achieved availability;
- Operational availability.

*Punctual availability* is the probability of a piece of equipment, subsystem, or system being available for a specific time  $t$ , represented by:

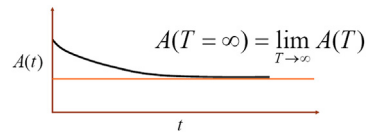
$$A(t) = R(t) + \int_0^t R(t-u)m(u)du$$

where  $R(t)$  = reliability,  $R(t-u)$  = probability of corrective action being performed since failure occurred, and  $m(u)$  = renewal density function.

*Average availability* is the availability average over time, represented by:

$$\overline{A(T)} = \frac{1}{T} \int_0^T A(t) dt$$

*Permanent regime availability* is the availability value when time goes to infinity, represented by:



*Operational availability* is the percentage of total time that a piece of equipment, subsystem, or system is available, represented by:

$$A_o = \frac{\text{Uptime}}{\text{Total operating cycle time}}$$

or:

$$D(t) = \frac{\sum_{i=1}^n t_i}{\sum_{i=1}^n T_i}$$

where  $t_i$  = real time in period  $I$  when the system is working and  $T_i$  = nominal time in period  $i$ .

*Inherent availability* is the operational availability that considers only corrective maintenance as downtime, represented by:

$$A_i = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$$

*Achieved availability* is the operational availability that considers preventive and corrective maintenance as downtime, represented by:

$$A_A = \frac{\text{MTBM}}{\text{MTBM} + \overline{M}}$$

where  $\text{MTBM}$  = mean time between maintenance and  $\overline{M}$  = preventive and corrective downtime.

Despite the many different availability concepts, operational availability is one of the most useful for assessing system efficiency. Inherent and achieved availability concepts are most often used by maintenance teams, and average operational availability is most often used by reliability professionals in software simulations, as will be discussed in [Section 4.2](#).

From a methodological point of view, RAM analysis is generally divided into failure and repair data analysis and modeling and simulation. Keep in mind that with RAM analysis, failure data is associated with equipment failure modes. The procurement of repair and failure data considers only critical failure modes that cause equipment unavailability.

RAM analysis methodology can be described step by step. First, the system is modeled considering failure and repair data and later is simulated to evaluate the results. Then, improvement solutions are proposed. Based on such considerations, to conduct RAM analysis methodology you must define the scope, perform repair and failure data analysis, model the system reliability block diagram (RBD),

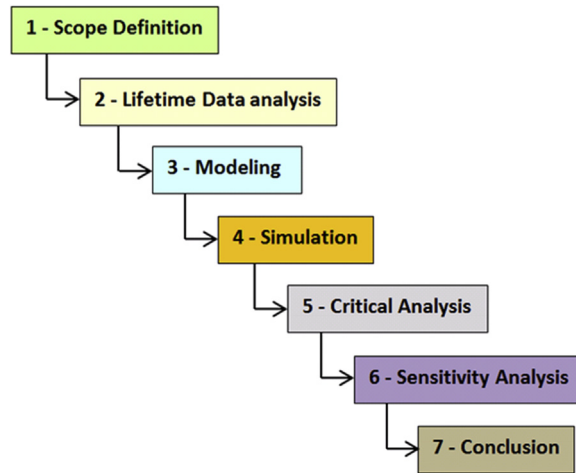


FIGURE 4.1

RAM analysis methodology steps.

conduct direct system simulation, perform critical system analysis, perform system sensitivity analysis, and then draw conclusions. RAM analysis methodology is shown in Fig. 4.1.

#### 4.1.1 SCOPE DEFINITION

Scope definition is critical and the first step of RAM analysis. Scope is defined based on the analysis goal, time available, and customer requirements. If the scope is poorly defined, the time needed to perform analysis will be higher and the final results will probably not be sufficient for the customer. Be careful not to underestimate a pivotal cause of poor performance. Sometimes important system vulnerabilities are not analyzed adequately, or the focus of the analysis changes and such vulnerabilities are not taken into account in RAM analysis. If that happens, to regard such vulnerabilities (eg, the effects of other plants and logistics issues) much more time than defined in the scope phase will be required to include such vulnerabilities in RAM analysis. If that happens, much more time than necessary will be required to conduct RAM analysis.

To prevent some of these problems from occurring, it is best to organize a kick-off meeting with all professionals taking part in the RAM analysis. The objectives of this meeting are:

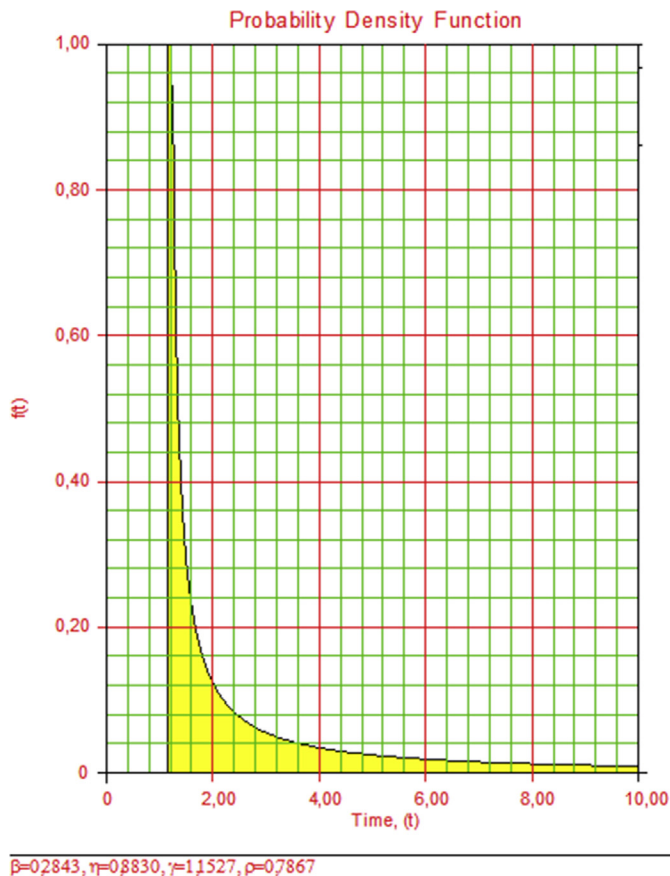
- To present the objectives, goals, and expectations of the project to the team;
- To define responsibilities;
- To explain necessary information for performing the analysis;
- To compile a checklist of each task and associated deadlines;
- To follow up and control RAM analysis phases, it is a good practice to plan meetings every one or two phases to guarantee that RAM analysis is being conducted with all information that all resources required for each phase are implemented and to keep people involved directly or indirectly with RAM analysis.

### 4.1.2 DATA FAILURE AND REPAIR ANALYSIS

Seeking to ensure the accurate representation of data, maintenance, operation, process, and reliability professionals with knowledge of such systems take part in this phase and a quantitative analysis of failure and repair data is performed (life cycle analysis).

A critical equipment analysis of the causes of system unavailability and the related critical failure modes is also performed, standardizing all equipment failure modes. In some cases, one failure mode will have different names in two or more reports and that can make it difficult to understand historical failure data, which may influence failure and repair data analysis.

The historical failure and repair data must be taken into account to create equipment probability density functions (PDFs). The example in Fig. 4.2 shows a coke formation PDF in the furnace of a distillation plant.



**FIGURE 4.2**

Furnace PDF.

**Table 4.1 Quantitative Failure and Repair Data**

TAG	Failure Mode	Failure Time (year)				Repair Time (hours)		
		Variables (PDF)				Variables (PDF)		
F-01 A	Coke formation	Normal		$\mu$ 4.95	$\rho$ 2.66	Normal	$\mu$ 420	$\rho$ 60
	Incrustation	Weibull	$\beta$ 0.51	$\eta$ 1.05	$\gamma$ 4.05	Normal	$\mu$ 420	$\rho$ 60
	Other failures	Exponential Bi p		$\lambda$ 0.28	$\gamma$ 3.22	Normal	$\mu$ 420	$\rho$ 60
F-01 B	Coke formation	Normal		$\mu$ 5.23	$\rho$ 2.55	Normal	$\mu$ 420	$\rho$ 60
	Other failures	Exponential Bi p		$\lambda$ 0.29	$\gamma$ 4.07	Normal	$\mu$ 420	$\rho$ 60

TAG, used for equipment identification; Bi p, bi-parametric.

When historical failure data is available the equipment failure data is treated statically to define the PDF that best fits the historical failure data, and it is advisable to have software for such analysis (eg, Weibull++ 7, Statistica, Care, Minitab, and others). For example, Table 4.1 shows examples of thermal cracking furnace failure modes, with failure and repair time PDF parameters.

When there is no failure data available a qualitative analysis is performed with maintenance professionals. In this case an equipment failure mode analysis for occurrence over time is conducted where PDF parameters for each failure mode are qualitatively defined. Most of the time only failures that cause downtime in the system are considered.

The other option when no historical failure data is available is to define a triangular or rectangular function to represent failure modes, labeled as pessimistic, most probable, and optimistic times, depending on each failure and repair time. This approach is better when applied to repair time PDFs, because in many cases repair time on reports also comprises logistic time as delayed time to deliver a component or delayed time to purchase such a component that was not in stock. In addition, in many cases there are doubts among specialists about repair time, and to discern what is being considered as maintenance activity it is good practice to describe maintenance activity steps as shown in Table 4.2.

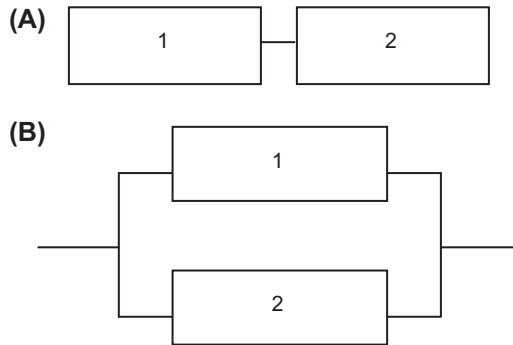
Table 4.2 describes all the activities performed when the vessel is under maintenance. In corrective maintenance, even though equipment is shut down, there are other components (eg, pipelines and valves) that must be stopped to perform safety maintenance. The other steps are also described, and in the second and third columns the time required to perform the activity is given. In the second column the optimistic times are given, and in the third column the pessimist times. Optimistic and pessimistic times give the best and worse failure cases, respectively. Using these values it is possible to use a rectangular PDF, normal PDF, or triangular PDF. In a rectangular PDF the two extreme values are 89 and 148 hours. Such methodology can also be used to estimate other parameter distributions for other PDFs such as lognormal or normal. It is important to note that repair time characteristics are specific to each maintenance team, and it is best not to use repair times from different maintenance teams, unless when reviewed by the maintenance team.

Vessel	Corrosion (hours)	
	Optimistic Time	Pessimistic Time
Stop equipment	12	24
Purge	10	16
Equipment prepared for maintenance	4	6
Preliminary hazard analysis	24	48
Scaffold	6	8
Isolate equipment	4	6
Open equipment	3	6
Inspection	8	8
Repair	8	10
Inspection	4	4
Remove equipment isolation	3	6
Close equipment	3	6
Repair total time	89	148

The failure and repair data analysis is critical to RAM analysis results, and time for this analysis must be allocated to guarantee RAM analysis quality. Since it is difficult and sometimes boring, in many cases there is not enough time dedicated to failure and repair time data analysis and many professionals just move on to the modeling and simulation phase in RAM analysis because it is more exciting. The modeling and simulation phase is more interesting because they allow professionals to work with software and have the availability results. However, in many cases, looking into system availability results it is possible to realize that there is something wrong, and most of the time, failure or repair time was underestimated or overestimated. When underestimated, actions will be proposed to achieve the system availability target, but often more actions than actually needed will be recommended, which means spending more money than necessary. However, when overestimated, system availability results are higher than what is actually expected, and because of this, no improvement action will be proposed to improve system availability.

### 4.1.3 MODELING AND SIMULATION

To define system and subsystems operational availability based on simulation the equipment failure and repair PDF parameters must be input into a system RBD and then simulated. To define a system RBD it is necessary to delimit the system's boundaries prior to performing the analysis. In such cases there will be an evaluation of subsystems, equipment, and components of which the failures represent impacts on system availability, or, in other words, loss of production. To create an RBD it is necessary to define a logic effect for any equipment in the system.



**FIGURE 4.3**  
System block diagram (different equipment).

This means what type of effects equipment unavailability causes in the system. When one piece of equipment fails and causes system loss of production or unavailability, such system is the model in the series. However, if two or more pieces of equipment fail, such equipment is modeled in a parallel block, and the whole parallel block is in series with the other blocks. As a result there is a set of blocks in series and in parallel, as illustrated in Fig. 4.3. Thus it is necessary to set up model equipment using block diagram methodology and be familiar with the production flow sheet details that influence losses in productivity.

In case A, system reliability is represented in series and is described mathematically by:

$$R(T) = R1(T) \times R2(T)$$

In case B, system reliability is represented in parallel and is described mathematically by:

$$R(T) = 1 - ((1 - R1(T)) \times (1 - R2(T)))$$

For identical equipment, system reliability, which includes  $n$  blocks in series, can be represented by:

$$R_s(T) = \prod_{i=1}^n R_i(t) = R(t)^n$$

where  $n$  = number of blocks.

In case  $n$ , identical parallel blocks and system availability requires  $k$  of  $n$  blocks at the same time. The system reliability can be represented by:

$$R_s(k, n, R) = \sum_{r=k}^n \binom{n}{r} R^r (1 - R)^{n-r}$$

where  $k$  = number of parallel blocks required,  $n$  = number of parallel blocks, and  $R$  = reliability.

This configuration uses independent effects. When dependent effects in block configuration are considered, when one parallel block (equipment) failure affects the other block (equipment) life cycle, a load-sharing model can be used to represent such a configuration by accelerated test models,

depending on the failure effects. In mechanical degradation, for example, the inverse power law model can be used:

$$t_V = \frac{1}{k \times V^n}$$

where  $t_V$  is life under stress conditions,  $N$  = stressor factor, which describes load stress effect in equipment life,  $k$  = constant, which depends on test conditions, and  $V$  = stress level.

In doing so it is possible to know the reliability of such a system when one component (block 1) is out and the others (block 2) are under the load-sharing effect. For a system with two components, for example, the load-sharing effect can also be described by:

$$R(t, L) = R_1(t, L_1) \times R_2(t, L_2) + \int_0^t f_1(x, L_1) \times R_2(x, L_2) \times \left( \frac{R_2(t_{1e} + (t - x), L)}{R_2(t_{1e}, L)} \right) dx \\ + \int_0^t f_2(x, L_2) \times R_1(x, L_1) \times \left( \frac{R_1(t_{2e} + (t - x), L)}{R_1(t_{2e}, L)} \right) dx$$

where  $L$  = total load,  $L_1$  = part of total load that block 1 supports when both blocks are working,  $L_2$  = part of total load that block 2 supports when both blocks are working,  $P_1$  = percentage of load that block 1 supports to total load when both blocks are working,  $P_2$  = percentage load that block 2 supports to total load when both blocks are working,  $t_{1e}$  = the equivalent time for block 1 if it had been operating at  $L$  instead of  $L_1$ ,  $t_{2e}$  = the equivalent time for block 2 if it had been operating at  $L$  instead of  $L_2$ , and:

$$L_1 = P_1 S$$

$$L_2 = P_2 S$$

The other parallel configuration with independent effect is standby. In such a configuration, one block is active and the other in parallel is inactive. Whenever an active block fails the inactive block takes its place to avoid system unavailability. An example of such a configuration is pumps that are projected in so many processes in standby parallel configuration. Such configuration is mathematically represented by:

$$R(t) = R_1(t) + \int_0^t f_1(x) \cdot R_{2,\text{inactive}} \cdot \frac{R_{2,\text{active}}(t_2 + t - x)}{R_{2,\text{active}}(t_2)} dx$$

where  $R_1(t)$  = reliability of active block,  $f_1(t)$  = PDF of active block,  $R_{2,\text{inactive}}(t)$  = reliability of standby block when active block is operating,  $R_{2,\text{active}}(t)$  = reliability of standby block when active block is not operating, and  $t_2$  = standby operating time.

If we consider the effect of change from active block to standby block, which is called the switch effect (like a switch in an electrical system), we have:

$$R(t) = R_1(t) + \int_0^t f_1(x) \cdot R_{2,\text{inactive}} \cdot \frac{R_{2,\text{active}}(t_2 + t - x)}{R_{2,\text{active}}(t_2)} \cdot R_{\text{sc},\text{inactive}}(x) \cdot R_{\text{sc},\text{required}}(x) dx$$



where  $R_{sc,inactive}(t)$  = reliability of switch on standby condition and  $R_{sc,required}(t)$  = reliability of switch when required to operate.

When using software to simulate the system the calculations are performed automatically because of the complexity and time required to perform them.

Series and parallel block concepts can also be applied to system availability. Thus if there is a system with equipment that is represented by blocks in series or in a parallel system, availabilities will be represented as shown in Fig. 4.1, for cases A and B, respectively:

In case A, availability is represented in series and is described mathematically by:

$$A(T) = A1(T) \times A2(T)$$

In case B, availability is represented in parallel and is described mathematically by:

$$A(T) = 1 - ((1 - A1(T)) \times (1 - A2(T)))$$

When the system is configured by blocks in series the system reliability will be equal to or lower than the lowest reliability block value. This is one of the most important concepts in RAM analysis, because with blocks in series the lowest availability will always be the most critical to system availability and the first to be improved. In addition, when improving the system availability to achieve the system availability target, in many cases, more than one equipment performance (availability) must be improved.

To obtain the availability results after modeling the system in an RBD it is necessary to use a recognized approach such as Monte Carlo simulation. Such a method allows data to be created based on the PDFs. For example, having a Weibull 2P ( $\beta, \eta$ ), the following equation is used:

$$T = n\{-\ln[U]\}^{\frac{1}{\beta}}$$

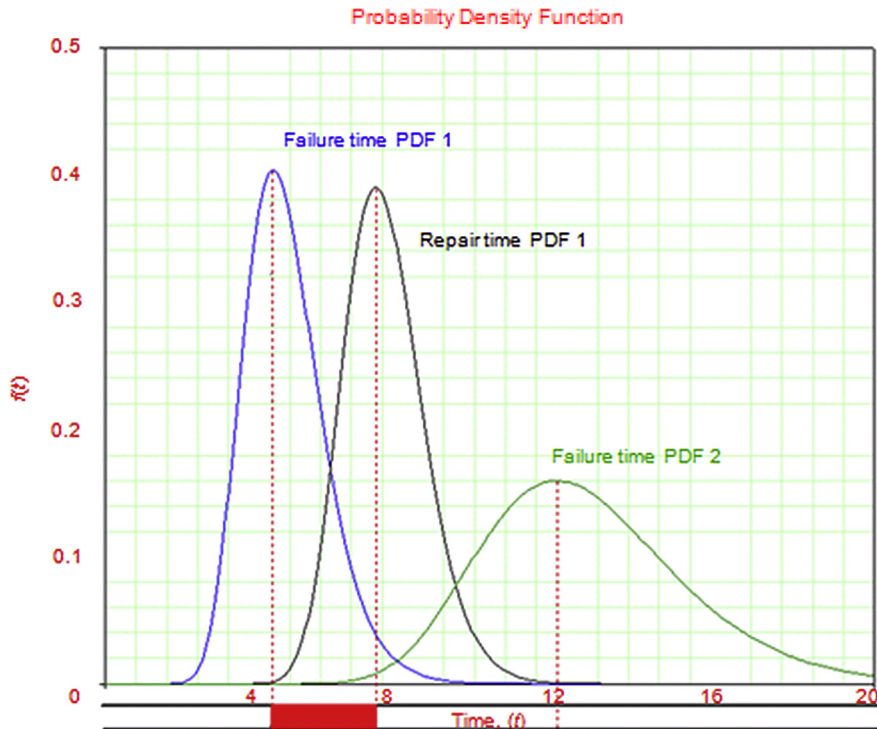
where  $U$  = random number between 0 and 1 and  $T$  = time.

When simulating a whole system, each block that represents one specific piece of equipment will have one PDF for failure times and another for repair time. In this way, Monte Carlo simulation will proceed with failures over simulation time for all block PDFs (failure and repair). In doing so, when a block fails and it is in series in the RBD, the unavailability will be counted in the system for failure and repair duration over simulation time. Simulation time depends on how long the system operates based on time established. Fig. 4.4 shows the effect of block unavailability on system availability.

In Fig. 4.4, regarding time in hours, the system operates until the first failure time ( $t = 4$  hours) and takes around 4 hours to be repaired, and the second failure occurs at 12 hours. There are PDFs to describe failure and repair, and Monte Carlo simulation defines the values of failure time and repair time to be considered. From a system availability point of view, regarding the system operating 12 hours, it means before the second failure occurs, operational system availability will be 66% because the system was unavailable 4 hours of the total 12 hours ( $8/12 = 0.66$ ). In more complex cases there are many blocks that can affect system availability over time and this is calculated based on Monte Carlo simulation.

#### 4.1.4 SENSITIVITY ANALYSIS

The main objective of RAM analysis is to find out system availability and identify the critical equipment that influences system unavailability. In addition, other analysis might be conducted to check system vulnerabilities or find opportunities for improvement. Regarding vulnerabilities, sensitivity analysis is a good approach to, for example, consider if there are influences of other plant



**FIGURE 4.4**

Block availability.

facilities in main system availability. The electric system, water system, and vapor system have in most cases high influence in plant availability in case of unavailability in the oil and gas industry. In so many cases, such facility availability is not taken into account in the system RAM analysis. Another important point to be considered in system vulnerability is logistic issues, which may also affect main system availability.

On the other hand, improvement opportunities arise like define stock policies, maintenance policies, number of redundancies, and reduce numbers of equipment in systems. Actually, RAM analysis is a good opportunity to test system configuration because it is possible to regard different assumptions in RBD and simulate to find out which impact it has on system availability. Consequently, RAM analysis is a good tool to support decisions in projects and operating enterprise phases.

#### 4.1.5 CONCLUSION AND REPORTS

Despite being a powerful tool to support decisions, RAM analysis results and recommendations must be evaluated and supported by management to achieve objectives to maintain or improve system availability. Compared to other tools, RAM analysis is more complex for most people because of the complex mathematics and software that is required. This must be considered when communicating results and reports.

Thus all people affected by RAM analysis recommendations must be informed of the results to clarify the main issues and when necessary to discuss them. In fact, in many cases managers do not read complex reports, so if they are not convinced of the recommendations in the final presentation, they will likely not implement them.

It is good practice to create a short chapter at the end of the report called the manager report that includes the main points of RAM analysis including objectives and recommendations. In this way, managers will be clear about the recommendations and if they want to know more about specific points they can go through the report.

RAM analysis can be applied in a project or during the operational phase of an enterprise. In the first case the historical failure data that feeds the RBD comes from similar equipment from other plants or from equipment suppliers. When data comes from similar equipment, caution must be used when defining the similar equipment. The equipment or system must be similar enough to allow failure and repair data to be used in RAM analysis. In addition, when such assumptions are defined, it is assumed that the system in the project will behave, in terms of failure, very close to the similar system. This is a safe assumption for many types of equipment that have no significant change in technology over time, such as tanks, pipelines, and heat exchangers. But dynamic equipment, such as pumps, blowers, compressors, and turbines, do change with technology more frequently. It is also especially important to be careful when defining reference data for electrical and electronic devices because such equipment changes often.

The other way to obtain failure data is to collect information from equipment suppliers, which in some cases is hard to do. Whenever such data is available it must include specific details about failure and repair times for all equipment components to establish maintenance policies, optimum replacement times, and compare the reliability among equipment components from different suppliers. Suppliers most often supply availability and reliability information for the equipment, but not its components. Even with reliability data for equipment it is still necessary to create failure and repair data reports to perform reliability studies and RAM analysis in the future.

In some cases it is possible to obtain reliability data from accelerated tests. This approach is harder to perform because such data is considered strategic for the supplier, but it is a good source of information.

In reality, if it is possible to obtain different sources of data and compare them to supply RBDs in RAM analysis, then it is possible to obtain more reliable and have robust information. However, it requires time to assess such data and depends on RAM analysis urgency, which is hard to perform by reliability professionals.

The other important point to remember is that RAM analysis is a powerful project tool for engineers because it can be used with most system configurations to assess or reduce redundancies and identify the impacts on system availability. When a system is being projected, from a RAM analysis point of view, it is hard to preview system degradation over time. In this case it is necessary to assume system degradation over time based on experience or to simulate the system for the first period of time, and consider that if overall and preventive maintenance are performed as expected the system will be as good as new for a long period of time. On the other hand, once failure data is obtained it is possible to calculate the degradation and input into RBD and simulate. System simulation time is limited by the data collected from a similar system. Thus if the collected data is from a system that has been in operation for 10 years, for example, the projected system simulation time will be conducted for at most 10 years. The following years will be speculation, even though degradation in such equipment is calculated.

RAM analysis of an operating system provides current and realistic system data, but it is still necessary to consider how the system will behave in the future after overall and preventive maintenance have been performed on the equipment. Some assumptions are also required, and degradation can be calculated until the last operating time and can be used to assess future system availability. RAM analysis of an operating system can be used to make decisions such as how to improve system availability. When a system operates it is important to keep in mind that one cannot expect a huge investment related with RAM analysis recommendation unless such recommendation has a real influence on system availability. Thus whenever it is possible it is important to perform RAM analysis in project phases. From an enterprise point of view the sooner improvements are implemented the better. That means the sooner RAM analysis is performed, the better the results such an analysis can achieve for the system.

## 4.2 MODELING AND SIMULATION

The modeling and simulation step is one of the most exciting phases in RAM analysis. From a modeling point of view there are two types of equipment (system): repairable and nonrepairable. Nonrepairable equipment cannot be repaired when failure occurs. Some examples of nonrepairable equipment include electrical or electronic devices such as lamps or internal computer components. In the oil and gas industry, examples of nonrepairable equipment include ruptured disks that have safety functions to relieve pressure and alarms or initiators and logic elements in safety instrumented function devices.

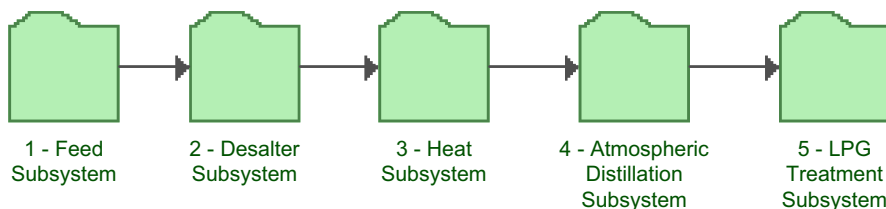
Nonrepairable equipment availability is the same as reliability and can be represented by:

$$A(t) = R(t) + \int_0^t R(t-u)m(u)du$$

When RAM analysis is conducted on unrepairable equipment (system), repair means replace, and in this case the failure equipment is replaced with a new one. The replacement time for unrepairable equipment is similar to the repair time for a repairable system, and in both cases may cause system unavailability.

### 4.2.1 RELIABILITY BLOCK DIAGRAM

In RBD configuration there are simple systems and complex systems to model. Simple systems have most of the RBD blocks in series, as shown in Fig. 4.5.



**FIGURE 4.5**

Atmospheric distillation plant RBD.

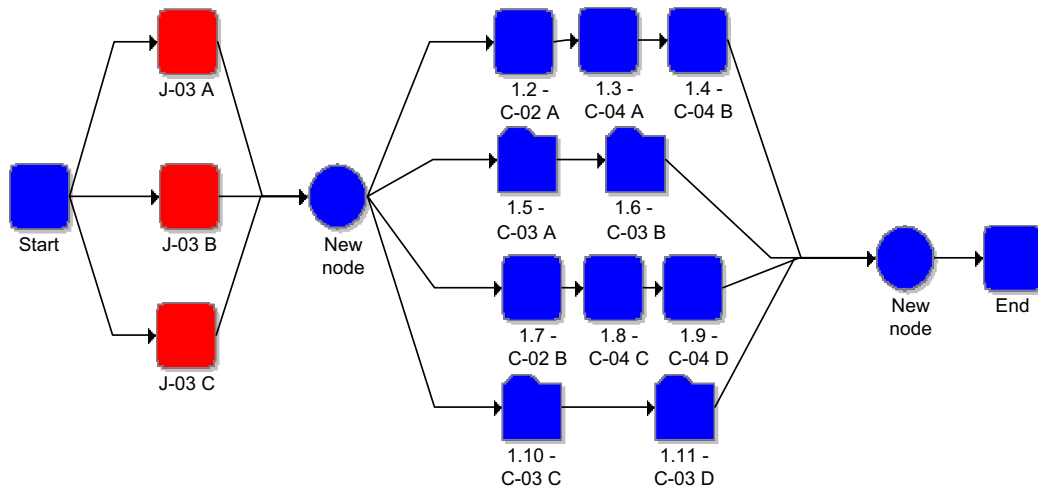


FIGURE 4.6

Heat subsystem in distillation plant RBD.

In fact, most of the blocks (equipment representation) are in series when looking at the top-level configuration, which means on a subsystems level, but looking into each subsystem, the RBD is more complex, and in some cases there are parallel blocks with other blocks in series, as shown in Fig. 4.6.

Fig. 4.6 shows a heat subsystem. In a distillation plant such a subsystem function is to heat up the feed oil before the furnace to save energy and improve distillation efficiency. Here there is a more complex RBD with two groups of equipment: pumps (J-03 A–C) and heat exchangers (C-02 A/B; C-03 A–D; C-04 A–D). Those groups of equipment are in series with other blocks and in parallel configuration. This means that if the parallel condition for one group of equipment goes down, the heat subsystem will shut down. With pumps, at least two of the three pumps must operate to avoid subsystem shutdown, and with heat exchanger pumps, at least two of the four exchanger lines must be available to prevent subsystem shutdown. In heat exchanger parallel blocks there are heat exchangers in series, which means that if one of them shuts down, the line shuts down.

In some cases the system is complex because the RBD is not only simple blocks in a series, which means there are also parallel configurations. For example, Fig. 4.7 shows the electrical, water, and gas facilities that supply the data center. Looking from the top to the bottom and from the right to the left, there are three start blocks that require software to perform simulation. The diesel generators supply energy with emergency blocks that include electrical equipment. In addition, the light company supplies energy and the main electrical distribution of gas generators. Such gas generators depend on a water-cooling system not to shut down, and in this case such blocks are in series. The three energy sources (diesel generators, light company, and gas generators) are redundant. In fact, only one of those three is necessary to have an energy supply, as is represented by the logic node ( $k/n = 1/3$ ). Below, on

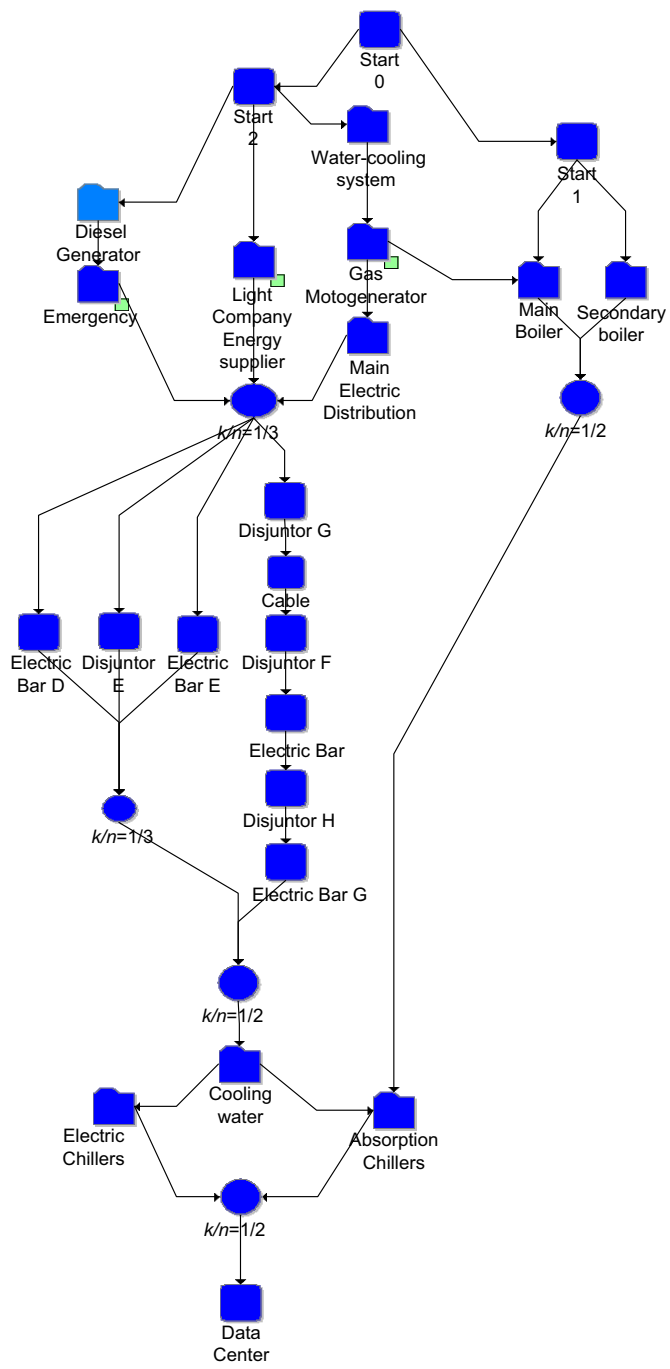
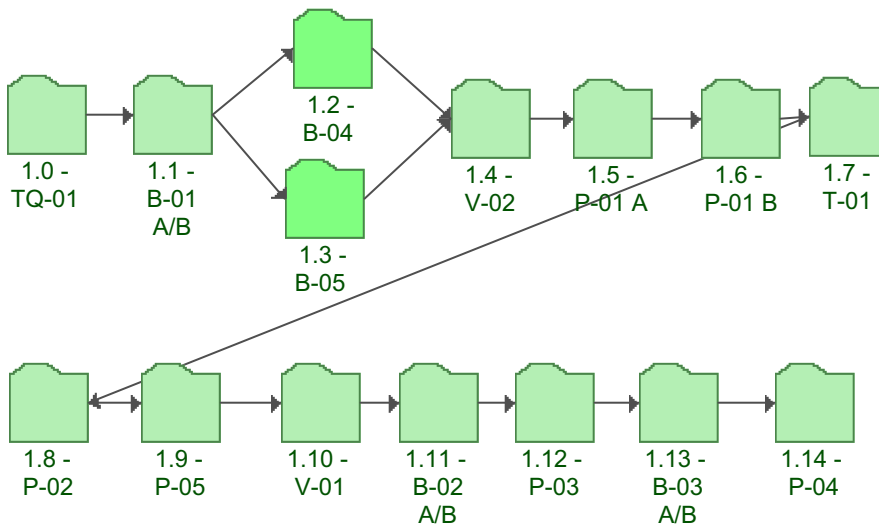


FIGURE 4.7

Data center utilities system RBD.



**FIGURE 4.8**

Diethylamine system RBD.

the left side, there are two bars (D and E) and between the disjunctors E in this configuration at least one of three must be available to supply energy. Such a logic configuration is represented by the logic node ( $k/n = 1/3$ ). There is a group of cables, bars, and disjunctors (F, G, and H) in series on the right. At least one of the two groups must be available and such logic is represented by the logic node ( $k/n = 1/2$ ), which is the electrical system in series with the cooling system, which is in series with the chillers where at least one of two (absorption or electrical) must be available to prevent data center shut down. On the right side of the RBD from the top to the bottom there are two boilers (main and secondary) and at least one of them must be available to prevent absorption chiller shutdown and such logic is represented by the logic node ( $k/n = 1/2$ ).

In this case there are many assumptions to be considered to model the RBD, and in such a case it is easy to make a mistake in RBD configuration and consequently cause the simulation results to be incorrect. To avoid this it is best to create an assumption list for all equipment to know the effects on the system when failure occurs. Fig. 4.8 shows the diethylamine system RBD.

The main objective of the diethylamine system is to remove the sulfur component from acid gas, and 14 pieces of equipment such as pumps, vessels, towers, and heat exchangers are required. For each piece of equipment there are specific failures that shut down such equipment, and it is important to know if such equipment shutdown causes loss of production in the diethylamine system. To define the RBD main assumptions, it is not necessary to know the details of the types of failures, but to model the complete RBD it is necessary to know which failures shut down the equipment or cause loss of production. Such analysis is performed prior to RAM analysis, and each block includes such failure modes that are represented by blocks in series. Each block failure has one PDF for failure time and another PDF for repair time.

To make the RBD model easier to understand, an assumption list should be created. An assumption list has the following advantages:

- Keeps process logic defined as assumptions in the RBD model;
- Is easier for other specialists who will use RAM analysis to understand the RBD model;
- When there is doubt among specialists the assumption list can be assessed;
- Whenever modifications are done in the process and it is necessary to model the system, a new RBD with the new assumptions list can be created, recorded, and compared with the previous one.

The RBD assumption list is a sequence of questions about the RBD logic. In a diethylamine system the assumption list would look like the following.

### ***DEA (Diethylamine) System—Assumption List to RBD Model***

---

1. How long does the diethylamine system operate? What is the daily production?  
→ 4 years. Daily production is 860 m<sup>3</sup>/day.

---

2. What is the diethylamine system lifetime?  
→ 25 years

---

3. How long does programmed maintenance take?  
→ 720 hours

---

4. When the diethylamine system is unavailable are the other systems also unavailable?  
→ Yes, the hydrodesulfurization plant is unavailable.

---

5. What happens if TQ-01 shuts down? Will the diethylamine system shut down or lose production capacity?  
→ Yes, if TQ-01 shuts down, the diethylamine system will shut down. Loss of 100% production capacity.

---

6. What happens if B-01 A/B shuts down? Will the diethylamine system shut down or lose production capacity?  
→ For the diethylamine system to shut down, B-01 A and B must be unavailable during the same period of time. Loss of 100% production capacity.

---

7. What happens if B-04 and B-05 shut down? Will the diethylamine system shut down or lose production capacity?  
→ For the diethylamine system to shut down, B-04 and B-05 must be unavailable during the same period of time. Loss of 100% production capacity.

---

8. What happens if V-02 shuts down? Will the diethylamine system shut down or lose production capacity?  
→ Yes, if V-02 shuts down, the diethylamine system will shut down. Loss of 100% production capacity.

---

9. What happens if P-01 A shuts down? Will the diethylamine system shut down or lose production capacity?  
→ Yes, if P-01 A shuts down, the diethylamine system will shut down. Loss of 100% production capacity.



---

10. What happens if P-01 B shuts down? Will the diethylamine system shut down or lose production capacity?  
→ Yes, if P-01 B shuts down, the diethylamine system will shut down. Loss of 100% production capacity.

---

11. What happens if T-01 shuts down? Will the diethylamine system shut down or lose production capacity?  
→ Yes, if T-01 shuts down, the diethylamine system will shut down. Loss of 100% production capacity.

---

12. What happens if P-02 shuts down? Will the diethylamine system shut down or lose production capacity?  
→ Yes, if P-02 shuts down, the diethylamine system will shut down. Loss of 100% production capacity.

---

13. What happens if P-05 shuts down? Will the diethylamine system shut down or lose production capacity?  
→ Yes, if P-05 shuts down, the diethylamine system will shut down. Loss of 100% production capacity.

---

14. What happens if V-01 shuts down? Will the diethylamine system shut down or lose production capacity?  
→ Yes, if V-01 shuts down, the diethylamine system will shut down. Loss of 100% production capacity.

---

15. What happens if B-02 A/B shuts down? Will the diethylamine system shut down or lose production capacity?  
→ For the diethylamine system to shut down, B-02 A and B must be unavailable during the same period of time. Loss of 100% production capacity.

---

16. What happens if P-03 shuts down? Will the diethylamine system shut down or lose production capacity?  
→ Yes, if P-03 shuts down, the diethylamine system will shut down. Loss of 100% production capacity.

---

17. What happens if B-03 A/B shuts down? Will the diethylamine system shut down or lose production capacity?  
→ For the diethylamine system to shut down, B-03 A and B must be unavailable during the same period of time. Loss of 100% production capacity.

---

18. What happens if P-04 shuts down? Will the diethylamine system shut down or lose production capacity?  
→ Yes, if P-04 shuts down, the diethylamine system will shut down. Loss of 100% production capacity.

Depending on the equipment in failure, part of the production capacity is lost in the system. For example, in some refinery plants there are heat exchangers and when one of these fails, part of production must be reduced. In some cases if the heat exchanger fails, production is reduced to avoid a feed tank with a product with a higher temperature than specified.

In the next section the Markov chain method is shown as an option for a modeling system to assess system availability.

## 4.2.2 MARKOV CHAIN METHODOLOGY

To increment model methodology the Markov chain approach will be used to give additional information about other possibilities for modeling the system and finding out system availability.

Such methodology is used to calculate system availability for two basic states: the fail state and the operational state. Thus failure is a transition from the operation state to the repair state and the

operation is a transition from the repair state to the operation state. Failure is represented by  $\lambda$  and repair by  $\mu$ , the constant rates of failure and repair. To implement Markov chain methodology, consider the following:

- Failures are independent.
- $\lambda$  and  $\mu$  are constants.
- The exponential PDF is applied for  $\lambda$  and  $\mu$ .

The availability is described by:

$$A(t + \Delta t) = (1 - \lambda\Delta t)A(t) + \mu\Delta tU(t)$$

where  $A(t)$  = availability,  $U(t)$  = unavailability,  $A(t + \Delta t)$  = probability the system will be in an operational state in a finite interval of time,  $(\lambda\Delta t)$  = probability of system failure in a finite interval of time,  $\lambda\Delta A(t)$  = loss of availability over  $\Delta t$ ,  $(\mu\Delta t)$  = the probability system will be repaired in a finite interval of time, and  $\mu\Delta U(t)$  = gain availability over  $\Delta t$  to have the system repaired.

On the other hand, the probability the system will not be available is:

$$U(t + \Delta t) = (1 - \mu\Delta t)U(t) + \lambda\Delta tA(t)$$

When time tends to zero we have:

$$\frac{dA(t)}{dt} = -\lambda A(t) + \mu U(t)$$

$$\frac{dU(t)}{dt} = -\mu U(t) + \lambda A(t)$$

Thus:

$$A(t + \Delta t) = (1 - \lambda\Delta t)A(t) + \mu\Delta tU(t)$$

$$A(t + \Delta t) = A(t) - \lambda\Delta tA(t) + \mu\Delta tU(t)$$

$$A(t + \Delta t) = \Delta t(-\lambda A(t) + \mu U(t)) + A(t)$$

$$\frac{A(t + \Delta t) - A(t)}{\Delta t} = -\lambda A(t) + \mu(1 - A(t))$$

$$\frac{A(t + \Delta t) - A(t)}{\Delta t} = -\lambda A(t) + \mu - \mu A(t)$$

$$\frac{A(t + \Delta t) - A(t)}{\Delta t} = -(\lambda + \mu)A(t) + \mu$$

For  $A(0) = 1$  and  $U(0) = 0$ , solving the equation using  $\exp(\lambda + \mu)$  and the integration factor the availability will be:

$$A(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} \exp[-(\lambda + \mu)t]$$

When time tends to infinity, availability assuming a constant value and availability will be:

$$A(\infty) = \lim_{t \rightarrow \infty} A(t) = \frac{\mu}{\mu + \lambda}$$

If:

$$\mu = \frac{1}{MTTR}$$

$$\lambda = \frac{1}{MTTF}$$

$$A(\infty) = \frac{\mu}{\mu + \lambda} = \frac{MTTF}{MTTF + MTTR}$$

When a Markov chain methodology is used it is necessary to define the system states; regarding the simplest cases of repairable systems, there are two states that are available and under repair, and for each state it is necessary to define the failure rate and repair rate. An example Markov chain is a system that includes two pumps where at least one must be available for the system to operate. So in this case there will be four states:

- State 1: System works with two pumps available;
- State 2: System works with pump A available and pump B unavailable;
- State 3: System works with pump B available and pump A unavailable;
- State 4: System unavailable because pumps A and B are unavailable.

Fig. 4.9 shows the Markov chain diagram for each state.

When the system goes from S1 to S2, pump A is available and pump B fails for failure rate  $\lambda_1$ . When the system goes from S2 to S1, pump B is repaired for  $\mu_1$ . A similar logic is applied when the system goes from S2 to S3, but in this case pump B is available and pump A fails for failure rate  $\lambda_2$ . When the system goes from S4 to S2, pump A is repaired and the repair rate is  $\mu_2$ . Therefore the system can return from one state to another, for example, from S2 to S1 if pump B has been repaired.

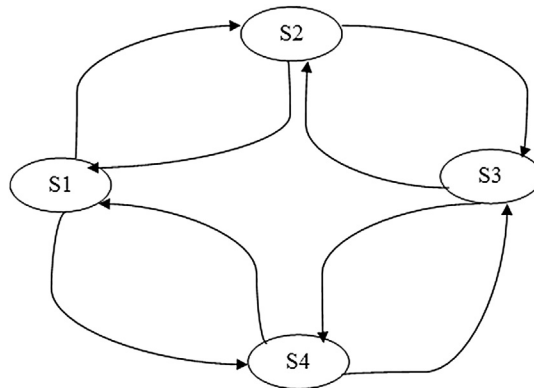


FIGURE 4.9

Graphic of Markov chain diagram.

There is software available to calculate availability using the Markov chain methodology but using matrix methods is complicated even for simple cases. Despite the basic assumptions in Markov chain methodology (constant failure and repair rates), it is still possible to use other PDFs. When modeling a huge system with more than 10 pieces of equipment and each piece of equipment includes at least two failure modes, Markov chain methodology is complex and requires much more time than the RBD model. Thus no examples will be given for this model because RBD will be applied to model most oil and gas industry systems.

### 4.2.3 SIMULATION

After creating an RBD it is necessary to calculate the operational availability, but it is first necessary to define the period of time the system will operate. The system can be available with a 100% capacity or lower depending on what level of production availability is being considered. In many cases when considering an operational availability target, the system is available when operating at 100% capacity, so operational availability is represented by:

$$A(t) = \frac{\sum_{i=1}^n t_i}{\sum_{i=1}^n T_i}$$

where  $t_i$  = real time when the system is available with 100% capacity and  $T_i$  = nominal time when the system must be available.

The other important index used to assess a system is efficiency, which shows the real production by nominal production, calculated by:

$$EP(t) = \frac{\sum_{i=1}^n pr_i \times t_i}{\sum_{i=1}^n Pr_i \times T_i}$$

where  $pr_i$  = real productivity in time  $i$ ,  $Pr_i$  = nominal productivity in time  $i$ ,  $t_i$  = real time when system is available, and  $T_i$  = nominal time when system must be available.

When 100% of capacity is being used, maximum availability is similar to efficiency when the system only operates at 100% of capacity, as shown by the following.

Case 1: System operates at 100% capacity only:

$$EP_1(t) = \frac{\sum_{i=1}^n pr_i \times t_i}{\sum_{i=1}^n Pr_i \times T_i}$$

if

$$pr_1 = pr_2 = pr_3 = \dots = pr_n$$

and

$$Pr_1 = Pr_2 = Pr_3 = \dots = pr_n$$

For when production is only 100% or 0%:

$$pr_i = Pr_i$$

$$EP_1(t) = \frac{pr_i(t_1 + t_2 + t_3 + \dots + t_n)}{Pr_i(T_1 + T_2 + T_3 + \dots + T_n)} = \frac{(t_1 + t_2 + t_3 + \dots + t_n)}{(T_1 + T_2 + T_3 + \dots + T_n)} = \frac{\sum_{i=1}^n t_i}{\sum_{i=1}^n T_i}$$

$$EP_1(t) = A(t)$$

Thus case 1 is appropriate for systems that when failures occur the system loses 100% production capacity. However, in some cases, with equipment failure there is only a partial loss of production. In such cases the system keeps operating, but at a production capacity that is lower than 100%. When this is the case the maximum capacity availability is lower than the efficiency, but it is possible to use real availability—that is, system availability in any production capacity from zero to 100%. This is represented by case 2.

Case 2: Capacity of production between 100% and 0%:

$$EP_2(t) = \frac{\sum_{i=1}^n Pr_i \times t_i}{\sum_{i=1}^n Pr_i \times T_i} = EP'(t) + EP''(t)$$

$$EP'(t) = \frac{\sum_{k=1}^n Pr_k \times t_k}{\sum_{k=1}^n Pr_k \times T_k}$$

This partial equation represents part of production only at 100% or 0%, that is, only the case 1 assumption:

$$EP'(t) = \frac{\sum_{k=1}^n Pr_k \times t_k}{\sum_{k=1}^n Pr_k \times T_k}$$

$$pr_i = Pr_i$$

$$EP'(t) = \frac{pr_k(t_1 + t_2 + t_3 + \dots + t_n)}{Pr_k(T_1 + T_2 + T_3 + \dots + T_n)} = \frac{(t_1 + t_2 + t_3 + \dots + t_n)}{(T_1 + T_2 + T_3 + \dots + T_n)} = \frac{\sum_{k=1}^n t_k}{\sum_{k=1}^n T_k}$$

$$EP'(t) = A(t)$$

In addition, when real productivity is lower than 100%, capacity is nominal productivity, because in this case if failure occurs the capacity will be at a level that is lower than 100%. This means that despite system availability, it is available lower than the maximum capacity, and in this case the real availability will always be higher than the efficiency, as shown by:

$$EP''(t) = \frac{\sum_{j=1}^n Pr_j \times t_j}{\sum_{j=1}^n Pr_j \times T_j}$$

$$pr_i < Pr_i$$

$$\frac{pr_i}{Pr_i} = k$$

$$0 < k < 1$$

$$EP''(t) = \frac{pr_j(t_1 + t_2 + t_3 + \dots + t_n)}{Pr_j(T_1 + T_2 + T_3 + \dots + T_n)} = \frac{pr_i(t_i)}{Pr_i(T_i)} = k \frac{(t_i)}{(T_i)}$$

For both situations, when the production is at 100% capacity and at lower than 100%, we have case 2:

$$\begin{aligned}
 EP_2(t) &< A_2(t) \\
 EP_2(t) &= \frac{\sum_{k=1}^n Pr_k \times t_k}{\sum_{k=1}^n Pr_k \times T_k} + \frac{\sum_{j=1}^n Pr_j \times t_j}{\sum_{j=1}^n Pr_j \times T_j} \\
 EP_2(t) &= EP'(t) + EP''(t) < A(t) + A'(t) \\
 EP_2(t) &< A_2(t)
 \end{aligned}$$

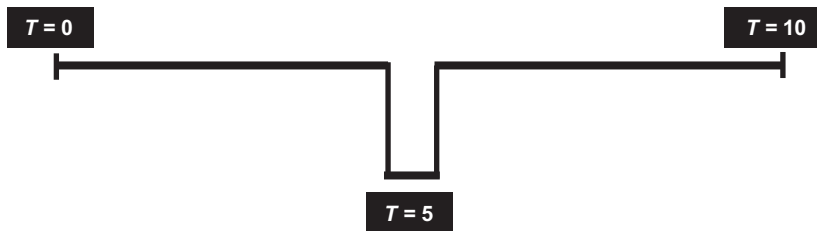
**Case 1**

To illustrate case 1 where the basic assumption is that when the system is available it operates only at 100% capacity, we regard one system that operates over 10 time units and in each unit of time the system produces one unit of product. At time 5 the system shuts down during one time unit. As the system is operating only at 100% capacity there will be 100% capacity loss on time 5. In terms of operational availability the system achieves 90% and in terms of efficiency the system also achieves 90%. Fig. 4.10 shows system operation.

$$\begin{aligned}
 A(t) &= \frac{\sum_{i=1}^n t_i}{\sum_{i=1}^n T_i} \\
 A(t) &= \frac{\sum_{i=1}^{10} t_i}{\sum_{i=1}^{10} T_i} = \frac{1 + 1 + 1 + 1 + \dots + 1}{1 + 1 + 1 + 1 + \dots + 1} = \frac{9}{10} = 90\%
 \end{aligned}$$

and:

$$\begin{aligned}
 EP(t) &= \frac{\sum_{i=1}^n Pr_i \times t_i}{\sum_{i=1}^n Pr_i \times T_i} \\
 EP(t) &= \frac{\sum_{i=1}^{10} Pr_i \times t_i}{\sum_{i=1}^{10} Pr_i \times T_i} = \frac{1 \times 1 + 1 \times 1 + \dots + 1 \times 1}{1 \times 1 + 1 \times 1 + \dots + 1 \times 1} = \frac{9}{10} = 90\%
 \end{aligned}$$



**FIGURE 4.10**

System operation.

**Case 2**

To illustrate case 2 where the basic assumption is that, when available, the system operates at between 0% and 100% of maximum capacity, we regard a system similar to the previous system represented by Fig. 4.8, which operates over 10 time units, and in each time unit the system produces one unit of product. In this case the difference is, in the instant 5, when failure happens the system reduces production during one time unit. At this time the equipment fails and the system reduces capacity by 50%, and there will be a 50% capacity loss in one unit of time. In terms of efficiency the system achieves 95%. But if we consider the operational availability at maximum capacity, we still have 90%, because in time 5 the system was not available for one unit of time at maximum capacity. However, the mean availability is 100% because the system operates 90% of the time at maximum capacity and the other 50% of reduced capacity on time 5 during one unit of time.

The operational availability at maximum capacity is:

$$A(t) = \frac{\sum_{i=1}^n t_i}{\sum_{i=1}^n T_i}$$

$$A(t) = \frac{\sum_{i=1}^{10} t_i}{\sum_{i=1}^{10} T_i} = \frac{1 + 1 + 1 + 1 + \dots + 1}{1 + 1 + 1 + 1 + \dots + 1} = \frac{9}{10} = 90\%$$

In this case, during the period of time 5, when the system fails, production is at 50% of total capacity during one unit of time. Therefore, such availability with 50% of capacity is not accounted because during time 5, the system is not operating with the maximum capacity (100%).

In efficiency production case is:

$$EP_2(t) = \frac{\sum_{i=1}^n pr_i \times t_i}{\sum_{i=1}^n Pr_i \times T_i} = EP'(t) + EP''(t)$$

$$EP'(t) = \frac{\sum_{k=1}^n pr_k \times t_k}{\sum_{k=1}^n Pr_k \times T_k} = \frac{1 + 1 + \dots + 1}{1 + 1 + \dots + 1} = \frac{9}{10}$$

The efficiency related to 50% capacity is:

$$EP''(t) = \frac{\sum_{j=1}^n pr_j \times t_j}{\sum_{j=1}^n Pr_j \times T_j}$$

$$pr_i = Pr_i$$

$$\frac{pr_i}{Pr_i} = k$$

$$EP''(t) = \frac{pr_j(t_1 + t_2 + t_3 + \dots + t_n)}{Pr_j(T_1 + T_2 + T_3 + \dots + T_n)} = k \frac{(t_i)}{(T_i)} = 0.5 \cdot \frac{1}{1} = 0.5$$

Thus the total efficiency will be:

$$\begin{aligned} EP_2(t) &= \frac{\sum_{i=1}^n \text{Pr}_i \times t_i}{\sum_{i=1}^n \text{Pr}_i \times T_i} = EP'(t) + EP''(t) \\ &= \frac{9}{10} + \frac{0.5}{10} = 95\% \end{aligned}$$

Thus the real availability when the system is operating at 100% of capacity and with instant 5 when the system is operating at 50% capacity is 100% because no matter how much capacity there is, the system is always available as shown in this equation:

$$\begin{aligned} A_2(t) &= \frac{\sum_{j=1}^n t_j}{\sum_{j=1}^n T_j} = \frac{(t_1 + t_2 + t_3 + \dots + t_n)}{(T_1 + T_2 + T_3 + \dots + T_n)} \\ &= \frac{1 + 1 + 1 + 1 + 1 + \dots + 1}{1 + 1 + 1 + 1 + 1 + \dots + 1} = \frac{10}{10} = 100\% \end{aligned}$$

### Case 3

In time 5, if we consider a 0.5 period of time with 100% capacity, despite one period of capacity with 50% maximum capacity, we have that efficiency is equal to availability as shown by:

$$\begin{aligned} EP_2(t) &= \frac{\sum_{i=1}^n \text{Pr}_i \times t_i}{\sum_{i=1}^n \text{Pr}_i \times T_i} = EP'(t) + EP''(t) \\ EP'(t) &= \frac{\sum_{k=1}^n \text{Pr}_k \times t_k}{\sum_{k=1}^n \text{Pr}_k \times T_k} = \frac{1 + 1 + \dots + 1}{1 + 1 + \dots + 1} = \frac{9}{10} \\ EP''(t) &= \frac{\sum_{j=1}^n \text{Pr}_j \times t_j}{\sum_{j=1}^n \text{Pr}_j \times T_j} \\ \text{pr}_i &= \text{Pr}_i \\ EP'(t) &= \frac{\text{pr}_j(t_1 + t_2 + t_3 + \dots + t_n)}{\text{Pr}_j(T_1 + T_2 + T_3 + \dots + T_n)} = \frac{\sum_{j=1}^n t_j}{\sum_{j=1}^n T_j} = 1 \cdot \frac{0.5}{10} = 0.05 \end{aligned}$$

Thus the efficiency will be:

$$\begin{aligned} EP_2(t) &= \frac{\sum_{i=1}^n \text{Pr}_i \times t_i}{\sum_{i=1}^n \text{Pr}_i \times T_i} = EP'(t) + EP''(t) \\ &= \frac{9}{10} + \frac{0.5}{10} = 95\% \end{aligned}$$



And the availability is:

$$A_2(t) = A(t) + k \cdot A'(t)$$

$$k = 1$$

$$A(t) = \frac{\sum_{j=1}^n t_j}{\sum_{j=1}^n T_j} = \frac{(t_1 + t_2 + t_3 + \dots + t_n)}{(T_1 + T_2 + T_3 + \dots + T_n)} = \frac{1 + 1 + 1 + 1 + 1 + \dots + 1}{1 + 1 + 1 + 1 + 1 + \dots + 1} = \frac{9}{10} = 0.9$$

$$A'(t) = \frac{\sum_{j=1}^n t_j}{\sum_{j=1}^n T_j} = k \cdot \frac{(t_1 + t_2 + t_3 + \dots + t_n)}{(T_1 + T_2 + T_3 + \dots + T_n)} = 1 \cdot \frac{0.5}{1 + 1 + 1 + 1 + 1 + \dots + 1} = \frac{0.5}{10} = 0.05$$

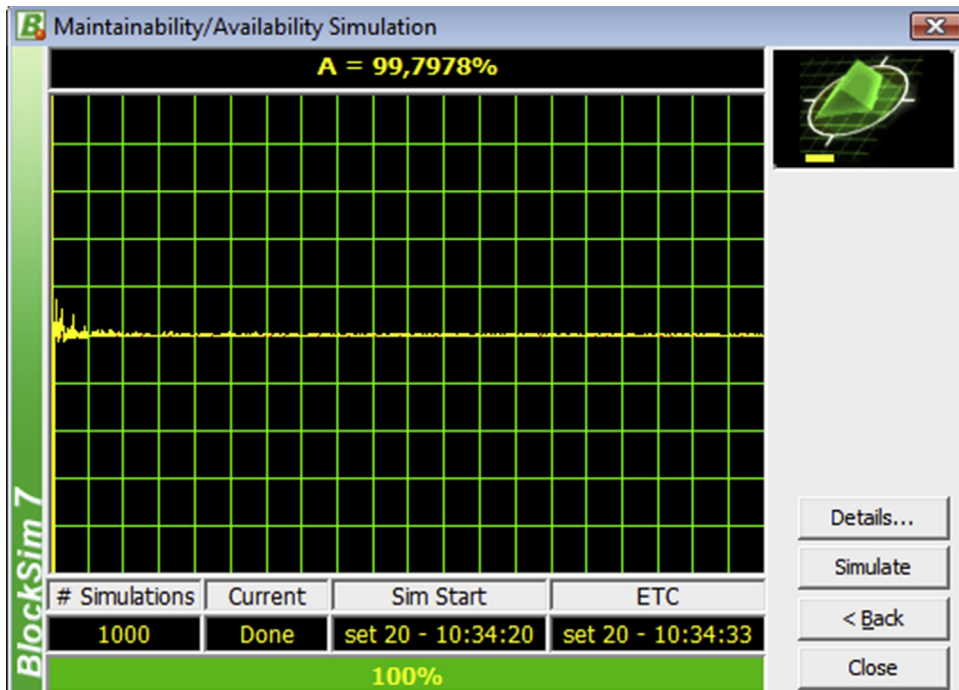
$$A_2(t) = \frac{\sum_{j=1}^n t_j}{\sum_{j=1}^n T_j} = \frac{(t_1 + t_2 + t_3 + \dots + t_n)}{(T_1 + T_2 + T_3 + \dots + T_n)} = \frac{1 + 1 + 1 + 1 + 0.5 + \dots + 1}{1 + 1 + 1 + 1 + 1 + \dots + 1} = \frac{9.5}{10} = 0.95$$

$$A_2(t) = A(t) + k \cdot A'(t) = 0.9 + 0.05 = 0.95 = 95\%$$

Case 3 is used when it is necessary to find out the efficiency using operational availability. In some cases there is software that can calculate availability for only total losses and does not consider partial loss, so whenever there will be a partial loss, such value (% of loss) may be discounted in repair time, and the final result in availability also shows the efficiency value.

These examples (cases 1, 2, and 3) help to simplify and better understand how availability and efficiency usually proceed. In a system with several pieces of equipment this approach is complex and requires time to proceed. Such an approach in reality is not deterministic; in other words, the availability and efficiency are usually probabilistic and Monte Carlo simulation is used to define availability or efficiency. The efficiency is an index that results from throughput simulation in software, and basically such an RBD is used to calculate throughput when it is similar to the process diagram. In this case, availability results regard any level of production. In the oil and gas industry it is necessary to know the availability at maximum capacity. Thus, in this case, the RBD must represent production losses at a maximum production level by RBD configuration as well as throughput in any level of production that is represented by a throughput diagram block. Some software is only able to calculate availability at maximum system capacity because they do not regard partial production loss in case of equipment failures.

To calculate operational availability it is easier and faster to simulate a system for a specific period of time using software that performs Monte Carlo simulation for all equipment in the RBD. The software will run several times as required and give the average operational availability, as shown in Fig. 4.11. The number of simulations depends on reliability analyst requirements for results assurance. There is not an optimum number of simulations, but the higher the number of simulations, the more accurate the results. However, if it is a complex system and a high number of simulations are set up, the results will take more time. Thus depending on system complexity a higher or lower number of simulations can be performed. The number of runs usually varies from 200 to 1000. In complex systems where time is a concern this number can be lower, but it is almost never necessary to be higher than 1000 unless required for accuracy.



**FIGURE 4.11**

Simulation.

Source: BlockSim 7++.

Fig. 4.11 shows the availability results for the average of 1000 simulations. The software shows approximately 99.8% operational availability. It is very important to remember that the number of simulations influences the result because operational availability is the average of all operational availability simulation results. The other important point is that no matter how many simulations are set up, the critical subsystems will always be the same.

There are many software packages on the market that give very good results for the RBD model and simulation approach. When you choose software to perform RAM analysis, it should:

- Be simple to operate;
- Provide quick result simulation;
- Be mathematically consistent;
- Require investment to buy software and training;
- Be linked with other software;
- Provide service and maintenance;
- Provide access to updated versions;
- Include simulation background results.

Most of the time all of these points are realized, but simulation background results must be provided because these results will support decisions and recommendations to improve systems availability and usually a lot of money is involved in such decisions.

Simulation results usually include efficiency, operational availability, point availability, reliability, number of failures, uptime, downtime, and throughput. Table 4.3 shows example simulation results.

<b>Table 4.3 Simulation Result</b>	
<b>System Overview</b>	
<b>General</b>	
Mean availability (all events)	0.9683
Standard deviation (mean availability)	0.0092
Mean availability(w/o PM and inspection)	0.9683
Point availability (all events) at 26,280	0.971
Reliability (26,280)	0
Expected number of failures	12.52
Standard deviation (number of failures)	3.5168
MTTFF	1942.593
System Uptime/Downtime	
Uptime	25,446.98
CM downtime	833.02
Inspection downtime	0
PM downtime	0
Total downtime	833.02
System Downing Events	
Number of failures	12.519
Number of CMs	12.519
Number of inspections	0
Number of PMs	0
Total events	12.519
Costs	
Total costs	0
Throughput	
Total throughput	0
PM, <i>preventive maintenance</i> ; CM, <i>corrective maintenance</i> .	

The first line gives the *mean availability* (96.83%), that is, the average of the number of simulation results of operational availability. The second line gives the *mean availability standard deviation*, which shows how reliable the mean availability result is. The third line is the *mean availability with inspection and preventive maintenance*. This value includes inspection time and preventive maintenance downtime to calculate the mean availability. In these cases, since there is no inspection and *preventive maintenance*, this value is similar to mean availability. The fourth line gives the *point availability*, the probability the system will be available for the defined time in simulations, which, in this case, is 26,280 hours (3 years). The fifth line is *reliability*, which is zero, and means there is a 100% chance of system failure until 26,280 hours (3 years). The sixth line gives the *expected number of failures*, which is 12 (12.52). The seventh line is the *MTTF* (mean time to first failure), the expected time for the first failure (1942.5). The 10th line is the *uptime*, that is, the time the system is available. The 11th line is the CM (*corrective maintenance*) downtime, which includes all the downtime dedicated to corrective maintenance. The following two lines are *inspection downtime* and PM (*preventive maintenance*) downtime, which is zero in this case for both because there was no inspection or preventive maintenance. The 15th line is the *total downtime*, which includes the inspections and corrective and preventive maintenance that cause downtime. In this case, as there were no inspection and preventive maintenance, the total downtime is similar to the correct maintenance downtime. The 16th line is the *total number of failures* (12,519), the approximate expected number of failures on the sixth line. The 17th line gives the *number of CM*, which is similar to the number of failures. The 22nd line is the *total cost*, which is zero in this case because there were not any costs for maintenance or inspections regarded in this case. Finally, the 24th line gives the *throughput*, which is also zero in this case because there was no stated value. This throughput is the total production in the total time defined in the simulation.

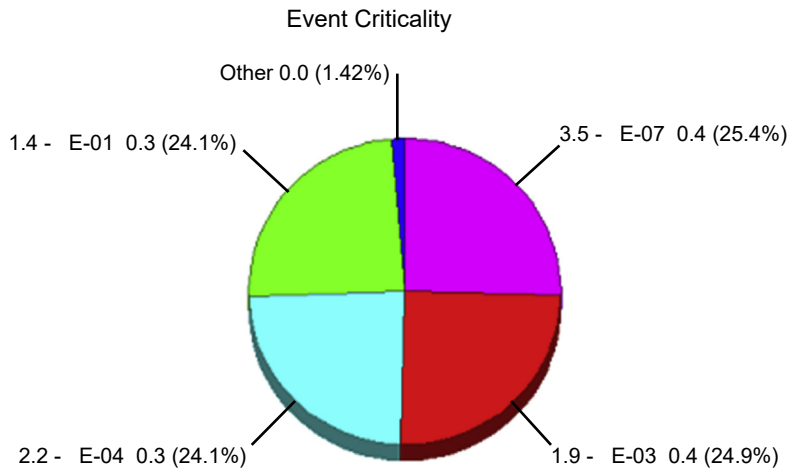
#### 4.2.4 RELIABILITY AND AVAILABILITY PERFORMANCE INDEX

Different software will produce different results, but most of the time the results will be similar to [Table 4.3](#) and show, directly or indirectly, results, which means that for some results it is possible to calculate some index. If software gives throughput as results, for example, it is possible to calculate efficiency. Efficiency is throughput results divided per nominal throughput. Nevertheless, such results are not enough to make decisions, because despite results it is not clear which subsystem or equipment has the most impact on system reliability and availability. Some common indexes used to indicate critical subsystems and equipment are:

- Percentage of losses index
- Failure rank index
- Downtime critical index
- Availability rank index
- Reliability importance (RI) index
- Availability importance (AI) index
- Utilization index

##### ***Percentage Losses Index***

The first index, percentage of losses, includes all losses in availability or production related to equipment downtime events that impact system availability. It is possible to know which equipment has a higher percentage of losses in terms of production or availability loss time, as shown in [Fig. 4.12](#).

**FIGURE 4.12**

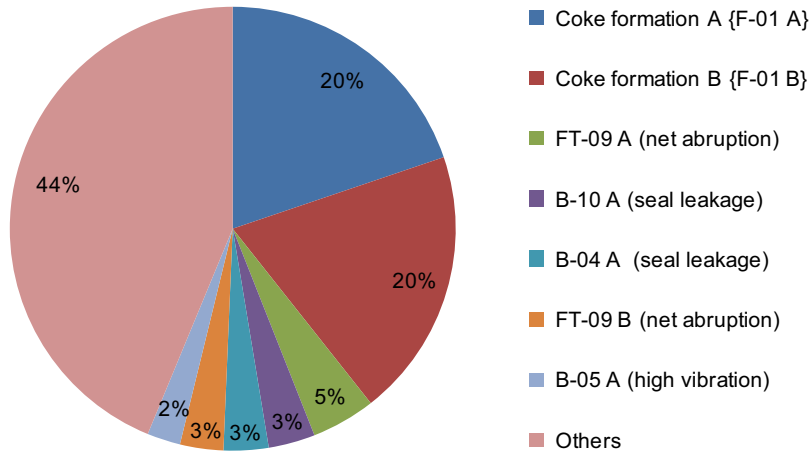
Percentage loss index.

The percentage of loss index is a relation between production or time loss and total loss (production or time). This index is good for finding, for example, which type of equipment causes more losses among different equipment types (eg, valves, pumps, heat exchangers), and it is possible to create a percentage of loss index for similar types of equipment to analyze different suppliers. Remember that the equipment in the index must have the same period of operating time. For example, if the equipment of A fails more than the equipment of B, but you forgot to consider that supplier A equipment operates much more than the equipment of supplier B, the baseline is not similar enough to compare equipment performance. In addition, operational conditions and maintenance policies must be considered. However, sometimes such indexes make specialists believe that if they improve the most critical equipment to reduce losses they will improve availability or efficiency proportionally, and that is not true because it is not a current Pareto problem. The percentage of losses index shows which equipment causes more downtime in the system and such equipment must be a priority if increasing system availability is an objective.

Fig. 4.12 shows a refinery plant where the most critical equipment are heat exchangers E-01, E-03, E-04, and E-07. The main failure is obstruction in tubes because of dirty water that passes through the heat exchanger tubes. In this case there are percentages for total loss for each heat exchanger, which show that it is necessary to improve all four heat exchangers, otherwise system availability will be limited to the low availability and it will not be possible to achieve the reliability target.

### **Failure Rank Index**

The failure rank index measures the percentage of total failures in the system for each piece of equipment, which means the number of one specific equipment failure divided by the total number of failures for all equipment failures in the system. This type of index is helpful because it indicates which equipment fails more often, and consequently it is possible to associate corrective maintenance costs related with such equipment. Here failure rate does not necessarily mean more impact on system



**FIGURE 4.13**

Failure index.

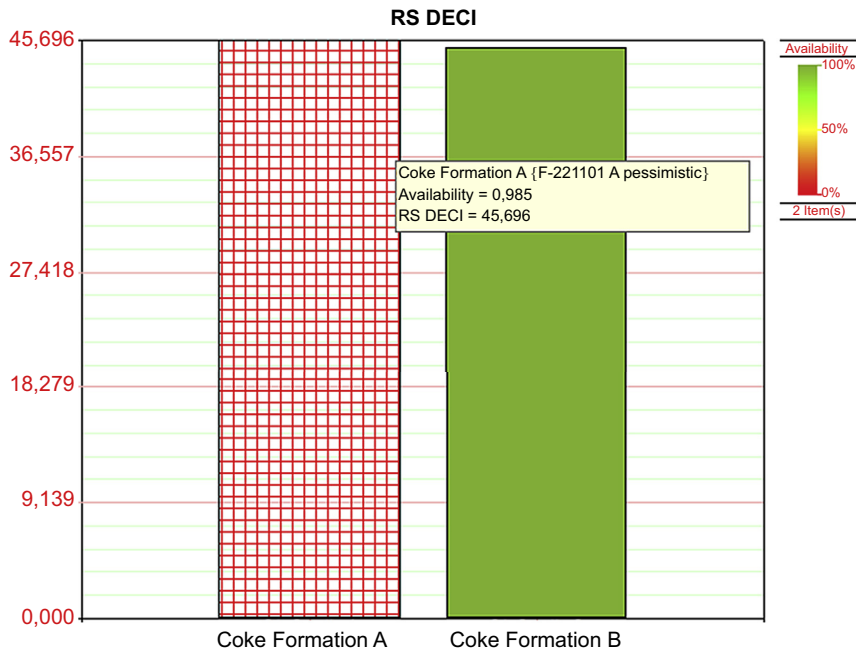
availability. In a refinery system the main critical equipment is furnaces A and B because of coke formation that is shown in Fig. 4.13, each one at 20% of the total number of failures. Depending on the case the failure index can indicate that equipment is responsible for a higher impact on availability or not. This means downtime is the main impact on system availability. In this example, 44% of other failure cases are more representative in the number of failures when compared with two furnace coke formations. The downtime caused by coke formation is higher than the downtime caused by the other 44% of equipment failures. If cost of corrective maintenance is considered, the equipment has different importance in terms of cost, because depending on the cost of corrective maintenance, some equipment can be more critical in terms of cost when compared with others with no significant maintenance cost.

### ***Downtime Event Critical Index***

The downtime critical event index measures which equipment causes more downtime to a system in a period of time. Thus such an index is related to the number of downtimes and is a good tool for preventing plant shutdowns and helps to prioritize which equipment causes the most impact on plant in terms of amount of downtime. However, this index does not support complete decisions for improving system availability because it does not show the total amount of system downtime caused by an equipment. Fig. 4.14 shows an example downtime critical index.

Fig. 4.14 shows an example of furnaces in a refinery plant (a similar system is used in Fig. 4.11) in which coke formation in furnace tube A occurs. Furnace A availability is 98.5% in 3 years and the downtime event criticality (EC) index is 45.6%, which means 45.6% of the total number of system downtimes.

It is important to remember that the number of downtimes does not mean total downtime. The percentage of loss index is related to system downtime impact and the downtime EC index is related to the number of system downtimes.



**FIGURE 4.14**  
Downtime event criticality index.

### Availability Rank Index

The availability rank index is a good index when the RBD is in series. In fact, as discussed previously, when the system RBD has all blocks in series, the system availability is lower than the lowest block’s availability, which is represented by one subsystem or piece of equipment. So, even if the whole RBD is not in series in high diagram level (subsystems), most of the time they are in series and it is possible to find out which subsystem is the availability bottleneck, or, in other words, has the lowest availability that will limit system availability. Be careful when using the availability rank index in complex systems because the equipment with the lowest availability may not impact the system since such equipment is configured in parallel with other equipment. Fig. 4.15 shows a refinery plant availability rank index.

Looking at the availability rank index in Fig. 4.15, we can see that the lowest availability value on the bottom is related to coke formation in furnaces A (F-01 A) and B (F-01 B). Such failure modes must be priorities if increasing system availability is an objective. Even if such equipment achieved 100% availability in 3 years (in simulation), the system availability would be limited to 99.46% because the next lowest availability is related to external corrosion in the heat exchanger (P-03). Thus improvements must be implemented from the bottom to the top of the availability rank list until the

Availability Ranking	
Block Names	Availability
B-04 A (Seal leakage)	99.87%
Internal Corrosion (P-03)	99.52%
External Corrosion (P-03)	99.46%
Coke Formation B (F-01 B)	98.53%
Coke Formation A (F-01 A)	98.51%

**FIGURE 4.15**

Availability rank index.

system availability target is achieved. Be careful with such a list because in some cases equipment that is modeled in parallel in the RBD will not influence system availability like equipment modeled in series. For example, B-04 A on the list has a seal leakage failure mode and the availability in 3 years is 99.87%. Despite such a value, pump B-04 A is in parallel (A/B) in the RBD and both pumps (B-04 A/B) achieve 100% availability in 3 years (simulated time) because the pump has the other pump as a standby (B-04 B). In this case, when B-04 A fails, B-04 B, which is on standby, will operate and keep the system available.

### **Reliability Importance Index**

The other important index is RI, which defines the subsystem or equipment with the most influence on system reliability and allows the specialist to know how much system reliability can be improved if improvements in a critical subsystem or equipment reliability are conducted. This index is not enough to support decisions for system improvement to achieve the availability or efficiency targets because it focuses on reliability.

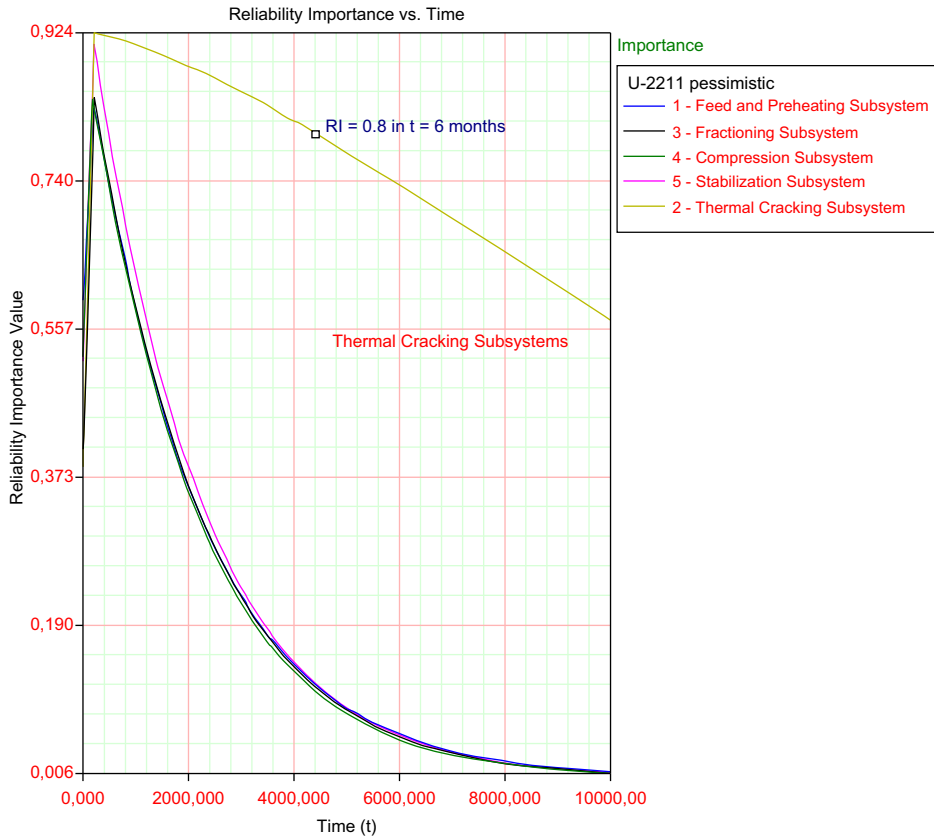
The RI index is defined as partial derivation of a system related to a subsystem (or equipment). The equation showing the relation is:

$$\frac{\partial R(\text{System})}{\partial R(\text{Subsystem})} = \text{RI}$$

Such an index can be defined by a fixed period of time or over time as shown in Fig. 4.16.

As shown in Fig. 4.16 the same system in the previous examples is assessed, and using the RI index we can see that the thermal cracking subsystem is the most critical in terms of reliability. Thus for system reliability to improve such a system must be prioritized. Looking at Fig. 4.16 there are different values in the RI index over time. An example of the RI index is a thermal cracking subsystem with RI = 0.8 in 6 months. So if 100% of improvements are conducted in the thermal cracking subsystem, the system reliability will improve 80%. It is important to realize that the thermal cracking subsystem includes furnaces F-01 A and F-1 B. Such equipment was the most critical in terms of failures, as shown in Fig. 4.13, which makes sense because the number of failures is completely related to reliability. In this case especially the availability rank index and the downtime EC index show that F-01 A and F-01 B are the most critical equipment in terms of system unavailability. In some cases that is not





**FIGURE 4.16**  
Reliability importance index.

true, because despite some equipment impacting system reliability more in number of failures, conversely, other equipment impacts system availability more because downtime is related to the number of failures. The availability impact takes into account reliability and downtime and this is the main index to use to make decisions because it is related to production loss; in other words, system unavailability.

**Availability Importance Index**

This index is similar in concept to the previous one, but the AI index measures the impact of a subsystem or equipment on system availability. There are indirect indexes that indicate subsystem or equipment impact on system availability, but the most important information is to know how much the system availability will be improved if the critical subsystem or equipment availability is improved. In this way, an idea similar to the RI index can be applied and the AI index will be defined as a partial

derivation of system availability related to subsystem (or equipment) availability. The equation is as follows:

$$\frac{\partial A(\text{System})}{\partial A(\text{Subsystem})} = \text{AI}$$

### **Utilization Index**

The utilization index measures how much equipment is used over a period of time and shows if systems are underestimated or overestimated in terms of equipment. Utilization can be represented by:

$$U = \frac{T_{\text{op}}}{T_{\text{av}}}$$

where  $T_{\text{op}}$  = total operation time and  $T_{\text{av}}$  = total available time.

Utilization can also be expressed in terms of production and in this case utilization will be:

$$U = \frac{T_{\text{prod}}}{T_{\text{nprod}}}$$

where  $T_{\text{prod}}$  = total production on available time and  $T_{\text{nprod}}$  = total nominal production on available time.

The utilization index can reflect two situations: the demand level or redundancy policy effectiveness. When demand for a system is low even though the system has high availability, the system is not used as it could be; in this case, low utilization is related to low demand. However, when equipment is not used even when the system has high demand, the system is overestimated. Redundancies such as pumps, pipelines, and tanks are good examples of equipment that usually has low utilization in some systems. In many cases, RAM analysis is a good tool to verify if the system is overestimated in redundancy and equipment and allows you to see if system availability is affected when there is equipment with low utilization.

Another point to note is that even when a company is aware about low equipment utilization on a system in case of redundancies, the final decision may be to keep the redundancies to reduce system vulnerability from events out of the company's control, such as natural catastrophes, terrorism attacks, or even uncertainty about the equipment supplier market. The following section discusses additional analysis that must be considered because it can influence RAM analysis results, or, in other words, system availability or efficiency. Such analysis will take into account logistics, maintenance plans, and stock policies.

---

## **4.3 SENSITIVITY ANALYSIS: REDUNDANCY POLICIES, MAINTENANCE POLICIES, STOCK POLICIES, AND LOGISTICS**

In this section the most common types of sensitivity analysis are introduced. Even if RAM analysis has been thoroughly conducted there are still other system vulnerabilities that can influence system availability including:

- Redundancy policies
- Maintenance policies
- Stock policies
- Logistics

### 4.3.1 REDUNDANCY POLICIES

The first sensitivity analysis is the redundancy policy applied as strategy to achieve the system performance (operational availability) without improve critical equipment reliability. This is always a good opportunity for reliability specialists to discuss redundancy policy and how to achieve the plant's operational availability, which means. better equipment reliability, redundant equipment, or both. Redundancy often increases the cost of projects and maintenance, and for many companies redundancy also introduces system risk (pipelines and tanks). In fact, in many cases, increased redundancy is the easiest way to reduce system vulnerability, and one way to help achieve system availability targets. RAM analysis is a good tool for testing redundancy policies to assess the impacts on system availability when redundancy is removed. There are two types of redundancies:

- Passive redundancy
- Active redundancy

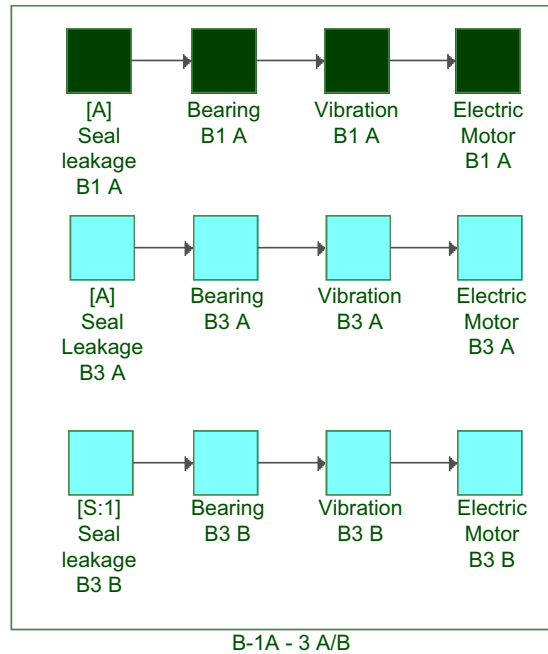
Passive redundancies are usually well known, and a good example is a standby pump configuration where one pump operates and the other remains on standby to avoid system shutdown in the case of pump failure. This configuration is often used in the oil and gas industry, and the interesting point is which standby policy condition will be applied, which means the standby equipment will be mostly passive, or, in other words, passive equipment operates only when active equipment fails. Some specialists believe that changing pumps A and B from time to time is better for a pump's life cycle, and other specialists believe that it is better to let pump A operate until it fails but to start up pump B to guarantee that it will work when demanded. It is possible to test both approaches by modeling the pumps' RBD and simulating for a period of time to find out which one is better for each particular case.

Active redundancy is when similar equipment with the same function in a system operates together and there is some condition that defines loss of production when a specific number of such equipment fail. In some cases there will be a load-sharing effect, which means when one piece of equipment fails, the other equipment will maintain the same level of production capacity but will degrade faster than usual.

No matter the type of redundancy, in most cases the redundancy policy can be tested by RAM analysis to find out if redundancies are necessary or not.

An example of an unnecessary redundancy that impacts project costs is shown in [Fig. 4.17](#). A projected plant has redundancy configuration for all pumps and a sensitivity analysis was performed to verify the possibility of reducing the number of redundant pumps. In this case the first step is to see if it is possible to use one standby pump for more than one pump and to verify that such pumps have no differences that will affect pump performance. After that, simulation is performed for the two pumps operating for a period of time with one pump on standby.

The availability of the pumps is 100%, so it is possible to reduce project costs by reducing standby pumps in this plant. In this case, pump B-01 B was cut off and pump B-03 B was the standby pump of B-01 A and B-03 B. This recommendation reduces project costs by \$72,100. To verify the pump availability it is necessary to define a reliability requirement, which in this case is 95.61% in 3 years with 90% confidence. Such methodology was implemented in seven new plant projects, and it was possible to save \$1,153,200 by reducing standby pumps.

**FIGURE 4.17**

One standby pump for two operating pumps.

Fig. 4.18 shows the new configuration without the diesel generators. The new electrical energy configuration achieved 99.99% availability and 83% reliability in 20 years. Such analysis saved \$2,500,000 in this project. A similar analysis was performed for another energy generation redundancy (light company energy supplier), and in this case the new electrical facility configuration achieved 99.99% availability and 93% reliability in 3 years. In this case the analysis helped save \$969,610. The final solution was to reduce diesel generation because it is possible to reduce more costs and also to reduce accident risk in diesel tanks.

The third redundancy case concerns the redundancy supply of a feed product for a hydrogen generation unit. This unit can be fed by natural gas or propane. In some cases, depending on the vulnerability in H<sub>2</sub> supply, it is possible to implement a second feed line to supply propane in the event of unavailability of natural gas. Regarding natural gas produced by a refinery process, such vulnerability is low, and, in fact, if such natural gas supply stops it means that some plants in the refinery stop, and consequently the hydrogen generation unit plant will probably stop as well. In the natural gas line there is only one vessel (V-01) that has a low failure probability in 3 years. Fig. 4.19 shows the two lines. The first one shows natural gas flow and includes only a natural gas feed vessel (V-01), and the second one represents the propane flow, which includes the propane feed vessel (V-08), the propane pump (J-03 A/B), and the propane vaporizer (C-08). The start and end blocks require RBD logic.

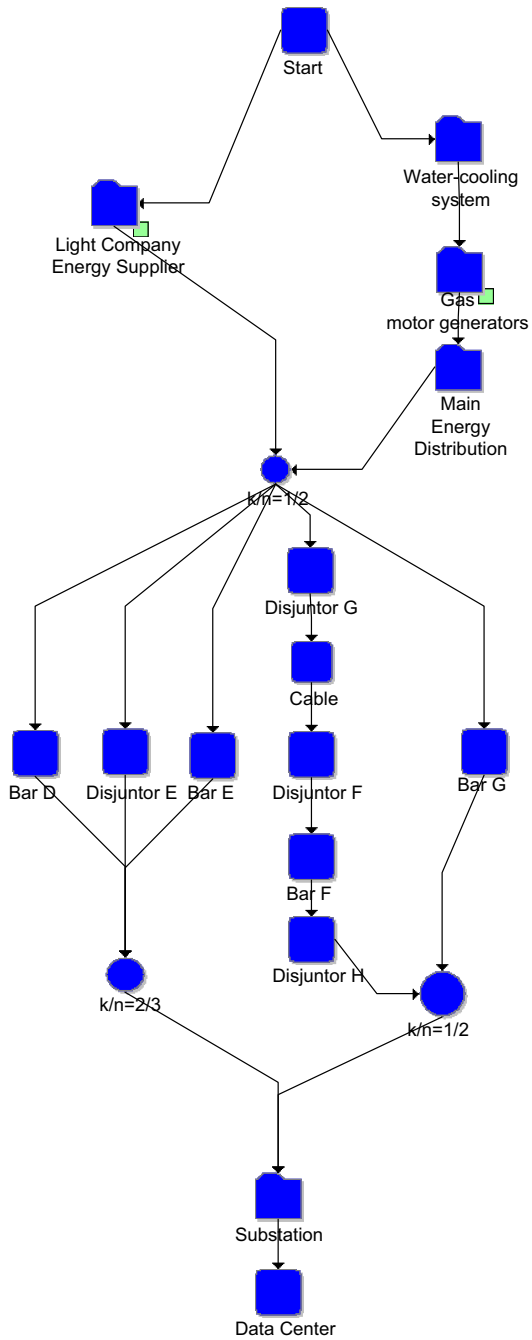
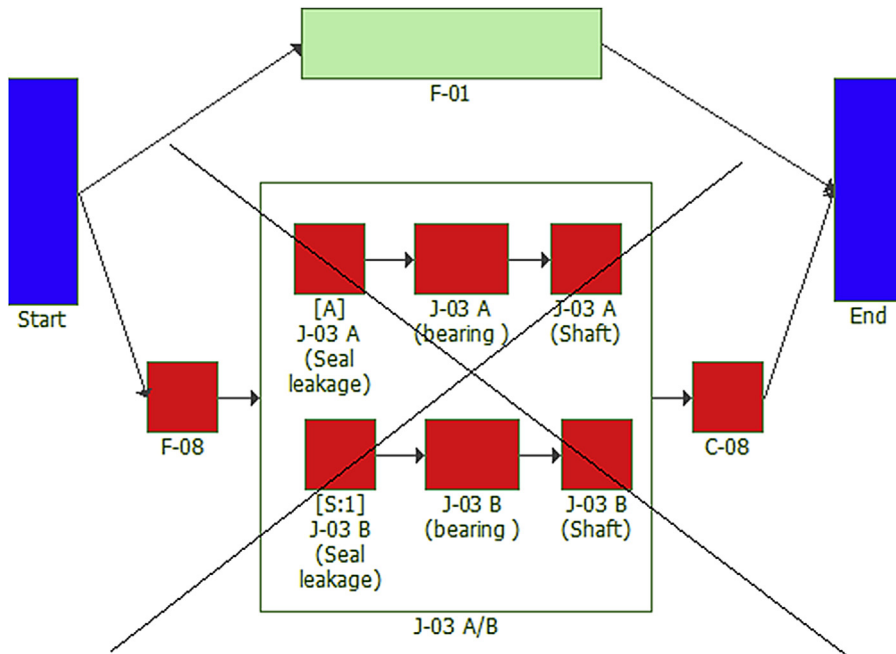


FIGURE 4.18

Reducing electrical energy redundancies.



**FIGURE 4.19**

Reducing hydrogen generation unit plant feed redundancy.

After performing simulation the feed subsystem has 100% availability in 3 years. In addition, when equipment from the second line, which supplies propane, is removed from the RBD, the feed subsystem availability is also 100% in 3 years. Reducing the number of equipment saved \$179,100 in this project. The following hydrogen generation unit projects in this company did not have feed redundancy based on this first project.

### 4.3.2 MAINTENANCE POLICIES

Preventive maintenance and inspection policies are very well defined when specific tools are carried out like Reliability Centred Maintenance (RCM) and Risk Based Inspection (RBI) analysis. Unfortunately, such methods do not predict the impact of preventive maintenance and inspection on system and equipment (component) reliability as well as operational availability.

In case of equipment or component with wear out which is represented by increasing failure rate, the preventive maintenance recover such equipment reliability when takes place before the wear out phase. The wear out pattern is well represented by different types of PDFs such as normal, logistic, Gumbel, or other generic PDFs, such as Weibull. In case of random failures, which are well represented by exponential PDFs, such reliability recovery is not possible. Let us consider case 1, with a Weibull PDF ( $\beta = 3$  and  $\eta = 3.5$ ). In case of preventive maintenance carried out in 1 year, the positive

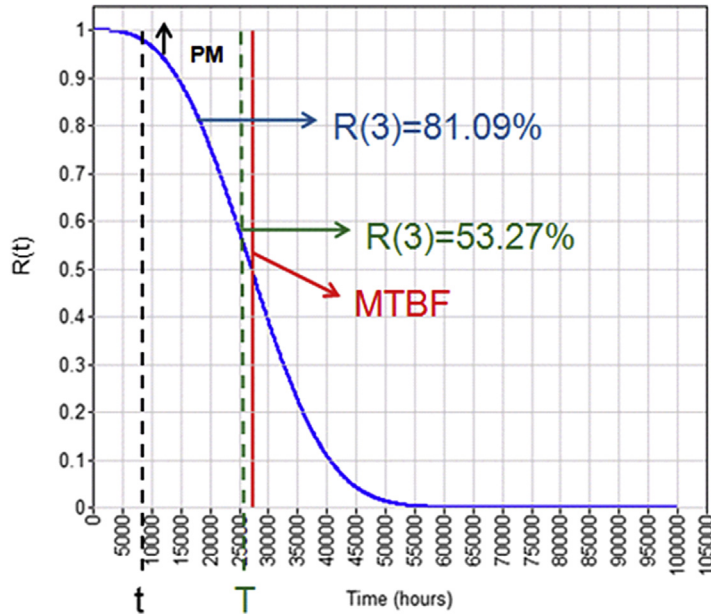


FIGURE 4.20

Reliability recovered by preventive maintenance (Software CAFDE from BQR).

impact is that the reliability in 3 years is 80.90%. If no preventive maintenance is carried out the reliability in 3 years is 53.27%. Fig. 4.20 shows the reliability recovered.

The mathematical approach to calculate the effect of preventive maintenance is demonstrated by the following equations.

Reliability in 3 years without preventive maintenance:

$$R(T) = e^{-\left(\frac{T}{n}\right)\beta}$$

$$R(T) = e^{-\left(\frac{3}{3.5}\right)^3} = 0.5327$$

Reliability in 3 years with preventive maintenance in 1 year:

$$R(T) = R(t) \times R(T - t)$$

$$R(T) = e^{-\left(\frac{t}{n}\right)\beta} \times e^{-\left(\frac{T-t}{n}\right)\beta}$$

$$R(T) = e^{-\left(\frac{10}{3.5}\right)^3} \times e^{-\left(\frac{3-10}{3.5}\right)^3}$$

$$R(T) = e^{-\left(\frac{10}{3.5}\right)^3} \times e^{-\left(\frac{3}{3.5}\right)^3}$$

$$R(T) = 0.9772 \times 0.8298 = 0.81099$$

The important fact is to observe the mistake when the mean time before failure (MTBF) is defined as an index and parameter to define the interval of preventive maintenance. In this case if the MTBF is used as a reference to define the preventive maintenance interval, there will be a high risk that the failure is not avoided by preventive maintenance.

Let us consider now case 2, where the same equipment failure is represented by a Weibull PDF ( $\beta = 1$  and  $\eta = 3.5$ ) with an exponential pattern. In this case, Fig. 4.21 shows that if preventive maintenance is carried out in 1 year, the reliability in 3 years is 42.44%, which is similar if no maintenance is performed in 1 year. In other words, for random failure, it is better not to perform preventive maintenance.

The mathematical approach to calculate the effect of preventive maintenance in random failures is demonstrated by the following equations.

Reliability in 3 years without preventive maintenance:

$$R(T) = e^{-\left(\frac{T}{\eta}\right)^\beta}$$

$$R(T) = e^{-\left(\frac{3}{3.5}\right)^1} = 0.4244$$

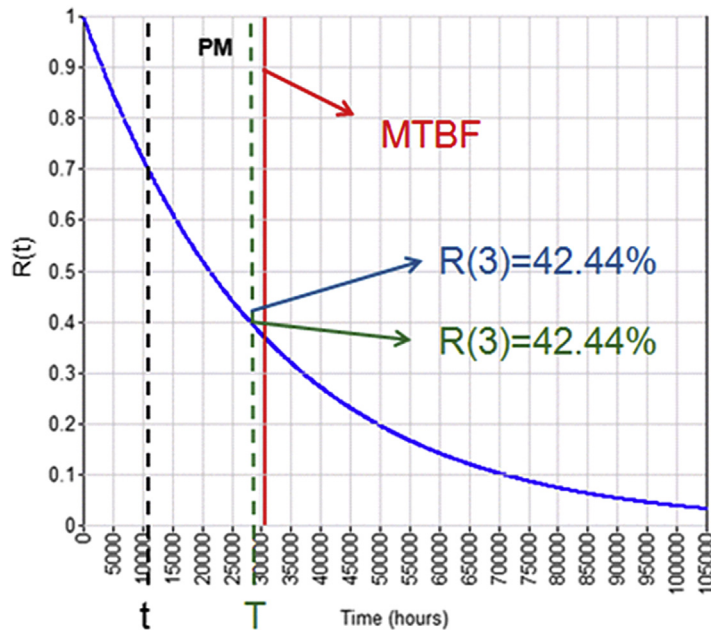


FIGURE 4.21

Reliability not recovered by preventive maintenance (CAFDE – BQR).



Reliability in 3 years with preventive maintenance in 1 year:

$$R(T) = R(t) \times R(T - t)$$

$$R(T) = e^{-\left(\frac{1.0}{3.5}\right)1} \times e^{-\left(\frac{3-1.0}{3.5}\right)1}$$

$$R(T) = e^{-\left(\frac{1}{3.5}\right)1} \times e^{-\left(\frac{2}{3.5}\right)1}$$

$$R(T) = 0.7557 \times 0.5647 = 0.4244$$

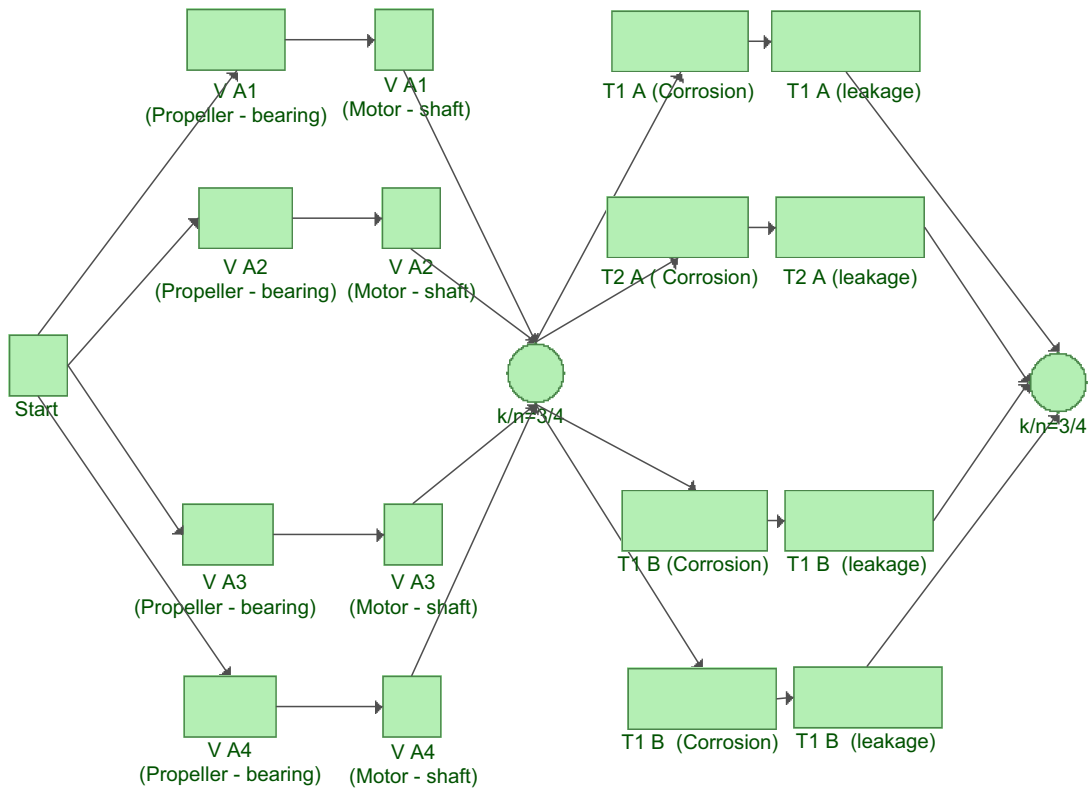
$$R(T) = e^{-\left(\frac{3}{3.5}\right)1} = 0.4244$$

The additional important assessment is to check the impact of such preventive maintenance system and equipment operational availability. Thus RAM analysis is a good tool for assessing maintenance policies. Some maintenance policies are defined by procedures, others by suppliers, and others by expert opinion, but all of them can be tested in RAM analysis. Despite this, it is not common to test maintenance policies in RAM analysis, because in some cases reliability engineers do not have maintenance specialists on the RAM analysis team or it is assumed that the maintenance plan will not affect plant availability. In real life, it is hard to define maintenance policies for all equipment and test such policies in RAM analysis to check maintenance policies' impact on system availability. This can be explained by different equipment characteristics, which require different maintenance policies that are the responsibility, in terms of maintenance, of a different group of specialists. In some cases, specialists have no idea about all equipment components. Some of them are responsible for mechanical components and others for electric and electronic components. Despite such complexity, RAM analysis simulation results and critical analysis show which is the most critical equipment for the system, and in this case maintenance policy can be tested in the RAM analysis to see the impact of critical equipment maintenance policy on system availability. Because of this, reliability specialists may support the maintenance team to verify whether their maintenance policy affects system availability.

As an example, the maintenance policy for an air cooler heat exchanger that will operate in different process conditions than in previous projects was tested by RAM analysis. Process engineers have some doubts about the air cooler performance, and believe it will not achieve the expected availability of 99.86% in 4.5 years. As the previous projected air cooler failure data cannot be used for this new project, the proposed solution is to perform preventive maintenance over 4.5 years to keep the availability target. Fig. 4.22 shows the air cooler RBD with the main components: the fans and tubes.

The expected failures in fan components are propellers, bearings, and motor shaft failure, and the expected failures in tubes are corrosion or leakage. The maximum expected reliability degradation is 60%, which means that components will fail around 2 years (PDF failure; normal:  $\mu = 2$ ,  $\sigma = 1$ ). Therefore the air cooler configuration requires at least three out of four fans available and three out of four tubes available not to shut down the air cooler. In the event that any such conditions do not achieve air cooler shutdown, consequently the system will reduce production capacity. Fig. 4.23 shows how to implement preventive maintenance in RAM analysis using software simulation (BlockSim 7). In the air cooler example, preventive maintenance will take place each year and in the 11th month fans and tubes will be implemented to reduce vulnerability.

As shown in Fig. 4.23, preventive maintenance did not bring the system down, and by performing such preventive maintenance the air cooler achieved 99.41% in 4.5 years, a little bit less than the previous expected availability (99.86% in 4.5 years). In this way, even in the pessimistic case where



**FIGURE 4.22**

Air cooler preventive maintenance RBD.

there would be reliability degradation, it is possible to achieve a similar availability target by performing preventive maintenance.

A further step after defining the preventive maintenance and inspections for system and equipment is to optimize such preventive maintenance and inspections tasks in order to maximize the operational availability and minimize the life cycle cost. Section 4.5 will demonstrate the concept of preventive and inspection optimization in minimize the life cycle cost and maximize the operational availability.

### 4.3.3 A GENERAL RENOVATION PROCESS: KIJIMA MODELS I AND II

To assess the impact of preventive maintenance on reliability it is also important to take into account the concept of independent and identically distributed.

Independent means the maintenance (preventive and corrective) and other events that happen in the past will not influence equipment (component) performance in the future.

Identically distributed means equipment (or components) after repair or replaced will have a similar PDF, or, in other words, the same failure behavior over time.

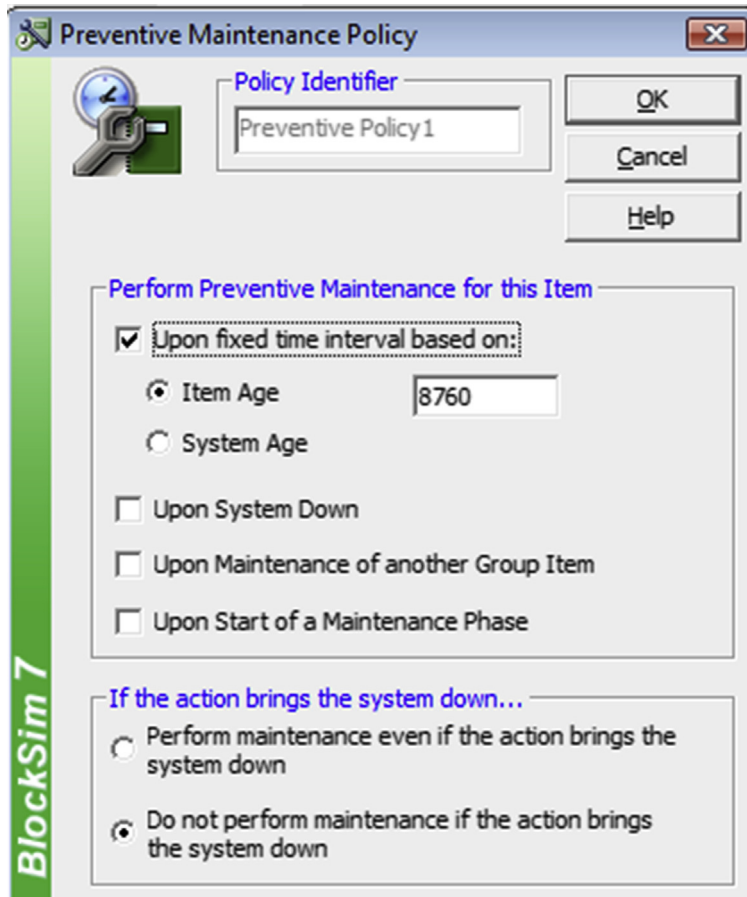


FIGURE 4.23

Air cooler preventive maintenance RBD (BlockSim 7).

Fig. 4.24 shows the independent and identically distributed equipment failure with similar time between failures after repair.

In fact, such assumptions are based on the hypothesis that after repair or replacement the equipment condition is “as good as new.” Such assumption is considered for many replaced (nonrepairable) items and also repairable items with as good as new condition after each repair.

However, the operational environment conditions as well as human error during transportation, installation, and maintenance led such items to degrade after repair and even replacement. Therefore it is necessary to take into account the degradation effect of repair or replacement in repairable and nonrepairable equipment.

To predict the equipment future number of failures, operational availability, and production efficiency, it is necessary to verify the degradation effect after replacement or repair. In fact, the reliability

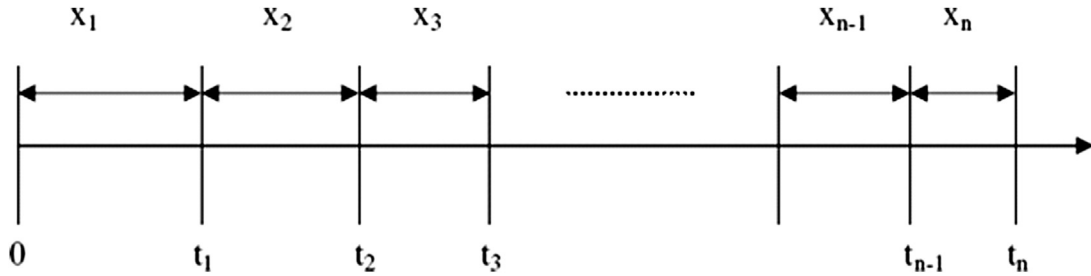


FIGURE 4.24

Independent and identically distributed equipment failure pattern.

growth method allows similar calculation for each individual equipment without taking into account the complex system configuration.

Because of this the degradation needs to be expressed as a restoration factor to be taken into account in an RBD model during RAM analysis.

The Kijima models I and II, proposed by Kijima and Sumita in 1986, are known as a general renovation process based on component virtual life. Such a method is used to measure how much is reduced in component age when some repair is performed and can be:

- Age reestablishment based on last intervention (Kijima I);
- Age reestablishment based on all interventions (Kijima II).

In the first case the Kijima model I considers that reestablishment component age occurs only for the last failure after maintenance is performed. In this way the model considers that the *i*th repair does not remove all reliability loss until the *i*th failure. Therefore, if *t<sub>i</sub>* is the time between failures, the component’s age with regard to degradation effect over a long time is represented by:

$$x_i = x_{i-1} + q \cdot h_i = qt_i$$

where *h<sub>i</sub>* = time between (*i* – 1) and an *i*th failure, *q* = restoration factor ( $0 \leq q \leq 1$ ), as-bad-as-old = 0 and as-good-as-new = 1, *x<sub>i</sub>* = age in time *i*, and *x<sub>i-1</sub>* = age in time *i* – 1.

In the second case the Kijima model II considers that reestablishment component age occurs for all failures over component life since the first one. This model considers that the *i*th repair removes all reliability loss until the *i*th failure. Thus the component age has a proportional effect over time, represented by:

$$x_i = q(h_i + x_{i-1}) = q(q^{i-1}h_1 + q^{i-2}h_2 + \dots + h_i)_i$$

For example, Kijima model II was applied to assess the effect of stock deterioration of a pump component. Such degradation is similar to the effect of an as-bad-as-old repair, because thanks to bad stock conditions, such pumps have their component in stock as as-bad-as-old when a failed pump needs a replacement. Thus for Kijima model II and *q* = 0.01 the pump availability reduced from 99.72% to 50.39% in 1 year. Fig. 4.25 shows pump operation over 1 year for as-good-as-new condition after corrective maintenance.

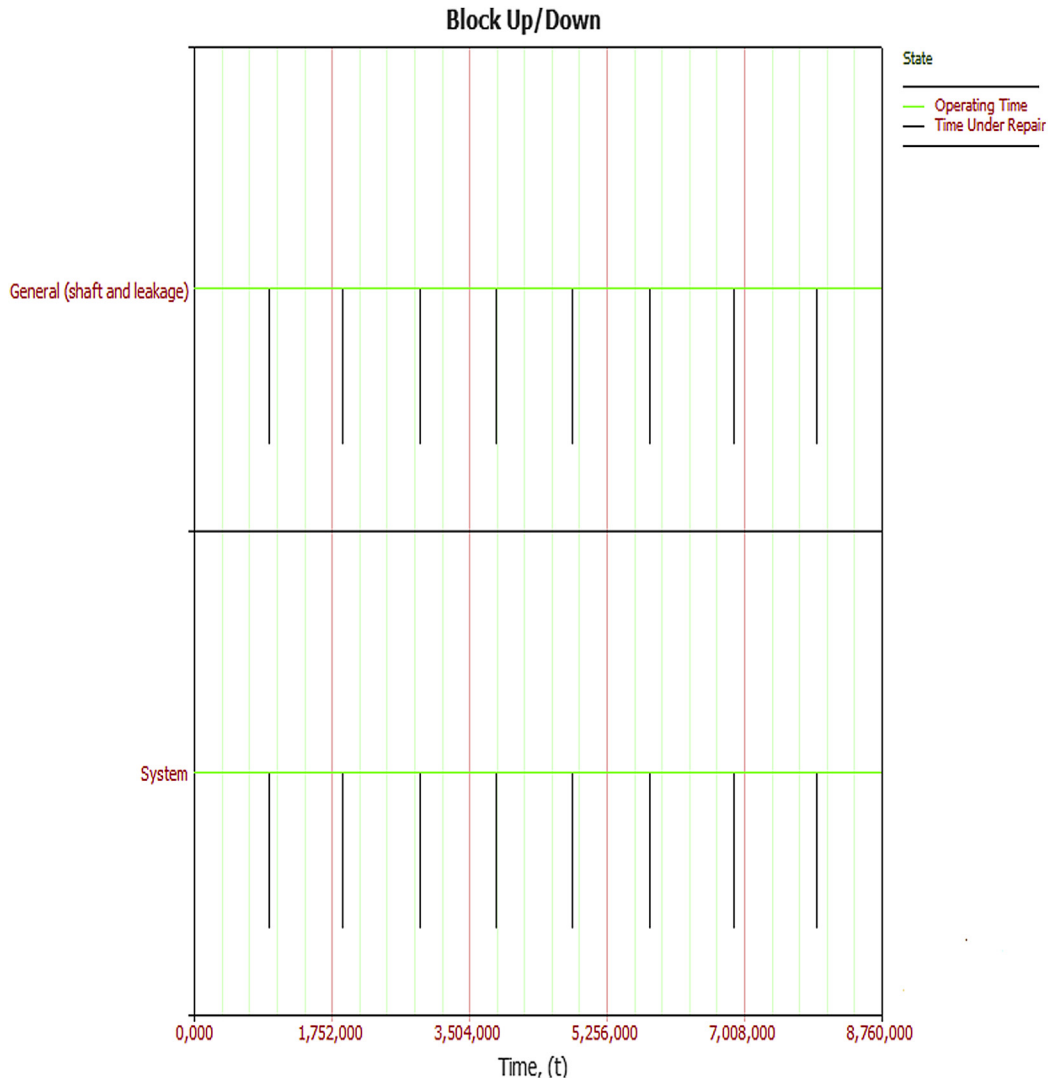
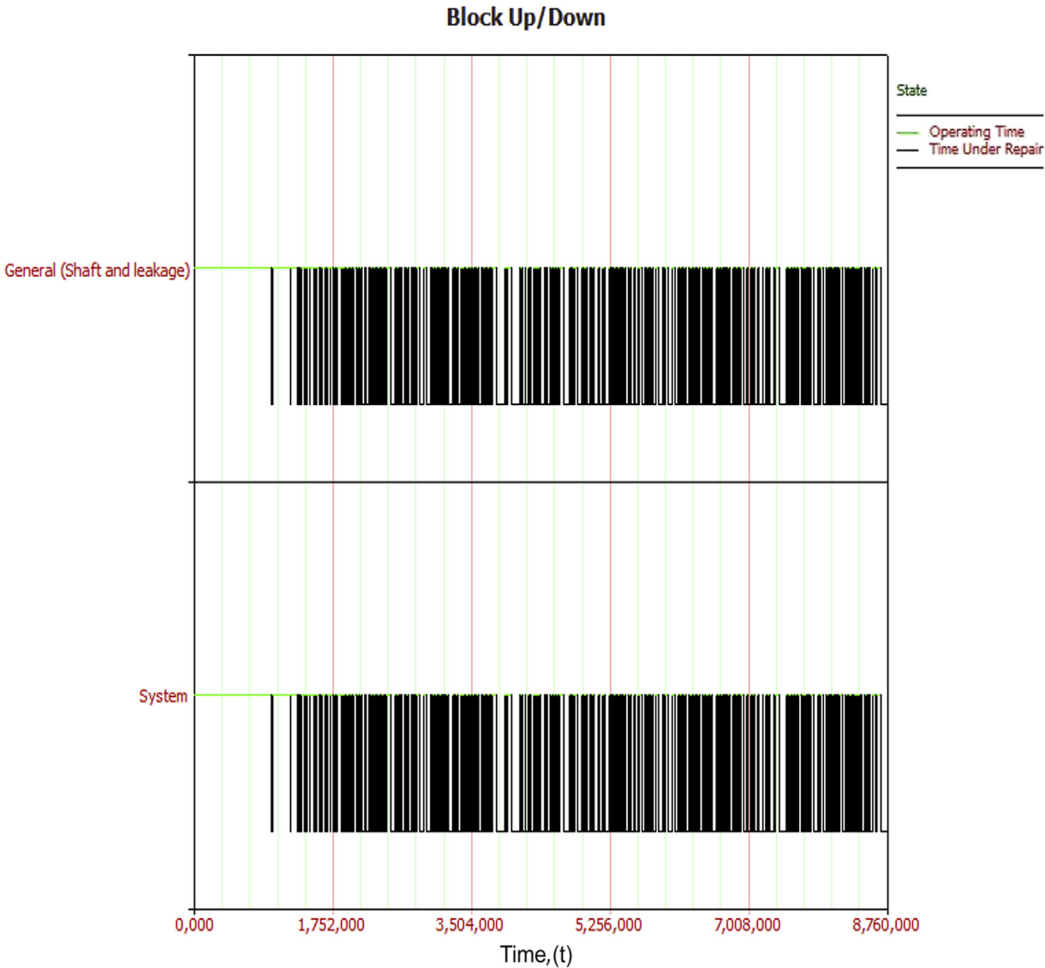


FIGURE 4.25

Pump operations (as-good-as-new).

As shown in Fig. 4.25, despite eight failures over 1 year the repair was as-good-as-new and reliability was totally reestablished after repair. Thus the time between failures is constant over time. Unfortunately, because of a bad stock condition, the pump in stock was as-bad-as-old when it replaced the failed one. Fig. 4.23 shows the effect of degradation.

As shown in Fig. 4.26, the repair is as-bad-as-old and as soon as the pump was repaired it failed again because the components were as-bad-as-old. The as-bad-as-old condition happens in many types of equipment such as pumps. An as-good-as-new condition is hard to achieve in real life, and in most cases restoration factors are between 0% and 100% with the tendency to reduce over a long time as long as repairs take place. Restoration factors with 100% mean as-good-as-new and mostly this is with regard to nonrepairable equipment. This means whenever there is a failure, equipment is replaced with new equipment. To improve repair efficiency, new procedures were established to manage components in stock to keep them as-good-as-new so as not to impact system availability when a failure component is replaced by another in stock.



**FIGURE 4.26**  
Pump operations (as-bad-as-old).

#### 4.3.4 STOCK POLICY

The stock policy is another consideration in sensitivity analysis because when there is excess stock more money is being spent than necessary. Stock policy in most cases does not affect system availability, but when there is not enough stock, the system may be unavailable more than necessary when a failure occurs because the required components are not in stock. Maintenance can also be delayed for this reason. In some cases, this is critical because it is necessary to import or even assemble such a component, and this has a huge impact on system availability. Best practice is usually to find out the optimum stock level of cost and demand. In system availability, demand means component failure, so a new component will be demanded when the current component fails and it is not possible to fix it or it is better to replace it than fix it. In refinery plants, drill facilities, and platforms, unavailability costs are often much higher than component stock costs, so the minimum stock level is a good stock policy.

Note that minimum stock level does not mean zero stock level for all equipment. Depending on reliability over time, some equipment can have a zero stock component level for a specific period of time, but other critical equipment that is expected to fail has to define the number of components in stock so as not to impact system availability, and in the case of failure, more time than necessary. This means that in addition to repair time, if a component is not in stock, additional time will be required to purchase a component and such additional time means additional system downtime.

A stock policy example was applied in a catalytic cracking plant in which coke formation occurs approximately every 6 months, and the furnace's tube is the most critical equipment component. If there is no stock for the furnace tube, when it is necessary to stop the furnace to remove coke formation and it requires new tubes, there will be additional furnace downtime related to additional time to purchase new tubes. In this case, purchase time will delay on average 360 hours (normal PDF:  $\mu = 360, \sigma = 240$ ). The availability of the furnace is reduced from 99.91% to 92.61% in 3 years. This directly impacts the catalytic cracking plant system availability, because if the furnace is unavailable, the system is unavailable. Additional stocks are required for heat exchangers P-03 and P-11, because there is a 23% chance that such equipment will fail after 3 years, and if such equipment fails, the system will be unavailable. Thus regarding the minimum stock level for all equipment, system availability will increase from 90.77% (zero stock policy) to 99.53% (minimum stock policy) in 3 years. A minimum stock level policy means having one tube package for each furnace, one tube package for heat exchangers, and zero stock for other equipment. Table 4.4 shows the stock policy simulation results.

In the first column in Table 4.4 the components in stock are given, and in the second column the average stock level (ASL) is shown. The stock of tubes for P-03 and P-11 is approximately one, and for the furnace it is approximately zero (0.3443), which means such a component is used constantly over 3 years. The third column gives the number of components from the warehouse, and it is possible to see that furnace tubes were demanded approximately six times in 3 years as expected. The fourth column gives the expected average time to restock each component. The fifth column shows the rejected components, that is, the components that were demanded but were not in stock. And, finally, the sixth column gives the emergency time, which is the time required to buy a new component when there is not such a component in stock.

It is also important to define when it is necessary to replace stock when there is a zero stock for one specific piece of equipment. In the previous case the plant will operate every 3 years, followed by programmed maintenance. This is a usual concept for refinery plants.

Stock	SA	Items Display	ATRS (hours)	Rejected Items	Emergency Time (hours)
Leak (pump)	0	0.27	414,233	0	0.27
Other pump stocks	0	1.24	649,667	0.02	1.24
Tube (heat exchanger 1)	0	0	0	0	0
Tube (heat exchanger 2)	0	0.005	497,124	0	0.005
Plate (external corrosion tower)	0	0	0	0	0
Plate (internal corrosion tower)	0	0	0	0	0
Tube (heat exchanger incrustation)	0	0	0	0	0
Plate (internal corrosion vase 1)	0	0	0	0	0
Plate (internal corrosion vase 2)	0	0	0	0	0
Tube (internal corrosion P-11)	0.8924	0.27	0	0	0
Electric motor (compressor)	0	0	0	0	0
Electric motor (compressor)	0	0	0	0	0
PE external corrosion reactor	0	0	0	0	0
PE internal corrosion reactor	0	0	0	0	0
Tube (coke formation F-01 A)	0.3443	5.705	0	0	0
Other furnace stocks	0	0	0	0	0
Tube (internal corrosion P-03)	0.8882	0.285	0	0	0

SA, stock average; ATRS, average time to replace stock.

There are other systems in the oil and gas industry such as platforms, drill facilities, and electrical facilities that operate for no specific period of time but for as long as possible. For this kind of system it is necessary to define when to restock equipment components. An example is electrical energy cogeneration that generates electrical energy by turbine, which is fed by vapor from refinery process plants. The longer such a system operates, the better, because it is the energy supply. Table 4.5 shows the main turbine component and the stock level when the turbine starts to operate. As discussed before, depending on component reliability, it is not necessary to have components in stock at the beginning of the equipment life cycle. However, in case of zero stock policy at the beginning of the equipment life cycle, it must be planned when it is necessary to get components in stock.

In Table 4.5 the component is shown in the third column, in the fourth column the initial stock level is shown, and the fifth column gives the maximum restock time. Such time is based on the PDF failure of each component, thus for the rotating part and labyrinth there is no restock time defined because such PDF failure is exponential. Despite a long period of time expected before a random failure occurs, failure may occur at any time and therefore a component needs to be in stock. Such components will require period inspections to define restock time periods.

Other components such as shafts, rotation axes, and couplings have defined periods of time to restock confirmed by inspections. The sixth column of Table 4.5 gives the details that support the restocking policy.



**Table 4.5 Turbine Stock Level**

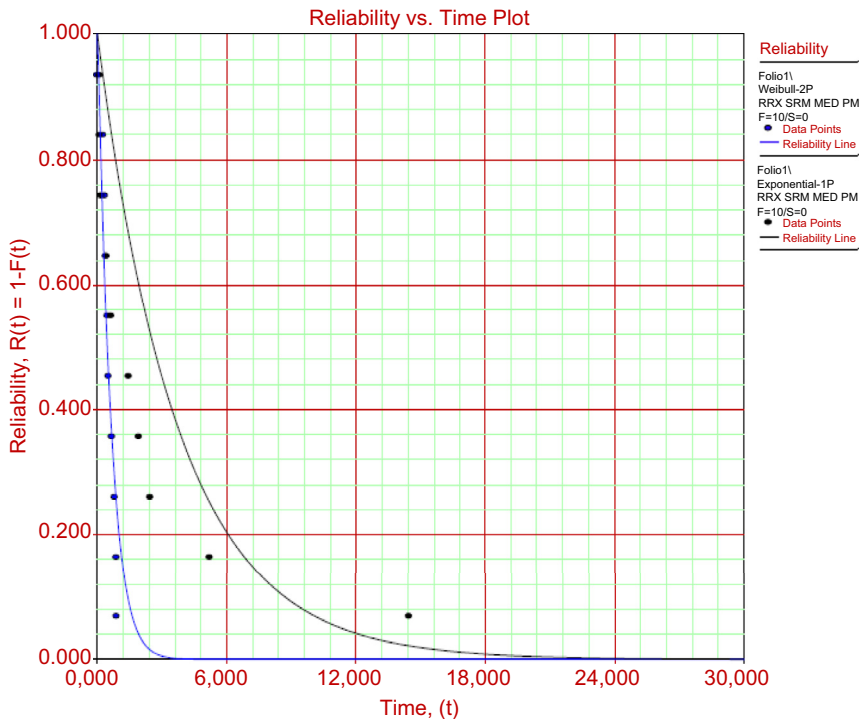
Equipment	Tag	Component	Minimum Stock Level	Maximum Restock Time (years)	Observation
Turbine	TG-01	Rotation part	1	0	Replace stock whenever stock achieves zero level. Random failure ( $\lambda = 0.005$ )
		Labyrinth	1	0	Replace stock whenever stock achieves zero level. Random failure ( $\lambda = 0.004$ )
		Shaft	0	7.5	The failure PDF is Gumbel with parameters $\mu = 10$ , $\sigma = 2$ . This means a low chance of failure occurring at the beginning of the life cycle. Thus 7.5 years would be the maximum replacement time, that is, 8 ( $10 - 2 = 8$ ) years less 180 days
		Rotation axis	0	12.5	The failure PDF is Gumbel with parameters $\mu = 15$ , $\sigma = 2$ . This means a low chance of failure occurring at the beginning of the life cycle. Thus 12.5 years would be the maximum replacement time, that is, 13 ( $15 - 2 = 13$ ) years less 180 days
		Coupling	1	7.5	The failure PDF is Gumbel with parameters $\mu = 10$ , $\sigma = 2$ . This means a low chance of failure occurring at the beginning of the life cycle. Thus 7.5 years would be the maximum replacement time

### 4.3.5 LOGISTICS

The final and no less important consideration in sensitivity analysis is logistics. Most of the time when performing RAM analysis it is considered that plant boundaries will not affect system availability, but facility plants such as those that supply electric energy, vapor, and gas, and other plants that supply other products may have some influence on the main plant's availability. In some cases, because engineers and project managers know that such influences exist, they created a robust logistic, which in some cases is enough to avoid main system shutdown but in some cases it is not. In this way, logistics must be assessed by reliability professionals to guarantee that outside issues do not influence the plant being assessed by RAM analysis. The first step is to assess facilities such as energy and products

system supplier availability. In most cases, unavailability of such facilities directly affects plants. The second step is to assess which plants affect the main plant considered in RAM analysis. Finally, the third step is to assess the stock and supply logistic resources such as tanks and pumps.

An example of the logistical impact in a sensitivity analysis is to assess how the impact of energy supply shutdown in a hydrodesulfurization plant affects availability. In this refinery, two energy shutdowns per year are expected with 16 hours to repair and reestablish the system. The energy supply system has 99.625% availability in 3 years, and 5.98 failures over 3 years are expected. Such availability impacts the hydrodesulfurization plant availability, which reduces from 98.237% to 97.04% in 3 years. Such availability is below the availability target, which is 98% in 3 years. In doing so, cogeneration is proposed to increase energy supply system availability. Fig. 4.27 shows how the reliability of the electrical energy supply system increases after cogeneration is implemented.



**FIGURE 4.27**

Energy supply  $\times$  cogeneration supply (reliability).

The first line on the left shows the electrical system supply without cogeneration (turbine) and the second one on the right is with cogeneration (turbine).

The turbine that generates electrical energy will be the main energy supplier, and if this system shuts down, the energy company supplier will be demanded to supply energy to the refinery. In terms of the RBD there are two blocks in parallel, the previous electrical energy supply system and the turbine, that is, the cogeneration system.

In this way the new availability of the cogeneration system is 99.9% in 3 years and consequently the hydrodesulfurization plant availability will be 98.154% in 3 years. Now, at most one (1.49) shutdown is expected with the cogeneration supply system. Looking only at the system the availability is 98.237% in 3 years. As such the system (hydrodesulfurization plant) is in series with the cogeneration system, and the final availability is given by:

$$A(\text{HDT final}) = A(\text{Cogeneration system}) \times A(\text{HDT})$$

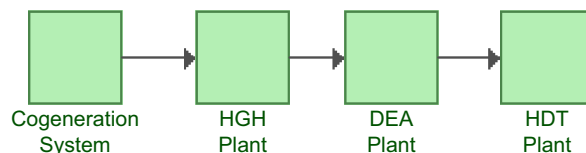
The additional sensitivity analysis is required to find out which impact other plants, such as a hydrogen generation plant and diethylamine plant, have on hydrodesulfurization plant system availability. The main objective of a hydrodesulfurization plant is to remove the sulfur component from the diesel product to meet customer specification requirements. Thus the hydrodesulfurization plant system must be supplied hydrogen from the hydrogen generation unit to perform reactions in the hydrodesulfurization plant reactors, and the diethylamine plant is needed to receive acid gas. Thus if the hydrogen generation unit or diethylamine systems shut down, the hydrodesulfurization plant will be unavailable. Representing such conditions in an RBD and for the electrical energy supply system, Fig. 4.28 shows the logistics condition.

In this case the availability of the cogeneration system, the hydrogen generation unit, and the diethylamine and hydrodesulfurization plants are 99.90%, 99.74%, 100%, and 98.237%, respectively. Thus the final availability in the hydrodesulfurization plant will be 97.997% in 3 years, which is approximately 98%. All these blocks are in series so the final hydrodesulfurization plant availability result from all system availability is represented by:

$$A(\text{HDT final}) = A(\text{Cogeneration system}) \times A(\text{UGH}) \times A(\text{DEA}) \times A(\text{HDT})$$

Note that even if each plant achieved its availability target, 98% in 3 years, the main plant, the hydrodesulfurization plant, would not achieve such a target because it will be impacted by the unavailability of other systems.

The third case in logistic sensitivity analysis is when logistic resources such as tanks and pipelines are considered system vulnerabilities. Most of the time such logistic resources have high availability, and in some cases are projected with redundancy to reduce system vulnerability. An example of such a



**FIGURE 4.28**

RBD (cogeneration system, HGH, Hydrogen generation Unit (UGH), Diethanolamine plant (DEA), and Hydrotreater Plant (HDT)).

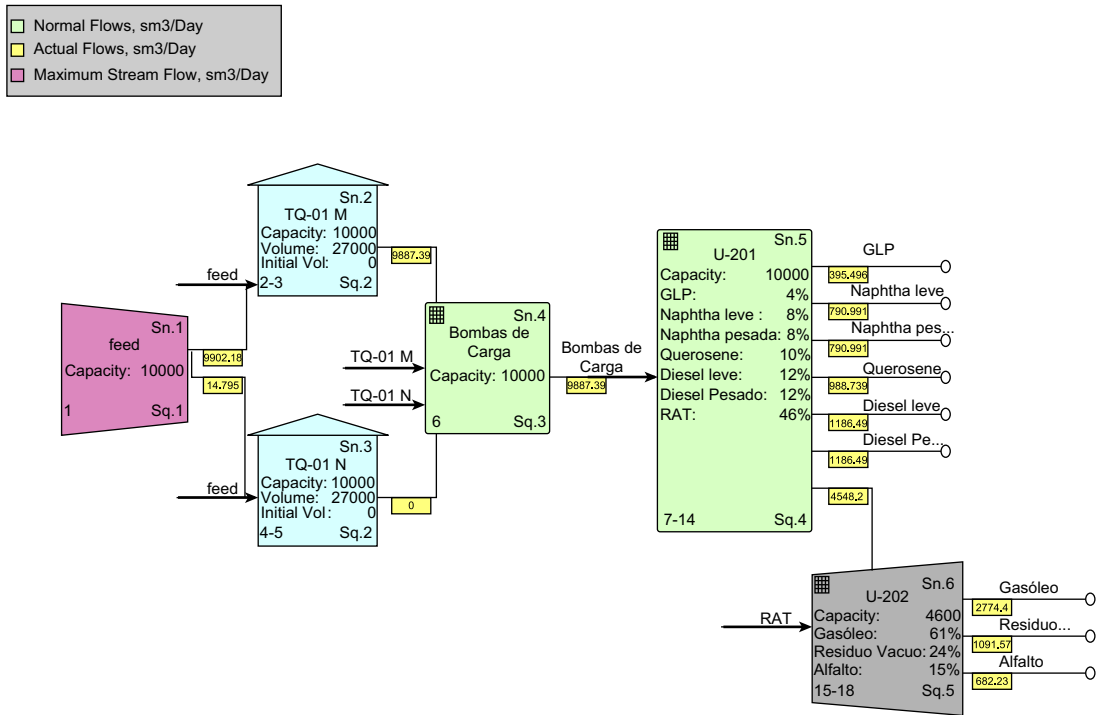


FIGURE 4.29

RBD (refinery I).

logistic resource is a refinery that produces diesel like the previous example, but now the main objective is to assess the upstream effect in hydrodesulfurization plant availability. Thus the logistic model uses two distillation plants, two tanks, and two feed pumps. Fig. 4.29 shows this complex logistic refinery system without the hydrodesulfurization plant, hydrogen generation unit, and diethylamine system.

The refinery represented in Fig. 4.29 achieves 98.87% availability in 5 years. This complex model also regards direct effects among systems and flow of product. So the unavailability that occurred before U-02 (distillation plant) affects all refineries, but in case of U-02 shutdown, the U-01 plant produces other products and refineries have partial production losses related to U-02 loss of production. Refinery II, as shown in Fig. 4.30, includes the hydrodesulfurization plant (U-10), hydrogen generation unit (U-09), and the diethylamine plant (U-11). Now the system (refinery) availability is 97.2% in 3 years and the plant that limits refinery availability is the hydrodesulfurization plant, which achieves 98.18% in 3 years.

The concept of refinery II is different from refinery I, because in the first case, both plants (U-01 and U-02) produce diesel, and if U-02 shuts down, part of the diesel is produced by U-01. The refinery II concept assumes all diesel products have to be treated by the hydrodesulfurization plant so such diesel production is limited by the hydrodesulfurization plant.

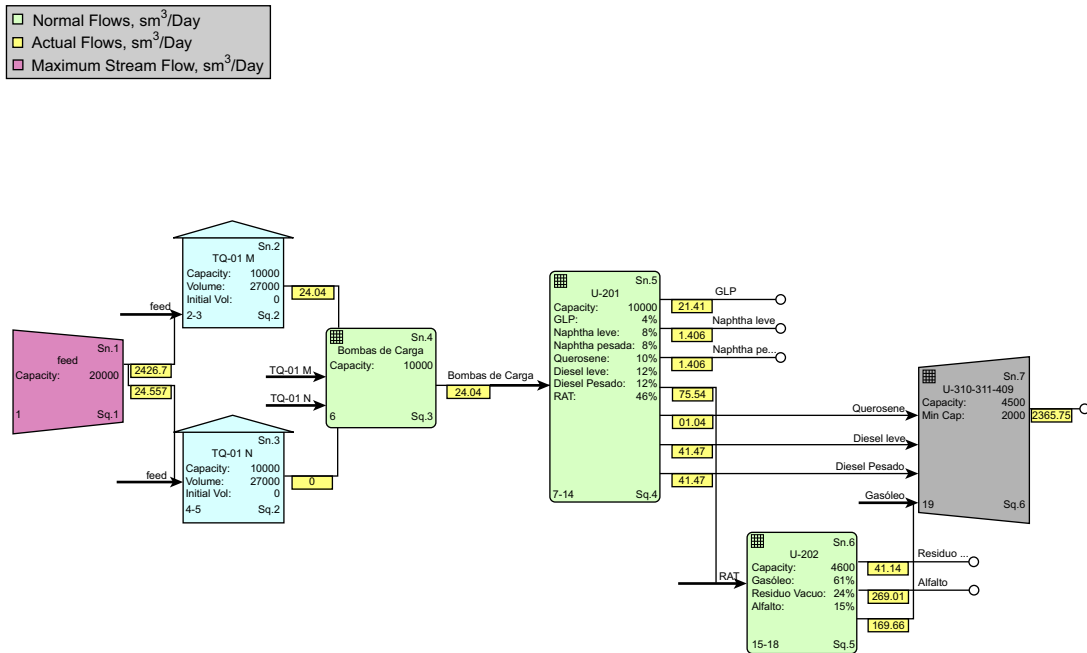


FIGURE 4.30

RBD (refinery II).

This case shows that, as expected, logistic resources are not the reliability bottleneck of the system; however, one important plant that influences system (refinery) availability is the hydrodesulfurization plant.

When regarding a complex system such as a refinery plant, whenever it is possible RAM analysis must include logistic issues because of the main effect on system availability. Such analysis is RAM + L analysis, that is, reliability, availability, maintainability, and logistic analysis. In the following, a RAM + L analysis case study concerning a complex refinery plant is presented.

#### 4.4 IMPROVEMENT ALLOCATION BASED ON AVAILABILITY

As discussed in Section 4.2.4 the RI and AI indexes supply information about which subsystem or equipment influences system performance in terms of reliability and availability. When subsystems and equipment are in series, another way to detect critical subsystems and equipment is to find out which one has the lowest reliability or availability.

As stated before, in a system in which the RBD is configured in series, the lowest reliability will limit system reliability and the lowest availability will limit system availability. This means that system reliability or availability will be equal to or lower than the lowest subsystem reliability or availability. For example, if a system with three subsystems has 100% availability in 1 year for

subsystems 1 and 2 and 90% availability for subsystem 3, the system availability in 1 year will be 90%, as shown in the following equation:

$$A(\text{System})(t) = A(\text{Subsystem 1})(t) \times A(\text{Subsystem 2})(t) \times A(\text{Subsystem 3})(t)$$

If  $t = \text{year}$ :

$$A(\text{System})(1) = A(\text{Subsystem 1})(1) \times A(\text{Subsystem 2})(1) \times A(\text{Subsystem 3})(1)$$

$$A(\text{System})(1) = 1 \times 1 \times 0.9 = 0.9 = 90\%$$

Most of the systems in the oil and gas industry, such as platforms, refinery plants, and drill facilities, are configured in series in the RBD at the subsystem level. In some cases, to identify which subsystem requires improvement to achieve system availability, the “availability improvement methodology” can be applied, and it is necessary to follow these steps:

1. Define the system availability target;
2. Define the minimum subsystem availability value;
3. Identify the critical subsystem that has availability lower than the minimum availability;
4. Define the availability target for the critical subsystem.

In the first step the system availability is defined by the company or by RAM analysis simulation. In the second step, to define the minimum subsystem availability, all subsystems are regarded in series, that is, if we have one system with three subsystems, system availability will be:

$$A(\text{System})(t) = A(\text{Subsystem 1})(t) \times A(\text{Subsystem 2})(t) \times A(\text{Subsystem 3})(t)$$

$$MA(\text{Subsystem})(t) = \text{Minimum subsystem availability}$$

$$\begin{aligned} MA(\text{Subsystem})(t) &= A(\text{Subsystem 1})(t) = A(\text{Subsystem 2})(t) \\ &= A(\text{Subsystem 3})(t) \end{aligned}$$

Then:

$$A(\text{System})(t) = A(\text{Subsystem 1})(t) \times A(\text{Subsystem 2})(t) \times A(\text{Subsystem 3})(t)$$

$$A(\text{System})(t) = MA(\text{Subsystem})(t) \times MA(\text{Subsystem})(t) \times MA(\text{Subsystem})(t)$$

$$A(\text{System})(t) = MA(\text{Subsystem})(t)^3$$

$$MA(\text{Subsystem})(t) = \sqrt[3]{A(\text{System})(t)}$$

The general equation to define the minimum availability for a system with  $n$  subsystems in series is defined by:

$$MA(\text{Subsystem})(t) = \sqrt[n]{A(\text{System})(t)}$$

In this case, regarding system availability of 95% in 1 year and applying the general equation for the system with three subsystems in series we have:

$$MA(\text{Subsystem})(t) = \sqrt[3]{A(\text{System})(t)}$$

$$MA(\text{Subsystem})(t) = \sqrt[3]{0.95}$$

$$MA(\text{Subsystem})(t) = \sqrt[3]{0.95} = 0.983 = 98.3\%$$

In addition to defining the minimum availability it is possible to identify critical subsystems. Step 3 is used to identify the critical subsystem, that is, the subsystem with availability lower than the minimum availability.

Thus considering that the system availability target is 95% in 1 year and subsystems 1, 2, and 3 have 100%, 90%, and 99% availability, respectively, in the previous example the critical subsystem is subsystem 2 because the availability is 90% in 1 year, lower than the minimum availability, that is, 98.3% in 1 year.

Step 4 defines the availability target for the critical subsystem regarding the other subsystems' availability. In a system with three subsystems we have:

$$A(\text{System})(t) = A(\text{Subsystem 1})(t) \times A(\text{Subsystem 2})(t) \times A(\text{Subsystem 3})(t)$$

$$A(\text{Subsystem 2})(t) = \frac{A(\text{System})(t)}{A(\text{Subsystem 1})(t) \times A(\text{Subsystem 3})(t)}$$

The general equation to define the critical subsystem availability target is:

$$A(\text{Critical subsystem})(t) = \frac{A(\text{System})(t)}{\prod_{i=1}^n A(\text{Subsystem}_i)(t)}$$

Thus the system availability target is 95% in 1 year and subsystems 1, 2, and 3 have 100%, 90%, and 99% of availability, respectively. The critical subsystem (subsystem 2) availability target will be:

$$A(\text{Critical subsystem})(t) = \frac{A(\text{System})(t)}{\prod_{i=1}^n A(\text{Subsystem}_i)(t)}$$

$$A(\text{Subsystem 2}) = \frac{A(\text{System})(t)}{\prod_{i=1}^n A(\text{Subsystem}_i)(t)}$$

$$= \frac{A(\text{System})(t)}{A(\text{Subsystem 1})(t) \times A(\text{Subsystem 3})(t)}$$

$$A(\text{Subsystem 2})(1) = \frac{A(\text{System})(1)}{A(\text{Subsystem 1})(1) \times A(\text{Subsystem 3})(1)} = \frac{0.95}{1 \times 0.98}$$

$$= 0.969 \cong 97\%$$

Similar steps to define the critical subsystem availability can be applied to critical subsystem equipment. Once critical equipment has its availability target it is also possible to define critical equipment reliability. The other option to calculate the availability target for each subsystem is nonlinear optimization methodology. Such an approach considers a nonlinear model to describe system availability and regards system and subsystems availability as assumptions. Thus regarding a

system with three subsystems with the availability in 1 year of 100%, 90%, and 98%, the nonlinear model will be:

$$\text{FO} \rightarrow \text{Max: } Z = A(\text{Subsystem 1})(t) \times A(\text{Subsystem 2})(t) \times A(\text{Subsystem 3})(t)$$

SA

$$A(\text{Subsystem 1})(t) \times A(\text{Subsystem 2})(t) \times A(\text{Subsystem 3})(t) \leq 0.95$$

$$A(\text{Subsystem 1})(t) \leq 1$$

$$A(\text{Subsystem 2})(t) \leq 1$$

$$A(\text{Subsystem 3})(t) \leq 1$$

$$A(\text{Subsystem 2})(t) \geq 0.9$$

$$A(\text{Subsystem 3})(t) \geq 0.98$$

The nonlinear model can be turned into a linear model as shown here:

$$\text{FO} \rightarrow \text{Max: } \ln Z = \ln A(\text{Subsystem 1})(t) \times A(\text{Subsystem 2})(t) \times A(\text{Subsystem 3})(t)$$

$$\text{FO} \rightarrow \text{Max: } \ln Z = \ln A(\text{Subsystem 1})(t) + \ln A(\text{Subsystem 2})(t) + \ln A(\text{Subsystem 3})(t)$$

SA

$$\ln(A(\text{Subsystem 1})(t) \times A(\text{Subsystem 2})(t) \times A(\text{Subsystem 3})(t)) \leq \ln(0.95)$$

$$A(\text{Subsystem 1})(t) \leq 1$$

$$A(\text{Subsystem 2})(t) \leq 1$$

$$A(\text{Subsystem 3})(t) \leq 1$$

$$\ln(A(\text{Subsystem 2})(t)) \geq \ln(0.9)$$

$$\ln(A(\text{Subsystem 3})(t)) \geq \ln(0.98)$$

$$\begin{aligned} \ln(A(\text{Subsystem 1})(t)) &= x_1, \ln(A(\text{Subsystem 2})(t)) \\ &= x_2, \ln(A(\text{Subsystem 3})(t)) = x_3 \end{aligned}$$

$$D = \ln Z$$

$$\text{FO} \rightarrow \text{Max: } D = x_1 + x_2 + x_3$$

SA

$$x_1 + x_2 + x_3 \leq -0.051$$

$$x_1 \leq 1$$

$$x_2 \leq 1$$

$$x_3 \leq 1$$

$$x_2 \geq -0.105$$

$$x_3 \geq -0.0202$$



The linear model can be solved by software or specific mathematical methodology such as the simplex method. The linear optimization method is not within the scope of this book and so will not be described here. The main objective here is to show such methodology as another possibility to define critical subsystem availability.

Both methods are a good application for a system where most of the subsystems and equipment are in series in the RBD. Even if there are subsystems or equipment in parallel in the RBD it is possible to represent a parallel configuration as a series for one block. That means the parallel configurations are in one block. For example, two pumps in parallel configuration can be represented by one block in series in the RBD, but it is necessary to know the reliability or availability of such components in parallel to model correctly based on parallel mathematics configuration.

The improvement availability method is very well applied to the system in which the subsystems and most of their components are in series. For a complex system with many parallel configurations it is necessary to represent such subsystems and their components mathematically appropriated, and in this case it is harder to apply this methodology.

The nonlinear optimization availability method is also very well applied when the subsystems and most of their components are in series, but even when some components or subsystems share parallel configuration such equations must be appropriately described. Different from the previous method, in this case, despite the analytical solution, it is possible to use software to solve the nonlinear model and in this case it is easier to deal with a complex model with parallel configurations.

The next section presents the concept of asset optimization, which encompasses performance indexes, preventive maintenance, and inspection as well as spare parts.

---

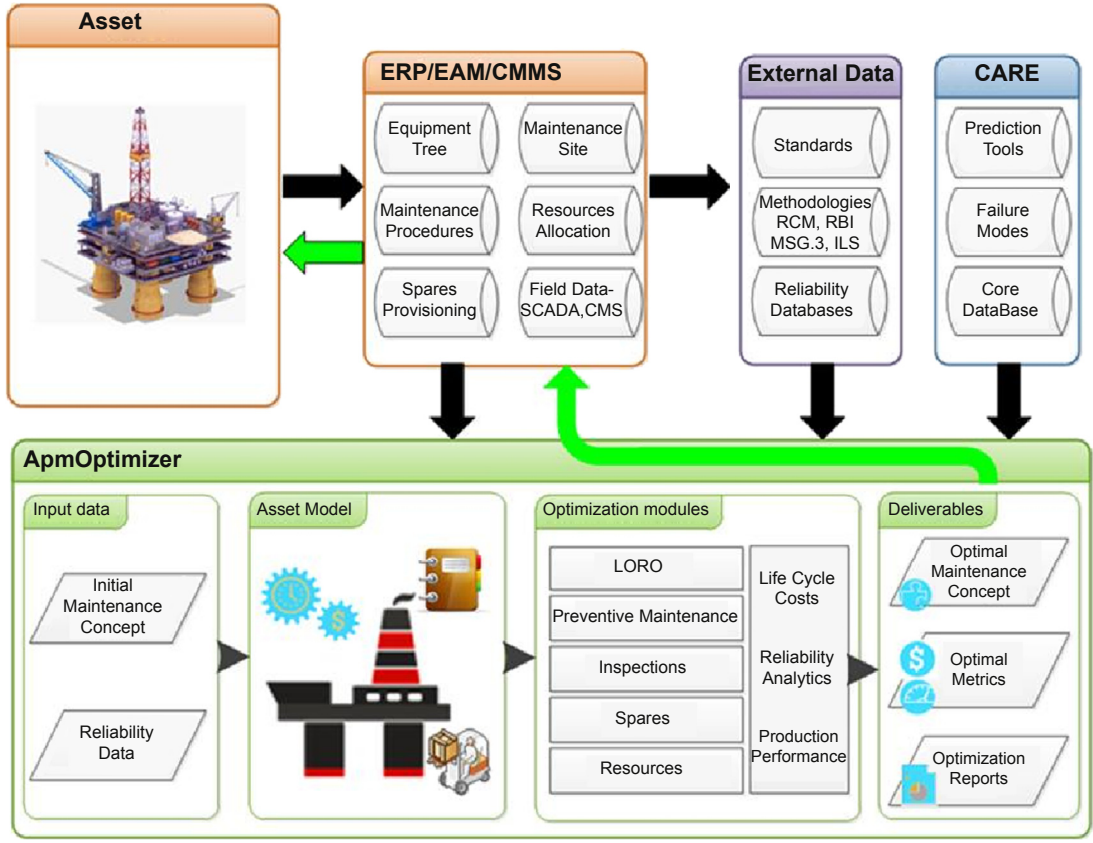
## 4.5 PERFORMANCE OPTIMIZATION

Different methods have been discussed so far with the main objective to support the asset performance achievement. The very limitation about the whole methods discussed is that such methods are applied for individual equipment and components without defining the optimal time to perform preventive inspections, which increase the whole system performance.

In fact, the usual reliability methodology is based on data collected and model analysis. The further and important step is to optimize the final solution by defining the best inspection and preventive time as well as the spare part level, which maximizes the operational availability and minimizes the life cycle cost. The whole asset performance optimization is demonstrated in [Fig. 4.31](#).

The best time to perform preventive maintenance and inspections depends on each equipment and component probability of failure, which is defined on lifetime data analysis (LDA) as well as degradation process, which is supported by RCM and RBI methods based on predictive maintenance results, standards, and online monitoring data.

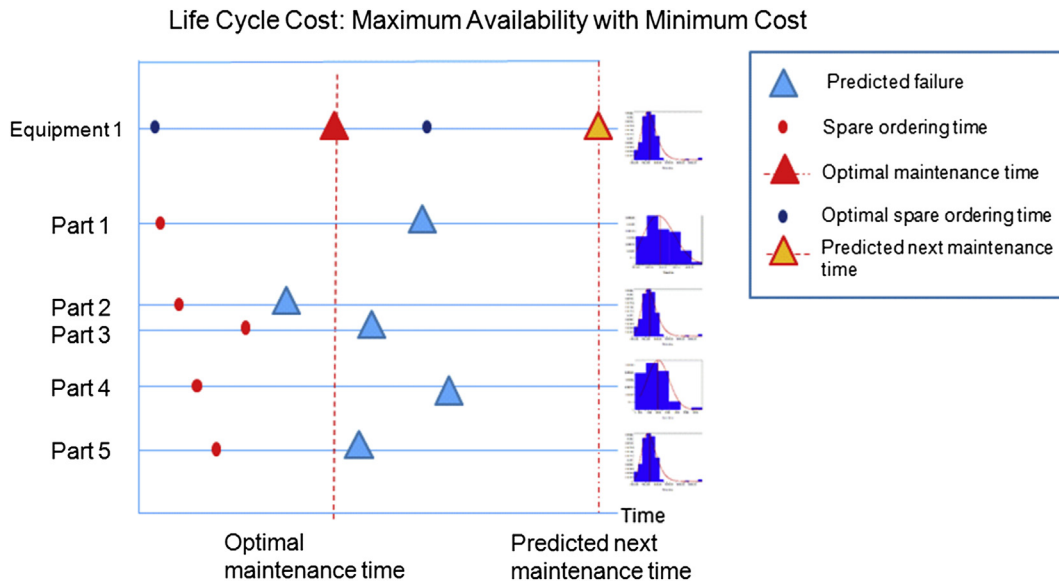
In addition, the spare parts will also be influential for such preventive maintenance, inspection, and failure times. Therefore to maximize one equipment performance it is necessary first to define the best time to perform a preventive maintenance for each component and further define the optimal time for the whole equipment, as shown in [Fig. 4.32](#). As soon as the best time to perform such preventive maintenance and inspection is decided, it is also possible to define the best time to purchase the spare part to minimize the stock level and life cycle cost.



**FIGURE 4.31**

Asset performance optimization.

Source: Calixto, E., Bot, I., 2015.



**FIGURE 4.32**

Equipment performance optimization.

*Source: Calixto, E., Bot, I., 2015.*

The optimal time is such time that minimizes the life cycle cost and maximizes operational availability of equipment. After optimizing the equipment a further step is to optimize the system asset considering the optimal solution defined for each individual piece of equipment, which affects this system asset performance.

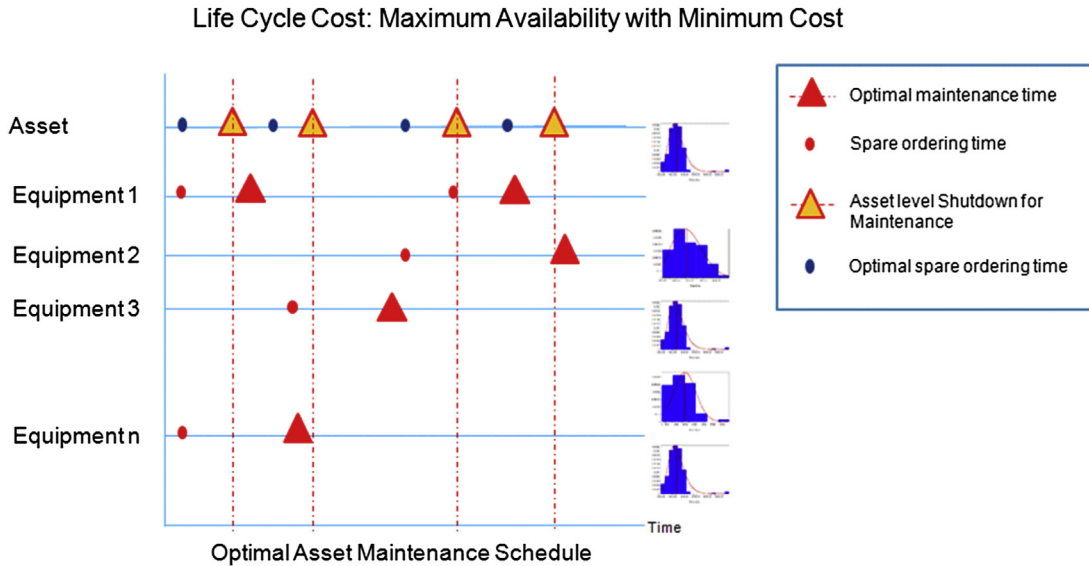
Indeed, in many cases, to optimize each piece of equipment individually will not optimize the whole asset performance. The system asset optimization takes into account all individual equipment constraints to give a better solution for the whole asset system, as shown in Fig. 4.33.

The challenge of optimizing the whole asset is related to the huge number of constraints such as environmental, safety, law, client, performance, and cost. In addition, there are different goals that in many cases do not optimize the whole asset, such as zero stock policy, minimal operational cost, and minimum number of teams.

The idea of asset optimization is to support the leader's decision based on a mathematical method approach, which saves time and has a potential to optimize system asset performance.

The optimization methodology encompasses information such as spare parts, preventive maintenance and inspection policies, reliability, and logistic parameters of equipment and components as well as the hierarchical relationship between them. For this reason Dynamic Program (DP) is the ideal tool for this task.

Gustafsson (2010) presented a DP method for maintenance optimization in which  $S_t$  and  $d_t$  represent the state of the system and decisions made, respectively, at time  $t$ . Furthermore,  $i_t$  is the



**FIGURE 4.33**

System asset performance optimization.

Source: Calixto, E., Bot, I., 2015.

exogenous information that arrives at time  $t$ .  $\varphi$  represents the transition function and with these notations the system evolves in time according to:

$$S_{t+1} = \varphi(s_t, d_t, i_t)$$

For each decision we make, a cost  $C(s_t, d_t)$  has to be paid. If we assume a stochastic system the objective is to minimize the expected total cost over some planning period.

If we assume that the system is in some state at time 0, and we have to make decisions for the time horizon  $0, \dots, T$ , our problem is to:

$$\text{MIN}_{x_0, x_1, \dots, x_T} : E \left( \sum_{t=0}^T C(s_t, d_t) \right)$$

Subject to:

$$S_{t+1} = \varphi(s_t, d_t, i_t)$$

The proposal DP method includes the operational availability target considering the maintenance policy decision, which is described as follows. For each item prepare a set of possible maintenance policies and calculate their cost and resulting item availability. Next, use these possibilities to construct a new set of possible maintenance policies for blocks each containing several items. In this way, possible maintenance policies are constructed for every level in the asset hierarchy and the optimal policy is eventually chosen.

The second optimization possibility is to consider the hierarchical system model optimization. The challenge is to optimize the maintenance policy for the system, that is, to find the cheapest policy subject to a requirement that system availability be larger or equal to  $A_{\text{required}}$ .

Suppose that the system optimal policy  $P_{1,1}$  is known ( $P_{i,j}$  denotes the policy for block  $j$  that belongs to level  $i$ ) and it has a system availability denoted by  $A_{1,1} \geq A_{\text{required}}$ . Similarly, the set of policies and availabilities for the blocks of level 2 is denoted by ( $P_{2,i}$ ) and ( $A_{2,i}$ ). The system optimal maintenance policy is a union of optimal policies belonging to level 2 blocks:

$$P_{1,1} = \bigcup_i P_{2,i}$$

Therefore with availabilities  $A_{2,i}$ , and more generally:

$$P_{m,j} = \bigcup_i P_{m+1,i(j)}$$

where  $i(j)$  denotes the indices of blocks in level  $m + 1$ , which are the children of block  $j$ . Since  $A_{2,j}$  is not known a priori, different optimal policies are constructed for different  $A_{2,j}$  values, and the optimal  $P_{1,1}$  is constructed by choosing the best combination of level 2 component policies. The process can easily be generalized to systems with many hierarchical levels.

In fact, there are different optimization algorithms that define an optimal solution. It is not within the scope of this book to discuss in detail each individual optimization model and algorithm, but to present a feasible solution that can be successfully applied to the oil and gas industry.

The optimization algorithm described previously was implemented into the apmOptimizer (BQR) software for different optimization modules such as preventive maintenance (PMO), inspection optimization (PIO), spare parts (S2A), resources (R2A), and level of repair (LORO).

The apmOptimizer is a modeling, analysis, and optimization tool designed to bring asset maintenance to an optimal state, maximize availability, and minimize cost of ownership over lifetime (Bot and Asoulay, 2014).

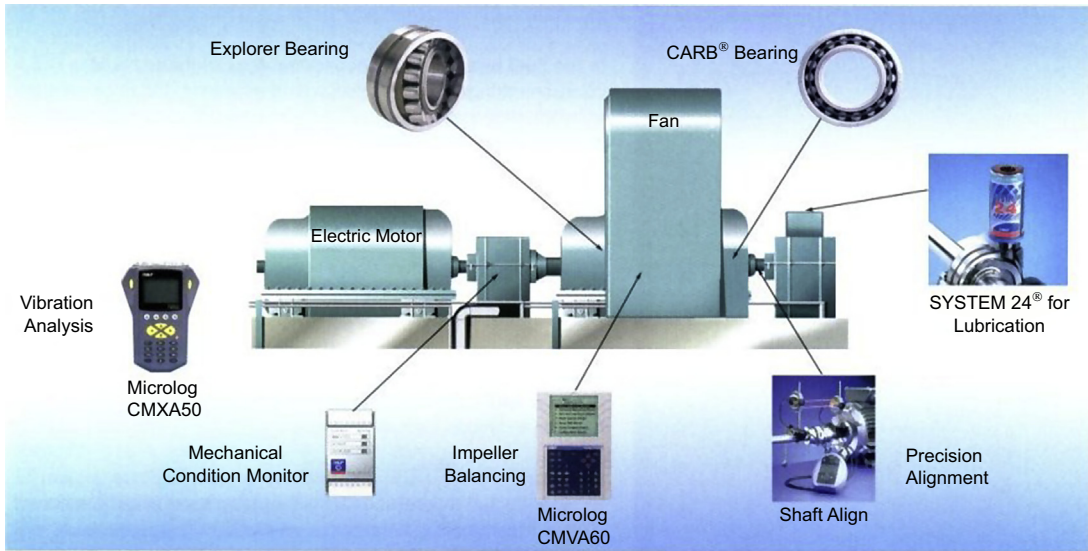
Consider the example of a fan, which is represented in Fig. 4.34. Basically, the current maintenance policy is to perform, remove, and install a new fan component after each failure. The fan life cycle is 10 years and the assembly cost is \$1M.

The additional constraints are:

- 7 hours repair and restart time for each failure;
- \$10,000 for each hour of downtime caused by a failure;
- During its life the fan assembly was replaced 12 times;
- Initial life cycle cost (LCC) = US\$13,288M for 10 years.

Based on optimization solution (apmOptimizer software form BQR), the best preventive maintenance for critical components was established, as shown in Fig. 4.35. By applying the optimization model it was possible to achieve the final solution, which by applying optimal preventive maintenance reduced the life cycle cost by 20%.

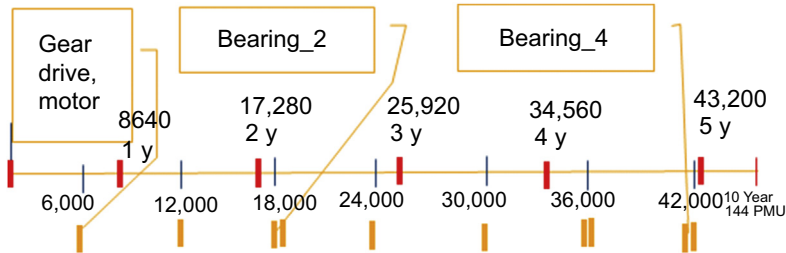
The next section will present a case studies applied to the oil and gas industry with inspection and spare part optimization.



**FIGURE 4.34**

Fan component parts.

Source: Bot and Asoulay, 2014.



**FIGURE 4.35**

Fan preventive maintenance performance optimization.

Source: Calixto, E., Bot, I., 2015.

## 4.6 CASE STUDIES

This section presents several RAM analysis case studies to illustrate the concepts discussed so far. Thus we begin from the simplest to the most complex analysis for different systems in the oil and gas industry. Some of the cases concern RAM analysis in the project phase and others are in operational phases. In this way, it will be possible to see different aspects of RAM analysis in each particular case.

The first case study, Sensitivity Analysis in Critical Equipment: The Distillation Plant Case Study in the Brazilian Oil and Gas Industry, is about a distillation plant in the operational phase, and RAM analysis was used to identify the most critical equipment to propose recommendations to improve system availability. Such recommendations were prioritized by availability impact and rank of recommendation regarding cost and budget limits.

The second case study, Systems Availability Enhancement Methodology: A Refinery Hydro-treating Unit Case Study, is about a hydrodesulfurization plant in the project phase, where more than one piece of critical equipment was identified, and based on system availability, the target developed the availability enhancement methodology for defining availability targets for critical subsystems and their critical equipment to propose recommendations to the system to achieve the availability target.

The third case study, The Nonlinear Optimization Methodology Model: The Refinery Plant Availability Optimization Case Study, is about a propane plant in the project phase where more than one piece of critical equipment was detected. Based on the system availability target a nonlinear optimization methodology model was developed to define availability targets to such critical subsystems and their critical equipment regarding recommendations to the system to achieve the availability target.

The fourth case study, CENPES II Project Reliability Analysis, is about facility systems in the project phase that are required to have high availability over 20 years to allow data centers to achieve 99.99% availability in such time. In such an analysis it was possible to reduce costs and assess system redundancies.

The fifth case study, The Operational Effects in Availability: Thermal Cracking Plant RAM Analysis Case Study, is about a plant in the project phase in which operational procedures influence system availability, and based on procedures sensitivity analysis will possibly reduce project costs, improving the project's economic feasibility.

The sixth case study, Partial Availability Based on System Age: The Drill Facility System Case Study, is about a drill facility in the operational phase that requires improved availability. In this case this system has an annual availability target. Thus, based on historical failure data, the partial availability methodology was developed regarding the system's age to define the critical equipment in the first and second years to define improvement actions as well as stock and inspection policy.

The seventh case study, High-Performance System Requires Improvements? The Compressor's Optimum Replacement Time Case Study, is about a fluid catalytic cracking plant in the operational phase that can be impacted by compressor failures even though such a compressor is being configured as  $k$ -out-of- $n$  ( $2/3$ ). Thus such a compressor will be assessed in terms of optimum replacement times as well as phase diagram methodology to avoid unavailability in the system in the following years.

The eighth case study, RAM + L Analysis: Refinery Case Study, is about a project and operational plants that are included in one system, a refinery. Such analysis includes RAM analysis for the different systems and considers logistic issues, and in the end shows the refinery availability, the critical equipment, and the vulnerabilities.

#### **4.6.1 SENSIBILITY ANALYSIS IN CRITICAL EQUIPMENT: THE DISTILLATION PLANT STUDY CASE IN THE BRAZILIAN OIL AND GAS INDUSTRY**

The main objective of this case study is to analyze if one specific distillation plant is achieving its required availability target (98% in 5 years) to be considered a high-performance plant and to find out which are the most critical subsystems and equipment. RAM analysis is usually divided into



failure and repair data bank procurement, block modeling, simulation diagram, and sensitivity analysis. In the first step, historical failure and repair data will be collected and a PDF will be defined to supply the block model and simulation diagram using the Weibull++ software model. To create the block diagram, some process assumptions were defined with process engineers to create the most effective configuration. Therefore the simulation will show the system availability and the most critical subsystems and equipment. The next step is sensitivity analysis of the most critical equipment to identify reliability improvements and the possibility of increasing system availability. The expected result is proposing improvement in operational plants focused on availability and performance rates.

### ***Failure and Repair Data Analysis***

Seeking to ensure the representation level of such data, maintenance professionals with knowledge in such systems took part in this stage and a quantitative analysis of failure and repair data was performed.

A critical equipment analysis on the causes of system unavailability and its respective critical failure modes was performed, standardizing all equipment failure modes responsible for most of the impacts on the subsystems.

The historical failure data was assessed and equipment PDFs were created. The example in Fig. 4.36 shows a coke formation PDF in a fan.

If no failure data is available, a qualitative analysis is performed together with a maintenance professional. The example in Table 4.6 shows two parallel fans with failure modes and the respective average failure and repair time. The failure modes are coke formation. The Weibull PDF was defined by historical data analysis. The repair time was defined by interviews conducted with maintenance technicians and engineers.

In the same way, the failure and repair data of each subsystem's equipment was defined and included in the model. In some cases, there was no historical failure available, motivating the introduction of a qualitative analysis among maintenance technicians and engineers. In these specific cases, criteria were created for defining a triangular or rectangular function to represent failure modes, labeled as pessimistic or optimistic depending on each failure and repair time.

### ***Modeling***

To perform the availability results in Monte Carlo simulation, it is necessary to set up model equipment using RBD methodology. In this way, it is necessary to be familiar with the production flowchart details that influence losses in productivity. Consequently, some statements and definitions, shown on item 4.1 and 4.2.3.

Some critical subsystems, such as preheating, salt treatment, heating, prefractioning, atmospheric distillation, vacuum distillation, water treatment, diesel drying, and Merox, were unavailable making the distillation unit unavailable.

- The efficiency target was 98.2%.
- The facility supply had 100% availability in 5 years.
- The total production per day was 30,000 m<sup>3</sup>.

The distillation subsystem RBD is displayed in Fig. 4.37.



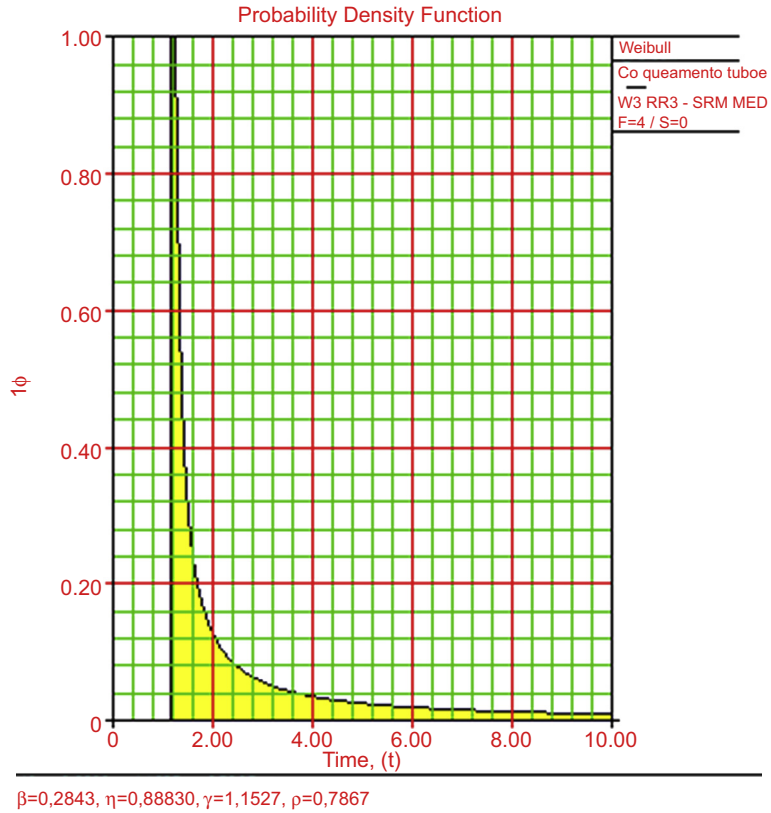
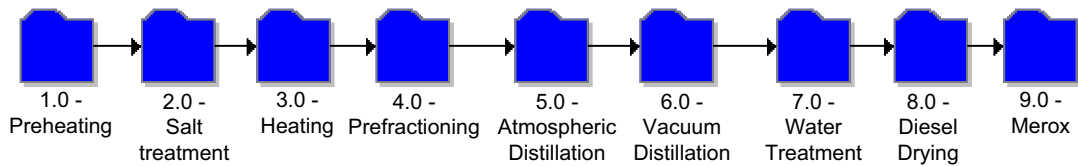


FIGURE 4.36

Fan PDF.

Table 4.6 Quantitative Failure and Repair Data						
TAG	Failures Modes (years)					Repair Time (hours)
	Distribution	Parameters			MTTF	Parameters
B-03202 A/B	Weibull (coke formation)	$\beta$	$\epsilon$	$\gamma$	5.48	276
		0.24	1.89	1.15		
B-03203 A/B	Weibull (coke formation)	$\beta$	$\epsilon$	$\gamma$	11.68	96
		0.2843	0.88	1.15		

MTTF, mean time to failure.

**FIGURE 4.37**

Distillation subsystem RBD.

### Preheating

The purpose of this subsystem is heating feed oil before salt treatment to foster salt precipitation. There is a group of exchangers in parallel under specific process condition as follows:

- There are three feed pumps in parallel, two in operation and one on standby.
- There are four exchanger trains and at least two of the four must be available.
- In each train, all exchangers are in series. In the case of unavailability the train becomes unavailable.

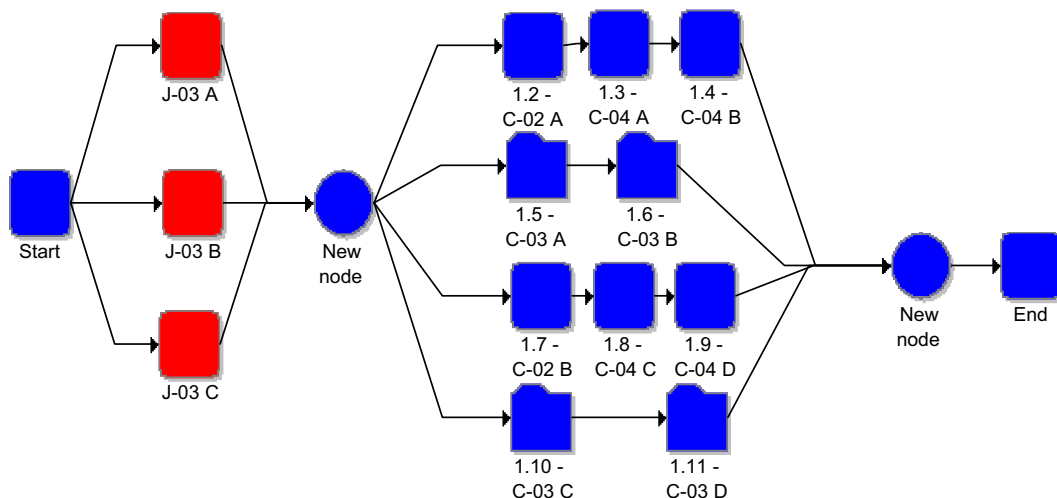
Fig. 4.38 shows the preheating RBD.

### Salt Treatment

This subsystem removes salt components from feed to preserve equipment and achieves a high-performance process. There are two groups of salt treatment horizontal vessels in parallel configuration (RBD) under specific process conditions as follows:

- All horizontal vases are active.
- At least one of the horizontal vases is active ensuring the availability of the subsystem.

Fig. 4.39 shows the salt treatment subsystem RBD.

**FIGURE 4.38**

Preheating RBD.

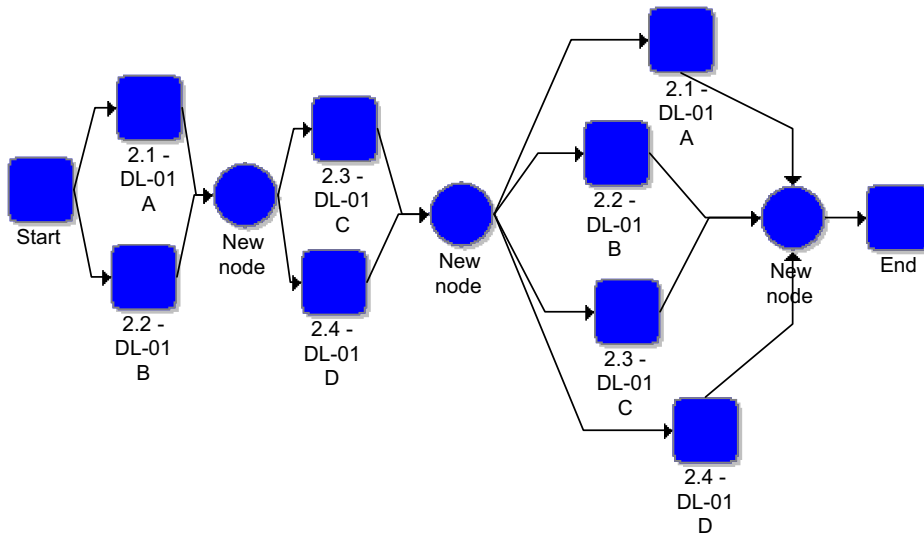


FIGURE 4.39

Salt treatment subsystem RBD.

### Heating

This subsystem focuses on heating feed to the prefractioning subsystem, aiming to save energy consumption and increase efficiency reactions. There are four groups of exchangers in parallel under specific process conditions as follows:

- At least two of the four exchanger groups must be available to make the subsystem available.
- In each group, the exchangers are in series and some of them are in parallel.
- In parallel blocks at least two of the four must be available.

The heating subsystem RBD is represented in Fig. 4.40.

### Prefractioning Subsystem

The prefractioning subsystem has the objective of separating feed into vapor and liquid before distillation. The most important process conditions are:

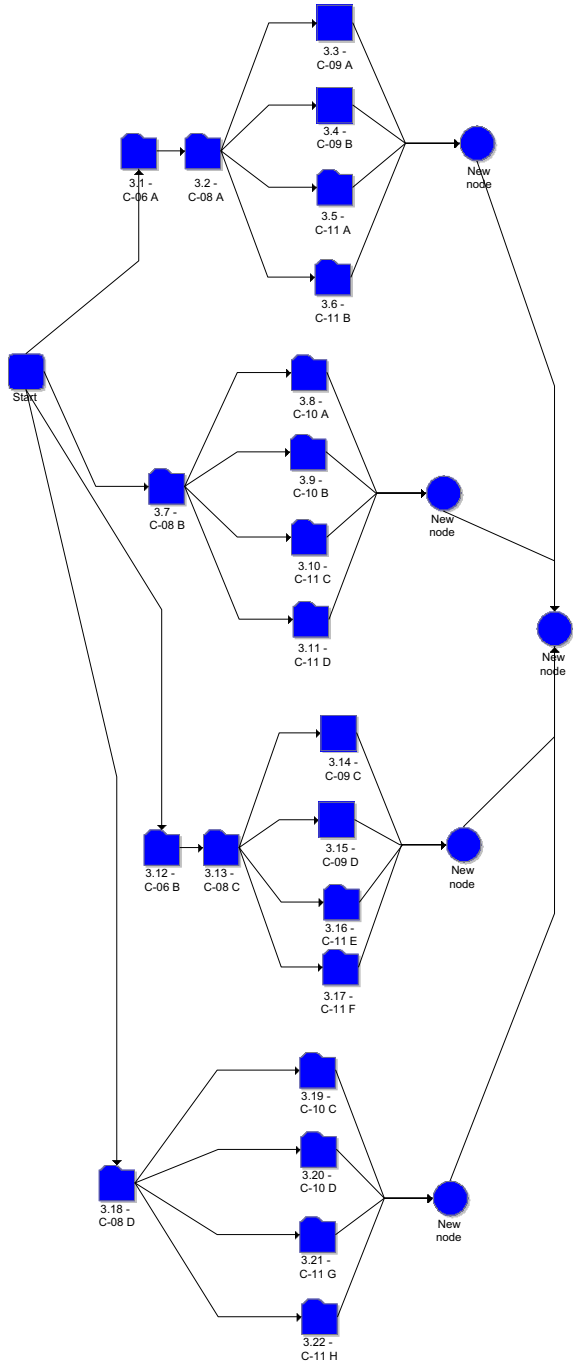
- Pumps J-32 A–C work, two active and one passive.
- The heat exchanger works in two trains, which means in parallel configuration (RBD).

Fig. 4.41 shows the prefractioning subsystem RBD.

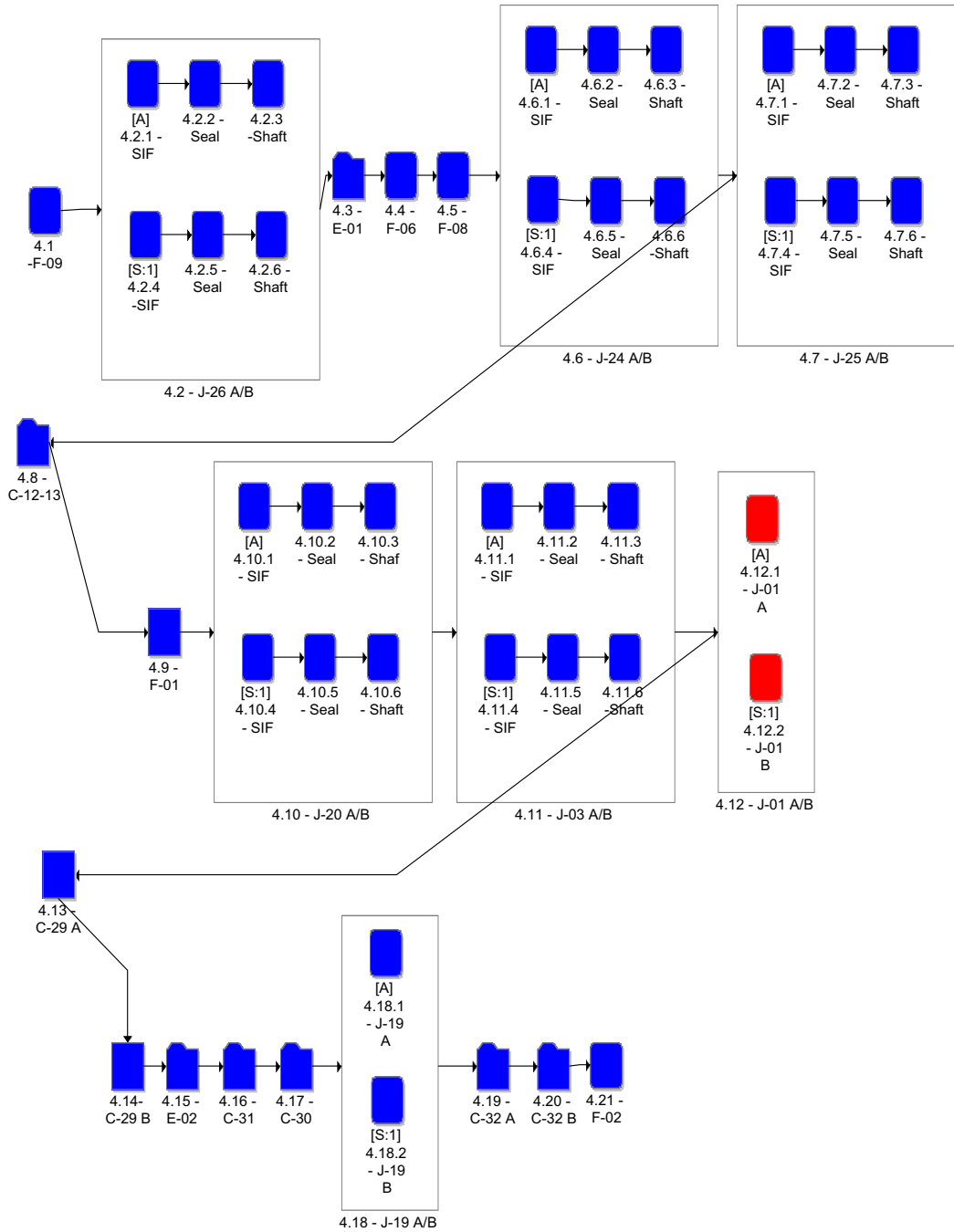
### Atmospheric Distillation

The atmospheric distillation subsystem aims at separating the oil subproduct, such as natural gas, naphtha, diesel, and other fuels. The most important process conditions are:

- Production reduction in any part of tower E-04 A, B, or C;
- Production reduction if any equipment fails at the top of the distillation tower;



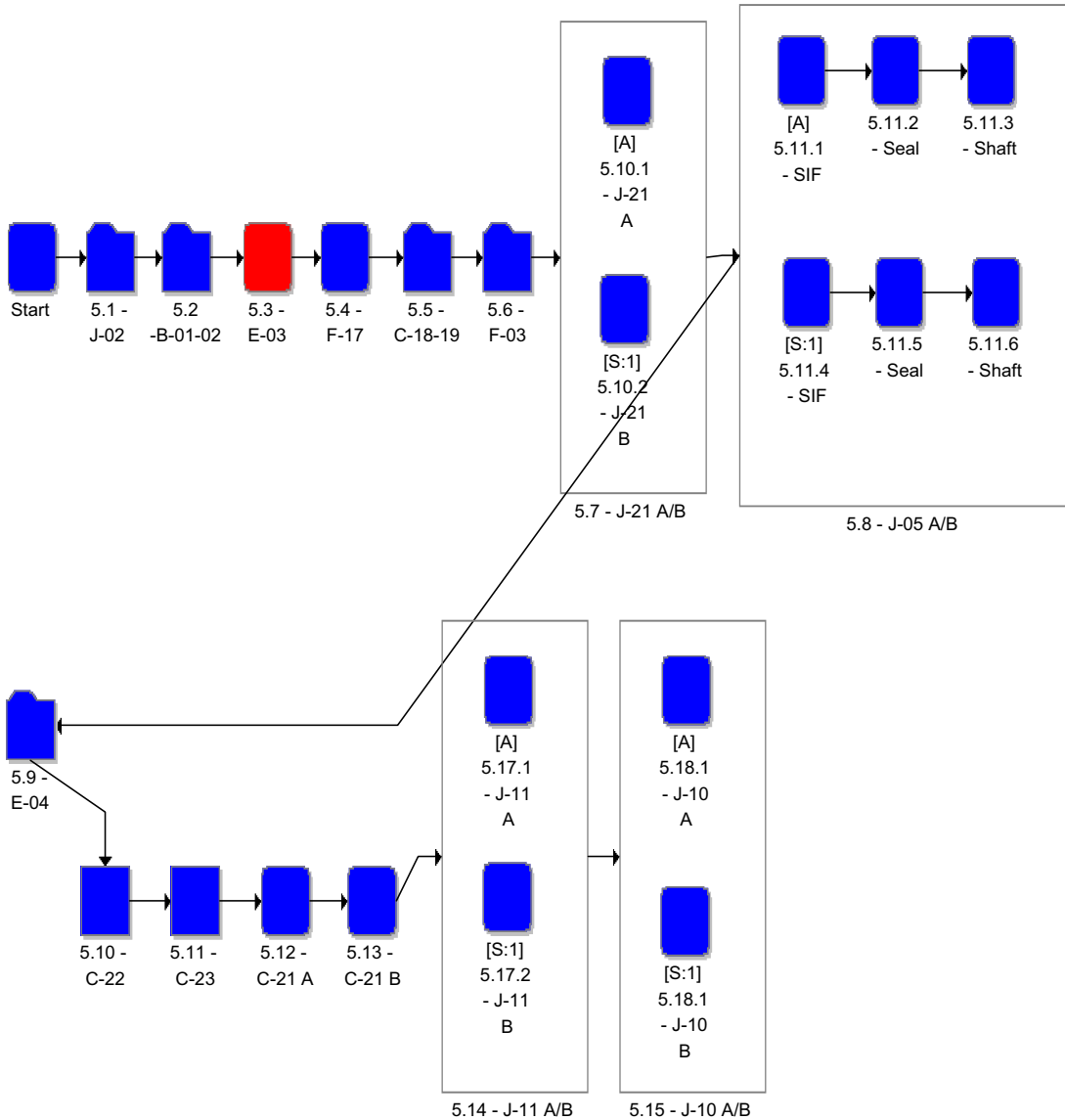
**FIGURE 4.40**  
Heating subsystem RBD.



**FIGURE 4.41**  
Prefractionating subsystem RBD.

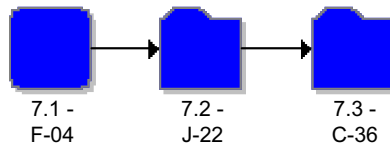
- Pumps J-32 work, with two actives and one passive;
- Fan B-01 is a B-02 redundancy when coke formation or other failure mode occurs.

Fig. 4.42 shows the atmospheric distillation subsystem RBD.

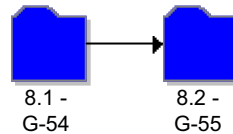


**FIGURE 4.42**

Atmospheric distillation subsystem RBD.

**FIGURE 4.43**

Water treatment subsystem RBD.

**FIGURE 4.44**

Diesel drying subsystem RBD.

### Water Treatment Subsystem

The water treatment subsystem cools down the process water. The most important process conditions are:

- Pumps J-22 work, with two active and one passive;
- Air cooler C-36 works under  $k$ -out-of- $n$  condition, which means five of eight must be available. Each part comprises one motor and one fan that are configured in series.

Fig. 4.43 shows the water treatment subsystem RBD.

### Diesel Drying Subsystem

The diesel drying process eliminates salt and sand components, filtering the feed beyond two groups of filters. The process conditions are:

- Two sand filters are active, implying a production reduction in case of failure;
- Three salt filters, implying a production reduction in case of failure.

Fig. 4.44 shows the diesel drying subsystem RBD.

### Vacuum Distillation Subsystem

The purpose of the vacuum distillation subsystem is separating heavy oil in natural gas, naphtha, diesel, and other fuels. The most important process conditions are:

- Production reduction in case of failure in tower E-05 for 48 hours, implying a shutdown after that;
- Production reduction in case of failure in fan B-03 A or B for 48 hours, implying a shutdown after that.

Fig. 4.45 shows the vacuum distillation subsystem RBD.

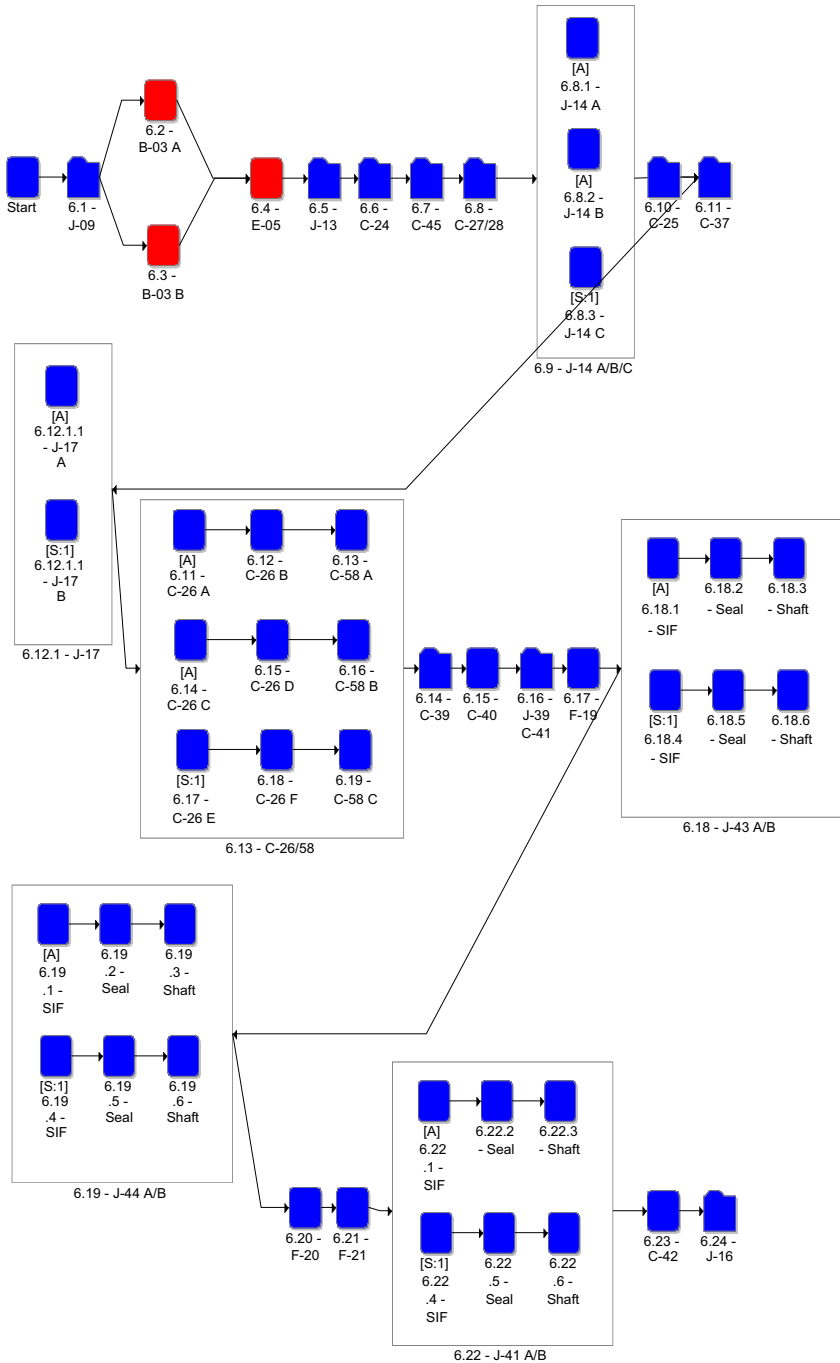


FIGURE 4.45 Vacuum distillation subsystem RBD.



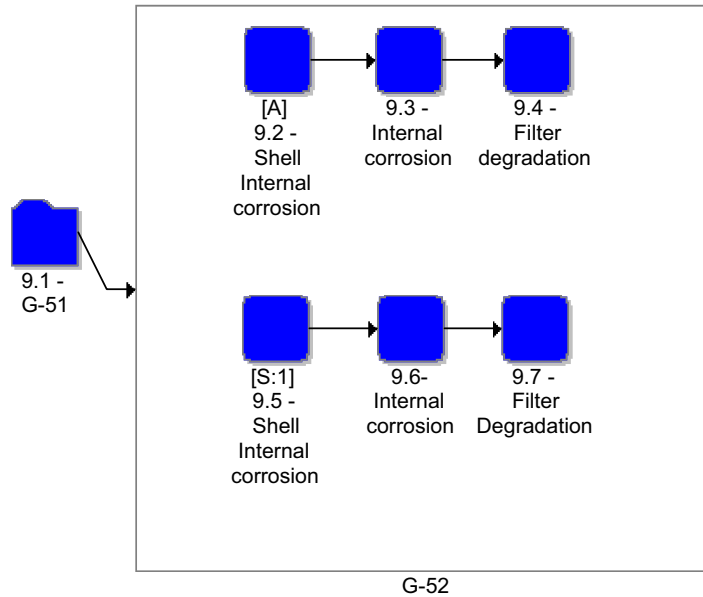


FIGURE 4.46

Meroux subsystem RBD.

### Meroux Subsystem

The goal of the Meroux subsystem is to separate  $H_2$  and other acid products going through a caustic solution. The process conditions are:

- One filter, G-51, is active, implying a production reduction in case of failure;
- Two filters, G-52 A and B, one active and the other passive, implying a production reduction in case of failure.

Fig. 4.46 shows the Meroux subsystem RBD.

### Simulation Subsystem

RAM analysis was evaluated using BlockSim and MAROS (Maintainability, Availability, Reliability, Operability Simulator) software. The simulation creates typical life cycle scenarios for proposed systems, with Monte Carlo simulation methodology. The entire unit was modeled through RBDs, considering the redundancies and the possibilities for bypass in each equipment or system configuration. Next, the evaluated model was loaded with failure and repair data. The simulation allows specialists to determine if the availability and efficiency results achieve the target of 98.2% in 5 years. If the efficiency target is not achieved, it becomes necessary to improve the operational capabilities of critical equipment:

- Through installing the redundancies in most critical equipment;
- Through enhancing the reliability and maintainability of equipment used, without the installation of new redundancies;
- Through maintenance policy that allows keeping the desired availability level.

The simulation was conducted for 5 years and 250 tests were run to converge results. The availability and efficiency were 96.285% and 98.627% in 5 years, respectively. The difference between those two indexes means that throughout part of the operational time the distillation unit production was not 100%. This shows that, in some examples, equipment failures do not represent total plant shutdown.

### **Critical Analysis**

The critical analysis defines which are the most critical subsystems and equipment with the most influence on production losses. There are two indicators showing criticality: the RI and EC.

The first index shows how much influence one subsystem or equipment has on system reliability. Thus using partial derivation it is possible to realize how much it is necessary to increase subsystem or equipment reliability to improve the whole system reliability.

The following equation shows the mathematical relation:

$$\frac{\partial R(\text{System})}{\partial R(\text{Subsystem})} = \text{RI}$$

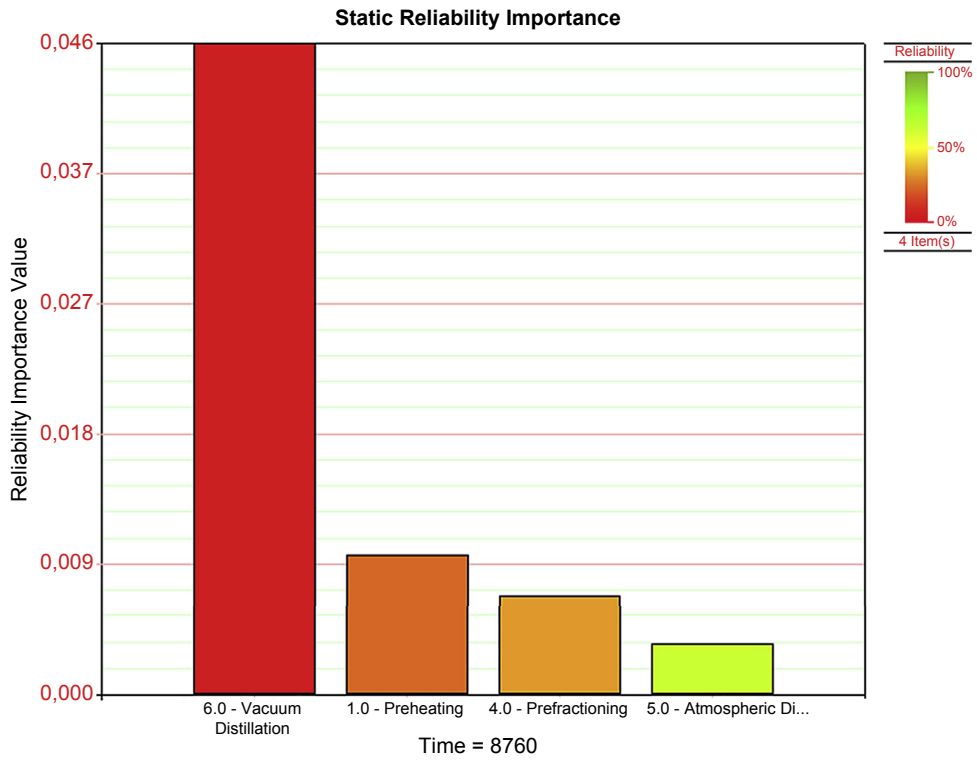
Despite this relation, some equipment or subsystems may be prioritized because of repair time having an expressive impact on production losses. This means that the availability impact is the most important index, despite reliability being highly influential in the system.

One specific subsystem or equipment might not be the most critical because of repair time impact. In this case a piece of equipment that has four shutdowns in a specific period of time might not be as critical as other equipment that has only one shutdown. For the second piece of equipment, total loss time is higher than the first. In fact, in most cases it is not possible to reduce repair time. Therefore equipment reliability improvement is the best solution for achieving availability targets. In this case the RI is the best index to show how much reliability improvement a system can accommodate. It is also necessary to consider production losses and equipment reliability. The EC index will indicate the most critical equipment and the RI will show how much it can be improved to achieve the availability target. In a distillation plant, the most critical subsystem is the vacuum distillation subsystem for the RI and EC, which imply that failure and losses in that subsystem are the most critical. The RI results are shown in [Fig. 4.47](#).

The results show that the RI for the vacuum distillation subsystem is 0.046, which means that 1% improvement made in this subsystem's reliability shows 4.6% improvement in system reliability in 8760 hours. However, the total subsystem losses represent 41.63%. Looking at the vacuum distillation subsystem, it is easy to see that the tower and fans are the most critical equipment, according to [Fig. 4.48](#).

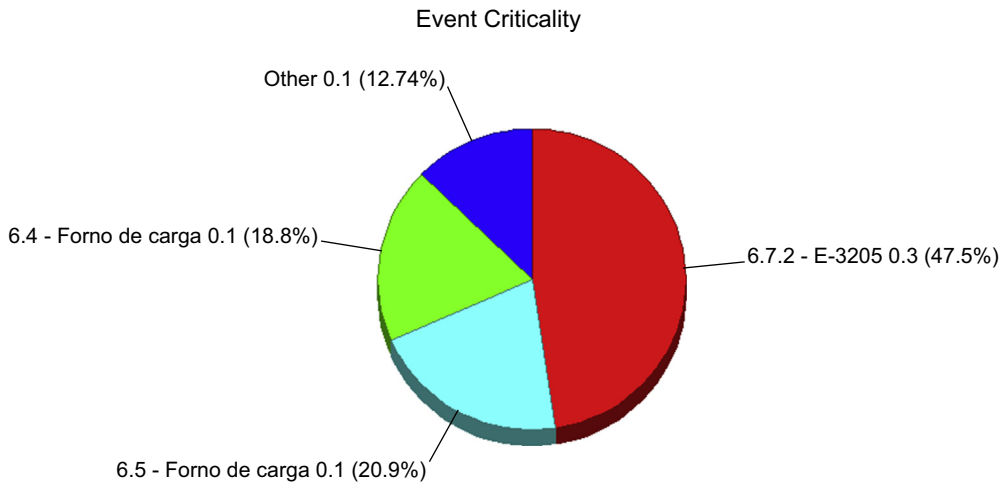
The RI in this subsystem indicates one pump as the most critical equipment in terms of reliability. But taking repair time into consideration, loss time in the tower and fans is higher than in pumps. The equipment RI is displayed in [Fig. 4.49](#).

Although the RI indicates pump J-09 is the most critical in terms of reliability, the fans and tower are definitely the most critical equipment in this subsystem. In this way, the RI indicates how feasible it is to improve this equipment to improve system reliability. For example, in tower E-05 the RI is 0.07. This shows that for each 1% improvement in this equipment the distillation plant improves 0.07% in terms of reliability in 8760 hours.



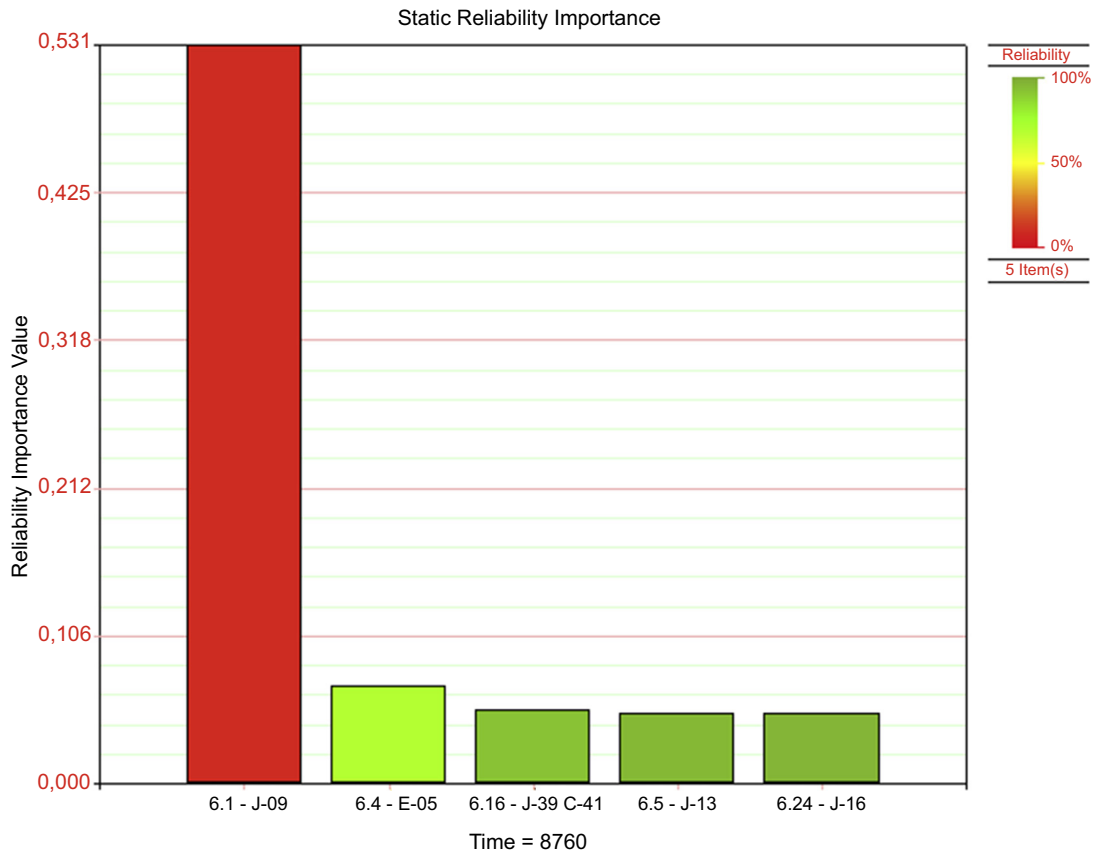
**FIGURE 4.47**

RI (reliability importance).



**FIGURE 4.48**

EC (event criticality).



**FIGURE 4.49**

Equipment RI (reliability index).

Some factors must be considered for this approach. The first factor is the limitation in equipment improvements, which means that the reliability improvement might not be enough to achieve the availability target. The second factor is the necessity to enforce improvement in other critical equipment until the availability target is achieved. However, this also does not guarantee achievement of the availability target.

In summary, it is necessary to consider both the RI and EC indexes. The improvements must be made based on critical rank, which means from the most critical to the least.

### ***Sensitivity Analysis***

After critical analysis it becomes clear that it is mandatory to implement the improvements in some equipment to achieve availability targets. Moreover, it is necessary to consider some critical events, such as energy supply, logistics, and other factors, for accomplishing a consistent analysis result.

The sensitivity analysis assesses system vulnerabilities and feasible possibilities for introducing improvements. So each tested event shows the impact on system availability.

The present distillation plant case study took into consideration the improvements in the vacuum distillation subsystem based on the improvements in the critical equipment reliability. In this case study the distillation plant achieved the availability target, but it is possible to increase the availability ratio even more, allowing some reliability improvement in the tower and fans.

In the first case, tower E-05 has a Weibull PDF with three parameters to represent an internal corrosion failure mode. This means that the PDF has a lognormal function configuration and that 67% of failures happen after 5.51 years. It is possible to improve the reliability, making some modifications in the tower's internal material to resist internal corrosion. In this case the new PDF parameters are  $\beta = 0.58$ ,  $\eta = 5.51$ , and  $\gamma = 0$ , which means that after only 2 years ( $\gamma = 2$ ) will internal corrosion occur, so the mean time to failure (MTTF) was 8.83 years and went up to 12.17 years. The distillation plant efficiency increased 0.18%, from 98.627% to 98.703%, which saves \$1,002,144 in 5 years.

In the second case, two fans, B-03 A and B, have coke formation, with PDF parameters are  $\beta = 0.2843$ ,  $\eta = 0.88$ , and  $\gamma = 1.15$ . This means that after 1.15 years there will be coke formation with the most failures happening at the beginning of the life cycle, so after 0.88 year, 67% of failures will occur. It is feasible to have some improvement to avoid coke formation, so the new PDF is well represented by normal distribution with parameters  $\mu = 6$  years and  $\sigma = 1$  year. The distillation plant efficiency increased 0.18%, going from 98.627% to 98.703%, which saves \$1,002,144 in 5 years.

The distillation plant efficiency increases 0.32%, from 98.627% to 98.944%, which saves \$1,804,998 in 5 years. For both improvements, in the tower and fans, it is possible to increase plant efficiency 0.38%, from 98.627% to 98.999%, which saves \$2,118,288 in 5 years.

The sensitivity analysis helps to assess which improvement to critical equipment improves system availability. It is also important to measure economic gains in each improvement action.

### **Conclusion**

The critical equipment sensitivity analysis is a very important step in RAM analysis, because it is a chance to take into account system vulnerabilities and feasible improvements. Before performing sensitivity analysis, it is necessary to define the most critical subsystem and equipment to understand the relation between the subsystems and equipment and the vulnerabilities.

In the distillation plant case study, regardless of the achievement of the efficiency target, it is possible to increase the improvement in critical equipment. And in all cases it is necessary to figure out if it is profitable or not, if the actions proposed are feasible or not, and if the technology limitations permit making improvements in the equipment. It is necessary to measure failure times after the improvements are made in critical equipment, thus verifying reliability growth.

## **4.6.2 SYSTEMS AVAILABILITY ENHANCEMENT METHODOLOGY: A REFINERY HYDROTREATING UNIT CASE STUDY**

The objective of this case study is optimization of the refinery unit availability to comply with the availability of 96.5% in 4 years defined in the project and based on market demand. Thus process restrictions, logistics, health, safety, and environmental concerns were considered, which demonstrate the nonviability of increased redundancies in most components if it is necessary to increase system availability.

The surveyed system presents eight subsystems in series: the selective hydrogenation unit (selective hydrogen unit), first hydrodesulfurization stage, second hydrodesulfurization stage, product stabilization, hydrogen supply, corrosion, and diethylamine regeneration.

There will be a presentation, as a result of optimization by availability of the subsystems, of the MTTF and mean time to repair (MTTR) that each critical component of the subsystems must have so that the system reaches the required availability, using enhancement availability target methodology.

### ***Failure and Repair Data Analysis***

Seeking to ensure the confidence of such data, maintenance professionals with knowledge of such systems were interviewed and a qualitative analysis of failure and repair data was performed. A critical equipment analysis of the causes of system unavailability and respective critical failure modes was performed, standardizing all equipment failure modes that most impact the respective subsystems. The logistic time is the time required to supply a piece of equipment or component that is not in stock to allow maintenance to be performed.

The total repair time includes repair and logistic time, considering three time scenarios: pessimist, most probable, and optimist. In RAM analysis the repair times are compatible with the theoretical data banks, although the logistic times are not. In this case the logistic time varies around 3 and 4 months. In cases of imported components the logistic time increases to 6 or 9 months. Thus we consider that the components will be available within an adequate logistic time.

The example in Table 4.7 shows a compressor system, its failure modes, and respective average failure and repair times. The failure modes are motor, instrumentation failure, and rotor breakdown. The times are defined as a pessimist (P), most probable (MP), and optimist (O) and were defined in the interviews conducted with maintenance technicians and engineers.

Again, the failure and repair data of each subsystem's equipment was defined and included in the model. The logistic time related to a zero stock policy, which means the time required to purchase the component was removed in the model analysis since such zero stock policy is not being considered in this analysis. Thus we consider that the policies for stock components will be optimized.

### ***Optimization (Minimum Availability Target)***

The availability optimization requires knowing the availability target to define which availability the subsystems and components must achieve to satisfy the required availability goal. First, to achieve the availability target it is necessary to define the minimum availability, considering that all subsystems are similar. This means that the subsystem's availability has the same value as shown in Eq. [1].

Equipment Class	Failure Mode	MTTF (years)			MTTR (hours)		
		P	MP	O	O	MP	P
Gas compressor	Motor	10		20	168		140
	Instrumentation		2		6		12
	Rotor	10		20	96		360

Eq. [1]—Minimum availability theoretical target

$$Se, D(\text{Goal})(t) \leq D(\text{Shu})(t) \times D(\text{1st Stage})(t) \dots$$

$$D(\text{Shu})(t) = D(\text{1st Stage})(t) = D(\text{2nd Stage})(t) = D(\text{Min})$$

$$D(\text{Min})(t) \geq \sqrt[8]{D(\text{Goal})(t)}$$

$$D = \text{Availability}$$

In this way, comparing this availability target with the availability simulation results, it is possible to recognize the critical subsystem.

Next, it is necessary to take into consideration the real subsystem availability to define the real minimum value of the critical subsystem by dividing the values as shown in Eq. [2].

Eq. [2]—Minimum availability real target

$$\begin{aligned} & D(\text{Shu})(t) \times D(\text{1st Stage})(t) \times D(\text{2nd Stage})(t) \times D(\text{Est})(t) \\ & = D(\text{Goal})(t) / D1(\text{H}_2\text{Mup})(t) \times D1(\text{Recycle})(t) \times D1(\text{C})(t) \end{aligned}$$

The same equation is going to be used in each subsystem to define the critical equipment and target availability. To achieve each availability target it is necessary to test out the MTTF and MTTR values in each component and simulate to assess the results.

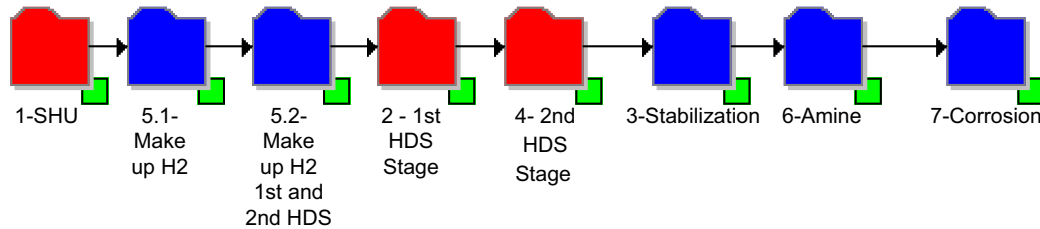
### ***The Hydrodesulfurization Process***

The hydrodesulfurization process is based on the addition of hydrogen to the petroleum fractions at elevated pressures and temperature in catalytic beds. Depending on the type of catalyst and operational conditions, there may be desulfurization, denitrification, saturation of fine oils, and cracking reactions. The process becomes hydrodesulfurization upon the removal of saturated components in catalysts based on molybdenum and cobalt. The hydrotreatment process may be subdivided into selective hydrogenation, first and second reaction stages, and entry of hydrogen and amine components, each described as follows:

- The objective of the selective hydrogenation unit is to remove sulfur from gasoline. This process is responsible for 80% of the gasoline specifications.
- The second stage will be the product's last specification stage, with the same type of reactors as in the first stage.
- In the stabilizer, the hydrocarbon steam and liquid stages are separated. The referred steam is distributed by the wet suction of the gas compressor unit of the fluid cracking catalyst.
- The hydrogen necessary for the hydrodesulfurization reactions of the first and second selective hydrogen unit stages is derived from the hydrogen generation unit passing through the make-up and cycle compressors.
- The amine section has the objective of removing the nitrogenated compounds.

### ***Modeling***

RAM analysis was developed using Reliasoft's BlockSim software. The modeling allows creation of typical life cycle scenarios for proposed systems, with Monte Carlo simulation techniques.



**FIGURE 4.50**

Reliability block—HDT.

The entire unit was modeled through RBDs, considering the redundancies and the possibilities for bypass in each piece of equipment or system configuration. Next, the development model was fed failure and repair data.

There are three basic ways to enhance plant availability:

- Through installation of redundancies of the most critical equipment;
- Through improvement of reliability and maintainability of equipment used, without installation of new redundancies;
- Through a maintenance policy that keeps the desired availability level.

In the case of an installation, such as the hydrodesulfurization plant, where there is work with hydrogen and high pressures and high temperatures, the safety concern is about toxic product leakage with high severity consequences. Thus it is normal for this type of installation to avoid the installation of additional equipment, unless the equipment is indispensable.

The subsystems are in series as illustrated in Fig. 4.50.

### **Simulation and Optimization**

The increase in system availability will be as a result of the increase in the reliability of the subsystems, avoiding redundancies in view of safety concerns. The system availability can be defined as follows ( $D$  means availability):

$$D(\text{HDT})(t) = D(\text{Cycle 1st and 2nd stage})(t) \times D(\text{Shu})(t) \times D(\text{MK H}_2)(t) \times D(\text{1st Stage})(t) \\ \times D(\text{2nd Stage})(t) \times D(\text{Stabilization})(t) \times D(\text{Amina})(t) \times D(\text{Corrosion})(t)$$

To propose improvements in system availability it is necessary to define the most critical subsystems, that is, the subsystem that impacts the system availability the most. Regarding system reliability impact, the reliability index by definition is the partial derivative of the system reliability function in relation to the subsystem reliability function. An example is how much Shu subsystem reliability impacts hydrodesulfurization plant reliability, as shown in Eq. [3].

Eq. [3]—Reliability target

$$\frac{\partial R(\text{HDT})}{\partial R(\text{Shu})} = \text{RI}$$

In this way, we can verify which subsystems most influence the system in terms of reliability. In this case it is the first stage, second stage, and selective hydrogen unit subsystems.



To reach the criticality of the subsystems in terms of availability, we can use the same methodology for defining the partial derivatives of the system’s availability function in relation to each subsystem or a second alternative. A different way to identify the systems that most impact system availability is to define the minimum availability that each subsystem must have for the system to reach the required availability. For the system availability being the multiplication of its subsystems availability, it means that all subsystems are in series, as shown in Eq. [4].

Eq. [4]—HDT minimum availability theoretical target

$$\begin{aligned}
 & Se, D(\text{Meta})(t) \leq D(\text{Shu})(t) \times D(\text{1st Stage})(t) \dots \\
 & D(\text{Shu})(t) = D(\text{1st Stage})(t) = D(\text{2nd Stage})(t) = D(\text{Min}) \\
 & D(\text{Min})(t) \geq \sqrt[8]{D(\text{Meta})(t)}, \text{ Logo:} \\
 & D(\text{Min})(8760) \geq 99.61
 \end{aligned}$$

Such a value is the result of this equation, that is, the approximate minimum point. Considering the subsystems availability in 1 year, it is verified that the result of such Monte Carlo simulations of each subsystem presents the availabilities given in Table 4.8.

The subsystems that most impact availability are those that present availability below 99.61%, that is, the first and second hydrodesulfurization stages, selective hydrogen unit, and stabilization as discussed previously. Thus these are the most critical subsystems. The next step uses the availability of each critical subsystem to reach the availability goal. Availability of the system in series will always be lower than the lowest subsystem availability. Considering this, we will adopt blocks in parallel as large blocks in series (eg, two pumps, one operating and the other in standby, are represented together in RBD as a block in series), and in such a manner we will define the critical subsystems and the minimum availability to be obtained by these subsystems, considering the availability of the remaining subsystems. Thus we will use Eq. [5], as follows, to perform an approximation of the minimum estimated value of such referred critical subsystems, and we will define the MTTF and MTTR so that such availability is reached. The Monte Carlo simulation will verify these values, so we can verify if the minimum availability of the systems is obtained optimizing the unit as a whole. Thus Eq. [5] shows a method for performing the estimate of minimum values, which uses the availability of such referred critical subsystems.

Subsystems	Availability (8760 hours)
Shu	98.84%
1st HDS stage	97.69%
2nd HDS stage	97.6%
Stabilization	99.42%
Amina	99.71%
Piping corrosion	99.98%
Hydrogen (Shu make-up)	99.95%
Hydrogen (recycle of 1st and 2nd HDS stages)	99.80%

Eq. [5]—Minimum real target subsystem availability

$$D(\text{Shu})(t) \times D(\text{1st Stage})(t) \times D(\text{2nd Stage})(t) \times D(\text{Est})(t) =$$

$$\frac{D(\text{Goal})(t)}{D1(\text{H}_2\text{Mup})(t) \times \dots \times D1(\text{C})(t)}$$

$$D(\text{Min})(t) = D(\text{Shu})(t) = D(\text{1st Stage})(t) = D(\text{2nd Stage})(t) = D(\text{Est})(t)$$

$$D(\text{Min})(t) = \sqrt[4]{\frac{D(\text{Goal})(t)}{D1(\text{H}_2\text{Mup})(t) \times \dots \times D1(\text{C})(t)}}$$

$$D(\text{Min})(8760) = 0.9925$$

Thus the minimum availability of the subsystems, selective hydrogen unit, first and second stage, must be 0.9925 (1 year). Although the stabilization system availability is 99.42% lower than the initial minimum value, regarding other subsystem availability, the cutting point reduces from 99.61% to 99.25%. This means that it is not necessary to optimize the stabilization subsystem. We will verify such referred values in the final Monte Carlo simulation.

An availability optimization of the following subsystems, selective hydrogen unit, first hydrodesulfurization stage, and second hydrodesulfurization stage was performed using Reliasoft's BlockSim software.

The remaining systems will not be optimized because such referred systems already present availability higher than the values deemed necessary. Therefore the minimum availability of the previous three systems, for the period of 1 year (8760 hours), is 99.25%.

The next step is to define the critical equipment in each subsystem using the same methodology to define the MTTF and MTTR and verifying the results through simulation.

### Selective Hydrogenation Section Optimization

Using the critical subsystem identification methodology we can verify that the critical equipment is the exchangers because of the availabilities being below 99.98, as per Eq. [6].

Eq. [6]—Minimum theoretical target availability of selective hydrogen subsystem equipment

$$\text{Se, } D(\text{Goal})(t) \geq D(\text{FT-01A/B})(t) \times D(\text{V-01})(t) \times D(\text{B-01A/B})(t) \times \dots \times D(\text{V-13})(t)$$

$$E, D(\text{FT-01A/B})(t) = D(\text{V-01})(t)$$

$$= D(\text{B-01A/B})(t) = D(\text{Min})$$

$$D(\text{Min})(t) \geq \sqrt[18]{D(\text{Goal})(t)}, \text{ Logo:}$$

$$D(\text{Min})(8760) \geq 99.98$$

The subsystem's simulation demonstrates that certain exchangers have availability below 99.98% in 8760 hours. This is the subsystem's critical equipment, as shown by the results of the simulation.

In the selective hydrogen unit subsystem, the minimum availability is 99.25%. So the following equipment (P-01, P-02, P-05, P-06, P-07, and P-09) must be optimized. The remaining equipment will not be optimized because they already present availability above the necessary value. Therefore the

minimum availability for the previously discussed equipment, considering the availability of the remaining equipment of the subsystem, will be 99.89% in 1 year, because the other equipment presents availability above the estimated minimum value, as shown in Eq. [7].

Eq. [7]—Minimum availability real target selective hydrogen unit equipment

$$\begin{aligned}
 & D(\text{P-01})(t) \times D(\text{P-02})(t) \times D(\text{P-05})(t)D(\text{P-06})(t) \times D(\text{P-07})(t) \\
 & \times D(\text{P-09})(t) = \frac{D(\text{Goal})(t)}{D(\text{Ft1})(t) \times D(\text{V1})(t) \times D(\text{B1})(t) \times \dots \times D(\text{V13})(t)} \\
 & D(\text{Min})(t) = D(\text{P-01})(t) = D(\text{P-02})(t) = D(\text{P-05})(t) \\
 & = D(\text{P-06})(t) = D(\text{P-07})(t) = D(\text{P-09})(t) \\
 & D(\text{Min})(t) = \sqrt[6]{\frac{D(\text{Goal})(t)}{D(\text{Ft1})(t) \times D(\text{V1})(t) \times D(\text{B1})(t) \times \dots \times D(\text{V13})(t)}} \\
 & D(\text{Min})(8760) = 0.9989
 \end{aligned}$$

To achieve this availability the MTTF has to be 131,400 hours, keeping the MTTR constant for the critical equipment being analyzed. This means that there is a specific value for the MTTR. When repair time is reduced there is always a risk; if a repair is performed in less time, it might not be reliable enough because there is not enough time to do all repair services properly. So the MTTR is 120 hours. The MTTF can be achieved using Eq. [8].

Eq. [8]—MTTF equipment target

$$\begin{aligned}
 D(\text{P-01})(t) & \cong \frac{\text{MTTF}(\text{P-01})(t)}{\text{MTTF}(\text{P-01})(t) + \text{MTTR}(\text{P-01})(t)} \\
 & + \frac{\text{MTTR}(\text{P-01})(t)}{\text{MTTR}(\text{P-01})(t) + 120} \times \exp(-(\lambda + \mu)t) \\
 0.9989 & \cong \frac{\text{MTTF}(\text{P-01})(t)}{\text{MTTF}(\text{P-01})(t) + 120} + \frac{\text{MTTR}(\text{P-01})(t)}{\text{MTTR}(\text{P-01})(t) + 120} \times \exp(-(\lambda + \mu)t)
 \end{aligned}$$

Consider,  $t = 8760$  hours

$$\frac{\text{MTTR}(\text{P-01})(t)}{\text{MTTR}(\text{P-01})(t) + 120} \times \exp(-(\lambda + \mu)t) \cong 0, \text{ Thus:}$$

$$0.9989 \cong \frac{\text{MTTF}(\text{P-01})(t)}{\text{MTTF}(\text{P-01})(t) + 120}$$

$$\text{MTTF}(\text{P-01})(t) - 0.9989\text{MTTF}(\text{P-01})(t) \cong 0.9989 \times 120$$

From now on we consider the following equation to achieve the MTTF target because in 8760 hours the availability equation is simplified to Eq. [9].

Eq. [9]—Availability simplified equation

$$D(t) \cong \frac{\text{MTTF}(t)}{\text{MTTR}(t) + \text{MTTF}(t)}$$

### HDS First-Stage Optimization

Using the critical subsystem identification methodology we can verify that the critical equipment is the exchangers and the furnace, because the availability is below 99.95%, based on Eq. [10].

Eq. [10]—Minimum availability real target of first-stage equipment

$$\begin{aligned} \text{Se, } D(\text{Goal})(t) &\geq D(\text{B-03A/B})(t) \times D(\text{P-11A})(t) \\ &\times D(\text{P-11B})(t) \times \dots \times D(\text{B-09A/B}) \\ \text{and } D(\text{B-03A/B})(t) &= D(\text{P-11A})(t) \\ &= D(\text{P-11B})(t) = D(\text{P-09A/B})(t) = D(\text{Min}) \\ D(\text{Min})(t) &\geq \sqrt[6]{D(\text{Goal})(t)}, \text{ Logo:} \\ D(\text{Min})(8760) &\geq 99.95 \end{aligned}$$

The subsystem's simulation shows that certain equipment has availability below 99.95% in 8760 hours. This is the critical subsystem equipment, as demonstrated by the simulation results.

To have the first stage present a minimum availability of 99.95%, equipment P-11 A–E, F-01, and P-12 must be optimized. The remaining equipment will not be optimized since it already presents availability above the necessary value. Therefore the minimum availability for the previously discussed equipment, considering the availability of the remaining equipment of the subsystem, will be 99.9% in 1 year, because the other equipment presents availability above the estimated minimum value, as shown in Eq. [11].

Eq. [11]—Minimum availability real target of first-stage equipment

$$\begin{aligned} &D(\text{P-11A - E})(t) \times D(\text{F-01})(t) \times D(\text{P-12})(t) \\ &= \frac{D(\text{Goal})(t)}{D(\text{B-03})(t) \times D(\text{B-04})(t) \times \dots \times D(\text{V-05})(t)} \\ D(\text{Min})(t) &= D(\text{P-11A - E})(t) = D(\text{F-01})(t) = D(\text{P-12})(t) \\ D(\text{Min})(t) &= \sqrt[7]{\frac{D(\text{Goal})(t)}{D(\text{B-03})(t) \times D(\text{B-04})(t) \times \dots \times D(\text{V-05})(t)}} \\ D(\text{Min})(8760) &= 0.9990 \end{aligned}$$

The next step is to define the MTTF and the MTTR of the critical equipment, that is, with availability below 99.9%, and simulate the first-stage subsystem to verify if the obtained availability is 99.25%. Therefore, using an MTTF of 14 years for exchangers P-11 A–F, an MTTF of 14 years for F-3501, and an MTTF of 13 years for exchanger P-12, keeping the MTTR of such equipment constant, because of the impossibility of changing the repair time, we were able to obtain an availability of 99.36% in the first-stage subsystem. If that equipment has 99.9% availability, we can verify, for example, the MTTF of the P-11 A–E calculation, considering an MTTR of P-11 A–E as 156 hours, based on historical data, as shown in Eq. [12]. The MTTR equipment values are defined in the repair database.

Eq. [12]—MTTF target of first-stage equipment

$$D(P-11A - F)(t) \cong \frac{MTTF(P-11A - F)(t)}{MTTR(P-11A - F)(t) + MTTF(P-11A - F)(t)}$$

$$0.9990 \cong \frac{MTTF(P-11A - F)(t)}{MTTF(P-11A - F)(t) + 156}$$

$$MTTF(P-11A - E)(t) - 0.9990 \times MTTF(P-11A - E)(t) \cong 0.9990 \times 156$$

$$MTTF(P-11A - E)(t) \cong 122,640 \text{ hours}$$

### HDS Second-Stage Optimization

Using the critical subsystem identification methodology we can verify that the critical equipment is the exchangers and the furnace, because the availability is below 99.946%, based on Eq. [13].

Eq. [13]—Minimum availability theoretical target of second-stage equipment

$$Se, D(Goal)(t) \geq D(B-03A/B) \times D(P-11A)$$

$$\times D(P-11B) \times \dots \times D(B-09A/B)$$

$$E, D(B-03A/B) = D(P-11A)$$

$$= D(P-11B) = \dots = D(B-09A/B) = D(\text{Min})$$

$$D(\text{Min})(t) \geq \sqrt[14]{D(Goal)(t)}, \text{ Logo: } D(\text{Min})(8760) \geq 99.95$$

The subsystem simulation shows that certain equipment has availability below 99.95% in 8760 hours. This is the subsystem’s critical equipment as demonstrated by the simulation results.

To have the second stage present a minimum availability of 99.25%, equipment P-13 A–E, F-02, and P-14 must undergo an increase in availability. The remaining equipment will not be optimized because it already presents availability above the necessary value. Therefore the minimum availability for the previously discussed equipment, considering the availability of the remaining subsystem equipment, will be 99.9% in 1 year, because the other equipment presents availability above the estimated minimum value, as shown in Eq. [14].

Eq. [14]—Minimum availability real target second-stage equipment

$$D(P-13A - E)(t)6 \times D(F-03)(t) \times D(P-14)(t)$$

$$= \frac{D(Goal)(t)}{D(B-03)(t) \times D(V-08)(t) \times \dots \times D(V-09)(t)}$$

$$D(\text{Min})(t) = D(P-13A - E)(t) = D(F-03)(t) = D(P-14)(t)$$

$$D(\text{Min})(t) = \sqrt[7]{\frac{D(Goal)(t)}{D(B-03)(t) \times D(V-08)(t) \times \dots \times D(V-09)(t)}}$$

$$D(\text{Min})(8760) = 0.9990$$

The next step is to define the MTTF and the MTTR of critical equipment, that is, with availability below 99.9%, and simulate the second-stage subsystem to verify if the obtained availability is 99.25%, that is, the subsystem's minimum value. Thus, using an MTTF of 14 years for exchangers P-13 A–E, 15 years for F-02, and 13 years for P-14, keeping the MTTR of such referred equipment constant, because of the impossibility of reducing repair time, we were able to obtain availability of 99.27 in the second-stage subsystem, with all equipment having availability above 99.9. The MTTR equipment values are defined in the repair database.

### ***Optimization of HDT***

After improvement of the critical subsystems, the next step is to verify if the system was optimized with the proposed MTTF improvements using Monte Carlo simulation in BlockSim software. Table 4.9 illustrates the MTTF increases for each subsystem and its critical components, considering the simulation in the period of 1 year and 4 years with the objective of verifying the reliability level that must be maintained to be able to reach an availability target, that is, in 4 years. Table 4.9 illustrates the improvements, availability values, reliability values, MTTF, and MTTR used in this study, as well as the new values proposed. In the proposed situation, the same repair time values (MTTR) used in the analysis were maintained, with only the MTTF values being optimized. For the variation of MTTR values it becomes necessary to perform a repair benchmarking practice to verify the feasibility of the repair time improvements as well as logistic and economic assumptions.

The data presented in Table 4.9 was specified for a time of 8760 hours. The same was done with the time simulation of 4 years (35,040 hours). The system availability achieved was 96.499%, as required by the project. The simulation in 8760 hours is necessary to verify reliability targets. The repair data was not optimized considering that upon removal of the logistic time such referred repair times are already optimized. Upon optimization, the subsystems that most impact the system are the same, showing the need for follow-up on such equipment. Upon evaluation of the results, considering only the reliability of the subsystems, we were able to verify that the same subsystems previously evaluated as critical continue being the most critical in terms of the reliability impact of the system, nonetheless without impacting the system's availability goal.

### ***Conclusions***

The improvement proposals took into consideration the project's availability goal and the limitations in creating redundancies in view of safety issues in the hydrodesulfurization plant, with the use of a methodology that allowed identification of the subsystems and critical components and improvement of availability.

The simulations were conducted for a period of 1 year (8760 hours) regarding equipment characteristics. In addition, the reliability target requirements were established for critical equipment and submitted to equipment suppliers. Such calculations only considered the MTTFs, making it necessary to observe possible MTTR decreases, considering the viability in light of associated costs.

The cost of such proposed solutions was not considered because of lack of information, although such information is important in the decision-making process. The presented solutions assume that the system availability will be lower than the lowest availability among the subsystems.

The objectives of the study were reached because the subsystems and critical equipment were identified and enhanced, allowing the improvement of availability as a whole according to the proposed methodology. This model represents a real-life case because there are usually limitations in

**Table 4.9 Equipment Optimization Proposal**

HDT Optimization									
Process	Equipment	Actual				Proposed			
		Availability	Reliability	MTTF	MTTR	Availability	Reliability	MTTF	MTTR
Shu	P-1/2/5/6/ 7/9	0.998	0.889	7.5	156	0.999	0.945	15	156
1st stage reaction	P-11	0.9984	0.889	7.5	156	0.999	0.932	14	156
	F-1	0.9914	0.61	2	156	0.999	0.938	14	156
1st stage separation	P-12	0.9984	0.889	7.5	29/4	0.999	0.932	13	29/4
2nd stage reaction	F-2	0.9914	0.61	2	156	0.999	0.945	15	156
	P-13	0.9984	0.889	7.5	156	0.999	0.938	14	156
2nd stage separation	P-14	0.9984	0.889	7.5	120	0.999	0.932	13	120

MTTF, mean time to failure; MTTR, mean time to repair.

MTTF and MTTR improvement, and most of the time we know the MTTR values, which are hard to improve. The final MTTF results suggest better material specifications for achieving availability targets. The optimization model is evaluated to compare the results of the two methodologies.

### 4.6.3 THE NONLINEAR OPTIMIZATION METHODOLOGY MODEL: THE REFINERY PLANT AVAILABILITY OPTIMIZATION CASE STUDY

The linear and nonlinear models have been used in many applications in several industries to support decisions in terms of the optimum number of resources, such as human, material, and products, under certain circumstances to maximize or minimize an objective function as profit or cost. This approach can be used to optimize plant availability for MTTF and MTTR limits, equipment reliability targets, and subsystem assumptions. Therefore the system configuration with subsystem and equipment availability can be defined as the first step to achieving the plant's project requirements.

This study has the main objective of defining a specific methodology for equipment and subsystem assumptions to achieve the system availability target using the nonlinear model. RAM analysis will be conducted to define subsystem and equipment availability, MTTR, and MTTF. Moreover, RAM analysis will allow assessment of the consistency of the nonlinear model results.

#### ***Failure and Repair Data Analysis***

Seeking to ensure the confidence of such data, maintenance professionals with knowledge about systems took part in quantitative analysis of failure and repair data. A critical analysis of the cause of system unavailability was conducted regarding critical equipment failure modes.

A historical failure data bank was used, and equipment PDFs were created. The example in Fig. 4.51 shows an incrustation formation PDF in a heat exchanger. If there is no failure data available a qualitative analysis is performed by maintenance professionals.

The example in Table 4.10 shows one heat exchanger, its failure modes, and respective average failure and repair times. The failure mode is incrustation formation. The normal PDF was defined by historical data analysis; repair time was defined by interviews conducted with maintenance technicians and engineers.

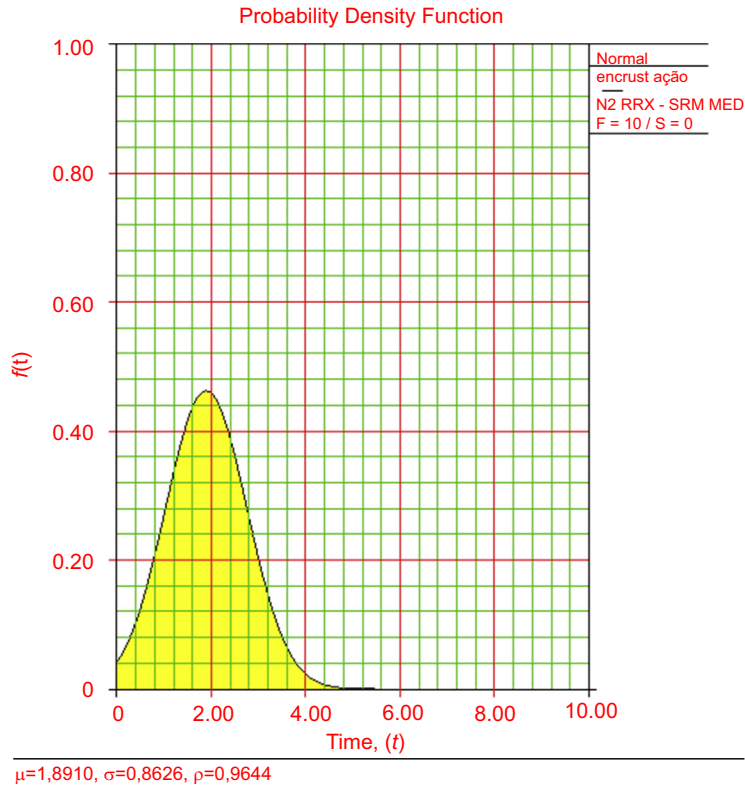
In the same way, the failure and repair data of each subsystem's equipment was defined, and included in the model. In some cases, there was no historical failure data available, so a qualitative analysis was conducted with maintenance technicians and engineers. In these specific cases, a triangular or rectangular function was defined to represent failures modes. So sometimes failure and repair times are defined most likely as pessimist and optimist times.

#### ***Modeling***

To perform the availability results in Monte Carlo simulation it is necessary to model equipment using block diagram methodology. In this way, it is necessary to know the process details that influence production losses. So the following statements and definitions of process limitations were considered:

- If a critical subsystem, such as the depropanizer, the deethanizer, or C3 separation, is unavailable, the propane unit will be unavailable.
- The efficiency target is 99.859%.
- The facility supply has 100% availability in 5 years.
- The total production per day is 41 m<sup>3</sup>/hours.

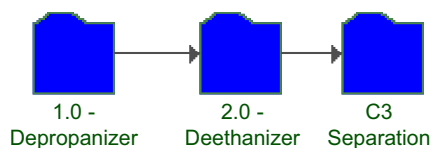




**FIGURE 4.51**  
Exchanger PDF.

Table 4.10 Quantitative Failure and Repair Data					
TAG	Failure Mode	Distribution	Failure Data (years)		
			Parameters		
			P	MP	O
E-7007	Internal corrosion	Triangular	18	20	22
	External corrosion	Triangular	18	20	22
	Incrustation	Normal		$\hat{\theta}$ 1.89	$\mu$ 0.86

P, pessimist; MP, most probable; O, optimist.

**FIGURE 4.52**

Propane subsystem RBD.

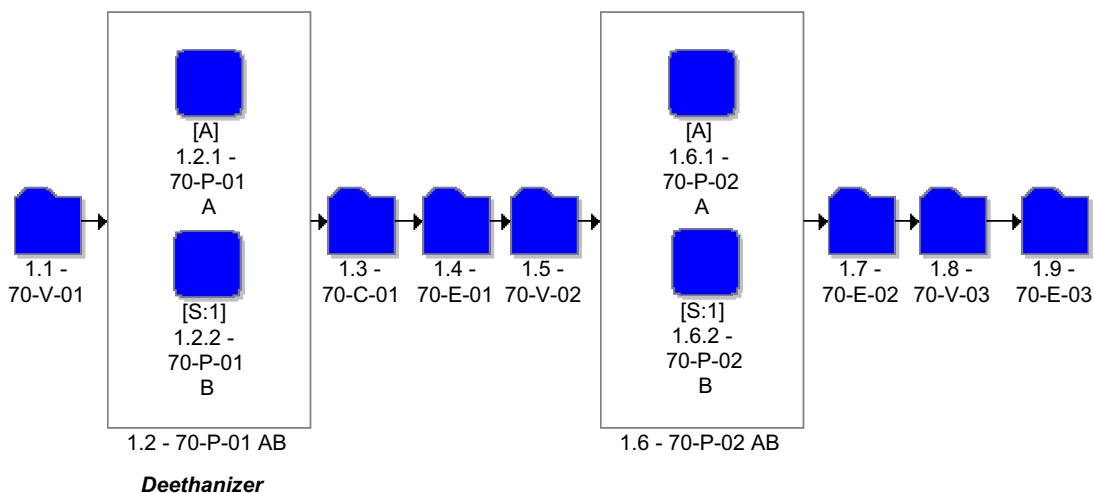
The propane subsystem RBD is given in Fig. 4.52.

### Depropanizer

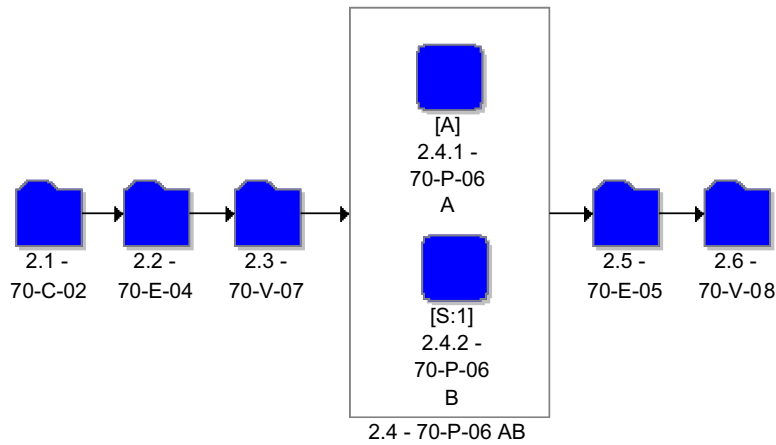
This subsystem has the main objective of separating propane from the feed. There are pumps, exchangers, towers, and vases in series. The pumps are in parallel, one passive and the other active, but both are in series with the other subsystem equipment. In case of failure in any equipment the subsystem will shut down (for pumps, both pumps must shut down to affect the whole subsystem). There is no partial production loss in the case of equipment failure, which means in case of equipment failure the system will lose 100% of production until the repair is done. Fig. 4.53 shows the depropanizer subsystem RBD.

### Deethanizer

This subsystem has the main objective of removing the ethane component. There are pumps, exchangers, towers, and vases in series. The pumps are in parallel, one passive and the other active, but both are in series with the other subsystem equipment. In case of failure in any equipment, the subsystem will shut down (but again, in the case of pump failure, both pumps must fail for the system to be

**FIGURE 4.53**

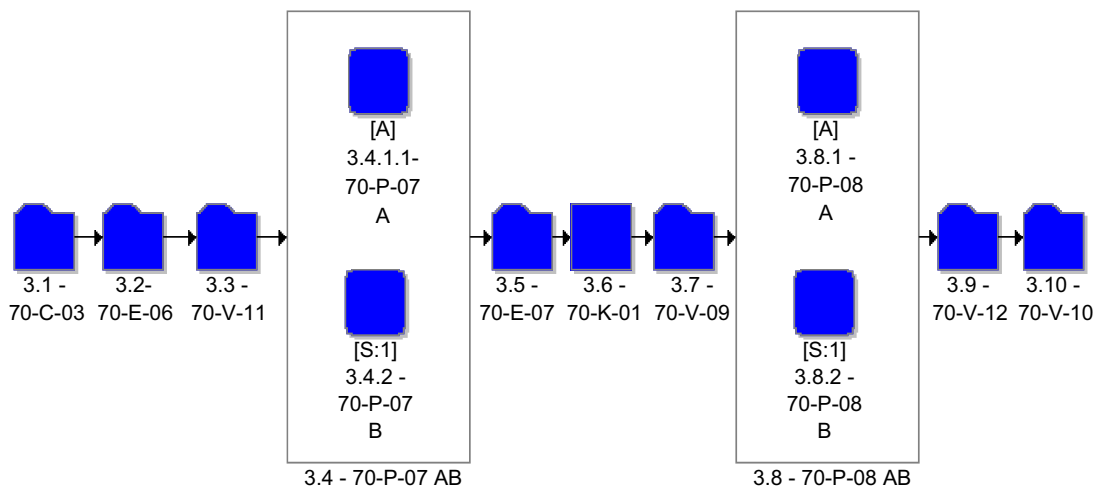
Depropanizer RBD.



**FIGURE 4.54**  
Deethanizer RBD.

affected). Except pumps, any equipment failure will affect the system with 100% of production losses until the repair is done. The deethanizer subsystem RBD is given in Fig. 4.54.

**C3 Separation.** This subsystem has the main objective of removing the ethylene component. There are pumps, exchangers, towers, and vases in series. The pumps are in parallel, one passive and the other active, but both are in series with the other subsystem equipment. In case of failure in any equipment the subsystem will shut down (for pumps, again, both pumps must fail). Except pumps, any equipment failures will affect the system with 100% of production losses until the repair is done. The C3 separation subsystem RBD is represented in Fig. 4.55.



**FIGURE 4.55**  
C3 separation RBD.

### **Simulation**

RAM analysis was done using BlockSim software. The simulation allows the creation of typical life cycle scenarios for the proposed systems with Monte Carlo simulation methodology. The entire unit was modeled through the use of RBDs, considering the redundancies and the possibilities for bypass in each piece of equipment or system configuration. Next, the evaluated model was fed with failure and repair data. The simulation allows the assessment of availability and efficiency results to see if the system is achieving the availability target of 99.859% in 5 years. If the efficiency target is not being achieved, it is necessary to make some improvements in critical equipment such as:

- Through installation of redundancies for the most critical equipment;
- Through improvement of reliability and maintainability of equipment used, without the installation of new redundancies;
- Through a maintenance policy that allows keeping the desired availability level.

The simulation was conducted to 5 years and 250 simulations were run to converge results. The availability and efficiency achieved were both 98.589% in 5 years. There is no difference between the two values because any equipment failure causes shut down in the propane plant, which means 100% loss.

### **Critical Analysis**

The critical analysis defines the most critical subsystems and equipment, which means the equipment that influences production losses the most. There are two indicators to show criticality: the RI and EC.

The first one shows how much one subsystem or equipment influences system reliability. In this way, using partial derivation, it is possible to know how much it is necessary to increase subsystem or equipment reliability to improve the whole system reliability.

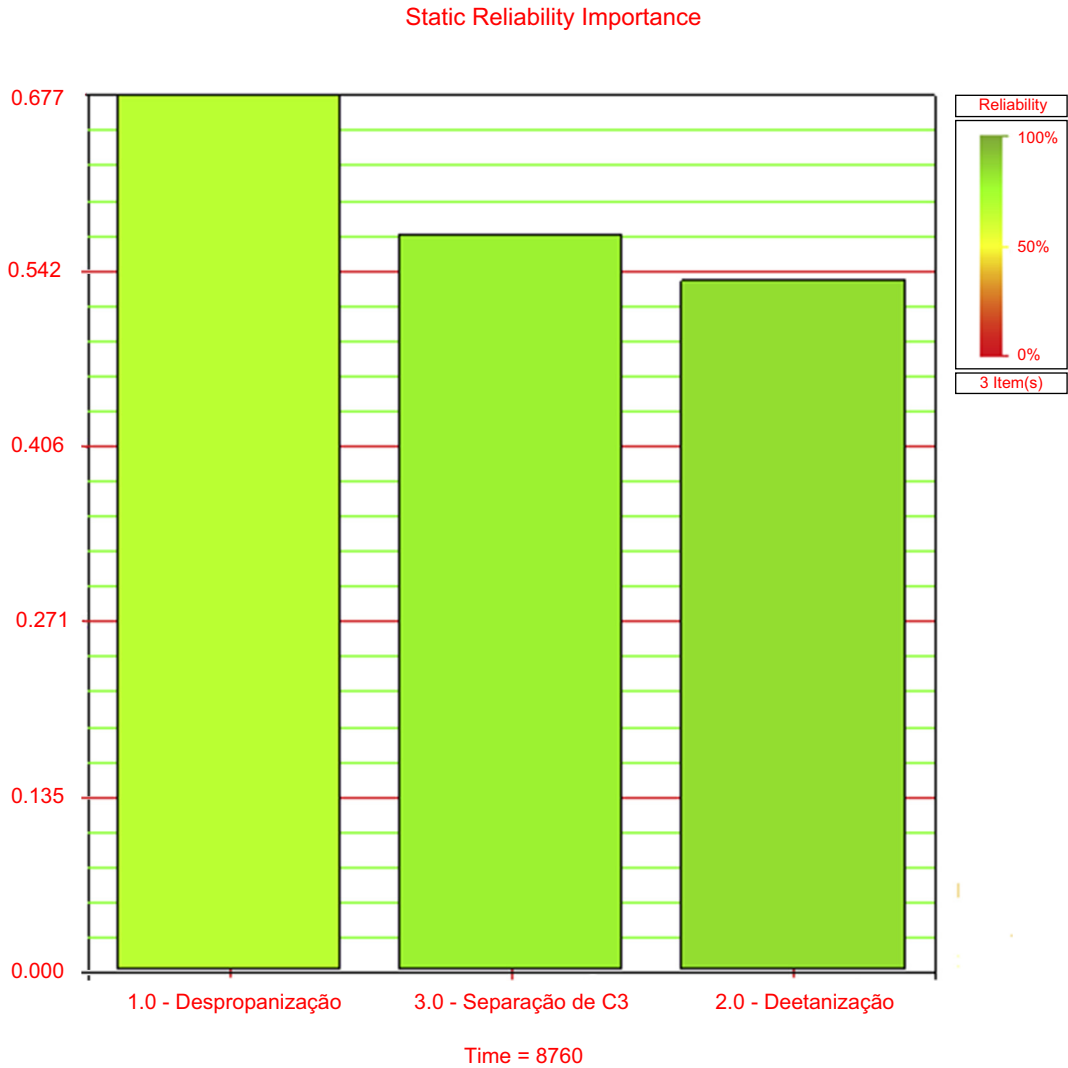
The following equation shows the mathematical relation:

$$\frac{\partial R(\text{System})}{\partial R(\text{Subsystem})} = \text{RI}$$

Despite this relation, some equipment or subsystem may be prioritized because of repair time, which greatly influences production losses. This means that the availability impact is the most important, but even reliability has a great influence on system performance. One specific subsystem or equipment might not be the most critical because of repair time impact. For example, one piece of equipment that has four shutdowns in a specific period of time might not be as critical as another piece of equipment that has only one shutdown, which means the total loss time is higher in the second case than in the first.

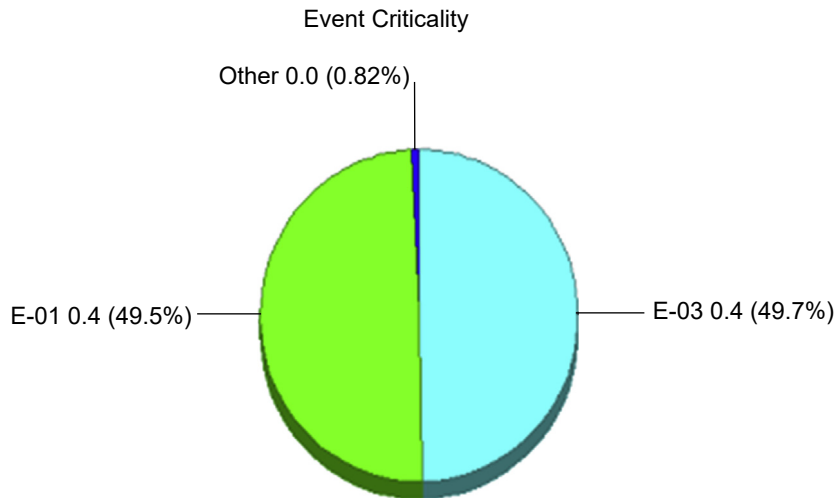
In fact, in most cases it is not possible to reduce repair time, so the equipment reliability improvement is the best solution to achieving the availability target, and in this case the RI is the best index to show how much system reliability can be improved. In fact, it is necessary to consider production losses and reliability equipment. So the EC will indicate the most critical equipment and the RI how much it can be improved to achieve the availability target.

In a propane plant, the most critical subsystem is the depropanizer for the RI and EC. This means that in terms of failure and losses that subsystem is the most critical. The RI results are shown in [Fig. 4.56](#).



**FIGURE 4.56**  
Reliability index.

The results show that the RI for the depropanizer subsystem is 0.577. This means that 1% improvement in this subsystem’s reliability means 0.577 improvement in system reliability in 8760 hours. However, the total subsystem losses represent 49.93%. Looking at the depropanizer subsystem, the exchangers (E-01 and E-03) are the most critical equipment, as shown in Fig. 4.57.

**FIGURE 4.57**

Event criticality.

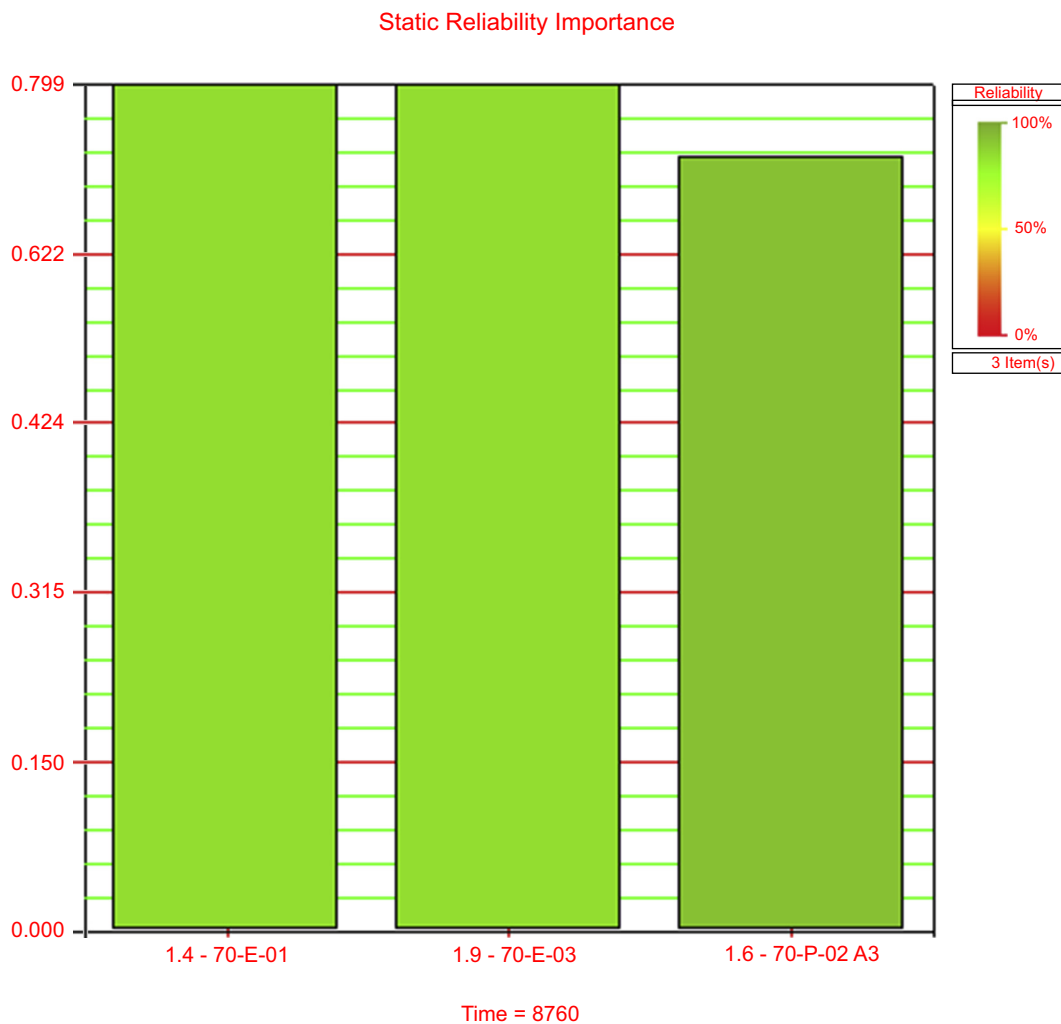
The RI for this subsystem indicates that the two exchangers are the most critical equipment in terms of reliability. The equipment RI is shown in Fig. 4.58. The figure shows E-01 and E-03 as the most critical in terms of reliability and loss time. In this way, the RI indicates how much it is feasible to improve this equipment to improve system reliability. In exchangers E-01 and E-03, for example, the RI is 0.79. This means that for each 1% improvement in this equipment the distillation plant will improve 0.79% in terms of reliability in 8760 hours.

Some limitations must be considered for this approach. The first one is the limitation in equipment improvement. Reliability improvements might not be enough to achieve the availability target. The second limitation is the necessity to improve other critical equipment until the availability target is achieved, and even then it still might not be enough to achieve the availability target.

### **Optimization**

After simulation and critical analysis it is necessary to decide which equipment must be improved to achieve the availability target. In fact, the main objective in this case study is maximizing the availability to achieve 99.859% in 5 years. In this way, it will optimize subsystems and equipment and it will be used as a nonlinear model.

To optimize one system it is necessary to use linear and nonlinear programming, which optimizes one objective function under certain restrictive conditions. Optimization means maximizing or minimizing the objective function. In this case the system availability will be maximized under availability subsystem restriction conditions. The equations and mathematical model are represented in Eq. [1].



**FIGURE 4.58**  
Equipment RI.

Eq. [1]

$$A(\text{System})(t) = A(\text{Despr})(t) \times A(\text{Deet})(t) \times A(\text{Sep C3})(t)$$

$$A(\text{Despr})(t) = \text{Depropanization subsystem availability}$$

$$A(\text{Deet})(t) = \text{Deethanization subsystem availability}$$

$$A(\text{Sep C3})(t) = \text{Separation of C3 availability}$$

$$\text{FO} = \text{Objective function}$$

$$\text{Max} = \text{Maximization}$$

$$\text{FO} \rightarrow \text{Max}: Z = A(\text{Despr})(t) \times A(\text{Deet})(t) \times A(\text{Sep C3})(t)$$

SA

$$A(\text{Despr})(t) \times A(\text{Deet})(t) \times A(\text{Sep C3})(t) \leq 0.9985$$

$$A(\text{Despr})(t) \geq 0.9927$$

$$A(\text{Deet})(t) \geq 0.9966$$

$$A(\text{Sep C3})(t) \geq 0.9965$$

$$A(\text{Despr})(t), A(\text{Deet})(t), A(\text{Sep C3}) \leq 1$$

To solve this mathematical model it is necessary to change the nonlinear model to a linear model and then use some specific method such as simplex or dual simplex. So as a first step it will be applied by  $\ln$  (Naperian log) to both sides of the equations to linearize the model, as shown in Eq. [2].

Eq. [2]

$$\text{FO} \rightarrow \text{Max}: \ln(Z) = \ln(A(\text{Despr})(t) \times A(\text{Deet})(t) \times A(\text{Sep C3})(t))$$

SA

$$\ln(A(\text{Despr})(t) \times A(\text{Deet})(t) \times A(\text{Sep C3})(t)) \leq \ln(0.9985)$$

$$\ln(A(\text{Despr})(t)) \leq \ln(0.9927)$$

$$\ln(A(\text{Deet})(t)) \geq \ln(0.9966)$$

$$\ln(A(\text{Sep C3})(t)) \geq \ln(0.9965)$$

$$\ln(\text{Despr})(t) = x_1, \ln(A(\text{Deet})(t)) = x_2, \ln(A(\text{Sep C3})) = x_3$$

$$\ln(0.9927) = -0.0073$$

$$\ln(0.9966) = -0.0034$$

$$\ln(0.9965) = -0.0035$$



So

$$\text{FO} \rightarrow \text{Max: } D = x_1 + x_2 + x_3$$

SA

$$x_1 + x_2 + x_3 \leq -0.0014$$

$$x_1 \geq -0.0073$$

$$x_2 \geq -0.0034$$

$$x_3 \geq -0.0035$$

$$x_1, x_2, x_3 \geq 0$$

In this way, the nonlinear model was turned into a linear model, but it is necessary to put the model into standard and canonic forms as follows:

Standard form:

$$\text{FO} \rightarrow \text{Max: } Z = cx$$

SA

$$A \cdot x \leq b$$

$$x \geq 0$$

$$c \in R^n, x \in R^n, A \in R^{m \times n}, b \in R^m$$

Canonic form:

$$\text{FO} \rightarrow \text{Max: } Z = cx$$

SA

$$A \cdot x = b$$

$$x \geq 0$$

$$b \geq 0$$

$$c \in R^n, x \in R^n, A \in R^{m \times n}, b \in R^{m+n}$$

Eq. [2] will be turned into canonic form to solve, so it will be necessary to put new variables called basic variables and artificial variables, as shown in Eq. [3]. The main objective of artificial and basic variables is to be able to put equation restriction in an equation form ( $Ax = 0$ ).

Eq. [2]

$$\text{FO} \rightarrow \text{Max: } D = x_1 + x_2 + x_3$$

SA

$$x_1 + x_2 + x_3 \leq -0.0014 \therefore$$

$$(x-1)x_1 \geq -0.0073(x-1) \therefore -x_1 \leq 0.0073$$

$$(x-1)x_2 \geq -0.0034(x-1) \therefore -x_2 \leq 0.0034$$

$$(x-1)x_3 \geq -0.0035(x-1) \therefore -x_3 \leq 0.0035$$

$$x_1, x_2, x_3 \geq 0$$

Adding basic and artificial variables the equations are:

So

$$\text{FO} \rightarrow \text{Max: } D = x_1 + x_2 + x_3$$

SA

$$x_1 + x_2 + x_3 - x_4 + x_5 = -0.0014$$

$$-x_1 + x_6 = 0.0073$$

$$-x_2 + x_7 = 0.0034$$

$$-x_3 + x_8 = 0.0035$$

$$x_1, x_2, x_3 \geq 0$$

This model could be solved using the simplex model, but to save time it can be run on Microsoft Excel's Solver tool. The results are as follows:

$$A(\text{System})(t) = 0.99859$$

$$A(\text{Despr})(t) = 0.99953$$

$$A(\text{Deet})(t) = 0.99953$$

$$A(\text{Sep C3})(t) = 0.99953$$

In fact, the next step is using the same methodology to each subsystem to find out equipment availability, so the depropanization subsystem model is shown in Eq. [3]:

Eq. [3]

$$\begin{aligned} A(\text{Despr})(t) &= A(70\text{-V-01})(t) \times A(70\text{-V-02})(t) \times A(70\text{-V-03})(t) \\ &A(70\text{-E-01})(t) \times A(70\text{-E-02})(t) \times A(70\text{-E-03})(t) \times A(70\text{-C-01})(t) \\ &\times A(70\text{-P-01})(t) \times A(70\text{-P-02})(t) \end{aligned}$$

$$A(\text{Despr})(t) = \text{Depropanization subsystem availability}$$

$$A(70\text{-V-01})(t) = \text{Vase 1 availability}$$

$$A(70\text{-V-02})(t) = \text{Vase 2 availability}$$

$$A(70\text{-V-03})(t) = \text{Vase 3 availability}$$

$$A(70\text{-E-01})(t) = \text{Exchanger 1 availability}$$

$$A(70\text{-E-02})(t) = \text{Exchanger 2 availability}$$

$$A(70\text{-E-03})(t) = \text{Exchanger 3 availability}$$

$$A(70\text{-C-01})(t) = \text{Tower 1 availability}$$

$$A(70\text{-P-01})(t) = \text{Pump 1 availability}$$

$$A(70\text{-P-02})(t) = \text{Pump 2 availability}$$

FO = Objective function

Max = Maximization

$$\begin{aligned} \text{FO} \rightarrow \text{Max: } Z &= A(70\text{-V-01})(t) \times A(70\text{-V-02})(t) \times A(70\text{-V-03})(t) \\ &A(70\text{-E-01})(t) \times A(70\text{-E-02})(t) \times A(70\text{-E-03})(t) \times A(70\text{-C-01})(t) \\ &\times A(70\text{-P-01})(t) \times A(70\text{-P-02})(t) \end{aligned}$$

SA

$$\begin{aligned} &A(70\text{-V-01})(t) \times A(70\text{-V-02})(t) \times A(70\text{-V-03})(t) \\ &A(70\text{-E-01})(t) \times A(70\text{-E-02})(t) \times A(70\text{-E-03})(t) \times A(70\text{-C-01})(t) \\ &\times A(70\text{-P-01})(t) \times A(70\text{-P-02})(t) \leq 0.99953 \end{aligned}$$

$$A(70\text{-V-01})(t) \geq \text{Vase 1 availability}$$

$$A(70\text{-V-02})(t) \geq 1$$

$$A(70\text{-V-03})(t) \geq 1$$

$$A(70\text{-E-01})(t) \geq 0.9965$$

$$A(70\text{-E-02})(t) \geq 1$$

$$A(70\text{-E-03})(t) \geq 0.9966$$

$$A(70\text{-C-01})(t) \geq 1$$

$$A(70\text{-P-01})(t) = 0.9999$$

$$A(70\text{-P-02})(t) \geq 1$$

To achieve the model results faster the Excel Solver tool was used. The simulation results are:

$$A(\text{Despr})(t) = 0.99953$$

$$A(70\text{-V-01})(t) = 1$$

$$A(70\text{-V-02})(t) = 1$$

$$A(70\text{-V-03})(t) = 1$$

$$A(70\text{-E-01})(t) = 0.9998$$

$$A(70\text{-E-02})(t) = 1$$

$$A(70\text{-E-03})(t) = 0.9998$$

$$A(70\text{-C-01})(t) = 1$$

$$A(70\text{-P-01})(t) = 0.9999$$

$$A(70\text{-P-02})(t) = 1$$

In the deethanizer subsystem model the results are:

$$A(\text{Despr})(t) = 0.99953$$

$$A(70\text{-V-07})(t) = 1$$

$$A(70\text{-V-08})(t) = 1$$

$$A(70\text{-E-04})(t) = 0.9998$$

$$A(70\text{-E-05})(t) = 0.9998$$

$$A(70\text{-C-02})(t) = 1$$

$$A(70\text{-P-06})(t) = 1$$

And in the C3 separation subsystem the results are:

$$A(\text{Despr})(t) = 0.99953$$

$$A(70\text{-V-09})(t) = 1$$

$$A(70\text{-V-10})(t) = 0.99963$$

$$A(70\text{-V-11})(t) = 1$$

$$A(70\text{-V-12})(t) = 1$$

$$A(70\text{-E-06})(t) = 1$$

$$A(70\text{-E-07})(t) = 1$$

$$A(70\text{-K-01})(t) = 0.9999$$

$$A(70\text{-C-03})(t) = 1$$

$$A(70\text{-P-07})(t) = 1$$

$$A(70\text{-P-08})(t) = 1$$

As the heat exchangers are similar in all subsystems, heat exchanger availability improvement will have the same effect on each subsystem's availability. As those heat exchangers are the most critical system equipment, to achieve the system's availability target it is necessary to achieve the heat exchangers' availability target. Thus to achieve availability of 99.98% in 5 years it is necessary to have a normal distribution with  $\mu = 6$  years and  $\sigma = 1$  year incrustation failure mode PDF. In this way, the whole system achieves 99.86% availability, the depropanizer subsystem achieves 99.92%, the deethanizer subsystem achieves 99.98%, and the C3 separation subsystem achieves 99.97% availability in 5 years.

### **Conclusion**

The nonlinear model is a good methodology for supporting RAM analysis decisions in terms of critical equipment optimization. There are many mathematical models that can be used, depending on model configuration and function features.

Despite the model results not being that similar to real results the results are a good starting point for sensitivity analysis.

The system availability will be achieved if incrustation failure is eliminated in 5 years, and it will be necessary to avoid such a failure mode. So efficiency in water treatment to avoid incrustation in tubes of heat exchangers is required.

The objective of such a model is to define equipment MTTF and then the equipment PDF. The additional important point is to consider some cost value in this mathematical model.

#### 4.6.4 CENPES II PROJECT RELIABILITY ANALYSIS CASE STUDY

The CENPES II project is a new research center that supports high-technology implementation and development in onshore and offshore subjects such as oil exploration, production, and refineries at the Petrobras Company. In this research center there will be a Petrobras data center (CIPD, center integrated processing data) that requires high availability. The CENPES II project reliability analysis has as a main objective to find out if the CIPD and important laboratories will have 99.99% availability in 200,000 hours as required. Therefore some subsystems, such as the electrical, natural gas, diesel oil, cold water, and water cooling subsystems, will be analyzed in terms of reliability, availability, and maintainability to verify the required availability for the CIPD and the laboratories. This reliability analysis will consider the subsystems and each piece of critical equipment and its failure and repair time to verify the availability required for this project. A failure and repair analysis, FMEA, block diagram and modeling, and optimization and efficiency cost analysis will be performed in this case study.

##### ***System Characteristics***

###### **Electrical Subsystem**

The electrical power required for running the CENPES II and CIPD installations will be provided via a cogeneration subsystem with three motor generators powered by natural gas, with 3.5 MVA each, at 13.2 kV, three phases, 60 Hz, suitable for continuous generation of electrical power and to be located in the utility building. The electrical subsystem of the cogeneration plant will operate together with the local electrical power provider, Light SESA, which, during a downtime of the generation equipment for unscheduled maintenance, will immediately activate, without interruptions, the site's electrical load. Power supply by Light, at a tension of 13.2 kV, three phases, 60 Hz, will be used as power backup and to supplement demand.

It will be necessary to contract from Light two independent underground feeders. Both circuits, one a spare of the other, with automatic feed transfer, will be capable of meeting estimated initial load plus 25% for future expansion. There will be an emergency power supply system included for the three generators powered by diesel oil, feeding the electrical system, in the event of loss of power from main generators and Light.

###### **Natural Gas Subsystem**

Natural gas will be the energy source for the CENPES II cogeneration system. Natural gas will be provided by CEG SA at 4 kgf/cm<sup>2</sup> for consumption of the entire CENPES II (labs, kitchen, etc.). The system will include three 1600-kW (first phase) Caterpillar motor generators and three boilers, with another three redundant fire-tube steam boilers. The steam produced in recovery boilers (one boiler for

each motor generator) comes out from thermal energy exhaust gases from combustion in gas-powered motor generators. The system will allow for remote operator performance. The system will provide saturated steam at  $8 \text{ kgf/cm}^2$  for cooling unit(s) for double-effect absorption, which will produce cold water at a temperature of  $6^\circ\text{C}$  for use by CENPES II and the CIPD Rio air-conditioning system. To meet the needs of the steam system of CENPES II (kitchen areas, labs, etc.) and the CIPD, production of steam should be via three automatic boilers powered by natural gas at a steam generating capacity of 4.15 t/hours.

#### Diesel Oil Subsystem

The diesel oil system will include a  $170\text{-m}^3$  storage tank located outside the utilities building and supplied as per emergency demand. There will be two smaller  $50\text{-m}^3$  tanks to supply the three 2.5-MVA gas-powered generators and for the Light supplier, with preferential customer CIPD using 90% of its capacity and CENPES II using 10%.

#### Water-Cooling Subsystem

The water-cooling subsystem will be built in the same area as the new CENPES II utilities center building to meet the cold water consumption needs of CIPD and CENPES II equipment. The cooling tower will have a final installed capacity that meets total water cooling consumption ( $6.6 \text{ m}^3/\text{hours}$ ). In each phase, only the water-cooling system equipment will be installed (pumps, cells, including fans and packing) that is required to meet such consumption. Thus, in the first phase, the main towers and circulation pumps will meet an (approximate) consumption of  $4500 \text{ m}^3/\text{hours}$ . There will be four cooling towers, four pumps, and components that will take water cooling of electrical and absorption chillers, generating a closed circuit among towers, pumps, and chillers. Water cooling is essential for the functioning of the cold water system, as it keeps chillers at their operating temperature. In the event of a cooling subsystem failure the CIPD will be unavailable.

#### Cold Water Subsystem

The cold water subsystem will include four absorption and four electrical chillers, with pumps, valves, and control meshes, requiring at least one chiller for the CIPD supply. Thus the electrical chillers will remain as cold water system redundancy. This subsystem is essential to CIPD availability, because in the event of downtime the CIPD will be unavailable.

In the event of failed gas supply to absorption chillers and motor generators, the three electrical chillers go into operational mode automatically, with power provided by Light. In the event of simultaneous failure of gas and electrical power supply by respective providers, only the CIPD will be maintained, with electrical power provided by diesel generators. Thus, in the first phase, under emergency conditions (electrical power supply failure by provider and/or gas supply failure), the water-cooling system will minimally provide the volume required to maintain one electrical chiller operational so as to supply the CIPD.

### ***Data Analysis***

Currently, one of the greatest obstacles to reliability studies at organizations is the lack of a reliable database representing the reality of equipment failure and repair. This is the result of several factors, including structural, cultural, and technological, among others. In this case study it is easy to note that the inexistence of a culture of data collection within operational ground may be related to the fact that

their equipment does not present failures on a daily basis, which has an impact on the system by causing significant downtimes and loss of production. Another important aspect is that units are projected with a high level of redundancy, and the existence of a long inventory of replacement parts makes failure impact less relevant. Despite the existence of technology available for the setting up of a large database, the size of the company makes it difficult to reach a conclusion as to the ideal model for the failure database. As a result, databases were consulted, such as OREDA, which have data on offshore equipment failure. However, this situation gives rise to the question of whether the database is representative of the system under analysis.

To ensure representativeness of data collected, interviews were conducted with maintenance professionals knowledgeable in the systems studied and a qualitative analysis was performed of failure and repair times. To define equipment to be qualified, FMEAs on the systems were run, with standardization of the main equipment failure modes that have the greatest impact on their respective subsystems. To qualify repair data, repair and logistic times were considered, with time defined as the time taken to supply the equipment or component required for use by the system, from the moment it was ordered until it was available in the stock room.

Total repair time is the sum of repair time, plus logistic time, with three time scenarios being considered: pessimistic, most likely, and optimistic. In this study, one may note that repair times are compatible with those in theoretical databases, as opposed to logistic times, which present great deviation. In this case it was perceived that the logistic time for acquisition of a component from the moment it is ordered until it is available in the stock room varies between 3 and 4 months on average. For imported components, logistic time increases to 6 or 9 months on average. Therefore we consider that components will be available within an appropriate logistic time that does not consider logistic time for delivery of components.

Pessimistic, optimistic, and most likely scenarios were considered for failure times based on likely, very likely, remote, and extremely remote occurrences. A failure rate was associated to each qualification, as shown in [Table 4.11](#).

$1 \times 10^{-5}$	Extremely difficult	Extremely difficult but possible <ul style="list-style-type: none"> <li>• This has never happened before</li> <li>• Multiple failures happen together</li> <li>• It has happened over 35 years</li> </ul>
$1 \times 10^{-4}$	Difficult	Very difficult but possible <ul style="list-style-type: none"> <li>• It has happened under special circumstances</li> <li>• This has never happened before</li> <li>• It happens between 15 and 3 years</li> </ul>
$1 \times 10^{-3}$	Possible	Possible to happen <ul style="list-style-type: none"> <li>• It has happened more than once</li> <li>• It can happen because of a single failure</li> <li>• It has happened between 1 and 15 years</li> </ul>
$1 \times 10^{-2}$	Very possible	Very possible to happen <ul style="list-style-type: none"> <li>• It has happened many times</li> <li>• It has happened more than once a year</li> </ul>

TAG Tank	Failure Mode 1						
	MTTF			SD	Failure Rate		
	P	MP	O		P	MP	O
T1 (Grande)	10,000	55,000	100,000	45,000	0.0001	6E-05	1E-05
VS1	10,000	55,000	100,000	45,000	0.0001	6E-05	1E-05
B1	1000	5500	10,000	4500	0.001	0.0006	1E-04
MC2	1000	5500	10,000	4500	0.001	0.0006	1E-04

MTTF, mean time to failure; P, pessimistic; MP, most likely; O, optimistic; SD, standard deviation.

As an example of failure data qualification, [Table 4.12](#) shows failure rates and repair times defined during interviews with maintenance technicians and engineers. The times are defined as pessimistic (P), most likely (MP), and optimistic (O). The example shows the diesel oil subsystem, with tank components (T1), tank output valves (VS1), pumps (B1), and control meshes (MC2). The same analysis was applied to the other subsystems and data was entered into the simulation model.

Similarly, repair times were defined for each subsystem, with repair time the sum of logistic time and equipment repair time. Logistic time was expurgated for model analysis as it would have a significant but nonrealistic impact. We therefore assume that policies for storage and distribution of components will be optimized.

### **System Modeling and Simulation**

#### **System Modeling**

For the modeling of the system, all subsystems and equipment were considered that will make the CIPD system unavailable in the event of failure. Natural gas, electrical, diesel oil, water cooling, and cold water were subsystems considered in the block diagram. Parallel systems and equipment are those that cause no direct system unavailability, requiring combined failure events for such conditions to occur.

Serially modeled systems and equipment are those that cause system unavailability in the event of failure. This study used an electrical system with generations serially modeled (Light, diesel oil, and gas) with a water-cooling system, since unavailability of either system will cause CIPD unavailability. The water-cooling system keeps electrical and absorption chillers available. In the event of failure, the cold water system becomes unavailable, shutting down the CIPD. The water-cooling system cools off chillers and the cold water system cools off the CIPD. Electrical chillers are in series with the water-cooling system and the electrical system as a redundancy in the event of failure of the absorption chillers in series with the water-cooling system and gas boilers. [Fig. 4.59](#) provides the full system model.

The availability required by the CIPD is 99.99% in around 20 years of operation. System simulation results were 100% availability ( $D(200,000) = 1$ ), with 2000 hours being considered (approximately 20 years). This means the system will be operational 100% of the time ( $t = 200,000$  hours). System reliability was 100%. This means the probability that the system will work 200,000 hours in accordance with its tasks is 100%. Simulation data is shown in [Table 4.13](#).



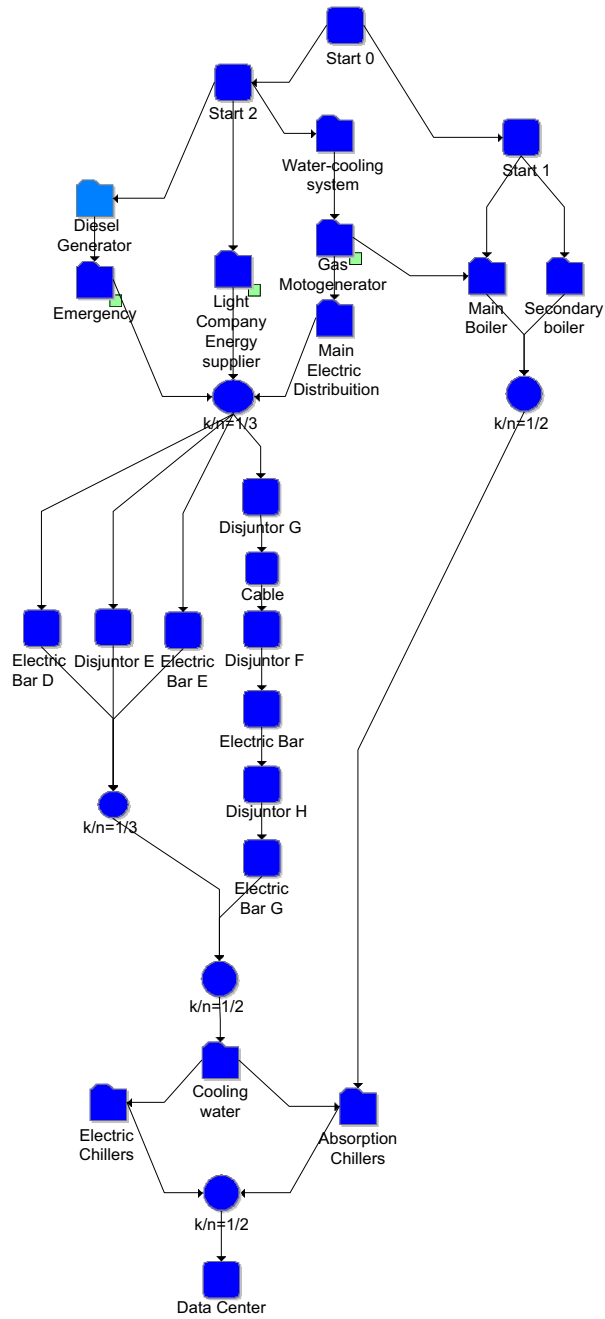


FIGURE 4.59

System modeling.

Source: Calixto and Schmitt, 2006.

<b>Table 4.13 Simulation Results</b>	
<b>System Overview</b>	
<b>General</b>	
Mean availability (all events)	1
Standard deviation	0
Mean availability (w/o PM and inspection)	1
Point availability (all events) at 200,000	1
Reliability at 200,000 hours	1
Expected number of failures	0
MTTFF	15,292,567
<b>System Uptime/Downtime</b>	
Uptime	200,000
CM downtime	0
Inspection downtime	0
PM downtime	0
Total downtime	0
<b>System Downing Events</b>	
Number of failures	0
Number of CMs	0
Number of inspections	0
Number of PMs	0
Total events	0
<b>Costs</b>	
Total costs	0
<b>Throughput</b>	
Total throughput	0
PM, <i>preventive maintenance</i> ; CM, <i>corrective maintenance</i> ; MTTFF, <i>mean time to total failure</i> .	

**Electric System Modeling.** The electrical subsystem includes a set of gas-powered motor generators, Light supply, and diesel oil-powered motor generators, with at least one of the generation subsystems operating for electrical power supply. The components of the distribution system are transformers, circuit breakers, cables, and buses, as shown in Fig. 4.60.

Electrical system availability is 100% in 200,000 hours of operation, programmed maintenance and inspection hours not included. This means that the system is available 100% of the time throughout 200,000 hours. System reliability was  $R(200,000) = 99\%$ . This means that the probability that the system will work in accordance with its established tasks is 99%. It is worth mentioning that the

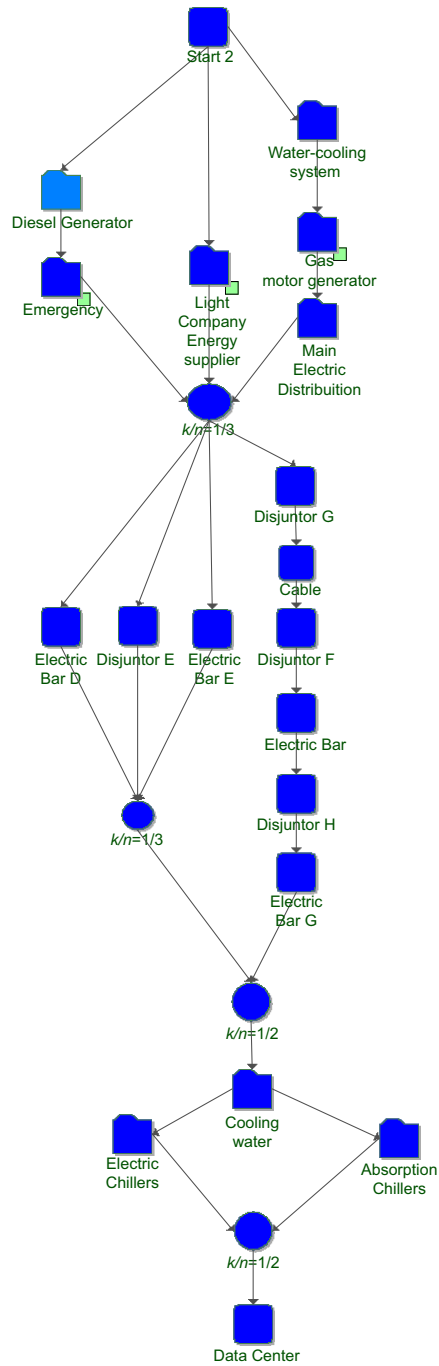


FIGURE 4.60

Electric subsystem modeling.

availability reached is owed to system redundancies and maintainability, where repairs are conducted within expected times and components are available with a high degree of restoration, so that equipment operating conditions after interventions are as good as new.

Studying the reliability index, Light and diesel subsystems offer a great opportunity for reliability improvement. For each 1% improvement in the Light subsystem there will be 0.995% of system improvement.

Mathematically, the reliability index is:

$$\frac{\partial R(\text{CIPD})}{\partial R(\text{Light})} = \text{RI}$$

**Water Cooling Subsystem Modeling.** The water cooling subsystem includes the cooling tower, pumps, and components going all the way up to the chillers. This system is responsible for keeping chillers at an ideal operating temperature. Thus, upon failure of this subsystem, chillers will stop because of overheating, causing unavailability of the cold water system and of the CIPD.

The cooling subsystem is a closed water circuit between the cooling towers and chillers. The sets of tower equipment and components, pumps, and chillers are in series, and it is essential that these components work as good as required to avoid system unavailability. Fig. 4.61 shows four lines of equipment going from the cooling tower to the set of pumps and from there to the chillers.

Availability for 200,000 hours ( $A(200,000) = 1$ ) is 100%, that is, the system will be available all 200,000 hours. System reliability is 91% ( $R(200,000) = 91.2\%$ ). This proves that system redundancies allow for high availability even if there is a failure.

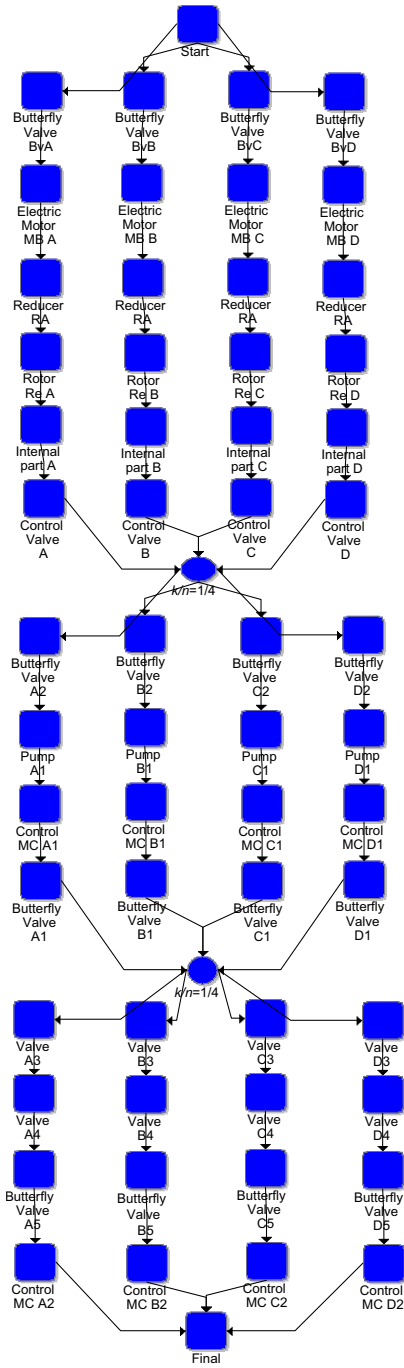
**Cold Water Subsystem Modeling.** The cold water subsystem includes electrical and absorption chillers, primary and secondary circuit pumps, and valves and control meshes in the system, making up a closed circuit as shown in Fig. 4.62. In the CIPD, only one operating electrical or absorption chiller is required for the system to work. Chiller unavailability may be caused by failure in equipment or circuits, with components in series. It is important to remember that the cold water subsystem achieves high availability as a result of preference given to the CIPD, which always has a cold water feed line. As a matter of fact, there are three active redundancies in this case.

The cold water subsystem has  $D(200,000) = 0.99999$ , despite its reliability in 200,000 hours being  $R(200,000) = 0.832$ .

**Laboratories Modeling.** The CENPES II has a group of laboratories that require electrical subsystem and substation availability to operate, as shown in Fig. 4.63. Lab availability is 100% in 200,000 hours, with 85% reliability, with 89% impact because of failure at the substation.

### Optimization

As noted in the results of the simulations, the analyzed system has high availability, and it may have some redundancies in excess. It is important to point out that the recommendation in this case is not to increase system reliability, but to reduce it by reduction of the number of redundancies, preserving the required availability ( $D(200,000) = 0.9999$ ). The first step in optimization is to verify which subsystems most affect the system's reliability. This may be achieved via an index that measures to what degree subsystem reliability influences the CIPD reliability within a given time. By evaluating a period of 1 year, it is easy to see that the absorption chiller subsystem has the most influence on system reliability.



**FIGURE 4.61**  
Water-cooling subsystem modeling.

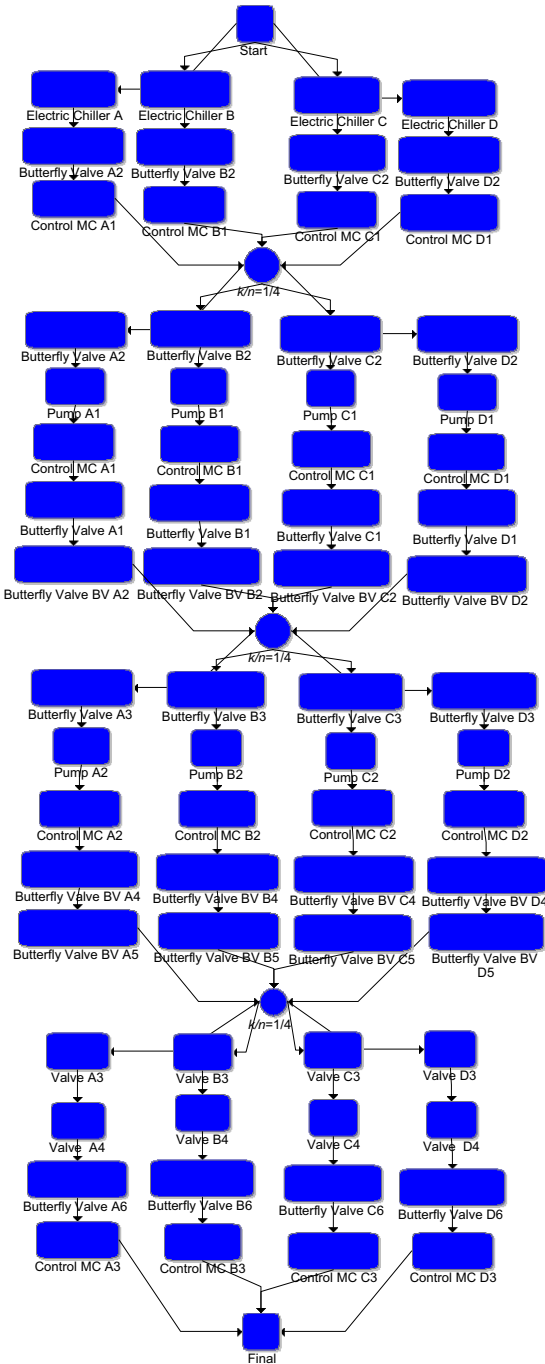


FIGURE 4.62

Cold water subsystem modeling.

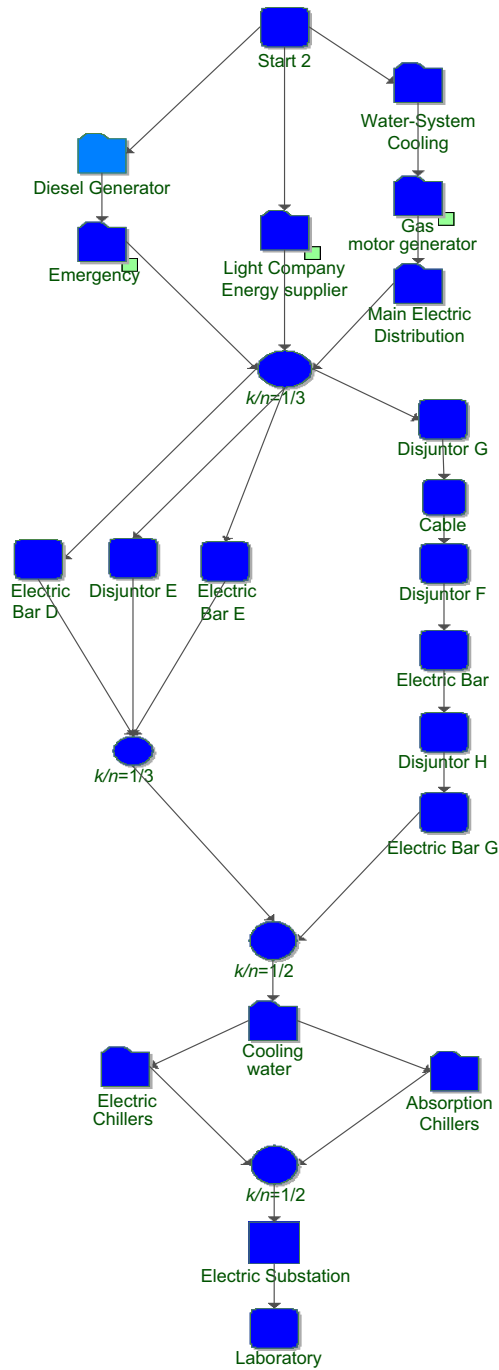


FIGURE 4.63

Laboratories modeling.

Thus these subsystems should be prioritized for measures aiming to increase system reliability. The absorption chiller subsystem has a 62% relationship with the system, which means that a 1% improvement in this system's reliability improves system reliability by 0.62%. Despite the impact on reliability, because of the high number of redundancies, the absorption chiller subsystem does not have a significant impact on system availability. Therefore greater emphasis will be given to the electrical system.

Consequently, we consider case 1, the removal of the Light subsystem as a redundancy in the electrical system, as it impacts the unavailability of the electrical system and its removal does not represent a loss of availability in either the electrical system or the CIPD. Case 2 is the removal of the diesel oil and emergency subsystem, which will not cause significant impact on the availability of the electrical system and the CIPD. In both cases, natural gas-powered motor generators will continue operating, with a single redundancy, diesel oil in case 1 and Light in case 2.

In case 1, availability continues at 100% and reliability drops from 100% to 98%. In relation to the electrical subsystem, removal of the Light subsystem does not have significant impact on the electrical subsystem availability, remaining at 100%, and reliability goes down from 99% to 92%.

In case 2, removal of the diesel oil subsystem also does not impact CIPD availability, with availability remaining at 100%, and reliability going down from 100% to 98%.

The impact on the electrical subsystem in case 2 is more significant in terms of reliability. Electrical subsystem availability remains at 100% and reliability drops from 99% to 90%, matching the value required under project specifications.

In laboratory modeling the high availability depends only on electrical power to work. In this case, optimization methods used for the CIPD will be repeated here, with case 1 being removal of the Light subsystem and case 2 the removal of the diesel oil subsystem.

In case 1, removal of the Light subsystem does not impact availability, remaining at 100%; however, the reliability drops from 85% to 81%, being most impacted by the substation with 68.48% of shutdowns.

In case 2, removal of the diesel oil subsystem does not impact availability; however, reliability goes down to 83%.

As seen, both solutions, cases 1 and 2, are aimed at reducing redundancies in the electrical system while keeping the required availability. Despite the impact on system reliability, absorption chillers present a large number of redundancies ensuring the high availability required. To optimize this subsystem, it would be necessary to evaluate availability required for other systems supplied by cold water and not considered in this study. In relation to the diesel oil and Light subsystems, our decision is to remove the diesel oil subsystem as a result of simulation data showing that it is possible to keep the level of availability. In spite of the reliability reduction, the advantages in terms of cost upon efficiency cost analysis will be clear.

Considering health, safety, and environmental criteria, the case 2 option is the best because of the risks involved in the operation of a 170-m<sup>3</sup> diesel oil tank. This risk should be considered since, in case of failure of this subsystem, a diesel oil spill can occur, which could cause soil contamination or serious damage to the health of workers, with the possibility of diethylamine in the case of fire or explosion.



Direct Cost	Cost D	Qde	Cost F	Cost V	Cost T
<b>Equipment</b>				0	0
Circuit breaker	21,850	4		87,400	87,400
Breaking switch	4400	2		8800	8800
Bus	100,000	5		500,000	500,000
Cable	4400	4		17,600	17,600
Transformer	209,500	2		419,000	419,000
Total					1,032,800
<b>Maintenance</b>					0
Labor	19	37,467		711,873	711,873
<b>Service</b>					0
Supply light	0.3	2084		625.2	625.2
Total					1,033,111.2

### **Efficiency Cost Analysis**

The efficiency cost analysis aims to quantify proposals for system optimization in terms of cost so that one can verify the impact of measures on the cost of the system's implementation and maintenance. In this study, case 1 considers Light removal, representing savings in terms of cost per hour of unavailability of the natural gas system, direct cost of equipment, and maintenance hours. We can thus estimate the cost of the proposal, as shown in [Table 4.14](#).

The cost of equipment was estimated by Icarus software, considering equipment costs and installation. In addition to these costs, maintenance costs were also verified, regarding \$19 HH (human hour) for the Light subsystem. In addition to these values we estimated a median value of \$0.3 related to diesel oil supply services with a total of 2084 downtime hours for the natural gas subsystem. Total estimated cost was \$1,034,263.94 in savings if the Light subsystem was removed without significant effects to the system, matching the required availability of  $D(200,000) = 99.99\%$ .

In case 2, the cost of equipment was also estimated by Icarus software, considering equipment costs and installation, maintenance costs contemplating \$19 HH, and 92 downtime hours for the diesel oil subsystem. In addition to these values, we estimated a median value of \$1 related to electrical energy supply services with a total of 2084 downtime hours for the natural gas subsystem. The total saved cost is \$4,633,663, as shown in [Table 4.15](#). Actually, if the diesel oil subsystem is removed there are no significant effects to the system, which means availability remains 99.99% in 200,000 hours. In addition, when the diesel subsystem is removed the risk related with diesel tanks is eliminated.

### **Conclusions**

This study aimed at verifying availability of systems analyzed and proposing recommendations for system optimization. It is important that the modifications and proposals be analyzed as per impact on system availability and that an analysis of the CENPES II system as a whole be conducted so the remaining parts of the system have an availability that ensures the quality of the services provided.

Analysis of failures and repairs shows the analyzed system, but it is advisable that real failure data be collected and worked with to know the way equipment and components behave in real life upon

<b>Direct Cost</b>	<b>Cost D</b>	<b>Qde</b>	<b>Cost F</b>	<b>Cost V</b>	<b>Cost T</b>
<b>Equipment</b>				0	0
Tank 1	255,400	1		255,400	255,400
Tank 2	119,500	1		119,500	119,500
Pump	129,300	2		258,600	258,600
Valves	1005	4		4020	4020
Valve	1,330,770	3		3,992,310	3,992,310
Total					4,629,830
<b>Maintenance</b>				0	0
Labor	19	92		1748	1748
<b>Service</b>				0	0
Supply diesel	1	2084		2085	2085
Total					4,633,663

failure. Consequently, we suggest setting up a failure and repair database so the system is seen as a whole and that preventive and predictive maintenance can be scheduled, as well as inspections, when required.

We noted that the required availability of 99.99% in 200,000 hours is met even without diesel oil generation, which means optimization in terms of costs and possible environmental damage. In relation to the electrical subsystem, we noted an opportunity for improvement of substations and buses, which should be analyzed upon definition of buses and substations.

#### **4.6.5 THE OPERATIONAL EFFECTS IN AVAILABILITY: THERMAL CRACKING PLANT RAM ANALYSIS CASE STUDY**

While failures are the most critical event that influence system availability, in some cases operational effects such as coke formation that occurs in thermal cracking plants also influence efficiency and availability, and it is necessary to have high efficiency in decoking processes not to lose more production than necessary. RAM analysis supports project decisions for defining which type of process can be conducted to reduce decoking time. Such analysis was conducted in this case study and different decoking procedures and the effects in terms of system availability were compared.

##### ***Failure and Repair Data Analysis***

In this RAM analysis the failure and repair data comes from plants in operation similar to the plant in the project. Thus all knowledge from other plants, such as improvements, equipment problems, and all issues related to availability, should be incorporated into the new project.

Thus, looking at failure and repair equipment files, it was possible to collect data and perform life cycle analysis using statistic software (eg, Weibull++7, Reliasoft) to define PDF parameters for each failure mode.

TAG	Failure mode	Failure time (years)			Repair time (hours)			
		Parameters (PDF)			Parameters (PDF)			
F-01 A	Coke formation	Normal	$\mu$	$\rho$	Normal	$\mu$	$\rho$	
			4.95	2.66		420	60	
	Incrustation	Weibull	$\beta$	$\eta$	$\gamma$	Normal	$\mu$	$\rho$
			0.51	1.05	4.05		420	60
	Others failures	Exponential Bi p	$\lambda$	$\gamma$	Normal	$\mu$	$\rho$	
			0.28	3.22		420	60	
F-01 B	Coke formation	Normal	$\mu$	$\rho$	Normal	$\mu$	$\rho$	
			5.23	2.55		420	60	
	Others failures	Exponential Bi p	$\lambda$	$\gamma$	Normal	$\mu$	$\rho$	
			0.29	4.07		420	60	

**FIGURE 4.64**  
Furnace failure and repair PDF parameters.

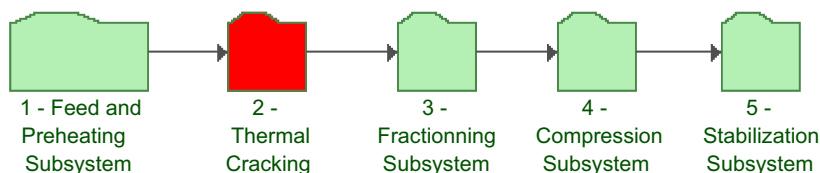
To ensure the accurate representation of such data, maintenance professionals with knowledge of such systems took part in this stage. A critical equipment analysis on the causes of system unavailability and the respective critical failure modes was performed, standardizing all equipment failure modes responsible for most of the impacts in the respective subsystems. The example in Fig. 4.64 shows a coke formation PDF in a fan.

In the same way, the failure and repair data of each subsystem’s equipment was defined, and included in the model. In some cases, there was no historical failure available, motivating the introduction of a qualitative analysis among maintenance technicians and engineers. In these specific cases, the failure and repair PDFs were defined based on specialist discussions about failure and repair time behavior over time.

**Modeling**

To perform the availability results in Monte Carlo simulation, it is necessary to set up model equipment using the block diagram methodology. In this way, it is necessary to be familiar with the production flowsheet details that influence losses in productivity. Consequently, some statements and definitions for process limitations were considered when:

Some critical subsystems such as feed and preheating, thermal cracking, fractioning, compression, and stabilization were unavailable, making the thermal cracking plant unavailable.

**FIGURE 4.65**

Thermal cracking system RBD.

The availability target is 98% in 3 years.

The facility supply had 100% availability in 3 years.

The total production per day was 1500 m<sup>3</sup>.

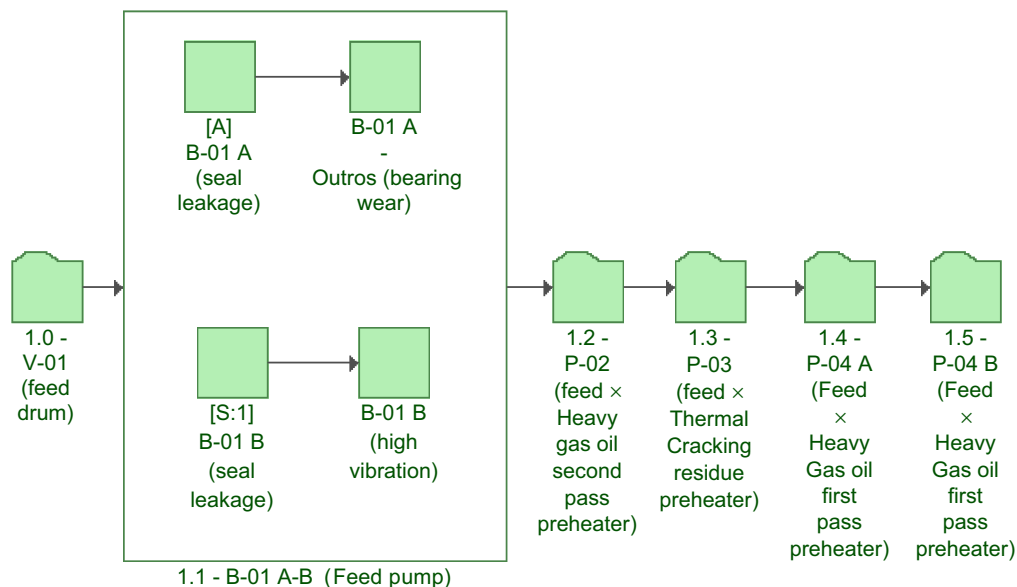
The thermal cracking system RBD is shown in Fig. 4.65.

### Feed and Preheating Subsystem

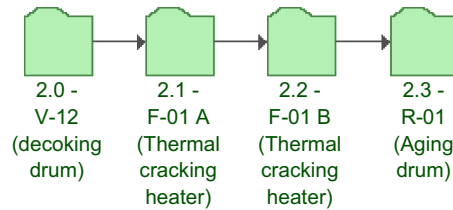
The purpose of this subsystem is heating feed oil to achieve the process temperature before it goes into the furnace. The feed and preheating subsystem RBD assumptions are:

- If V-01 shuts down, the feed and preheating subsystem will be unavailable.
- If B-01 A and B are unavailable during the same period of time, the feed and preheating subsystem will be unavailable.
- If one of the exchangers (P-02, P-03, P-04 A, or P-04 B) shuts down, the feed and preheating subsystem will be unavailable.

The feed and preheating subsystem RBD is shown in Fig. 4.66.

**FIGURE 4.66**

Feed and preheating subsystem RBD.

**FIGURE 4.67**

Thermal cracking subsystem RBD.

### Thermal Cracking Subsystem

The purpose of this subsystem is to perform a thermal crack reaction in the oil feed product. The thermal cracking subsystem RBD assumptions are:

- If V-12 shuts down, the thermal cracking subsystem will be unavailable.
- If F-01 A or B shuts down, the thermal cracking subsystem reduces to 50% of production capacity.
- If R-01 shuts down, the thermal cracking subsystem will be unavailable.

The thermal cracking subsystem RBD is shown in [Fig. 4.67](#).

### Fractioning Subsystem

The purpose of this subsystem is to separate the light component from the heavy component that is happening in the tower (F-01). The fractioning subsystem RBD assumptions are:

- If V-01 shuts down, the feed and preheating subsystem will be unavailable.
- If B-01 A and B are unavailable during the same period of time, the feed and preheating subsystem will be unavailable.
- If one of the exchangers (P-02, P-03, P-04 A, or P-04 B) shuts down, the feed and preheating subsystems will be unavailable.

The fractioning subsystem RBD is represented in [Fig. 4.68](#).

### Compression Subsystem

The purpose of this subsystem is to separate naphtha from a feed in T-03 and send it to the stabilization subsystem. The compression subsystem RBD assumptions are:

- If C-01 shuts down, the compression subsystem will be unavailable.
- If pumps A and B (B-11 A/B, B-12 A/B, and B-13 A/B) are unavailable during the same period of time, the feed and preheating subsystem will be unavailable.
- If one of the exchangers (P-16 A, P-16 B, P-17 A, or P-17 B) shuts down, the compression subsystem will be unavailable.
- If one of the vases (V-04, V-05, or V-06) shuts down, the feed and preheating subsystem will be unavailable.
- If T-03 shuts down, the compression subsystem will be unavailable.

The compression subsystem RBD is represented in [Fig. 4.69](#).

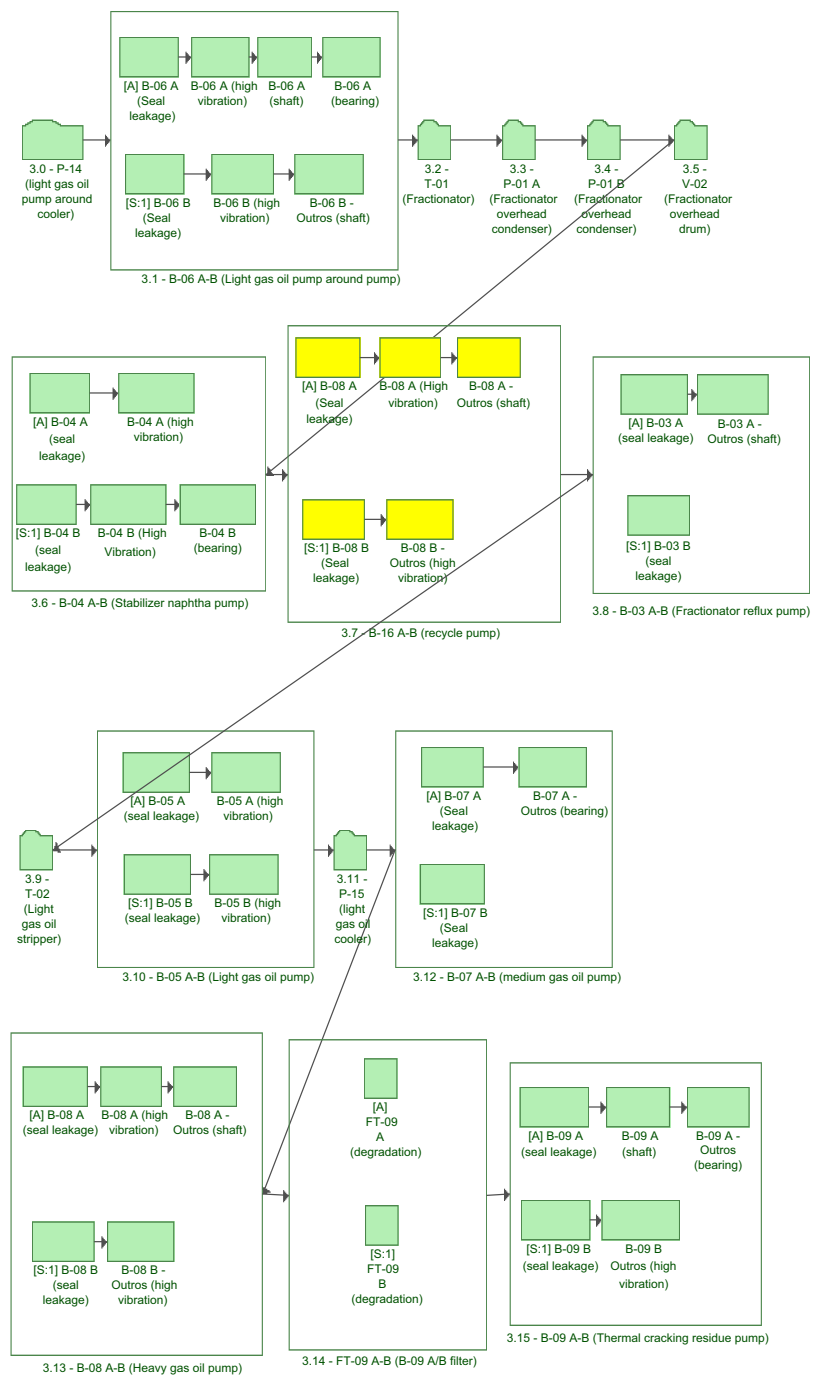
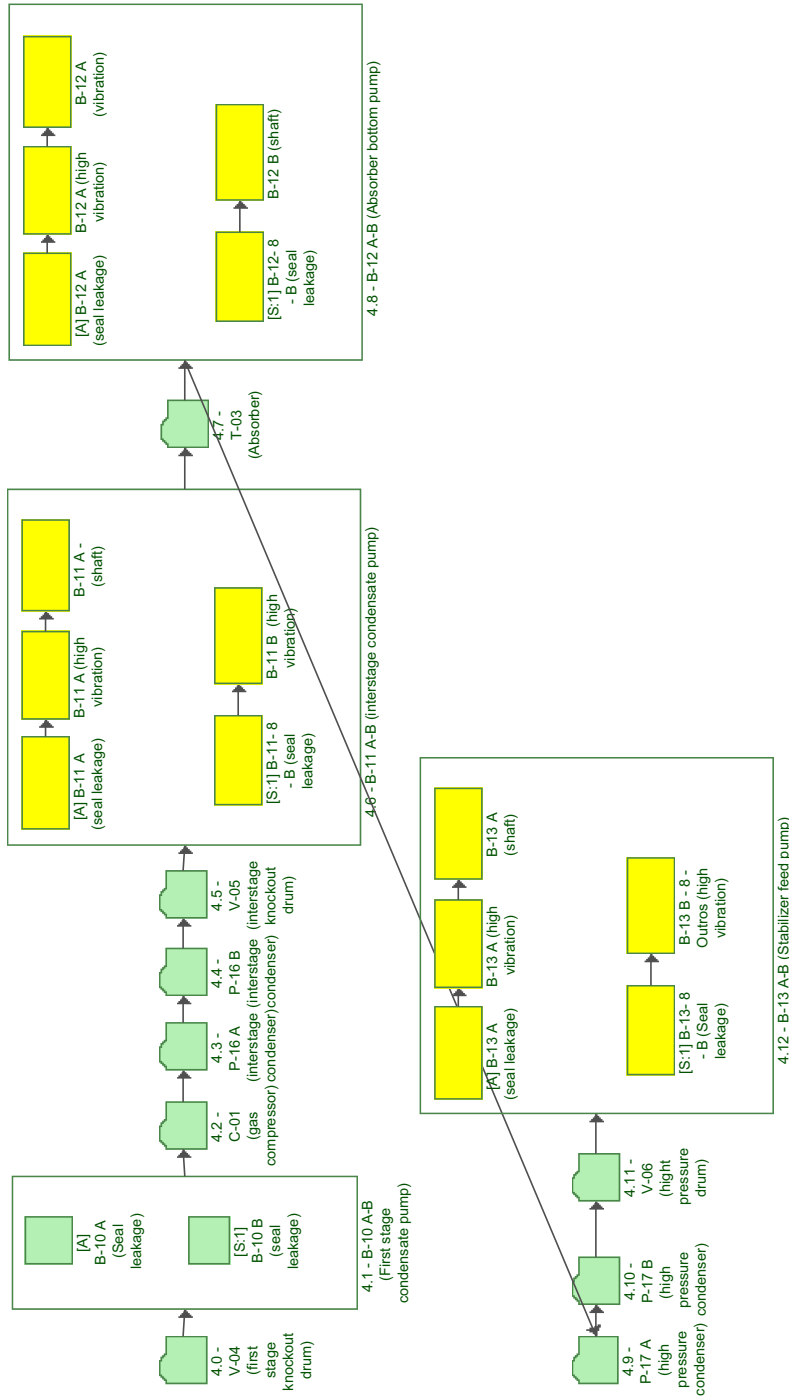


FIGURE 4.68

Fractioning subsystem RBD.



**FIGURE 4.69**

Compression subsystem RBD.

Stabilization

The stabilization subsystem objective is to produce stabilized naphtha and LPG. The stabilization subsystem RBD assumptions are:

- If T-04 shuts down, the compression subsystem will be unavailable.
- If pumps A and B (B-14 A/B and B-15 A/B) are unavailable during the same period of time, the feed and preheating subsystem will be unavailable.
- If one of the exchangers (P-11, P-18 A, P-18 B, P-19 A, P-19 B, P-20 A, or P-20 B) shuts down, the compression subsystem will be unavailable.
- If vase V-07 shuts down, the feed and preheating subsystem will be unavailable.

The stabilization subsystem RBD is represented in Fig. 4.70.

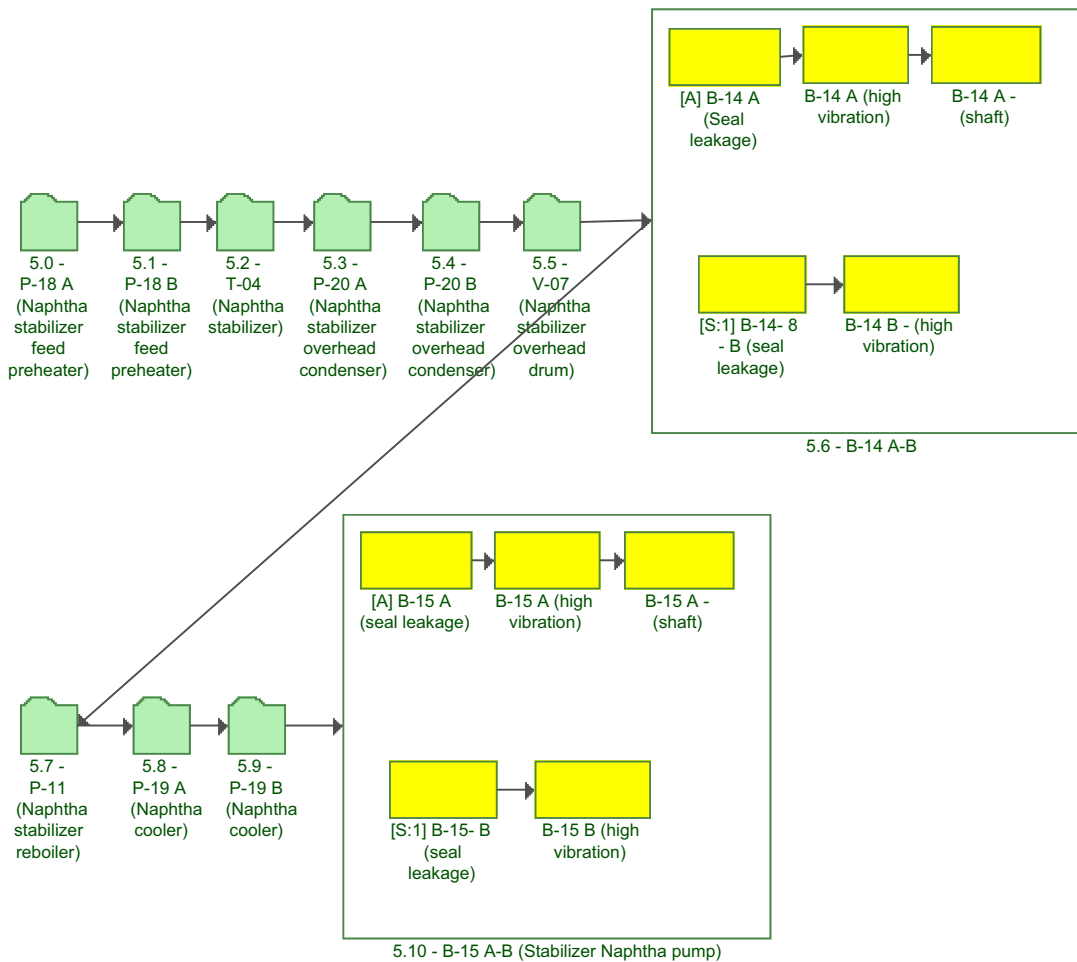


FIGURE 4.70

Stabilization subsystem RBD.



### **Simulation**

RAM analysis was conducted using BlockSim software. The simulation creates typical life cycle scenarios for proposed systems, with Monte Carlo simulation methodology. The entire unit was modeled through RBDs, considering the redundancies and the possibilities for bypass in each piece of equipment or system configuration. Next, the evaluated model was fed to failure and repair data. The simulation allows the assessment of whether the availability results achieve the target of 98% in 3 years. If the efficiency target is not achieved, it becomes necessary to improve the operational capabilities of critical equipment.

The simulation was conducted to 3 years and 1000 tests were run to converge results. The availability was 96.83% in 3 years; 12.52 failures are expected in 3 years, which are related to decoking the furnace. Coke formation is not considered a failure because it is expected to happen in the thermal cracking system.

### **Critical Analysis**

The critical analysis defines which are the most critical subsystems and equipment with the most influence on production losses. There are two indicators showing criticality: the RI and EC.

The first index shows how much influence one subsystem or equipment has on system reliability. Thus, using partial derivation, it is possible to realize how much it is necessary to increase subsystem or equipment reliability to improve the whole system reliability.

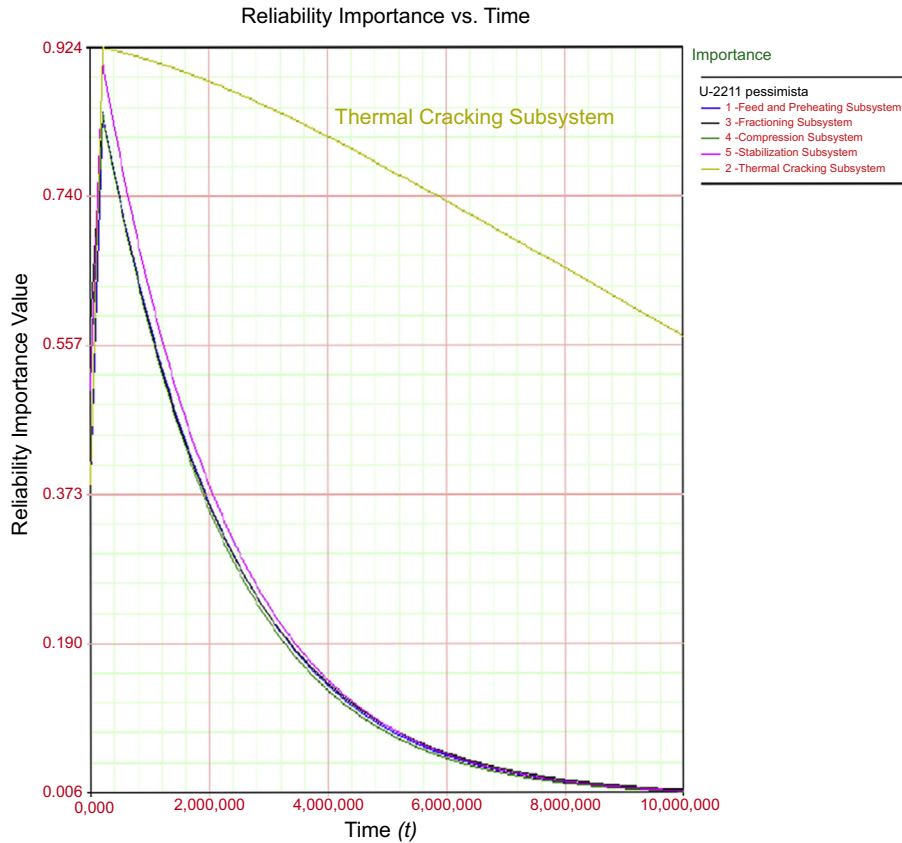
The following equation shows the mathematical relation:

$$\frac{\partial R(\text{System})}{\partial R(\text{Subsystem})} = \text{RI}$$

Despite this relation, some equipment or subsystems may be prioritized because of repair time having an expressive impact on system availability. This means that the availability impact is the most important, despite reliability being highly influential on the system. One specific subsystem or piece of equipment might not be the most critical because of repair time impact. In this case a piece of equipment that has four shutdowns in a specific period of time might not be as critical as another piece of equipment that has only one shutdown. For the second piece of equipment, total loss time is higher than the first. In fact, in most cases it is not possible to reduce repair time. Therefore equipment reliability improvement is the best solution for achieving availability targets. In this case the RI is the best index to show how much reliability improvement the system can accommodate. But as discussed it is necessary also to consider availability. In the thermal cracking system the most critical subsystem is the thermal cracking subsystem for the RI and EC. This implies that in terms of failures and losses that subsystem is the most critical. The RI results are shown in Fig. 4.71. If 1% improvement of the thermal cracking subsystem reliability is achieved, the system will improve 0.926% of reliability. Thus if it is intended to improve system reliability over time the thermal cracking subsystem is the correct subsystem to improve.

Looking at the thermal cracking subsystem, we can see that furnaces A and B are the most critical equipment in terms of reliability, as shown in Fig. 4.72. If there is a 100% improvement of furnace (F-01) reliability, the thermal cracking subsystem reliability will improve 100%. But it is necessary to assess which impact subsystems cause in system availability.

The downing event criticality index (DECI) was also used to assess which equipment causes more shutdowns in the thermal cracking system, and again furnaces A and B are the most critical in terms of



**FIGURE 4.71**

Reliability importance (thermal cracking system).

the number of system shutdowns, as shown in Fig. 4.73. The DECI for both furnaces (F-01 B and F-01 A) are 50.81% and 49.14%, respectively.

Such criticality is confirmed if we look at the percentage of failure, which shows that the percentage of system downtime is related to the critical equipment failures, as shown in Fig. 4.74.

The other index that must be used as a reference to define improvement actions in critical equipment is the availability rank index, and in the thermal cracking system case, as most of the equipment is in series configuration in the RBD, this index will indicate which equipment must be improved to improve system availability, as shown in Table 4.16.

In this way, the equipment to be improved is based on the availability rank from the bottom to top as shown in Table 4.16, because when the system is in series the system availability will be equal to or lower than the lowest availability block (block is in series in the RBD). Thus it is necessary to improve coke formation in furnaces A and B and then corrosion in heat exchanger P-03. Coke formation is not a failure, but a process and operational condition, so new procedures must be

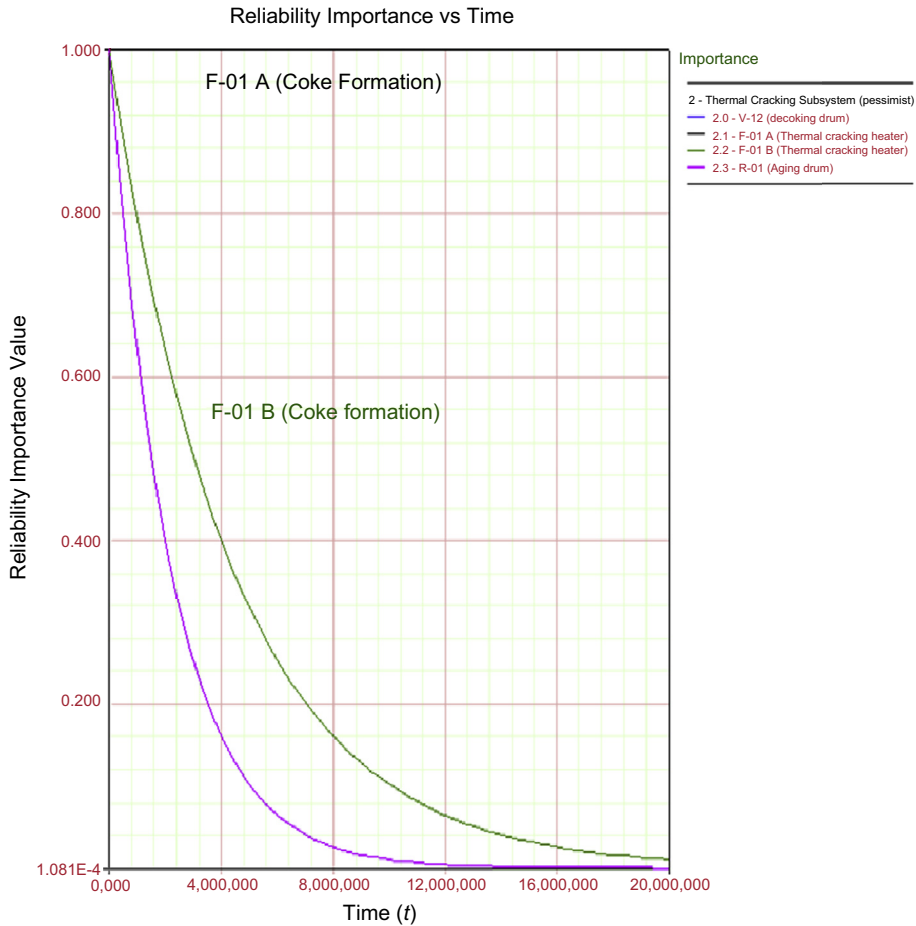
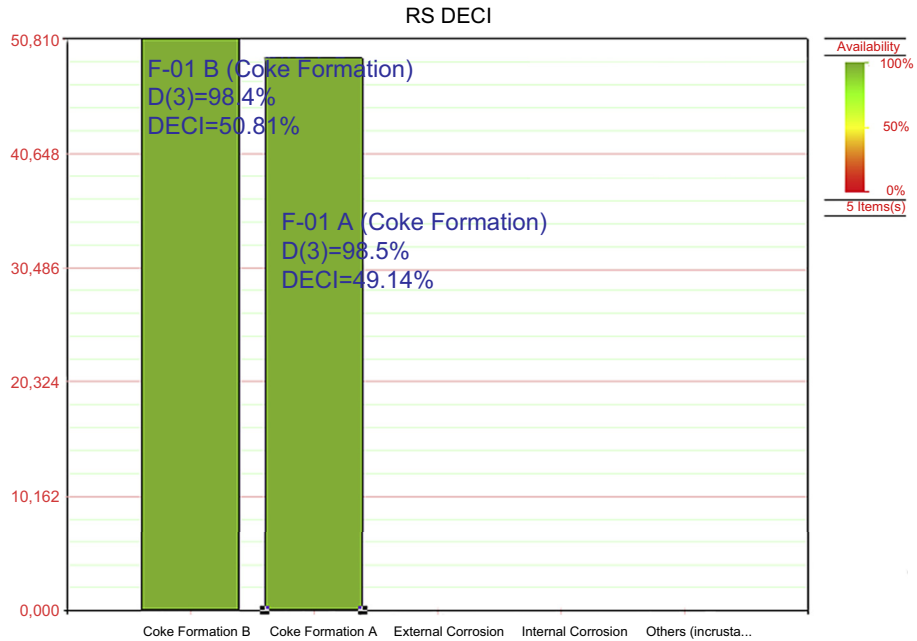


FIGURE 4.72

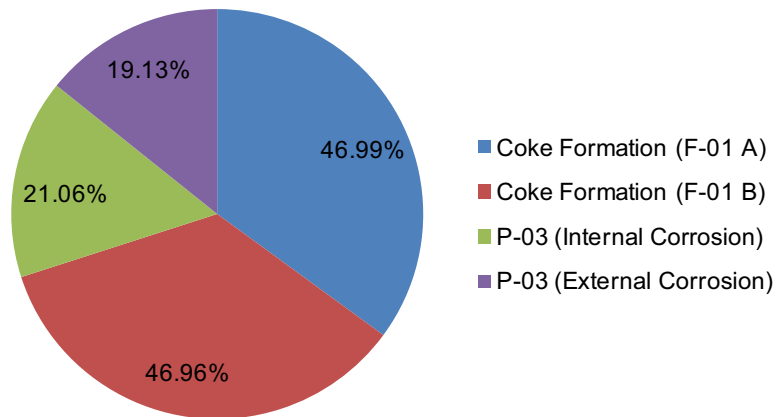
Reliability importance.

considered to reduce unavailability time when decoking furnaces. Because of the furnace decoking impact on system availability, two furnaces were projected to reduce this impact, and in this case when decoking one furnace, only 50% of system production loss will occur. If other procedures to decoke furnaces are adopted, it is possible to reduce system unavailability time. Such procedures include:

- Performing the online Spalling decoking process, the time required to decoke a furnace is 30 hours. In doing so the thermal cracking system will be 98.53% for two furnaces.
- The second option is to decoke the furnace with a pipeline inspection gauge (PIG), and in this case the decoke process lasts 48 hours. In doing so the thermal cracking system with two furnaces will achieve 97.89% availability in 3 years.

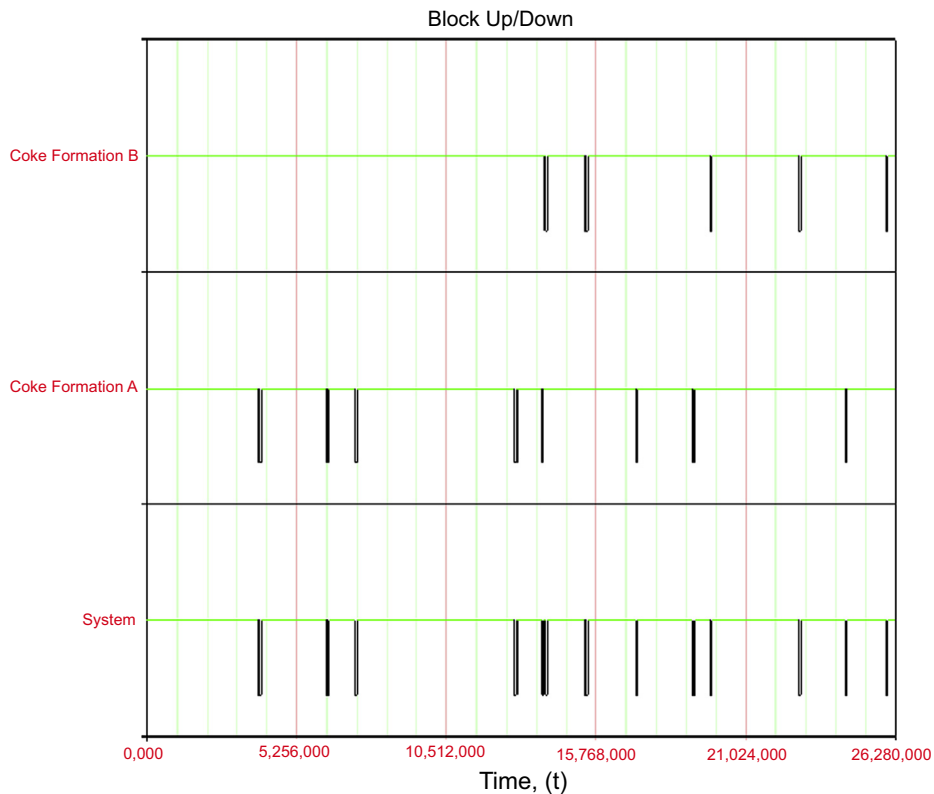


**FIGURE 4.73**  
Downtime event criticality index.



**FIGURE 4.74**  
Percentage failure index (reliability index).

Availability	Ranking
Block names	Availability
Internal corrosion (P-03)	99.39%
External corrosion (P-03)	99.33%
Coke formation B (F-01 B)	98.51%
Coke formation A (F-01 A)	98.51%



**FIGURE 4.75**

System operating and system not operating (thermal cracking subsystem).

Once these two options allow the system to achieve the availability target of 98% in 3 years, an important issue arises. If decoking time is reduced by such procedures, maybe it is possible to operate with only one furnace and achieve the system availability target. Fig. 4.75 shows the Monte Carlo simulation results for F-01 A and F-01 B coke formation over time and the impact on system availability. The first two lines show F-01 A and F-01 B shutdowns caused by coke formation and the third line shows the thermal cracking system shutdown affected by coke formation in both furnaces.

For the online Spalling procedure, if the thermal cracking subsystem operates with only one furnace, the thermal cracking system will achieve 98.28% availability in 3 years. However, if the PIG procedure is adopted to decock the furnace and the thermal cracking system operates with only one furnace, the thermal cracking system will achieve 97.58% availability in 3 years. In doing so it is possible to save around \$3,000,000 by reducing to one furnace in this project.

### **Sensibility Analysis**

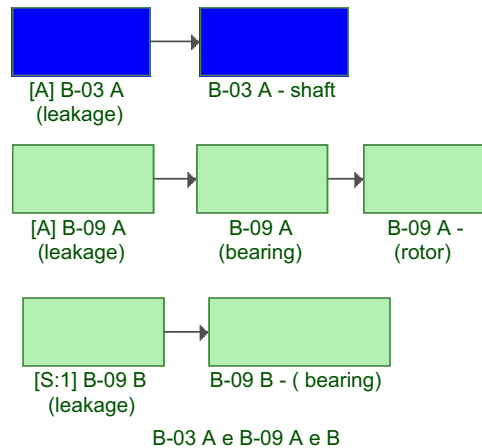
After critical analysis it becomes clear that it is mandatory to implement the improvements in some equipment to achieve the availability target. Moreover, it is necessary to consider some critical events such as energy supply, logistics, and other factors for accomplishing a consistent analysis result. Sensitivity analysis analyzes the system vulnerabilities and feasible possibilities for introducing improvements. Each tested event shows the impact on system availability. In the thermal cracking system case the following will be considered in the sensitivity analysis:

- Stock policy
- Pump redundancy policy

In the first case, if zero stock is adopted as stock policy for all equipment, the system availability will reduce from 98.28% to 88.31% in 3 years. Thus, despite zero stock policy, the minimum stock policy will be applied, and in this case, tubes to replace damaged tubes in furnace F-01 and tubes to heat exchangers P-11 and P-03 will be stocked. In this way, system availability is 98.28% in 3 years. The optimum stock policy simulation results are shown in [Table 4.17](#).

<b>Stock</b>	<b>SA</b>	<b>Items Display</b>	<b>ATRS (hours)</b>	<b>Rejected Items</b>	<b>Emergency Time (hours)</b>
Leak (pump)	0	0.27	414,233	0	0.27
Other pump stocks	0	1.24	649,667	0.02	1.24
Tube (heat exchanger 1)	0	0	0	0	0
Tube (heat exchanger 2)	0	0.005	497,124	0	0.005
Plate (external corrosion tower)	0	0	0	0	0
Plate (internal corrosion tower)	0	0	0	0	0
Tube (heat exchanger incrustation)	0	0	0	0	0
Plate (internal corrosion vase 1)	0	0	0	0	0
Plate (internal corrosion vase 2)	0	0	0	0	0
Tube (internal corrosion P-11)	0.8924	0.27	0	0	0
Electric motor (compressor)	0	0	0	0	0
Electric motor (compressor)	0	0	0	0	0
PE external corrosion reactor 2	0	0	0	0	0
PE internal corrosion reactor	0	0	0	0	0
Tube (coke formation F-01 A)	0.3443	5705	0	0	0
Other furnace stocks	0	0	0	0	0
Tube (internal corrosion P-03)	0.8882	0.285	0	0	0

SA, stock average; ATRS, average time to replace stock.

**FIGURE 4.76**

Reduce standby pumps.

The second sensitivity analysis regards the pump standby policy. In general, such projects adopt one standby pump for all pumps. Therefore, the standby policy was assessed to verify which standby pumps would supply more than one pump. For example, Fig. 4.76 shows two pumps with one standby redundancy.

It was proposed to take out pump B-03 B and use pump B-09 B as a standby for pumps B-09 A and B-03 A. Since fluid flow operation range and type of product on both pumps are operationally similar, it is necessary to perform RBD configuration as shown in Fig. 4.76 and simulate over 3 years the new configuration to check pumps' configuration availability. Thus the availability is 99.33% in 3 years. To achieve 100% availability, minimum reliability requirements were proposed, and in this case minimum reliabilities of 71.09% (B-03 A), 78.68% (B-09 A), and 78.42% (B-09 B) in 3 years with 90% confidence were proposed.

Such analysis was extended for other pumps and \$300,000 was saved by reducing the number of standby pumps.

### Conclusion

RAM analysis performed for the thermal cracking system identified critical equipment and proposed a new procedure for decoking furnaces to achieve the system's availability target. As well as achieving the availability target it was proved that in regard to such procedures, it is not necessary to have two furnaces, and consequently it was possible to make the project more economically attractive by reducing it by \$3,000,000.

Sensitivity analysis was conducted and with an optimum stock level policy it was possible to save money with unnecessary components in stock. Usually there is required stock for all equipment components, which represents at least 10% of the project cost. Finally, sensitivity analysis was proposed to reduce standby pumps and this is able to reduce around \$300,000 of the project cost without any impact on system availability.

### 4.6.6 PARTIAL AVAILABILITY BASED ON SYSTEM AGE: THE DRILL FACILITY SYSTEM CASE STUDY

The main objective of this case study is to propose a methodology for defining the drill facility system availability target for different periods of time over simulation. Nowadays, most software that performs Monte Carlo simulation for system RBDs gives cumulative results and does not show system availability results in interval time. This means that if simulation is performed for 3 years, there are no partial results for availability for the first, second, and third years. In most cases, there are no operational availability results that show how a system performs during a specific period of time. Depending on the situation, it is necessary to define the system availability target for a specific period, and such a value is estimated based on the cumulative availability value. To solve this problem it is proposed to regard system age in simulation. Such a method uses equipment age based on different periods of time that will result in partial availability. This means, for example, that in the case of 2 years of simulation there will be cumulative availability and partial availability results in the first and second years. To illustrate this methodology a drill facility case study, where it is necessary to define the system operational availability during the first and second years to plan inspections, stocks, and purchase policies, is discussed.

#### *Introduction*

Today, many different software packages perform RAM analysis and find operational availability. Such a result is cumulative over simulation time, which means it uses all system downtimes over the simulation period of time to calculate operational availability. Regarding a high-performance system, when direct simulation is carried out, operational availability will be mostly higher achieving targets in cumulative time intervals between zero and final time simulation. However, looking into the partial period of time between zero and the final simulation time, availability per period of time is neither clear nor shown in many simulation cases. For a system with high availability performance in the simulation period of time, partial results are not a problem because such a system achieves the availability target in the cumulative period of time.

In some cases, from a resource planning point of view, it is interesting to preview which operational availability system will be achieved in a specific period of time, and consequently define stock and inspection policies to keep operational availability in the expected target level. This is usual for a system with low operational availability for a long period of time. For example, systems with operational availability targets defined for 1 year are not simulated over 1 year, because most software accumulates downtimes and final availability results will not show what happens over the years. In this case it is necessary to use age over time and use a period of 1 year for simulating the following years. Regarding system age, simulation is always conducted for 1 year. For example, in order to predict the operational availability in the second year of life cycle, the system is simulated for 1 year period with 1 year aged. In this way, each year will have its own operational availability and it will be possible to define stock and inspection policies over the years. In many cases, professionals define availability targets by average over the years, and to reduce vulnerability it is necessary to overestimate stock and preventive maintenance resources.

#### *Partial Availability*

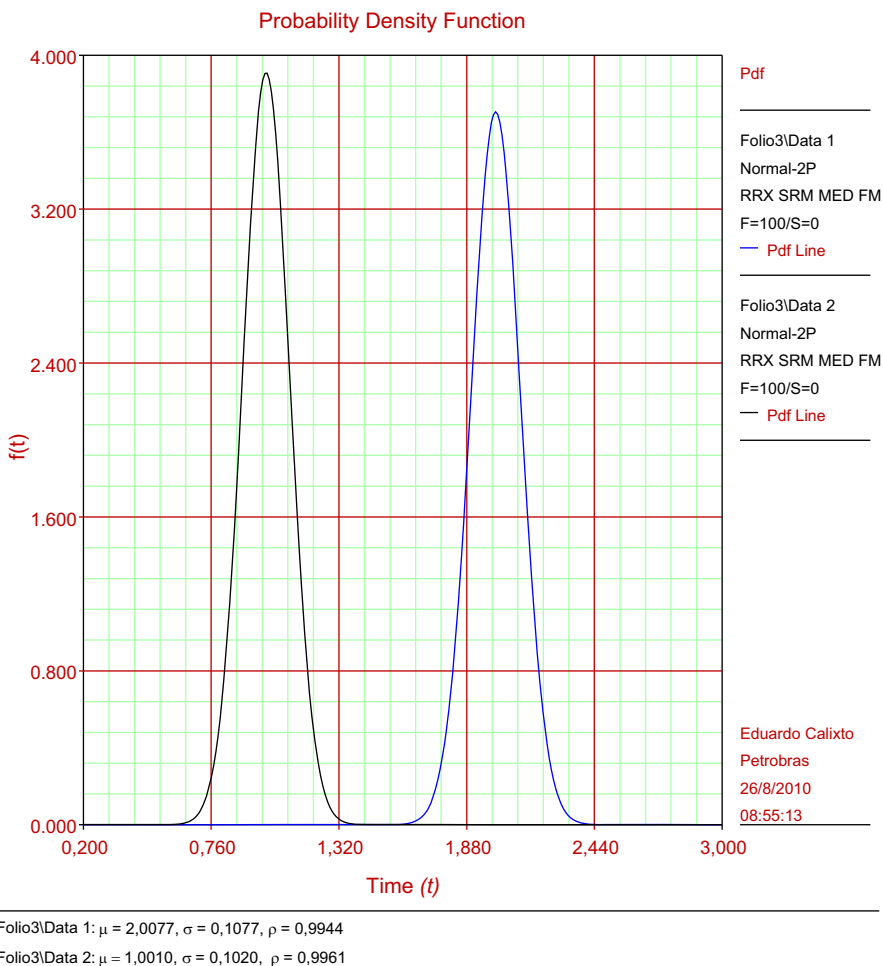
The Monte Carlo simulation in RAM analysis has the main objective of defining system operational availability and critical equipment to support decisions for implementing improvement actions when



necessary. Such operational availability results are cumulative over simulation time, and to obtain partial operational values two approaches are used:

- System age approach discount time on PDF parameters;
- System age approach for time.

In the first case it is necessary to modify the scale parameter but not to modify PDF characteristics. For example, to age equipment 1 year, the value is discounted in the scale parameter, and if it is necessary to postpone, 1 year is added to the value in the scale parameter. This is easy to realize if you look for a PDF with a Gaussian shape like normal, lognormal, Gumbel, logistic, and loglogistic (scale parameter is  $\mu$ ). Fig. 4.77 shows the normal PDF aged 1 year to simulate the second year of such



**FIGURE 4.77**

PDF parameters discounted time.

equipment life and to find out operational availability in this period of time. The second PDF in Fig. 4.77 is the original PDF and the first one is the aged PDF. The equipment operational availability is 100% in 1 year because there is no failure (normal PDF:  $\mu = 2$ ,  $\sigma = 0.1$ ). In addition, to find out the equipment operational availability in the second operational year, it is discounted for 1 year in the position parameter ( $\mu = 2 \rightarrow \mu = 1$ ). Monte Carlo simulation is conducted for 1 year of simulation time.

When the scale parameter is discounted for 1 year, the next failure will occur earlier than expected. Thus it is only possible when the value of the scale parameter discounted by a specific time is higher than the period of simulation time.

For other PDFs, such limitations are similar. For the Weibull 3P, for example, it is necessary to discount time to the position parameter. For example, considering the Weibull position parameter value is 5 years and it's intended to simulate the second year of life cycle, it's necessary to discount of 1 year of position parameter and perform the simulation for one year (1 year simulation time).

Such limitation of discounted time happens because the discounted time approach works only for the first failure in the period of simulation, and the following failure will occur earlier than expected. In Weibull 3P, for example, the second failure will not be postponed by position parameters' values. In addition, if after repairs equipment is considered as-good-as-new, such earlier failure is not expected to happen. In as-bad-as-old it is acceptable that failure occurs in a short period of time after repair. Fig. 4.78 shows an example of Monte Carlo simulation to describe equipment behavior in the second operational year using 1 year discounted in the PDF parameter ( $\gamma$ ).

The Weibull drawwork PDF parameter is ( $\beta = 2.01$ ,  $\eta = 0.29$ ,  $\gamma = 0.86$ ). For position parameters discounted in 1 year, to simulate the second year the new PDF parameters will be ( $\beta = 2.01$ ,  $\eta = 0.29$ ,  $\gamma = 0$ ). Thus when the position parameter is discounted and the value is not less than the simulation period of time, the second failure will not be considered the period of time of 0.86 years as shown Fig. 4.78. Thus the MTBF is 3.625, which would be 7533 hours ( $\gamma = 0.86$ ).

The second possibility regards system age to find out partial operational availability by run simulation and uses only downtimes that occur in a specific period of time to calculate such partial operational availability.

The operational availability must be defined as total time the system is available to operate by total nominal time, as shown in the following equation:

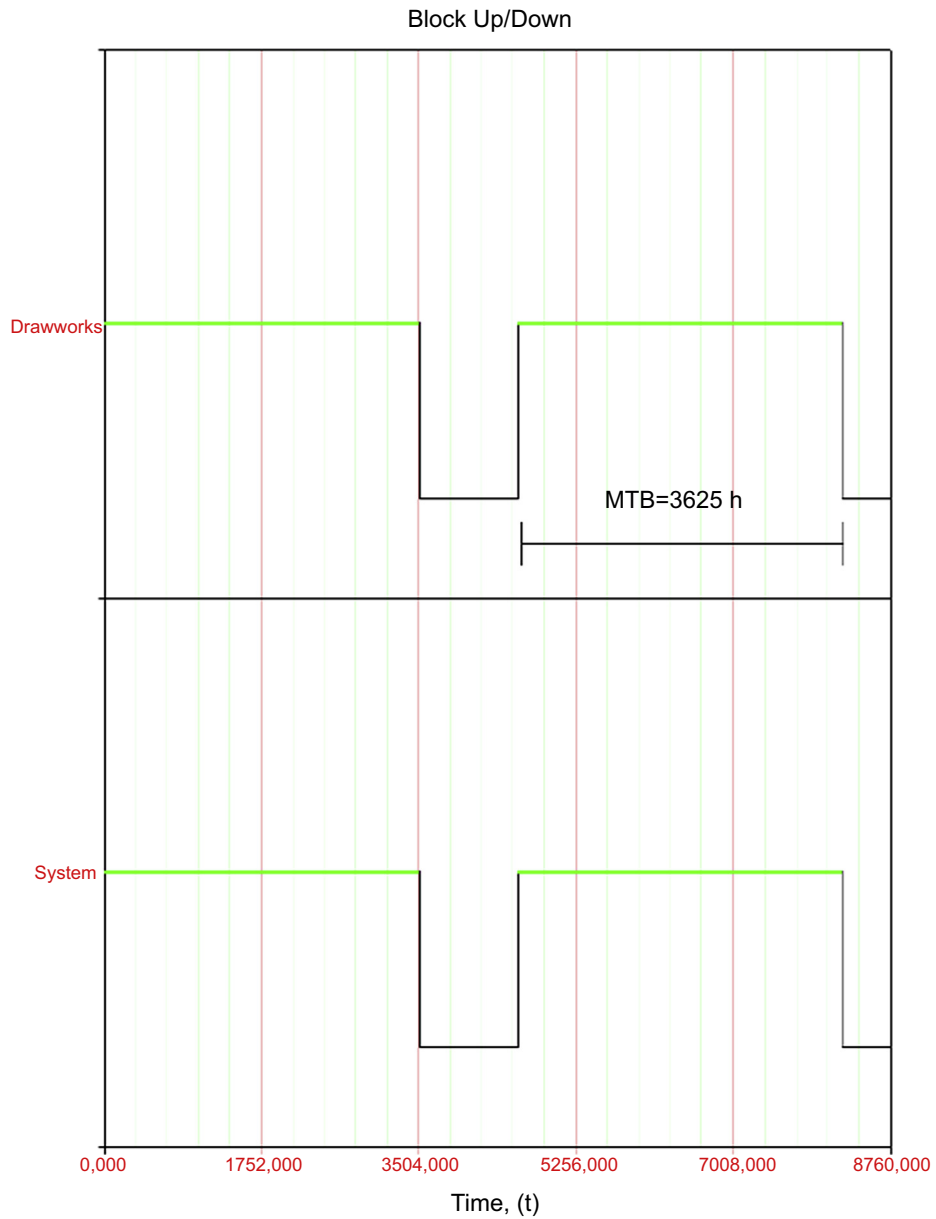
$$D(t) = \frac{\sum_{i=1}^n t_i}{\sum_{i=1}^n T_i}$$

where  $t_i$  = real time when system is available and  $T_i$  = nominal time when the system must be available.

As discussed, the Monte Carlo simulation mostly shows accumulated operational availability, but to know partial availability in different periods of time it is necessary to define such periods of time over the total period of time and then include downtimes in each period of time. An example of time line  $T(0,n)$  is shown in Fig. 4.79.

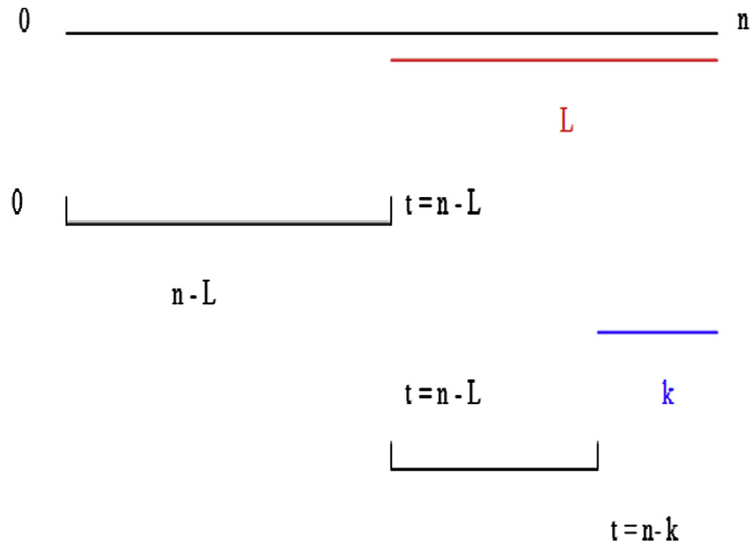
The equation that represents operational availability along  $T(0,n)$  is:

$$D(t) = \frac{\sum_{i=1}^{n-L} t_i}{\sum_{i=1}^{n-L} T_i} + \frac{\sum_{i=n-L}^{n-k} t_i}{\sum_{i=n-L}^{n-k} T_i} + \dots + \frac{\sum_{i=n-k}^n t_i}{\sum_{i=n-k}^n T_i} = \frac{\sum_{i=1}^n t_i}{\sum_{i=1}^n T_i}$$



**FIGURE 4.78**

Drawwork (second year simulated).



**FIGURE 4.79**  
Timeline  $T(0, n)$ .

And regarding three different intervals of time, the operational availability over each period of time is as follows:

Period I:

$$D(0 \leq t \leq n - L) = \frac{\sum_{i=1}^{n-L} t_i}{\sum_{i=1}^{n-L} T_i}$$

Period II:

$$D(n - L \leq t \leq n - k) = \frac{\sum_{i=n-L}^{n-k} t_i}{\sum_{i=n-L}^{n-k} T_i}$$

Period III:

$$D(n - k \leq t \leq n) = \frac{\sum_{i=n-k}^n t_i}{\sum_{i=n-k}^n T_i}$$

where  $t_i$  = real time when system is available and  $T_i$  = nominal time when the system must be available.

It is possible to consider as many intervals of time as necessary depending on the requirements and available data. In Monte Carlo simulation it is necessary to define the start age of the system and use periods of simulation, which in this case is 1 year. Thus the starting age for the first year is zero, for the second is 1 year, and for the third is 2 years.

Equipment	Component	Time to Failure (years)			
		Distribution	Parameters		
Air compressor	Compressor	Weibull	$\beta$ 0.67	$\eta$ 1.69	$\gamma$ 0.74
	Electric motor	Exponential		MTTF 0.08	

MTTF, mean time to failure.

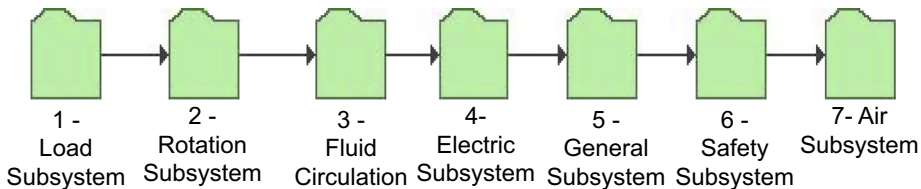
**Partial Availability Case Study**

Modeling and Simulation

To illustrate the partial availability approach this method will be applied in the drill facility case study where the system availability target is 90% annually. In addition, it is necessary to define the stock policy and maintenance policy for the next 5 years based on RAM analysis results. The drill facility does not achieve high performance for over 1 year, and some equipment failures in the first year and others in the second year. Thus two simulations will be conducted for equipment age to define availability and critical equipment for the first and second year. Before modeling the RBD, equipment life cycle analysis was performed, and one of the most critical pieces of equipment is the compressor in the air compressor subsystem. Table 4.18 shows an example of a compressor failure PDF.

After the life cycle analysis was conducted the modeling phase for the six subsystems of the drill facility system was performed, as shown in Fig. 4.80.

Performing simulation for the first year, the system achieved 85.44% operational availability in 1 year and 23 failures are expected. The most critical equipment in terms of reliability are the electrical and air subsystems, defined by the RI index. This index defines which subsystem or equipment most influences system reliability and allows specialists to know how much system reliability will improve if improvements in reliability subsystems or equipment are done. While important the RI is not enough to support system decisions for improvement to achieve availability or efficiency targets.



**FIGURE 4.80**

Drill facility subsystem.

The RI index is defined as the partial derivation of the system related to the subsystem (or equipment). The following equation shows the mathematical relation:

$$\frac{\partial R(\text{System})}{\partial R(\text{Subsystem})} = \text{RI}$$

Fig. 4.81 shows the subsystem’s RI index over time.

Despite the impact on system reliability measures by the RI index, when systems have series configurations on RBD, availability measures by availability rank are also important to check each equipment impact on the system’s availability. In this way, the compressor is the availability bottleneck because it has the lowest availability of the drill facility system. The availability rank index is shown in Table 4.19.

As the compressor is the most critical piece of equipment, a recommendation was proposed to analyze the reliability of the other compressors to find the one with the highest reliability to define

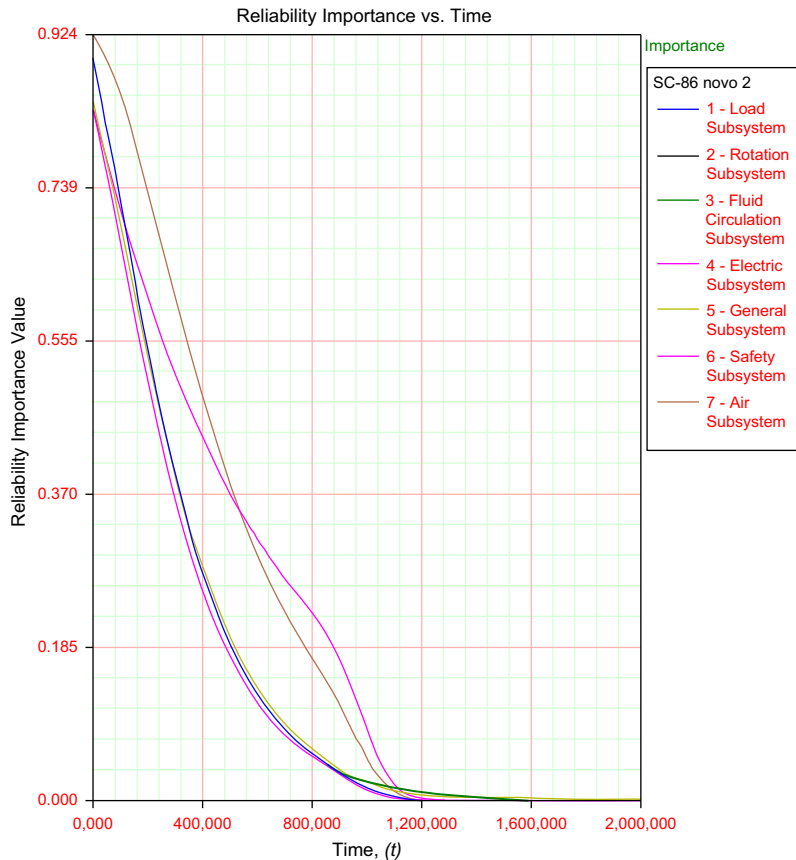


FIGURE 4.81

Reliability importance index (year 1).

**Table 4.19 Availability Rank (Year 1)**

Partial Operational Availability (First Year)	
Crown block	96.93%
Diesel pump	96.59%
Compressor	95.38%

**Table 4.20 Availability Rank Index (Year 2)**

Partial Operational Availability (Second Year)	
Mud pump	96.81%
Transmission box	86.86%
Compressor	85.48%

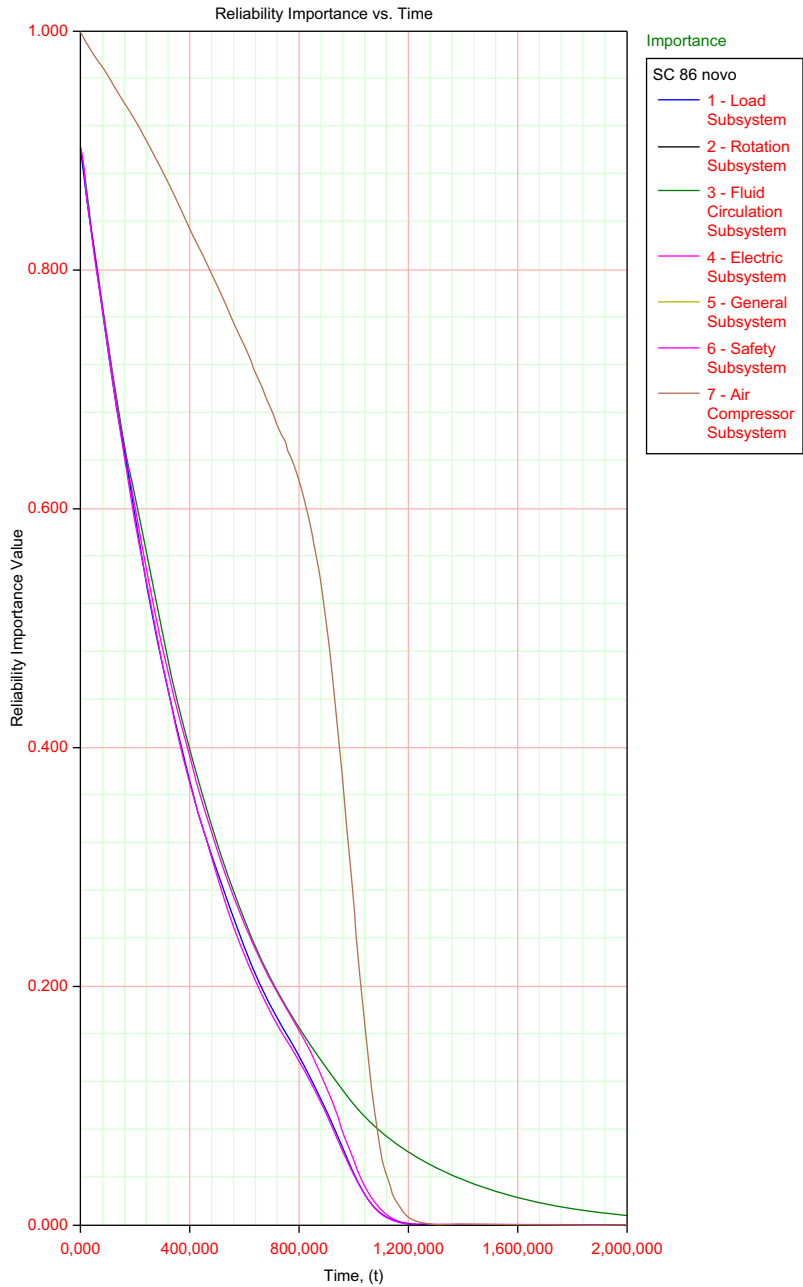
higher reliability requirements for compressor suppliers. The compressor is expected to achieve at least 100% reliability in 2 years, so the drill facility system will achieve 88.58% availability in 1 year. The following improvement action proposed is to define the reliability target for the diesel pump to require this target for the pump supplier. Another option is to have the standby pump achieve 100% availability in at least 1 year. For those additional recommendations the drill facility system will achieve 91.87% in 1 year, a little higher than the availability target of 90% in 1 year.

Applying partial availability methods the drill facility system availability in the second year is 68.84% if no improvement in the compressor is done, although for high compressor reliability the drill facility system will achieve 81.95% in the second year. In the second year, other equipment is more critical in terms of impact on system availability. [Table 4.20](#) shows the availability rank index for the second operational year.

For reliability impact the air compressor system is the most critical, as shown in [Fig. 4.82](#) for the second year. Despite improvements in the compressor, some other improvements such as in the transmission box (chain) are required, as shown in [Table 4.20](#), to achieve the operational availability target (90% in 1 year). Thus reliability requirements must be defined for such equipment, but in this case, wear is normal in such equipment, and even if it is possible to have 100% reliability for such equipment, it is advisable to perform inspections and planned maintenance whenever possible to keep the transmission box available as long as possible in the second year. Thus if the transmission box is 100% available in the second year, the drill facility system will achieve 91.25% availability in the second year.

### Stock Policy

Stock level is an important issue that must be considered because it can affect system availability when repair is delayed more than necessary because a component is not in stock and it is necessary to purchase one. In such cases the system is unavailable, and to avoid this the stock policy must be well defined.



**FIGURE 4.82**  
Reliability importance index (year 2).



<b>Spare Part Pool Summary</b>					
<b>Equipment</b>	<b>ASL</b>	<b>Items Dispensed</b>	<b>ATTD</b>	<b>Items Rejected</b>	<b>Emergency</b>
Electric motor	1	0	0	0	0
Compressor	1	0	0	0	0
Ezy torque	0.5907	1.971	0	0	0
Diesel motor	1	0	0	0	0
Diesel pump	1	0	0	0	0
Hydraulic key	0.9638	0.078	0	0	0
Regulation valve	0.9364	0.145	0	0	0
Plug	0.1636	15.339	0	0	0
Transformers	0.7287	0.981	0	0	0
Cable	0.597	1.92	0	0	0
Mud pump	0.2788	7.76	0	0	0
Torque converter	0.8172	0.555	0	0	0
Drawn motor	1	0	0	0	0
Drawn	0.9647	0.076	0	0	0
Drawn cable	0.8615	0.383	0	0	0
Swivel	0.9547	0.099	0	0	0

ASL, average stock level; ATTD, average time to deliver.

In the drill facility system, even though improvement is implemented, other equipment would impact system availability if zero stock was adopted as the stock policy for all equipment because of increased shutdown time that is related with equipment purchase time. Therefore the drill facility system availability will be reduced from 91.87% to 11.93% in the first year. Such an impact occurs because of delays in the purchase process and delivery time difficulty, which would be 6 months. Based on equipment PDFs and simulation results the appropriate stock level of equipment is shown in [Table 4.21](#).

Looking at [Table 4.21](#) from left to right, the first column lists the equipment that requires at least one group of components in stock. Some components (eg, electric motor, compressor, diesel motor, diesel pump, cable, plug, and mud pump) are the most critical, and if there is no stock of such components, it will have high impact on availability. For other components (eg, Ezy torque, hydraulic key, regulation valve, torque converter, drawn motor, drawn, drawn cable, and swivel) it is advisable to have these in stock because they cause marginal impact in system availability. Despite improvement actions in the compressor and diesel pump, it is advisable to have at least one group of these components in stock. This is correct because even if the supplier is sure of 100% reliability for such equipment, it is first necessary to verify such reliability. In some cases, equipment degradation is not a problem of quality operation and maintenance and these issues must be taken into consideration also.

In the second column the ASL for each piece of equipment is given and values vary from zero to 1.

<b>Spare Part Pool Summary</b>					
<b>Equipment</b>	<b>ASL</b>	<b>Items Dispensed</b>	<b>ATTD</b>	<b>Items Rejected</b>	<b>Emergency</b>
Plug	0.1783	13.814	0	0	0
Transformer	0.7582	0.815	0	0	0
Generator motor	0.7855	0.709	0	0	0
Cable	0.6227	1.703	0	0	0
Mud pump	0.3022	6.925	0	0	0
Traveling block	0.8704	0.333	0	0	0
Swivel	0.9108	0.213	0	0	0

ASL, average stock level; ATTD, average time to deliver.

The third column lists the components dispensed, that is, the main components required because of equipment failure. When the value is zero the equipment did not fail, such as the compressor and diesel pump.

In the fourth column the average time to deliver (ATTD) is given, and when the value is zero there is no delay for delivery because the component was in stock. In the fifth column the rejected components are listed, this means items that are required from stock and are not available. When the value is zero this means no components were rejected when required in stock.

In the sixth column the emergency time is given, that is, the time required to replace an equipment component when stock is zero. In this case for all equipment the value is zero because they all have one component in stock; and when equipment fails and the component is out of stock, a component is replaced.

For the second year, the stock level changes for some equipment because there is equipment that fails annually and other equipment has more of a chance of failing in the second year. If zero stock policy is applied in the second year the availability reduces from 91.25% to 9.52%. Thus it is necessary to implement the optimum stock policy in the second year as performed for the first year, as shown in [Table 4.22](#).

In the second year, plugs and cables still require stock level because they fail annually, and the new equipment is mud pumps, which require one group of components in stock.

#### A General Renovation Process—Degradation in Stock

In repairable equipment, whenever repair is performed the effect of the activity on equipment reliability must be considered. In many cases, specialists are optimists and consider that equipment is as-good-as-new. When that does not happen, only part of equipment reliability is reestablished by maintenance. In this way, when simulating such equipment availability over time for corrective maintenance it is necessary to use reliability degradation because of maintenance effects.

The Kijima models I and II, proposed by Kijima and Sumita in 1986, are known as general renovation processes based on component virtual life. Such methods are used to measure how much is reduced in component age when some repair is performed and can be:

- Age reestablishment based in last intervention (Kijima I);
- Age reestablishment based in all interventions (Kijima II).

In the first case the Kijima model I regards that reestablishment component age occurs only for the last failure before maintenance is performed. In this way, such a model regards that  $i$ —the repair—does not remove all reliability loss until  $i - 1$ —the failure. Therefore if there is time between failures the component age has a proportional effect for a long time, as represented by the equation:

$$x_i = x_{i-1} + q \cdot h_i = qt_i$$

where  $h_i$  = time between an  $(i - 1)$ th and an  $i$ th failure,  $q$  = restoration factor,  $x_i$  = age in time  $i$ , and  $x_{i-1}$  = age in time  $i - 1$ .

In the second case the Kijima model II assumes that reestablishment component age occurs for all failures over component life since the first one. This model assumes that the  $i$ th repair removes all reliability loss until the  $i$ th failure. Thus the component age has a proportional effect for a long time and is represented by:

$$x_i = q(h_i + x_{i-1}) = q(q^{i-1}h_1 + q^{i-2}h_2 + \dots + h_i)_i$$

An example Kijima model was applied to assess the effect of stock deterioration of a diesel pump component. In fact, such degradation is similar to the effect of an as-bad-as-old repair, because thanks to poor stock management, such pumps have their components in stock in an as-bad-as-old condition when they are required to replace a failed component. Thus for Kijima model II, and  $q = 0.01$ , the pump's availability reduces from 99.72% to 50.39% in 1 year. Fig. 4.83 shows pump operation over 1 year taken in failure times for as-good-as-new after corrective maintenance.

As shown in Fig. 4.83, despite eight failures over 1 year the repair was as good as new and reliability was totally reestablished after repair. Thus the time between failures is constant over time. Unfortunately, because of poor stock conditions, the pump in stock is as-bad-as-old when it is used to replace the failed one. Fig. 4.84 shows the effect of degradation.

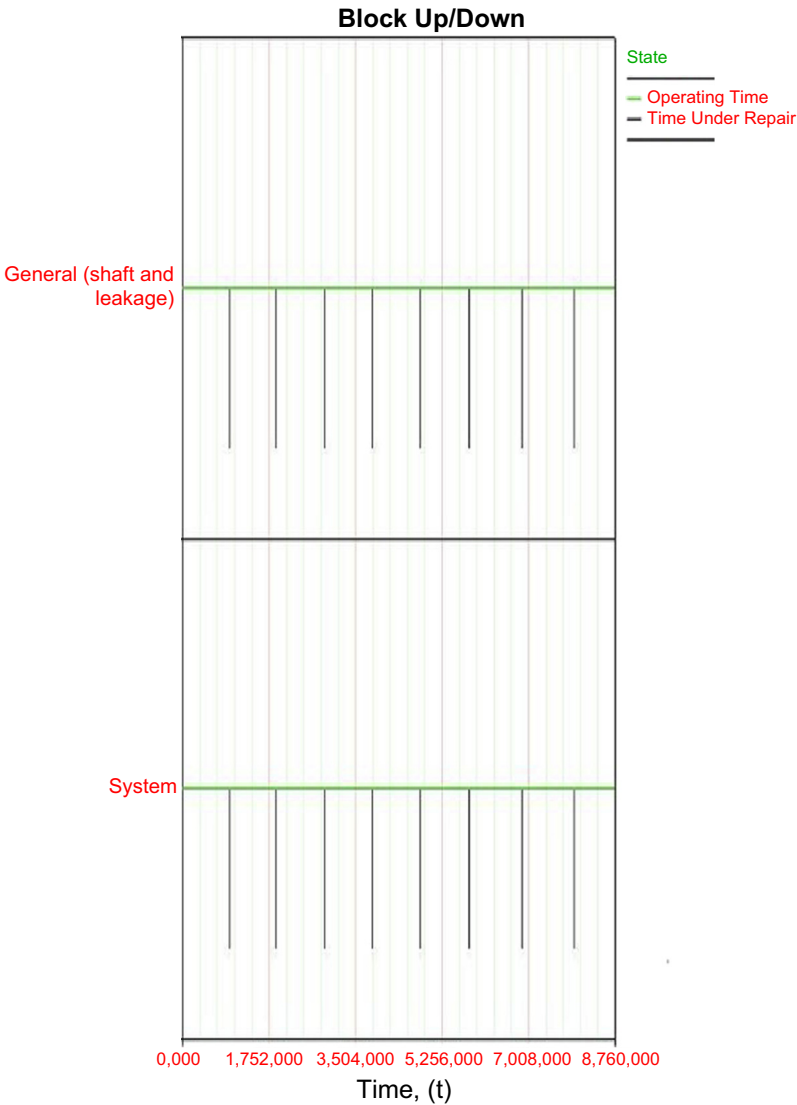
### Inspection Based on Reliability Growth

The reliability growth approach is applied to product development and support decisions for achieving reliability targets after improvements have been implemented (Crow, 2008).

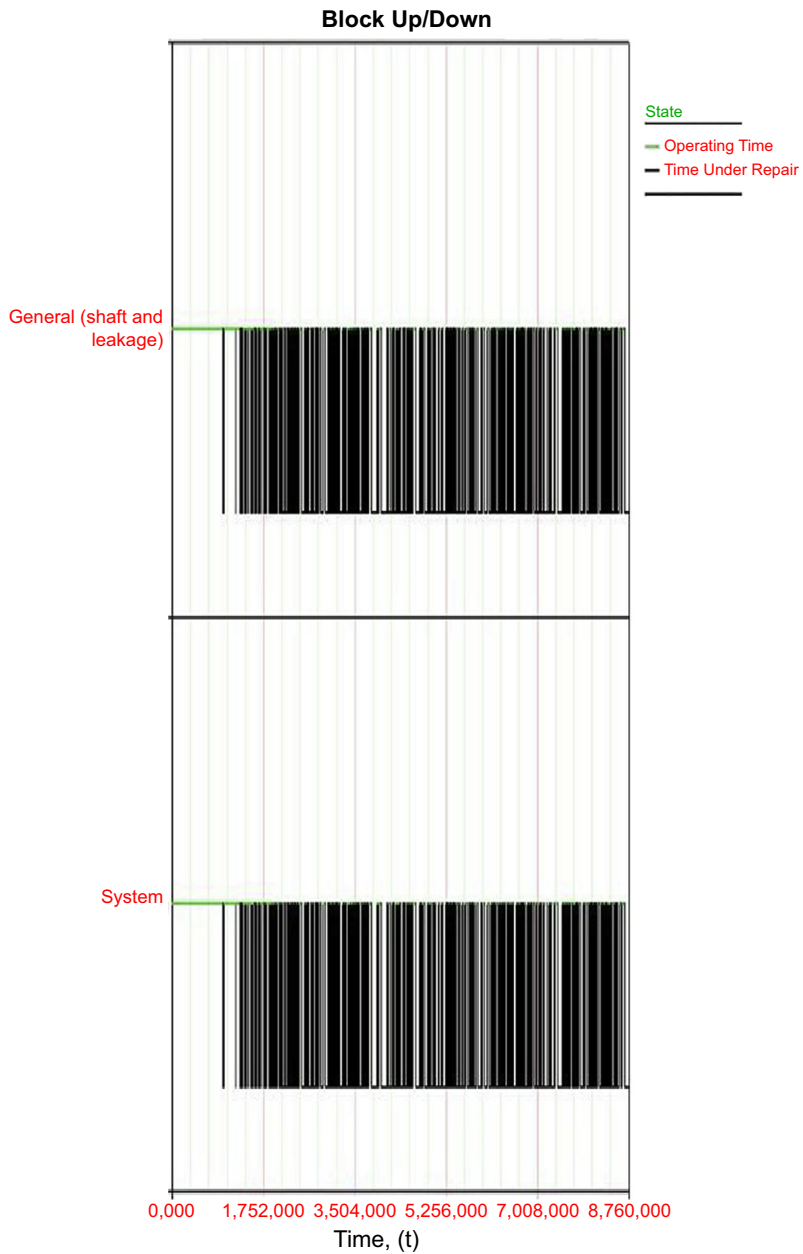
Various mathematical models may be applied in reliability growth analysis (RGA) depending on how the test is conducted:

- Duane
- Crow-AMSAA
- Crow extended
- Lloyd–Lipow
- Gompertz
- Logistic
- Power law

The reliability growth-based inspection (RGBI) method uses power law analysis methodology to estimate future inspections, which is also applied to assess repairable systems (equipment). Thus for complete data that includes repairs, the nonhomogeneous Poisson process is applied, as shown in Eq. [1].



**FIGURE 4.83**  
Pump operation (as-good-as-new).



**FIGURE 4.84**

Pump operation (as-bad-as-old).

Eq. [1]

$$E[N(T)] = \int_0^T p(t)dt$$

The expected cumulative number of failures can be described also by Eq. [2].

Eq. [2]

$$E(N(t)) = \lambda T^\beta$$

To determine the inspection time it is necessary to use the cumulative number of failure functions and, based on equipment failure data, to define the following cumulative failure number. Based on this number, it is necessary to reduce from this the time for the inspection activity.

For example, applying this methodology to the drilling diesel motor it is possible to predict when the next failure will occur, and if reducing this time by the time required to perform the inspection we have the inspection start time. The cumulative number of failures is 10. Therefore substituting the expected accumulative number of failures and using the power law function parameters ( $\lambda = 1.15$  and  $\beta = 1.02$ ) in Eq. [1], the next failure will be expected to occur in 8.32 years, as shown in Eq. [3].

Eq. [3]

$$E(N(t)) = \lambda T^\beta$$

$$T = \left( \frac{E(N(t))}{\lambda} \right)^{\frac{1}{\beta}}$$

$$T = \left( \frac{10}{1.15} \right)^{\frac{1}{1.02}} = 8.32$$

The same approach is used to define the following failure using Eq. [3], in which 11 is used as the expected accumulated number of failures, as shown in Eq. [4].

Eq. [4]

$$E(N(t)) = \lambda T^\beta$$

$$T = \left( \frac{E(N(t))}{\lambda} \right)^{\frac{1}{\beta}}$$

$$T = \left( \frac{11}{1.15} \right)^{\frac{1}{1.02}} = 9.15$$

In Eq. [5], the expected number of failures used is 12.

Eq. [5]

$$E(N(t)) = \lambda T^\beta$$

$$T = \left( \frac{E(N(t))}{\lambda} \right)^{\frac{1}{\beta}}$$

$$T = \left( \frac{12}{1.15} \right)^{\frac{1}{1.02}} = 9.96$$

After defining the expected time of the next failure it is possible to define the appropriate inspection period of time. If we consider 1 month (0.083 year) as an adequate time to perform inspection the following inspection time after the 9th, 10th, and 11th failure will be:

- First inspection: 8.23 years ( $8.32 - 0.083$ );
- Second inspection: 9.07 years ( $9.15 - 0.083$ );
- Third inspection: 9.87 years ( $8.32 - 0.083$ ).

The remarkable point when applying reliability growth methodology is to predict future failures regarding degradation on equipment over time. In addition, in the RGBI method, whenever new failures occur it is possible to update the model and get more accurate values of the cumulative expected number of failures.

The example of cumulative failure plotted against time for a diesel motor is presented in Fig. 4.85, using cumulative failure function parameters  $\beta = 1.02$  and  $\lambda = 1.15$ . Based on such analysis it is

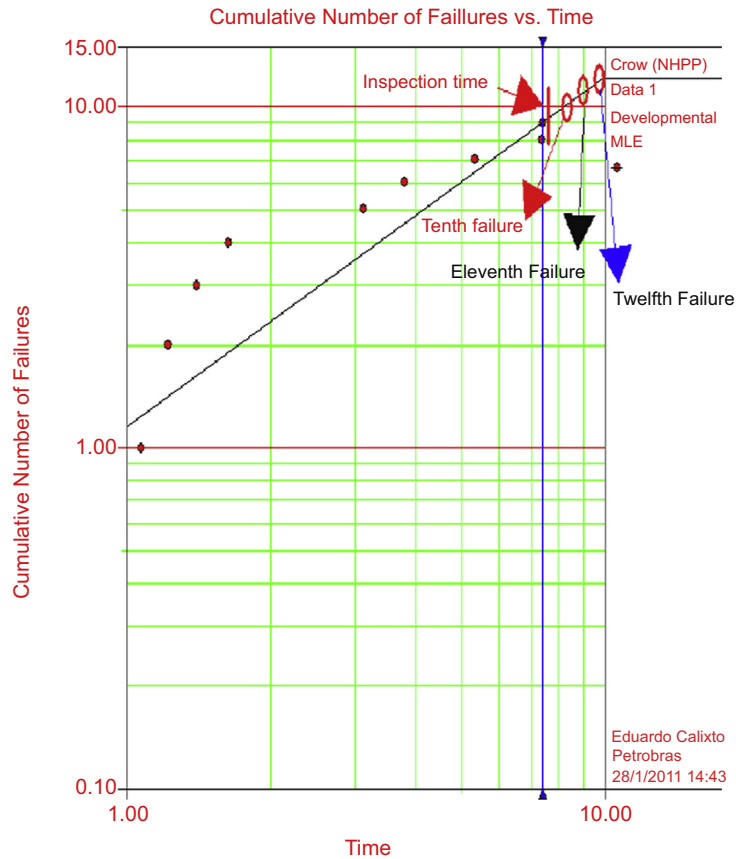


FIGURE 4.85

Inspection based on reliability growth.

<b>Inspection Times (year)</b>			
<b>Equipment</b>	<b>1st Inspection</b>	<b>2nd Inspection</b>	<b>3rd Inspection</b>
Compressor	0.36	0.81	1.25
Diesel motor	0.84	1.67	2.48
Crown block	1.40	1.47	1.53
Transmission box	1.36	1.42	1.47

possible to graphically observe that the next failures (10th, 11th, and 12th) will occur in 8.32, 9.15, and 9.6 years, respectively. This means 0.92, 1.75, and 2.56 years after the last failure (7.4 years).

Despite its simplicity, RGBI analysis requires the power law parameters for the cumulative expected number of failures. Such parameters can be estimated by the maximum likelihood method or by using software. In doing so, whenever possible it is best to use software to directly plot the expected number of failure graphs. In this case, it is possible to update historical data with new data and plot the expected future failures directly on the graph.

Applying this methodology for other drill facility equipment it is possible to define inspection periods of time, and depending on inspection results preventive maintenance may be planned to anticipate equipment failure.

Table 4.23 shows the inspection policy defined for the compressor, diesel motor, crown block, and transmission box. Despite the RGBI defining an exact time for inspection, additional information must be considered such as logistic time. Such time must be discounted in inspection time, and the best solution is to define a range of time to conduct inspections on equipment. In the drill facility system, equipment is being used 1 month (0.083) to be discounted for predicted failure time. Thus inspection time is predicted failure time less 1 month. In the case of a diesel motor, for example, the first, second, and third inspection time will be 0.92, 1.75, and 2.56 years.

### **Conclusions**

The partial availability methodology has demonstrated how to perform RAM analysis for partial periods of time for the system that does not have high performance for long periods of time. In this way it is possible to assess system performance over time, but in each intended period of time it provides data to make better decisions about stock and inspection policies.

In this way, based on partial availability methodology, it is clear which the critical equipment is in the first and second year and it is possible to make better decisions on the correct time. The degradation in stock was considered in this case study, and it is a powerful tool for assessing poor warehouse procedures and management in system availability.

In addition, RGBI was conducted and highlighted as a tool for planning inspections for equipment degradation over time.

The partial availability method would be input in some software to make analysis easier, which is very important to analyze many system performances by each defined period of time.



In partial availability methodology it is important to know which equipment will be aged for a period of time and which equipment will not. For example, when using 1 year as a reference, equipment that fails each year will not be aged. Thus the third and fourth years will be considered similar to the first and second years in terms of system behavior. Failure and repair data will be updated over time and new PDFs used for future analysis.

#### 4.6.7 HIGH-PERFORMANCE SYSTEM REQUIRES IMPROVEMENTS? THE COMPRESSOR'S OPTIMUM REPLACEMENT TIME CASE STUDY

##### *Failure and Repair Data Analysis*

In life cycle analysis, regarding historical failure data, operational plants have the advantage of having more realistic data when compared to plants in the project phase, which in RAM analysis, failure and repair data comes from similar plants. Thus looking at the failure and repair equipment files it was possible to collect data and perform life cycle analysis in statistic software (Weibull++ 7 Reliasoft) to define PDF parameters for each failure mode in this case study.

To ensure the accurate representation of such data, maintenance professionals with knowledge of such systems (fluid catalytic cracking, FCC) took part in this stage. FCC plants convert the high-boiling, high-molecular weight hydrocarbon fractions of petroleum crude oils to more valuable gasoline, olefinic gases, and other products.

A critical equipment analysis of the causes of system unavailability and respective critical failure modes was performed, standardizing all equipment failure modes responsible for most of the impact in the respective subsystems. The example in Fig. 4.86 shows the compressor PDF parameters.

In the same way the failure and repair data of each subsystem's equipment was defined and included in the model. In some cases, there was no historical failure data available, motivating the introduction of a qualitative analysis among maintenance technicians and engineers. In these specific cases, the failure and repair PDFs were defined based on specialist opinion about the failure and repair time behavior over time.

##### *Modeling*

Before performing Monte Carlo simulation, it is necessary to create an RBD. In this way, it is necessary to be familiar with the production flowsheet details that influence losses in productivity. Consequently, some statements and definitions for process limitations are necessary. Firstly, in system level, some critical subsystems, such as warming, conversion, cold area, diethylamine, and cleaning, were unavailable, making the fluid catalytic cracking system unavailable. Additionally, some states and assumptions to enable the proper system model and simulation are necessary such as:

- The availability target is 98% in 5 years.
- The facility supply had 100% availability in 5 years.
- The total production per day was 55 m<sup>3</sup>.

The fluid catalytic cracking system RBD is shown in Fig. 4.87.

##### Warming Subsystem

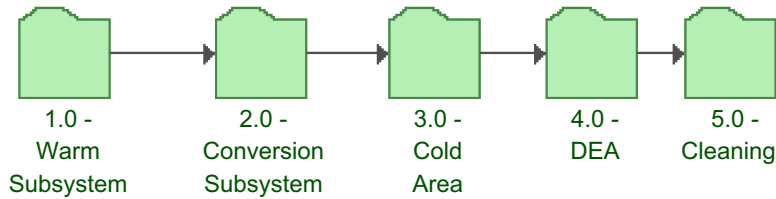
The purpose of this subsystem is heating product feed to achieve process temperature before going to the conversion subsystem. The warming subsystem RBD assumptions are:

- If P-02-03-04 shut down, the warming subsystem will be unavailable.
- If pumps EP-03 A and B are unavailable during the same period of time, the warming subsystem will be unavailable.
- If furnace F-01 shuts down, the warming subsystem will be unavailable.

TAG	Failure Mode	Failure Time (Years)			Repair Time (hour)			
		PDF	Parameters		PDF	Parameters		
EC-301 A	Turbine Bearing	Gumbel	$\mu$	$\partial$	Lognormal	$\mu$	$\partial$	
			4.5	2.04		3.08	0.64	
	Gas Valve 1	Exponential	$\lambda$	$\gamma$	Normal	$\mu$	$\partial$	
			0.5426	0.0946		47.6	40.8	
EC-301 B	Gas valve 2	Weibull	$\beta$	$\eta$	$\gamma$	Normal	$\mu$	$\partial$
			0.5418	1.2061	0.6185		36.4	20.94
EC-301 B	Seal leakage	Gumbel	$\mu$	$\partial$	Weibull	$\beta$	$\eta$	$\gamma$
			4.97	0.24		0.77	4.23	2.36
	Gas valve 1	Weibull	$\beta$	$\eta$	$\gamma$	Lognormal	$\mu$	$\partial$
			0.51	2.85	0.298		3.21	1.73
EC-301 B	Gas valve 2	Weibull	$\beta$	$\eta$	$\gamma$	Loglogistic	$\mu$	$\partial$
			0.418	0.64	0.6049		3.3	0.75
EC-301 C	Turbine Bearing	Normal	$\mu$	$\partial$	Normal	$\mu$	$\partial$	
			3.56	0.1		24	1	
	Turbine Bearing	Gumbel	$\mu$	$\partial$	Lognormal	$\mu$	$\partial$	
			4.09	1.61		2.93	0.92	
EC-301 C	Gas valve 1	Gumbel	$\mu$	$\partial$	Lognormal	$\mu$	$\partial$	
			4.3	1.77		3.05	1.09	
EC-301 C	PSV valve and others	Normal	$\mu$	$\partial$	Lognormal	$\mu$	$\partial$	
			2.07	1.21		2.72	1.52	

FIGURE 4.86

Furnace failure and repair PDF parameters.



**FIGURE 4.87**

Fluid catalytic cracking system RBD.

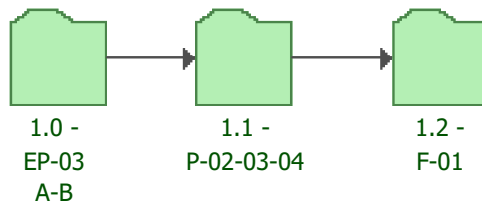
The warming subsystem RBD is represented in Fig. 4.88.

### Conversion

This subsystem targets performing crack reaction on feed heating product. The conversion subsystem assumptions are:

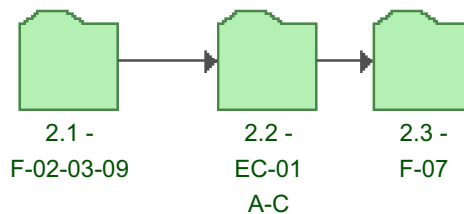
- If F-02-03-04 shut down, the conversion subsystem will be unavailable.
- At least two of the three compressors (EC-03 A–C) must be available during the same period of time not to shut down the conversion subsystem.
- If furnace F-07 shuts down, the conversion subsystem will be unavailable.

The conversion subsystem RBD is represented in Fig. 4.89.



**FIGURE 4.88**

Warming subsystem RBD.



**FIGURE 4.89**

Conversion subsystem RBD.

### Cold Area

The purpose of this subsystem is to separate products of vapor feed from the conversion subsystem in the tower (F-05). The cold area RBD assumptions are:

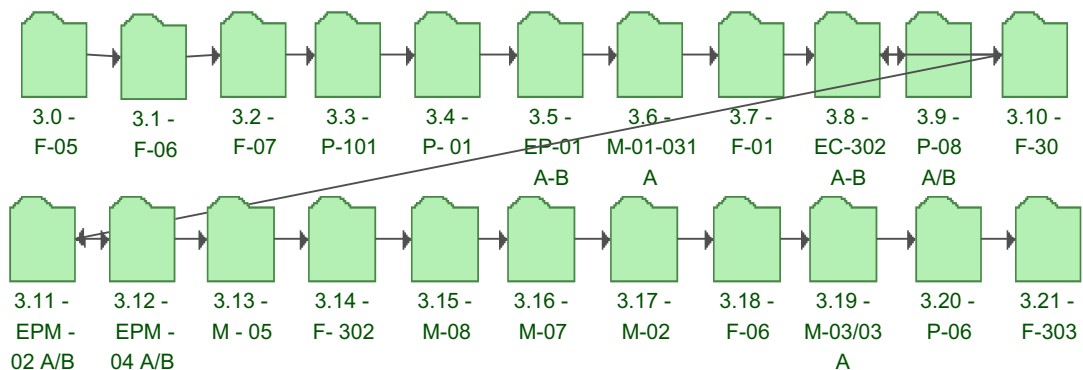
- If strippers F-05 or F-6 shut down, the cold area subsystem will be unavailable.
- If any of the vases (F-01, F-30, F-207, F-301, F-302, F-303, F-306, or F-3000) are unavailable, the feed and cold area subsystem will be unavailable.
- If one of the exchangers (P-01, P-101, P-04 A, P-04 B, M-01–031 A, M-05, M-08, M-07, M-02, or M-03/03 A) shuts down, the cold area subsystem will be unavailable.
- At least one of two compressors (EC-302 A/B) must be available, otherwise the cold area subsystem will be unavailable.
- At least one of two pumps (EP-01 A/B, EPM-02 A/B, and EPM-04 A/B) must be available, otherwise the cold area subsystem will be unavailable.

The cold area subsystem RBD is shown in Fig. 4.90.

### Diethylamine Subsystem

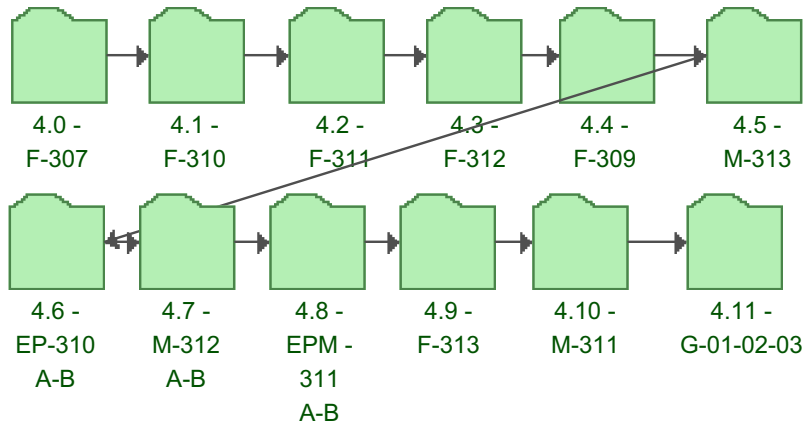
The purpose of this subsystem is to separate  $H_2$  from gas. The diethylamine RBD assumptions are:

- If the splitters (F-307, F-309, F310, or F-311) shut down, the diethylamine subsystem will be unavailable.
- If pumps A and B (EPM-310 and EPM-311 A/B) are unavailable during the same period of time, the feed and preheating subsystem will be unavailable.
- If one of the exchangers (M-311, M-312 A, M-312 B, or M-313) shuts down, the compression subsystem will be unavailable.
- If one of the vases (F-312 or F-313) shuts down, the diethylamine subsystem will be unavailable.
- If at least two of three tanks (G-01-02-03) shut down, the diethylamine subsystem will be unavailable.



**FIGURE 4.90**

Cold area subsystem RBD.



**FIGURE 4.91**  
Diethylamine subsystem RBD.

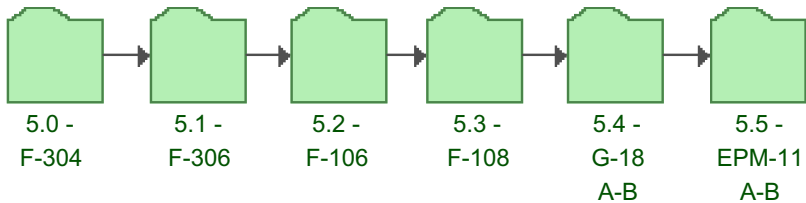
The diethylamine subsystem RBD is shown in [Fig. 4.91](#).

### Cleaning

The cleaning subsystem objective is eliminating unwanted components such as sulfur and nitrogen. The cleaning subsystem RBD assumptions are:

- At least one of two tanks (G-18 A/B) must be available, otherwise the cleaning subsystem will be unavailable.
- If pumps EPM-11 A and B are unavailable during the same period of time, the cleaning subsystem will be unavailable.
- If one of the vases (F-304, P-306 A, F-106, or F-108) shuts down, the cleaning subsystem will be unavailable.

The cleaning subsystem RBD is shown in [Fig. 4.92](#).



**FIGURE 4.92**  
Cleaning subsystem RBD.

### **Simulation**

RAM analysis was conducted using BlockSim software. The simulation allows the creation of typical life cycle scenarios for proposed systems, with Monte Carlo simulation methodology. The entire unit was modeled through RBDs, considering the redundancies and the possibilities for bypass in each equipment or system configuration. Next, the evaluated model was fed failure and repair data. The simulation allows assessment of whether availability results are achieving the target of 98% in 3 years. If the efficiency target is not achieved, it becomes necessary to improve the operational capabilities of critical equipment.

The simulation was conducted to 5 years and 1000 tests were run to converge results. The availability was 99.81% in 5 years and the expected failures were 5.3.

### **Critical Analysis**

The critical analysis defines which are the most critical subsystems and equipment having the most influence on production losses. There are two indicators showing criticality: the RI and EC.

The first one shows how much influence one subsystem or equipment has on system reliability. Thus, using partial derivation, it is possible to realize how much it is necessary to increase subsystem or equipment reliability to improve the whole system reliability.

The following equation shows the mathematical relation:

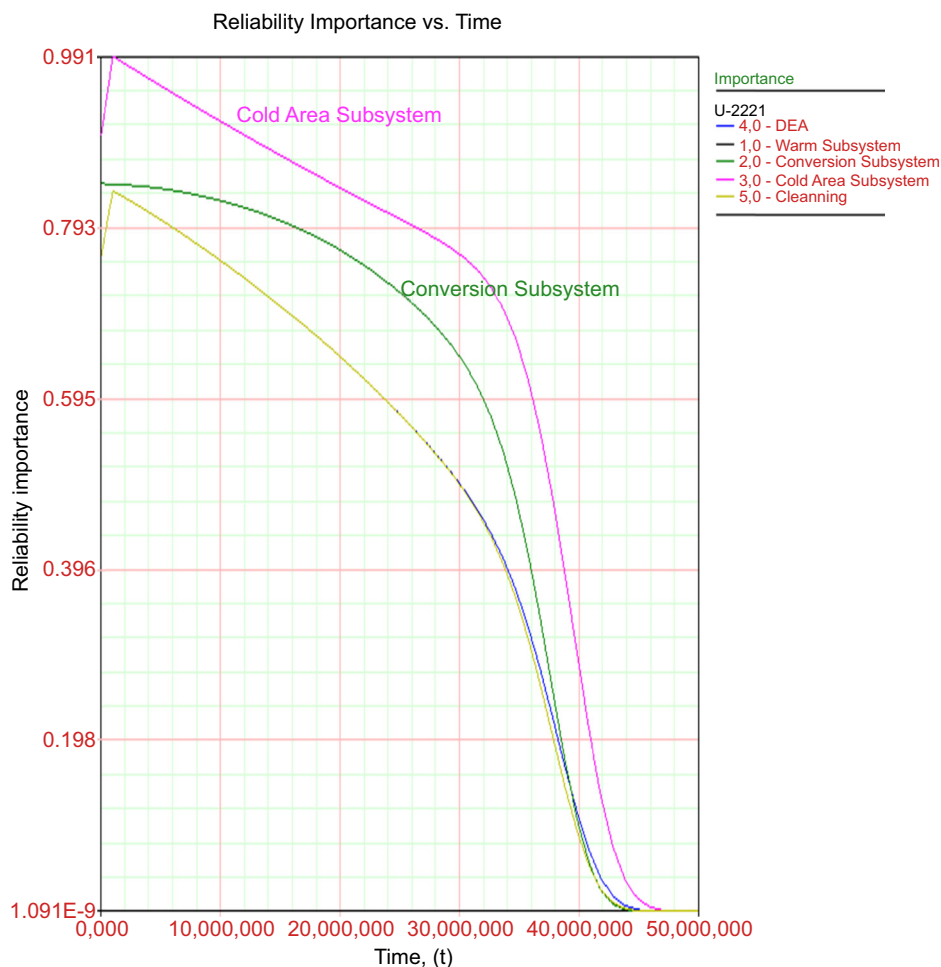
$$\frac{\partial R(\text{System})}{\partial R(\text{Subsystem})} = \text{RI}$$

Despite this relation, some equipment or subsystems may be prioritized because of repair time having an expressive impact on system availability. This means that the availability impact is the most important parameter, despite reliability being highly influential on the system. A specific subsystem or piece of equipment might not be the most critical because of the repair time impact. In this case, equipment that has four shutdowns in a specific period of time might not be as critical as another piece of equipment that has only one shutdown. For the second piece of equipment, the total loss time is higher than the first. In most cases it is not possible to reduce repair time. Therefore equipment reliability improvement is the best solution for achieving the availability target. In this case the RI is the best index to show how much improvement reliability the system can accommodate. But, as discussed, it is necessary to consider availability. In the fluid catalytic cracking system the most critical subsystems are the cold area and conversion subsystems for the RI and EC. This implies that in terms of failures and losses that subsystem is the most critical. The RI results are shown in Fig. 4.93.

The DECI was also used to assess which equipment causes more shutdowns in the fluid catalytic cracking system, and despite the low number of shutdowns and  $k/n$  configuration, compressors EC-01 A–C are responsible for most of them, as shown in Fig. 4.94.

Despite the compressor being the most critical piece of equipment, the fluid catalytic cracking system achieved the availability target (99.91% in 5 years) and no improvements are required in this system.

However, this compressor has operated for over 20 years, and despite increasing corrective and preventive maintenance costs, requires optimum replacement time analysis.



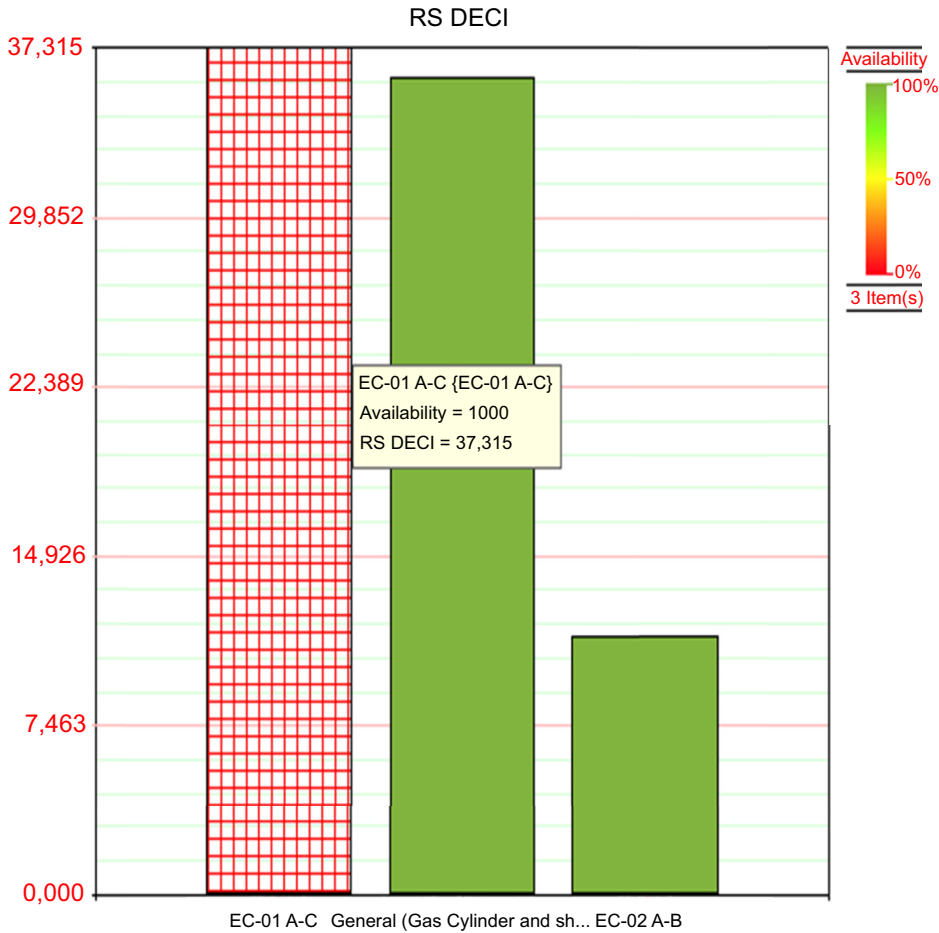
**FIGURE 4.93**

Reliability importance.

### **Sensitivity Analysis**

After critical analysis, it becomes clear that no improvement actions are required in the fluid cracking catalytic system because this system achieves its availability target. However, optimum replacement time analysis is required, so in the fluid catalytic cracking system case, the following will be considered in the sensitivity analysis:

- Optimum replacement time;
- Phase block diagram analysis.

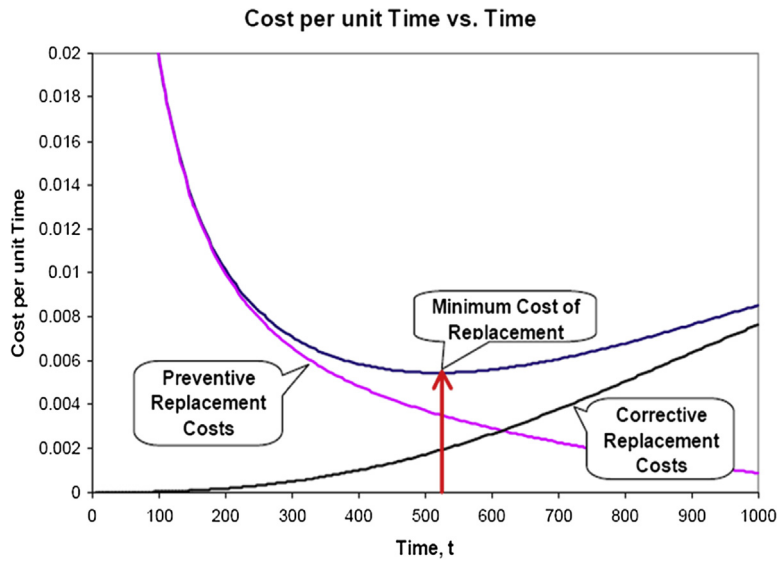


**FIGURE 4.94**  
Downing event criticality index.

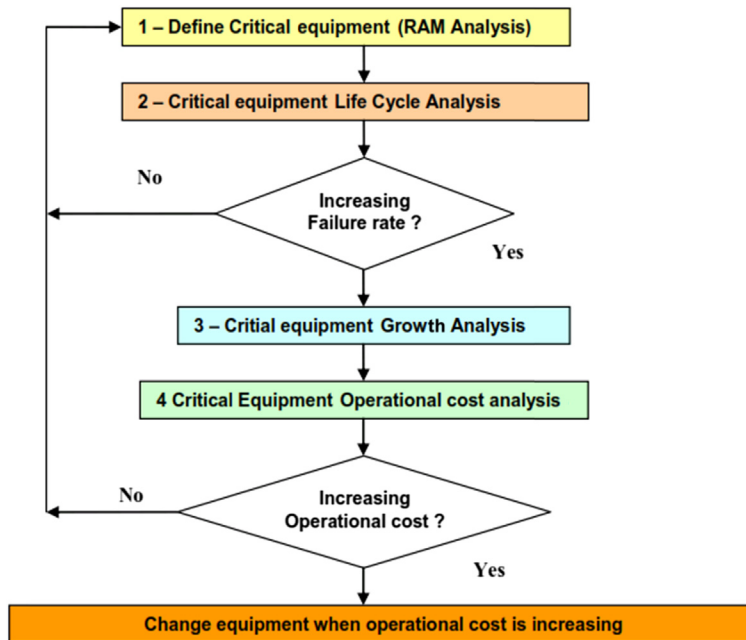
In the first case, it is necessary to assess each compressor and assess the optimum replacement time for the operational costs of the equipment, which includes maintenance, purchases, and costs related to the loss of production. Despite *kn* configuration, such compressors do not impact system availability much, but have operational costs increasing over time. Fig. 4.95 shows the optimum replacement time philosophy.

Indeed, the cost is not the only driver to be considered to replace the equipment. In addition to cost it is also necessary to access additional aspects such as failure rate function and the reliability growth prediction. The complete approach to assess the best time to replace the equipment is described in Fig. 4.96.





**FIGURE 4.95**  
Optimum replacement time.

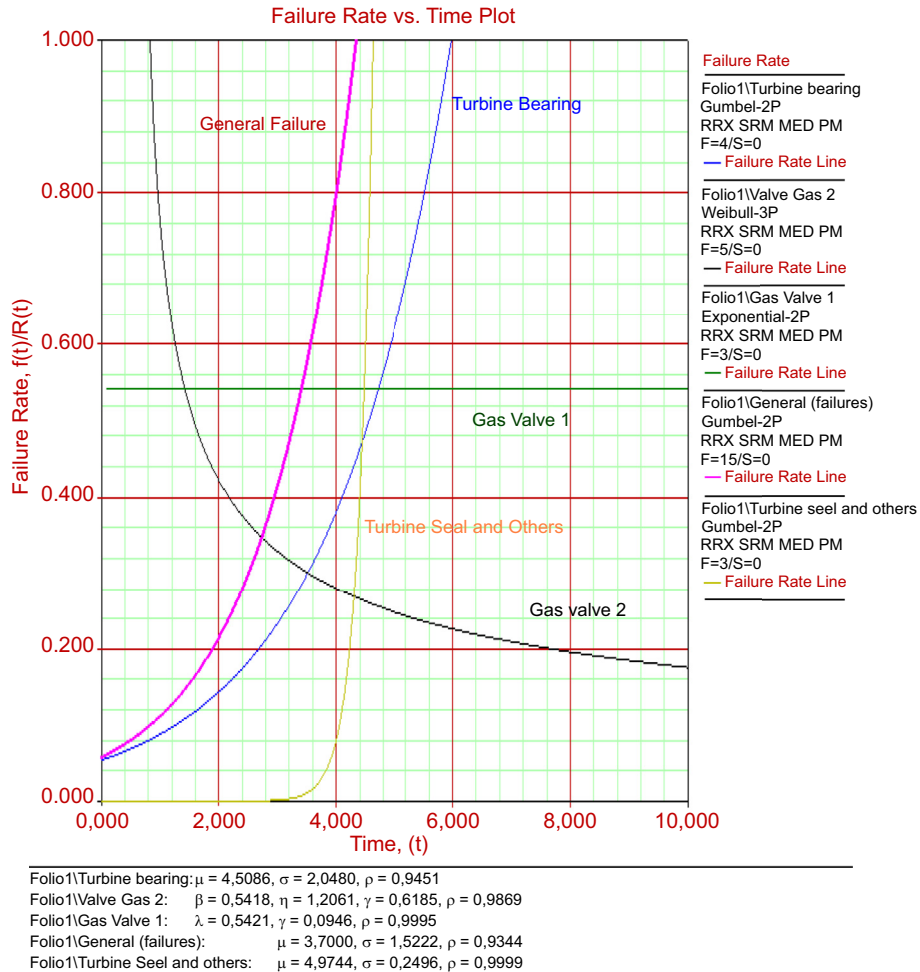


**FIGURE 4.96**  
Optimum replacement time methodology.

Using compressor A, for example, the life cycle analysis after overhauling revealed increasing failure rates for most of the components, as shown in Fig. 4.97.

However, the life cycle analysis is not enough to decide if equipment must be replaced, and operational costs must also be considered in such decisions. The compressor purchase cost was divided over compressor operation years and maintenance costs were included. The following equation shows operational costs per time:

$$C(t_r) = C(Aq) + \int_0^{t_r} \left( \frac{1}{t\sigma_{T_r}\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t_r - \mu}{\sigma_{T_r}}\right)^2} \right) \times C(M_t) dt$$



**FIGURE 4.97**

Compressor A lifetime data analysis failure rate functions.

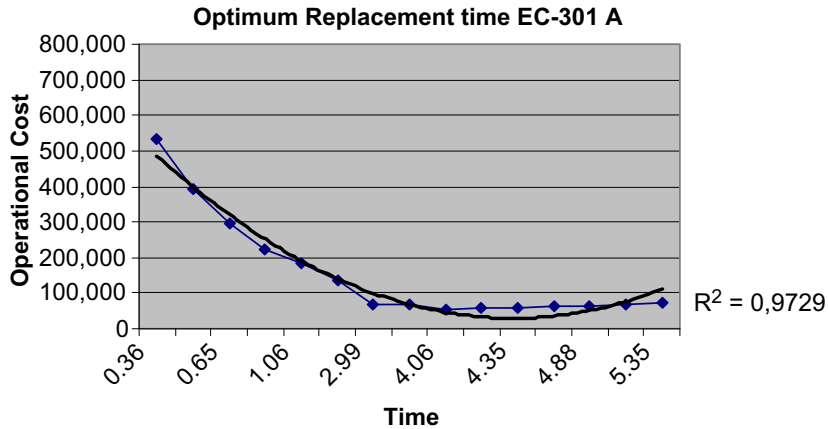


FIGURE 4.98

Compressor A life cycle analysis.

The expected cost is a cumulative density function multiplied by maintenance costs for each period of time. In this case the cumulative density function that shows compressor A failure is the normal function with parameters  $\mu = 8.7$  and  $\sigma = 1.5$ .

In doing so, creating the optimum replacement time graph, it is possible to see the operational costs increase from 4.5 years, as shown in Fig. 4.98.

The optimum replacement time was performed for other compressors and all of them presented increasing costs over 4 years and must be replaced.

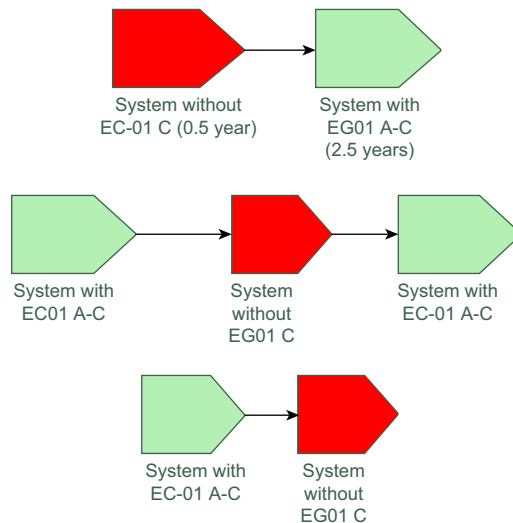
The second sensitivity analysis uses phase block diagram analysis to assess the impact on system availability related to not replacing such compressors. The phase diagram methodology's main propose is to simulate the system in which configuration changes over time (simulation time). Thus in the fluid catalytic cracking system case it was possible to simulate three scenarios, as shown in Fig. 4.99.

The phase diagrams are simulating in three phases. The first one shows the system operating for the first 6 months without one compressor and the other 2.5 years with three compressors. The second scenario shows the system operating with two compressors from 1.5 years over 6 months, and the third scenario shows the system operating without one compressor in the last 6 months to 3 years of operation.

In the first case the system achieved 97.7% availability in 3 years; in the second case the system achieved 97.34% availability in 3 years; and in the third case the system achieved 98.49% availability in 3 years. In this analysis, 3 years of operation time was used because in the near future such systems (FCC) will operate and supply other systems that operate by 3 years.

### Conclusion

RAM analysis performed in the fluid catalytic cracking plant showed that even when a system achieves its target it is possible to improve system performance from an economical point of view by performing optimum replacement time analysis for equipment with increasing operational

**FIGURE 4.99**

System phase diagram.

costs. In addition, the phase block diagram methodology was applied to assess different system configurations over time. It is a powerful tool for modeling systems that change their configurations over time.

#### 4.6.8 RAM + L ANALYSIS: REFINERY CASE STUDY

The main objective of RAM analysis is assessing equipment or system performance throughout critical equipment improvements to achieve an availability target. To conduct RAM analysis it is necessary to define the equipment failure modes that have the highest impact on system availability. The analysis is conducted using historical failure data and repair time and simulation using a reliability diagram model. Despite widespread applicability of this methodology on large, complex systems it is vitally important that logistic issues be considered. There are two different approaches. The first one focuses only on reliability issues and the second one on reliability and logistics. At this time in Brazil there is no methodology that considers both issues, logistics and reliability, in only one methodology to assess huge systems regarding reliability and logistic issues in the same model.

The RAM + L analysis methodology considers logistic and reliability issues for a more representative result to support improved decisions. This case study consists of a complex system that includes refineries and plants (vacuum and atmospheric distillation plant, thermal cracking plant, acid water plant, catalytic cracking plant, reforming catalytic plant, fractioning plant, diethylamine plant, and naphtha and diesel hydrodesulfurization plant). Analysis will be conducted to assess advantages and disadvantages and to compare RAM analysis results with the results obtained using RAM + L analysis.

**Table 4.24 Failures and Repair Data**

TAG	Failure Mode	Failure Time (years)				Repair Time (hours)		
		Variables (PDF)				Variables (PDF)		
F-01 A	Coke formation	Normal		$\mu$	$\rho$	Normal	$\mu$	$\rho$
				4.95	2.66		420	60
	Incrustation	Weibull	$\beta$	$\eta$	$\gamma$	Normal	$\mu$	$\rho$
			0.51	1.05	4.05		420	60
	Other failures	Exponential Bi p		$\lambda$	$\gamma$	Normal	$\mu$	$\rho$
				0.28	3.22		420	60
F-01 B	Coke formation	Normal		$\mu$	$\rho$	Normal	$\mu$	$\rho$
				5.23	2.55		420	60
	Other failures	Exponential Bi p		$\lambda$	$\gamma$	Normal	$\mu$	$\rho$
				0.29	4.07		420	60

Bi p, bi-parametric.

**Failure and Repair Data Analysis**

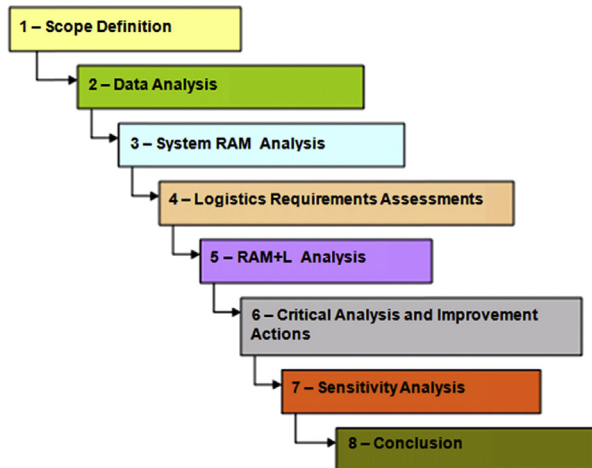
A huge challenge for the Brazilian oil and gas industry is getting data to perform RAM analysis. To ensure the reliability of such data, maintenance professionals with knowledge of these systems took part in this stage, and a semiquantitative analysis of failure and repair data was conducted in some cases.

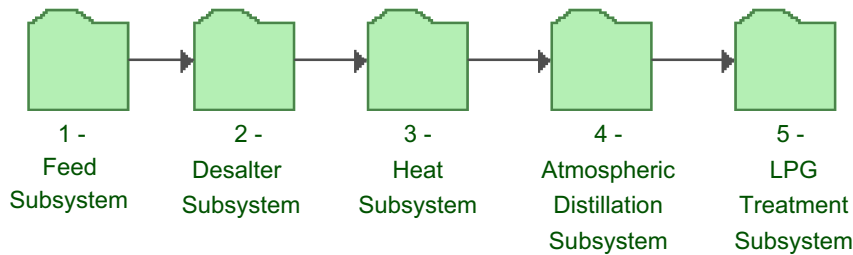
To conduct RAM analysis to find out system shutdown related with equipment failures it is necessary to collect historical failure data. Then the equipment failure data is treated statistically to define the PDFs that best fit the historical failure data, and it is necessary to use software to do such analysis (Weibull 7++ Reliasoft). Table 4.24 gives the thermal cracking furnace failure mode PDFs and repair time.

Statistical analysis was performed for more than 200 pieces of equipment to allow direct simulation (Monte Carlo) for operation time in 3 years. Coke formation is the most critical event in refinery plants, and coke formation is considered the most critical failure mode in the RBD modeling, but it is considered a process failure. Fig. 4.100 summarizes RAM + L methodology.

**FIGURE 4.100**

RAM + L methodology.





**FIGURE 4.101**

Atmospheric distillation RBD.

Source: Calixto, et al., 2010.

### System Modeling

To perform the availability results in Monte Carlo simulation, it is necessary to set up an RBD model. Although the system is complex, RBD methodology was used. To perform Monte Carlo simulation, it is necessary to be familiar with the production flow data that influences losses in productivity. Consequently, some statements and definitions for process limitations are needed and are given in the following.

#### Atmospheric Distillation Plant (U-11)

Based on general process assumptions, the RBD of the atmospheric distillation plant includes five blocks in series, which represent feed, desalter, heating, furnace, atmospheric distillation, and LPG treatment subsystems. This means that if one block fails, the whole system will be unavailable.

Each subsystem represented in the RBD includes several pieces of equipment and the respective PDFs based on failure modes data. The assumptions for creating the RBD model are:

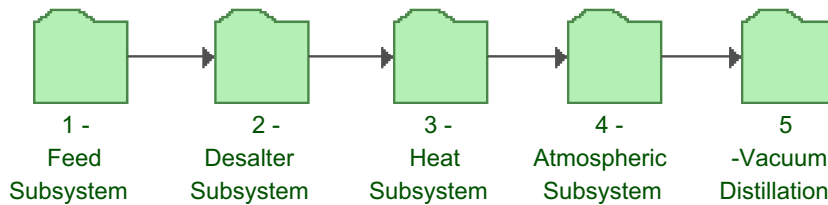
- It is not being considered that other facilities' unavailability has an influence on U-10 availability.
- Subsystem unavailability represents system failure time.
- The average availability target is 97% over 3 years.
- Total production per day is 1.5 m<sup>3</sup>.

Fig. 4.101 shows the RBD, which includes the five main block diagrams.

To have a heavy oil feeding most of the time, the correct equipment reliability specifications and correct maintenance policies over time must be applied to allow the system to achieve the availability target in 5 years. In fact, most system unavailability is related to static equipment. Most dynamic equipment such as pumps have redundancy and permit high performance even though equipment reliability is not that high.

#### Atmospheric and Vacuum Distillation Plant (U-10)

The vacuum distillation plant's main objective is to obtain a light product from the heavy oil portion. Based on general assumptions, the RBD of the vacuum distillation plant includes five blocks in series, which represent the feed, desalter, heating, furnace, atmospheric distillation, and vacuum distillation subsystems. Thus if one block fails, the whole RBD will be unavailable. Each subsystem represented



**FIGURE 4.102**

Distillation RBD.

Source: Calixto, et al., 2010.

in the RBD includes several pieces of equipment and respective PDFs based on failure mode data. The main assumptions for creating the RBD are:

- The equipment failure modes are based on historical failure data of the plant from 2000 to 2010.
- Subsystem unavailability represents system failure.
- The average availability target is 98% in 5 years.
- Total production per day is 5.6 m<sup>3</sup>.

Fig. 4.102 shows the RBD, which includes the three main block diagrams.

Different from the atmospheric distillation plant (U-10), the vacuum distillation plant (U-11) is fed by heavy oil all the time. In addition, the correct equipment reliability requirement and maintenance policies over time allow the system to achieve the availability target in 5 years.

#### Thermal Catalytic Cracking Plant (U-211)

The main objective of the thermal catalytic cracking plant is to convert heavy oil feed from the vacuum distillation plant (U-11) into diesel product. Based on general assumptions, the RBD of the thermal catalytic cracking plant includes five blocks in series, which represent the feed and preheater, thermal cracking, fractioning, compression, and stabilization subsystems. This means that if one block fails, the whole RBD will be unavailable. Each subsystem represented in the RBD includes several pieces of equipment and the respective PDFs based on failure modes data. The main assumptions for creating the RBD are:

- It is not being considered that other facilities' unavailability has an influence on U-211 availability.
- The equipment failure modes are based on historical failure data of similar plants from other refineries.
- Subsystem unavailability represents system failure.
- The availability target is 97% in 3 years.
- Total production per day is 1.5 m<sup>3</sup>.

Fig. 4.103 shows the RBD, which includes the five main block diagrams.

#### Diesel Hydrodesulfurization Plant (U-13)

The main objective of the diesel hydrodesulfurization plant is to separate the sulfur component from diesel, which comes from the atmospheric and vacuum distillation plant (U-10), atmospheric distillation

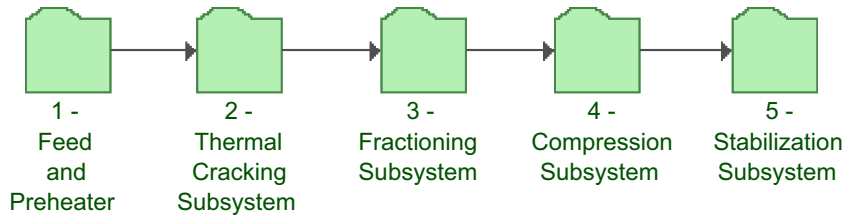


FIGURE 4.103

Thermal cracking plant RBD.

plant (U-11), and the thermal cracking plant (U-211). Based on the general assumptions, the RBD of the diesel hydrodesulfurization plant includes seven blocks in series, which represent the feed, reaction, H<sub>2</sub> make-up, H<sub>2</sub> cycle, diesel fractioning, drying, and cleaning water subsystems. This means that if one block fails, the whole RBD system will be unavailable. Each subsystem represented in the RBD includes eight pieces of equipment and the respective PDFs based on the historical failure modes data. The main assumptions for this system RBD are:

- The equipment failure modes are based on historical failure data of similar plants from other refineries.
- Subsystem unavailability represents system failure.
- The average availability target is 98% in 3 years.
- Total production per day is 2500 m<sup>3</sup>.

Fig. 4.104 shows the RBD, which includes the eight main block diagrams.

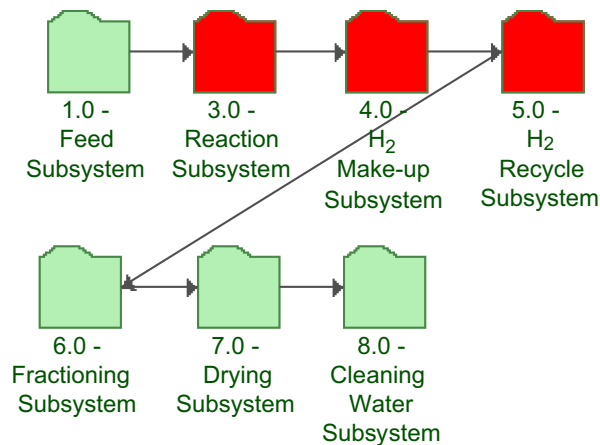


FIGURE 4.104

Diesel hydrodesulfurization RBD.



### Naphtha Hydrodesulfurization Plant (U-12)

The main objective of the naphtha hydrodesulfurization plant is to separate the sulfur component from the naphtha feed from the atmospheric and vacuum distillation plant (U-10), the atmospheric distillation plant (U-11), and the thermal cracking plant (U-211).

Based on general assumptions, the RBD of the naphtha hydrodesulfurization plant includes four blocks in series, which represent the feed, reaction, Fractioning and H<sub>2</sub> cycle subsystems. This means that if any one block fails, the whole system is shut down. Each subsystem represented in the RBD includes eight pieces of equipment and the respective PDFs based on failure mode data. The following assumptions are used to create the RBD:

- The equipment failure modes are based on the historical failure data of similar plants from other refineries.
- Subsystem unavailability represents system failure.
- The average availability target is 98% in 3 years.
- Total production per day is 2500 m<sup>3</sup>.

Fig. 4.105 shows the RBD, which includes the eight main block diagrams.

One of the most important process conditions is the H<sub>2</sub> make-up compressors (A/B) in the diesel hydrodesulfurization plant (U-13). Such equipment supplies H<sub>2</sub> to both plants (U-12 and U-13). In doing so, in the case of unavailability in the H<sub>2</sub> make-up compressors both plants will be unavailable.

### Acid Gas Treatment Plant (Diethylamine Plant, U-23)

The main objective of the acid gas treatment plant is to separate the sulfur component from the gas produced in the naphtha and diesel hydrodesulfurization plant. Based on general assumptions, the RBD of the diethylamine plant includes many types of equipment such as vases, pumps, heat exchangers, and towers in series. This means that if one piece of equipment fails, the whole system will be unavailable. In this case, like other subsystems and systems, the pumps are in parallel configuration. This means both pumps must fail to shut down the diethylamine plant. The main assumptions for creating the RBD are:

- The equipment failure modes are based on the historical failure data of similar plants from other refineries.
- Subsystem unavailability represents system failure.
- The availability target is at least 98% in 3 years.

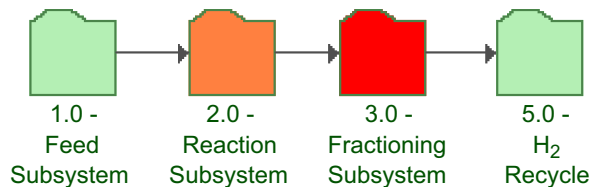
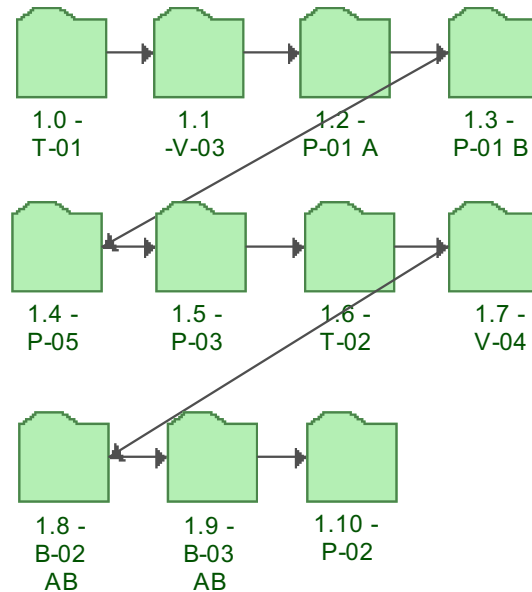


FIGURE 4.105

Naphtha hydrodesulfurization RBD.



**FIGURE 4.106**  
DEA plant RBD.

In Fig. 4.106 the diethylamine subsystem RBD is represented and includes vases, pumps, and towers.

#### Acid Water Treatment Plant (U-26)

The main objective of the acid water treatment plant is to separate the sulfur from the gas produced in the naphtha and diesel hydrosulfurization plant. Based on general assumptions, the RBD of the diethylamine plant includes many types of equipment such as vases, pumps, heat exchangers, and towers in series. This means that if one of the blocks fails, the whole RBD will be unavailable. In this case, like in other subsystems and systems, the pumps are in parallel configuration. This means both pumps would have to fail to shut down the diethylamine plant. The main assumptions for creating the RBD are:

- The equipment failure modes are based on the historical failure data of similar plants from other refineries.
- Subsystem unavailability represents system failure.
- The availability target is at least 98% in 3 years.

In Fig. 4.107 the acid water treatment subsystem RBD is shown including its vases, pumps, and towers.

One of the most important assumptions in the acid water plant is that in the case of unavailability of such plants, other plants are unavailable including the atmospheric and vacuum distillation plant (U-10), the atmospheric distillation plant (U-11), the thermal cracking plant (U-211), the naphtha and

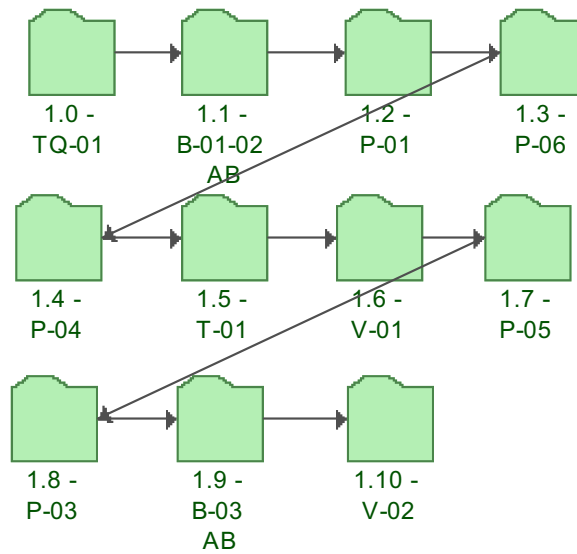


FIGURE 4.107

Acid water plant RBD.

diesel desulfurization plant (U-2312/U-2313), and the catalytic cracking plant. Actually, acid water achieves high availability, and because of this there is no significant impact on the refinery for acid water plant unavailability.

#### Catalytic Cracking Plant (U-21)

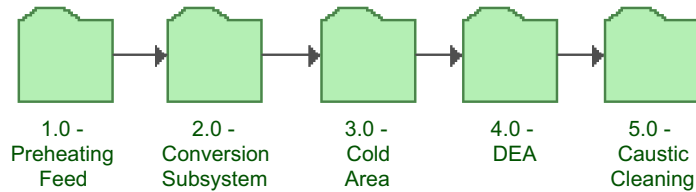
The main objective of the catalytic cracking plant is to convert heavy feed from atmospheric and vacuum distillation (U-10) into light oil product.

Based on general assumptions, the RBD of the catalytic cracking plant includes five blocks in series, which represent the preheating feed, conversion, cold area, diethylamine, and caustic cleaning subsystems. This means that if one block fails (ie, one subsystem), the whole system will be unavailable. Each subsystem represented in the RBD includes several pieces of equipment and the respective PDFs based on failure modes data. The main assumptions for creating the RBD are:

- The equipment failure modes are based on historical failure data of their own unit plant.
- Subsystem unavailability represents system failure.
- The availability target is 98% in 3 years.
- Total production per day is 55 m<sup>3</sup>.

Fig. 4.108 shows the RBD, which includes the five main block diagrams.

The most critical equipment in this type of plant is the compressor in terms of the number of increasing failures, despite  $k$ -out-of- $n$  (2/3) configuration, which means at least two of three compressors must be available not to shut down the system, and compressor operation cost is increasing over time.

**FIGURE 4.108**

Catalytic cracking plant RBD.

### Reforming Catalytic Cracking Plant (U-22)

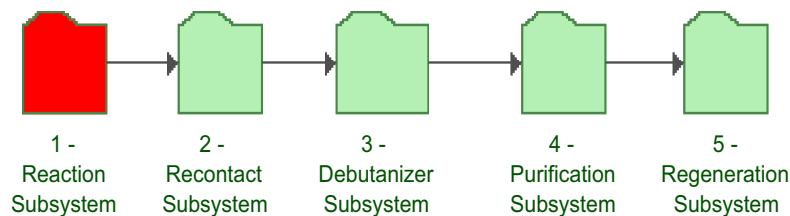
The main objective of the reforming catalytic cracking plant is to convert heavy naphtha from the fractionating plant (U-20) into reforming naphtha product. Based on general assumptions, the RBD of the reforming catalytic cracking plant includes five blocks in series, which represent the reaction, recontact, debutanizer, purification, and regeneration subsystems. That means that if one block fails, the whole RBD will be unavailable. Each subsystem represented in the RBD includes several pieces of equipment and the respective PDFs based on failure modes data. The main assumptions for creating the RBD are:

- The equipment failure modes are based on the reliability requirement and failure data from similar equipment.
- Subsystem unavailability represents system failure.
- The availability target is 98% in 3 years.
- Total production per day is 800 m<sup>3</sup>.

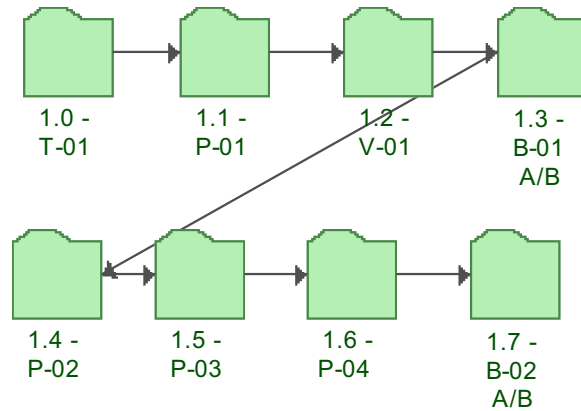
Fig. 4.109 shows the RBD, which includes the five main block diagrams.

### Fractionating Plant (U-20)

The main objective of the fractionating plant is to convert the naphtha from the naphtha hydrotreatment plant (U-13) into heavy and light naphtha products. Based on general assumptions, the RBD of the fractionating plant includes eight blocks in series, which represent towers, pumps, vases, and heat exchangers. This means that if one of the blocks fails, the whole RBD will be unavailable. Each

**FIGURE 4.109**

Reforming catalytic cracking plant RBD.



**FIGURE 4.110**

Fractionating plant RBD.

subsystem represented in the RBD includes several pieces of equipment and the PDFs based on failure modes data. The main assumptions used for creating the RBD are:

- The equipment failure modes are based on failure data from similar equipment of other refineries.
- Subsystem unavailability represents system failure.
- The availability target is 98% in 3 years.
- Total production per day is 1500 m<sup>3</sup>.

Fig. 4.110 shows the RBD, which includes the five main block diagrams.

### **Logistic Resources**

Logistics management is the part of the supply chain process that plans, implements, and controls the efficient, effective flow and storage of goods, services, and related information from the point of origin to the point of consumption to meet customer requirements. Logistic resources, such as tanks, pipelines, and ships, have the main objective of making products, equipment, and raw material flow easier throughout processes to maximize profits.

The logistic resources configuration mostly is applied to systems for its dependence and related demands and supply of products. In general, in logistic model assessment, equipment reliability, which highly influences profits, is not considered. In many cases, logistics is also not considered in RAM analysis. The main discussion in this case study is the importance of including plant reliability issues and logistic resources, which together have a complex model.

The main logistic resources in a refinery are tanks, which provide oil to distillation plants. Such tanks reduce system unavailability whenever pumps or other equipment that supply oil to the tanks shut down. Fig. 4.111 gives a good example of logistics mixed with RBD methodology.

In the first case, both distillation plants are feed for tanks. The U-10 is fed by G-01 and G-404. Both tanks are available, and only one of them is enough to supply U-10 and G-404, an active redundancy. There is equipment associated with tanks, such as pipelines and pumps, that also impacts system availability. The RBD model regards tank failures (internal and external corrosion) in series with two pumps in parallel, one of them being a passive redundancy.

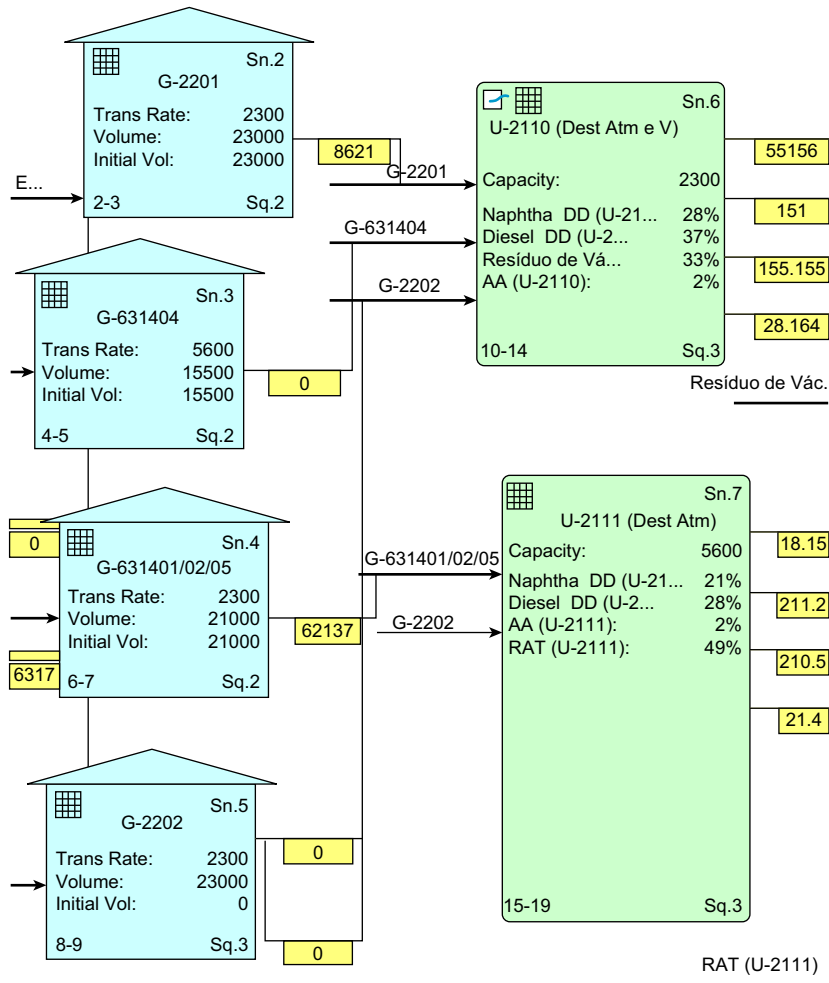


FIGURE 4.111

Tank feed distillation plants.

In the second case, U-11 is fed from G-401/402/405 or G-02, which supplies U-11 and U-10 as an active redundancy. G-401/402/405 shows a  $k/n$  (1/3) configuration RBD, which means at least one of three must be available to keep U-11 from shutting down.

The tank's configuration comprises three tanks, G-401/402/405, and at least one of them must be available to avoid U-11 unavailability.

In this example, tanks cause no high impact in the final result because there are redundant tanks and such equipment has high availability. On the other hand, the acid water subsystem can impact system availability because acid gas is in series with many plants (U-10, U-11, U-12, U-13, and U-21). In case of acid water (U-26) shutdown, a number of plants shut down.

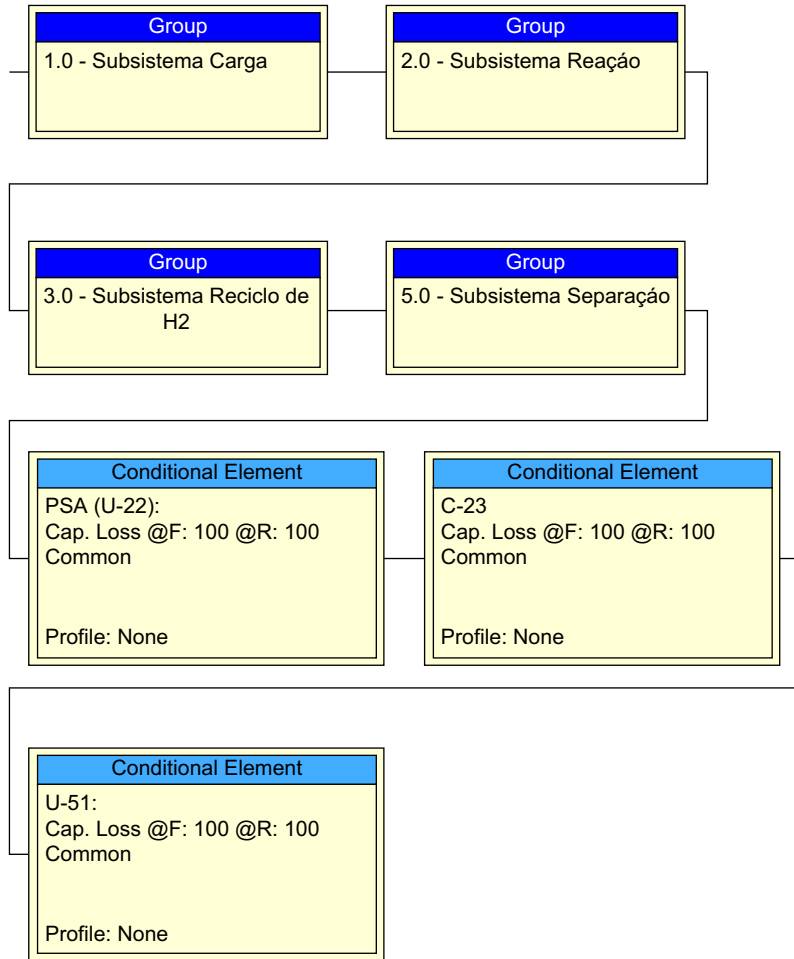


FIGURE 4.112

Outside U-12 impacts.

Another good example is U-12; in case of shutdown, the compressor of U-13 and pressure swing absorption (PSA) (H<sub>2</sub> purification) of U-22 will shut down.

If logistic analysis is carried out, those assumptions will probably not be considered, because logistics focus on product flow and stock. In doing so, in RAM + L such assumptions must be represented in RBD by condition block, as shown in Fig. 4.112.

For such assumptions we can conclude that it is not possible to model a complex system without considering logistic and reliability issues. A refinery model example, which is considered a complex system with 10 plants and tanks, will be given to show the RAM + L application.

### Systems Simulation

Simulation (Monte Carlo) has the main objective of confirming the system availability results to determine critical equipment or logistic resources (tanks) in terms of availability and utilization to support improvement decisions. The model regards all equipment failure modes modeled by RBD methodology.

For each system previously discussed a simulation is performed, and after the whole system is done, it will be assessed based on RBD methodology.

To run a simulation, software, such as MAROS (Maintainability, Availability, Reliability, and Operability Simulator [DNV]) and BlockSim (Reliasoft), is used, and the final results are compared to assess the results.

Even when system characteristics are not represented completely, it is still possible to simulate the effects of equipment failures on system availability. According to simulation methodology, it is also possible to represent the system life cycle over time and consider system downtime.

The system simulations were performed one by one showing the main result. The availability and efficiency are approximately the same in case 1 and different in case 2. The cases are:

- Case 1 assumes that all equipment (in series) shutdowns cause 100% unavailability of one specific system capacity production.
- Case 2, part of plant capacity production is lost when equipment (in series) shuts down.

The following equation shows case 1, where availability and efficiency are the same over time. In this case the production is always in two conditions over time: 0% when equipment shuts down or 100% when the system is working properly:  $D(t)$  is availability,  $EP(t)$  is efficiency,  $t$  is time that the system is working,  $T$  is nominal time,  $p$  is real production, and  $P$  is nominal production.

$$EP(t) = \frac{\sum_{i=1}^n pr_i \times t_i}{\sum_{i=1}^n Pr_i \times T_i}$$

$$EP(t) = \frac{pr_1 \times t_1 + pr_2 \times t_2 + \dots + pr_n \times t_n}{Pr_1 \times T_1 + Pr_2 \times T_2 + \dots + Pr_n \times T_n}$$

$$D(t) = \frac{\sum_{i=1}^n t_i}{\sum_{i=1}^n T_i}$$

$$pr_1 = pr_2 = pr_3 = \dots = pr_n$$

$$Pr_1 = Pr_2 = Pr_3 = \dots = Pr_n$$

$$EP(t) = \frac{pr_1 \times (t_1 + t_2 + \dots + t_n)}{Pr_1 \times (T_1 + T_2 + \dots + T_n)}$$

$$pr_i = Pr_i$$

$$EP(t) = \frac{pr_1 \times (t_1 + t_2 + \dots + t_n)}{pr_1 \times (T_1 + T_2 + \dots + T_n)}$$

$$EP(t) = \frac{\sum_{i=1}^n P t_i}{\sum_{i=1}^n P T_i}$$

$$EP(t) = \frac{(t_1 + t_2 + \dots + t_n)}{(T_1 + T_2 + \dots + T_n)}$$

$$EP(t) = \frac{\sum_{i=1}^n t_i}{\sum_{i=1}^n T_i} = D(t)$$



The following equation shows case 2, and in this case, production depends on the loss that equipment causes in the system ranging from zero to 100%. Again,  $D(t)$  is the availability,  $EP(t)$  is efficiency,  $t$  is time that the system is working,  $T$  is nominal time,  $p$  is a real production, and  $P$  is nominal production. Such conditions happen, for example, when certain heat exchangers shut down. In some cases, it is possible to still produce, but it is necessary to reduce production while the heat exchanger is being repaired.

$$EP(t) = \frac{\sum_{i=1}^n pr_i \times t_i}{\sum_{i=1}^n Pr_i \times t_i} + \frac{\sum_{i=1}^n p/r_i \times t_i}{\sum_{i=1}^n P/r_i \times t_i}$$

$$EP(t) = \frac{\sum_{i=1}^n pr_i \times t_i}{\sum_{i=1}^n Pr_i \times T_i}$$

$$EP(t) = \frac{pr_1 \times t_1 + pr_2 \times t_2 + \dots + pr_n \times t_n}{Pr_1 \times T_1 + Pr_2 \times T_2 + \dots + Pr_n \times T_n}$$

$$pr_1 = pr_2 = pr_3 = \dots = pr_n$$

$$Pr_1 = Pr_2 = Pr_3 = \dots = Pr_n$$

$$EP(t) = \frac{pr_1 \times (t_1 + t_2 + \dots + t_n)}{Pr_1 \times (T_1 + T_2 + \dots + T_n)}$$

$$pr_i = Pr_i$$

$$EP(t) = \frac{pr_1 \times (t_1 + t_2 + \dots + t_n)}{pr_1 \times (T_1 + T_2 + \dots + T_n)}$$

$$EP(t) = \frac{(t_1 + t_2 + \dots + t_n)}{(T_1 + T_2 + \dots + T_n)}$$

$$EP(t) = \frac{\sum_{i=1}^n t_i}{\sum_{i=1}^n T_i} = D(t)$$

$$EP(t) = \frac{pr_1 \times (t_1 + \dots + t_{n-1})}{Pr_1 \times (T_1 + \dots + T_{n-1})} + \frac{p/r_1 \times (t'_1 + \dots + t'_n)}{P/r_1 \times (T'_1 + \dots + T'_n)}$$

$$pr_i = Pr_i$$

$$p/r_i = P/r_i$$

$$EP(t) = \frac{pr_1 \times (t_1 + \dots + t_{n-1})}{pr_1 \times (T_1 + \dots + T_{n-1})} + \frac{p/r_1 \times (t'_1 + \dots + t'_n)}{p/r_1 \times (T'_1 + \dots + T'_n)}$$

$$EP(t) = \frac{(t_1 + t_2 + \dots + t_n)}{(T_1 + T_2 + \dots + T_n)} + \frac{(t'_1 + t'_2 + \dots + t'_n)}{(T'_1 + T'_2 + \dots + T'_n)}$$

$$EP(t) = \frac{\sum_{i=1}^n t_i}{\sum_{i=1}^n T_i} + \frac{\sum_{i=1}^n t'_i}{\sum_{i=1}^n T'_i} = D(t) + D'(t)$$

System	Efficiency Target	Efficiency Result
UDA	98.0%	100%
UDV	98.0%	100%
UFCC	98.0%	100%
AA	98.0%	100%
DEA	98.0%	100%
CTB	98.0%	95.74%
CCR	98.0%	97.44%
Fractioning	98.0%	99%
Naphtha HDT	98.0%	95.77%
Diesel HDT	98.0%	97.64%

UDA, unit distillation atmospheric; UDV, unit distillation vacuum; UFCC, unit; AA, acid water; DEA, Diethylamine; CTB, cracking treatment; CCR, cracking catalytic; HDT, hydrodesulfurization treatment.

Looking at [Table 4.25](#) we can conclude that the most critical systems are cracking thermal (CTB), cracking catalytic reform (CCR), naphtha, the hydrodesulfurization plant, and the diesel hydrodesulfurization plant because system efficiency is defined by the lowest subsystem efficiency value when subsystems are modeled in series.

For RBD methodology, refinery availability will be lower than the lowest system availability because the systems are in series. The same is true for efficiency. In fact, this is a very conservative assumption, and it can be used to represent complex systems that include all systems, which means that in the case of a shutdown in any system the whole complex system will shut down. In this case, refinery efficiency is lower than 95.77% over the 3-year period. The results will be improved if improvements are implemented in each critical system. However, regarding logistic resources, such as tanks, the plant's unavailability is reduced. This is the RAM + L approach, which considers reliability and logistics to create a complex model, which is different from the RBD approach, where all plants are in series and tanks are in parallel. In the next analysis, improvement actions will be used to compare RAM + L results with RAM methodology results.

### **Critical Analysis and Improvement Actions**

For system results, the CCR, CTB, naphtha, and diesel hydrosulfurization plant are the most critical plants. Therefore improvements are to be done on systems to eliminate failures or reduce the consequences and therefore improve system efficiency and consequently complex system efficiency.

In the CCR plant the most critical equipment is the reactors because of leakage failure modes; therefore the system improvement action is:

- Implement procedures related to pipeline assembly to avoid leakage in such equipment.
- In the CTB plant the most critical equipment is the furnace because of coke formation; therefore the system improvement action is:
  - Reduce decoking time, the online Spalling procedure will be conducted to reduce the time it takes to decoke the furnace to reduce unavailability time.

System	Efficiency Target	Efficiency Result
UDA	98.0%	100%
UDV	98.0%	100%
UFCC	98.0%	100%
AA	98.0%	100%
DEA	98.0%	100%
CTB	98.0%	98.53%
CCR	98.0%	98.26%
Fractioning	98.0%	99%
Naphtha HDT	98.0%	99.05%
Diesel HDT	98.0%	98.56%

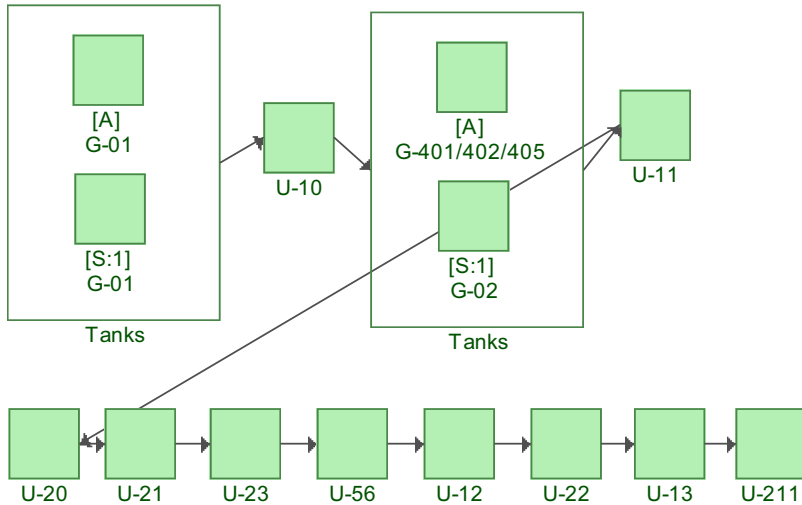
In the naphtha and diesel hydrodesulfurization plant the most critical equipment is the reactors because of leakage failure modes; therefore the system improvement action is:

Implement procedures related to pipelines assembly to avoid leakage in such equipment.

These improvement actions will result in efficiency improvements, as shown in Table 4.26.

After all system improvements it is necessary to create a macrosystem for all plants in series based on RBD methodology. In doing so the macrosystem availability is 93.89% in 3 years, and its configuration is as shown in Fig. 4.113.

This result shows that the refinery will produce 93.89% of total production capacity (3 years). In fact, such a conservative approach requires a RAM + L methodology configuration that will be conducted in the next section for logistic issues (tank) and reliability.



**FIGURE 4.113**

Macrosystem RBD configuration.

**RAM + L Simulation**

The RAM + L methodology considers logistic resources as well as equipment reliability in a complex system modeled by the RBD method. The final results will show the total efficiency in all products for the relation between demand and supply in equipment and systems.

The whole system (refinery) will be represented per actual and future configuration as shown in Figs. 4.114 and 4.115. The actual refinery configuration includes seven tanks and three plants (U-11, U-10, and U-21), and the model is shown in Fig. 4.115.

The future configuration considers seven more plants (U-56, U-23, U-12, U-13, U-22, U-20, and U-211), as shown in Fig. 4.115. In this configuration, the U-56 is in series with U-10, U-11, U-211, and U-21, which means that in the case of unavailability in this type of plant the other plants will shut down.

The second important condition is that PSA in U-22 supplies H<sub>2</sub> to U-12 and U-13. This means that in case of PSA unavailability, U-12 and U-13 will shut down.

The third important condition is that the compressor in U-13 supplies H<sub>2</sub> to the reactors in U-13 and U-12. In the case of compressor (U-13) unavailability both plants will shut down; therefore such a compressor is in series with two plants (U-12 and U-13).

The final complex system efficiency is 100% in 3 years for all products in the actual configuration (tanks, U-10, U-11, and U-21). In the future, final complex system efficiency will vary from 99.14% to 99.86% of total production RBD in 3 years. The result is different from the RBD methodology, which does not consider logistic resources (tanks and pumps) as well as all final products.

**Conclusions**

The RAM analysis methodology includes logistic issues in RAM analysis and it is a more robust assessment of complex systems such as refineries.

To perform such analysis, information about equipment failures is required, and the logical dependency of systems, equipment, and logistic resources has to be defined.

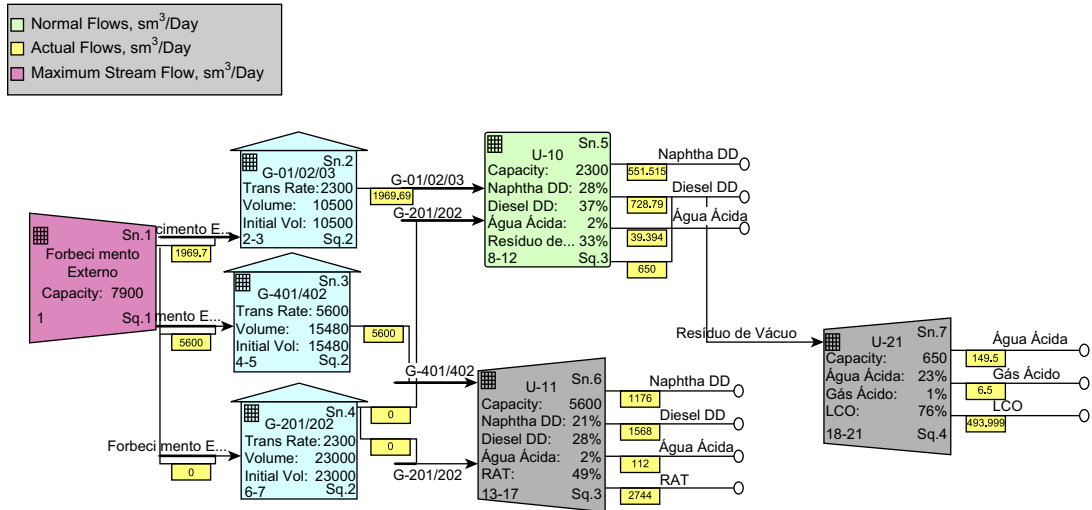
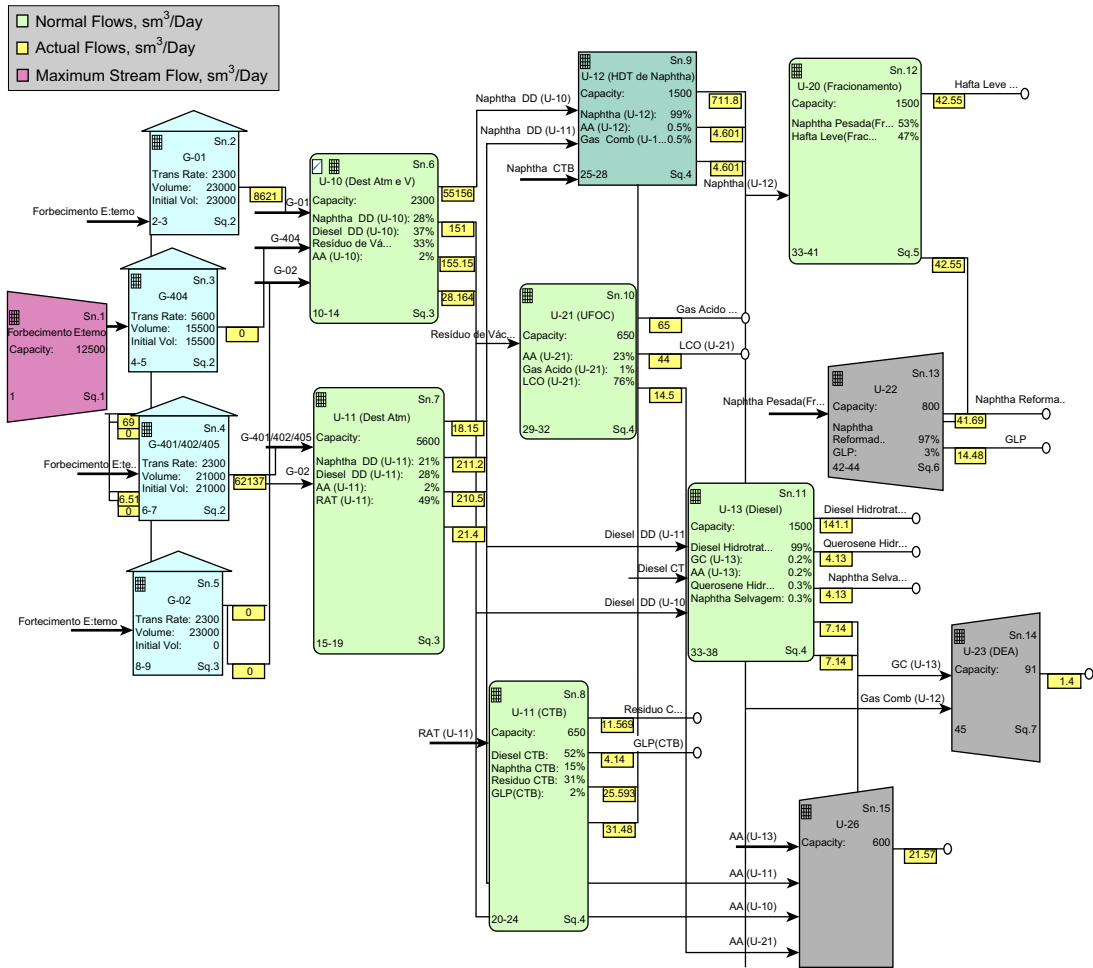


FIGURE 4.114

Actual refinery (RAM + L).



**FIGURE 4.115**  
Actual refinery (RAM + L).

Although it is a more realistic analysis, it is often not because of lack of information or an integrated system vision. In general, two groups of models with different focuses show different results to optimize complex systems.

In general, software usually focuses on system reliability or system logistics, emphasizing one or the other, but without considering both. In case of more focus on reliability issues, the results are more pessimistic. In case of focus on logistical issues, the results are more optimistic because logistic resources like tanks can reduce equipment shutdown impact on plants when there is enough product in stock to supply them while equipment is being repaired.

Software, such as MAROS and BlockSim, focuses on reliability issues.

However, other software focuses more on logistics, such as ARENA and Taro. The best solution is to use software that includes reliability and logistic issues such as Taro and MAROS, use logistics software (eg, ARENA) to consider reliability issues, or use reliability software (eg, BlockSim) to consider logistic issues.

In this case study the logistic issues were simple to represent, but if ships and other logistic resources were considered, modeling of such software would be more difficult. The most important aspect is to consider logistic and reliability issues when complex systems are being assessed to have more reliable optimizations and improvements.

#### 4.6.9 RAM ANALYSIS APPLIED TO DECOMMISSIONING PHASE: COMPARISON AND ASSESSMENT OF DIFFERENT METHODS TO PREDICT FUTURE FAILURES

##### *Introduction*

RAM analysis is a recognized management and engineering discipline for the purpose of guaranteeing the specified functionality of a system over its complete life cycle. RAM analysis also aims to ensure the operation, maintenance, and disposal costs remain below the acceptable level, by establishing the relevant performance characteristics at the beginning of the procurement cycle, and through monitoring and control of their implementation throughout all asset life cycle phases (Vozella et al., 2006).

The general definition of reliability used throughout industry and quoted in many engineering books published on this subject follows the example taken from MIL-STD-785:

**Reliability:** the ability of a product to perform a required function under given conditions for a given time interval.

**Availability:** ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.

**Maintainability:** a state in which an item can perform a required function, when maintenance is performed under given conditions and using stated procedures and resources.

Despite RAM analysis being the most common method utilized by reliability engineers, most of the time the degradation caused by equipment age and maintenance effects is not taken into account. In many cases the reliability data is obtained from a generic database concerning constant failure rate, and the equipment failure rate data obtained is treated as an average (Gerbec, 2010).

The null hypothesis of the homogeneous Poisson process with the alternative being a nonhomogeneous Poisson process is defined by a trend test such as the Laplace test or the Military Handbook test (Lindqvist, 2006).

The degradation effect must be taken into account to represent the increasing number of asset failures during asset wearout. Whenever this type of degradation is not represented by “direct simulation,” the equipment is considered as good as new after repair.

RAM analysis performed concerning the decommissioning phase must take into account the degradation effect to predict the future failures of the assets.

Indeed, nowadays many RAM analyses use data from generic databases (exponential PDF) that in most of the cases will not represent the real performance of the system assessed. In addition, these databases do not consider the restoration factor or the different PDFs that are more applicable to failure modes in the analysis.

This section will now discuss the importance of considering the restoration factor by comparing the RGA (Crow-AMSAA model) and General Renewal Model (GRM) when performing a RAM analysis to predict system performance by applying a case study concerning the decommissioning phase.

### ***RAM Analysis in Decommissioning Phase***

To understand the application of RAM analysis in the asset decommissioning phase it is necessary first to understand the asset management concept, as well as how reliability engineering is applied during the asset life cycle.

Asset management is defined as the best practices applied during the asset life cycle to achieve the best performance result. Indeed, such practices are carried out with the support of a leader at different organizational levels, specifically strategic, tactical, and operational.

Therefore different reliability engineering methods must be used in different asset life cycle phases, as shown in Fig. 4.116. The optimal asset performance is achieved when most early life failures are eliminated during the design phase, which enables excellent performance during the operational phase. This is shown by the green bathtub curve in Fig. 4.116, representing a lower failure rate, or, in other words, higher reliability.

To achieve optimal performance it is necessary to implement different methods throughout the asset life cycle. Indeed, all efforts begin in the design phase, applying different qualitative ((Design Failure Mode Analysis (DFMEA), Reliability centered maintenance (RCM) Risk Based Inspection (RBI), High Accelerated Life Test (HALT), Failure Report Analysis and Corrective Actions System (FRACAS), human reliability) and quantitative (Reliability, availability and maintainability analysis (RAM), Accelerated Life test (ALT), Reliability Growth Analysis (RGA), and warranty analysis) methods. The main objective of these methods is to identify the early life failures during design and eliminate them whenever possible. During the operational phase, different qualitative (Process Failure Mode and Effect analysis (PFMEA), RCM, RBI) and quantitative (LDA and RAM analysis) methods must be utilized to maintain asset performance until the end of asset life, when decommissioning of the equipment is defined and supported by RAM analysis, optimum replacement time (ORT), and RGA.

The ORT for all equipment must be analyzed to reduce operational cost, maintain high availability of the system and below the acceptable risk level for failure.

The decommissioning phase is the most challenging in terms of RAM analysis because it requires different analyses to be performed, such as RGA, the GRM, and the usual LDA during the LDA step to predict the future system performance.

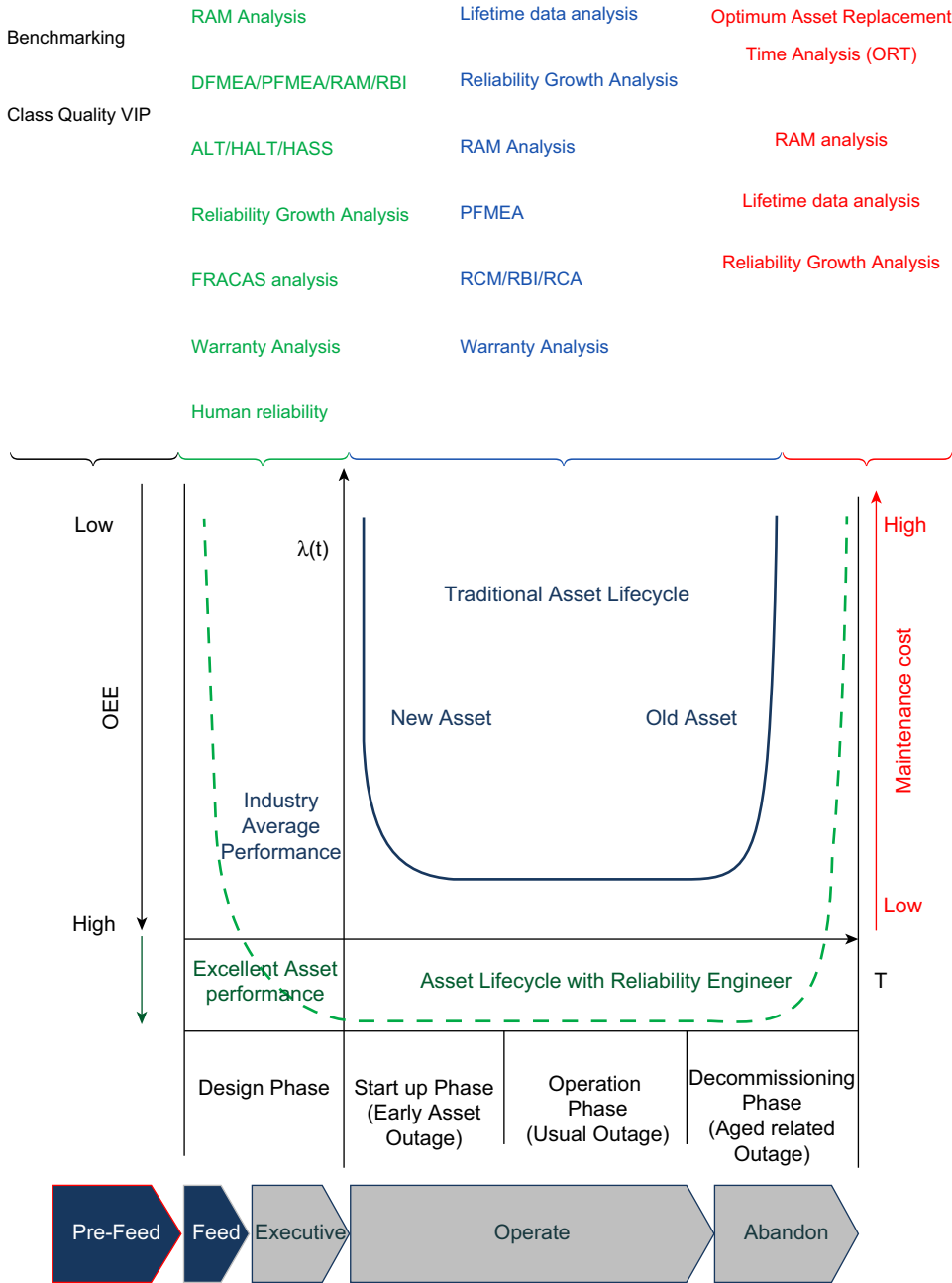
In addition, in some cases it is also important to carry out the ORT analysis to define when it is best to replace equipment based on operational cost analysis. In general terms, the RAM analysis methodology applied for the decommissioning phase can be defined by the steps represented in Fig. 4.117.

Regarding the decommissioning phase, it is very important to take into account the equipment age to predict future failures that will reduce system performance in the decommissioning phase. Therefore it is important to perform the RGA using the Crow-AMSAA method, as well as performing the GRM to accurately predict the expected number of future failures.

Indeed, these methods are applied for single equipment and components, but it is a very important result in comparison with the Monte Carlo simulation result from RAM analysis. In fact, the best approach is to carry out RGA analysis and then adjust the Monte Carlo simulation for each equipment item.

Despite a good approach the software packages that perform system direct simulation (Monte Carlo simulation) have some limitations and are not able to predict the exact expected number of failures predicted by RGA. Indeed, it is possible to take into account the restoration factor predicted by the GRM, but it is only possible to have equipment in the state “as good as new” or “as bad as old.”

Theoretically, this is the best condition that some equipment can achieve in terms of performance after preventive or corrective maintenance, but in some cases it is possible to have reliability growth.



**FIGURE 4.116**

Asset management.

Source: Calixto, E., 2014. Safety science: methods to prevent incident and health damage at the workplace. Bethamscience. (Release in July 2014). <http://www.benthamsience.com/ebooks/forthcomingtitles.htm>.



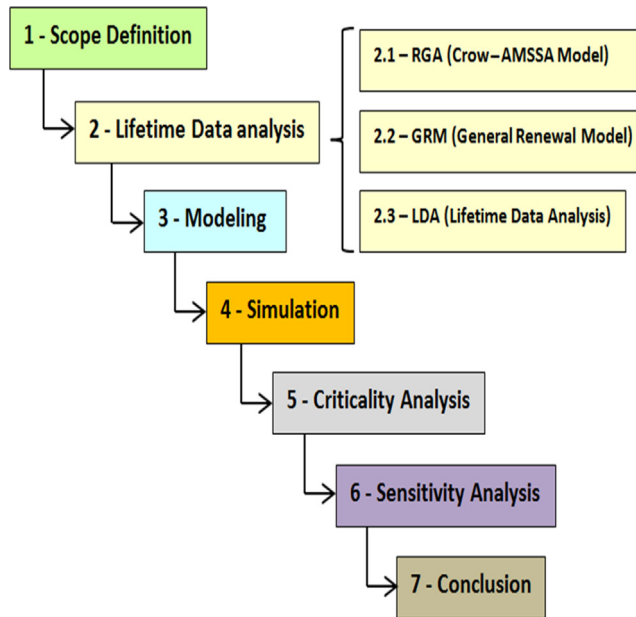


FIGURE 4.117

RAM methodology in the decommissioning phase.

This is achieved by swapping internal components for more reliable ones or even modifications that increase equipment reliability when performed.

### **Reliability Growth Analysis**

The Crow-AMSAA model was introduced by Dr. Larry H. Crow in 1974 to be applied to product improvement assessment during the design phase. Nowadays, this model is also applied during the operational phase of the asset life cycle to assess the equipment degradation over time, as well as the effect of maintenance on repairable equipment to predict future failures.

The Crow-AMSAA is a statistical model that uses the Weibull failure rate function to describe the relationship between accumulated time to failure and test time, being a nonhomogeneous Poisson process model. This approach is applied to demonstrate the effect of corrective and preventive actions on reliability when a product is being developed or for repairable systems during the operation phase (Crow, 2012). Thus whenever improvement is implemented during the test (test—fix—test) or maintenance, the Crow-AMSAA model is appropriate to predict reliability growth and expected cumulative number of failures. The expected cumulative number of failures is mathematically represented by the following equation:

That is approximately:

$$E(N_i) = \int_0^T \rho(t) dt$$

$$E(N) = \lambda T^\beta$$

The Crow-AMSAA model assumes that intensity failure is approximately the Weibull failure rate, thus the intensity of failure on time is:

$$\rho(t) = \frac{\beta}{\eta^\beta} T^{\beta-1}$$

where the initial failure rate is:

$$\lambda = \frac{1}{\eta^\beta}$$

If the cumulative failure rate is approximately failure intensity we have:

$$\lambda_i = \beta \lambda T^{\beta-1}$$

This equation describes the failure intensity during the test and depends on the value increasing, decreasing, or staying constant through time. It is very important to bear in mind that  $\beta$  in the Crow-AMSAA model describes intensity failure behavior and does not have the same meaning as the Weibull PDF shape parameter.

In fact,  $\beta$  is a shape parameter of intensity failure function in the Crow-AMSAA model. Thus in this model when  $\beta > 1$ , reliability decreases through time because failure intensity is increasing. In other words, corrective product actions are not improving the product. When  $\beta < 1$ , intensity of failure decreases through time; in other words, reliability is increasing. Therefore corrective product actions are improving product reliability. When  $\beta = 1$  there is no improvement or product reliability degradation. In this case the product behaves as if no corrective action takes place and intensity failure is constant through time. The growth rate in the Crow-AMSAA model is  $1 - \beta$ .

### **General Renewal Process**

The GRM (Kijima I and II) was proposed by Kijima and Sumita in 1986. The Kijima model, known as the “general renovation process” or “general renewal process,” is based on the component virtual life concept. This method considers the reduction in component age when an intervention is performed; it can be described in two forms:

- Age reestablishment based on last intervention (Kijima I);
- Age reestablishment based on all interventions (Kijima II).

In the first case, the “model Kijima I” assumes that reestablishment of component age occurs only for the last repair. Therefore the model assumes that the “*i*th” repair does not remove all reliability losses until the “*i*th” failure. Therefore if “*t<sub>i</sub>*” is time between failures, the component age through time is represented by the equation:

$$V_n = V_{n-1} + qX_n$$

where  $X_n$  = time between ( $n - 1$ )th and an  $n$ th failure,  $q$  = restoration factor,  $V_n$  = age in time  $n$ , and  $V_{n-1}$  = age in time  $n - 1$ .

In the second case, the “model Kijima II” assumes that reestablishment of component age occurs for all failures throughout component life since the first repair. Thus this model regards that the “*i*th” repair removes all reliability losses until the “*i*th” failure. Therefore the component age through time is represented by the equation:

$$V_n = q(V_n + X_n)$$

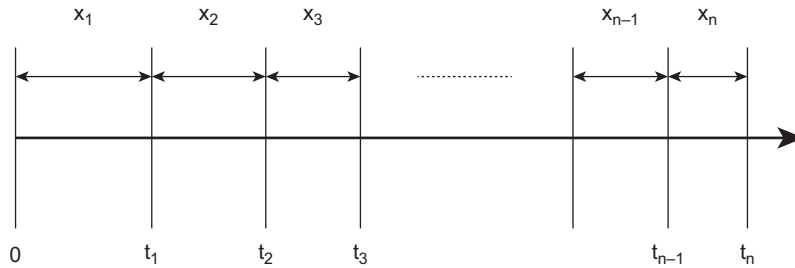


FIGURE 4.118

General Renewal Model.

Fig. 4.118 graphically represents the concept of the GRM, which takes into account the effect on maintenance. The Kijima factor applied in the case study was defined using the software “Weibull 9.0” based on the likelihood method applied in Crow-AMSAA model parameters.

### **Lifetime Data Analysis**

To define equipment, product, and service reliability it is necessary to collect historical failure data and treat it statistically.

Therefore the first step in an LDA study is to know how failures occur through time; this is critical for definition of indexes such as failure rate, reliability, availability, and reliability through time (to support decisions in defining the best time to inspect), and maintenance, to check if equipment achieves the reliability warranty required and to support information on new projects.

Indeed, the decisions based on reliability are based on LDA results. This analysis requires historical data about failure modes and repair time. The failure mode is the way that the equipment or product lost part or all of its capacity to carry out its function.

Therefore understanding the type of data required is the first step in the LDA process. Essentially, the type of data sample can be grouped or not grouped, meaning that reliability is predicted based on only one equipment item or based on a group of similar equipment. In most cases, when equipment from a process plant is being assessed the sample is not grouped because, when comparing the equipment to the sample from a similar process plant, factors such as maintenance policy, operational environment, and process variation affect equipment reliability differently.

Regarding the data it is important to understand how data is recorded. Indeed, the data can be complete, right suspension, left suspension, in the interval, or a combination of such configurations.

The next step is to apply different goodness of fit methods, such as rank regression and maximum likelihood, to estimate the PDF parameters as well as the best PDF that fits the data assessed.

The final product of LDA is the PDF and its parameters that best fit the failure or repair data assessed, as shown in Fig. 4.119.

The PDF describes the possibility of events occurring through time. In equipment life cycle analysis it describes failure or repair time occurrence through time. This provides good information to a maintenance and reliability professional to make decisions regarding maintenance policy, inspection policy, and failure behavior. However, to make these decisions, other indexes are required, such as failure rate and reliability function. Fig. 4.120 summarizes the main steps of LDA.

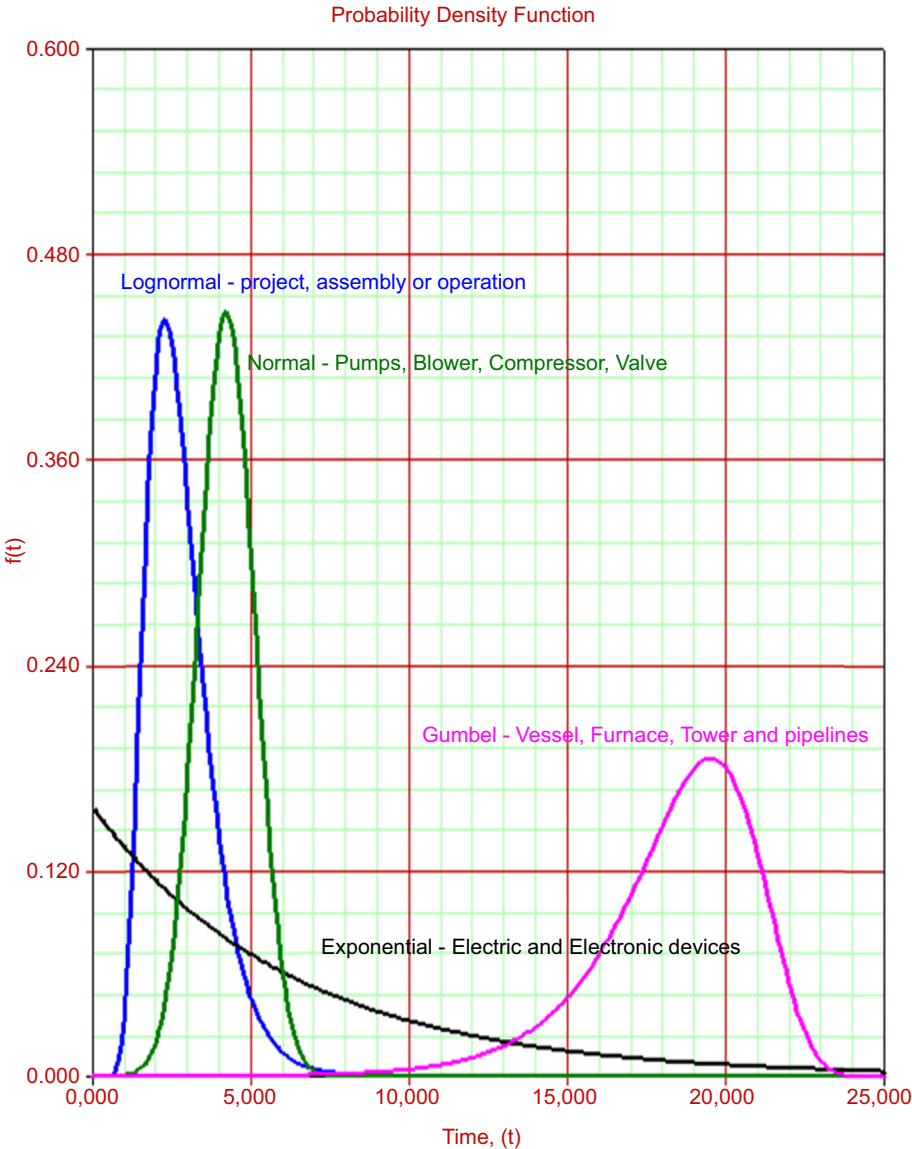
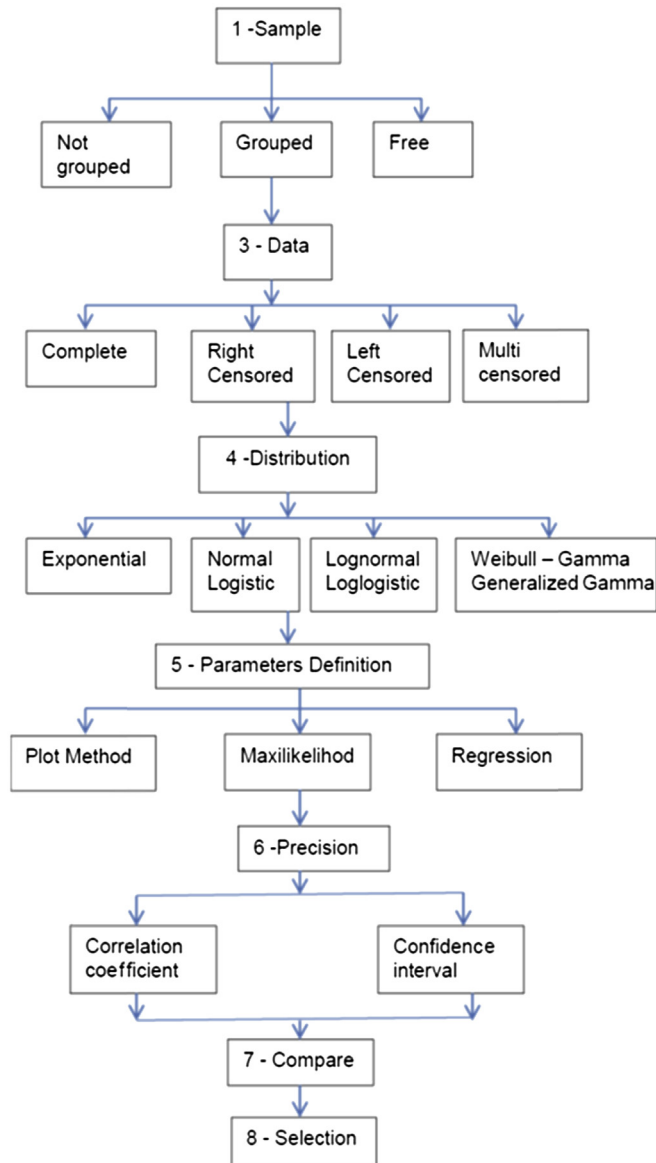


FIGURE 4.119

Oil and gas equipment PDF.

Source: Calixto, E. 2012. Gas and Oil Reliability Engineer: Modeling and Analysis, Elsevier ISBN:9780123919144.


**FIGURE 4.120**

Lifetime data analysis steps.

Despite a very important method, the LDA does not consider the effect of maintenance on equipment degradation. In fact, when applying the PDF parameters of RBD models and then running the direct simulation in RAM analysis, the following events will be similar to the first one.

Therefore it is important to take into account the degradation effect analysis, which is defined by applying the GRM and Crow-AMSAA model, as will be demonstrated in the next section.

### ***Comparing Different Methods***

To predict future failures it is necessary to take into account the positive or negative maintenance and environmental effect on equipment reliability. Therefore RGA can be performed to predict the cumulative number of failures regarding the degradation effect on repairable equipment. The second option is to perform the GRM to predict the restoration factor and apply it to the RBD for each equipment item or failure mode and run the direct simulation.

In the first case, to predict future failures, the RGA (Crow-AMSAA model) is applied to define the improvement or degradation in each equipment item as well as taking into account the effect of corrective and preventive maintenance.

This analysis is the most accurate in predicting future failures because it considers all positive or negative effects on equipment performance.

Certainly, the ideal situation is performing this analysis for each component, but because of a lack of precise information in the historical data archive, the analysis is carried out at the equipment level. Fig. 4.121 shows an example of an RGA carried out for a blower.

The cumulative number of failures during the assessed period is exactly what is recorded on the database. In addition, the beta parameter,  $\beta > 1$ , indicates that the reliability of this blower decreases over time ( $\beta = 1.74$ ).

Similar analyses were carried out for other equipment to define the cumulative number of failures, as well as to evaluate the effect of maintenance and operational environment by assessing the beta parameter value.

Regarding the second option, the GRM, which defines the type of restoration factor (Kijima I or II), can also be applied. Indeed, this analysis might be adjusted to achieve similar results provided by RGA in terms of cumulative number of failures. Considering that the restoration factor is at the maximum, 1 (100% of restoration), some adjustment is necessary when adjusting the GRM based on RGA results. This adjustment is based on the assumption that the RGA represents the best prediction of future failures. Once the equipment needs to be assessed in the context of a system and not individually, it is necessary to define the PDF and restoration factor for each one and then input the values into the RBD model.

Table 4.27 shows an example of the final reliability data as a result of the RGA, GRM, and LDA.

The final step is to validate the reliability database presented in Table 4.27 by performing individual direct simulations (Monte Carlo—MC) to check if the PDF and the restoration factor were adjusted well to the RGA model prediction. Therefore the simulation was performed in 10, 15, and 20 years. Table 4.28 shows an example of future predictions for some equipment, comparing the RGA and MC methods results.

Tank 1 was assessed only through the MC method because the small number of failures does not enable the RGA. The pumps were assessed by both methods and achieved a similar expected number of failures.

Finally, this approach was applied to all boiler systems. Thus it was demonstrated that the PDF and restoration factor were accurate enough to predict future numbers of failures by the MC method, as the RGA method produced similar results. The next section demonstrates the boiler system modeled by RBD and the final direct simulation results.

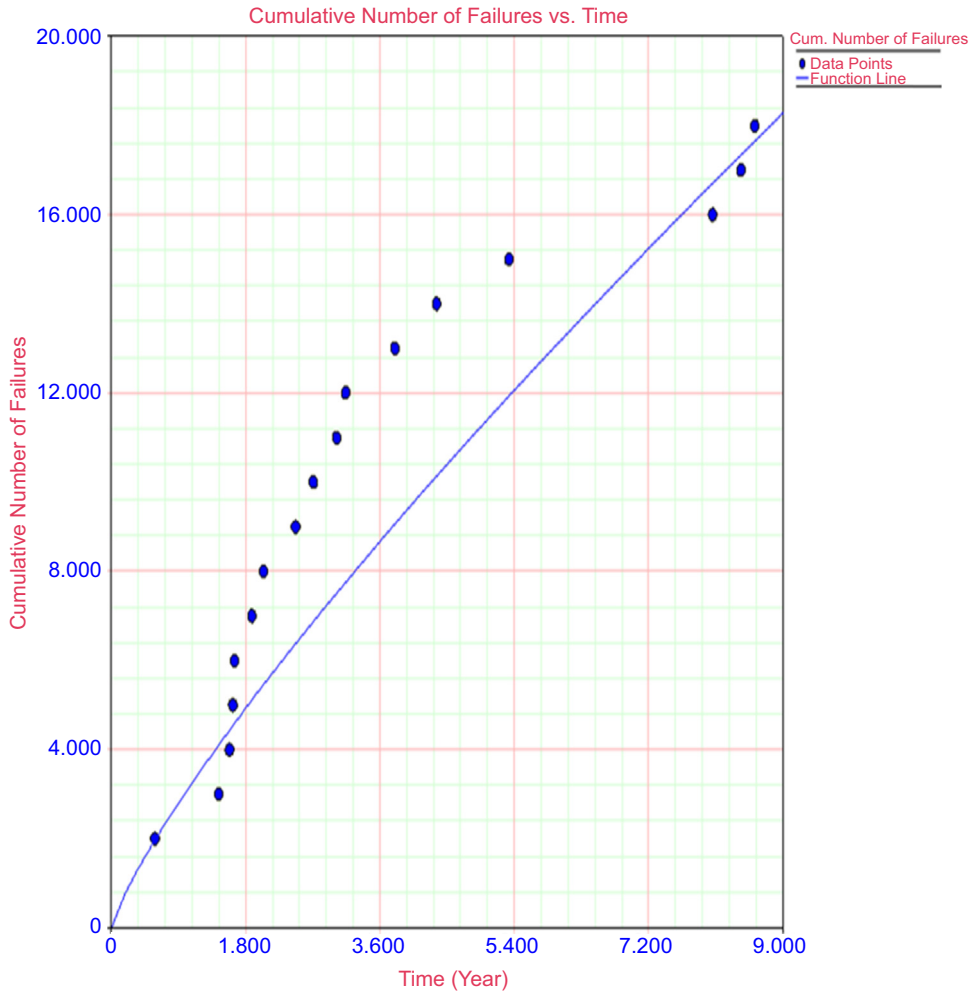


FIGURE 4.121

RGA analysis.

**RAM Analysis in the Decommissioning Phase Case Study**

To demonstrate the importance of all methods described in the previous section, a RAM analysis will be performed to assess the boiler system in the decommissioning phase. The main objective is to define the critical equipment in terms of performance and support decisions about which equipment must be replaced.

In this particular case, the boiler system may cause loss of production in the whole refinery in case of outage during winter time. Therefore RAM analysis took into account the simulation for a specific range of time that, in this case, is winter time.

**Table 4.27 Reliability Database**

Equipment	Failure			Repair		Kijima Factor			Crow-AMSAA Model	
	PDF	Parameter (year)		PDF	Parameter (hours)	Type	q	RF	$\lambda$	$\beta$
Tank 1	PDF 2	Parameter (year)		PDF	Parameter (hours)	Type	q	RF	$\lambda$	$\beta$
	Gumbel	$\mu$   $\sigma$		Normal	$\mu$   $\sigma$					
Pump 2	PDF 2	Parameter (year)		PDF	Parameter (hours)	Type	q	RF	$\lambda$	$\beta$
	Weibull	$\beta$   $\eta$   $\gamma$		Constant	repair time					
Pump 3	PDF 2	Parameter (year)		PDF	Parameter (hours)	Type	q	RF	$\lambda$	$\beta$
	Weibull	$\beta$   $\eta$   $\gamma$		Constant	repair time					
Pump 4	PDF 2	Parameter (year)		PDF	Parameter (hours)	Type	q	RF	$\lambda$	$\beta$
	Weibull	$\beta$   $\eta$   $\gamma$		Constant	repair time					
Pump 5	PDF 2	Parameter (year)		PDF	Parameter (hours)	Type	q	RF	$\lambda$	$\beta$
	Weibull	$\beta$   $\eta$		Constant	repair time					
	PDF 2	Parameter (year)		PDF	Parameter (hours)	Type	q	RF	$\lambda$	$\beta$
	Weibull	$\beta$   $\eta$		Constant	repair time					



**Table 4.28 RGA × MC**

Equipment	10 Years		15 Years		20 Years	
	MC	RGA	MC	RGA	MC	RGA
Tank 1	1		1.99		2	
Pump 2	9.7	8.89	14.09	10.98	18.3	12.76
Pump 3	4.24	3.15	6.44	4.28	8.56	5.28
Pump 4	15.37	12.88	22.6	19.3	29.91	25.27
Pump 5	9.06	8.87	13.23	12.13	17.42	15.24

RGA, reliability growth analysis; MC, Monte Carlo.

In addition, the LDA, RGA, and GRM are part of the RAM module in the decommissioning phase. Once the LDA step is complete the following step is to model the RBD and perform the direct simulation.

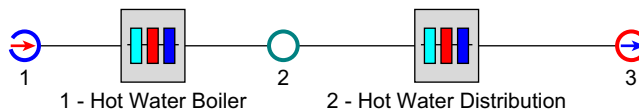
Fig. 4.122 shows the boiler system RBD (RBD BQR software), which basically has two subsystems that are Hot Water Boiler and Hot Water Distribution.

The hot water boiler subsystem is represented by the RBD (RBD BQR software) in Fig. 4.123. In this case all equipment has a standby configuration that enables a high operational availability. Despite high operational availability the operational cost is high because of the number of failures in such equipment.

Fig. 4.124 shows the hot water distribution subsystem RBD (RBD BQR software), which has pipes 1, 7, and 8 as the most critical in terms of boiler system unavailability.

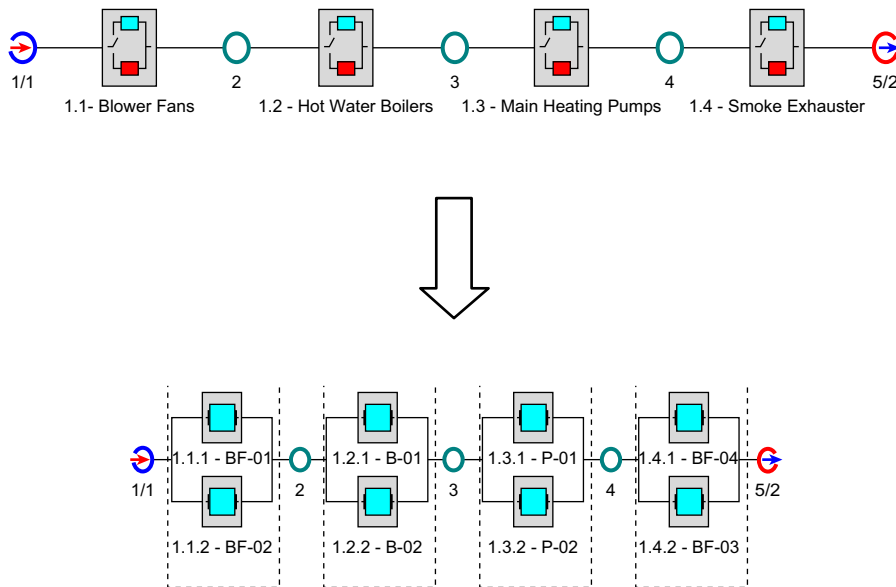
After modeling the system the next step is to carry out the direct simulation (MC). In this particular case, for the cumulative time in 8 years, the boiler has 97.48% of operational availability. The most critical equipment is pipes 1, 7, and 8 because they present the lower operational availability that is 97%, 97.1%, and 97.4%, respectively.

Based on simulation results, the future loss of production was predicted based on failure on critical pipes (1, 7, and 8). The simulation to predict future loss of production regarded that once the pipes fail during the winter such pipes will be out until the end of the winter. This is a worst case scenario, as shown in Fig. 4.125. From the top to the bottom, the first red line represents pipe 1 shutdown during the



**FIGURE 4.122**

Boiler system.



**FIGURE 4.123**

Hot water boiler subsystem.

winter time. The second red line shows the impact of such failure in the boiler system that will be unavailable during the winter once pipe 1 shuts down.

Based on boiler system direct simulation, the chance of having such pipe failure during the winter time is 60%. Such probability regards all types of failures on pipes. In case of corrosion, the probability reduces to 10%.

The sensitivity case regarding new subsystems was carried out and in this case, the operational availability will achieve 99.92% for the next 5 years if the hot water boiler remains as bad as old. If all critical equipment are replaced for new ones the system operational availability will be 100% in the next 5 years.

The important aspect related to decisions in the decommissioning phase is the ORT assessment, which defines when each equipment item must be replaced because of the increase in operational cost. Regarding this analysis, the boilers must be replaced at 2.34 years because despite not causing an impact on system operational availability because of standby configuration the operational cost will increase in time, as shown in Fig. 4.126.

### **Conclusion**

The main objective of this section was to demonstrate the importance of RAM analysis to support decisions regarding asset improvement during the decommissioning phase.

In addition, the section has demonstrated the importance of restoration factors in predicting the future failures of assets that require additional models such as the GRM and Crow-AMSAA model.

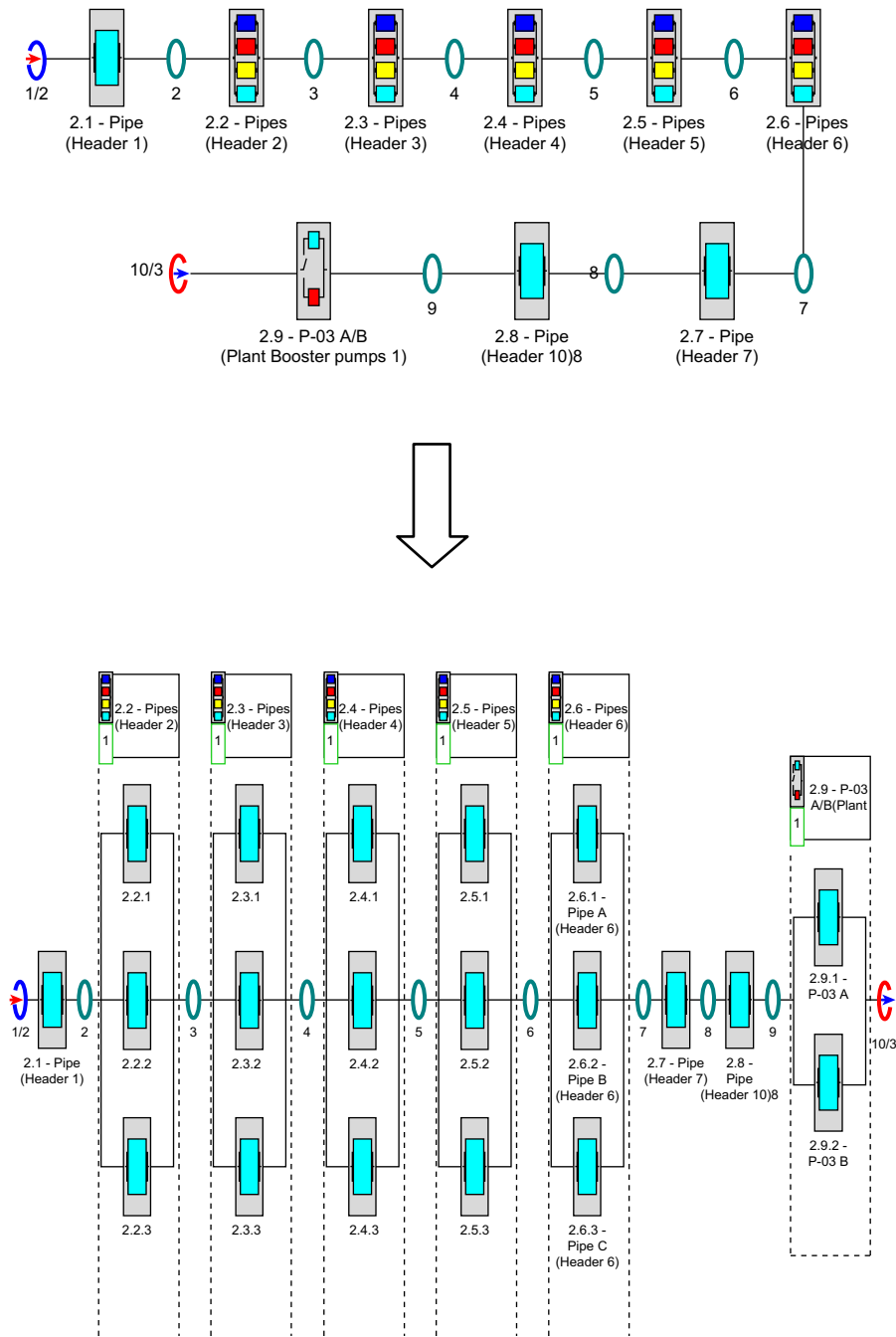
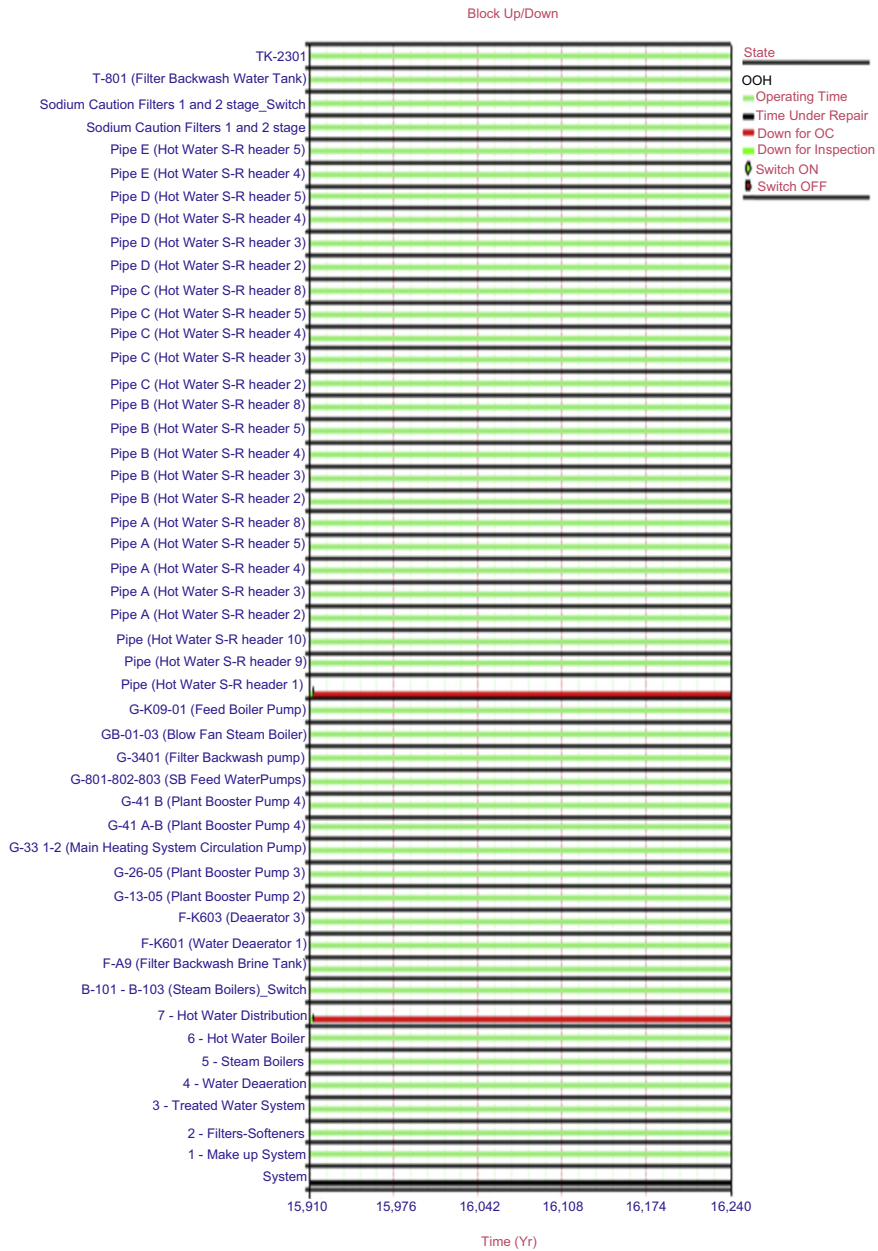


FIGURE 4.124

Hot water distribution subsystem.



**FIGURE 4.125**

Loss of production during winter.

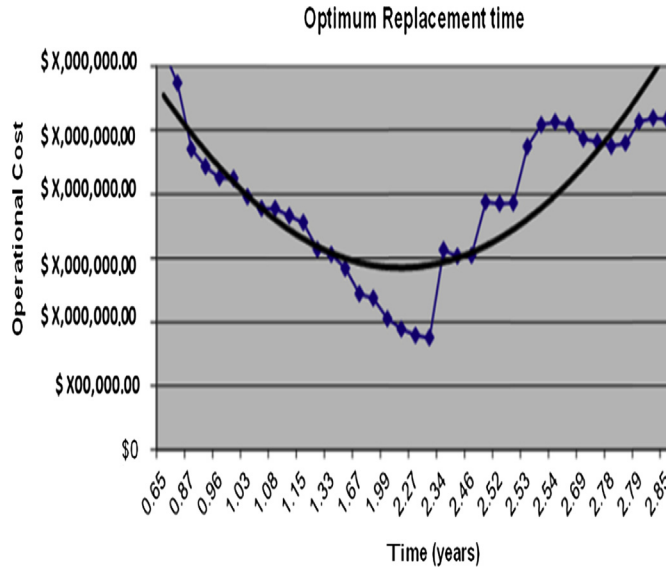


FIGURE 4.126

Optimum replacement time—water boiler.

Direct simulation (MC) and Crow-AMSAA model were compared and demonstrated similar results related to equipment future failure prediction. It is important to highlight that it is only possible when the restoration factor in direct simulation and the PDF as well as restoration factory are adjusted to predict the similar number of failures obtained with the Crow-AMSAA method.

In this particular case study, the simulation during a specific period of time (winter) allows prediction of the loss of production. These model characteristics are not present in all software packages, but must be considered as an opportunity to improve, to enable simulations for a specific period of time.

The decommissioning phase is critical in the asset life cycle and an accurate decision about which equipment must or must not be replaced should be supported by the best reliability engineering methods.

The ORT method is not applied in many cases and must be considered in the decommissioning phase for all equipment, even for equipment that does not have a direct impact on system availability in the event of failure. In many cases the operational cost increases with time, making the asset inefficient from an economic point of view.

#### 4.6.10 RAM ANALYSIS DURING THE DESIGN PHASE: THE BEST PLATFORM OFFSHORE CONFIGURATION CASE STUDY

##### *Introduction*

Producing hydrocarbons in deep water offshore requires subsea and topside assets such as different types of platform.

Subsea wells have been used in support of fixed installations as an alternative to satellite or minimum facility platforms for recovering reserves located beyond the reach of the drill string or used

in conjunction with floating systems such as floating production, storage and offloading (FPSO) units and floating production systems (FPSs).

Platform applicability should be accessed in the context of field development planning and concept selection for any specific offshore project. Basically, the types of platforms are follows:

- Fixed platform;
- Semisubmersible platform;
- FPSO;
- Floating storage and offloading (FSO) system;
- Floating storage unit (FSU);
- Floating liquefied natural gas (FLNG).

A fixed platforms are built on concrete or steel legs, or both, anchored directly to the seabed, supporting a deck with space for drilling rigs, production facilities, and crew quarters. Such platforms are, by virtue of their immobility, designed for very long-term use (for instance, the Hibernia platform). Fixed platforms are economically feasible for installation in water depths up to about 520 m.

The semisubmersible platform has hulls (columns and pontoons) of sufficient buoyancy to cause the structure to float, but of weight sufficient to keep the structure upright. Semisubmersible platforms can be moved from place to place and can be ballasted up or down by altering the amount of flooding in buoyancy tanks. Semisubmersibles can be used in water depths from 60 to 3000 m (200–10,000 ft).

The FPSO consists of large monohull structures, generally (but not always) ship shaped, equipped with processing facilities. These platforms are moored to a location for extended periods, and do not actually drill for oil or gas.

The FSO or FSU is used exclusively for storage purposes, and hosts very little process equipment. This is one of the best sources of floating production.

The FLNG facility refers to water-based liquefied natural gas (LNG) operations employing technologies designed to enable the development of offshore natural gas resources.

Depends on the type of oil reservoir, different configuration of platform is required to maximize the production.

This case study will demonstrate the prediction of platform performance based on predefined configurations as well as sensitivity cases of different possible configurations to maximize the platform performance.

### ***Methodology***

The RAM analysis methodology can be described step by step. First, the system is modeled considering failure and repair data and later is simulated to evaluate the results. Then, improvement solutions are proposed. Based on such considerations, to conduct RAM analysis methodology you must define the scope, perform repair and failure data analysis, model the system RBD, conduct direct system simulation, perform critical system analysis, perform system sensitivity analysis, and then draw conclusions. The RAM analysis methodology is shown in [Fig. 4.127](#).

### ***Lifetime Data Analysis***

LDA, regarding historical failure data of operational assets, has the advantage of having more realistic data when compared to a generics database such as OREDA. Thus, looking at the failure and repair

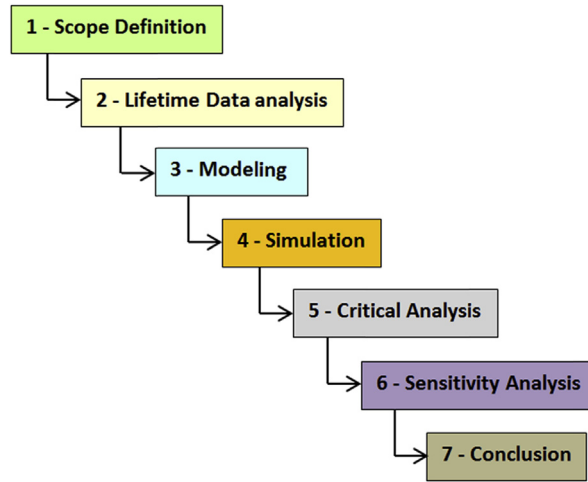


FIGURE 4.127

RAM analysis methodology.

equipment files, it was possible to collect data and perform life cycle analysis in statistic software (Weibull++ 7, Reliasoft) to define PDF parameters for each failure mode in this case study.

To ensure the accurate representation of such data, maintenance professionals with knowledge of such equipment took part in this stage.

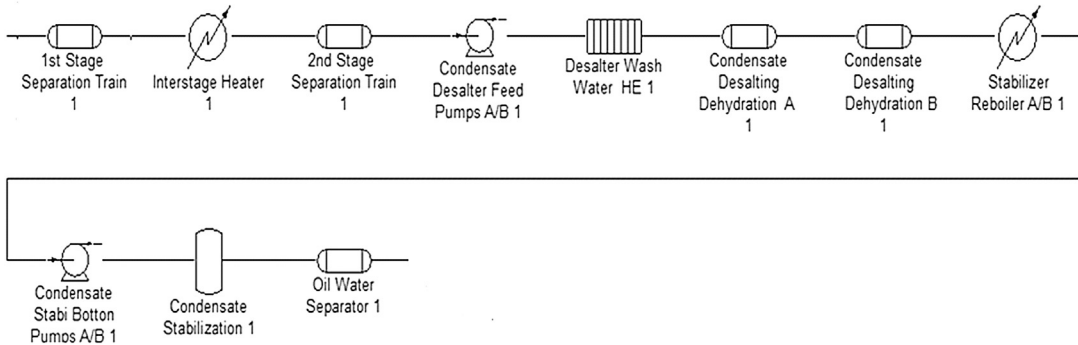
Table 4.29 shows some examples of LDA results applied in the RBD model.

**Modeling**

In order to model the offshore system it is necessary to define the assets boundaries defined in asset management scope for this phase. In this case, the RAM analysis is being applied during the concept

Table 4.29 Lifetime Data Analysis PDF Result							
Equipment	Source Information	PDF	Failure (years)		PDF	Repair (hours)	
			$\mu$	$\sigma$		$\mu$	$\sigma$
ESDV	Company data	Normal	3.5	0.5	Normal	8	4
Compressors	Company data	Normal	3.5	0.5	Normal	84	26
Pumps	Company data	Normal	3.0	0.5	Normal	28	4
Vessel (drum, scrubber, column)	Company data	Gumbel	25	1	Normal	136	22
Heat exchanger (air cooler and shell and tube)	Company data	Normal	9	1	Normal	136	22

PDF, probability density function; ESDV, emergency shutdown valve.



**FIGURE 4.128**

Separation train.

development phase. Therefore, the assessment will be carried out concerning equipment level. In fact, depends on asset life cycle, different details about the equipment assets take place in the RAM analysis. In the end of design phase for example, it's possible to include the component details for each equipment into RAM analysis. The asset scope encompasses the offshore platform and utilities systems.

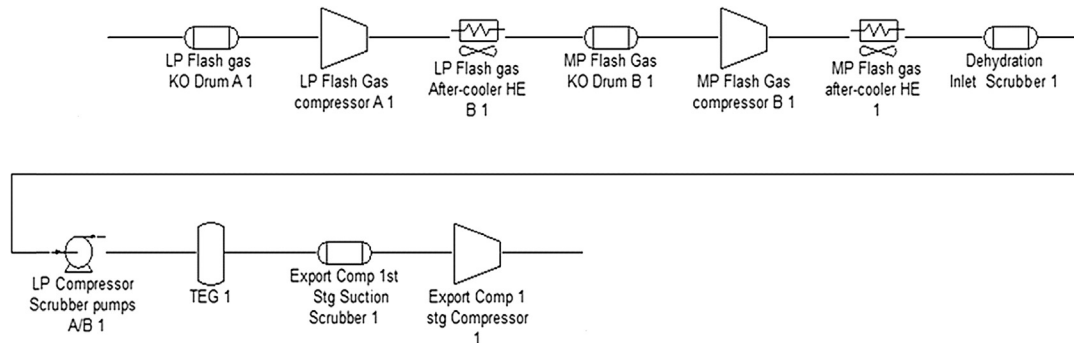
The platform system encompasses the following as:

- Feed
- Separation
- Recompression
- Water treatment

Fig. 4.128 shows the separation train represented by RBD configuration.

Fig. 4.129 shows the recompression train represented by RBD configuration.

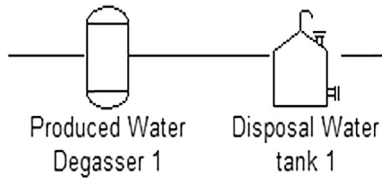
Fig. 4.130 shows the water treatment train represented by RBD configuration.



**FIGURE 4.129**

Recompression train.





**FIGURE 4.130**

Water treatment.

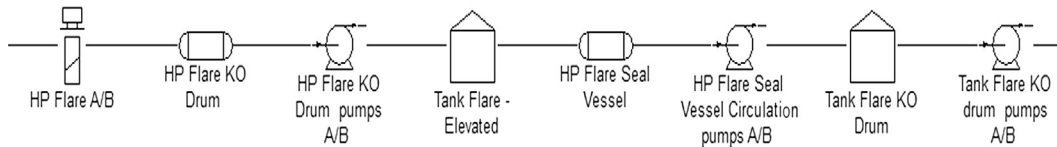
In addition to the platform asset the critical utility system encompasses the following as:

- Flare
- Medium heating
- Instrument air

Fig. 4.131 shows the flare system represented by RBD configuration.

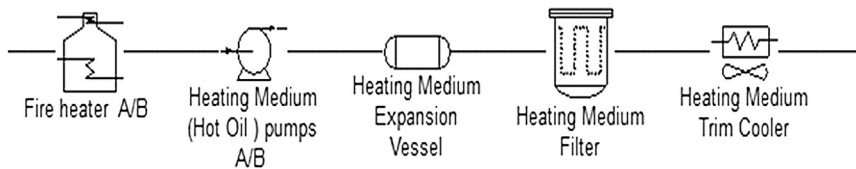
Fig. 4.132 shows the medium heating represented by RBD configuration.

Fig. 4.133 shows the instrument air represented by RBD configuration.



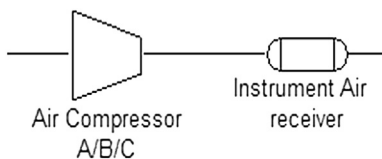
**FIGURE 4.131**

Flare system.



**FIGURE 4.132**

Medium heating.



**FIGURE 4.133**

Instrument air.

<b>Facility</b>	<b>Production Efficiency</b>	<b>Operational Availability</b>	<b>Reliability</b>
Platform	98.33%	98.88%	20%
<b>Utilities</b>	<b>Production Efficiency</b>	<b>Operational Availability</b>	<b>Reliability</b>
Instrument and plant air	98.78%	99.99%	99.99%
Heating medium	98.64%	98.89%	97.5%
Flare-vent system	99.99%	99.99%	99.99%
Facility + utility	98.14%	99.97%	17%

### **Simulation**

Simulation creates typical life cycle scenarios for proposed systems, with Monte Carlo simulation methodology. The entire asset was modeled through RBDs, considering the redundancies in each piece of equipment or system configuration. The simulation was conducted for 10 years and 1000 tests were run to converge results. The production efficiency, operational availability, and reliability achieved in 5 years are, respectively, 98.14%, 99.97%, and 17%. In addition, 12.52 failures are expected in 5 years. The specific performance of each individual system is demonstrated in [Table 4.30](#). This system configuration considers two trains of separation and two trains of recompression with 50% of total capacity.

The production efficiency and operational availability target are, respectively, 98% and 99%, which requires analysis of the critical equipment and, furthermore, to perform sensitivity analysis to improve the performance indexes if possible.

### **Criticality Analysis**

The critical analysis defines which are the most critical subsystems and equipment with the most influence on production losses. The global relative loss means the percentage of total production loss and the downtime impact means the percentage of the total downtime loss. [Table 4.31](#) shows the critical equipment based on global relative loss and downtime impact.

The other index that must be used as a reference to define improvement actions in critical equipment is the availability rank index, and, in the platform system case, the equipment configuration in the RBD because the equipment in parallel has no 100% unavailability effect on the whole system. Even in cases of partial effect, like the compressors presented in [Table 4.32](#), this index will indicate critical equipment to be monitored for the achievement of the target.

[Table 4.32](#) shows the equipment with the lowest operational availability. All other equipment has higher operational availability than 98.69%, which shows that the compressor is the most critical equipment.

### **Sensitivity Analysis**

After critical analysis, it becomes clear that it is mandatory to implement the improvements in some equipment to achieve the performance indexes target whenever it is possible. In addition, the other

<b>Equipment</b>	<b>Global Relative Loss (%)</b>	<b>Downtime Impact (%)</b>
Export compressor 1 Stg train 2	15.75	15.87
Export compressor 1 Stg train 1	15.53	15.30
Low-pressure flash gas compressor train 1	15.83	11.60
Low-pressure flash gas compressor train 2	15.58	11.25
Middle-pressure flash gas compressor train 1	15.37	10.18
Middle-pressure flash gas compressor train 2	15.38	10.53
<b>Total</b>	<b>93.48</b>	<b>64.30</b>

1 Stg, *first stage*.

<b>Equipment</b>	<b>Operational Availability Rank (10 years) (%)</b>
Export compressor 1 Stg train 1	98.69
Export compressor 1 Stg train 1	98.69
Low-pressure flash gas compressor train 1	98.69
Low-pressure flash gas compressor train 2	98.69
Middle-pressure flash gas compressor train 1	98.69
Middle-pressure flash gas compressor train 2	98.69

1 Stg, *first stage*.

possibility is to test different system configurations. The tradeoff of reliability improvement need spares configuration needs to take into account the impact of LCC, the feasibility of performance achievement, and the time to implement and develop more reliable equipment. In this specific case, the reliability index definition for each equipment is considered very high based on the company database, which shows the highest reliability performance for each equipment. Therefore the solution was to model different asset configurations to compare the performance achieved in 10 years. The following configurations were considered as baseline to decide the best configuration to be implemented:

- Two separations and decompression trains with 50% of capacity each one;
- Three separations and decompression trains with 33.33% of capacity each one;
- One separation and decompression trains with 100% of capacity each one.

<b>Table 4.33 Asset Performance by Year</b>			
<b>Asset Performance Prediction (10 years)</b>			
<b>Year</b>	<b>Production Efficiency by Configuration</b>		
	<b>1 × 100</b>	<b>2 × 50</b>	<b>3 × 50</b>
1	98.89%	99.99%	98.79%
2	98.87%	98.88%	98.88%
3	98.09%	98.55%	98.77%
4	95.62%	96.35%	98.49%
5	97.67%	97.83%	98.43%
6	97.47%	97.94%	98.41%
7	97.13%	97.98%	99.99%
8	96.34%	98.97%	98.89%
9	96.81%	97.88%	98.89%
10	96.11%	98.89%	98.89%
Average production efficiency	97.30%	98.33%	98.84%

Table 4.33 shows the asset performance sensitivity case comparison.

Based on the results of Table 4.33 the best result is achieved by the configuration 3 × 50% trains (separation and recompression), although such configuration increases the operational cost by increasing the maintenance and inspection cost as well as the acquisition cost. To improve the configuration 2 × 50%, preventive maintenance will be implemented. The preventive maintenance and inspection for the main platform equipment were defined as follows:

- Test and inspection for all vessels and tanks in each 5 years;
- Schedule maintenance for compressor in each 3 years;
- Schedule maintenance for critical valves for each 2.5 years;
- Predictive maintenance and monitoring online for all pumps during life cycle operation. It is expected to detect pump failures over 2.5 years;
- Monitoring online for all compressors. It is expected to detect compressor failures after 3 years.

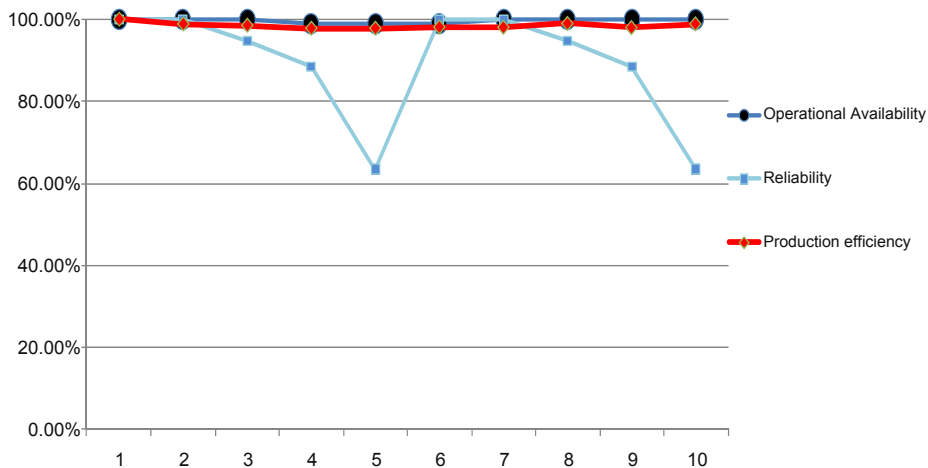
Based on the limitation of RAM analysis software by simulating the effect of predictive maintenance and online monitoring, the main assumption considered in the model is that all equipment will achieve the warranty target, which will mean no failures before the defined schedule maintenance.

By implementing such preventive maintenance policies, the effect of asset performance is to increase the production efficiency, operational availability and maintain high reliability. The performance of the asset after the implementation of preventive maintenance is described in Table 4.34.

The average operational availability and production efficiency are 99.69% and 98.52%, respectively. Such a positive effect of preventive maintenance on asset performance improves

Years	Operational Availability	$R(t)$	Production Efficiency
1	99.99%	100%	99.99%
2	99.99%	99.90%	98.88%
3	99.99%	94.80%	98.55%
4	98.98%	88.50%	97.85%
5	98.98%	63.40%	97.83%
6	98.99%	100%	98.14%
7	99.99%	99.90%	98.08%
8	99.98%	94.80%	98.97%
9	99.98%	88.50%	97.98%
10	99.98%	63.40%	98.89%

performance by reducing the downtime caused by corrective maintenance. In fact, the downtime related to preventive maintenance in many cases is similar to the downtime caused by the corrective maintenance. What is avoided by preventive maintenance is the logistic delays caused when corrective maintenance needs to be implemented. The additional positive effect of preventive maintenance is reliability recovery, which reduces the risk of failure and unexpected system shutdown, as shown in Fig. 4.134.



**FIGURE 4.134**

Asset performance after preventive maintenance by years.

### Conclusion

RAM analysis is a powerful reliability engineering, quantitative method, which supports oil and gas asset projects by taking better decisions about asset configuration and the effect of such configuration on asset performance. The main advantages demonstrated in this case study to implement RAM analysis during the design phase in the oil and gas industry were:

- To predict asset performance, such as production efficiency, operational availability, and reliability;
- To define the critical equipment that impacts on asset performance;
- To define the minimum reliability requirement to be achieved during warranty time to enable the asset to achieve the performance target;
- To enable different asset configuration performance;
- To analyze the effect of preventive maintenance policy on asset performance.

As far as the design specification of different equipment is defined, a more detailed RAM analysis must be performed based on top-level RAM analysis. In addition, once the equipment configuration is defined, the maintenance policies in component level must be defined as well. In this case, the RCM analysis is a very good approach to define detailed maintenance tasks based on component failure modes. The result of the RCM analysis will be the confirmation of the maintenance task defined in the previous phase and additional maintenance tasks. Furthermore, such maintenance task must be input in RAM analysis, which will be carried out in component level, to predict the effect of such tasks on system performance.

---

## REFERENCES

- Bot, Y., Asoulay, D., September 1, 2014. In: Asset Maintenance Optimization: The Case-study of an Offshore Wind Farm. ESREL 2014. CRC Press, ISBN 9781138026810.
- Calixto, E., Carneiro, L., Alves, A.C., 2010. RAM + L analysis: A case study in Brazilian refinery. Esrel 2010, Rhodos, Greece. Reliability, Risk and Safety – Ale, Papazoglou & Zio (eds) © 2010 Taylor & Francis Group, London. ISBN 978-0-415-60427-7.
- Calixto, E., 2012. Gas and Oil Reliability Engineer: Modeling and Analysis. Elsevier, ISBN 9780123919144.
- Calixto, E., 2014. Safety science: methods to prevent incident and health damage at the workplace. Bethamsience (Release in July 2014). <http://www.benthamsience.com/ebooks/forthcomingtitles.htm>.
- Crow, L.H., 2008. A Methodology for Managing Reliability Growth during Operational Mission Profile Testing Copyright © 2008 IEEE. Reprinted from “2008 PROCEEDINGS Annual RELIABILITY and MAINTAINABILITY Symposium,” Las Vegas, Nevada, USA. January 28-31.
- Crow, L.H., 2012. Reliability Growth Planning, Analysis and Management. International Applied Reliability Symposium, Warsaw, Poland.
- Gerbec, M., 2010. Case Study: Reliability Analysis of Natural-gas Pressure-regulating Installation. Taylor & Francis Group, London, ISBN 978-0-415-60427-7.
- Gustafsson, E., 2010. Maintenance Optimization in Stochastic Multi-component Systems. Thesis for the Degree of Master of Science. Department of Mathematical Sciences Division of Mathematics Chalmers University of Technology SE-412 96 Geoteborg, Sweden. August 2010.
- Lindqvist, B.H., 2006. On the statistical modeling and analysis of repairable system. Statistical Science 21, 532–551.
- Vozella, A., Gigante, G., Travascio, L., Compare, M., 2006. RAMS for aerospace: Better early or late than never. ESREL. Safety and Reliability for Managing Risk –Taylor & Francis Group, London. ISBN 0-415-41620-5.

---

**BIBLIOGRAPHY**

- Calixto, E., Schimitt, W., 2006. Cenpes II project RAM analysis. In: ESREL 2006, Estoril. Safety and Reliability for Managing Risk—Guedes Soares & Zio (eds) © 2006 Taylor & Francis Group, London, ISBN 0-415-41620-5.
- Calixto, E., 2006. The enhancement availability methodology: a refinery case study. In: ESREL 2006, Estoril. Safety and Reliability for Managing Risk—Guedes Soares & Zio (eds) © 2006 Taylor & Francis Group, London, ISBN 0-415-41620-5.
- Calixto, E., 2007a. Sensitivity analysis in critical equipments: the distillation plant study case in the Brazilian oil and gas industry. In: ESREL 2007, Stavanger. Risk, Reliability and Societal Safety—Aven & Vinnem (eds) © 2007 Taylor & Francis Group, London, ISBN 978-0-415-44786-7.
- Calixto, E., 2007b. Integrated preliminary hazard analysis methodology regarding environment, safety and social issues: the platform risk analysis study. In: ESREL 2007, Stavanger. Risk, Reliability and Societal Safety—Aven & Vinnem (eds) © 2007 Taylor & Francis Group, London, ISBN 978-0-415-44786-7.
- Calixto, E., 2007c. The safety integrity level as hazop risk consistence. The Brazilian risk analysis case study. In: ESREL 2007, Stavanger. Risk, Reliability and Societal Safety—Aven & Vinnem (eds) © 2007 Taylor & Francis Group, London, ISBN 978-0-415-44786-7.
- Calixto, E., 2007d. Dynamic equipments life cycle analysis. In: 5<sup>o</sup> International Reliability Symposium SIC 2007, Brazil.
- Calixto, E., Rocha, R., 2007. The non-linear optimization methodology model: the refinery plant availability optimization case study. In: ESREL 2007, Stavanger. Risk, Reliability and Societal Safety—Aven & Vinnem (eds) © 2007 Taylor & Francis Group, London, ISBN 978-0-415-44786-7.
- Calixto, E., Michael, S.S., 2011. The optimum replacement time considering reliability growth, life cycle and operational costs. In: ARS 2011, Amsterdam.
- Droguett, E.L., 2007. Avaliação bayesiana da eficácia da manutenção via processo de renovação generalizado. Pesquisa Operacional 27 (3). Rio de Janeiro.
- Kececioglu, D., Sun, F.-B., 1995. Environmental Stress Screening — Its Quantification, Optimization and Management. Prentice Hall PTR, New Jersey.
- Lafraia, J.R.B., 2001. Manual de Confiabilidade, Manutenibilidade e Disponibilidade, Qualimark. Petrobras, Rio de Janeiro.
- ReliaSoft Corporation, Blocksim++ 7.0 Software Package, Tucson, AZ. [www.Weibull.com](http://www.Weibull.com).

## HUMAN RELIABILITY ANALYSIS

**CHAPTER OUTLINE**

<b>5.1 Introduction .....</b>	<b>472</b>
5.1.1 Human Reliability Concepts .....	473
<b>5.2 Technique for Human Error Rate Prediction (THERP).....</b>	<b>476</b>
<b>5.3 Operator Action Tree (OAT).....</b>	<b>482</b>
<b>5.4 Accident Sequence Evaluation Program (ASEP).....</b>	<b>485</b>
5.4.1 Pre-Accident Analysis Methodology .....	485
5.4.2 Post-Accident Analysis Methodology .....	491
<b>5.5 Human Error Assessment Reduction Technique (HEART) .....</b>	<b>495</b>
<b>5.6 Sociotechnical Analysis of Human Reliability (STAH-R) .....</b>	<b>500</b>
<b>5.7 Standardized Plant Analysis Risk-Human Reliability (SPAR-H).....</b>	<b>504</b>
<b>5.8 Success Likelihood Index Methodology Implemented Through Multi-Attribute Utility Decomposition (SLIM-MAUD).....</b>	<b>510</b>
<b>5.9 Systematic Human Error Reduction and Prediction Approach (SHERPA) .....</b>	<b>512</b>
<b>5.10 Bayesian Network.....</b>	<b>514</b>
<b>5.11 Case Study.....</b>	<b>519</b>
5.11.1 THERP Case Study Application.....	520
5.11.2 OAT Case Study Application .....	521
5.11.3 SPAR-H Case Study Application .....	523
5.11.4 HEART Case Study Application.....	525
5.11.5 STAH-R Case Study Application.....	527
5.11.6 SLIM-MAUD Case Study Application .....	532
5.11.7 Bayesian Network Application.....	535
5.11.8 Methodologies Comparison .....	538
5.11.9 Conclusion.....	539
<b>5.12 Human Error Impact on Platform Operational Availability .....</b>	<b>540</b>
5.12.1 Human Error Assessment During Commissioning Phase .....	540
5.12.2 Human Error Effect on Platform System Operational Availability.....	540
5.12.3 Conclusion.....	545
<b>5.13 ESDV (Emergency Shutdown Valve): Operational Human Error Analysis .....</b>	<b>545</b>
5.13.1 ESDV Shutdown Case Study .....	545



5.13.2 SPAR-H.....	547
5.13.3 SPAH-R: Commission Error Probability.....	550
<b>References .....</b>	<b>551</b>

---

## 5.1 INTRODUCTION

The last four chapters described quantitative and qualitative reliability tools for assessing equipment failures and system performance based on historical data (failure and repair), test results data, or even professional opinion. Such methodology did not directly take into account human factors, but many equipment failures or repair delays are caused by human error. When such failures impact system performance, root causes are discussed, and if human error influenced the failure, recommendations such as training, improved workplace ergonomics, or procedures are proposed to avoid such human error.

This chapter discusses human reliability models to help reliability professionals assess human errors in systems analysis. Thus some human reliability analysis methods will be proposed based on the author's experience and examples will be applicable to the oil and gas industry.

Many human reliability analysis methods were developed by the nuclear industry, and because of this, caution must be exercised when applying these methods in the oil and gas industry. Whenever possible it is best to perform more than one methodology to check the consistency of human error probability results. Actually, it is necessary to apply such methods to validate or even change values for more appropriate application in the oil and gas industry. Thus to validate such methods and values of human error probabilities, specialist opinions and even a data bank must be used.

This chapter presents seven different human reliability methodologies with applications in the oil and gas industry. At the end of the chapter a case study is provided, performed for the different methodologies, to check human error probability results and compare methods.

Human reliability analysis began in the 1950s. A basic timeline is as follows.

In 1958 Williams suggested the importance of considering human reliability system reliability analysis (Williams, 1988).

In 1960 reliability studies showed that some equipment failures were influenced by human actions, and in 1972 the Institute of Electrical and Electronics Engineers (IEEE) published a report about human reliability.

The last four chapters have described quantitative and qualitative reliability engineering tools to assess equipment failures and system performances based on historical data (failure and repair), test results data, or even professional opinion. Such methodology did not take into account direct human factors, but actually when investigated, many equipment failures or repair delays are caused by human error. When such failures impact system performance, root causes are usually discussed and if human error influenced the failure, recommendations are proposed such as training, improving workplace ergonomics, or procedures to avoid such human error.

In 1975 Swain and Guttman proposed the first human reliability approach to solving human failures in atomic reactor operations (Swain and Guttman, 1980). The main objective of THERP (Technique for Human Error Prediction) was to understand operational sequential actions to define human error probability and prevent human failures (Spurgin, 2010).

From the 1970s on several methodologies were proposed and published by the US Nuclear Regulatory Commission (USNRC) and other industries and governmental organizations.

In general terms, human reliability methods were developed in three stages. The first stage (1970–1990) was known as the first generation of human reliability methods, and it focused on human error probabilities and human operational errors.

The second phase (1990–2005) was known as the second generation of human reliability methods, and it focused on human performance-shaping factors (PSFs) and cognitive processes. Human PSFs are internal or external and, in general, include everything that influences human performance, such as workload, stress, sociological issues, psychological issues, illness, etc.

Finally, the third phase, the third generation of human reliability methods, started in 2005 and continues today and focuses on human PSFs, relations, and dependencies.

Today, human reliability methods are applied by different industries to reduce accidents and the costs of human errors in operation and maintenance activities. Major Hazard Incident Data Analysis Service (MHIDAS) data reports that out of the 247 accidents in refineries, 21.86% were related to human failure (Silva, 2003).

In pipeline industries, 41% of system failures have human error as the root cause. Operation is responsible for 22% and maintenance is responsible for 59% (Mannan, 2005).

To apply such methodologies, human failure data are collected from historical data procurements or specialist opinions. There are several ways of aggregating experts' opinions: they can be estimated along with their opinions, then aggregated mathematically, they can be estimated alone, but have limited discussions for clarification purposes, or they can meet as a group and discuss their estimates until they reach a consensus (Grozdanovic, 2005). Thus the methods are:

- Aggregated individual method: In this method experts do not meet, but create estimates individually. These estimates are then aggregated statistically by taking the geometric mean of all the individual estimates for each task.
- Delphi method: In this method experts makes their assessments individually and then all the assessments are shown to all the experts.
- Nominal group technique: This method is similar to the Delphi method, but after the group discussion, each expert makes his or her own assessment. These assessments are then statistically aggregated.
- Consensus group method: In this method, each member contributes to the discussion, but the group as a whole must then arrive at an estimate upon which all members of the group agree.

In the oil and gas industry, there is not much data about human reliability compared to the data available in the nuclear industry. In the Brazilian oil and gas industry, for example, many of the human reliability analyses in the last 10 years were applied to drilling projects using the Bayesian network method (third generation of human reliability methods), but, in general, human reliability methods are not applied.

To have specific tools to assess human error this chapter will describe a number of human reliability models to support reliability professionals to deal better with human error in their system analysis, which comprises safety, maintenance, and operational tasks. Thus there will be proposed methods for human reliability analysis based on the author's experience and examples will be given that apply to the oil and gas industry.

### 5.1.1 HUMAN RELIABILITY CONCEPTS

Human reliability is the probability of humans conducting specific tasks with satisfactory performance. Tasks may be related to equipment repair, equipment or system operation, safety actions,

analysis, and other kinds of human actions that influence system performance. Human error is contrary to human reliability and basically the human error probability ( $P(\text{HE})$ ) is described as:

$$P(\text{HE}) = \frac{\text{Number of errors}}{\text{Number of error opportunities}}$$

Human reliability analysis focuses on estimating human error probability. But it is also important to understand the human context in system performance. Consequently, the main questions human reliability analysis tries to answer are:

- What can be wrong?
- Which are the human failure consequences?
- Which human PSFs influence human reliability the most?
- What is necessary to improve human reliability to avoid or prevent human error?

To answer such questions an appropriate method must be applied, which depends on three critical issues, as follows:

- The first issue is human reliability analysis objectives, which are applied to investigate incidents, to improve maintenance procedures, and to improve operational steps.
- The second issue is the human error data available for performance analysis. To perform human reliability analysis, specialist opinions or human error data must be available. Whenever data is not available and specialists are not able to estimate the human error probability, it is necessary to verify the reliability of data from the literature.
- The last and most critical issue in human reliability analysis is time to perform analysis. Time is always a critical issue because human reliability analysis can last for hours or a few days.

To decide which human reliability analysis methods to apply it is also necessary to know about human reliability method characteristics, their objectives, and limitations. But first it is necessary to understand human reliability concepts. In general terms, human error can be:

- Omission error, which happens when one action is not performed because of lapse or misperception. For example, in preventive incident actions, omission error is the misperception of an alarm (and consequently not performing the actions required). In maintenance, omission error is when equipment fails as soon as corrective maintenance is conducted because of lapse, which means certain steps of corrective maintenance procedures were not performed.
- Commission error, which happens when an action is performed incorrectly because of an incorrect quantity or quality of action or a mistake in selecting or proceeding with a sequence. For example, in preventive incident actions, commission error is selecting the wrong command or making a mistake in the sequence of actions required. Equipment degradation repair is a commission error when the repair is performed incorrectly.
- Intentional error, which happens when operational actions are conducted wrongly with awareness of the consequences. In some cases procedural steps are not followed or systems are intentionally shut down or put in unsafe conditions. For example, in preventive incident actions, intentional error occurs when an operator does not follow safety procedures to reestablish the system faster. Equipment degradation would occur when intentional incorrect action is performed during repairs. For example, a maintenance professional intentionally using a tool on a piece of equipment to damage it.

In addition to understanding the human error types it is necessary to understand the factors that influence them. There are many factors that influence human error such as human PSFs (internal or external) and human behavior. Internal human PSFs depend on individual characteristics including:

- Psychological: Related to emotional issues such as stress, overworked psyche, depression, demotivation, and lack of concentration;
- Physiological: Related to physical issues such as health conditions and diseases.

Such factors can be monitored to guarantee that employees will be in better physical and psychological shape to perform critical actions.

External human PSFs are technological and social:

- Technological: Related to work conditions, tools, and technology, such as ergonomics, procedures, and equipment;
- Social: Related to social issues in and out of the workplace, such as poor social conditions and lack of acceptance in the group.

There are a number of social issues that influence employees' behavior that are beyond a company's control. However, technological issues can be controlled and better conditions lead to better employee performance. Fig. 5.1 shows the human reliability analysis factors that influence human error.

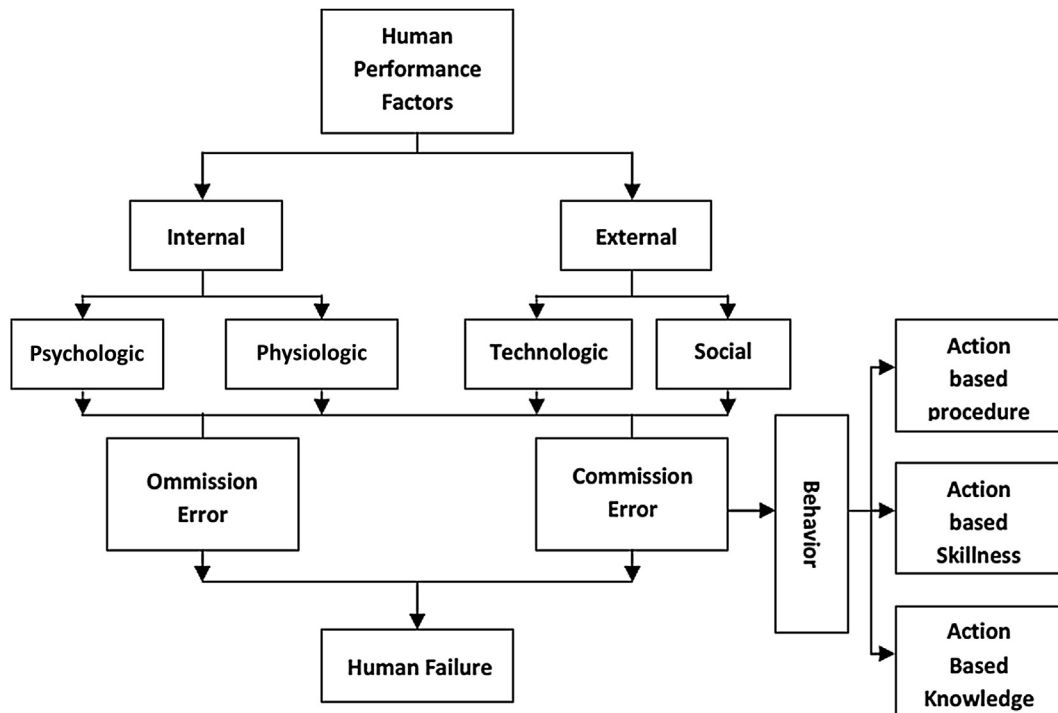


FIGURE 5.1

Influence factors in human error.

<b>Table 5.1 First-Generation Methods Examples</b>		
<b>Human Reliability Analysis Methods</b>		
<b>First Generation</b>		
	<b>Name</b>	<b>Objective</b>
THERP	Technique for Human Error Rate Prediction	Assess failure in task or action sequence. It is applied in maintenance, operational, or incident analysis with complex graphic representation (1975)
OAT	Operator Action Trees	Assess failure in task or action sequence. It is applied in maintenance, operational, or incident analysis with simple graphic representation (1982)
SLIM	Success Likelihood Index Methodology	Assess failure in task or action sequence. It is applied in maintenance, operational, or incident analysis and regards human factors performance based on specialist opinion (1984)
SHARP	Systematic Human Action Reliability Procedure	Assess cognitive human process of failure (detection, understanding, decision, and action), being applied in maintenance, operational, or incident analysis (1984)
STAHR	Sociotechnical Assessment of Human Reliability	Assess failure in task or action sequence and is applied in maintenance, operational, or incident analysis and regards human factors performance based on specialist opinion (1983)

Human behavior also influences task performance, that is, maintenance, operation, or preventive incident sequence actions, and such behavior is based on procedures, skills, and knowledge. When action behavior is based on a procedure, the procedure greatly influences action performance mainly when employees do not have the experience to execute a task.

When action behavior is based on skill, practical experience in a specific task and time to perform that task greatly influence human performance. When action behavior is based on knowledge, human performance is greatly influenced by human knowledge of conducting a complex task that requires time enough for information to be processed, assessed, and implemented.

To perform human reliability analysis, it is necessary to know the features and objectives of this analysis. Table 5.1 shows some of the first-generation human reliability analysis methods that emphasize the sequence of actions and human error probability.

Table 5.2 gives examples from the second and third generation of human reliability analysis methods, which emphasize human cognitive processes and human factor dependency, respectively.

Depending on the human reliability analysis objective and the problem characteristics, it is advisable to implement the most appropriate method to be successful. Whenever possible it is best to apply more than one method and compare results because it provides a chance to verify results about which human performance factor influences human error and check human error probability value consistency.

## 5.2 TECHNIQUE FOR HUMAN ERROR RATE PREDICTION (THERP)

THERP was one of the first probabilistic analyses and was developed by specialists who detected problems in nuclear reactors (1975). But the real effort to develop a human analysis methodology was

Table 5.2 Second- and Third-Generation Methods Examples		
Human Reliability Analysis Methods		
Name		Objective
<b>Second Generation</b>		
ATHEANA	A Technique for Human Error Analysis	Assess cognitive human process of failure (detection, understanding, decision, and action), being applied in maintenance, operational, or incident analysis (1996)
CREAM	Cognitive Reliability and Error Analysis Method	Assess cognitive human process of failure (detection, understanding, decision, and action), being applied in maintenance, operational, or incident analysis (1998)
<b>Third Generation</b>		
Bayesian network		Assess failure in task or action sequence and is applied in maintenance, operational, or incident analysis and regards human factors performance based on specialist opinion; in addition, such methods regard human factors performance dependency (2005)

conducted by Swain when he published the Technique for Human Error Rate Prediction in 1983. The THERP methodology uses a human reliability tree that represents a sequence of probable omission or commission errors with success or human error probability. The following steps are needed to perform THERP analysis:

- Understand the problem to be assessed;
- Identify the system functions that may be influenced by human error;
- List and analyze the related human tasks;
- Estimate the error probabilities for each task;
- Estimate the final human error probability of tree events;
- Propose recommendations to reduce the human error probability;
- Estimate the recommendations effects on the human error probability of three events.

As described, the first step is to understand what is being assessed to see if THERP is the best tool for finding the answer. The second step is important for understanding the human error context and how human tasks influence the system or activity being assessed. The third step describes task steps, and in some cases tasks can be summarized. Not all task steps must be considered in the analysis because due to difficulties in estimating human error, in some cases it is clear that some task steps do not influence the human error being assessed.

Caution is necessary, but it is important to remember that long tasks are more difficult to analyze, and whenever possible it is best to simplify to understand the human error involved in the problem being assessed to allow for more accurate results. The fourth and more difficult step is to estimate human error probability, which can be done using a data bank, specialist opinion, literature, or a combination of these. In this step it must be clear that the main objective is to estimate human error, so that the final human error probability is representative of the problem assessed. An example of human error probability values is shown in Fig. 5.1.

Fig. 5.2 shows that the human error probability depends on task duration and activity context. The task duration influences the human error probability, and the shorter the task, the higher the human

Type of error	Time	Skillness	Procedure	Knowledge
<b>Omission Error</b>	Short	0.003	0.05	1
<b>Omission Error</b>	Long	0.0005	0.005	0.1
<b>Commission Error</b>	15 min	0.001	0.03	0.3
<b>Commission Error</b>	5 min	0.1	1	1

FIGURE 5.2

Human error probability.

Source: Kumamoto and Henley (1996).

error probability. The main question to ask when using such data is if it is representative of the case being assessed, the specialist involved in such analysis must be able to confirm if such data fit well or not. If not, the specialist must propose other values of human error probability when there is no historical data available. Some human errors are uncommon, and there is often no available reports or data, and in this case it can be estimated by specialist opinion. In newer plants when there has not been enough time to estimate human error, a specialist can also estimate how much human error is expected to occur over the plant life cycle. It is often easier to estimate the frequency of occurrence of failure than probability, but it is not a problem itself, because in this case it is possible to turn the frequency of failure into the probability of failure for the time requested by the exponential cumulative density function (CDF) when the failure is random, which is represented by:

$$F(t) = \int_0^t f(x) dx = \int_0^t \lambda e^{-\lambda t} = 1 - \frac{\lambda}{\lambda} e^{-\lambda t} = 1 - e^{-\lambda t}$$

where  $\lambda$  = expected number of human errors per time;  $T$  = time; and  $F(t)$  = probability of human error occurring until time  $t$ .

After estimating human error probability, by task, it is necessary to calculate the final human error probability for the whole activity and this can be done using a THERP event tree. A THERP event tree has two sides where successes and failures are counted. Tasks are represented by letters. The uppercase letters represent failures and the lowercase letters represent successes. On the right side where there are input failure probabilities it is possible also to use successes, but on the left side it is not. An example will be given to illustrate the human reliability event tree diagram.

The THERP methodology can be applied to understanding maintenance human error in exchanging obstructed tubes in heat exchangers because of human failure to close equipment correctly. The PSF “workplace environment” was the requirement to quickly perform maintenance to finish it as soon as possible. Fig. 5.3 shows the tube and shell heat exchanger, and the task steps are:

- Check if operator stops equipment (success: a; fail: A);
- Check if lines linked to equipment are depressurized and purged (success: b; fail: B);
- Check if scaffold is safe (success: c; fail: C);
- Isolate equipment lines (success: d; fail: D);
- Open an inspection tube (success: e; fail: E);
- Replace obstructed tubes (success: f; fail: F);
- Close equipment (success: g; fail: G).

**FIGURE 5.3**

Tube and shell heat exchanger.

All of these steps can shut down equipment if human error succeeds. Such a task sequence can be represented by a THERP event tree as shown in Fig. 5.4. Notice that all events are independent.

To calculate human error probability it is necessary to define the probability failure for each of the seven tasks, because if any of them fail, the maintenance in the heat exchanger will not succeed. Thus human error probability based on the THERP event tree is described by:

$$\text{HEP} = 1 - P(\text{success})$$

$$P(\text{Success}) = P(a) \times P(b) \times P(c) \times P(d) \times P(e) \times P(f) \times P(g)$$

$$\text{HEP} = 1 - [P(a) \times P(b) \times P(c) \times P(d) \times P(e) \times P(f) \times P(g)]$$

$$\text{HEP} = 1 - \prod_1^n P(x_n)$$

$$x_1 = a; \quad x_2 = b; \quad x_3 = c; \quad x_n = n$$

Thus, based on Fig. 5.4 and probabilities values, human error probabilities will be:

$$P(a) = 1 - P(A) = 1 - (0.0005)$$

$$P(b) = 1 - P(B) = 1 - (0.0005)$$

$$P(c) = 1 - P(C) = 1 - (0.0005)$$

$$P(d) = 1 - P(D) = 1 - (0.03)$$

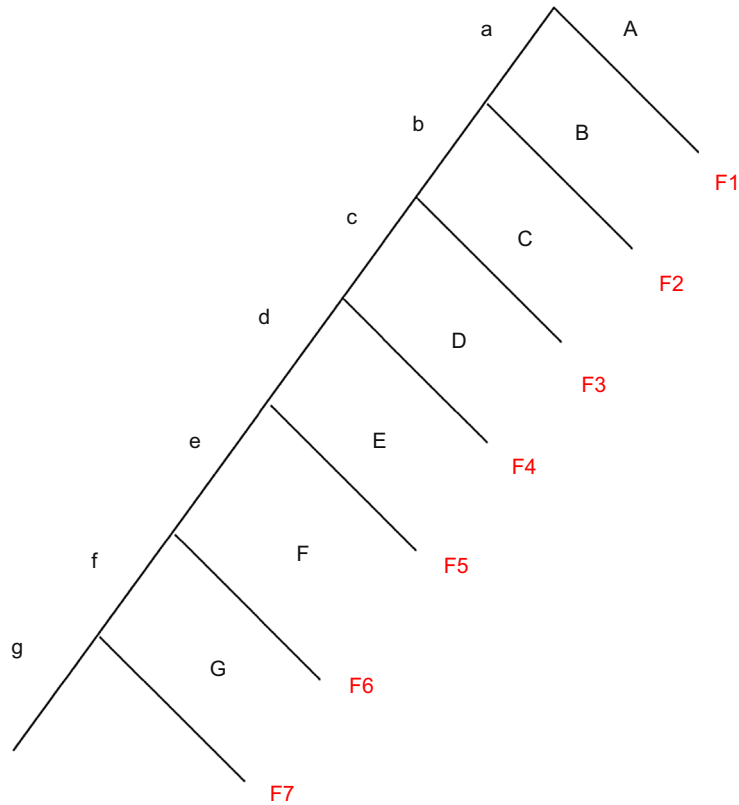
$$P(e) = 1 - P(E) = 1 - (0.01)$$

$$P(f) = 1 - P(F) = 1 - (0.1)$$

$$P(g) = 1 - P(G) = 1 - (0.1)$$

$$\begin{aligned} \text{HEP} &= 1 - P(s) = 1 - ((0.9995) \times (0.9995) \times (0.9995) \times (0.97) \times (0.99) \times (0.9) \times (0.9)) \\ &= 21.63\% \end{aligned}$$





**FIGURE 5.4**  
THERP event tree.

Such probability shows that at the end of maintenance, because there was not adequate time to perform the maintenance in the tube and shell heat exchanger, there will be a higher probability of failure in the tasks of replacing the obstructed tube ( $P(F) = 0.1$ ) and closing the heat exchanger ( $P(F) = 0.1$ ). Thus there is a high probability of chance for human error in such maintenance.

After estimating human error probability it is necessary to assess improvements for reducing human error probability and to estimate the human error probability after recommendations are implemented. When there is enough time to complete the task in the two final tasks ( $F$  and  $G$ ) the probability of failure is reduced from 0.1 to 0.001 and consequently the new human error probability is:

$$\begin{aligned} \text{HEP} &= 1 - P(s) = 1 - ((0.9995) \times (0.9995) \times (0.9995) \times (0.97) \times (0.99) \times (0.999) \times (0.999)) \\ &= 4.3\% \end{aligned}$$

In such maintenance the first four tasks are related to safety. To perform maintenance under safe conditions, such tasks are required, but in many cases those tasks are not conducted properly and

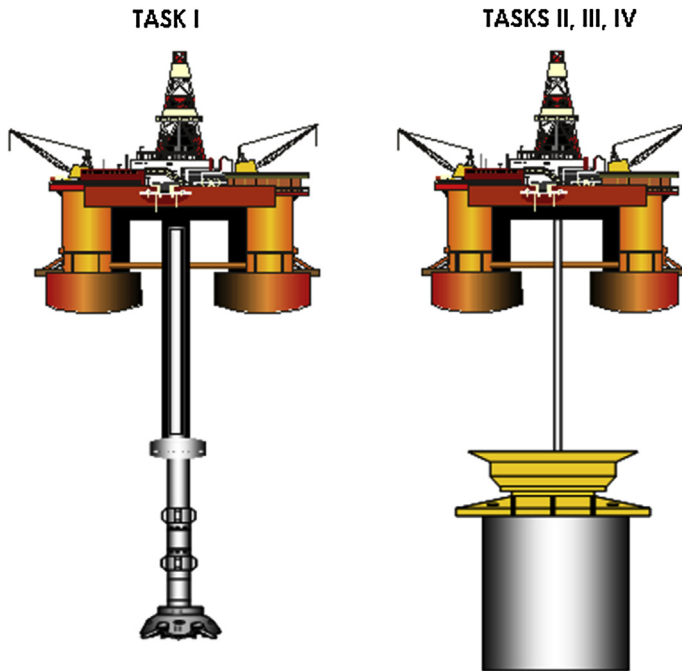


FIGURE 5.5

Drilling phase tasks.

checked by maintenance professionals. If accidents occur, in addition to human injuries and equipment damage, maintenance is not completed and a system can be shut down and consequently there will be additional delays in startup. Because of this the first four tasks are considered part of maintenance, and when they are not performed properly, they are considered human errors in maintenance.

To better illustrate THERP methodology, a second example of human reliability analysis will be conducted using drilling phases, as shown in Fig. 5.5. In general, the steps are:

1. Drill and condition (success: a; fail: A);
2. Circulation (success: b; fail: B);
3. Casing (success: c; fail: C);
4. Cementation (success: d; fail: D).

In the case of human error there will be delays on a drilling project or accidents such as a blowout. The event tree can be represented as shown in Fig. 5.6.

Based on specialist opinion, each event has the following probabilities:

$$P(a) = 1 - P(A) = 1 - (0.01) = 0.99$$

$$P(b) = 1 - P(B) = 1 - (0.02) = 0.98$$

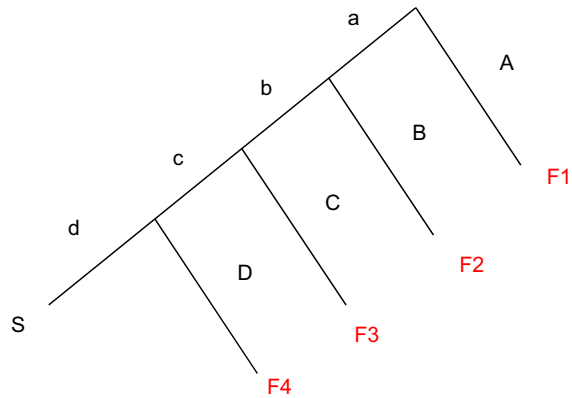
$$P(c) = 1 - P(C) = 1 - (0.01) = 0.99$$

$$P(d) = 1 - P(D) = 1 - (0.005) = 0.995$$

$$\text{HEP} = 1 - P(s) = 1 - ((0.99) \times (0.98) \times (0.99) \times (0.995)) = 4.43\%$$

**FIGURE 5.6**

THERP event tree (drilling phase tasks).



Human error in drilling tasks can result in the tool being stuck. Human failure in circulation can result in a kick, and if not controlled can result in a blowout accident. Human error in a casing task can also result in casing prison. And finally, human error in cementation can cause instability in a well.

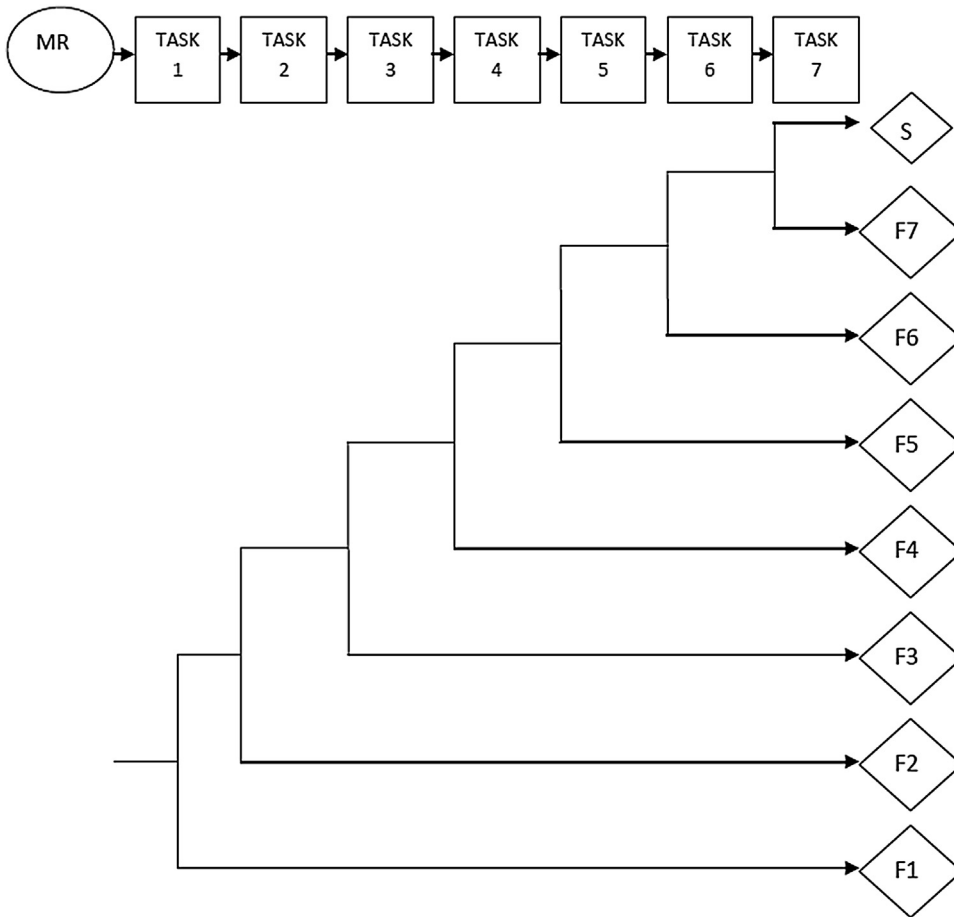
Thus using THERP human reliability methods it is possible to assess human error in task sequences. These drill steps comprise several other tasks in different drill phases that can also be assessed in the details when it is necessary. In conclusion, the important points of the THERP methodology are:

- For simple tasks, using the event tree it is possible to assess sequences of human actions where human error may occur.
- The THERP method has been widely applied across industries, producing a large pool of experienced analysts and example applications.
- For complex tasks with many steps it is hard to model an event tree.
- To calculate human error probability it is necessary to define the human error probability for each task and sometimes this is not easy to do.
- Such methodology does not consider human PSFs that cause human error, which is a remarkable characteristic of the first generation of human reliability analysis methodologies.

### 5.3 OPERATOR ACTION TREE (OAT)

OAT methodology was developed in 1982 to calculate the human error probability in a sequence of tasks. The OAT method has been used in probabilistic risk analysis for nuclear plants. This method uses a horizontal event tree format to model the probability of success in a sequence of tasks influenced by human behaviors. The event tree in the OAT methodology is different from the one in THERP analysis. The event tree in OAT methodology also focuses on task sequences but also shows the possibilities of success and failure for each task and gives the probability of successful results. Thus the sequence of tasks is created from the left to the right for task sequences.

To illustrate the OAT event tree an example will be given using the tube and shell heat exchanger example shown in Fig. 5.7, which shows the seven heat exchanger maintenance tasks.



**FIGURE 5.7**

OAT (tube and shell maintenance).

Thus the result of the first event tree is the probability of failure in maintenance, which is the complement of probability of success, calculated by multiplying all task success probabilities, represented by:

MR = Maintenance requirements chance (was considered 100% = 1)

Task 1—Check if operator stops equipment (Fail1);

Task 2—Check if lines linked to equipment are depressurized and purged (Fail2);

Task 3—Check scaffold is safe (Fail3);

Task 4—Isolate equipment lines (Fail4);

Task 5—Open an inspection tube (Fail5);

Task 6—Take place obstructured tubes (Fail6);

Task 7—Close equipment (Fail7);

S = Success on maintenance

Thus the tree event first result is the probability of failure in maintenance that is complemented by the probability of success and is calculated by multiplying all tasks by success probability. Thus, the general OAT calculation is defined by the following equation:

$$HEP = 1 - P(\text{success})$$

$$P(\text{success}) = (1 - P(\text{Fail1})) \times (1 - P(\text{Fail2})) \times \dots \times (1 - P(\text{Fail7}))$$

$$P(S_i) = (1 - P(\text{Fail}_i))$$

$$HEP = 1 - [P(S1) \times P(S2) \times P(S3) \times P(S4) \times P(S5) \times P(S6) \times P(S7)]$$

$$HEP = 1 - \prod_1^n P(S_n)$$

Regarding the probability of success in each task, the HEP result is:

$$HEP = 1 - [(0.9995) \times (0.9995) \times (0.9995) \times (0.97) \times (0.99) \times (0.9) \times (0.9)]$$

$$HEP = 21.63\%$$

In addition, there will be another combination of events that can be estimated by multiplying the combination of successes and failures. Thus the probabilities of maintenance failure because of a specific task failure regarding the other task successes are:

$$P(\text{Fail1}) = P(\text{Fail1})$$

$$P(\text{Fail2}) = P(S1) \times P(\text{Fail2})$$

$$P(\text{Fail3}) = P(S1) \times P(S2) \times P(\text{Fail3})$$

$$P(\text{Fail4}) = P(S1) \times P(S2) \times P(S3) \times P(\text{Fail4})$$

$$P(\text{Fail5}) = P(S1) \times P(S2) \times P(S3) \times P(S4) \times P(\text{Fail5})$$

$$P(\text{Fail6}) = P(S1) \times P(S2) \times P(S3) \times P(S4) \times P(S5) \times P(\text{Fail6})$$

$$P(\text{Fail7}) = P(S1) \times P(S2) \times P(S3) \times P(S4) \times P(S5) \times P(S6) \times P(\text{Fail7})$$

Applying success and failure probability for each task the probabilities are:

$$P(\text{Fail1}) = 0.0004999$$

$$P(\text{Fail2}) = 0.9995 \times 0.0005 = 0.0004997$$

$$P(\text{Fail3}) = 0.9995 \times 0.9995 \times 0.0005 = 0.00049950$$

$$P(\text{Fail4}) = 0.9995 \times 0.9995 \times 0.9995 \times 0.03 = 0.02995$$

$$P(\text{Fail5}) = 0.9995 \times 0.9995 \times 0.9995 \times 0.97 \times 0.01 = 0.0009685$$

$$P(\text{Fail6}) = 0.9995 \times 0.9995 \times 0.9995 \times 0.97 \times 0.99 \times 0.1 = 0.09675$$

$$P(\text{Fail7}) = 0.9995 \times 0.9995 \times 0.9995 \times 0.97 \times 0.99 \times 0.9 \times 0.1 = 0.8708$$

So, for example, the probability of tube and shell heat exchanger maintenance failure as a result of it being closed incorrectly (task 7) is 8.708%, with the assumption that all other tasks were performed correctly. Such analysis is similar for other tasks, and it is possible to create a ranking system for the

most critical tasks that would shut down the tube and heat exchanger. In this example, the sequence from the most critical to the less critical task is: task 6 (9.6%); task 7 (8.708%); task 4 (2.9%); task 1 (0.04999%); task 2 (0.04997%); task 3 (0.04905%); and task 5 (0.096%). Such analysis identifies the tasks that impact maintenance performance the most. Thus the important points for the OAT method are:

- For simple or complex tasks, using the event tree it is possible to assess a sequence of human actions during which human error can occur.
- To calculate human error probability it is necessary to define the human error probability for each task, but sometimes this is difficult.
- Such methodology does not consider human PSFs that cause human error, which is a remarkable characteristic of the first generation of human reliability analysis methodologies.
- It is possible to define the most critical tasks of sequences to prevent human error in such tasks.

---

## 5.4 ACCIDENT SEQUENCE EVALUATION PROGRAM (ASEP)

The Accident Sequence Evaluation Program (ASEP) approach assesses an action before an accident happens. The ASEP human reliability analysis procedure consists of a pre-accident human reliability analysis and post-accident human reliability analysis. The ASEP is an abbreviated and slightly modified version of THERP in some terms. The ASEP provides a shorter route to human reliability analysis as human error probability is predefined, requiring less training to use the tool compared to other human reliability analysis methods (Bell and Holroyd, 2009). The four procedures and two general approaches involved in this method are described as follows:

- Pre-accident tasks: Those tasks that, if performed incorrectly, could result in the unavailability of necessary systems or components to respond appropriately to an accident.
- Post-accident tasks: Those tasks that are intended to assist the plant in an abnormal event, that is, to return the plant's systems to safe conditions.
- Even pre-accident and post-accident analysis has screening and nominal approaches that differ from less and more conservative human error probability values, respectively.

### 5.4.1 PRE-ACCIDENT ANALYSIS METHODOLOGY

To assess pre-accident and post-accident it is necessary to take into account recovering actions and dependence between human error probabilities (Swain, 1987).

In pre-accident nominal human reliability analysis the regular probabilistic risk assessment is conducted on tasks. This approach uses what the human reliability analysis team judges to be more realistic values, but they are still somewhat conservative (ie, pessimistic) to allow for the team's inability to consider all of the possible sources of error and all possible behavioral interactions.

In pre-accident screening, human reliability analysis probabilities and response times are assigned to each human task as an initial type of sensitivity analysis. If a screening value does not have a material effect in the systems analysis, it may be dropped from further consideration. Screening reduces the amount of detailed analyses to be performed. Human reliability analysis at this stage deliberately uses conservative estimates of human error probabilities.

According to [NUREG/CR-4772](#), the human error probabilities for pre-accident analysis are based on the following conditions:

- Basic condition 1 (BC1): No safety equipment device signal to notify of unsafe conditions is available whenever the device is under maintenance or other kind of intervention.
- Basic condition 2 (BC2): Component status has not been verified by a post-maintenance (PM) or a post-calibration (PC) test.
- Basic condition 3 (BC3): There is no recovery factor to check unsafe conditions.
- Basic condition 4 (BC4): Check of component status is not completely effective.

The basic human error probability (BHEP) in pre-accident analysis based on the ASEP method is 0.03, that is, the probability of error omission (EOM) occurring or error commission (ECOM) occurring and EOM not occurring. Mathematically, this is represented by:

$$F_T = P(\text{EOM}) + ((1 - P(\text{EOM})) \times P(\text{ECOM}))$$

Based on the ASEP procedure the EOM and ECOM are:

$$P(\text{EOM}) = 0.02$$

$$P(\text{ECOM}) = 0.01$$

Thus:

$$F_T = 0.02 + ((1 - 0.02) \times 0.01) = 0.0298 \approx 0.03$$

$$F_T = 0.03$$

In addition to basic conditions there are four optimum condition assumptions:

- Optimum condition 1 (OC1): Unavailable component status is indicated in the control room by some compelling signal such as an annunciation when the maintenance or calibration task or subsequent test is finished.
- Optimum condition 2 (OC2): Component status is verifiable by a PM or PC test. If done correctly, full recovery is assumed. A human error probability of 0.01 is assessed for failure to perform the test correctly (including failure to do the test).
- Optimum condition 3 (OC3): There is a requirement for a recovery factor (RF) involving a second person to verify component status after completion of a PC or PM task. A human error probability of 0.1 is assessed for failure of this RF to catch an error by the original task performer.
- Optimum condition 4 (OC4): There is a requirement for a current check of component status, using a written list. A human error probability of 0.1 is assessed for the failure of such a check to detect the unavailable status.

Thus for basic conditions and optimum conditions, human error probabilities with error factors and upper bounds are suggested, as given in the following nine cases:

Case 1: After a human error (omission or commission), neither PM nor PC is able to recover the error or other RFs. Thus all basic conditions are applied. The probability of human error is:  $F_T = 0.03$  (error factor [EF] = 5 and upper bound [UB] = 0.15).

Case 2: After a human error (omission or commission), neither PM or PC is able to recover the error or other RFs. Thus basic conditions 1 and 2 are applied as well as optimum conditions 3 and 4. Therefore the probability of human error is:  $FT = 0.0003$  ( $EF = 16$  and  $UB = 0.05$ ).

Case 3: After a human error (omission or commission), neither PM or PC is able to recover the error or the feedback signal, but the second person or other RF is used. Thus basic conditions 1, 2, and 4 are applied as well as optimum condition 3. Therefore the probability of human error is:  $FT = 0.003$  ( $EF = 10$  and  $UB = 0.03$ ).

Case 4: After a human error (omission or commission), neither PM or PC is able to recover the error or the feedback signals, but a periodic check is performed. Thus basic conditions 1, 2, and 3 are applied as well as optimum condition 4. Therefore the probability of human error is:  $FT = 0.003$  ( $EF = 10$  and  $UB = 0.03$ ).

Case 5: After a human error (omission or commission), PM or PC is able to recover the error and at least optimum condition 1 is applied. Therefore the probability of human error is:  $FT = \text{negligible}$  ( $UB = 0.00001$ ).

Case 6: After a human error (omission or commission), PM or PC is able to recover the error. Thus basic conditions 1, 3, and 4 are applied as well as optimum condition 4. Therefore the probability of human error is:  $FT = 0.0003$  ( $EF = 10$  and  $UB = 0.003$ ).

Case 7: After a human error (omission or commission), PM or PC is able to recover the error. Thus basic condition 1 is applied as well as optimum conditions 2, 3, and 4. Therefore the probability of human error is:  $FT = 0.00003$  ( $EF = 16$  and  $UB = 0.0005$ ).

Case 8: After a human error (omission or commission), PM or PC is able to recover the error. In addition, a second person is used to recover the error. Thus basic conditions 1 and 4 are applied as well as optimum conditions 2, 3, and 4. Therefore the probability of human error is:  $FT = 0.0003$  ( $EF = 10$  and  $UB = 0.003$ ).

Case 9: After a human error (omission or commission), PM or PC is able to recover the error. In addition, periodic tests are performed. Thus basic conditions 1 and 3 are applied as well as optimum conditions 2 and 4. Therefore the probability of human error is:  $FT = 0.00003$  ( $EF = 16$  and  $UB = 0.0005$ ).

To better understand ASEP methodology applied to pre-accident human reliability analysis, a liquefied petroleum gas (LPG) storage sphere accident example will be given and assessed by ASEP methodology.

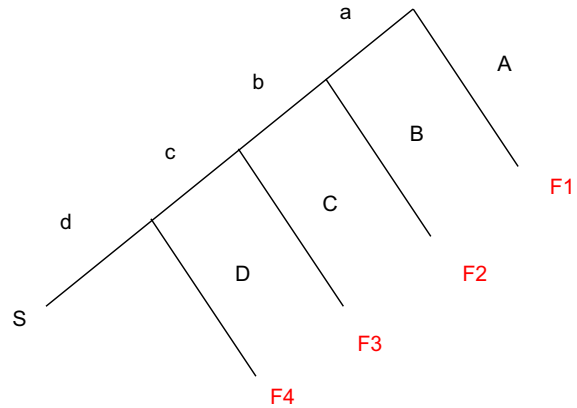
The task of draining the sphere bottom is part of the storage sphere routine, and when draining the sphere it is required to open a manual valve for a period of time, then close it. The procedure to perform such a task states that the operator must be local and observe the product from the bottom to be drained, and then close it. Otherwise the valve may fail to close because of a low temperature, and if that happens it is not possible for the operator to manually close it and consequently there will be LPG leakage. In the worst case, if there is a puddle and ignition from a heat source, such as a piece of equipment or vehicle, there will be a fire on the sphere bottom that may develop into a sphere BLEVE (boiled liquid evaporation vapor). The task steps to drain an LPG sphere are:

- Check if there is a vehicle in operation around the LPG sphere (success: a; fail: A);
- Check if there is maintenance or another service with ignition sources being performed around the LPG sphere area (success: b; fail: B);
- Check if the valve to drain the LPG sphere is working properly (success: c; fail: C);
- Conduct the draining in the LPG sphere (success: d; fail: D).



FIGURE 5.8

ASEP event tree (LPG sphere pre-accident).



The tasks can be represented by the human reliability analysis tree in Fig. 5.8. Remember that the first three tasks normally do not trigger an accident, but when not performed correctly, a task is a human error in terms of procedure and an unsafe condition.

The pre-accident analysis in the sphere is caused by human error in:

- Task 3 because the valve was not checked by the operator.
- Task 4 because the operator did not stay and watch the drain.

Unfortunately, there were no RFs. Based on ASEP cases the probability for each task is 0.03 (see case 1) and the probability of leakage (human error probability) is:

$$\text{HEP} = 1 - P(s) = 1 - (0.97 \times 0.97 \times 0.97 \times 0.97) = 11.5\%$$

If a recover action or second person checks steps 3 and 4, the probability of failure in such tasks is reduced to 0.003 (see case 3), and the new probability of leakage in the LPG sphere will be:

$$\text{HEP} = 1 - P(s) = 1 - (0.97 \times 0.97 \times 0.997 \times 0.997) = 6.5\%$$

If RFs are implemented in the drain procedure there is a better chance of avoiding leakage in the LPG sphere. In some cases, such leakage combined with an ignition source can result in BLEVE. The LPG BLEVE accident is shown in Fig. 5.9.

There are two types of dependence in ASEP methods: between-person dependence and within-person dependence. Between-person dependence is handled in the treatment of RFs; in other words, another person checks the first person's task. Within-person dependence refers to the dependence among human actions by one person who is performing operations in more than one component. Within-person dependence is handled with a new dependence model described as follows. Thus, according to NUREG/CR-4772, the human reliability probabilities for pre-accident analysis with within-person dependence are based on basic and optimum conditions. The basic conditions are:

Basic condition 1 (BC1): No signal device to notify of an unsafe condition is available in the control room, and such condition will be realized only when performing maintenance, calibration, inspections, or test tasks.

Basic condition 2 (BC2): Component status has not been verified by a PM or a PC test.

**FIGURE 5.9**

BLEVE in LPG sphere, Feyzin, France, 1966  
(LPG sphere pre-accident).

Source: <http://www.musee-pompiers.asso.fr/images/cs-dat-01.jpg>.

Basic condition 3 (BC3): There is no RF to check an unsafe condition and no second person to verify after a maintenance or calibration test.

Basic condition 4 (BC4): Check if component status is performed shift-wise or daily but without a checklist or is not done at all.

In addition to the basic conditions there are four other optimum condition assumptions:

Optimum condition 1 (OC1): Unavailable component status is indicated in the control room by some compelling signal such as an annunciation when the maintenance or calibration task or subsequent test is finished.

Optimum condition 2 (OC2): Component status is verifiable by a PM or PC test. If done correctly, full recovery is assumed. A human error probability of 0.01 is assessed for failure to perform the test correctly (including failure to do the test).

Optimum condition 3 (OC3): There is a requirement for an RF involving a second person to directly verify component status after completion of a PM or PC task. A human error probability of 0.1 is assessed for failure of this RF to catch an error by the original task performer.

Optimum condition 4 (OC4): There is a requirement for a current check of component status, using a written list. A human error probability of 0.1 is assessed for the failure of such a check to detect the unavailable status.

Thus for basic conditions and optimum conditions, human error probabilities for with-person dependence are suggested, which include the following nine cases:

Case 1: After human error (omission or commission), neither PM nor PC is able to recover the error or other RFs. Thus all basic conditions are applied. The probability of human error is:  $FT = 0.03$  ( $EF = 5$ ).

Case 2: After human error (omission or commission), neither PM nor PC is able to recover the error or other RFs. Thus basic conditions 1 and 2 are applied as well as optimum conditions 3 and 4. Therefore the probability of human error is:  $FT = 0.0003$  ( $EF = 16$ ).

Case 3: After human error (omission or commission), neither PM nor PC is able to recover the error and the feedback signal, but a second person or other RF is used. Thus basic conditions 1, 2, and 4 are applied as well as optimum condition 3. Therefore the probability of human error is:  $FT = 0.003$  ( $EF = 10$ ).

Case 4: After human error (omission or commission), neither PM nor PC is able to recover the error or feedback signals, but periodic checks are performed. Thus basic conditions 1, 2, and 3 are applied as well as optimum condition 4. Therefore the probability of human error is:  $FT = 0.003$  ( $EF = 10$ ).

Case 5: After human error (omission or commission), PM or PC is able to recover the error and at least optimum condition 1 is applied. Therefore the probability of human error is:  $FT = \text{negligible}$  ( $UB = 0.00001$ ).

Case 6: After human error (omission or commission), PM or PC is able to recover the error. Thus basic conditions 1, 3, and 4 are applied as well as optimum condition 4. Therefore the probability of human error is:  $FT = 0.0003$  ( $EF = 10$ ).

Case 7: After human error (omission or commission), PM or PC is able to recover the error. Thus basic condition 1 is applied as well as optimum conditions 2, 3, and 4. Therefore the probability of human error is:  $FT = 0.00003$  ( $EF = 16$ ).

Case 8: After human error (omission or commission), PM or PC is able to recover the error. In addition, a second person is used to recover the error. Thus basic conditions 1 and 4 are applied as well as optimum conditions 2, 3, and 4. Therefore the probability of human error is:  $FT = 0.0003$  ( $EF = 10$ ).

Case 9: After human error (omission or commission), PM or PC is able to recover the error. In addition, periodic tests are performed. Thus basic conditions 1 and 3 are applied as well as optimum conditions 2 and 4. Therefore the probability of human error is:  $FT = 0.00003$  ( $EF = 16$ ).

For the situation when an action is being performed on more than one component, if a failure occurs in one of the components, being an omission or commission error and consequently a system shutdown, such a configuration is considered in series. However, if a combination of failures is required for system failure, for example, if there are two components and both must fail for system failure to occur, this is considered a parallel system.

For the LPG case study, if, for example, it is necessary to close two valves after draining the LPG sphere to avoid leakage, the human event tree within-person dependence can be represented by Fig. 5.10 for the two tasks, check valve 1 and check valve 2.

a = Success in check valve 1.

A = Omission error in check valve 1.

b/a = Success in check valve 2 regarding valve 1 was checked successfully.

B/a = Omission error in check valve 2 regarding valve 1 was checked successfully.

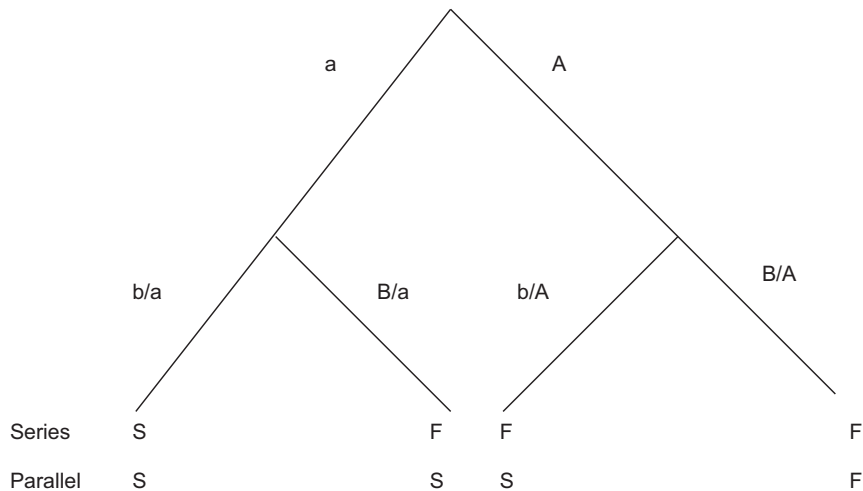
b/A = Success in check valve 2 regarding omission error in check valve 1.

B/A = Omission error in check valve 2 regarding omission error in check valve 1.

If a system is in series it means that for a pre-accident condition to occur there is only one of two valves that is not closed because of an omission error. As it is regarded as a within-person condition, case 3 can be used as a reference, and in this case the human error probability will be 0.003:

$$HEP = 1 - P(s) = 1 - (P(a) \times P(b/a))$$

$$HEP = 1 - ((1 - 0.003) \times (1 - 0.003)) = 0.59\%$$

**FIGURE 5.10**

ASEP event tree (LPG sphere pre-accident—within-person dependence).

The ASEP model described in [NUREG/CR-4772](#) has additional concepts regarding dependence levels including zero dependence (ZD), high dependence (HD), or complete dependence (CD). The ASEP dependence model is presented in two formats. The first one is presented in the form of a binary decision tree. The second one, based on results of this decision tree, provides tabled guidelines for assessing within-person dependence levels. The tree dependence decisions are shown in [Fig. 5.10](#). As shown in [Fig. 5.11](#), depending on the condition of the equipment under human intervention, the level of dependence varies from ZD to HD.

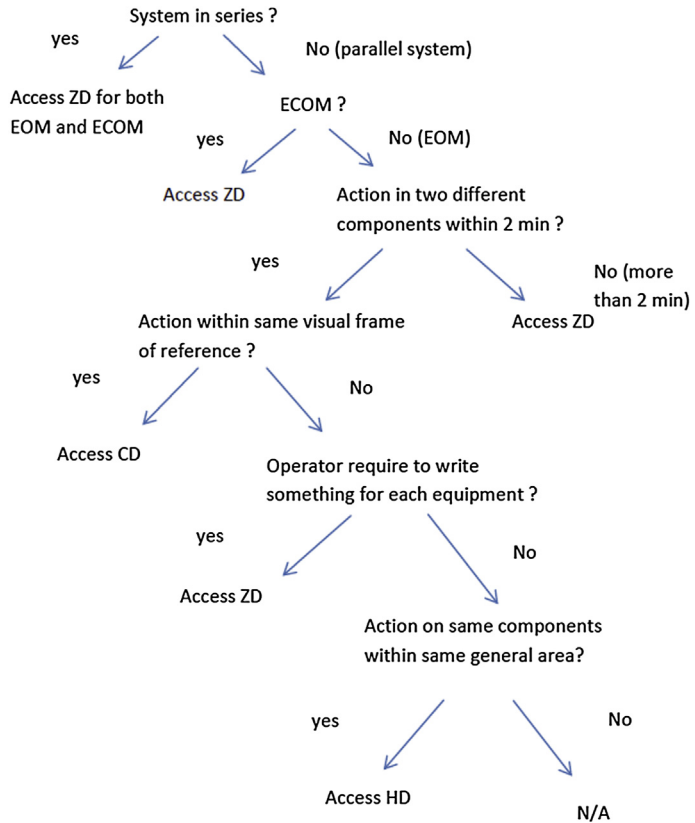
### 5.4.2 POST-ACCIDENT ANALYSIS METHODOLOGY

The ASEP methodology discussed until now is for assessing the pre-accident condition, but [NUREG/CR-4772](#) also proposes a methodology for assessing human error probability for post-accident analysis. In this case, the time to detect an accident is very important and highly influences human error probability in post-accident actions. Detecting accidents on time, performing correct diagnoses, and correcting decisions are essential to performing corrective action to control accident scenarios. If diagnosing and decision making takes longer than necessary there will not be enough time to perform corrective action, and the accident will not be under control. In addition, even though correct diagnosis and decisions take place, if the corrective action is wrong or not performed in the required time, the accident will not be under control. In such a model all resources for controlling accidents are considered available, but in the real world this is not always the case. The total time to perform corrective action is divided into diagnosis time and action time, as shown in [Fig. 5.12](#).

**FIGURE 5.11**

The ASEP model for assessing within-person positive dependence levels for nominal human reliability analysis of pre-accident tasks.

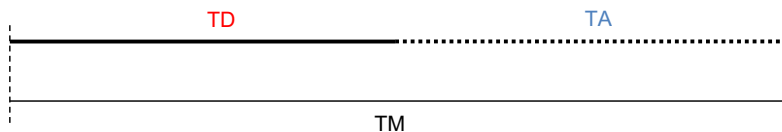
Source: NUREG/CR-4772.



$$TM = TD + TA$$

where TM = maximum time to detect accident, diagnose, take a decision, and perform a post-diagnosis action to control accident; TD = time to detect accident, diagnose, and take a decision to define actions to control accident; and TA = time to perform a post-diagnosis action to control accident.

The probability of success or failure in post-accident analysis is dependent on time. Thus the shorter the time to diagnose or perform corrective action, the higher the probability of human error. Detection and diagnosis involve knowledge-based behavior and post-diagnosis actions involve rule-based behavior or skill-based behavior.



**FIGURE 5.12**

Time to response corrective action in an accident.

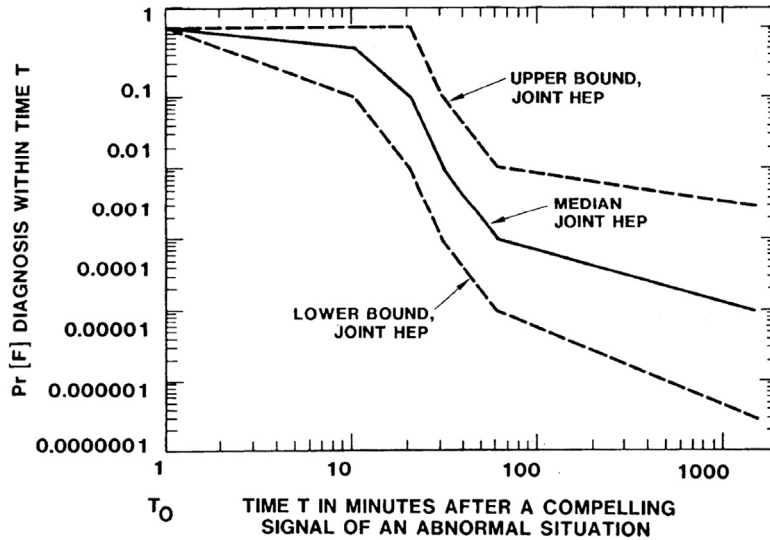


FIGURE 5.13

Nominal diagnosis model (estimate human error probabilities and uncertainty bounds [UCBs] for diagnoses within time).

Source: NUREG/CR-4772.

The ASEP methodology for post-accident analysis proposes the graph shown in Fig. 5.13, which gives the time and human error probability for diagnosing action. Thus it is possible to estimate human probability error based on time having upper and lower limits depending on how conservative the analysis is. The nominal model has more conservative values than the screening model, also proposed to analyze human error probability in diagnosing tasks within time.

After estimating human probability error for diagnosing, it is necessary to estimate the human error probability for post-accident actions. Based on the ASEP methodology proposed in NUREG/CR-4772, such probability is related to particular conditions as shown in Table 5.3.

Table 5.3 Post-Accident Diagnosis of Human Error Probability (Nominal Diagnose Model)		
HEP	EF	Assumptions
100%		Action outside control room is required
100%		It is necessary to perform skill-based behavior action or rule-based behavior action when no procedure is available
5%	5	Perform a critical procedural action correctly under moderately high stress
25%	5	Perform a critical procedural action correctly under extremely high stress
1%	5	Perform a post-diagnosis action, which can be classified as skill-based actions and there is a backup written procedure

HEP, human error probability; EF, error factor.  
Source: NUREG/CR-4772.

To illustrate the post-accident analysis methodology application a similar LPG accident is considered. But this time after the human error in the pre-accident condition, the omission error was because the operator forgot that the drain valve was open and consequently there was LPG leakage; the product then met the ignition source and started a fire below the LPG sphere. Under such circumstances an emergency action is required to avoid BLEVE. To avoid an accident, 10 min to diagnose and at most 50 min for post-diagnosis action are required. Thus, looking at Fig. 5.13, the human error probability to diagnose is 10%, and in this case, because there was a very clear accident scenario, such a situation was detected and the action proposed was based on procedures and protection systems existing close to the LPG sphere. This means the diagnosis was correct and was made on time. However, the post-diagnosis action was performed under a high stress level, and based on Table 5.3 the human error probability for the post-diagnosis action under such circumstances is 25%. The total error probability is calculated by the human reliability analysis event tree, as shown in Fig. 5.14.

$$\begin{aligned}
 &A = \text{Human error diagnosis} \\
 &B = \text{Human error post-diagnosis action} \\
 &P(\text{BLEVE}) = 1 - P(S) = 1 - (P(a) \times P(b))
 \end{aligned}$$

if:

$$\begin{aligned}
 P(a) &= 1 - P(A) = 1 - 0.1 = 0.9 \\
 P(b) &= 1 - P(B) = 1 - 0.25 = 0.75
 \end{aligned}$$

thus:

$$P(\text{BLEVE}) = 1 - P(S) = 1 - (P(a) \times P(b)) = 1 - (0.9 \times 0.75) = 32.5\%$$

The probability of BLEVE in the spheres is high, but the such human error probability is based on the ASEP procedure. If professional opinions are sought or historical data is used, it is possible that the BLEVE probability would be lower.

During ASEP procedures a similar post-accident model is also proposed for screening analysis, that is, a less conservative analysis. As the purpose of this chapter is to introduce human reliability analysis

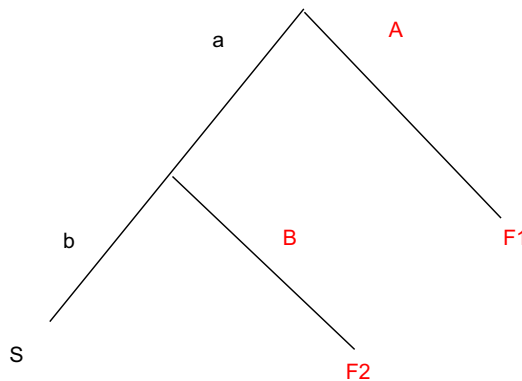


FIGURE 5.14

Human reliability analysis event tree post-accident analysis (LPG sphere fire).

concepts for application in the oil and gas industry, this procedure will not be described because of the human error probability being applied to the nuclear industry and there is no relevant difference from the nominal post-accident model.

The important remarks about ASEP methodology are:

- In general, the terms and the THERP tree to model human error probability are simple to apply.
- This methodology provides a reasonable, simplified version of the THERP dependence model.
- Some accident contexts are presented as guidance for analysis.
- To calculate human error probability it is necessary to define the human error probability for each task based on the cases given.
- There is limited guidance for characterizing applicable PSFs and contextual aspects.

---

## 5.5 HUMAN ERROR ASSESSMENT REDUCTION TECHNIQUE (HEART)

In 1985 the Human Error Assessment Reduction Technique (HEART) was presented by Williams and after 3 years was described in detail. Thus, in general, this methodology is applied to analyzing human tasks with defined values for human error probability (nominal human reliability) related to activities and for contexts where each activity is involved. Based on such values the final human error probabilities formula for activities and error-producing conditions are calculated. The general application steps are as follows:

1. Define the activity;
2. Define the corresponding generic task and define the nominal human unreliability;
3. Define the error-producing condition related to the activity;
4. Assess the rate of the error-producing condition;
5. Calculate the final human error probability.

To calculate the final human error probability the following equation is applied:

$$\text{Final HEP} = \text{GEP} \times \prod R(i) \times (W(i) - 1) + 1$$

where GEP = generic error probability (defined in generic tasks, [Table 5.4](#));  $R(i)$  = value of context task (based on generic context task, [Table 5.5](#) values); and  $W(i)$  = weight for each context task defined for specialist opinion.

To define final human error probability the first step is to define the task that is best defined in [Table 5.4](#). Thus nominal human unreliability is chosen from the proposed range of values on the right.

Thus the main idea is to find the generic task (from A to H) that fits the task under human reliability analysis and further define the human error probability value (nominal human unreliability) based on [Table 5.4](#).

The following step defines the human PSFs, called the error-producing conditions in the tasks, using the HEART methodology. Each error-producing condition has a specific weight, as shown in [Table 5.5](#). In this case, more than one error-producing condition item can be chosen for different tasks and will be applied to the formula to calculate final human error probability.

To illustrate the HEART methodology, a control valve example will be discussed where an old valve is replaced by a new one because of total open failure. The operator bypasses the line where the



	<b>Generic Tasks</b>	<b>Nominal Human Unreliability</b>	
A	Totally unfamiliar, performed at speed with no real idea of likely consequences	0.55	(0.35–0.97)
B	Shift or restore system to a new or original state on a single attempt without supervision or procedures	0.26	(0.14–0.42)
C	Complex task requiring high level of comprehension and skill	0.16	(0.12–0.28)
D	Fairly simple task performed rapidly or given scant attention	0.09	(0.06–0.13)
E	Routine, highly practiced, rapid task involving relatively low level of skill	0.02	(0.07–0.045)
F	Restore or shift a system to original or new state following procedures with some checking	0.003	(0.0008–0.007)
G	Completely familiar, well-designed, highly practiced, routine task occurring several times per day, performed to highest possible standards by highly motivated, highly trained and experienced personnel, with time to correct potential error, but without the benefit of significant job aid	0.0004	(0.00008–0.009)
H	Respond correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of system state	0.00002	(0.000006–0.009) 5th–95th percentile bound

*Source: Willian, J.C., 1988. A data-based method for assessing and reducing human error to improve operational performance. In: Proceeding of IEEE Fourth Conference on Human Factors in Power Plants, pp. 436–450 (Monterey, CA).*

	<b>Error-Producing Condition</b>	<b>Weight</b>
1	Unfamiliarity with a situation that is potentially important but only occurs infrequently or is novel	17
2	A shortage of time available for error detection and correction	11
3	A low signal-to-noise ratio	10
4	A means of suppressing or overriding information of features that is too easily accessible	9
5	No means of conveying spatial and functional information to operators in a form they can readily assimilate	8
6	A mismatch between an operator's model of the world and that imagined by the designer	8
7	No obvious means of reversing an unintended action	8
8	A channel capacity overload, particularly one caused by simultaneous presentation of nonredundant information	6
9	A need to unlearn a technique and apply one that requires the application of an opposing philosophy	6

**Table 5.5 Error-Producing Condition—cont'd**

	<b>Error-Producing Condition</b>	<b>Weight</b>
10	The need to transfer specific knowledge from task to task without loss	5.5
11	Ambiguity in the required performance standards	5
12	A means of suppressing or overriding information of features that is too easily accessible	4
13	A mismatch between perceived and real risk	4
14	No clear, direct, and timely confirmation of an intended action from the portion of the system over which control is exerted	4
15	Operator inexperience (eg, a newly qualified tradesman but not an expert)	3
16	An impoverished quality of information conveyed by procedures and person-person interaction	3
17	Little or no independent checking or testing of output	3
18	A conflict between immediate and long-term objectives	2.5
19	Ambiguity in the required performance standards	2.5
20	A mismatch between the educational achievement level of an individual and the requirements of the tasks	2
21	An incentive to use other more dangerous procedures	2
22	Little opportunity to exercise mind and body outside the immediate confines of a job	1.8
23	Unreliable instrumentation (enough that it is noticed)	1.6
24	A need for absolute judgments that are beyond the capabilities or experience of an operator	1.6
25	Unclear allocation of function and responsibility	1.6
26	No obvious way to keep track of process during an activity	1.4
27	A danger that finite physical capabilities will be exceeded	1.4
28	Little or no intrinsic meaning in a task	1.4
29	High level of emotional stress	1.3
30	Evidence of ill-health among operatives especially fever	1.2
31	Low workforce morale	1.2
32	Inconsistency of meaning of displays and procedures	1.2
33	A poor or hostile environment	1.15
34	Prolonged inactivity or highly repetitious cycling of low mental workload tasks (first half hour)	1.1
34	(Thereafter)	1.05
35	Disruption of normal work/sleep cycles	1.1
36	Task pacing caused by the intervention of others	1.06
37	Additional team members over and above those necessary to perform task normally and satisfactorily (per additional team member)	1.03
38	Age of personnel performing percentual tasks	1.02

*Source: Willian, J.C., 1988. A data-based method for assessing and reducing human error to improve operational performance. In: Proceeding of IEEE Fourth Conference on Human Factors in Power Plants, pp. 436-450 (Monterey, CA).*

valve failure is located and the maintenance professional replaces the failed valve with the new one to repair the valve failure. After the line has been isolated by the maintenance professional, the valve is replaced. In this case, while the operator has experience with such a task, the maintenance professional does not. Thus, after the repair, when the operator sets up the main line with the new valve, leakage was detected 10 min after because of failure to place the new valve correctly. A control valve replacement like this includes five steps:

- Task 1: Check if operator bypassed the line to carry on repair
- Task 2: Check if lines linked to the valve that failed are depressurized and purged
- Task 3: Isolate valve lines
- Task 4: Replace failed valve with new one
- Task 5: Set up the main line with new valve

When applying the HEART procedure the first step is to check [Table 5.4](#) and see which generic tasks are related to those five control valve maintenance tasks. Tasks 1, 2, 3, and 5 are related to generic activity “H,” and nominal human unreliability for such activity is considered 0.00002. However, task 4 is related to generic activity “B,” and nominal human unreliability for such activity is considered 0.26.

The next step is to find the error-producing condition defined in [Table 5.5](#) that is related to each task. Thus error-producing condition number 2, “a shortage of time available for error detection and correction,” is related to tasks 1, 2, and 3 having a weight of 11. The error-producing condition 15, “operator inexperience,” is related to task 4 with weight 3 and also error-producing condition number 29, “high level of emotional stress” with weight 1.3. And finally, task 5 is related to error-producing condition 35, “task pace caused intervention of others,” with weight 1.06.

Now after defining the nominal human unreliability based on [Table 5.4](#) and error-producing condition weights based on [Table 5.5](#) it is necessary to define the importance of each error-producing condition based on specialist opinion.

Therefore for tasks 1, 2, 3, and 5 since there is only one error-producing condition the importance is 100%. For task 4 this importance based on a specialist’s opinion is 70% for “operator inexperience” and 30% for a “high level of emotional stress.” Thus the final human error probability is calculated based on the following equation and as shown in [Table 5.6](#):

$$\text{Final HEP} = \text{GEP} \times \prod R(i) \times (W(i) - 1) + 1$$

In [Table 5.6](#) the first column is the task and the second column is the nominal human unreliability related to the generic tasks based on [Table 5.4](#). The third column is the error-producing condition described in [Table 5.5](#) related to each task, from 1 to 5. Each task may have more than one error-producing condition, but in this case study this only happens to task 4, and it depends only on specialist opinion definitions when assessing the case study. In the fourth column the weight for each error-producing condition is based on [Table 5.5](#). In the fifth column is the importance for each error-producing condition defined by the specialist group that takes part in the human reliability analysis. In the sixth column the partial calculation of the final human error probability for each task is given, that is, by:

$$\prod R(i) \times (W(i) - 1) + 1$$

**Table 5.6 Final Human Error Probability (piori)**

Tasks	Nominal Human Unreliability	Error-Production Condition	Weight	Importance	Weight × Importance	Human Error Probability
1. Check if operator bypassed valve to be repaired	0.00002	A shortage of time available for error detection and correction	11	1	11	0.00022
2. Check if lines linked to valve that failed closed are displeasure and purged	0.00002	A shortage of time available for error detection and correction	11	1	11	0.00022
3. Isolate valve lines	0.00002	A shortage of time available for error detection and correction	11	1	11	0.00022
4. Replace failed valve with new one	0.26	Operator inexperience	3	0.7	2.4	0.68016
		High level emotional stress	1.3	0.3	1.09	
5. Set up the main line with new valve	0.00002	Task pace causes intervention of others	1.06	1	1.06	0.0000212
Human error probability to replace the control valve						68%

where  $R(i)$  = value of context task (defined based on generic context task table values) and  $W(i)$  = weight for each context task defined for specialist group. Regarding task 5 the value in the sixth column is:

$$\prod R(i) \times (W(i) - 1) + 1 = ([1 \times (1.06 - 1)] + 1) = 1.06$$

In the seventh column the human error probability for each task obtained by multiplying the value of the second column by the sixth column is given and is represented by:

$$\text{Final HEP} = \text{GEP} \times \prod R(i) \times (W(i) - 1) + 1$$

For example, for task 4 the value in the sixth column is:

$$\text{Task 4 HEP} = 0.26 \times ([0.7 \times (3 - 1)] + 1) \times ([0.3 \times (1.3 - 1)] + 1) = 0.68$$

After calculating all the human error probability tasks the last step is to sum all the human error probability tasks and finally the final human error probability is:

$$\text{Final HEP} = 0.00022 + 0.00022 + 0.00022 + 0.68016 + 0.0000212 = 0.68$$

Based on the HEART methodology there is a high human error probability (68%) for failure to open the control valve by an inexperienced maintenance professional. If the control valve is replaced by an experienced maintenance professional the final human error is reduced from 68% to 0.5%, as shown in [Table 5.7](#). Thus if task 4 is conducted by an experienced maintenance professional the nominal human error is related to generic task F, “restore or shift a system to original or new state following procedures with some checking,” and the nominal human unreliability is 0.003. In addition, the error-producing condition is only related to number 29, “high level of emotional stress,” with weight 1.3. A similar calculation is made to define the human error probability for each task and to define the final human error probability. The difference in [Table 5.7](#) is that task 4 now has only one error-producing condition because of the new context where experienced maintenance professionals conduct the task. In conclusion, the HEART method has the following advantages:

- Generic values for human error probabilities are based on generic tasks that can be applied in most cases.
- It is an easy method to understand and apply in real human reliability analysis cases.
- It allows specialists to choose human error probability based on a range of probability values.

The disadvantages include:

- In some cases, generic tasks may not fit the case study being assessed;
- HEART was developed to be used in the nuclear and petrochemical industry and may require modification for application in other industries.
- Neither dependence nor error-producing condition interaction is accounted for by HEART.

## 5.6 SOCIOTECHNICAL ANALYSIS OF HUMAN RELIABILITY (STAH-R)

The Sociotechnical Analysis of Human Reliability (STAH-R) method was developed by [Nielson and Philip \(1993\)](#) and uses specialist opinion about human PSFs that influence human error. Furthermore, it is necessary to create a human reliability tree that includes associated human errors and PSFs to

**Table 5.7 Final Human Error Probability (posteriori)**

Tasks	Nominal Human Unreliability	Error-Production Condition	Weight	Importance	Weight × Importance	Human Error Probability
1. Check if operator bypassed valve to be repaired	0.00002	A shortage of time available for error detection and correction	11	1	11	0.00022
2. Check if lines linked to valve that failed closed are displeasure and purged	0.00002	A shortage of time available for error detection and correction	11	1	11	0.00022
3. Isolate valve lines	0.00002	A shortage of time available for error detection and correction	11	1	11	0.00022
4. Replace failed valve with new one	0.003	High level of emotional stress	1.3	1	1.3	0.0039
5. Set up the main line with new valve	0.00002	Task pace causes intervention of others	1.06	1	1.06	0.0000212
Human error probability in take place total open control valve						0.5%

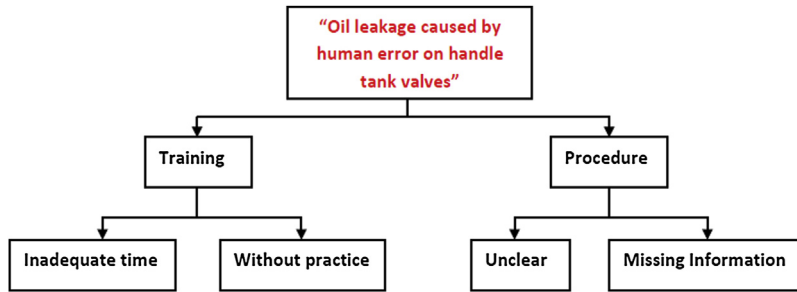


FIGURE 5.15

Human reliability tree (STHR).

represent the human error case under assessment. Thus such a human reliability tree is input into tables and weights are defined for each human performance to calculate the final human error probability.

To illustrate this method an example will be applied in an oil tank product transference case study, which because of human error in properly handling transfer valves, triggered a huge oil leak with environmental impacts.

A group of specialists conducted accident analysis and discovered that training and procedures were the main human factors that influenced the human error. In addition, for training, the root causes of bad performance were inadequate time and not enough operational practice. For the procedure the root causes of human error were an unclear procedure and missing information. Thus, based on this specialist information, the human reliability tree was built and is represented in Fig. 5.15.

The following step is used to define the weight of the PSFs and their cause and to define the human performance factor weight based on specialist opinion. Thus the main questions are:

- What is the time influence on training effectiveness: “enough” or “not enough”?
- What is the practical influence on training effectiveness: “enough” or “not enough”?
- What is the unclear information influence on procedure effectiveness: “much” or “less”?
- What is the missing information influence on procedure effectiveness: “much” or “less”?

Table 5.8 shows the weights for good quality and bad quality training based on the combination of conditions (time and practice). In the first and second columns are the different condition combinations

Table 5.8 Training Weight							
Training							
If	and	So	Chance of Training Quality to Be:		Final Weights (Time and Practice)		
			Good	Bad	Time	Practice	Result
Not enough	Enough		0.7	0.3	0.9	0.2	0.18
Not enough	Not enough		0.1	0.9	0.9	0.8	0.72
Enough	Enough		0.95	0.05	0.1	0.2	0.02
Enough	Not enough		0.6	0.4	0.1	0.8	0.08
	Total		0.265	0.735			

Table 5.9 Procedure Weight							
Procedure							
If	and	So	Chance of Procedure Quality to Be:		Final Weights (Unclear and Missing Information)		
Unclear	Missing Information		Good	Bad	Unclear	Missing Information	Result
Much	Much		0.5	0.5	0.8	0.9	0.72
Much	Little		0.1	0.9	0.8	0.1	0.08
Little	Much		0.3	0.7	0.2	0.9	0.18
Little	Little		0.6	0.4	0.2	0.1	0.02
	Total		0.434	0.566			

assessed line by line. Thus in the first line, if the time is “not enough” and practice is “enough” there is a 70% chance of having good quality in training and a 30% chance of having bad quality. Further, lines for combinations and such probabilities are defined based on specialist opinion concerning the current combination. In the sixth and seventh lines the importance weight for each condition is defined. Thus in the first line, if training time is “not enough,” from 0 to 1, it has 0.9 importance on bad training quality. If practice in training is “enough,” from 0 to 1, it has 0.2 importance on bad training quality. In the final line (total) in the fourth and fifth columns the chance of having a good or bad quality of training is given. The final values in the fourth and fifth columns are obtained by multiplying each probability stated in each line by the value in the last column (result) and adding the following lines. So we have:

$$P(\text{Training quality be good}) = (0.7 \times 0.18) + (0.1 \times 0.72) + (0.95 \times 0.02) + (0.6 \times 0.08) = 0.265$$

The same steps are followed to calculate the chance of bad training quality. The final column value is obtained by multiplying the fifth and sixth column line values. A similar procedure was followed for assessing the chance of the procedure having a good or bad quality, as shown in Table 5.9.

After doing these calculations the values will be put into Table 5.10 as weights to define the final probability for correctly or incorrectly handling the tank valve, and the human error probability is found.

Table 5.10 Human Error Probability (Handling Tank Valve Incorrectly)							
If	and	So	Handle Tank Valves		Weight (Training and Procedure)		
Training	Procedure		Right	Wrong	Training	Procedure	Result
Good	Bad		0.7	0.3	0.265	0.566	0.150
Bad	Good		0.6	0.4	0.735	0.434	0.319
Good	Good		0.99	0.01	0.265	0.434	0.115
Bad	Bad		0.01	0.99	0.735	0.566	0.416
	Total		0.4144	0.58559			



The values in the fifth and sixth columns (training and procedure) came from [Tables 5.9 and 5.10](#) as “chance of training quality” and “chance of procedure quality.” The last column value is the product of the fifth and sixth column values. Thus for the condition combinations given in the first and second columns, specialists give opinions about the chance of the tank valve being handled correctly or incorrectly in the fourth and fifth columns. Similar to other tables the human error probability, or in other words, the chance of handling the tank valve incorrectly, is:

$$\text{HEP} = (0.3 \times 0.15) + (0.4 \times 0.319) + (0.01 \times 0.115) + (0.99 \times 0.416) = 0.585$$

Thus we conclude that the advantages of the STAHR method are:

- Simple to apply;
- Requires experienced specialists to estimate weight and probabilities;
- Uses the human performance factor in human reliability analysis;
- Allows fast human error probability calculation.

The disadvantages of the STAHR method are:

- Depends heavily on specialist point of view;
- Requires more applications to be validated.

---

## 5.7 STANDARDIZED PLANT ANALYSIS RISK-HUMAN RELIABILITY (SPAR-H)

In support of the Accident Sequence Precursor (ASP) program, the USNRC, in conjunction with the Idaho National Laboratory, in 1994 developed the Accident Sequence Precursor Standardized Plant Analysis Risk Retain Human Reliability (ASP/SPAR) model for the human reliability analysis method, which was used in the development of nuclear power plant models. Based on experience gained in field testing, this method was updated in 1999 and renamed SPAR-H, for Standardized Plant Analysis Risk-Human Reliability method ([NUREG/CR-6883](#)).

The main objective is to define human error probability based on human performance factors influence. Such methodology requires a specialist opinion to define the human factors influence based on PSF values. The performance factors include human error probability as shown in the following equation:

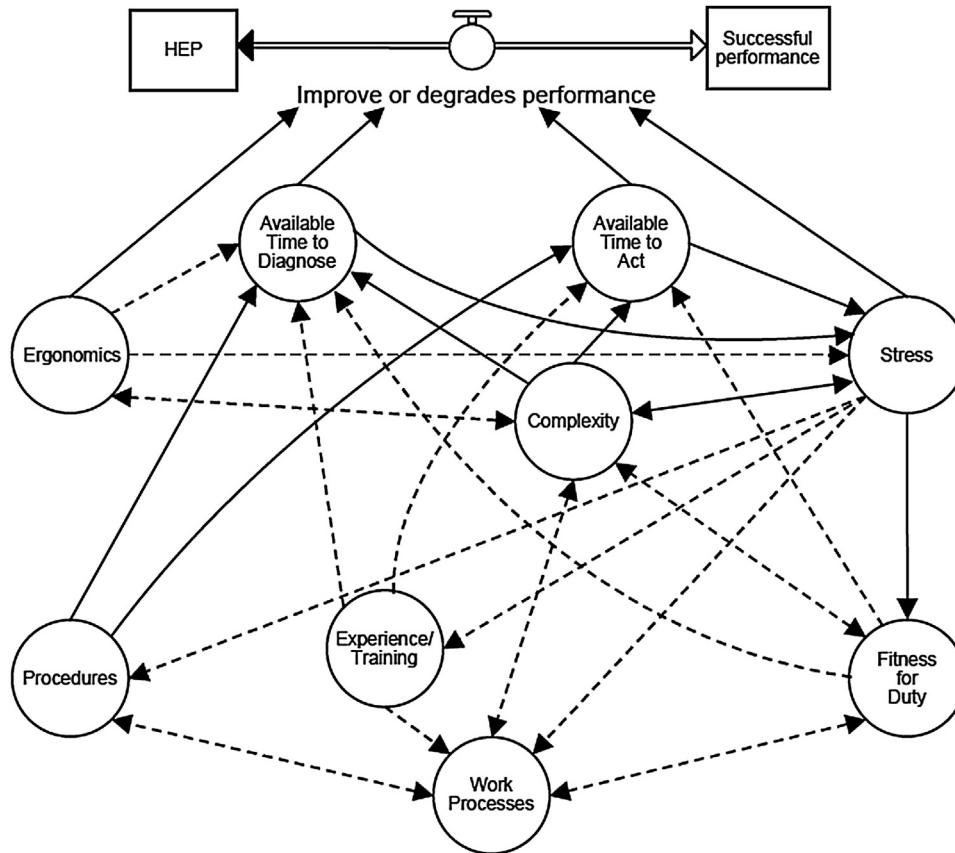
$$\text{HEP} = \frac{\text{NHEP} \cdot \text{PSF}_{\text{composite}}}{\text{NHEP} \cdot (\text{PSF}_{\text{composite}} - 1) + 1} \quad (1)$$

Such a method establishes the value of human error probability of omission error (0.01) and commission error (0.001). The SPAR-H method is based on eight PSFs ([Boring and Gertman, 2005](#)) that encapsulate the majority of the contributors to human error. These eight PSFs are as follows: available time to complete task, stress and stressors, experience and training, task complexity, ergonomics, the quality of any procedures in use, fitness for duty, and work processes. Each PSF feature is listed with different levels and associated multipliers. For example, the presence of extremely high stress would receive a higher multiplier than moderate stress. [Table 5.11](#) shows the PSF values used to define the  $\text{PSF}_{\text{composite}}$ .

The SPAR-H method is straightforward, easy to apply, and is based on human performance and results from human performance studies available in the behavioral sciences literature ([NUREG/CR-6883](#)).

<b>Table 5.11 PSF Values</b>		
<b>PSFs</b>	<b>PSF Level</b>	<b>Multiplier for Action</b>
Available time	Inadequate time	$P(f) = 1$
	Time available $\approx$ time required	10
	Nominal time	1
	Time available $\geq 5 \times$ time required	0.1
	Time available $\geq 50 \times$ time required	0.01
Stress	Insufficient information	1
	Extreme	5
	High	2
Complexity	Nominal	1
	Insufficient information	1
	Highly complex	5
	Moderately complex	2
Experience/Training	Nominal	1
	Insufficient information	1
	Low	3
	High	0.5
Procedures	Insufficient information	1
	Not available	50
	Incomplete	20
	Available but poor	5
	Nominal	1
Ergonomics	Insufficient information	1
	Missing/Misleading	50
	Poor	10
	Nominal	1
Fitness for duty	Good	0.5
	Insufficient information	1
	Unfit	$P(f) = 1$
	Degraded fitness	5
Work process	Nominal	1
	Insufficient information	1
	Poor	5
	Good	0.5
	Insufficient information	1

Source: NUREG, CR-6883.



**FIGURE 5.16**

Path diagram showing relationships among PSFs.

Source: NUREG/CR-6883.

The main question concerning human factors in the SPAR-H method is the relation between such human factors and how they influence human reliability. The relation between PSFs can be represented as shown in Fig. 5.16.

To illustrate the SPAR-H method an example is given of human error in the startup of a compressor in a propylene plant, which shows that a supply energy breakdown caused the propylene plant shutdown. One of most complex pieces of equipment to start up is a compressor, and in this case the compressor was new and the operators and maintenance team were not familiar with the startup steps and relied on a general procedure. In addition, whenever there is a propylene plant shutdown there is a high stress level to get the plant started again so as not to experience an additional loss of production. Based on the compressor startup scenario information, Table 5.12 shows the classification for human PSFs.

<b>Table 5.12 PSF Values (priori)</b>		
<b>PSFs</b>	<b>PSF Levels</b>	<b>Multiplier for Action</b>
Available time	Inadequate time	$P(f) = 1$
	Time available is $\approx$ the time required	10
	Nominal time	1
	Time available $\geq 5 \times$ the time required	0.1
	Time available $\geq 50 \times$ the time required	0.01
Stress/Stressor	Insufficient information	1
	Extreme	5
	High	2
	Nominal	1
Complexity	Insufficient information	1
	Highly complex	5
	Moderately complex	2
	Nominal	1
Experience/ Training	Insufficient information	1
	Low	3
	Nominal	1
Procedures	High	0.5
	Insufficient information	1
	Not available	50
	Incomplete	20
	Available but poor	5
Ergonomics/HMI	Nominal	1
	Insufficient information	1
	Missing/Misleading	50
	Poor	10
	Nominal	1
Fitness for duty	Good	0.5
	Insufficient information	1
	Unfit	$P(f) = 1$
	Degraded fitness	5
Work process	Nominal	1
	Insufficient information	1
	Poor	5
	Nominal	1
	Good	0.5
	Insufficient information	1

HMI, human machine interface.

Based on the SPAR-H procedure the commission human error probability is 0.001, and regarding human factors, the human error probability to start up the compressor is:

$$\begin{aligned} \text{PFS}_{\text{composite}} &= \prod_1^8 \text{PFS} = 10 \times 5 \times 5 \times 3 \times 1 \times 0.5 \times 1 \times 0.5 = 187.5 \\ \text{HEP} &= \frac{\text{NHEP} \cdot \text{PFS}_{\text{composite}}}{\text{NHEP} \cdot (\text{PFS}_{\text{composite}} - 1) + 1} \\ &= \frac{0.001 \cdot 187.5}{0.001 \cdot (187.5 - 1) + 1} = 0.158 \cong 15.8\% \end{aligned}$$

The human error probability is high and can explain how much such PSFs influence human error probability in compressor startup. After realizing the problem and discussing the root cause, the maintenance and operation team came to the conclusion that it was not an equipment problem but the human skill required to start the compressor. Thus the compressor supplier provided more details on the startup procedure and consequently the human error probability was reduced (a posteriori). The new values for PSFs (a posteriori) are given in [Table 5.13](#).

Based on the SPAR-H procedure the compressor startup human error probability is 0.001, and for the new human factor scores the human error probability to start up the compressor is:

$$\begin{aligned} \text{PFS}_{\text{composite}} &= \prod_1^8 \text{PFS} \\ \text{PFS}_{\text{composite}} &= 10 \times 2 \times 2 \times 1 \times 1 \times 0.5 \times 1 \times 0.5 = 10 \\ \text{HEP} &= \frac{\text{NHEP} \cdot \text{PFS}_{\text{composite}}}{\text{NHEP} \cdot (\text{PFS}_{\text{composite}} - 1) + 1} \\ &= \frac{0.001 \cdot 10}{0.001 \cdot (10 - 1) + 1} = 0.0099 \cong 0.99\% \end{aligned}$$

After training, the maintenance and operation teams were able to create a better and clearer procedure with all the startup steps. Experience increased; however, the stress to start up the compressor in the available time is still a PSF that influences human error in compressor startup.

The SPAR-H procedure was created for the nuclear industry but can be used for other industries such as oil and gas. But the omission and commission error values and PSF values given earlier in [Table 5.11](#) must be validated by a specialist when applied to the oil and gas industry cases.

The omission and commission errors can be calculated if human error data is available or estimated by a specialist. The values in [Table 5.11](#) have different weights, and a different table with different values for each PSF can be created and validated for specific activities. A good test for validating [Table 5.11](#) values is to apply different human reliability analysis models and compare the final human error probabilities.

The SPAR-H model disadvantages are:

- Does not consider the direct interaction effects between the PSFs;
- Depends on the situation and it is necessary to consider other PSFs (ie, those not given in [Table 5.11](#)).

<b>Table 5.13 PSF Values (posteriori)</b>		
<b>PSFs</b>	<b>PSF Levels</b>	<b>Multiplier for Action</b>
Available time	Inadequate time	$P(f) = 1$
	Time available is $\approx$ the time required	10
	Nominal time	1
	Time available $\geq 5 \times$ the time required	0.1
	Time available $\geq 50 \times$ the time required	0.01
Stress/Stressor	Insufficient information	1
	Extreme	5
	High	2
	Nominal	1
Complexity	Insufficient information	1
	Highly complex	5
	Moderately complex	2
	Nominal	1
Experience/ Training	Insufficient information	1
	Low	3
	Nominal	1
Procedures	High	0.5
	Insufficient information	1
	Not available	50
	Incomplete	20
	Available, but poor	5
Ergonomics/HMI	Nominal	1
	Insufficient information	1
	Missing/Misleading	50
	Poor	10
	Nominal	1
Fitness for duty	Good	0.5
	Insufficient information	1
	Unfit	$P(f) = 1$
	Degraded fitness	5
Work process	Nominal	1
	Insufficient information	1
	Poor	5
	Nominal	1
	Good	0.5
	Insufficient information	1

The SPAR-H model disadvantages are:

- Does not consider the direct effects of PSFs;
- Depends on the situation and it is necessary to consider other PSFs (ie, those not given in [Table 5.11](#)).

---

## 5.8 SUCCESS LIKELIHOOD INDEX METHODOLOGY IMPLEMENTED THROUGH MULTI-ATTRIBUTE UTILITY DECOMPOSITION (SLIM-MAUD)

In the 1980s, the USNRC embarked on a multiyear research program to investigate different methods for using expert judgments to estimate human error probabilities in nuclear power plants. One of the methods investigated, derived from multiattribute utility theory, is the Success Likelihood Index Methodology implemented through Multi-Attribute Utility Decomposition (SLIM-MAUD).

Brookhaven National Laboratory developed and evaluated one method of obtaining human reliability estimates from expert judges using SLIM. SLIM comprises a set of procedures based on Multi-Attribute Utility Theory for eliciting and organizing estimates by experts of the probability of success or failure of specific human actions in nuclear power plants.

The feasibility and implementability of SLIM were evaluated in a multiphase investigation. In the first phase the basic characteristics of SLIM were defined ([Embrey et al., 1984](#)). Phases 2 and 3 consisted of an experimental evaluation and field test of SLIM. In Phase 4, SLIM was linked to an interactive computer program based on MAUD, and procedures for applying the resultant SLIM-MAUD methodology were developed ([Embrey et al., 1984](#)).

The following is a description of the method. The SLIM method steps are:

1. Constitution of the group of experts and first approach to the case of analysis;
2. Definition and selection of the PSFs in the case analysis;
3. Assignment of weighting factors for each PSF;
4. Scoring of each PSF;
5. Calculation of the success likelihood index (SLI);
6. Conversion of the SLI in HEP.

The first step requires knowledge of the activity that is being assessed. Therefore it is necessary to involve employees who have a good knowledge of such activity to identify PSFs and which one has more influence in such human error activity.

Therefore, the second step was to request the specialist opinion about the performance factors by taking into account the weight which varies from 0% to 100%. In doing so, it is necessary to score each PSF per task which the value varies from 1 to 9, depends on PSF characteristics. In cases of PSFs that require high performance, for example, training case, the best score is 9. However, in cases of PSFs that require lower performance, for example, stress, the best score is 1.

To carry out such an assessment it is advisable to create a table that describes the tasks and PSFs so that it is easier to understand and calculate HEP. [Table 5.14](#) describes an example of a PSF score regarding the case of four tasks concerning three different performance factors to be assessed using the SLIM method with a specialist opinion about PSF levels. The tasks are related to a valve repair, which are:

Task 1: Emergency shutdown valve failure detection

Task 2: Pipeline isolation

**Table 5.14 SLIM-MAUD Score**

Score Table			
Tasks	Procedure	Training	Supervision
Task 1	6	8	9
Task 2	7	8	9
Task 3	6	9	9
Task 4	9	8	9

Task 3: Emergency shutdown valve repair  
 Task 4: Pipeline liberation

After defining the score for PSF and its weights it is necessary to calculate SLIM by multiplying scores per weights and adding values to achieve one SLIM per task, as shown in Table 5.15.

In Table 5.14 the following were considered as weights for each PSF:

- 20% for supervision;
- 50% for procedure;
- 20% for training.

After calculating SLIM is necessary to calculate HEP using the following equation:

$$\log P = aSLI + b$$

To define “a” and “b” parameters it is necessary to have the  $P(HEP)$  value that can be considered by specialist opinion. In doing so, and regarding 0.1 and 0.0001 for task 1 and 2, respectively, the final equation will calculate HEP for each task, thus the equation will be:

$$HEP = 10^{(-2 \times SLI + 12.4)}$$

The final step is to apply the SLI value for each task in the preceding equation. Table 5.16 shows the final human error probability.

Based on this result, the HEP is 1.3%. Task 1 has with more impact on HEP but in general the task has a low human error probability. In case of high HEP, a recommendation must be implemented to reduce the HEP based on PSF effects mitigation. Therefore a new score assessment must take place, which results in a new lower HEP, which will be achieved after recommendation.

**Table 5.15 SLIM-MAUD Score and Weights**

SLIM Table				
Tasks	Procedure	Training	Supervision	SLIM
Task 1	6 × 0.5	8 × 0.3	9 × 0.2	7.2
Task 2	7 × 0.5	8 × 0.3	9 × 0.2	7.7
Task 3	6 × 0.5	9 × 0.3	9 × 0.2	7.5
Task 4	9 × 0.5	8 × 0.3	9 × 0.2	8.5



<b>Task</b>	<b>aSLI + b</b>	<b>HEP</b>
Task 1: Emergency shutdown valve failure detection	-2	0.01
Task 2: Pipeline isolation	-3	0.001
Task 3: Valve repair	-2.6	0.002511
Task 4: Pipeline liberation	-4.6	0.00002511
Final HEP		0.01353611

In general, SLIM-MAUD has the following advantages:

- Simple to apply;
- Takes into account the performance factors and its influence on HEP;
- Allows fast HEP calculation.

The SLIM-MAUD disadvantages are:

- Does not consider the direct effect among PSFs;
- Depends on specialist elicitation, which in some cases can lead to a high HEP value.

## 5.9 SYSTEMATIC HUMAN ERROR REDUCTION AND PREDICTION APPROACH (SHERPA)

The Systematic Human Error Reduction and Prediction Approach (SHERPA) (Embrey et al., 1984) uses hierarchical task analysis (HTA; Annett et al., 1971) together with error taxonomy to identify credible errors associated with a sequence of human activity. Basically, such a human reliability analysis method uses specialist elicitation to define human error probability based on its experience for different levels of task defined by hierarchy level as well as the type of human error, cause, consequence, and recovery action.

The SHERPA first step is to define the activity that is supposed to be critical and define the activity at different task levels. Therefore to have a consistent task definition at different levels the HTA takes place.

Indeed, the HTA is based on factors such as goals, operations, and plans. The goals are related to what is expected to be achieved in a task. The operations are the actions to achieve the goals and the plan is defined as the sequence of actions required to achieve the goals. However, in the SHERPA method the tasks are classified as follows:

- Action (eg, close a valve, trigger a button, shut down a piece of equipment);
- Retrieval (eg, collect information from an indicator, monitor, or manual);
- Checking (eg, perform a procedural verification);
- Selection (eg, chose an alternative solution);
- Information communication (eg, send or receive information from another employee).

Action	Checking	Information Entry	Information
Action omitted	Check omitted	Information not required	Information not communicated
Right action, wrong object	Wrong object checked	Information entered into wrong place	Wrong information communicated
Action incomplete	Check incomplete	Information wrong	Information communicated incomplete
Action too late/too early	Check too late/too early	Information entry not verified	Information communicated unclear

In addition to HTA it is also necessary to implement further steps. The SHERPA method can be described in six basic steps:

- HTA: The main objective is to structure the task hierarchy to enable a clear human reliability analysis.
- Task classification: The task classification describes the type of human error that has occurred in each type of task such as omission and commission error, as described in [Table 5.17](#).
- Human error identification: Describes the nature of human error.
- Consequence analysis: Identifies the severity of the human error that occurred in the task.
- Recovery analysis: Describes the action that is able to mitigate or eliminate the human error related to a certain task.
- Tabulation: The main objective is to summarize the information assessed in a table, which may also include the probability and consequence of human error for each task. Such tabulation can also have the risk assessment based on a risk matrix classification, which includes occurrence and severity assessment.

To exemplify the SHERPA methodology, let us consider human error during a platform maintenance when moving equipment parts. This can have as an incident material dropped into the sea, which affects flowline integrity with serious consequences to the environment and also to operational cost. Based on SHERPA methodology the first step is to define the task hierarchy, which is defined as:

- Level 0: Equipment part movement on top site
- Level 1: Task 1—Check the procedure
- Level 1: Task 2—Isolate the area
- Level 1: Task 3—Communication between operators
- Level 1: Task 4—Equipment part movement

The second step is task classification, which based on [Table 5.17](#).

- Action
- A1: Action omitted
- A2: Right action, wrong equipment
- A3: Action incomplete

**Table 5.18 Risk Matrix**

		FREQUENCY CATEGORY					
		A (extremely remote)	B (remote)	C (Little frequency)	D (Frequent)	E (Very frequent)	F (Extremely frequent)
		At least 1 between 1000 and 100000 years	At least 1 between 50 and 1000	At least 1 between 30 and 50 years	At least 1 between 5 and 30 years	At least 1 in 5 years	At least 1 in 1 year
SEVERITY CATEGORY	IV	M	NT	NT	NT	NT	NT
	III	M	M	NT	NT	NT	NT
	II	T	T	M	M	M	M
	I	T	T	T	M	M	M

- A4: Action too late/too early
- A5: Wrong action
- A6: Action too fast/too slow
- Checking
- C1: Check omitted
- C2: Wrong document checked
- C3: Updated document not checked
- C4: Check incomplete document
- C5: Check too late/too early
- Communication
- Co1: Information not communicated
- Co2: Wrong information communicated
- Co3: Information communicated incomplete
- Co4: Information communicated unclear

The next step is to describe the human error associated with each task and the consequence, which is described in Table 5.20. To perform a risk assessment of human error associated with each task, the risk matrix and severity classification are defined in Tables 5.18 and 5.19.

### 5.10 BAYESIAN NETWORK

The Bayesian network method was developed in the 1980s to make a prediction in artificial intelligence analysis easier (Pearl, 1998). It can be defined as graphical frameworks that represent arguments

**Table 5.19 Severity**

Description and Characteristic						
			Personal Safety	Installation	Environment and Image	Social
Severity category	IV	Catastrophic	Catastrophic injuries with death; it is possible to affect people outside	Losses of equipment and plant with high cost to buy new one	Loss of ecosystem with poor national and international company reputation	Economic effects on local activities, health cost to local population, economic losses to tourism, ecosystem local losses and quality of life losses (between R\$101,000,000.00 and R\$336,000,000.00)
	III	Critical	Critical injuries. Employees stay a period of time out of workplace	Equipment seriously damaged with high cost to repair	Critical effects to environment being hard to improve ecosystem condition even with human actions. Poor national and international company reputation	Economic effects on local activities, health cost to local population, economic losses to tourism, ecosystem local losses (between R\$2,500,000.00 and R\$101,000,000.00)
	II	Marginal	Moderate injuries with first aid assistance	Low equipment damage with low repair cost	No serious environmental effect but it is necessary for human intervention and actions to improve environment Poor national company reputation	Economic effects on local activities, health cost to local population, economic losses to tourism, fishing and other areas (from R\$0.00 to R\$2,500,000.00)
	I	No effect	There are no injuries or damage to health	There is no damaged to equipment and plant	Insignificant environmental effect. There is no necessity for human action to ecosystem improvement. There is no effect on national company reputation	There are no economic effects on local activities or health cost to local population

**Table 5.20 SHERPA Tabulation**

Task	Error Code	Description	O	Consequence	S	R	Recovery	O	S	R	
1	C1	Lack of procedure	F	Drop of objects into the sea, which causes damage to the flowline	III	FIII	Provide a procedure to move equipment part on top of the platform	B	III	BIII	
2	A4	Late area isolation	F			FIII	Establish isolation before starting to move equipment part	B			BIII
3	Co4	Informal communication	E			FIII	Establish standard communication in procedure	B			BIII
4	A6	Equipment part moving too fast	F			FIII	Define the time to perform the task considering safe aspects and all procedural steps	B			BIII

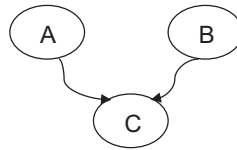


FIGURE 5.17

Bayesian network.

in uncertain domains (Korb and Nicholson, 2003). Such frameworks are unicycle graphs because they cannot create closed cycles and have only one direction. The nodes represent random variables and arcs represent direct dependency between variable relations. The arc directions represent the cause—effect relationship between variables (Menezes, 2005). In Fig. 5.17, the Bayesian network represented as node C is a consequence of nodes A and B.

In Fig. 5.17, nodes A and B are the fathers of C, and node C is called the son of A and B. At each node there are conditional probabilities that represent the variable values of the event. The conditional probability is calculated by the Bayes equation and for two events is represented mathematically as:

$$P(A|B) = \frac{P(B|A) \times P(A)}{P(B)}$$

where:

$P(A|B)$  = Posteriori probability of A when B is known

$\frac{P(B|A)}{P(B)}$  = Maxi likelihood related to B with A evidence occurrence.

$P(A)$  = Is priori probability of event A.

The previous equation is a Bayesian representation for two conditional events, but in some cases more events are included in the Bayesian network and are harder to calculate. The bigger the Bayesian network, the more complex it is to calculate, and it is best to use software for such calculations when possible. In addition, the larger the Bayesian network, the harder the PSFs associated with human error are to obtain precisely, and predicting conditional probabilities is also harder. In general terms, the Bayesian network probability can be represented by:

$$P(U) = P(X_1, X_2, X_3, \dots, X_n) = \prod_{i=1}^n P(X_i / Pf(X_i))$$

where:

$P(U)$  = Probability;  $P(X_i / Pf(X_i))$  = Conditional probability of X related to their network father.

The Bayesian belief networks method provides greater flexibility, as it not only allows for a more realistic representation of the dynamic nature of a human system, but also allows for representation of the relationship of dependence among the events and PSFs (Drouguett, 2007).

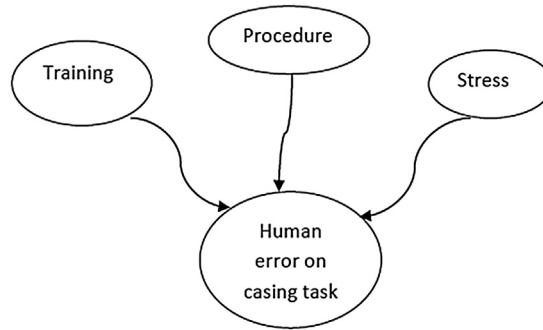


FIGURE 5.18

Bayesian network (casing drilling).

To clarify such methodology, a Bayesian network example applied to assess human error in a casing task when drilling a well can be assessed for training, procedure, and stress as human performance factors. Thus the Bayesian network is represented in Fig. 5.18.

Let  $T_1$  be the variable related to the level of training of the operator in such a way that  $T_1 = 0$  implies adequate training and  $T_1 = 1$  represents inadequate training. In the same way, let  $P_2$  and  $S_3$  be the variables associated with the adequacy of execution of the available procedure and the level of stress of the operator, respectively. Finally, let  $C$  be the human performance, where  $C = 0$  implies adequate performance and  $C = 1$  implies human error.

Thus human error probability =  $P(C = 1)$ . In general,  $P(C = 1)$  is represented by:

$$\text{HEP} = \sum_{i=0}^1 \sum_{j=0}^1 \sum_{k=0}^1 P(T_1 = i) \times P(P_2 = j) \times P(S_3 = k) \times P(C = 1 | T_1 = i, P_2 = j, S_3 = k)$$

where  $\bar{C}$  = human error in casing task = ( $C = 1$ );  $T$  = good training ( $T_i = 0$ );  $\bar{T}$  = bad training ( $T_i = 1$ );  $P$  = good procedure ( $P_i = 0$ );  $\bar{P}$  = bad procedure ( $P_i = 1$ );  $S$  = good stress level ( $S_i = 0$ ); and  $\bar{S}$  = bad stress level ( $S_i = 1$ ).

Thus:

$$\begin{aligned} \text{HEP} = & P(\bar{C} | \bar{T}, \bar{P}, \bar{S}) \times P(\bar{T}) \times P(\bar{P}) \times P(\bar{S}) + P(\bar{C} | T, \bar{P}, \bar{S}) \times P(T) \times P(\bar{P}) \times P(\bar{S}) \\ & + P(\bar{C} | \bar{T}, \bar{P}, S) \times P(\bar{T}) \times P(\bar{P}) \times P(S) + P(\bar{C} | T, \bar{P}, S) \times P(T) \times P(\bar{P}) \times P(S) \\ & + P(\bar{C} | \bar{T}, P, \bar{S}) \times P(\bar{T}) \times P(P) \times P(\bar{S}) + P(\bar{C} | T, P, \bar{S}) \times P(T) \times P(P) \times P(\bar{S}) \\ & + P(\bar{C} | \bar{T}, P, S) \times P(\bar{T}) \times P(P) \times P(S) + P(\bar{C} | T, P, S) \times P(T) \times P(P) \times P(S) \end{aligned}$$

Such probability values are estimated by specialist opinion by using the following questionnaire:

1. What is the probability of failure in the “casing task” if training is not good? (Optimist = 40% and pessimist = 60%)
2. What is the probability of failure in the “casing task” if the procedure is not good? (Optimist = 60% and pessimist = 90%)
3. What is the probability of failure in the “casing task” if stress is not good? (Optimist = 20% and Pessimist = 40%)

4. What is the probability of failure in the “casing task” if training, procedure, and stress are not good? (Optimist = 90% and pessimist = 100%)
5. What is the probability of failure in the “casing task” if procedure and stress are not good and training is good? (Optimist = 80% and pessimist = 90%)
6. What is the probability of failure in the “casing task” if procedure and training are not good and stress is good? (Optimist = 80% and pessimist = 90%)
7. What is the probability of failure in the “casing task” if the procedure is not good and stress and training are good? (Optimist = 60% and pessimist = 70%)
8. What is the probability of failure in the “casing task” if stress and training are not good and procedure is good? (Optimist = 20% and pessimist = 30%)
9. What is the probability of failure in the “casing task” if stress is not good and procedure and training are good? (Optimist = 10% and pessimist = 20%)
10. What is the probability of failure in the “casing task” if training is not good and procedure and stress are good? (Optimist = 20% and pessimist = 40%)
11. What is the probability of failure in the “casing task” if stress, procedure, and training are good? (Optimist = 1% and pessimist = 2%)

In doing so, substituting the probability values in this equation, we have:

$$\begin{aligned}
 \text{HEP} = & [P(\bar{C}|\bar{T}, \bar{P}, \bar{S}) \times P(\bar{T}) \times P(\bar{P}) \times P(\bar{S})] + [P(\bar{C}|T, \bar{P}, \bar{S}) \times P(T) \times P(\bar{P}) \times P(\bar{S})] \\
 & + [P(\bar{C}|\bar{T}, \bar{P}, S) \times P(\bar{T}) \times P(\bar{P}) \times P(S)] + [P(\bar{C}|T, \bar{P}, S) \times P(T) \times P(\bar{P}) \times P(S)] \\
 & + [P(\bar{C}|\bar{T}, P, \bar{S}) \times P(\bar{T}) \times P(P) \times P(\bar{S})] + [P(\bar{C}|T, P, \bar{S}) \times P(T) \times P(P) \times P(\bar{S})] \\
 & + [P(\bar{C}|\bar{T}, P, S) \times P(\bar{T}) \times P(P) \times P(S)] + [P(\bar{C}|T, P, S) \times P(T) \times P(P) \times P(S)] \\
 \text{HEP} = & [1 \times 0.6 \times 0.9 \times 0.4] + [0.9 \times 0.4 \times 0.9 \times 0.4] + [0.9 \times 0.6 \times 0.9 \times 0.6] \\
 & + [0.7 \times 0.4 \times 0.9 \times 0.6] + [0.3 \times 0.6 \times 0.1 \times 0.4] + [0.2 \times 0.4 \times 0.1 \times 0.4] \\
 & + [0.4 \times 0.6 \times 0.1 \times 0.6] + [0.02 \times 0.4 \times 0.1 \times 0.6] = 81.36\%
 \end{aligned}$$

In general, the advantages of Bayesian networks are:

- The relations between PSFs and human error probability can be calculated by conditional probabilities.
- If applied using Bayesian network software, the human error probability calculations are easier.
- Bayesian networks are easy to understand graphically when applied to human reliability problems.

The disadvantages are:

- There are difficulties in obtaining conditional probabilities in data banks.
- The higher the number of PSFs that influence human error probabilities, the harder it is to get reliable information from specialists.

---

## 5.11 CASE STUDY

In this chapter we presented several human reliability techniques with different case studies, despite the advantages and disadvantages. Additionally, when applying different human reliability analysis



techniques for similar case studies, the most critical human PSF will be the same for all and human error probability may be similar. To check this assumption, we will conduct a case study with the same group of specialists and assess the same problem for different human reliabilities approaches, and in the end there will be an interesting conclusion about human error probability and performance factors.

Thus the following case study is presented that analyzes human failure in opening and closing valves to start up a turbine after maintenance. The startup steps are as follows:

- Step 1: Close vapor valve
- Step 2: Close suction valve
- Step 3: Open suction valve
- Step 4: Open vapor valve

In the event of failure in startup sequence tasks the turbine can shut down and may have damage that could take from 2 h to 1 month to fix, depending on the severity of the damage to the turbine. The turbine shutdown does not cause any damage to other systems, but the economic consequences of using electrical energy vary from \$1250 to \$450,000 for 2 h or 1 month of turbine damage, respectively.

The startup procedure was conducted by one inexperienced employee and his supervisor checked his steps and realized that the sequence was performed incorrectly, but there was time to correct it. Further, the failure was assessed and improvement was implemented in the procedure that was not clear to the operator.

To find out how much loss of money is expected in the failure of the turbine startup a human reliability analysis was conducted to define the human error probability regarding two scenarios: before and after improvement. The consensus group method was applied to define probabilities and other score values, and each member contributed to the discussion and defined score values.

The main objective of this case study is to define the human error probability, and, furthermore, to compare different human reliability analysis methods to implement in operational routines to assess human failure. Six methods (THERP, OAT, STAHR, HEART, SPAR-H, and Bayesian network) will be applied and compared.

### 5.11.1 THERP CASE STUDY APPLICATION

When applying the THERP method the first step after understanding the case study is to create the human reliability tree and further define the probabilities based on specialist opinion. Thus Fig. 5.19 shows a human reliability tree for the four turbine startup steps:

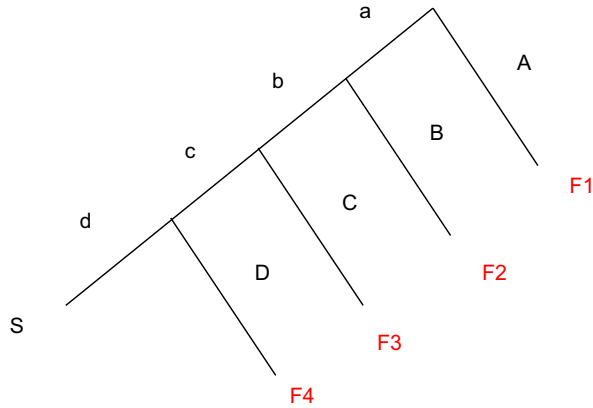
- Task 1: Close vapor valve (success: a; fail: A)
- Task 2: Close suction valve (success: b; fail: B)
- Task 3: Open suction valve (success: c; fail: C)
- Task 4: Open vapor valve (success: d; fail: D)

Based on specialist opinion, the probabilities of human error in turbine startup for each task are:

$$P(\text{turbine start up human error}) = 1 - P(\text{success})$$

$$P(\text{success}) = P(a) \times P(b) \times P(c) \times P(d) = 0.85 \times 0.9998 \times 0.95 \times 0.9999 = 0.8073$$

$$P(\text{turbine start up human error}) = 1 - 0.8073 = 19.27\%$$

**FIGURE 5.19**

Human reliability tree (THERP).

Despite not having the human PSF in THERP analysis, the discussion among specialists indicated that if the procedure was improved the human error probability would reduce to 14.59%, as shown in the following equation:

$$P(\text{turbine start up human error}) = 1 - P(\text{success})$$

$$P(\text{success}) = P(a) \times P(b) \times P(c) \times P(d) = 0.9 \times 0.999 \times 0.95 \times 0.9999 = 0.854.$$

$$P(\text{turbine start up human error}) = 1 - 0.854 = 14.6\%$$

The main advantage of the THERP application is the direct and relative simple methodology to calculate human error probability. By the other hand, the main disadvantage of the THERP is the lack of the human performance factors in human error probability calculation.

### 5.11.2 OAT CASE STUDY APPLICATION

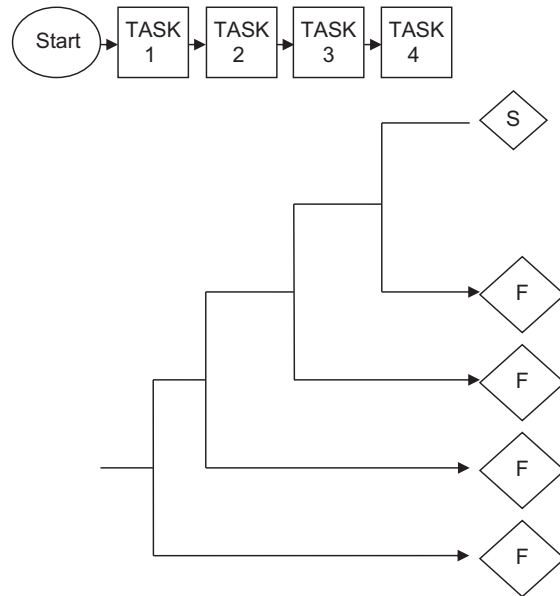
When applying the OAT methodology the first step after understanding the case study is to create the human reliability event tree and further define the probabilities based on specialist opinion and then calculate the human error probability. Thus Fig. 5.20 shows the human reliability event tree for four the turbine startup steps:

- Task 1: Close vapor valve (F1—fail Task 1)
- Task 2: Close suction valve (F2—fail Task 2)
- Task 3: Open suction valve (F3—fail Task 3)
- Task 4: Open vapor valve (F4—fail Task 4)

$$P(\text{turbine startup human error}) = 1 - P(\text{success})$$

FIGURE 5.20

Operator action tree (OAT).



For the same Turbine start up case study, the similar human error probability result is achieved by applying the OAT analysis as shows the equation below.

$$P(\text{success}) = (1 - P(F_1)) \times (1 - P(F_2)) \times (1 - P(F_3)) \times (1 - P(F_4))$$

$$= 0.85 \times 0.9998 \times 0.95 \times 0.9999 = 0.8073$$

$$P(\text{turbine startup human error}) = 1 - 0.8073 = 19.27\%$$

Similar to the THERP case, despite having the human PSFs in the OAT analysis, the discussion among specialists indicated that if the procedure was improved the human error probability would reduce to 14.59%, as shown by:

$$P(\text{success}) = (1 - P(F_1)) \times (1 - P(F_2)) \times (1 - P(F_3)) \times (1 - P(F_4))$$

$$= 0.9 \times 0.9999 \times 0.95 \times 0.9999 = 0.854.$$

$$P(\text{turbine startup human error}) = 1 - 0.854 = 14.6\%$$

Similar to the THERP case, the main advantage of the OAT application is an easy methodology to calculate the human error probability, despite not having the human PSFs, which is again the main disadvantage of this technique. The expected cost of human error is similar for both THERP and OAT because of similar probabilities. Thus for 19.27% human error probability the expected cost of human failure varies from \$240.87 (19.27% × \$1250) to \$86,715 (19.27% × \$450,000) in optimist (1-h shutdown) and pessimist (1-month shutdown) terms, respectively.

After improvement, for 14.6% human error probability the expected cost of human failure varies from \$182.50 (14.6% × \$1250) to \$65,700 (14.6% × \$450,000). The reduction in cost varies from \$58.37 to \$21,015.

PSFs	Task 1	Task 2	Task 3	Task 4
Available time	1	1	1	1
Stress	1	1	1	1
Complexity	1	1	1	1
Experience/Training	1	1	1	1
Procedures	5	5	5	5
Ergonomics	1	1	1	1
Fitness for duty	1	1	1	1
Work process	1	1	1	1
Total	5	5	5	5

### 5.11.3 SPAR-H CASE STUDY APPLICATION

The SPAR-H method was conducted to define human failure probability and a similar group of specialists estimated the human probability values to human failures from tasks 1 to 4. The operator opinion was also considered to describe the PSF<sub>composite</sub>. In general, the SPAR-H method is used to assess a complete activity, but in this case Eq. (1) was applied to define the human error probability for each task.

$$HEP = \frac{NHEP \cdot PFS_{\text{composite}}}{NHEP \cdot (PFS_{\text{composite}} - 1) + 1}$$

Table 5.21 shows PSF<sub>composite</sub> values for each task. It is possible to observe that PSFs had the same values because the tasks are very similar and are affected by PSFs the same way.

The PSFs were considered adequate, nominal stress level, nominal complexity, poor procedure, nominal ergonomics, nominal fitness for duty, and nominal work process. Nominal means that PSFs are under good conditions and have low influence on failure.

Table 5.22 shows the human error probabilities. HEP1 gives the specialist opinion about the task human error probability. The SPAR-H procedure suggests using 0.1 for human error probability with commission error and 0.001 for omission error. In this case, specialist opinion was considered and

	HEP2	HEP1
Open vapor valve—Task 1	0.357143	0.1
Open suction valve—Task 2	0.0005	0.0001
Close suction valve—Task 3	0.208333	0.05
Open vapor valve—Task 4	0.0005	0.0001
Total	0.566476	

PSFs	Task 1	Task 2	Task 3	Task 4
Available time	1	1	1	1
Stress	1	1	1	1
Complexity	1	1	1	1
Experience/Training	1	1	1	1
Procedures	1	1	1	1
Ergonomics	1	1	1	1
Fitness for duty	1	1	1	1
Work process	1	1	1	1
Total	1	1	1	1

human error probability was defined for each task, as given in the HEP1 column in Table 5.15. Further, in the HEP2 column the final human error probability regarding PSFs applying Eq. (1) is given. Thus the final human error probability is 56%.

To reduce the human error probability, improvements in the procedure were suggested to make the process clear. The new values for the PSFs are shown in Table 5.23.

After procedure improvements all PSFs are nominal not having high influence on the final human error probability, as shown in Table 5.24. Thus the final human error probability after procedure improvement is 15.02%. For 56% human error probability the expected cost of human failure varies from \$700 ( $56\% \times \$1250$ ) to \$252,000 ( $56\% \times \$450,000$ ) in optimist and pessimist terms, respectively.

Regarding 56% human error probability the expected cost of human failure varies from \$700 ( $56\% \times \$1250$ ) to \$252,000 ( $56\% \times \$450,000$ ) in optimist and pessimist terms, respectively.

After improvement, for 15% human error probability the expected cost of human failure varies from \$187 ( $15\% \times \$1250$ ) to \$67,500 ( $15\% \times \$450,000$ ). The reduction in cost varies from \$513 to \$184,500.

The group of specialists conducting the SPAR-H analysis commented that:

- SPAR-H is easy to implement.
- The omission and commission human error probabilities must be representative for the turbine case study and specialist opinion must be used to define them.

	HEP2	HEP1
Open vapor valve—Task 1	0.1	0.1
Open suction valve—Task 2	0.0001	0.0001
Close suction valve—Task 3	0.05	0.05
Open vapor valve—Task 4	0.0001	0.0001
Total	0.1502	

	<b>Generic Tasks</b>	<b>Nominal Human Unreliability</b>	
A	Totally unfamiliar, performed at speed with no real idea of likely consequences	0.55	(0.35–0.97)
B	Shift or restore system to a new or original state on a single attempt without supervision or procedures	0.26	(0.14–0.42)
C	Complex task requiring high level of comprehension and skill	0.16	(0.12–0.28)
D	Fairly simple task performed rapidly or given scant attention	0.09	(0.06–0.13)
E	Routine, highly practiced, rapid task involving relatively low level of skill	0.02	(0.07–0.045)
F	Restore or shift a system to original or new state following procedures with some checking	0.003	(0.0008–0.007)
G	Completely familiar, well-designed, highly practiced, routine task occurring several times per	0.0004	(0.00008–0.009)
H	Respond correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of the system	0.00002	(0.000006–0.009) 5th–95th percentile bound

- It is possible in some cases to consider other human PSFs not used in the SPAR-H procedure (Table 5.7), and in this case some human PSFs in the procedure could be replaced.

#### 5.11.4 HEART CASE STUDY APPLICATION

The HEART procedure was also applied to the turbine case. Thus the first step after understanding the case study context is to define the generic task associated with turbine startup. Thus, based on Table 5.25, generic task F, “restore or shift a system to original or new state following procedures with some checking,” is used, and based on specialist opinion, the nominal human unreliability is 0.007.

The next step is to define the error-producing condition associated with the turbine startup steps, and in this case two error-producing conditions (“14” and “15” from Table 5.26) were chosen as the error-producing condition, as shown in Table 5.27.

The next and final step is applying the HEP equation to calculate final HEP, as shown in Table 5.27, based on equality:

$$\text{Final HEP} = \text{GEP} \times \prod R(i) \times (W(i) - 1) + 1$$

	<b>Error-Producing Condition</b>	<b>Weight</b>
14	No clear, direct, and timely confirmation of an intended action from the portion of the system over which control is exerted	4
15	Operator inexperience (eg, a newly qualified tradesman but not an expert)	3

Tasks	Nominal Human Unreliability	Error-Producing Condition	Weight	Importance	Weight × Importance	Human Error Probability
Open vapor valve	0.007	Not clear	4	0.8	3.4	0.04284
		Inexperience	3	0.4	1.8	
Open suction valve	0.007	Not clear	4	0.8	3.4	0.04284
		Inexperience	3	0.4	1.8	
Close vapor valve	0.007	Not clear	4	0.8	3.4	0.04284
		Inexperience	3	0.4	1.8	
Close suction valve	0.007	Not clear	4	0.8	3.4	0.04284
		Inexperience	3	0.4	1.8	
Turbine startup HEP						17%

Thus we have human error probabilities as shown in [Table 5.27](#).

The human error probability for turbine startup is 17%. The mean improvement solution is to improve the procedure. After such improvements the human error probabilities in startup are reduced from 17% to 5%. The new human error probability is shown in [Table 5.28](#). And in this case, because of procedure improvement, only error-producing condition is considered in the final human error probability calculation.

As stated, calculating the human error probability by the HEART methodology is relatively simple and requires only identifying the generic task and error-producing condition values in the tables. Such values are confirmed by specialists and a weight is stated for each as an “error-producing condition.”

Tasks	Nominal Human Unreliability	Error-Producing Condition	Weight	Importance	Weight × Importance	Human Error Probability
Open vapor valve	0.007	Inexperience	3	0.4	1.8	0.0126
Open suction valve	0.007	Inexperience	3	0.4	1.8	0.0126
Close vapor valve	0.007	Inexperience	3	0.4	1.8	0.0126
Close suction valve	0.007	Inexperience	3	0.4	1.8	0.0126
Turbine startup HEP						5%

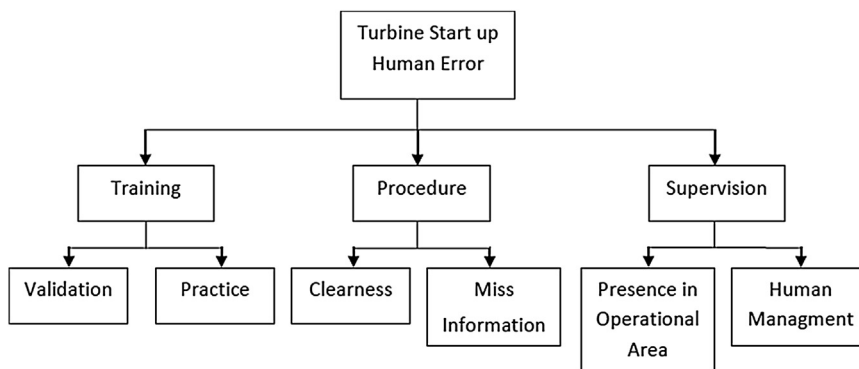
The expected cost of human error when turbine startup is not performed correctly varies from \$252 ( $17\% \times \$1250$ ) to \$76,500 ( $17\% \times \$450,000$ ) in optimist and pessimist terms, respectively. After improvement, for 5% human error probability the expected cost of human failure varies from \$62 ( $5\% \times \$1250$ ) to \$22,500 ( $5\% \times \$450,000$ ). The reduction in cost varies from \$190 to \$54,000.

### 5.11.5 STAHR CASE STUDY APPLICATION

The same group of specialists assessed the human error in turbine startup based on the STAHR methodology and defined that training, procedures, and supervision were the main human factors influencing human error. In addition to training, the root causes of bad performance in training were inadequate training, validation to check operator knowledge, and not enough operational practice. For the procedure the root causes were unclear procedures and missing information. Finally, regarding supervision the root causes that influence such performance factors are presence in operational ground and human management. Thus, based on specialist information, the human reliability tree is as shown in Fig. 5.21.

The following steps define the weight of each PSF and its influence on human error. Thus the main questions are:

- What is the validation influence on training effectiveness if training is “adequate” or “inadequate”?
- What is the practice influence on training effectiveness if it is “done” or “not done”?
- What is the unclear information influence on procedure effectiveness if it is “too much” or “too little”?
- What is the missing information influence on procedure effectiveness if it is “high importance” or “low importance”?
- What is the presence on operational area influence on supervision effectiveness if it is “too much” or “too little”?
- What is the human management influence on supervision effectiveness if it is “good” or “bad”?



**FIGURE 5.21**

Human reliability tree (STAHR).



**Table 5.29 Training Weights (STAHR)**

Training							
If	and	So	Probability of Training Having Quality:		Final Weights (Validation and Practice)		
			Good	Bad	Validation	Practice	Result
Validation	Practice						
Indequate	Done		0.7	0.3	0.8	0.2	0.16
Indequate	Not done		0.1	0.9	0.8	0.8	0.64
Adequate	Done		0.9	0.1	0.2	0.2	0.04
Adequate	Not done		0.7	0.3	0.2	0.8	0.16
	Total		0.324	0.676			

In addition to such questions it is necessary to define weights for PSFs (training, procedure, and supervision) for the previous questions. Thus for training, based on specialist opinion, Table 5.29 summarizes the procedure weights and probabilities when training quality is good or bad.

The values in Table 5.29 show the probability of training having a good quality (32.4%) or bad quality (67.6%) in the current case, reflected by the weights stated in specialist opinion concerning validation (inadequate = 0.8 or adequate = 0.2) and practice (done = 0.2 or not done = 0.8). The next step is to define the procedure weights, as shown in Table 5.30.

The values in Table 5.30 show the probability of the procedure having a good quality (53.6%) or bad quality (46.4%) based on the current case, reflected by the weights stated by specialists concerning unclear (too much = 0.9 or too little = 0.1) and missing information (high importance = 0.8 or low importance = 0.2). The next step is to define the supervision weights, as shown in Table 5.31.

The values in Table 5.31 show the probability of supervision having a good quality (35.58%) or bad quality (64.43%) based on the current case, reflected by the weights stated in specialist opinion concerning the presence in the operational area (too much = 0.05 or too little = 0.95) and human management (good = 0.3 or bad = 0.7). Finally, the next and last step is to define the turbine startup human error probability using the values stated in Tables 5.29–5.31 and specialist opinion concerning PSF combinations, as shown in Table 5.32.

**Table 5.30 Procedure Weights (STAHR)**

Procedure							
If	and	So	Probability of Procedure Quality to Be:		Weights (Unclear and Misinformation)		
			Good	Bad	Unclear	Misinformation	Results
Unclear	Misinformation						
Too much	High importance		0.5	0.5	0.9	0.8	0.72
Too much	Low importance		0.8	0.2	0.9	0.2	0.18
Little	High importance		0.3	0.7	0.1	0.8	0.08
Little	Low importance		0.4	0.6	0.1	0.2	0.02
	Total		0.536	0.464			

Supervision							
If	And	So	Probability of Supervision Having Quality:		Weights (Presence in Operational Area and Human Management)		
			Good	Bad	Presence in Operational Area	Human Management	Results
Too much	Good		0.95	0.05	0.05	0.3	0.015
Too much	Bad		0.8	0.2	0.05	0.7	0.035
Too little	Good		0.4	0.6	0.95	0.3	0.285
Too little	Bad		0.3	0.7	0.95	0.7	0.665
	Total		0.3558	0.6443			

Using the human performance (training, procedure, and supervision) probability values from Tables 5.29–5.31 as weights in Table 5.32 in columns 7, 8, and 9, and specialist opinion concerning combinations of PSF conditions from columns 1, 2, and 3 in columns 5 and 6, the final turbine startup human error probability is 62.43%, calculated by:

$$\text{HEP} = (0.01 \times 0.062) + (0.3 \times 0.112) + \dots + (0.8 \times 0.112) = 0.624$$

To reduce such an error, improved procedures and training are recommended. Thus the new performance's weight values are:

- Training (bad: 63.8%; weights: validation inadequate: 0.7; practice not done: 0.8);
- Procedure (bad: 21.2%; weights: unclear/too much: 0.2; missing information/high importance: 0.2);
- Supervision (bad: 32.3%; weights: presence in operational area/too little: 0.9; human management/bad: 0.7).

The weights and probabilities are complementary so to calculate the other values of probabilities and weights in only precede one less value shown above ( $1 - x$ ). Thus the turbine startup human error probability after improvements is 20.3%. Table 5.33 shows the final human error calculation.

The STahr methodology has the following advantages:

- The possibility of defining performance human factors in analysis and considering their relation to and influence on human error;
- Easy to apply and perform for specialists.

The disadvantage is:

- Total dependence on specialist opinion, and if such specialists are not familiar with the situation being assessed, the human error probability may not be accurate.

The expected cost of human error when the turbine is not started correctly varies from \$780 ( $62.4\% \times \$1250$ ) to \$280,800 ( $62.4\% \times \$450,000$ ) in optimist and pessimist terms, respectively. After improvement, for 20% human error probability the expected cost of human failure varies from \$250 ( $20\% \times \$1250$ ) to \$90,000 ( $20\% \times \$450,000$ ). The reduction in cost varies from \$530 to \$190,800.

**Table 5.32 Turbine Startup Human Error Probabilities (STHR)**

Turbine Start Up Human Error									
If	and	and	So	Probability of Turbine Startup:		Weights (Training, Procedure, and Supervision)			
				Right	Wrong	Training	Procedure	Supervision	Result
Good	Good	Good		0.99	0.01	0.324	0.536	0.356	0.062
Good	Good	Bad		0.7	0.3	0.324	0.536	0.644	0.112
Good	Bad	Bad		0.6	0.4	0.324	0.464	0.644	0.097
Good	Bad	Good		0.6	0.4	0.324	0.464	0.356	0.053
Bad	Good	Good		0.4	0.6	0.676	0.536	0.356	0.129
Bad	Good	Bad		0.3	0.7	0.676	0.536	0.644	0.233
Bad	Bad	Bad		0.01	0.99	0.676	0.464	0.644	0.202
Bad	Bad	Good		0.2	0.8	0.676	0.464	0.356	0.112
Total				0.3756	0.62439				

**Table 5.33 Turbine Startup Human Error Probabilities (STahr—After Improvements)**

Turbine start up human error									
If	and	and	So	Probability of Turbine Startup:		Weights (Training, Procedure, and Supervision)			
				Right	Wrong	Training	Procedure	Supervision	Result
Good	Good	Good		1	0	0.362	0.788	0.677	0.193
Good	Good	Bad		0.9	0.1	0.362	0.788	0.323	0.092
Good	Bad	Bad		0.9	0.1	0.362	0.212	0.323	0.025
Good	Bad	Good		1	0	0.362	0.212	0.677	0.052
Bad	Good	Good		0.8	0.2	0.638	0.788	0.677	0.340
Bad	Bad	Good		0.6	0.4	0.638	0.788	0.323	0.162
Bad	Bad	Bad		0.3	0.7	0.638	0.212	0.323	0.044
Bad	Good	Bad		0.7	0.3	0.638	0.212	0.677	0.092
		Total		0.797	0.203				

SPAHR methodology has these advantages:

- The possibility of defining performance human factors on analysis and considering their relation and influence on human error;
- Easy to apply and perform for specialists.

The disadvantage is:

- Total dependence on specialists’ opinion and if such specialists are not familiar with situation assessed the human error probability may not be representative.

The human error expected cost when the turbine is not started up correctly varies from \$780 (62.4% × \$1250) to \$280,800 (62.4% × \$450,000) in optimist and pessimist terms, respectively.

After improvement, regarding 20% human error probability the expected cost of human failure varies from \$250 (20% × \$1250) to \$90,000 (20% × \$450,000). The reduction in cost varies from \$530 to \$190,800.

### 5.11.6 SLIM-MAUD CASE STUDY APPLICATION

The other method applied to the turbine case is SLIM as described in Section 5.8. Thus, based on method description, the first step is to define PSFs regarding specialist opinion and in this case procedure, training, and supervision were defined. The next step is to give scores importance in terms of leverage of compliance to each PSF for each task. The scores vary from 1 to 9, and 9 means the highest compliance. Table 5.34 shows PSF scores based on specialist opinion. In this case the score is the same for all tasks because their similarity.

The next step is necessary to define the importance value for each PSF varying from 0% to 100%. Total importance values of all scores must be 100%. Thus Table 5.35 shows importance values for each PSF.

The next step is to define the SLI by multiplying scores per each PSF value, as shown in Table 5.36.

The next step is necessary to define the HEP for each task and thereafter for total startup activity. Thus it is necessary to define variables values for the following equation:

$$\log P = aSLI + b$$

To define the “a” and “b” parameters it is necessary to have the P(HEP) value, which can be considered by specialist opinion. Therefore, regarding the HEP value of 0.1 (10%) and 0.0001 (0.01%) for task one and two respectively, it’s possible to calculate the parameter a and b. Finally, HEP final equation will be:

$$HEP = 10^{(-0.24 \times SLI + 0.18)}$$

<b>Score Table</b>			
<b>PF Rate</b>	<b>Procedure</b>	<b>Training</b>	<b>Supervision</b>
Open vapor valve—Task 1	6	8	9
Open suction valve—Task 2	6	8	9
Close suction valve—Task 3	6	8	9
Open vapor valve—Task 4	6	8	9

**Table 5.35 Importance Values (Before Improvement)**

PSF Importance	
Procedure	50%
Training	30%
Supervision	20%
Total	100%

**Table 5.36 SLI Values (Before Improvement)**

Tasks	Procedure	Training	Supervision	SLI
Open vapor valve—Task 1	3	2.4	1.8	7.2
Open suction valve—Task 2	3	2.4	1.8	7.2
Close suction valve—Task 3	3	2.4	1.8	7.2
Open vapor valve—Task 4	3	2.4	1.8	7.2

The final step is to apply an SLI value for each task in the preceding equation. Table 5.37 shows the final human error probability.

Based on specialist opinion, the procedure is the PSF which take more influence in human error probability. Is doing so, after procedure improvement, is expected to reduce the HEP to 10%. The new expected procedure score value is 9, as shown in Table 5.38.

The next step is to update the importance values and in this case procedure importance will reduce because the lower influence in the turbine starts up after improvement, as shown in Table 5.39.

The new SLI values are shown in Table 5.40 regarding new scores and importance values.

The final step is to define the new HEP for each task and thereafter the total startup activity regarding procedure improvement. Thus it is necessary to define variables values for the following equation:

$$\log P = aSLI + b$$

**Table 5.37 SLI Values (Before Improvement)**

Tasks	aSLI + b	$10^{(-0.24 \times SLI + 0.18)}$
	$(-0.024 \times SLI) + 0.18$	
Open vapor valve—Task 1	-1	0.10
Open suction valve—Task 2	-1	0.10
Close suction valve—Task 3	-1	0.10
Open vapor valve—Task 4	-1	0.10
Total		40%

PF Rate	Procedure	Training	Supervision
Open vapor valve—Task 1	9	8	9
Open suction valve—Task 2	9	8	9
Close suction valve—Task 3	9	8	9
Open vapor valve—Task 4	9	8	9

PSF Importance	
Procedure	0.1
Training	0.5
Supervision	0.4
Total	1

Tasks	Procedure	Training	Supervision	SLI
Open vapor valve—Task 1	0.9	4	3.6	8.5
Open suction valve—Task 2	0.9	4	3.6	8.5
Close suction valve—Task 3	0.9	4	3.6	8.5
Open vapor valve—Task 4	0.9	4	3.6	8.5

In order to define the new “a” and “b” parameters it is necessary to have the (HEP) value for at least two specific tasks. Based on specialist opinion, the HEP value of 0.1 (10%) and 0.0001 (0.01%) are applied for task one and two respectively. Thereby, it’s possible to calculate the parameter a and b. The final HEP equation is:

$$\text{HEP} = 10^{(3 \times \text{SLI} - 27.18)}$$

The final step is to applying new SLI values for each task in the preceding equation. [Table 5.41](#) shows the final human error probability.

Regarding 40% human error probability the expected cost of human failure varies from \$500 to \$180,000 in optimist and pessimist terms, respectively.

After improvement, regarding 10% human error probability the expected cost of human failure varies from \$125 to \$45,000. The reduction in cost varies from \$375 to \$135,000.

The group of specialists that carried out the SLIM analysis commented that:

- SLIM is not easy to implement because, beyond specialist opinion, it requires arithmetic treatment;
- Specialist opinion highly influences the HEP value.

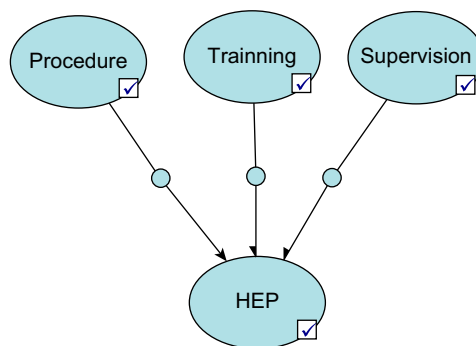
Tasks	aSLI + b	HEP = $10^{(3 \times \text{SLI} - 27.18)}$
	$(3 \times \text{SLI}) - 27.1$	
Open vapor valve—Task 1	-2	0.03
Open suction valve—Task 2	-2	0.03
Close suction valve—Task 3	-2	0.03
Open vapor valve—Task 4	-2	0.03
Total		10%

### 5.11.7 BAYESIAN NETWORK APPLICATION

The final method is the Bayesian network method, and the advantage of this method is being able to consider PSFs related to the human error probability. Therefore for the PSFs procedure, supervision, and training, the Bayesian network is as shown in Fig. 5.22.

To calculate the HEP it is necessary to get a specialist opinion to define the probability values as shown in the following list of questions:

- What is the probability of failure in turbine startup if the procedure is not good? (Optimist = 10% and pessimist = 60%)
- What is the probability of failure in turbine startup if supervision is not good? (Optimist = 20% and pessimist = 40%)
- What is the probability of failure in turbine startup if training is not good? (Optimist = 40% and pessimist = 20%)
- What is the probability of failure in turbine startup if training, procedure, and supervision are not good? (Optimist = 90% and pessimist = 40%)



**FIGURE 5.22**

Startup turbine Bayesian network.



- What is the probability of failure in turbine startup if procedure and supervision are not good and training is good? (Optimist = 80% and pessimist = 90%)
- What is the probability of failure in turbine startup if procedure and training are not good and supervision is good? (Optimist = 70% and pessimist = 70%)
- What is the probability of failure in turbine startup if the procedure is not good and supervision and training are good? (Optimist = 60% and pessimist = 60%)
- What is the probability of failure in turbine startup if supervision and training are not good and procedure is good? (Optimist = 20% and pessimist = 20%)
- What is the probability of failure in turbine startup if supervision is not good and procedure and training are good? (Optimist = 10% and pessimist = 10%)
- What is the probability of failure in turbine startup if training is not good and procedure and supervision are good? (Optimist = 5% and pessimist = 5%)
- What is the probability of failure in turbine startup if supervision, procedure, and training are good? (Optimist = 5% and Pessimist = 0.1%)

These questions come from the conditional probability equation and such values are put into the Bayesian equation. Applying such values, and performing simulation, the human error probability is 43.69%, as shown in Fig. 5.23. To calculate the human error probability values it is necessary to substitute probability values (pessimist) in the following equation, so we have:

HEP = P(C = 1). In general, P(ST = 1). Thus:

$$HEP = \sum_{i=0}^1 \sum_{j=0}^1 \sum_{k=0}^1 P(T_1 = i) \times P(P_2 = j) \times P(S_3 = k) \times P(ST = 1 | T_1 = i, P_2 = j, S_3 = k)$$

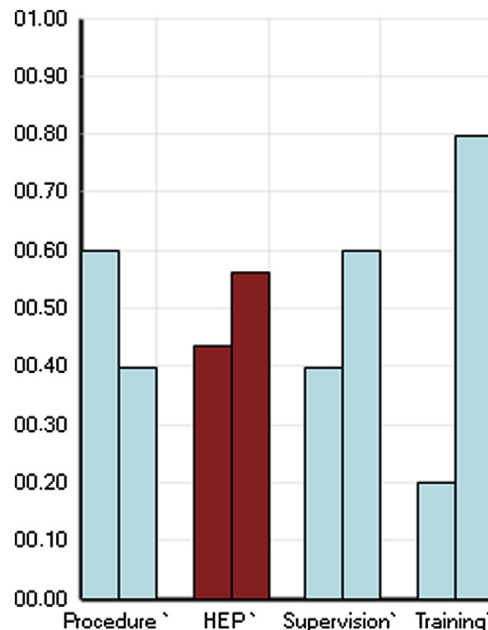


FIGURE 5.23

Bayesian network results (before improvement).

where  $\overline{ST}$  = human error in startup turbine = ( $ST = 1$ );  $T$  = good training ( $T_i = 0$ );  $\overline{T}$  = bad training ( $T_i = 1$ );  $P$  = good procedure ( $P_i = 0$ );  $\overline{P}$  = bad procedure ( $P_i = 1$ );  $S$  = good supervision ( $S_i = 0$ ); and  $\overline{S}$  = bad supervision ( $S_i = 1$ ).

Thus:

$$\begin{aligned} \text{HEP} &= P(\overline{ST}|\overline{T}, \overline{P}, \overline{S}) \times P(\overline{T}) \times P(\overline{P}) \times P(\overline{S}) + P(\overline{ST}|T, \overline{P}, \overline{S}) \times P(T) \times P(\overline{P}) \times P(\overline{S}) \\ &+ P(\overline{ST}|\overline{T}, \overline{P}, S) \times P(\overline{T}) \times P(\overline{P}) \times P(S) + P(\overline{ST}|T, \overline{P}, S) \times P(T) \times P(\overline{P}) \times P(S) \\ &+ P(\overline{ST}|\overline{T}, P, \overline{S}) \times P(\overline{T}) \times P(P) \times P(\overline{S}) + P(\overline{ST}|T, P, \overline{S}) \times P(T) \times P(P) \times P(\overline{S}) \\ &+ P(\overline{ST}|\overline{T}, P, S) \times P(\overline{T}) \times P(P) \times P(S) + P(\overline{ST}|T, P, S) \times P(T) \times P(P) \times P(S) \end{aligned}$$

To calculate HEP values it is necessary to substitute the probability values (pessimist) in the following equation, so we have:

$$\begin{aligned} \text{HEP} &= P(\overline{ST}|\overline{T}, \overline{P}, \overline{S}) \times P(\overline{T}) \times P(\overline{P}) \times P(\overline{S}) + P(\overline{ST}|T, \overline{P}, \overline{S}) \times P(T) \times P(\overline{P}) \times P(\overline{S}) \\ &+ P(\overline{ST}|\overline{T}, \overline{P}, S) \times P(\overline{T}) \times P(\overline{P}) \times P(S) + P(\overline{ST}|T, \overline{P}, S) \times P(T) \times P(\overline{P}) \times P(S) \\ &+ P(\overline{ST}|\overline{T}, P, \overline{S}) \times P(\overline{T}) \times P(P) \times P(\overline{S}) + P(\overline{ST}|T, P, \overline{S}) \times P(T) \times P(P) \times P(\overline{S}) \\ &+ P(\overline{ST}|\overline{T}, P, S) \times P(\overline{T}) \times P(P) \times P(S) + P(\overline{ST}|T, P, S) \times P(T) \times P(P) \times P(S) \\ \text{HEP} &= [0.4 \times 0.2 \times 0.6 \times 0.4] + [0.9 \times 0.8 \times 0.6 \times 0.4] + [0.7 \times 0.2 \times 0.6 \times 0.6] \\ &+ [0.6 \times 0.8 \times 0.6 \times 0.6] + [0.2 \times 0.2 \times 0.4 \times 0.4] + [0.1 \times 0.8 \times 0.4 \times 0.4] \\ &+ [0.05 \times 0.8 \times 0.4 \times 0.6] + [0.001 \times 0.8 \times 0.4 \times 0.6] = 43.69\% \end{aligned}$$

After implementing procedure improvement the specialists believe that failure in turbine startup will be reduced from 43.69% to 12.92%, as shown in Fig. 5.24. Substituting optimistic probability values in the following equation we have the human error probability after procedure improvements:

$$\begin{aligned} \text{HEP} &= P(\overline{ST}|\overline{T}, \overline{P}, \overline{S}) \times P(\overline{T}) \times P(\overline{P}) \times P(\overline{S}) + P(\overline{ST}|T, \overline{P}, \overline{S}) \times P(T) \times P(\overline{P}) \times P(\overline{S}) \\ &+ P(\overline{ST}|\overline{T}, \overline{P}, S) \times P(\overline{T}) \times P(\overline{P}) \times P(S) + P(\overline{ST}|T, \overline{P}, S) \times P(T) \times P(\overline{P}) \times P(S) \\ &+ P(\overline{ST}|\overline{T}, P, \overline{S}) \times P(\overline{T}) \times P(P) \times P(\overline{S}) + P(\overline{ST}|T, P, \overline{S}) \times P(T) \times P(P) \times P(\overline{S}) \\ &+ P(\overline{ST}|\overline{T}, P, S) \times P(\overline{T}) \times P(P) \times P(S) + P(\overline{ST}|T, P, S) \times P(T) \times P(P) \times P(S) \\ \text{HEP} &= [0.9 \times 0.1 \times 0.2 \times 0.4] + [0.8 \times 0.6 \times 0.1 \times 0.2] + [0.7 \times 0.4 \times 0.2 \times 0.8] \\ &+ [0.6 \times 0.6 \times 0.1 \times 0.8] + [0.2 \times 0.4 \times 0.9 \times 0.2] + [0.1 \times 0.6 \times 0.9 \times 0.2] \\ &+ [0.05 \times 0.4 \times 0.9 \times 0.8] + [0.05 \times 0.6 \times 0.9 \times 0.8] = 12.92\% \end{aligned}$$

For the 44% human error probability, the expected cost of human failure varies from \$575 to \$207,000 in optimist and pessimist terms, respectively. After improvement, for 13% human error probability the expected cost of human failure varies from \$162.50 to \$58,500. The reduction in cost varies from \$412.50 to \$148,500.

The group of specialists conducting the network Bayesian analysis commented that:

- The Bayesian network is not easy to implement because of mathematical treatments and questionnaire.
- Specialist opinions highly influence the human error probability value.
- Software must be available to make calculations easier.

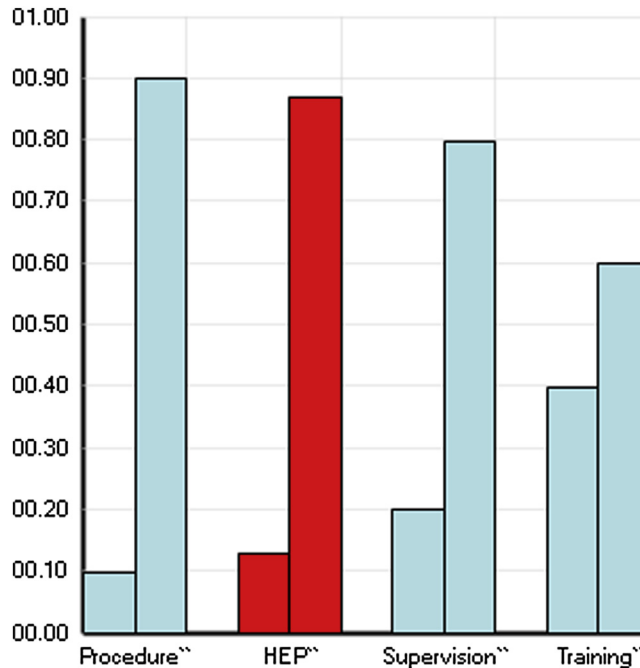
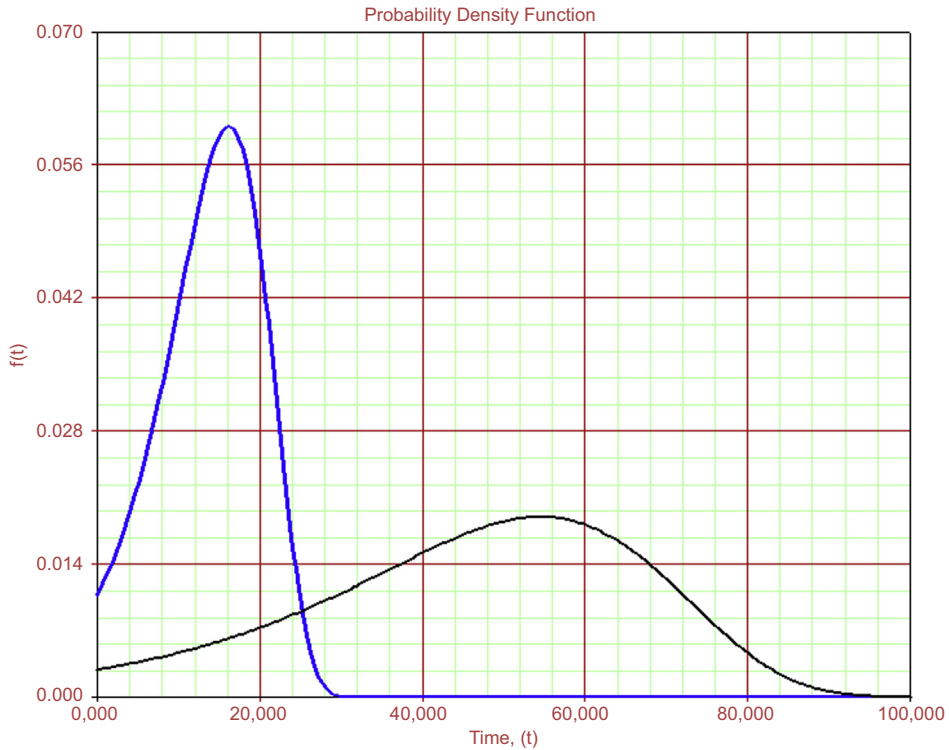


FIGURE 5.24

Bayesian network results (after improvement).

### 5.11.8 METHODOLOGIES COMPARISON

Despite different methodologies, human error probability in turbine startup has similar behavior. In all cases, after improvements in procedures, human error probability reduced. Also, as expected, human reliability analysis that uses human factors (STahr, HEART, SPAR-H, and Bayesian network) normalized correctly to being well represented by the Gumbel distribution value for human error probability, as shown in Fig. 5.25. The black PDF (probability density function) (Gumbel:  $\mu = 54.61$ ;  $\sigma = 19.38$ ;  $\rho = 0.9736$ ) represents the human error probability before procedure improvement and the gray PDF represents the human error probability after procedure improvement (Gumbel:  $\mu = 16.18$ ;  $\sigma = 6.12$ ;  $\rho = 0.9885$ ). Even for the THERP and OAT human error probabilities PDF, the behavior is similar and is well represented by Gumbel distribution. Thus in terms of methodology consistency the results tend to be higher than found in the THERP and OAT methods. Such deviation found in PDFs is acceptable, for example, in risk analysis applications and even for reliability analysis. If human performance was compared individually based on human error probabilities such differences must be considered, but only if performed for different human reliability analyses to assess different teams.



**FIGURE 5.25**

Human error probability PDF.

### 5.11.9 CONCLUSION

After performing the different methods discussed in this chapter, some important points arise:

- Despite different methodologies, the final human error probability results are similar in the case study, with small differences in value, which shows that all methods are good enough to perform human reliability analysis considering PSFs.
- A specialist opinion is highly influential in all the methods presented. Regarding the Bayesian network, it is possible to obtain historical data, but in real life it is difficult to do because historical reports with conditional probabilities are very hard to obtain.
- Despite a high range of expected costs because of human failure in turbine startup, the expected cost of human failure is a good proposal for measuring economical values to support decisions in human reliability analysis and implementing recommendations.
- Despite similar results from the different methods, it is necessary to test such methodologies in other cases to find other disadvantages and advantages to have information enough to define the case for which each methodology is the most applicable. In the future there will be additional case studies to compare to and make decisions about the best method for each specific case.

## 5.12 HUMAN ERROR IMPACT ON PLATFORM OPERATIONAL AVAILABILITY

### 5.12.1 HUMAN ERROR ASSESSMENT DURING COMMISSIONING PHASE

Based on the SPAR-H method, the first step is to consider the type of error. In the platform case, the operational error during the first 5 years, which means commission error, has been considered. The objective is to assess the impact of such human error in platform operational availability.

To define the weight of each PSF a meeting was organized with specialists based on the consensus group method. Such specialist elicitation method considers each member's contribution to the discussion to get a unique value for each parameter estimated with the group agreement. Considering the first case, which means the first 5 years of operation, the specialist defined the scores highlighted in [Table 5.42](#).

The human error during the commissioning scenario is defined by applying the PFS based on specialist opinion. The  $PFS_{\text{composite}}$  for each case is:

#### Case 1—Early-life phase (5 years)

Based on such values, the  $PFS_{\text{composite}}$  is:

$$PFS_{\text{composite}} = PFS(\text{available time}) \times PFS(\text{stress}) \times PFS(\text{complexity}) \times PFS(\text{experience/training}) \\ \times PFS(\text{procedures}) \times PFS(\text{ergonomics}) \times PFS(\text{fitness for duty}) \times PFS(\text{work process})$$

$$PFS_{\text{composite}} = 1 \times 1 \times 2 \times 2 \times 5 \times 1 \times 1 \times 2 = 40.$$

The next step is to calculate the HEP. To calculate the human error probability it is necessary to define the nominal human error probability. Based on current SPAR-H procedures, the NHEP for commission error is 0.001. In fact, this value defined by the standard is very low and will not reflect the human error during platform early-life phase. To define the NHEP for early-life phase, [Table 5.43](#) will be applied based on HEART.

Based on [Table 5.43](#), task D represents the human error and the NHEP defined is 0.06. Therefore the final human error probability is:

#### Case 1—Early-life phase (5 years)

$$HEP = \frac{NHEP \cdot PSF_{\text{composite}}}{NHEP(PSF_{\text{composite}} - 1) + 1}$$

$$HEP = \frac{0.06 \times 40}{0.06 \times (40 - 1) + 1} = 0.7185$$

### 5.12.2 HUMAN ERROR EFFECT ON PLATFORM SYSTEM OPERATIONAL AVAILABILITY

To consider the effect of human error probability in the system, it is necessary to incorporate such HEP in a system reliability block diagram (RBD) defined in RAM analysis. Therefore it is necessary to translate the human error probability into a PDF. Assuming that the human error occurs randomly

**Table 5.42 PSF Values**

PSFs	PSF Level	Multiplier for Action
Available time	Inadequate time	$P(f) = 1$
	Time available $\approx$ time required	10
	Nominal time	1
	Time available $\geq 5 \times$ time required	0.1
	Time available $\geq 50 \times$ time required	0.01
	Insufficient information	1
Stress	Extreme	5
	High	2
	Nominal	1
Complexity	Insufficient information	1
	Highly complex	5
	Moderately complex	2
	Nominal	1
Experience/ Training	Insufficient information	1
	Low	3
	Nominal	1
	High	0.5
Procedures	Insufficient information	1
	Not available	50
	Incomplete	20
	Available but poor	5
	Nominal	1
Ergonomics	Insufficient information	1
	Missing/Misleading	50
	Poor	10
	Nominal	1
	Good	0.5
Fitness for duty	Insufficient information	1
	Unfit	$P(f) = 1$
	Degraded fitness	5
	Nominal	1
Work process	Insufficient information	1
	Poor	5
	Nominal	1
	Good	0.5
	Insufficient information	1

Source: NUREG, CR-6883.

	<b>Generic Tasks</b>	<b>Nominal Human Unreliability</b>	
A	Totally unfamiliar, performed at speed with no real idea of likely consequences	0.55	(0.35–0.97)
B	Shift or restore system to a new or original state on a single attempt without supervision or procedures	0.26	(0.14–0.42)
C	Complex task requiring high level of comprehension and skill	0.16	(0.12–0.28)
D	Fairly simple task performed rapidly or given scant attention	0.09	(0.06–0.13)
E	Routine, highly practiced, rapid task involving relatively low level of skill	0.02	(0.07–0.045)
F	Restore or shift a system to original or new state following procedures with some checking	0.003	(0.0008–0.007)
G	Completely familiar, well-designed, highly practiced, routine task occurring several times per day, performed to highest possible standards by highly motivated, highly trained and experienced personnel, with time to correct potential error, but without the benefit of significant job aid	0.0004	(0.00008–0.009)
H	Respond correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of system state	0.00002	(0.000006–0.009) 5th–95th percentile bound

*Source: HEART procedure.*

during a specific period of time, the PDF that fits better in such phenomenon is the exponential. The following equation shows the failure rate prediction based on the probability of having a human error during commission phase. The exponential cumulative density function is represented by the equation:

$$F(T) = 1 - e^{-t}$$

Therefore assuming the values of human error probabilities defined in item 1, the failure rate will be:

**Case 1—Early-life phase (5 years)**

$$F(T) = 1 - e^{-t}$$

$$0.7185 = 1 - e^{-5}$$

$$0.7185 - 1 = -e^{-5}$$

$$0.2815 = -e^{-5}$$

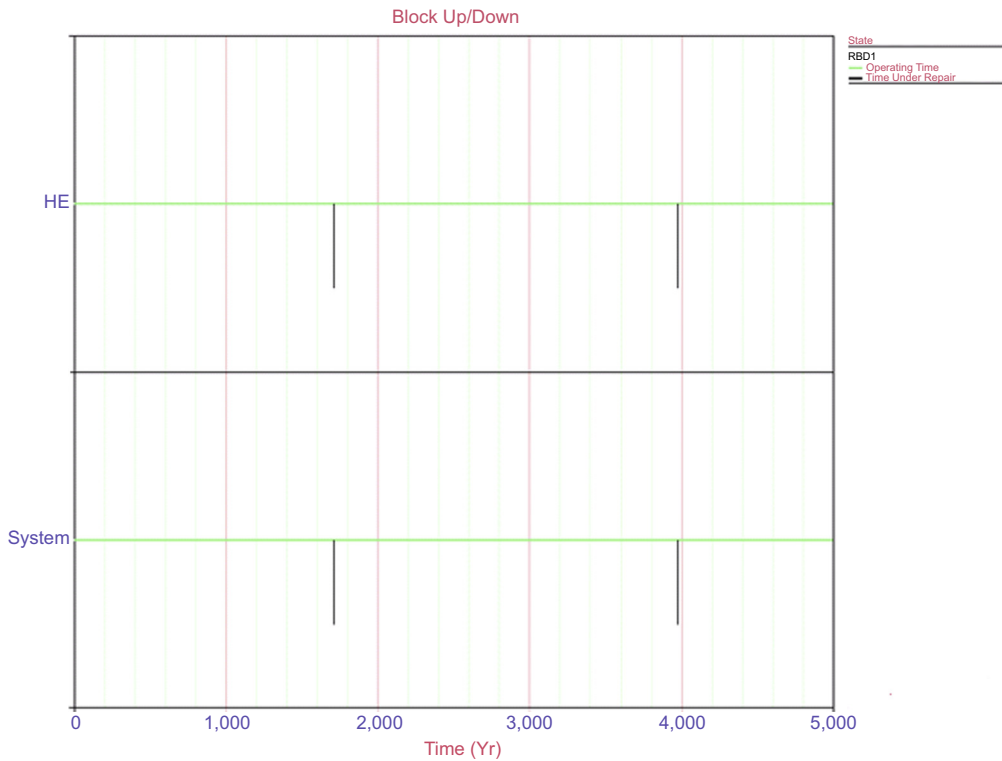
$$\ln(0.2815) = \ln(-e^{-5})$$

$$1.2676 = 5\lambda$$

$$= 0.2535$$

$$= \frac{1}{\text{MTTF}}$$

$$\text{MTTF} = 3.944$$



**FIGURE 5.26**

Human error block diagram simulation.

The final step is to input such failure rates to an RBD and incorporate such a block in series with a system RBD defined in RAM analysis. In addition, it is also necessary to define the repair time related to restore the system when a human error during operation occurs.

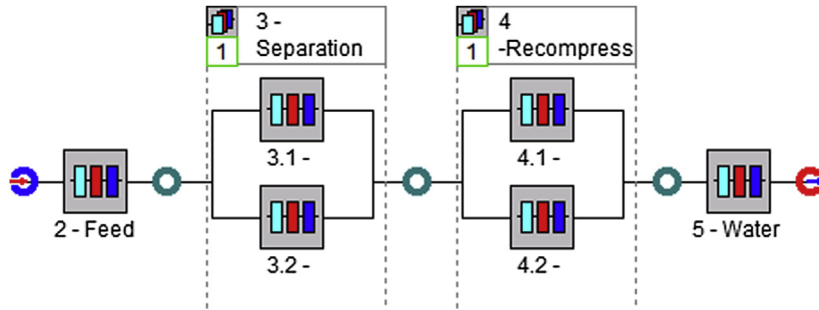
Fig. 5.26 represents the human error effect on the system. In case 1, two human errors happened during early-life failure. In each human reliability block will be input the PDF human error (MTTF = 3.5 years) and the PDF recovery time (5 days).

The final step is to include the human error in the RBD to predict the effect on human error probability. Fig. 5.27 shows the platform system RBD, which achieves 99.92% operational availability in 5 years.

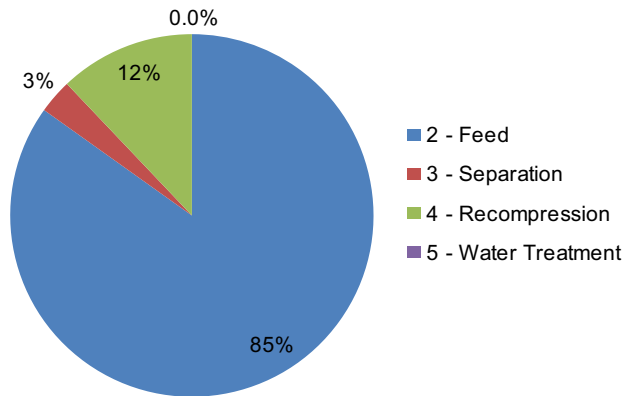
Despite the higher operational availability, the critical subsystem is the feed, caused by 85% of downtime in the platform, as shows in Fig. 5.28.

To take into account the effect of human error on platform operational availability, the diagram block named “Human error” is put in series with the previous diagram block concerning human error for each subsystem (feed, separation, compression, and water treatment). Therefore Monte Carlo simulation will take into account the effect of the block human error, which represents human error that shut down the subsystem over 5 years. Fig. 5.29 shows the platform system diagram block including the human error for each system. The impact of human error causes a reduction in operational availability to 98.47%.

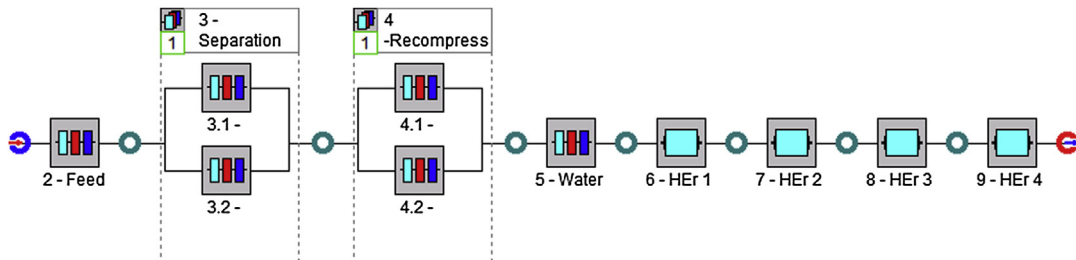




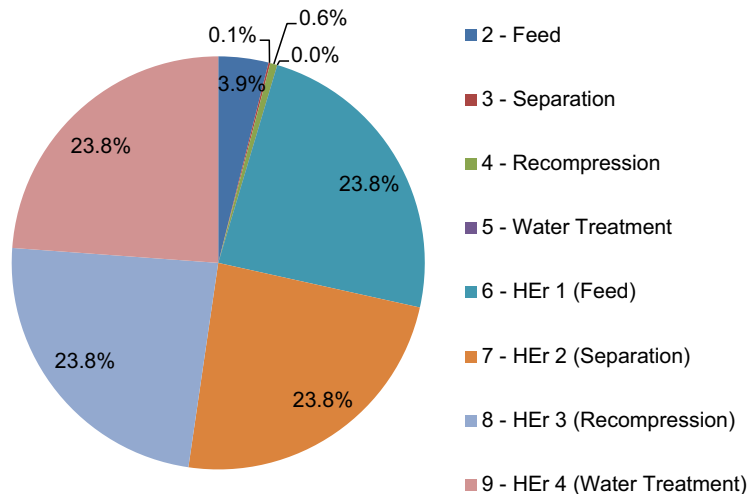
**FIGURE 5.27**  
Platform system diagram block.



**FIGURE 5.28**  
Relative downtime loss.



**FIGURE 5.29**  
Platform system diagram block with human error.

**FIGURE 5.30**

Relative downtime loss.

After including the human error in RAM analysis, the most critical event is human error, which represents 95.2% of total downtime, as shown in Fig. 5.30.

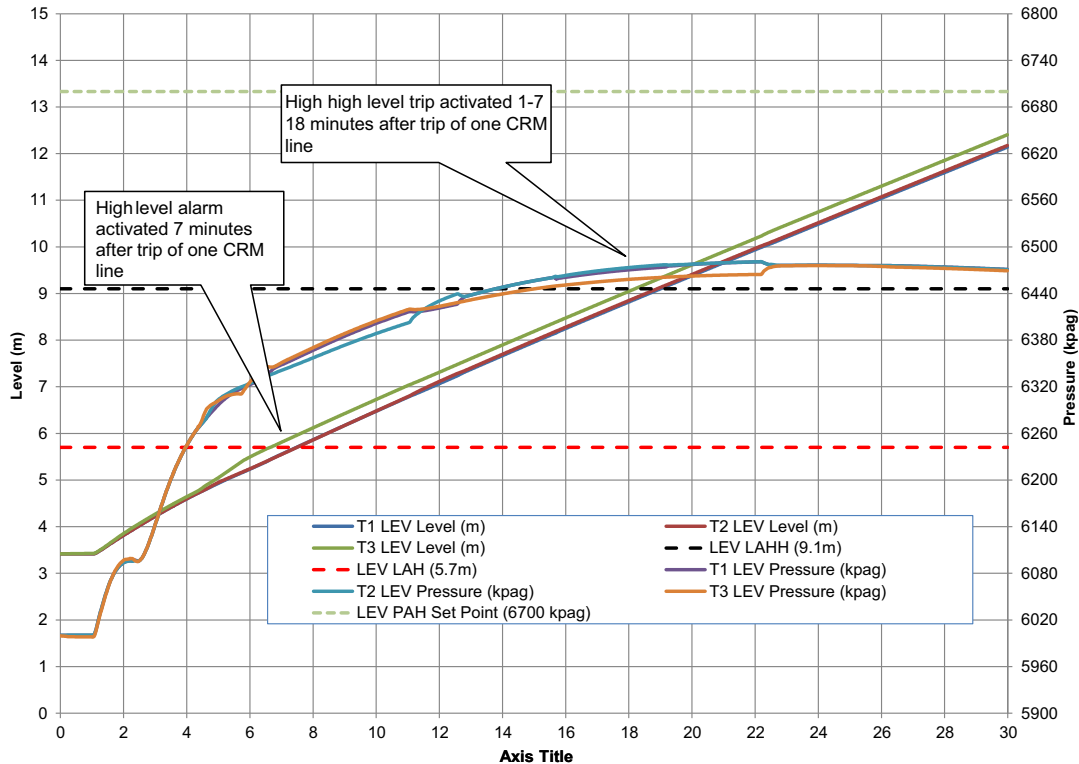
### 5.12.3 CONCLUSION

Human error during the different asset life cycles, such as design, transportation, commissioning and operation, may affect asset performance and must be avoided. Unfortunately, in many projects human error is not taken into account during RAM analysis based on the assumption of no human error. In fact, human error can be identified in the early asset life cycle design during FMEA as a cause of failure mode. In addition, human error happens also during maintenance activities, which increase the downtime and has an impact on asset performance. Therefore it is good practice to identify human error in different asset life cycle phases, which will affect asset performance during the operational phase. In case of a new asset concept, new equipment, and technology, it is necessary to consider the impact of human error in the asset performance by carrying out human reliability analysis and inputting such information in the RAM analysis to find out the quantitative effect on production efficiency and operational availability and propose mitigate action to avoid them.

## 5.13 ESDV (EMERGENCY SHUTDOWN VALVE): OPERATIONAL HUMAN ERROR ANALYSIS

### 5.13.1 ESDV SHUTDOWN CASE STUDY

The purpose of this case study is to demonstrate hybrid risk analysis, including human reliability analysis, bow tie, and fault tree analysis. Therefore the case study focuses on shutdown caused by the spurious closure of an ESDV on a transfer line leading to zero flow through that line. The purpose of the



**FIGURE 5.31**

CRM transfer line flow and pressure. CRM, condensate rich MEG; MEG, ethylene glycol.

case study is to determine whether there is smooth operation following the trip of a single production line (CRM) and identify any consequential process trips. Fig. 5.31 shows that when the ESDV closes, the mass flow through the east transfer line drops to zero. The total mass export rate also falls, before recovering to a flow rate of around 530,000 kg/h, which is lower than the initial total export flow of around 690,000 kg/h.

Fig. 5.31 is the result of a dynamic simulation result, which considers the following sequence of events.

At:

$T = 0$  min, initial conditions as above.

$T = 1$  min, ESDV at transfer line inlet closes with a closure time of 12 s.

$T = 17$  min, liquid level in the three Liquid Export Vessels (LEVs) will reach the Level Trip High High (LZHH) trip set point with a single flowline operating. The trip actions were not simulated as part of this run.

$T = 30$  min, simulation ends.

### 5.13.2 SPAR-H

Human reliability analysis qualifies human intervention in terms of the probability of the operator making an error and consequently leading to a total plant shutdown. This paragraph effectively calculates the frequency of total shutdown incurred as a result of this scenario when relying on a specific operator action.

The error is effectively the operator either:

- Missing completely the first-out alarm that came up, that is, the high pressure at the inlet of the CRM line, that is, an omission error; or
- Recognizing the alarm, but not performing the correct action as per the procedure, that is, a commission error.

Note that for the former omission error it takes a single operator, that is, the control room operator, to miss the alarm.

In addition, the later commission error involves both the control room and the field operator. The scenario is as follows:

1. It is expected that by time  $t = 14$  min (10 min from the first alarm) the operator should be able to understand the issue and the root cause. At that time he has, however, been receiving continuous alarms since the incident, which may impede his judgment (distractions) or enhance his judgment. He is expected to receive at least five alarms during that period, that is, two high-pressure CRM alarms and three high-level LEV alarms.
2. General standards allow the operator 10 min to react to an alarm. So by this time he will try to contact the field operator to fix the problem and open the valve.
3. The field operator, if he is close to the valve, can try to open it locally. If the valve does not open he will call back to the control room operator to explain the situation. It is assumed here that the valve cannot open or reset from the control room because it is a shutdown valve. It can only open or reset from the field.
4. If the field operator happens to be away from the valve, it is impossible to react to any instructions within 10 min.
5. The control room operator has to coordinate the actions of the field operator with his decision whether to trip the single train following the procedure. If the time since the alarm approaches 10 min then he needs to trip the train.
6. Tripping the train involves pressing two physical ESD pushbuttons that are located very close to the operator console: one for the Liquid Export Pump (LEP)/Liquid Export Vessel (LEV) trains and one for the production train.

The commission error in steps (1)–(3) can be one of the following:

1. The control room operator forgetting that he needs to act within 10 min, that is, neglecting the procedure.
2. The control room operator does recognize the alarm for some time after it occurred, say 5 min. He does not realize that the time to act is less than 10 min, that is, only 5 min, because the alarm activated long before he acknowledged it.
3. The field operator starts talking to the control room operator about other issues diverting his attention.
4. Another incident happens that also diverts the attention of the control room operator.

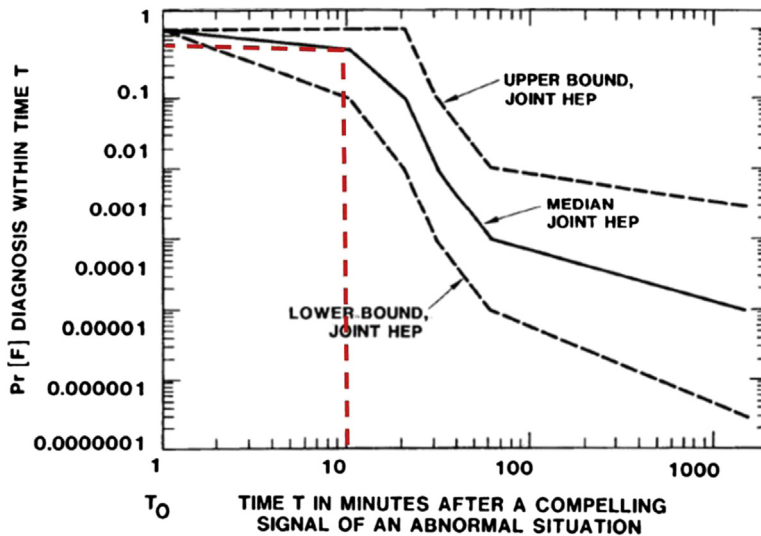


FIGURE 5.32

Nominal diagnosis model (estimate HEPs and UCBs for diagnoses within time).

- The control room operator does everything right, but presses the wrong ESD pushbutton and either does not trip any train or he trips the whole plant.

The computation of the probability of error is as follows.

The omission human error probability is computed using the ASEP method. Fig. 5.32 suggests that a 10-min response time leads to a 60% probability of error.

Concerning the NHEP = 0.6, the same value of HEP can be achieved by SPAH-R based on the nominal value for all PSFs. In fact, concerning the human performance factors effect, the task is not complex (pressing a single physical pushbutton), therefore there is no reason to suggest that procedures, training, and ergonomics are not in place for such an activity. The available time is, however, the same as the required time if in the 10 min we include the diagnosis. High stress is not considered, because prior to the CRM blockage it is assumed that there has not been any other incident, otherwise a double jeopardy case arises. Hence the  $PSF_{\text{composite}}$  value is 1, as described in Table 5.44. As a result, based on the following equation the HEP = 0.6 which is the same as the value of 0.6 predicted by the ASEP method.

$$PFS_{\text{composite}} = PFS(\text{available time}) \times PFS(\text{stress}) \times PFS(\text{complexity}) \times PFS(\text{experience/training}) \\ \times PFS(\text{procedures}) \times PFS(\text{ergonomics}) \times PFS(\text{fitness for duty}) \times PFS(\text{work process})$$

$$PFS_{\text{composite}} = 1 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 = 1$$

$$HEP = \frac{0.6 \times 1}{0.14 \times (1 - 1) + 1} = 0.6 = 60\%$$

<b>Table 5.44 PSF Values</b>		
<b>PSFs</b>	<b>PSF Levels</b>	<b>Multiplier for Action</b>
Available time	Inadequate time	$P(f) = 1$
	Time available $\approx$ time required	10
	Nominal time	1
	Time available $\geq 5 \times$ time required	0.1
	Time available $\geq 50 \times$ time required	0.01
	Insufficient information	1
Stress	Extreme	5
	High	2
	Nominal	1
Complexity	Insufficient information	1
	Highly complex	5
	Moderately complex	2
	Nominal	1
Experience/ Training	Insufficient information	1
	Low	3
	Nominal	1
	High	0.5
Procedures	Insufficient information	1
	Not available	50
	Incomplete	20
	Available but poor	5
	Nominal	1
Ergonomics	Insufficient information	1
	Missing/Misleading	50
	Poor	10
	Nominal	1
	Good	0.5
Fitness for duty	Insufficient information	1
	Unfit	$P(f) = 1$
	Degraded fitness	5
	Nominal	1
Work process	Insufficient information	1
	Poor	5
	Nominal	1
	Good	0.5
	Insufficient information	1

Source: NUREG, CR-6883.

To calculate the commission human error probability the method SPAR-H can also be applied. Therefore, based on the HEART method NHEP values defined in Table 5.44, NHEP = 0.13 for a simple task performed rapidly (task type: D), which in this case is the recognition of the alarm and the action to trip one train in 10 min. The NHEP is 0.13, that is, the upper bound of category D.

### 5.13.3 SPAH-R: COMMISSION ERROR PROBABILITY

In fact, there are clearly two potential errors to be considered in this case: one in the field and one for the control room operator. The rate of failure of the commission error is computed based on the SPAR-H method. The PFS values considered for the field operator error probability are shown in Table 5.44, along with the justification. The PFS<sub>composite</sub> is predicted as shown in the following equation:

$$\begin{aligned} \text{PFS}_{\text{composite}} &= \text{PFS}(\text{available time}) \times \text{PFS}(\text{stress}) \times \text{PFS}(\text{complexity}) \times \text{PFS}(\text{experience/training}) \\ &\quad \times \text{PFS}(\text{procedures}) \times \text{PFS}(\text{ergonomics}) \times \text{PFS}(\text{fitness for duty}) \times \text{PFS}(\text{work process}) \end{aligned}$$

$$\text{PFS}_{\text{composite}} = 1 \times 2 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 = 2$$

For the control room operator error, the PFS<sub>composite</sub> predicted is:

$$\begin{aligned} \text{PFS}_{\text{composite}} &= \text{PFS}(\text{available time}) \times \text{PFS}(\text{stress}) \times \text{PFS}(\text{complexity}) \times \text{PFS}(\text{experience/training}) \\ &\quad \times \text{PFS}(\text{procedures}) \times \text{PFS}(\text{ergonomics}) \times \text{PFS}(\text{fitness for duty}) \times \text{PFS}(\text{work process}) \end{aligned}$$

$$\text{PFS}_{\text{composite}} = 10 \times 5 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 = 50$$

The next step is to calculate the total HEP considering field and control room operators. To calculate the human error probability it is necessary to define the nominal human error probability. Based on current SPAR-H procedures, the NHEP for commission error is 0.001. In fact, this value defined by the standard is very low and will not reflect the human error during the operational phase. In the case of operational phase, such value can be applied to predict the HEP. To define the NHEP for the operational phase, it will be applied based on HEART, as described in Table 5.45.

Based on the HEART nominal human error definition, the respective task and human probability error are:

- Field operator action—task B—NHEP = 0.14;
- Control room operator action (commission error)—task F—NHEP = 0.007.

Thus the field operator and control room operator commission error human probability are:

Field operator action error:

$$\text{HEP} = \frac{0.14 \times 2}{0.14 \times (2 - 1) + 1} = 0.25 = 25\%$$

Control room operator action (after field operator fails to recover):

$$\text{HEP} = \frac{0.007 \times 100}{0.007 \times (100 - 1) + 1} = 0.26 = 26\%$$

	<b>Generic Tasks</b>	<b>Nominal Human Unreliability</b>	
A	Totally unfamiliar, performed at speed with no real idea of likely consequences	0.55	(0.35–0.97)
B	Shift or restore system to a new or original state on a single attempt without supervision or procedures	0.26	(0.14–0.42)
C	Complex task requiring high level of comprehension and skill	0.16	(0.12–0.28)
D	Fairly simple task performed rapidly or given scant attention	0.09	(0.06–0.13)
E	Routine, highly practiced, rapid task involving relatively low level of skill	0.02	(0.07–0.045)
F	Restore or shift a system to original or new state following procedures with some checking	0.003	(0.0008–0.007)
G	Completely familiar, well-designed, highly practiced, routine task occurring several times per day, performed to highest possible standards by highly motivated, highly trained and experienced personnel, with time to correct potential error, but without the benefit of significant job aid	0.0004	(0.00008–0.009)
H	Respond correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of system state	0.00002	(0.000006–0.009) 5th–95th percentile bound

*Source: HEART procedure.*

The next step in human reliability analysis is to combine the ESDV fail with human error to repair it and therefore predict the frequency of shutdown during operation on a yearly basis. Such analysis will be performed in Chapter 6 by applying the hybrid bow tie analysis and Fault tree analysis (FTA).

## REFERENCES

- Annett, J., Duncan, K.D., Stammers, R.B., Gray, M.J., 1971. Task analysis. Training information No. 6, HMSO, London.
- Bell, J., Holroyd, J., 2009. Justin Review of Human Reliability Assessment Methods. The Health and Safety Laboratory for the Health and Safety Executive. Research Report 679. HSE 2009.
- Boring, R.L., Gertman, D.I., 2005. Advancing Usability Evaluation Through Human Reliability Analysis. Human Computer Interaction International.
- Calixto, E., Brito, G., Alves, L., Firmino, P.R., 2013. Alves 3 Comparing SLIM, SPAR-H and Bayesian Network Methodologies. Open Journal of Safety Science and Technology (3), 31–41. <http://dx.doi.org/10.4236/ojsst.2013.32004>. Published Online June 2013. <http://www.scirp.org/journal/ojsst>.
- Embrey, D.E., Humphreys, P., Rosa, E.A., Kirwan, B., Rea, K., 1984. SLIM-maud: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment, Volume 2: Detailed Analysis of the Technical Issues. NUREG/CR-3518. Brookhaven National Laboratory, Upton, NY.
- Grozdanovic, M., 2005. Usage of human reliability quantification methods. International Journal of Occupational Safety and Ergonomics (JOSE) 11 (2), 153–159.



- Korb, K.B., Nicholson, A.E., 2003. Bayesian artificial intelligence. Chapman & Hall/CRC, Florida.
- Kumamoto, H., Henley, E.J., 1996. probabilistic Risk Assessment and Management for Engineers and Scientists. IEEE PRESS, ISBN 0780360176.
- Lopez, D.E., 2007. Menezes Regilda da Costa Lima. Análise da confiabilidade humana via redes Bayesianas: uma aplicação à manutenção de linhas de transmissão. *Produção* 17 (1), 162–185. Jan./Abr.
- Mannan, S. (Ed.), 2005. *Lees' Loss Prevention in the Process Industries*, third ed. Elsevier, New York.
- Menezes, R., 2005. da Costa Lima. Uma metodologia para avaliação da confiabilidade humana em atividades de Substituição de cadeias de isoladores em linhas de transmissão. Dissertação de Mestrado. UFPE, Recife, Junho.
- Nureg/Cr 4772.
- Nureg/CR-6883, INL/EXT-05e00509.
- Nielson, J., Phillips, V.L., 1993. Estimating the relative usability of two interfaces: heuristics, formal and empirical methods compared, in *InterCHI'93*, ACM. New York, pp. 214–221.
- Pearl, J., 1998. *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. second ed. Morgan Kaufmann, California.
- Swain, A.D., February 1987. Accident Sequence Evaluation Program Human Reliability Analysis Procedure. NUREG/CR-4772.
- Swain, A.D., Guttmann, H.E., October 1980. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. draft, NUREG/CR-1278.
- Silva, V.A., 2003. O planejamento de emergências em refinarias de petróleo brasileiras: um estudo dos planos de refinarias brasileiras e uma análise de acidentes em refinarias no mundo e a apresentação de uma proposta de relação de canários acidentais para planejamento. Dissertação (Mestrado em Sistemas de Gestão). Universidade Federal Fluminense, Niterói, p. 158, 2003.
- Spurgin, A.J., 2010. *Human Reliability Assessment: Theory and Practice*. CRC Press. Taylor & Francis Group.
- Vestrucci, P., 1990. In: *Modelli per la Valutazione dell’Affidabilità umana*. Franco Angeli Editore.
- William, J.C., 1988. A data-based method for assessing and reducing human error to improve operational performance. In: *Proceeding of IEEE Fourth Conference on Human Factors in Power Plants*, pp. 436–450 (Monterey, CA).

# RELIABILITY AND SAFETY PROCESSES

## CHAPTER OUTLINE

<b>6.1 Introduction</b> .....	<b>554</b>
<b>6.2 Risk Analysis Methods</b> .....	<b>561</b>
<b>6.3 Preliminary Hazard Analysis (PHA)</b> .....	<b>564</b>
<b>6.4 Hazard and Operability Analysis (HAZOP)</b> .....	<b>567</b>
<b>6.5 Fault Tree Analysis (FTA)</b> .....	<b>572</b>
6.5.1 Time-Independent FTA .....	573
6.5.2 Time-Dependent FTA .....	577
6.5.3 FTA as Qualitative Risk Analysis Support.....	580
6.5.4 FTA as a Root Cause Analysis Tool .....	583
<b>6.6 Event Tree Analysis (ETA)</b> .....	<b>584</b>
6.6.1 Time-Independent ETA .....	585
6.6.2 Time-Dependent ETA.....	587
<b>6.7 Layers of Protection Analysis (LOPA)</b> .....	<b>590</b>
6.7.1 Independent Time LOPA .....	591
6.7.2 Time-Dependent LOPA.....	591
6.7.3 Time-Dependent LOPA as Qualitative Risk Analysis Support.....	594
<b>6.8 Safety Integrity Level Analysis (SIL Analysis)</b> .....	<b>596</b>
6.8.1 Hazard Matrix Methodology .....	600
6.8.2 Risk Graph Methodology .....	604
6.8.3 Frequency Target Methodology.....	606
6.8.4 Individual and Societal Risk Methodology.....	607
6.8.5 Quantitative Approach to Defining Probability of Failure on Demand .....	608
<b>6.9 Bow Tie Analysis</b> .....	<b>611</b>
6.9.1 Time-Independent Bow Tie Analysis.....	613
6.9.2 Time-Dependent Bow Tie Analysis .....	616
<b>6.10 Risk Analysis Case Studies</b> .....	<b>621</b>
6.10.1 Case Study 1: Applying LOPA to Decide Whether Risk is Acceptable When Layers of Protection Are Not Available.....	622
6.10.2 Case Study 2: RAMS Analysis Methodology Applied to Measure Safety Process Effects on System Availability.....	629
<i>Safety Processes</i> .....	630
<i>RAM Analysis Case Study</i> .....	632

6.10.3 Case Study 3: Shutdown Emergency Valve Risk Analysis: FTA, Bow Tie, and HRA Integrated Approach .....	641
<i>Human Reliability: Standardized Plant Analysis Risk-Human Reliability (SPAR-H)     and Accident Sequence Evaluation Program (ASEP) Application</i> .....	642
<i>SPAHR: Commission Error Probability</i> .....	644
<i>Bow Tie Case Study Application</i> .....	645
<i>FTA Case Application</i> .....	646
<i>Hybrid Method Case Application</i> .....	646
6.10.4 Case Study 4: Blowout Accident Analysis Based on Bow Tie Methodology .....	648
6.10.5 Case Study 5: Safety Integrity Level Risk Assessment: SIL Selection and Verification Analysis .....	650
<i>HAZID</i> .....	653
<i>LOPA</i> .....	653
<i>SIL Selection</i> .....	654
<i>SIL Verification</i> .....	659
<b>References</b> .....	<b>662</b>
<b>Appendix A</b> .....	<b>663</b>

---

## 6.1 INTRODUCTION

Risk analysis and management began around the middle of the 20th century in different industries with different approaches such as:

- In the 1960s—the aerospace industry with quantitative risk assessment methods and the nuclear industry with a probabilistic risk assessment approach;
- In the 1970s—the chemical industry with quantitative risk assessment and the Seveso directive;
- In the 1980s—the oil and gas industry with quantitative risk assessment and safety case.

By definition, risk is the combination of a hazardous event and its consequence. To analyze and evaluate risk, the qualitative and quantitative approach can be performed. In fact, when risk is assessed and evaluated based on qualitative methods, such assessment is performed qualitatively based on specialist opinion regarding a risk matrix with the frequency and consequence criterion established.

There are different configurations of risk matrix and such configuration must reflect the law and companies' risk policy. In fact, before making an appropriate risk matrix it is necessary to define clearly the frequency or probability category as well as severity. The discussion between risk specialists regarding the best risk matrix is usually a difficult one: frequency or probability, but in reality most of the time it is easier for the specialist who takes part in risk analysis to predict frequency rather than probability concerning the causes of accidents. Fig. 6.1 shows an example of a risk matrix with four severity categories and six frequency categories. Again, the risk matrix configuration must fit well to companies and their process, and in some cases it is necessary to use a different risk matrix for different processes in the same company.

In addition, severity classification must list all parties affected in the case of an accident, such as employees, the community and environment, as well as company installation costs. Table 6.1 shows an example of a severity category.

		FREQUENCY CATEGORY					
		A (extremely remote)	B (remote)	C (Little frequency)	D (Frequent)	E (Very frequent)	F (Extremely frequent)
		At least 1 between 1000 and 100,000 years	At least 1 between 50 and 1000	At least 1 between 30 and 50 years	At least 1 between 5 and 30 years	At least 1 in 5 years	At least 1 in 1 year
SEVERITY CATEGORY	IV	M	NT	NT	NT	NT	NT
	III	M	M	NT	NT	NT	NT
	II	T	T	M	M	M	M
	I	T	T	T	M	M	M

FIGURE 6.1

Risk matrix.

Source: Calixto, 2011.

Table 6.1 shows four severity categories regarding personal safety, installation, environment, and image as well as social impact, which is measured by impact on economic activity.

Risk can also be assessed by a quantitative approach and in this case individual and societal risk is the most appropriate and frequently used method.

Individual risk is frequency of death per year for people located in a vulnerable area. The individual risk index is represented by the ISO—risk curve or the as low as reasonably practicable (ALARP) limits.

The ISO—risk curve is a graphic representation of a vulnerable area that an individual or population is exposed to considering the value of individual risk. In some countries, there is a risk criterion, which depends on an individual risk value, for example,  $1 \times 10^{-6}$ . The contour curve cannot achieve an unacceptable region in the presence of the community, as shown in Fig. 6.2.

The ALARP factor is principally used in project analysis as a risk criterion. A crucial point in this criterion is the consideration of how much a risk must be mitigated below an acceptable level. There is an investment implication and in most cases it is not clear how much return such additional investment gives in term of safety. Fig. 6.3 shows the ALARP risk tolerability.

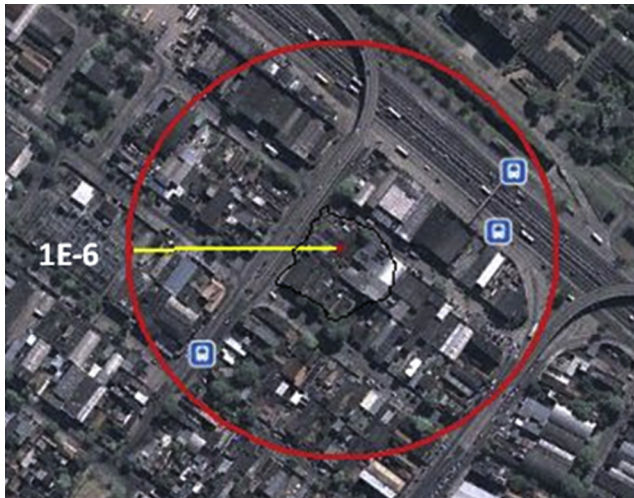
Individual risk is calculated from the sum of all risks of each accident scenario in a plant facility, and is expressed in terms of the number of deaths per year. To define the number of deaths in each accident scenario, it is necessary to carry out a Consequence and Effect analysis (CEA) to predict such a number based on the effect on employees in a vulnerable area. Such a calculation considers the consequences (radiation, toxic level, pressure wave) and tolerance that are defined by PROBIT equations. This will be discussed in more detail with examples of a CEA.

Remarkably, in some countries only societal risk is a decision criterion for acceptance of new projects; individual risk is not. Regardless of how many deaths occur during a plant installation, if such an accident does not affect the community outside the plant, the project is accepted. From a safety point a view, this makes no sense and means that projects with a low level of safety are accepted by authorities when they are located in places where no community is present, or where there will be no significant effect on the community.

**Table 6.1 Severity Category**

			Description and Characteristic			
			Personal Safety	Installation	Environment and Image	Social
Severity category	IV	Catastrophic	Catastrophic injuries with death; it is possible to effect people outside	Losses in equipment and plant with high cost to buy new one	Loss of ecosystem with poor national and international company reputation	Economic effects on local activities, health costs on local population, economic losses on tourism, local ecosystem losses, and quality of life losses (between R\$101,000,000.00 and R\$336,000,000.00)
	III	Critical	Critical injuries. Employees stay a period of time out of workplace	Equipment serious damaged with high cost to repair	Critical effects to environment being hard to improve ecosystem condition even with human actions. Poor national and international company reputation	Economic effects on local activities, health costs on local population, economic losses on tourism, local ecosystem losses (between R\$2,500,000.00 and R\$101,000,000.00)
	II	Marginal	Moderate injuries with first aid assistance	Low equipment damage with low repair cost	No serious environment effects but human intervention is necessary and actions to improve environment. Poor national company reputation	Economic effects on local activities, health costs on local population, economic losses in tourism, fishing and other areas (from R\$0.00 to R\$2,500,000.00)
	I	No effect	There are no injuries or damage to health	There is no damage to equipment and plant	Insignificant environmental effect. There is no necessity for human action to improve ecosystem. There is no effect on national company reputation	There are no economic effects on local activities or health costs to the local population

Source: Calixto, 2011.

**FIGURE 6.2**

ISO—risk curve.

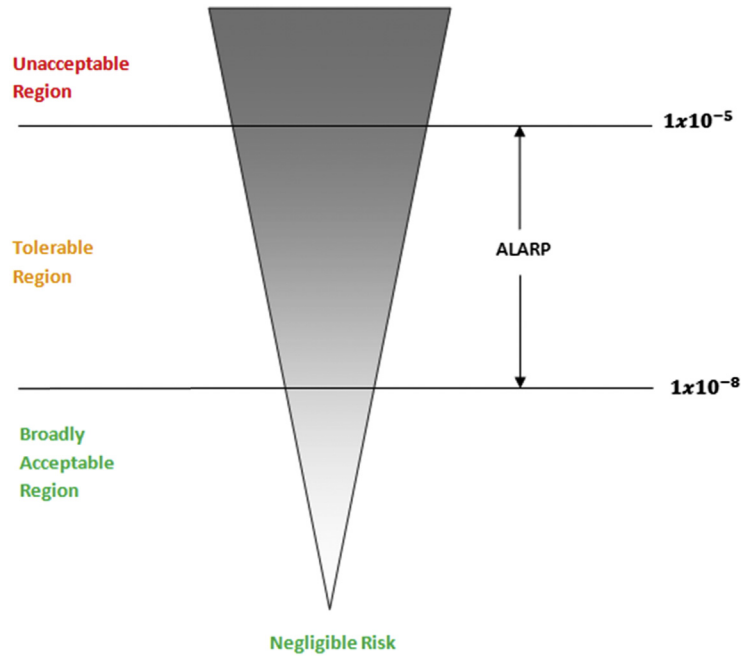
Source: Calixto, 2011.

Furthermore, in most of cases in individual risk calculation, such risk is considered independent of time. That means the calculated risk remains constant for a long period of time. This is unrealistic because initiating events are mostly equipment failures that are dependent on time and are better represented by cumulative density function distribution. Consequently, the probability of failure increases over a long period of time, and this results in the associated risk increasing over a period of time. To keep risk at an acceptable level, inspection and preventive maintenance are required so that failure in layers of protection and equipment with possible unsafe failures may be detected.

Societal risk is the frequency of death per year to which a community outside the industrial area is exposed. Societal risk is usually represented by the F—N curve that shows the cumulative expected number of fatalities on each frequency level. Such a curve represents the combination of the expected number of deaths and the frequency, and is thus a cumulative curve, which takes into account all the hazard scenarios from one or more specific hazard sources in the plant facility, which may affect the community outside the plant facility area. ALARP is also represented by the F—N curve to define when societal risk is acceptable or not. A high level of reliability on layers of protection and equipment can also help to mitigate risk, as well as the implementation of preventive maintenance to keep a high level of reliability and availability of such devices. Fig. 6.4 shows an example of an F—N curve within the ALARP region.

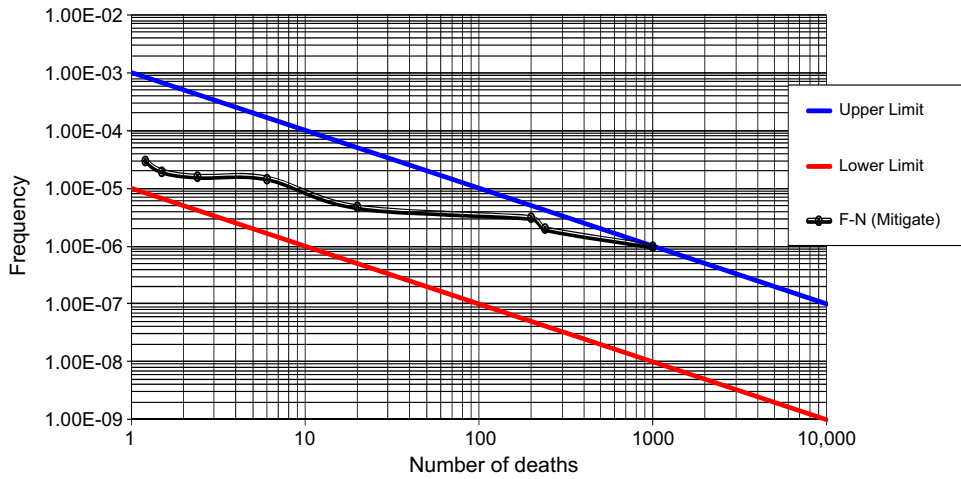
Two of the most important concepts in quantitative risk analysis are the probability and frequency of an event. The probability of failure is the inverse of reliability. Reliability is the probability of equipment, products, or services operating successfully over a specific period of time, and is the mathematical complement of the probability of cumulative failure.

Thus, in risk analysis, the probability of event occurrence can be assessed by cumulative density functions (CDFs), or, in other words, unreliability time, as shown in Fig. 6.5. In this way, the quantitative methods for defining probability density functions (PDFs) and CDFs (unreliability) discussed in Chapter 1 will be used in risk analysis to define the probability of failure over time.



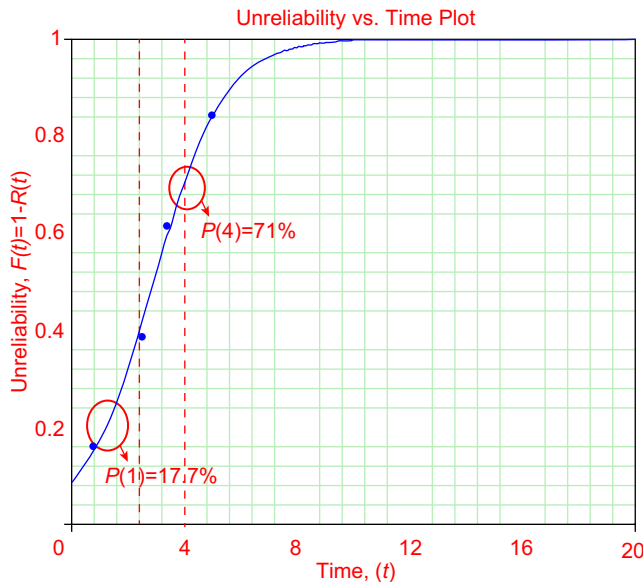
**FIGURE 6.3**

ALARP individual risk (Netherlands).



**FIGURE 6.4**

Societal risk.

**FIGURE 6.5**

Probability of failure.

In Fig. 6.5 it is clear that depending on the time considered in risk analysis, the probability of failure will be different. The probability is higher if no maintenance on equipment is performed to reestablish a part of reliability. Thus if 1 year is used the probability of failure is 17.7%, but if 4 years is used the probability of failure is 71%. Such concept will be applied to the quantitative risk methods in the following sections.

To define, assess, and mitigate risk, the risk management process is vital. In fact, risk management is applied to maintain process risk under acceptable levels and avoid whenever possible incidents and accidents. Based on ISO 31000 standard, risk management is established based on the Plan, Do, Check and Act (PDCA) concept, which encompasses different steps such as:

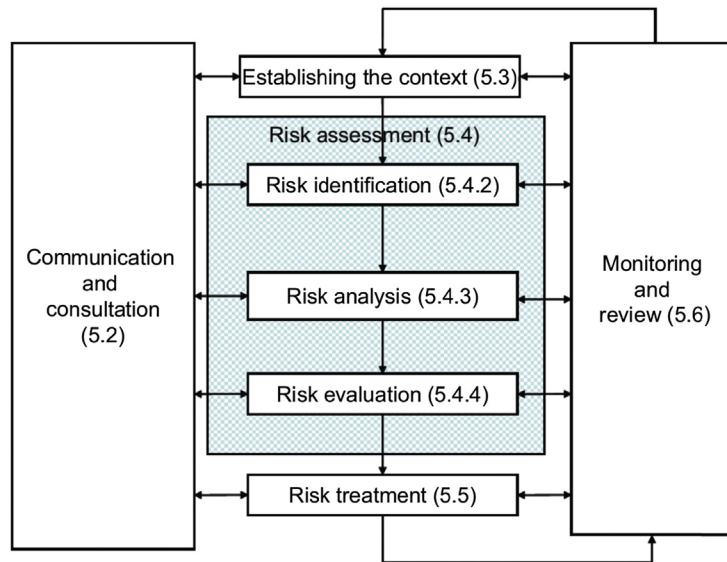
- Mandate and commitment: requires risk management policy establishment at strategic level and such policy will drive all goals and indexes throughout the organization.
- Design of a framework: supports the first step more effectively and will guarantee that the risk policy is adequate for the company taking into account the internal and external organization's context.
- Implementing risk management: comprises four phases, which are risk assessment, risk treatment, risk communication, and risk monitoring and review.

Fig. 6.6 shows the risk management process based on ISO 31000 concepts.

To mitigate process risk, different layers of protection with significant reliability are applied to assure that in case of unsafe process conditions the system will return to a safe condition. Therefore the acceptable risk level in industrial processes relies on multiple layers of protection.

There are different types of layers of protection such as design features, control systems, safety protection functions, and emergency response plans. The best approach to maintain an acceptable risk level is to start risk management during the design phase. Moreover, it is also necessary to





**FIGURE 6.6**

Risk management process.

Source: ISO 31000, 2009.

implement risk analysis recommendation throughout the asset phases and update risk analysis whenever a process modification takes place. In fact, during the project phase, there are increased flexibilities for modifications to incorporate new ideas to improve asset safety rather than during the operational phase.

The major approach to inherently safer process designs is divided into the following categories (Crow and Louvar, 2002):

- Intensification
- Substitution
- Attenuation
- Simplification

Intensification means minimizing risk whenever possible based on less hazardous equipment and products. Substitution means replace whenever it is possible the current equipment for more safety equipment and products. Attenuation means processes should be designed to mitigate the effects of accidents. Simplification means establishing process control as simple as possible for case of incidents and accident.

An additional important concept related with risk management is risk perception, which means how much employees and other affected parties like communities are aware of the risks to which they are exposed. Risk perception is related to risk communication and is a very important task of risk management. In fact, risk communication is difficult to apply because of the requirements of different groups of employees and even society. A powerful tool to communicate risk is *safety dialogue*,

which is a discussion about a safety-related issue carried out for a particular employee. The main objective is to make groups aware of such issues and enable discussion. To communicate process risk to operators a safety dialogue is appropriate because it enables discussion about risks rather than an electronic message. In the same way, whenever a meeting is conducted with the community, in most cases such communication is about emergency procedures that are very important to the community in case of an accident. Whenever possible the communication management team must be involved in such a process because they know the best ways to communicate and to deal with information within the company.

Risk communication has a high influence on risk perception but does not guarantee that risk perception will trigger preventive behavior in the workplace because this depends on safety culture as well. In addition, even though employees and society realize the risk they are exposed to, there is a third factor that influences their behavior: their risk profile. In general terms, risk profile can be aversive, neutral, or searching and varies from person to person depending on the situation and people's attitudes. Such a risk profile is very important to understand a leader's attitude to prevent and mitigate risks.

Finally, risk analysis results have to be considered in an emergency plan and such plan must be part of risk management. An emergency plan is a set of activities carried out in case of an accident, as well as resources and responsibilities for each task. A well-defined emergency plan is essential to have a good emergency response in case of accidents, but in addition it is necessary to carry out practical exercises in emergency plan application regarding an accident scenario. Thus it is very important to take into account the risk analysis results in the emergency plan otherwise the emergency response team will not be prepared to effectively respond to a predicted accident scenario. However, risk analysis does not cover all accident scenarios but the challenge is to be prepared for all possible events, even natural catastrophes and terrorist attacks.

---

## 6.2 RISK ANALYSIS METHODS

Previous chapters have described quantitative and qualitative reliability engineering tools for assessing equipment failures, system performance, human error based on historical data (failure and repair), test results data, and even specialist opinion. Such methodologies usually detect a poor factor in system performance or product development based on different tools, which is supported by historical data or specialist opinion. In these cases, functional failures that cause equipment and system unavailability are considered, but unsafe failure can also be assessed and supported by the tools used to achieve safe operational and maintenance performance.

Qualitative reliability approaches can be performed to support safety engineering goals as described in Chapter 3 for applications of RBI and FMEA. Even RCM can be applied to define maintenance and inspections for components with unsafe failures. In some cases, equipment does not lose functionality but operates in unsafe conditions that can cause accidents to occur.

Quantitative reliability approaches, mainly life cycle analysis, can also support risk analysis to define events and unsafe failure probabilities over time using PDFs and CDFs to better define risk values. Risk is a combination of probability/frequency of accident occurrence and consequences. Thus risk analyses are methodologies that detect hazard and quantify risk in equipment, processes, and human activities.

Despite the importance of quantifying risk based on quantitative risk analysis methods, it is also important to apply qualitative methods to identify the hazard, unsafe process condition, or even the unsafe failures. The most applied qualitative and quantitative risk analysis methods in the oil and gas industry are:

- PHA (preliminary hazard analysis)
- HAZOP (hazard operability study)
- HAZID (hazard identification study)
- FMEA (failure mode event analysis)
- FTA (fault tree analysis)
- ETA (event tree analysis)
- LOPA (layers of protection analysis)
- SIL (safety integrity level)
- Bow tie analysis

PHA is a qualitative preliminary hazard analysis that consists of identifying hazards in systems or activities, their causes and consequences, and proposes recommendations to prevent such consequences. In some cases, the PHA includes risk classification, and in this case is performed qualitatively based on a risk matrix supported by specialist opinion.

HAZOP is a hazard analysis that consists of identifying process hazard deviations in a system based on process condition keywords (high level, low level, high pressure, low pressure, high flow, low flow, high temperature, and low temperature), their causes, consequences, and safeguards. The system is divided into several subsystems, and each subsystem is divided into nodes, which are part of the process being analyzed. This analysis is conducted to make process analysis easier. Based on consequences and existing safeguards, recommendations are proposed to prevent such unsafe process conditions and consequences.

HAZID is a hazard analysis that consists of identifying process hazards in a system and their causes, consequences, and safeguards. Similar to HAZOP, the system is divided into subsystems, and each subsystem is divided into nodes. Based on consequences and existing safeguards, recommendations are proposed to prevent such unsafe conditions and consequences.

FMEA is a failure mode analysis that consists of identifying equipment failures, their causes and consequences, and proposes recommendations to prevent such failure consequences. In some cases, FMEA focuses on unsafe failures to prevent unsafe conditions.

FTA is a quantitative risk analysis that consists of identifying combinations of events that cause unwanted top events. The final result is the probability of the top event and this method is based on probability calculations, or, in other words, Boolean logic.

ETA is a quantitative risk analysis that consists of identifying the combinations of sequences of events that cause accidents. The final result is the probability or frequency of accidents and this method is based on probability calculations.

LOPA is a quantitative risk analysis that consists of identifying trigger events that cause an incident and combinations of sequences of layers of protection that prevent these incidents from turning into an accident. The final result is a probability or frequency of accidents and this method is based on probability calculations.

**Table 6.2 Risk Analysis Throughout the Asset Phases**

Situations	Asset Phases				
	Predesign	Design	Basic Project	Operational	Decommissioning
1. Identify hazards	System PHA	Subsystem and equipment PHA	Occupational PHA	PHA FTA ETA Bow tie <sup>a</sup>	PHA
2. Identify hazards in the process or equipment to mitigate risk	DFMEA	DFMEA	HAZOP FMEA PHA LOPA SIL ETA FTA	PHA FMEA/ FMECA PHA LOPA SIL ETA FTA	PHA
3. Define vulnerable areas, ISO—risk, and societal risk			Consequence and effect analysis	Consequence and effect analysis	
4. Decide which technology has lower risk	Consequence and effect analysis <sup>b</sup> FMECA <sup>c</sup> FTA	Consequence and effect analysis FMECA FTA	Consequence and effect analysis FMECA FTA		

<sup>a</sup>Use only the bow tie logic diagram without quantifying probability.  
<sup>b</sup>Use analysis of similar plants.  
<sup>c</sup>Use analysis of similar equipment.  
 Source: Calixto, E., 2015. *Safety Science: Methods to Prevent Incidents and Worker Health Damage at the Workplace*. eISBN:978-1-60805-952-2, 2015. ISBN:978-1-60805-953-9. <http://dx.doi.org/10.2174/97816080595221150101> (bethamebook).

SIL is semiquantitative risk analysis that consists of identifying probability failure on demand required for the SIF (safety instrumented function) to reach an acceptable risk level.

Bow tie analysis is a quantitative risk analysis that consists of assessing an accident and identifying and calculating the accident consequence probability.

The important issue when performing risk analysis is to be clear about the objective and also the right asset phase to perform the proper risk analysis. Table 6.2 shows the best phase to perform the different risk analysis methods, taking into account the level of information available in each asset phase and also the situation and demand for a risk analysis.

The following sections will describe each of the foregoing risk analysis methods with examples. At the end of the chapter, case studies will demonstrate the applicability of such risk analysis methods to support the risk management process.

### 6.3 PRELIMINARY HAZARD ANALYSIS (PHA)

PHA analysis has its origins in the military as a technique applied to check missile launch systems. As a result, 4 of 72 intercontinental Atlas missiles were destroyed at high cost.

In the oil and gas industry, PHA is applied during the project phase to assess system and subsystem hazards as well as during the operational phase to prevent accidents during routine and nonroutine activities. Thus no matter the application, the main objective is to support decisions to avoid accidents and eliminate unsafe conditions (Calixto, 2007b).

In general terms the PHA steps are:

- Step 1—To collect information about the system.
- Step 2—To define a risk analysis team.
- Step 3—To define a risk matrix when applicable.
- Step 4—To define the scope (system, subsystem and process).
- Step 5—To proceed with PHA.

In the first step it is necessary to collect all information about the system, technological as well as accident and incident historical information.

In the second step, once system information is known, it is necessary to define a PHA team who will use their specialist knowledge to carry out a PHA. Mainly such specialists are professionals from the safety, operational, maintenance, instrumentation, environment as well as the engineering fields who are responsible for equipment and the process plant (or project).

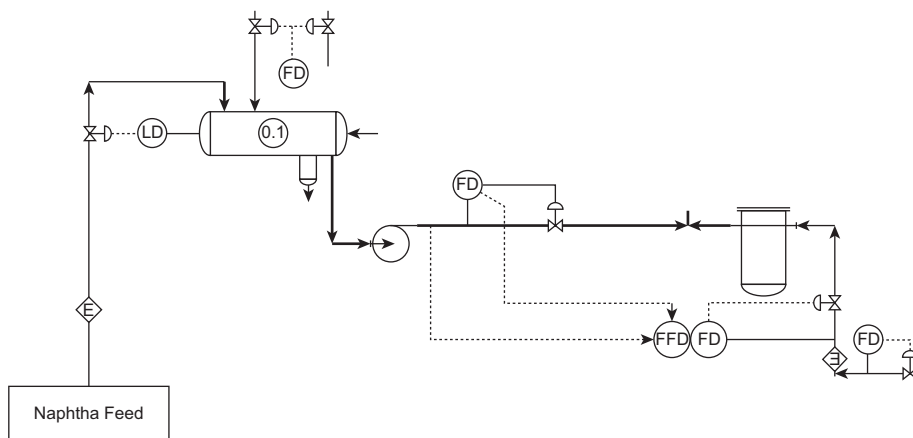
In the third step, before startup of a PHA, it is necessary to define which risk matrix will be applied to a PHA. This is a very important task and if attention is not paid the PHA can be rejected by companies or even by authorities, for example, the PHA for an environmental license. When a PHA is carried out to obtain an environmental license it is very important to compare the risk matrix that is intended to be used with that defined by environment agencies.

The fourth step is necessary to define the scope of analysis. In some cases it is clear which system and subsystem will be assessed and in others it is not. For example, when a modification is carried out and there are new hazards or processes, a hazard effect may be local or not. Thus it is very important to assess the impact on modification of the whole process to define the scope of analysis regarding all systems and subsystems affected.

The fifth step is to proceed with the PHA and it is necessary to pay attention to framework issues such as the room and electronic devices necessary in the PHA as well as to plan the required time to carry out analysis regarding the availability of all professionals. In many cases it is hard to retain professionals working in operations and maintenance for a long period of time (over 2 weeks). In fact, all efforts must be made to retain the same staff for reasons of consistency.

The PHA can be applied to software or the usual Office tools (Word or Excel) and the file configuration must have as a minimum: hazard, cause, consequence, probability (frequency), severity, risk, detection, and recommendation.

Hazard means unsafe condition, product, process, or equipment condition, which can cause harm to an employee. For instance, in the oil and gas industry, toxic product leakage is a hazard that can lead to different consequences such as jet fire, toxic cloud, cloud explosion, and fireball. Each of these



**FIGURE 6.7**

Naphtha feed to hydrogen generation plant.

consequences has different effects on employees' health and also the environment, which is classified at different severity levels.

In some cases after recommendation, the risk is assessed again to show how much is expected to be mitigated by the implementation of recommendations. An example of a naphtha feed subsystem, which is part of hydrogen generation plant, is demonstrated in Fig. 6.7. A huge leakage of naphtha can cause serious harm to employees' health and also the environment. Fig. 6.8 shows the PHA applied to the naphtha feed case.

An additional example of PHA application is the platform PHA, where a huge oil leakage creates many hazards. Fig. 6.9 shows a simple schematic offshore production. Fig. 6.10 shows the PHA template applied to the offshore production feed.

The partial PHA just discussed highlights possible hazards on a platform load subsystem as well as all causes, consequences, detection and safeguards, risks and recommendations. In this case, risk was assessed based on the risk matrix described in Fig. 6.1 and for each consequence there is a severity category, which results in different risk classifications. It is also possible to have one frequency category for each specific cause and in this case there will be several risks assessed. For each hazard described on a PHA with a nontolerable risk level, it is recommended to apply consequence and effect analysis to define the vulnerable area and effects more precisely.

Additional assessments based on quantitative risk analysis methods such as FTA and ETA can predict the frequency of a hazard more precisely.

In fact, qualitative methods such as PHA identify the hazard with no acceptable risk level as input for quantitative methods such as FTA, bow tie, ETA, and also consequence and effect analysis.

Quantitative methods will be presented in the following section, but consequence and effect analysis is beyond the scope of this book but can be found in other references.

Preliminary Hazard Analysis (PHA)																						
System: Hydrogen Generation Plant – U-510						SISTEM: 1-Hydrogen Generation Feed						DATE: 28/11/2005										
SUBSYSTEM: 1.1 – Naphtha feed				DESCRIÇÃO: From feed manifold to heat exchanger E-09, passing by V-01, P-01 A-B and filter FT-02						Document:												
HAZARD	CAUSES	CONSEQUENCES	DETECTION	F	Safety		Asset		Env		Image		Recommendation	F	Safety		Asset		Env		Image	
					S	R	S	R	S	R	S	R			S	R	S	R	S	R	S	R
Small Leakage	<ul style="list-style-type: none"> <li>– Pump Seal leakage</li> <li>– Joint leakage</li> </ul>	<ul style="list-style-type: none"> <li>– Explosion</li> <li>– Fire</li> <li>– Underground contamination</li> <li>– Health damage</li> <li>– Equipment Damage</li> </ul>	– Gas System Detection	D	II	M	II	M	II	M	II	M	R01) Install HC detector close to Naphtha Feed. Action by: Project	E	II	M	II	M	II	M	II	M
Huge Leakage	<ul style="list-style-type: none"> <li>– Pipe ruptures</li> <li>– Pipes corrosion</li> <li>– Joint leakage</li> </ul>	<ul style="list-style-type: none"> <li>– Explosion</li> <li>– Fire</li> <li>– Underground contamination</li> <li>– Health damage</li> <li>– Equipment Damage</li> </ul>	<ul style="list-style-type: none"> <li>– Gas System Detection</li> <li>– Process Alarm</li> </ul>	C	IV	NT	IV	NT	IV	NT	IV	NT	R01) Install HC detector close to Methane Feed. Action by: Project  R02) Protect the pipeline against external shock caused by material movement or constructions. Action by: Operation  R03) Perform NDT such as Ultrasound to avoid corrosion failure. Action by: Maintenance	A	IV	M	IV	M	IV	M	IV	M

FIGURE 6.8

PHA applied to naphtha feed to hydrogen generation plant.

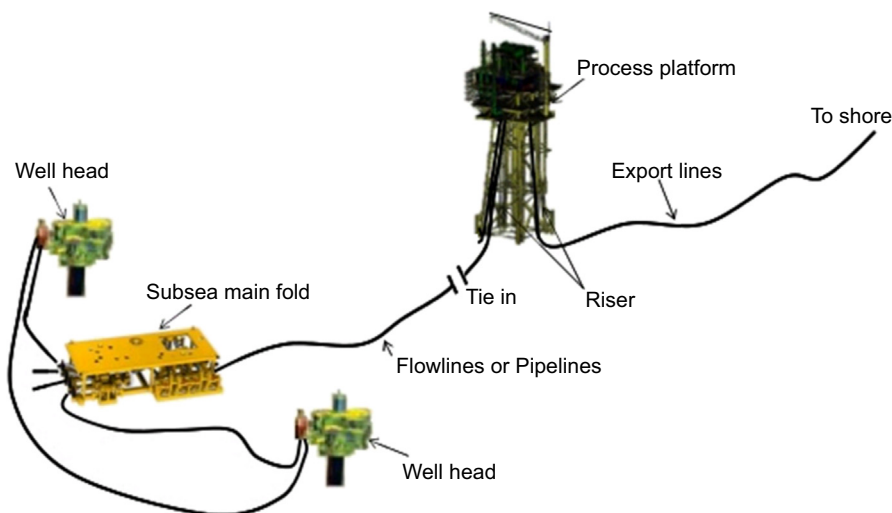
These two examples show the main PHA features that are simple and applicable in all enterprise phases. PHA has advantages and disadvantages:

Advantages:

- Easy to be applied to the oil and gas industry.
- Can be applied in different enterprise phases and can also be updated during enterprise phases.
- Clear understanding and definition of rank, which is the most critical hazard associated with risk.

Disadvantages:

- As a qualitative analysis the risk can be underestimated and recommendations or mitigating actions may not be implemented.
- Depends on specialist experience and historical data, which means if specialists do not recognize one specific hazard such hazard will not be assessed.
- Does not explain in detail the equipment and process failures and consequently does not define specific actions.



**FIGURE 6.9**

Platform production.

Source: <http://image.slidesharecdn.com/98338181-overview-to-subsea-system-131023214853-phapp02/95/subsea-2-638.jpg?cb=1382564946>.

## 6.4 HAZARD AND OPERABILITY ANALYSIS (HAZOP)

HAZOP means hazard and operability and it is a well-known risk analysis method in the chemical and oil and gas industries. This technique was introduced for ICI Chemical company engineers in 1970 to prevent process deviation. It consists of a very structured methodology, which provides a guideline to assess process deviation, causes, consequences, and whenever possible to propose recommendations to mitigate risk.

HAZOP analysis is mainly carried out during the basic project phase to have enough time to implement the recommendations during the project. HAZOP can also be carried out for plants during the operational phase, but this is unusual because it is not expected to be implemented or to perform modifications in the plant during this phase. However, it is very important to carry out HAZOP analysis during the operational phase whenever a specific modification process is implemented. In this case it is also necessary to take into account the impact of such modification on other subsystems and to consider them in HAZOP. Therefore it is also important after HAZOP to communicate the new process risk to all specialists involved in such plant operation and maintenance.

HAZOP methodology consists in defining which are the consequences of process deviation and tries to mitigate the risk by implementing recommendations as layer protection. This is a good structural analysis, which specific process deviation, guide world and concepts.

The first step in HAZOP analysis defines the system and subsystems, and in each subsystem it is necessary to define nodes. These nodes will limit the assessment of subsequent process deviations and include groups of equipment, alarms, valves, and so on. Depending on the HAZOP leader definition,



Preliminary Hazard Analysis (PHA)																																			
Asset: Hydrogen Generation Plant – U-510						PHA leader: Eduardo Calixto						DATE: 28/11/2005																							
SUBSYSTEM: 1.1 – Naphtha feed			Description: From feed manifold to heat exchanger E-09, passing by V-01, P-01 A-B and filter FT-02.						Document:																										
HAZARD	CAUSES	CONSEQUENCES	DETECTION	F	Safety				Asset				Env				Image	Recommendation	F	Safety				Asset				Env				Image			
					S	R	S	R	S	R	S	R	S	R	S	R				S	R	S	R	S	R	S	R	S	R	S	R	S	R	S	R
Small Leakage	<ul style="list-style-type: none"> <li>– Pump Seal leakage</li> <li>– Joint leakage</li> </ul>	<ul style="list-style-type: none"> <li>– Explosion</li> <li>– Fire</li> <li>– Underground contamination</li> <li>– Health damage</li> <li>– Equipment Damage</li> </ul>	– Gas System Detection	D	II	M	II	M	II	M	II	M	II	M	II	M	R01) Install HC detector close to Naphtha Feed. Action by: Project	E	II	M	II	M	II	M	II	M	II	M	II	M	II	M			
Huge Leakage	<ul style="list-style-type: none"> <li>– Pipe ruptures</li> <li>– Pipe corrosion</li> <li>– Joint leakage</li> </ul>	<ul style="list-style-type: none"> <li>– Explosion</li> <li>– Fire</li> <li>– Underground contamination</li> <li>– Health damage</li> <li>– Equipment Damage</li> </ul>	– Gas System Detection – Process Alarm	C	IV	NT	IV	NT	IV	NT	IV	NT	IV	NT	IV	NT	R01) Install HC detector close to Methane Feed. Action by: Project R02) Protect the pipeline against external shock caused by material movement or constructions. Action by: Operation R03) Perform NDT such as Ultrasound to avoid corrosion failure. Action by: Maintenance	A	IV	M	IV	M	IV	M	IV	M	IV	M	IV	M	IV	M	IV	M	

FIGURE 6.10

Preliminary hazard analysis (platform).

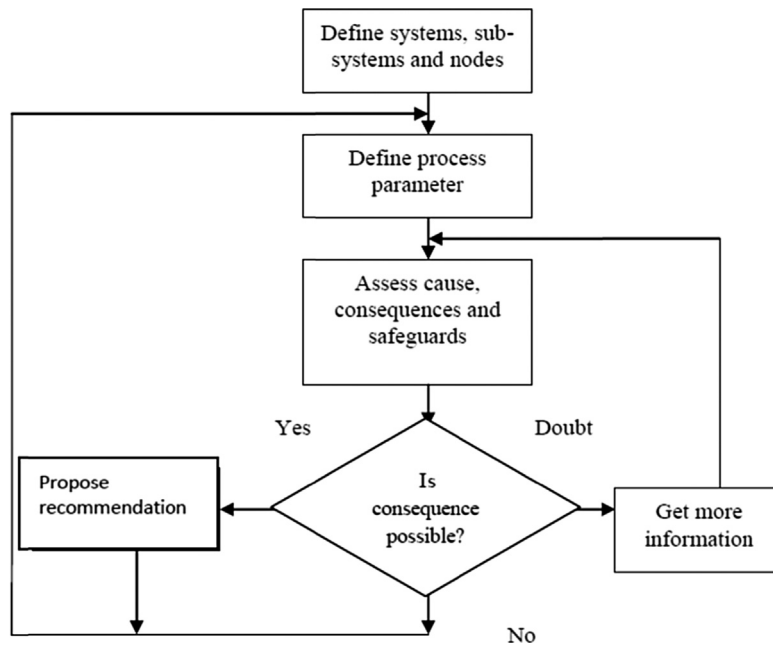
Source: Calixto, 2007a.

it’s been considered the causes and safeguard into the nodes assessed, out of node assessed or both cases. In fact, if it’s been considered the process deviation consequence into the nodes and causes and safeguards in anywhere, the focus is on a node without forgetting any important issues out of that. In fact, on most of cases, the process deviation consequence is considered into the nodes assessed and causes and safeguards in the node assessed or outside the node assessed. The main important issue is to not forget any consequence of process deviation.

The second step is to enquire about process deviation such as pressure, levels, temperature, flow, and contamination, but to do so guide words are necessary, as shown in Table 6.3.

Based on these words, it is good practice to ask the HAZOP analysis group about the effect of process parameter deviation such as low and high pressure, low and high temperature, low and high levels, and low (no) and high flow. Afterward, the causes, consequences, and safeguards are assessed, which is necessary if additional safety functions to mitigate the risk are needed. Safeguard is considered as the equipment that functions independently to bring the process to a safe condition or draw the operator’s attention to unsafe conditions. The difference between safeguarding and layer of

Guide Word	Meaning
None	There is no parameter
Less	Quantitative reduction
More	Quantitative increase
Part of	Qualitative reduction
Either	Qualitative increase
Reverse	Opposite flow than usual
Other	Complete substitute



**FIGURE 6.11**

HAZOP steps.

*Source: Calixto, 2007a,b.*

protection is that layer of protection operates independently without human action to bring the process to a safe condition. Thus all layers of protection are safeguards but not all safeguards are layers of protection, such as an alarm. The HAZOP steps are summarized in Fig. 6.11.

It is very important to have a successful HAZOP and a multidisciplinary group, which means different specialists from operations, maintenance, instrumentation, process, project, and safety (Calixto, 2007b). In addition, it is also necessary to have a HAZOP leader who coordinates HAZOP analysis. Usually, when HAZOP analysis is carried out for a whole process it takes 1 week or more.

This is a big challenge for the HAZOP leader to maintain specialist for a long period of time in the HAZOP workshop. What happens in many cases is that specialization has taken place alongside HAZOP, which makes analysis more difficult because whenever a new member comes to the group it is necessary to clear up all assumption. An important issue with HAZOP is logistics issues such as available and reliable media and electronic devices as well as adequate room. Like all risk analysis, documentation is also very important, which means Piping and Instrumentation Diagram (P&D) draw, process description, equipment data as well as accident historical data. It is vital to have such documentation updated and to make references to HAZOP files. In many cases, to delay HAZOP analysis means that the documentation will not be updated and the HAZOP leader must pay particular attention to this and make reference to HAZOP to ensure that the documentation is up to date.

This means that if there are no devices in P&D draw, even though the specialist confirms such equipment in the next P&D draw version, the equipment must be considered in HAZOP as a recommendation. This usually happens, for example, in the case of a missed alarm or SIF. Fig. 6.12 shows an example of a HAZOP file that has been assessed coke feed subsystem.

In this example, contamination of the product is caused by filter failure. In addition, to install a control valve downstream of the filter, it is necessary to assess the cause of the failure to prevent it.

HAZARD AND OPERABILITY ANALYSIS (HAZOP)				
Asset: Coke Plant (U-511)			System: Coke feed	
			Date: 26/08/2007	
Subsystem: Node 1: From limit battery feed passing by the Filter FT-51101 until the vessel V-51101			Document: 345333-101-10 – A0 Rev-A DE	
Guide Word	Causes	Effects	Detection	Recommendation
High Flow	- Increasing production in Coke Naphtha Plant	- System overload	- PDHH in FT-01. - PSV in FT01.	R01) To define specification about the flow level in the operational procedure Action by: Operation
Low Flow	- Decreasing production in Coke Naphtha Plant	- Small Loss of production	-	
No Flow	- Other Plants shut down - Control Valve failed closed	- Loss of production	-	R002) To define alarm for low flow in V-51101 Action by: Project Team
Reverse Flow	- Flow diverged to TQ-001. - Pressure out of control in V-51101.	- Low level in V-51101.	- Low level alarm in V-51101	
Contamination	- FT-51101 failed	- Product contamination	- PRV in FT-51101	R003) Install control Valve downstream of FT-51101 Action by: Project Team

FIGURE 6.12

Coke plant HAZOP example.

HAZARD IDENTIFICATION (HAZID)																						
System: Subsea				HAZID Leader: Eduardo Calixto						DATE: 10/07/2013												
SUBSYSTEM: 1.1 – Flexible Riser				Node: From the Subsea manifold to Tie in.						Document: 541001-001-00 – A1 Rev-A DE												
HAZARD	CAUSES	CONSEQUENCE	PREVENTION	F	Safety		Asset		Env		Image		Recommendation	F	Safety		Asset		Env		Image	
					S	R	S	R	S	R	S	R			S	R	S	R	S	R	S	R
Huge Leakage	- Flexible riser ruptures caused by Barge impact	- Explosion - Fire - Underground sea contamination - Health damage - Equipment Damage	- Flexible Riser Integrity - Process Alarm	D	IV	NT	IV	NT	IV	NT	IV	NT	R01) To monitor Barge movement close to Platform. Action by: Project	A	IV	M	IV	M	IV	M	IV	M
	- Flexible Riser corrosion			C	IV	NT	IV	NT	IV	NT	IV	NT	R02) To implement NDT (Ultrasound test) by applying ROV inspection. Action by: Operation/Maintenance	A	IV	M	IV	M	IV	M	IV	M
	- Rupture caused by drop of Object			D	IV	NT	IV	NT	IV	NT	IV	NT	R03) To define Top movement part procedure and monitoring. Action by: Maintenance	A	IV	M	IV	M	IV	M	IV	M

FIGURE 6.13

Flexible riser HAZID example.

Therefore additional risk assessment such as FMEA and also reliability analysis will support the decision to prevent filter failure.

Some specialists try to use the risk matrix in HAZOP to assess risk and prioritize recommendation. This is not effective best practice because usually in HAZOP a catastrophic accident will not occur because process control has been established by the process engineer in addition to a layer of protection.

In this way, most process deviation risks will be classified as moderate and in this situation it is not necessary to implement additional actions to mitigate the risk.

It is best practice to carry out SIL analysis regarding all layers of protection to classify correctly the SIF.

Generally, a catastrophic accident is detected in PHA and a risk matrix is used to assess risk to identify which accident scenario must be assessed by consequence and effect analysis to calculate individual and societal risk.

When PHA is unavailable an alternative is to carry out a HAZID analysis, which means hazard identification, as shown in Fig. 6.13, which demonstrates a flexible riser HAZID analysis. The concept is the same as PHA but one difference is that all systems, subsystems, and node files used in HAZOP are also used in HAZID analysis. Finally, it is possible to compare HAZOP and HAZID recommendations and it will be clear which is best to deal with the catastrophic event on the plant. HAZID can be carried out by another group at same time that HAZOP is being carried out, but the best approach is to carry out HAZID before HAZOP usually by same specialist.

In general terms, we can say that the drawbacks of HAZOP are:

- As a qualitative analysis the process hazard can be underestimated and a recommendation or mitigating action may not be implemented.
- In some cases too many recommendations cannot be implemented because of cost and it is not clear how much impact on process risk this will have.
- It does not explain in detail the equipment failures and therefore it does not define specific action for the equipment.
- It does not give priority to terms of recommendation implementation.

HAZOP advantages are:

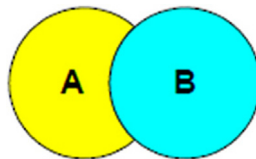
- It is a very well defined risk analysis tool and covers all processes, systems, and subsystems in P&D draw.
- It is possible to assess the impact of one process deviation in other subsystems.

## 6.5 FAULT TREE ANALYSIS (FTA)

FTA has been used since 1961, and the first application was conducted to assess a missile control system. FTA is a quantitative risk analysis method that defines event combinations that trigger top events (Ericson, 1999). In FTA the first step is to define top events and then the main event (intermediary and basic) and logic gates that are necessary to calculate the top event probability. Thus top events are usually accidents or equipment failures, and from top event down to basic events the combination of events is depicted. To calculate the top event probability based on intermediary and basic event combinations, Boolean logic is needed, which is basically for two events:

$$P(A) \cup P(B) = P(A) + P(B) - (P(A) \times P(B))$$

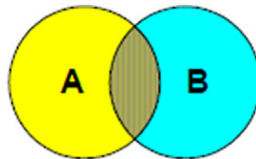
This is represented by the whole area in the following figure:



Or:


$$P(A) \times P(B) \text{ } \frac{1}{4} P(A)P(B)$$


This is represented by the interception area in the following figure:





The fault tree can include more than two event combinations, and it is advisable whenever it is possible to calculate two by two, that is, a probability result of two event combinations and a further


combination of the result with another event, and so on. Such event combinations are represented by logic gates that basically are:


 (top event)


 (logic gate “OR”)


 (logic gate “AND”)

 (standby event)

 ( $k/n$  event)

 (basic event)

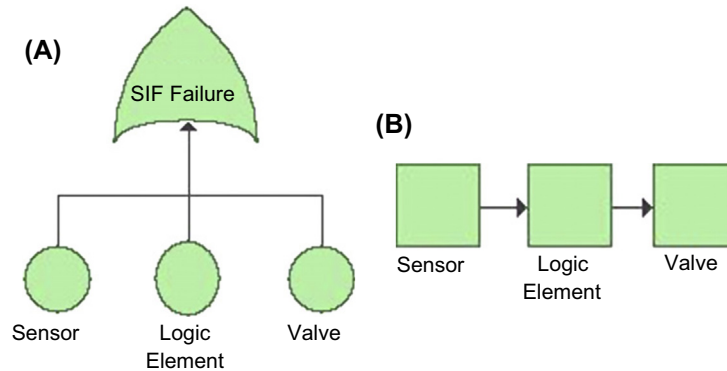
 (exclusive OR gate). This gate is triggered when one of the events happens.

 (priority AND gate). This gate is triggered if all the events happen in a defined sequence.

The FTA represented for independent events is called static FTA. There are other logic gates that represent dependence among events and can also be represented in FTA. In this case, we have dynamic FTA. Such logic gates are basically conditional and spare, but we can also have standby and load sharing. Conditional events are able to represent one event occurrence that is related to other event triggers. Standby and load-sharing logic were discussed in Chapter 4. With the standby case, the standby replaces the failed one. In the load-sharing case, when one event or component fails, the others have their degradation process accelerated. Spare gates represent a condition in which a failed component will be replaced with another one. All the logic events that give a dynamic configuration (condition and spare) to dynamic FTA are also represented in reliability block diagram (RBD) and have been used by commercial software for the last decade. In my experience, such events are rare and do not impact FTA and RBD significantly in the oil and gas industry models in most cases. The other point is that such an event can also be represented by one basic event at a superior level and in this way is represented for a simple static FTA or RBD. In real life it is very difficult to find historical data to describe the dependence among events. The remarkable point in FTA and other risk models is that representation is dependent on time. This means that event probabilities change over a long time and, in terms of risk, this is the most important point to be discussed and will be focused on here.

### 6.5.1 TIME-INDEPENDENT FTA

Time-independent FTA is used when the probabilities of basic events are constant over time. No matter what the probability characteristic is, the fault tree is created from the top event to the basic event for event combinations. For top event analysis, FTA is simpler than RBD in terms of representation, but both actually give the same result for opposite logic. A simple example of FTA and RBD is represented



**FIGURE 6.14**  
Fault tree RBD.

by a simple SIF that includes an initiating element (sensor), logic element, and final element (valve), as shown in Fig. 6.14A. Fig. 6.14B represents the SIF RBD, the inverse logic of FTA, and shows similar results. To calculate the probability of SIF failure based on FTA and RBD we have, respectively:

1. The probability of SIF failure in the fault tree diagram is:

$$P(\text{Sensor}) = 0.1$$

$$P(\text{Logic Element}) = 0.1$$

$$P(\text{Valve}) = 0.1$$

$$P(\text{SIF Failure}) = P(\text{Sensor}) \cup P(\text{Logic Element}) \cup P(\text{Valve})$$

$$\begin{aligned} R1 &= P(\text{Sensor}) \cup P(\text{Logic Element}) = (P(\text{Sensor}) + P(\text{Logic Element})) - (P(\text{Sensor}) \\ &\quad \times P(\text{Logic Element})) \end{aligned}$$

$$= (0.1 + 0.1) - (0.1 \times 0.1) = 0.2 - 0.01 = 0.19$$

$$\begin{aligned} R1 \cup P(\text{Valve}) &= (R1 + P(\text{Valve})) - (R1 \times P(\text{Valve})) = (0.19 + 0.1) - (0.19 \times 0.1) \\ &= 0.29 - 0.019 = 0.271 \end{aligned}$$

2. The probability of SIF failure on RBD is:

$$P(\text{SIF Failure}) = 1 - \text{Reliability}$$

$$\text{Reliability} = (1 - P(\text{Sensor})) \times (1 - P(\text{Logic Element})) \times (1 - P(\text{Valve}))$$

$$\text{Reliability} = (1 - 0.1) \times (1 - 0.1) \times (1 - 0.1) = 0.729$$

$$P(\text{SIF Failure}) = 1 - 0.729 = 0.271$$

The SIF example is simple in terms of FTA configuration, but in some cases fault trees are more complex to model and calculate. In the SIF example, other logic gates such as  $k/n$  (a parallel condition where  $k$  means number of components required and  $n$  means the number of total components in parallel) and standby can also be used, as shown in Fig. 6.15A and B, respectively.

To calculate the probability of SIF failure based on FTA and RBD we have, respectively:

The probability of SIF failure if:

$$P(\text{sensor 1}) = 0.1$$

$$P(\text{sensor 2}) = 0.1$$

$$P(\text{sensor 3}) = 0.1$$

$$P(\text{logic element}) = 0.1$$

$$P(\text{control valve}) = 0.1$$

$$P(\text{manual bypass valve}) = 0.1$$

$$\text{Thus } P(\text{SIF failure}) = P(\text{VT } (2/3)) \cup P(\text{logic element}) \cup P(\text{SB})$$

$$P(\text{VT}(2/3)) = 1 - R(\text{VT}(2/3))$$

Thus as the probability of events is the same we apply the following equation:

$$R_S(k, n, R) = \sum_{r=k}^n \binom{n}{r} R^r (1 - R)^{n-r}$$

where  $k$  = number of parallel blocks required;  $n$  = number of parallel blocks; and  $R$  = reliability.

$$R = \sum_{r=2}^3 \binom{3}{r} (0.9^r) (1 - 0.9)^{3-r} = \binom{3}{2} (0.9^2) (1 - 0.9)^{3-2} + \binom{3}{3} (0.9^3) (1 - 0.9)^{3-3}$$

$$= (3 \times 0.81 \times 0.1) + (1 \times 0.729 \times 1) = 0.243 + 0.729 = 0.972$$

$$P(\text{VT}(2/3)) = 1 - R(\text{VT}(2/3)) = 1 - 0.972 = 0.028$$

$$P(\text{SB}) = 1 - R(\text{SB})$$

$$R(\text{SB}) = R(\text{control Valve}) + ((1 - R(\text{control Valve})) \times R(\text{Manual Bypass valve}))$$

$$= (0.9) + ((0.1) \times (0.9)) = 0.99$$

$$P(\text{SB}) = 1 - 0.99 = 0.01$$

$$\text{Res1} = P(\text{VT}(2/3)) \cup P(\text{logic Element})$$

$$= P(\text{VT}(2/3)) + P(\text{logic Element}) - (P(\text{VT}(2/3)) \times P(\text{logic Element}))$$

$$= 0.028 + 0.1 - (0.028 \times 0.1) = 0.128 - 0.0028 = 0.1252$$

$$P(\text{SIF failure}) = P(\text{VT}(2/3)) \cup P(\text{logic Element}) \cup P(\text{SB}) = \text{Res1} \cup P(\text{SB})$$

$$= \text{Res1} + P(\text{SB}) - (\text{Res1} \times P(\text{SB})) = 0.1252 + 0.01 - (0.1252 \times 0.01)$$

$$= 0.1352 - 0.001252 = 0.133958 = 13.4\%$$



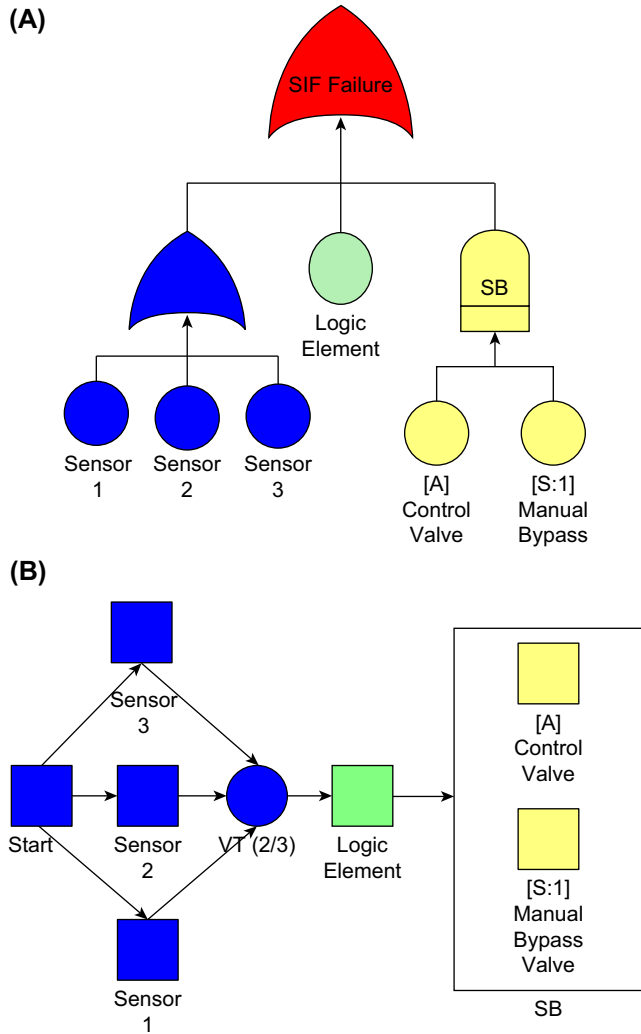


FIGURE 6.15

Fault tree RBD: (A)  $k/n$  and (B) standby configuration.

The probability of SIF failure is:

$$R(\text{Sensor1}) = 1 - P(\text{Sensor1}) = 1 - 0.1 = 0.9$$

$$R(\text{Sensor2}) = 1 - P(\text{Sensor2}) = 1 - 0.1 = 0.9$$

$$R(\text{Sensor3}) = 1 - P(\text{Sensor3}) = 1 - 0.1 = 0.9$$

$$R(\text{Logic Element}) = 1 - P(\text{Logic Element}) = 1 - 0.1 = 0.9$$

$$R(\text{Control Valve}) = 1 - P(\text{Control Valve}) = 1 - 0.1 = 0.9$$

$$R(\text{Manual Bypass Valve}) = 1 - P(\text{Manual Bypass Valve}) = 1 - 0.1 = 0.9$$

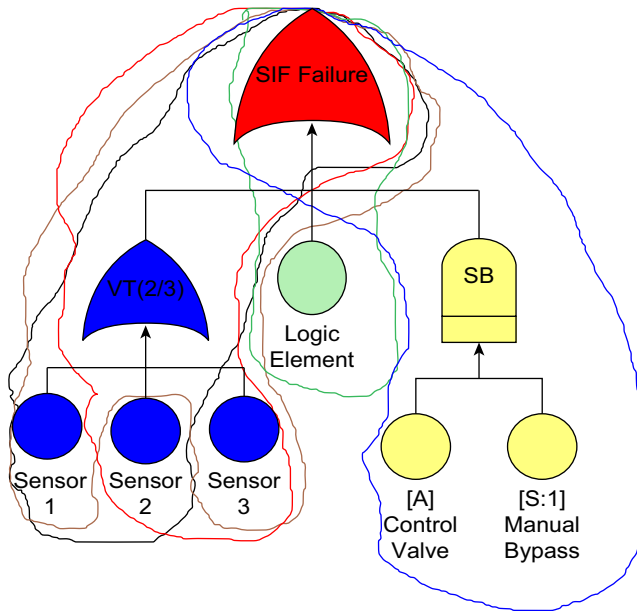


FIGURE 6.16

Cut set in fault tree.

$$\begin{aligned} \text{Thus } P(\text{SIF failure}) &= 1 - (R(\text{VT}(2/3)) \times R(\text{Logic Element}) \times R(\text{SB})) \\ &= 1 - (0.972 \times 0.9 \times 0.99) = 1 - 0.866052 = 0.133948 = 13.4\% \end{aligned}$$

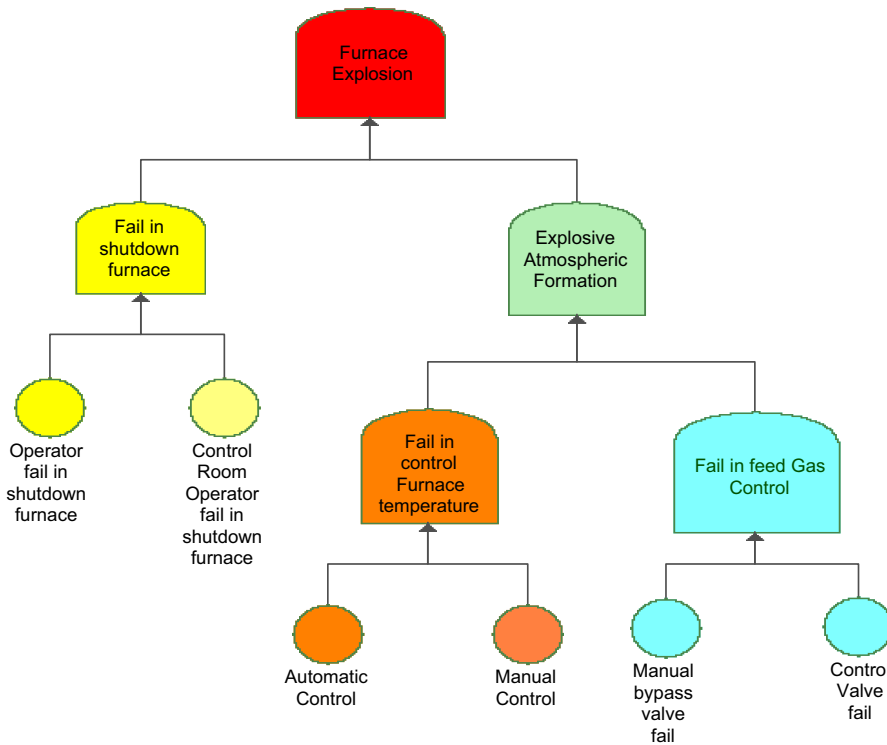
The important feature of FTA in addition to calculating top event probability is to identify events or combinations of events that trigger top events, which are called cut set events. The cut set events are important for assessing an incident and knowing how close the incident is in the top event based on the current event. In the SIF failure fault tree in Fig. 6.15A, there are five cut sets, as shown in Fig. 6.16.

- Failure of sensors 1 and 2 ( $kn = 2/3$ );
- Failure of sensors 1 and 3 ( $kn = 2/3$ );
- Failure of sensors 2 and 3 ( $kn = 2/3$ );
- Failure of logic element;
- Failure of control valve and manual bypass valve.

### 6.5.2 TIME-DEPENDENT FTA

Time-dependent FTA uses the CDF as the basic event value, and depending on the time used for the top event, it will have different values for probability, which will get higher over time. This means that in most cases the higher the risk, the higher the chance of the accident or failure occurring. Fig. 6.17 shows an example of top event analysis called “furnace explosion” conducted by time-dependent FTA.

For a furnace explosion to occur, it is necessary to have an explosive atmosphere formation and for the furnace to be in operation. In addition, in an explosive atmosphere formation it is necessary to have failure in the control furnace temperature and failure in the feed gas control. If failure to shut down the



**FIGURE 6.17**

Furnace explosion FTA.

furnace happens, it is because of the operator on the ground as well as the operator in the control room. Failure in control furnace temperature requires both manual and automatic control failures. And finally, feed gas control requires failures in both valves, that is, the manual bypass valve and control valve.

For the failure rate for each basic event, the probability of furnace explosion varies over time. Thus it is possible to calculate, for example, the probability of having a furnace explosion until 1.5 years or until 3 years. Thus using the exponential CDF for all events and considering:

- E0 = Operator failure in furnace shutdown
- E1 = Control room operator failure in furnace shutdown
- E2 = Automatic control
- E3 = Manual control
- E4 = Manual valve failure
- E5 = Control valve failure

The CDFs for each event are:

$$P(E0)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.0001t}$$

$$P(E1)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00002t}$$

$$P(E2)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.0001t}$$

$$P(E3)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.0005t}$$

$$P(E4)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00001t}$$

$$P(E5)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00005t}$$

In time 1.5 years (13,140 h) the probability values are:

$$P(E0)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.0001t} = 1 - e^{-0.0001(13140)} = 0.7312$$

$$P(E1)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00002t} = 1 - e^{-0.00002(13140)} = 0.2311$$

$$P(E2)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.0001t} = 1 - e^{-0.0001(13140)} = 0.7312$$

$$P(E3)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.0005t} = 1 - e^{-0.0005(13140)} = 0.9985$$

$$P(E4)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00001t} = 1 - e^{-0.00001(13140)} = 0.1231$$

$$P(E5)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00005t} = 1 - e^{-0.00005(13140)} = 0.4815$$

Thus to calculate the top event in FTA we have:

$$\begin{aligned} \mathbf{P(\text{Fail in Shutdown Furnace})} &= P(E0) \cap P(E1) = (P(E0) \times P(E1)) = (0.7312 \times 0.2311) \\ &= 0.1689 \end{aligned}$$

$$\begin{aligned} \mathbf{P(\text{Fail in Control Furnace Temperature})} &= P(E2) \cap P(E3) = (P(E2) \times P(E3)) \\ &= (0.7312 \times 0.9985) = 0.7301 \end{aligned}$$

$$\begin{aligned} \mathbf{P(\text{Fail in Feed Gas control})} &= P(E4) \cap P(E5) = (P(E4) \times P(E5)) = (0.1231 \times 0.4815) \\ &= 0.05927 \end{aligned}$$

$$\begin{aligned} \mathbf{P(\text{Explosive Atmospheric Formation})} &= P(\text{Fail in Control Furnace Temperature}) \cap \\ &\quad \times P(\text{Fail in Feed Gas control}) = 0.7301 \times 0.05927 \\ &= 0.04327 \end{aligned}$$

$$\begin{aligned} \mathbf{P(\text{Furnace Explosion})} &= P(\text{Fail in Shutdown Furnace}) \cap P(\text{Explosive Atmospheric Formation}) \\ &= P(\text{Fail in Shutdown Furnace}) \times P(\text{Explosive Atmospheric Formation}) \\ &= 0.1689 \times 0.04327 = 0.0073. \end{aligned}$$

Thus the probability of having an explosion in the furnace until 1.5 years is 0.73%. If time changes, the top event probability also changes, increasing the chance of occurrence in the specific time.

Thus for 3 years in the furnace explosion FTA we have the following.

At time 3 years (26,280 h) the probability values are:

$$P(E0)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.0001t} = 1 - e^{-0.0001(26280)} = 0.9972$$

$$P(E1)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00002t} = 1 - e^{-0.00002(26280)} = 0.4087$$

$$P(E2)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.0001t} = 1 - e^{-0.0001(26280)} = 0.9972$$

$$P(E3)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.0005t} = 1 - e^{-0.0005(26280)} = 0.9999$$

$$P(E4)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00001t} = 1 - e^{-0.00001(26280)} = 0.2311$$

$$P(E5)(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00005t} = 1 - e^{-0.00005(26280)} = 0.7312$$

Thus calculating gate resultant probability we have:

$$\begin{aligned} \mathbf{P(\text{Fail in Shutdown Furnace})} &= P(E0) \cap P(E1) = (P(E0) \times P(E1)) = (0.9972 \times 0.4087) \\ &= 0.4075 \end{aligned}$$

$$\begin{aligned} \mathbf{P(\text{Fail in Control Furnace Temperature})} &= P(E2) \cap P(E3) = (P(E2) \times P(E3)) \\ &= (0.9972 \times 0.9999) = 0.9971 \end{aligned}$$

$$\mathbf{P(\text{Fail in Feed Gas control})} = P(E4) \cap P(E5) = (P(E4) \times P(E5)) = (0.2311 \times 0.7312) = 0.1689$$

$$\begin{aligned} P(\text{Explosive Atmospheric Formation}) &= P(\text{Fail in Control Furnace Temperature}) \cap \\ &P(\text{Fail in Feed Gas control}) = 0.9971 \times 0.1689 = 0.1684 \end{aligned}$$

$$\begin{aligned} \mathbf{P(\text{Furnace Explosion})} &= P(\text{Fail in Shutdown Furnace}) \cap P(\text{Explosive Atmospheric Formation}) \\ &= P(\text{Fail in Shutdown Furnace}) \times P(\text{Explosive Atmospheric Formation}) \\ &= 0.4075 \times 0.1684 = 0.068 \end{aligned}$$

Thus the probability of having an explosion on the furnace until 3 years is 6.8%, which is higher than 1.5 years.

### 6.5.3 FTA AS QUALITATIVE RISK ANALYSIS SUPPORT

FTA can be used to assess combinations of events from qualitative risk analysis, such as PHA, PRA, and HAZOP, to better predict the probability of occurrence to verify risk classification and assess the real effect of recommendations to mitigate risk. For example, Fig. 6.18 shows a partial platform PRA related to load operation. The highest risk is for personal damage from the consequences of an explosive atmosphere caused by gas leaks such as explosion, flash fire, fireball, or even toxic gas release. In PRA, the probability of occurrence is assessed qualitatively for types of causes, and consequences are also assessed qualitatively for consequence category classification (Fig. 6.18). Actually, in qualitative risk analysis, such as PRA, combinations of failures that may happen in real life are not usually considered.

PRELIMINARY RISK ANALYSIS (PRA)														
UN: Platform P-90					SYSTEM: 1- LOAD					DATA: 26/07/2009				
SUBSYSTEM: 1.1 - Load			DESCRIPTION: From well until SDV of production manifold						Draw: DE-XXXX.XX-XXX-001 REV0 05/06/2009					
Hazard	Causes	Consequences	Detection / Safeguards	Freq.	Personal		Instal.		Env		Social		Recommendation / Remarks	AH
					S	R	S	R	S	R	S	R		
Huge Gas and Oil spill	- Pipeline or connections ruptures - PIG operation failure.	- Puddle formation - Atmospheric explosive formation - Oil spill on sea - Health damage	- Visual - Pressure sensor - Gas detectors - Others detectors	C	IV	NT	III	M	II	M	II	M	R01) Follow procedure to PIC operation. Action: Operation Team	1
	- Submarine connections rupture - Equipment falling down on rise - Riser rupture caused by ship accident. - Riser rupture due to material fatigue	- Atmospheric explosive formation - Oil spill on sea - Health damage	- Visual - Pressure sensor	B	III	M	III	M	IV	M	IV	M	R02) Follow procedure to load Platform. Action: Operation Team. R03) Riser will have special protection to minimize fatigue	2

FIGURE 6.18

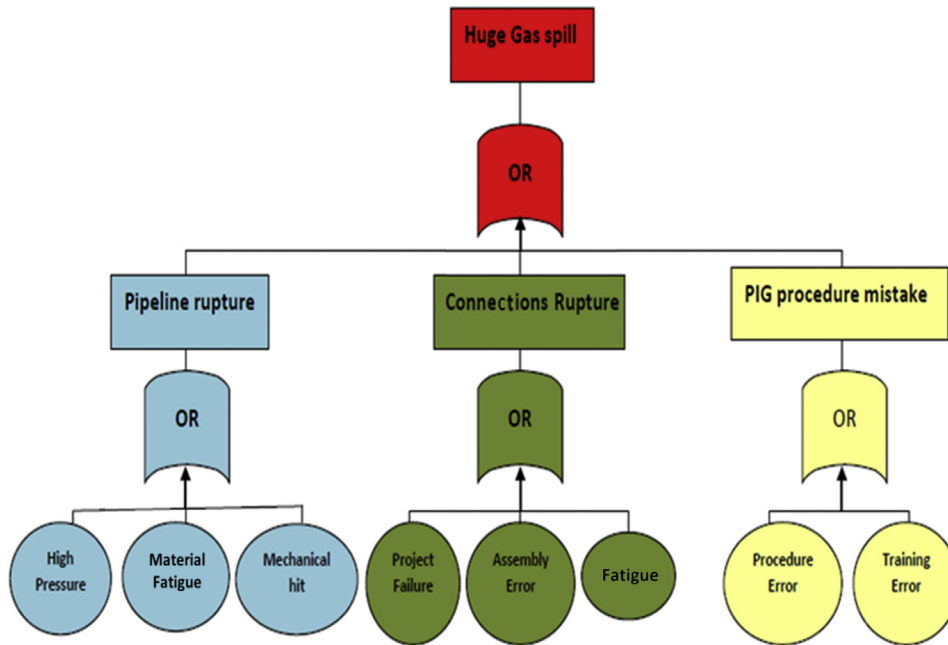
Preliminary risk analysis (platform). *M*, moderate; *NT*, not tolerable.

Thus the huge gas spill in the first line of the PRA can be represented by an FTA, as shown in Fig. 6.19, and additional root causes can be assessed to better understand the incident occurrence. The other advantage of using fault trees is to find the combination of events that triggers the top events.

Observing Fig. 6.19 it is clear that any one of the eight basic events can trigger the huge gas spill, which is not clear from the PRA. In addition, if following PRA recommendations, there is nothing to prevent assembly error, project failure, and fatigue in pipelines and connections. Furthermore, if the probability of the basic event is put on the fault tree, it is possible to have a more realistic probability of failure for a huge gas spill.

The other qualitative risk analysis often used in the oil and gas industry is HAZOP. Similar to PRA, HAZOP does not consider failure combinations as causes of process deviations. These failure combinations can be assessed by FTA to better measure the risk of accidents in process deviations. Fig. 6.20 shows a HAZOP table that assesses high pressure in a vessel (O-06). In HAZOP analysis, each of the causes can trigger high pressure in vessel O-06. Despite such apparent vulnerability there is a group of safeguards that prevents high pressure. Some of them do not bring the process to safe conditions, such as alarms, but alert the operator to unsafe process conditions. In these cases, if there is human error and safe actions are not followed, the process will remain in an unsafe condition. As a qualitative risk analysis, there is no clear idea about the probability of occurrence in HAZOP, and therefore it is essential to perform FTA if it is necessary to know such process deviation probabilities.

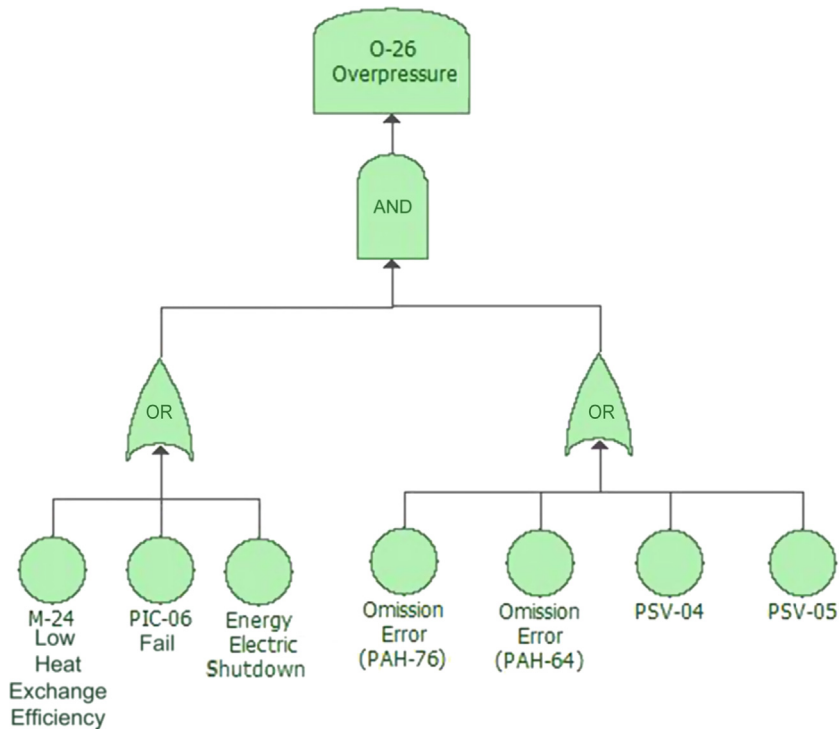
The HAZOP analysis can be represented by the fault tree in Fig. 6.21, and in this way it is possible to calculate the probability of vessel O-06 being overloaded. In addition, it is possible to input



**FIGURE 6.19**  
Fault tree (huge platform gas spill).

<b>Company: Oil &amp; Gas</b>		<b>HAZOP (Hazard and Operability)</b>		
<i>Unit: U-57</i>		<i>System: Vessel O-06</i>		<i>Date: 26-03-2011</i>
<i>Subsystem: Vessel O-06</i> <i>Node 1: From inlet to outlet O-06 vessel</i>			<i>Draw N°:</i> <i>DE-XXXX.XX-XXXX Rev. A de</i> <i>21/02/2011</i>	
<b>Deviation</b>	<b>Causes</b>	<b>Effects</b>	<b>Safeguards</b>	<b>Recommendations</b>
<b>High Pressure</b>	<ul style="list-style-type: none"> <li>- Failure in heat exchanger M-24</li> <li>- Failure in PIC-06</li> <li>- Electrical Energy shutdown</li> </ul>	<ul style="list-style-type: none"> <li>- Operational discontrol</li> <li>- O-06 overloaded</li> <li>- High pressure in all systems</li> </ul>	<ul style="list-style-type: none"> <li>- PAH-76</li> <li>- PAH-64</li> <li>- PSV-04</li> <li>- PSV-05</li> </ul>	R01) Create a new SIF to high pressure Action: Project Instrumentation Engineer

**FIGURE 6.20**  
HAZOP (high pressure in vessel).

**FIGURE 6.21**

Fault tree (high pressure in vessel).

safeguards recommended by HAZOP into the fault tree and calculate the new probability of O-26 suffering an overload by overpressure.

#### 6.5.4 FTA AS A ROOT CAUSE ANALYSIS TOOL

In many cases of equipment failure the root cause or a group of root causes that triggered the equipment failure is not clear. In these cases, it is necessary to consider a combination of different factors, technological or human. Sometimes laboratory tests are needed to prove the root causes of failure, but the first step is to discuss the probable failure causes and possible combinations of root causes that triggered the failure with a multidisciplinary group. Thus when there is only one consequence, FTA is an appropriate tool for qualitatively assessing probable combinations of the root causes of failure, or even an event in the case of an accident. Fig. 6.22 gives a pump failure example, with probable failure causes and basic events that represent the root causes of the pump failure.

The basic event can be assessed until the group finds the real root causes. A similar methodology can be applied to assess incidents, but in some cases incidents include more than one accident consequence scenario, and in this case bow tie analysis is more appropriate, as will be shown in Section 6.9.



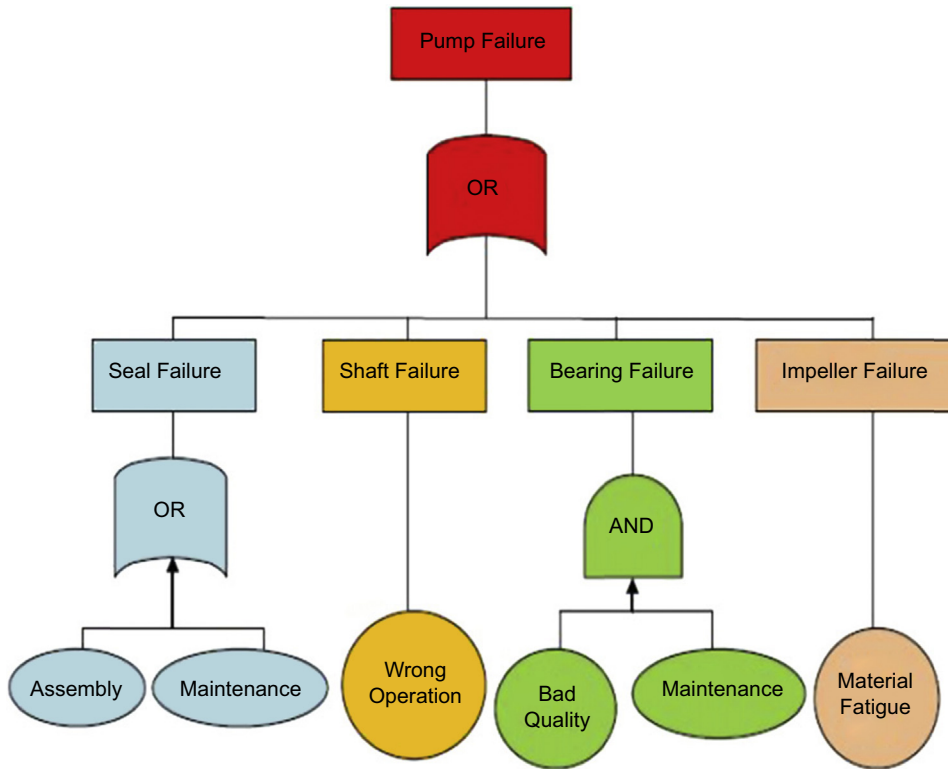


FIGURE 6.22

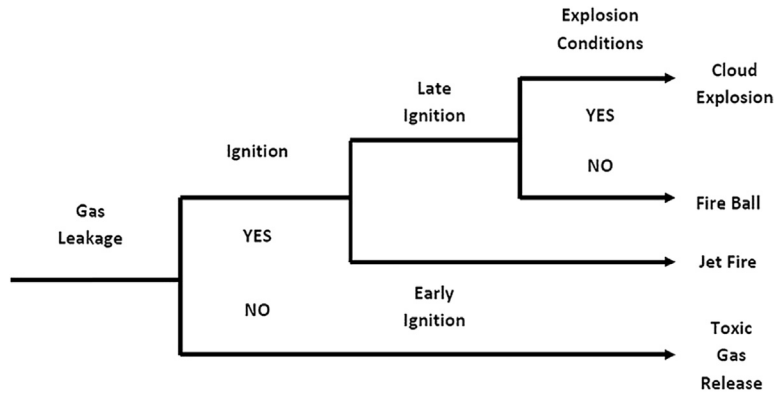
Fault tree (root cause analysis).

FTA is a powerful tool for assessing event combinations and defining the cut sets that lead to accidents. Many accidents in the oil and gas industry worldwide have occurred because of event combinations that were not considered in risk analysis during the project phase or even in systems in the operational phase.

## 6.6 EVENT TREE ANALYSIS (ETA)

ETA assesses the possible results based on sequences of success and failure events triggered by initiating events, which are usually incidents. The ETA logic is different to FTA. In an event tree, the model is created from left to right, beginning with the initiating event and continuing to the sequence of events. A good example is a toxic gas leak that can result in a toxic cloud release, jet fire, fireball, or cloud explosion, as shown in Fig. 6.23.

At the beginning of an incident, the gas is at a low concentration and is not toxic, but after a few minutes it becomes more concentrated, toxic, and the four types of accident are possible. In terms of risk analysis, it is necessary to define the probability or frequency of occurrence of each event. It is common



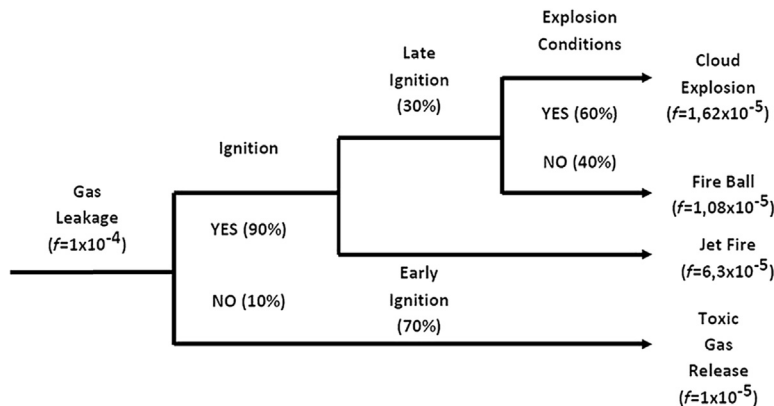
**FIGURE 6.23**

Event tree (gas leak).

to consider the frequency of the initiating event (gas leak) and multiply the probability of each of the other events (ignition, early ignition, late ignition, and explosion conditions). The result of each accident is frequency, which is multiplied per number of deaths, resulting in risk. The expected number of deaths is calculated using another methodology, called consequences and effects analysis, not covered here. In addition to fault trees, there will also be static event trees and dynamic tree events, depending on if the probability value is constant or is represented by CDFs with different values over time.

### 6.6.1 TIME-INDEPENDENT ETA

Time-independent ETA considers values of probabilities and frequency constants over time, which are considered in most types of risk analysis, despite not representing the equipment degradation over time. Using the gas release example, the static event tree for the probability of events (ignition, early ignition, late ignition, and explosion conditions) and frequency of initiating event (gas leak) is shown in Fig. 6.24.



**FIGURE 6.24**

Static event tree (gas leak).

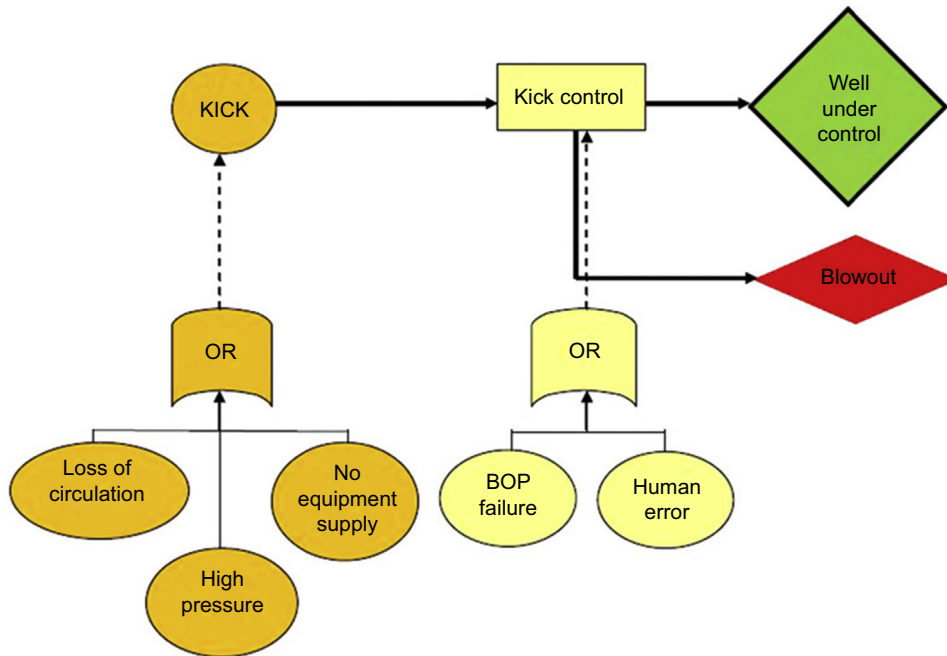


FIGURE 6.25

Hybrid risk analysis (ETA and FTA).

The frequency of accident results is calculated by multiplying the initiating event frequency by each branch event probability. Thus the frequencies of each of the consequence scenarios are:

$$f(\text{Toxic Gas release}) = f(\text{gas leakage}) \times P(\text{no ignition}) = (1 \times 10^{-4}) \times (0.1) = 1 \times 10^{-5}$$

$$\begin{aligned} f(\text{Jet Fire}) &= f(\text{gas leakage}) \times P(\text{ignition}) \times P(\text{Early ignition}) = (1 \times 10^{-4}) \times (0.9) \times (0.7) \\ &= 6.3 \times 10^{-5} \end{aligned}$$

$$\begin{aligned} f(\text{Fire Ball}) &= f(\text{gas leakage}) \times P(\text{ignition}) \times P(\text{late ignition}) \times P(\text{No explosion conditions}) \\ &= (1 \times 10^{-4}) \times (0.9) \times (0.3) \times (0.4) = 1.08 \times 10^{-5} \end{aligned}$$

$$\begin{aligned} f(\text{Cloud Explosion}) &= f(\text{gas leakage}) \times P(\text{ignition}) \times P(\text{late ignition}) \times P(\text{explosion conditions}) \\ &= (1 \times 10^{-4}) \times (0.9) \times (0.3) \times (0.6) = 1.62 \times 10^{-5} \end{aligned}$$

Despite being represented by frequency, the initiating event (gas leak) can also be represented by probability values, and in this case the final result of each accident scenario will be a probability value.

The initiating event can be triggered by a combination of simple events, a complex event combination, or a single event. Thus when the initiating event is represented by probability, it is possible to model a fault tree to define the initiating event probability. An example where such an initiating event

must be calculated for a fault tree is a blowout accident in a well drilling project risk analysis. Fig. 6.25 shows the hybrid analysis of the fault tree to calculate the initiating event of the ETA.

Kick occurrence depends on loss of circulation or high pressure or no equipment supply in the well. This event combination is represented by:

$$\begin{aligned} P(\text{kick}) &= P(\text{lost of circulation}) \cup P(\text{high pressure}) \cup P(\text{no equipment supply}) \\ &= P(\text{lost of circulation}) + P(\text{high pressure}) + P(\text{no equipment supply}) \\ &\quad - (P(\text{lost of circulation}) \times P(\text{high pressure})) - (P(\text{lost of circulation}) \\ &\quad \times P(\text{no equipment supply})) - (P(\text{high pressure}) \times P(\text{no equipment supply})) \end{aligned}$$

In case of human error or the Blowout preventer (BOP) failure kick is out of control, the probability of such event is represented by:

$$\begin{aligned} P(\text{kick control}) &= P(\text{BOP failure}) \cup P(\text{human error}) \\ &= P(\text{BOP failure}) + P(\text{human error}) - ((P(\text{BOP failure}) \times P(\text{human error}))) \end{aligned}$$

The probability of the well being under control is calculated by the event tree and is represented by:

$$P(\text{well under control}) = P(\text{kick}) \times P(\text{kick control})$$

The complementary event is the probability of having a blowout:

$$P(\text{blowout}) = P(\text{kick}) \times (1 - P(\text{kick control}))$$

### 6.6.2 TIME-DEPENDENT ETA

Time-dependent ETA considers events' CDF parameters having probability varying over time, and this approach is more realistic because it represents the increasing chance of equipment failure over time. Using the gas release example, the dynamic event tree regards constant probabilities of some events (ignition, early ignition, late ignition, and explosion conditions) and an exponential CDF for the initiating event (gas leak). Consequently, there will be different probabilities of accidents over time. The gas leak may be caused by corrosion in the pipeline and such incidents can be represented by a Gumbel PDF ( $\mu = 25$ ,  $\sigma = 2$ ) because this event mostly occurs at the end of the life cycle. Fig. 6.25 shows the pipeline corrosion failure rate over time.

Based on Fig. 6.26, there are two values for the failure rate. In 10 years the failure rate is  $2 \times 10^{-5}$  and in 25 years it is 0.45. Applying these values in the event tree of Fig. 6.25 we have two cases:

Case 1 (10 years)—Frequency of gas leakage =  $\lambda(10) = 1 \times 10^{-5}$

$$f(\text{Toxic Gas release}) = f(\text{gas leakage}) \times P(\text{no ignition}) = (2 \times 10^{-5}) \times (0.1) = 2 \times 10^{-6}$$

$$\begin{aligned} f(\text{Jet Fire}) &= f(\text{gas leakage}) \times P(\text{ignition}) \times P(\text{Early ignition}) = (2 \times 10^{-5}) \times (0.9) \times (0.7) \\ &= 1.27 \times 10^{-5} \end{aligned}$$

$$\begin{aligned} f(\text{Fire Ball}) &= f(\text{gas leakage}) \times P(\text{ignition}) \times P(\text{late ignition}) \times P(\text{No explosion conditions}) \\ &= (2 \times 10^{-5}) \times (0.9) \times (0.3) \times (0.4) = 2.1 \times 10^{-6} \end{aligned}$$

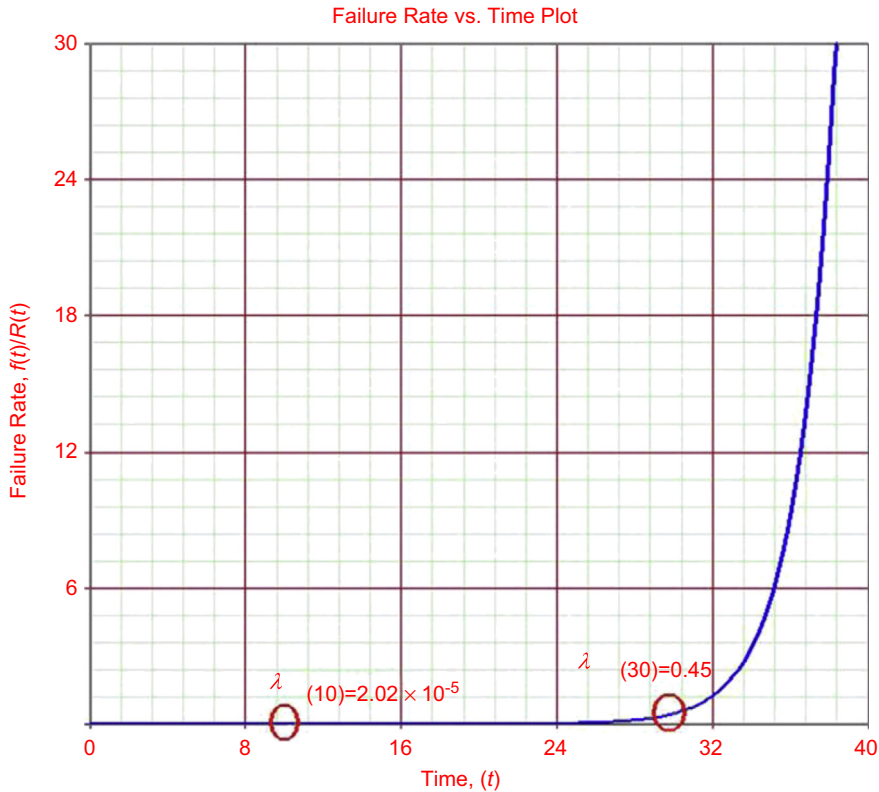


FIGURE 6.26

Initiating event failure rate function (corrosion on pipeline).

$$\begin{aligned} f(\text{Cloud Explosion}) &= f(\text{gas leakage}) \times P(\text{ignition}) \times P(\text{late ignition}) \times P(\text{explosion conditions}) \\ &= (2 \times 10^{-5}) \times (0.9) \times (0.3) \times (0.6) = 3.2 \times 10^{-6} \end{aligned}$$

Case 2 (30 years)—Frequency of gas leakage =  $\lambda(30) = 0.45$

$$f(\text{Toxic Gas release}) = f(\text{gas leakage}) \times P(\text{no ignition}) = (0.45) \times (0.1) = 0.045$$

$$f(\text{Jet Fire}) = f(\text{gas leakage}) \times P(\text{ignition}) \times P(\text{Early ignition}) = (0.45) \times (0.9) \times (0.7) = 0.28$$

$$\begin{aligned} f(\text{Fire Ball}) &= f(\text{gas leakage}) \times P(\text{ignition}) \times P(\text{late ignition}) \times P(\text{No explosion conditions}) \\ &= (0.45) \times (0.9) \times (0.3) \times (0.4) = 0.048 \end{aligned}$$

$$\begin{aligned} f(\text{Cloud Explosion}) &= f(\text{gas leakage}) \times P(\text{ignition}) \times P(\text{late ignition}) \times P(\text{explosion conditions}) \\ &= (0.45) \times (0.9) \times (0.3) \times (0.6) = 0.0729 \end{aligned}$$

In 10 years the accident frequency is remote based on the risk matrix frequency classification in Fig. 6.1, and the risk of accidents is moderate, but in 30 years it is not. Thus observing the matrix in

		FREQUENCY CATAGORY					
		A (Extremely remote)	B (Remote)	C (Little frequency)	D (Frequent)	E (Very frequent)	F (Extremely frequent)
		At least 1 between 1000 and 100,000 years	At least 1 between 50 and 1000 years	At least 1 between 30 and 50 years	At least 1 between 5 and 30 years	At least 1 in 5 years	At least 1 in 1 year
SEVERITY CATEGORY	IV	M	NT	NT	NT	NT	NT
	III	Jet Fire	M	NT	Jet Fire	NT	NT
	II	T	T	M	M	M	M
	I	T	T	T	M	M	M

FIGURE 6.27

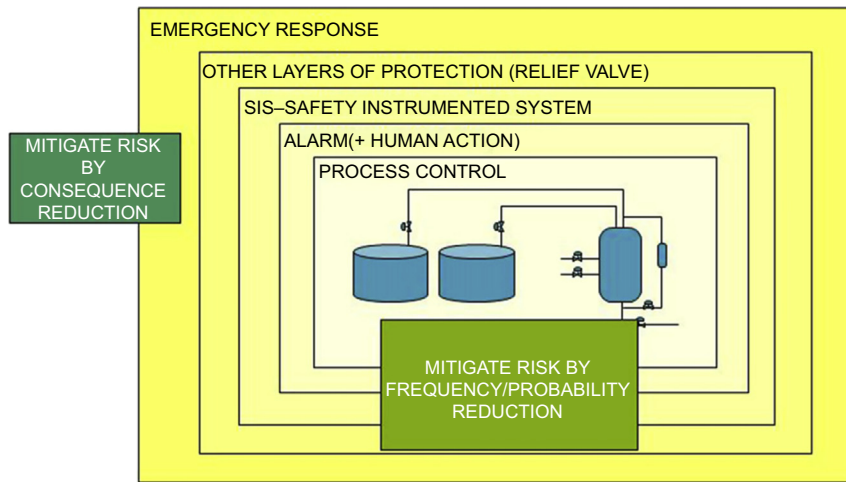
Frequency of jet fire from 10 years to 30 years in the risk matrix.

Fig. 6.27, the frequency of jet fire, the highest accident scenario frequency, moves from very remote to frequent, and after 30 years the risk of such accidents is not tolerable. In terms of risk assessment, some action must be done to keep the risk at an acceptable level, at the very least.

The main advantage of the time-dependent event tree approach is to realize the risk level over time, which helps to define preventive actions to keep risk at an acceptable level. This shows the real importance of reliability engineering in risk management, that is, providing information about failure rate and probability of equipment failures and event occurrence. Reliable equipment has a direct relation to safety because unsafe failures take longer to occur and consequently the workplace is safer. For this reason, it is important to have a quantitative approach to life cycle analysis of unsafe failures to support risk decisions. Thus to have an acceptable level of risk, it is important to define the equipment’s reliability requirement.

Even though a piece of equipment has high reliability over a long period of time without an unsafe failure, there is always a chance of failure because of equipment degradation or from human error in operation and maintenance. Despite the risk of human error in maintenance, reestablishing part of equipment reliability over time is very important. Consequently, inspections and maintenance must be conducted properly. But performing inspections and maintenance is not enough; it is also necessary to decide when to perform them to anticipate the unsafe failure and maintain acceptable risk. The correct time for inspections and maintenance is based on reliability engineering tools, as discussed in Chapter 3.

In addition, to prevent accidents, safety process devices are used to act when unsafe conditions are detected. This is the concept of layers of protection, the expected reliable action to keep a process in safe conditions and act properly between incidents and accident occurrence. The next section describes LOPA methodology.



**FIGURE 6.28**

Layers of protection.

## 6.7 LAYERS OF PROTECTION ANALYSIS (LOPA)

LOPA methodology is an extension of ETA, which considers initiating events and layers of protection to prevent the initiating event from turning into an accident. The layers of protection are layers that are able to prevent an accident from occurring or minimize the effects of an accident. In most cases, layers of protection are devices, but human action can also be considered a layer of protection. The main objective of layers of protection is to keep risk at a tolerable level. To keep risk at an acceptable level more than one layer of protection must be used to achieve the risk target and reduce vulnerability. From a preventive point of view, whenever it is possible it is better to use layers of protection that mitigate risk by reducing the chance of an accident occurring. To achieve a tolerable risk level, it is also possible to have layers that mitigate risk by reducing accident consequence. Many accidents in the gas and oil industry have been underestimated and layers of protection were not in place to minimize the effects. A recent accident occurred in the Gulf of Mexico on April 20, 2010, when a blowout preventer was not able to control the blowout, which had serious consequences to employee health and the environment.

Examples of preventive layers of protections include rupture disks, relief valves, SIFs, and even operator actions. There are some layers of protection that minimize accident effects such as the deck area, which contains oil spills around the tanks, walls around the operational area to contain toxic product release, and even windows that support pressure waves in an explosion. Fig. 6.28 shows the layers of protection concept to prevent accidents or reduce accident consequences.

Like the previous quantitative risk analysis, LOPA can also use constant probability for layers of protection or CDFs for layers of protection and initiating an event having different values of probability over time. In the first case, constant failure rate and probability values are found by static LOPA. In the second case, CDFs are found using dynamic LOPA, as will be shown in the next sections.

### 6.7.1 INDEPENDENT TIME LOPA

Independent time LOPA uses constant values for initiating an event rate and probabilities of layers of protection. The initiating event can also have a constant probability value, and in this case the final result will be an accident probability. If the initiating event has a constant failure rate value and the layers of protection have constant failure probability values, the final result will be the accident constant rate (Fig. 6.29). This means multiplying the initial event constant failure rate by the constant probabilities of each layer of protection.

An example of LOPA is an explosive atmosphere formation incident in a furnace, as shown in Fig. 6.30. In this case, high flow of gas is sent to the furnace, and explosive atmosphere formation must be controlled to avoid an explosion in the furnace. In this way, there are three layers of protection: SDCD (distributed digital control system), SIF, and operator action. When all layers of protection fail, the furnace will explode. Thus the values of the initiating event frequency and layers of protection probability are:

- Explosive atmospheric formation ( $f = 1 \times 10^{-1}$ );
- SDCD failure ( $P = 1 \times 10^{-1}$ );
- SIF failure ( $P = 1 \times 10^{-2}$ );
- Operator action ( $P = 1 \times 10^{-1}$ ).

Based on the values of the initiating event rate and the layers of protection failure probability, we calculate the frequency of furnace explosion:

$$f(\text{Furnace explosion}) = f(\text{explosive atmospheric}) \times P(\text{SDCD}) \times P(\text{SIF}) \times P(\text{human error})$$

$$f(\text{Furnace explosion}) = (1 \times 10^{-1}) \times (1 \times 10^{-1}) \times (1 \times 10^{-2}) \times (1 \times 10^{-1}) = 1 \times 10^{-5}$$

Looking at the risk matrix in Fig. 6.28, the risk level is similar to the jet fire case and is moderate (severity category III and frequency category A), so in this way the system is well projected at an acceptable risk level. The other way to conduct time-independent LOPA is using a report where each aspect of LOPA is described, and the furnace explosion failure is calculated as shown in Fig. 6.31. The advantage of this file is it is an easier layer of protection analysis and such a configuration can be easily understood by other professionals.

### 6.7.2 TIME-DEPENDENT LOPA

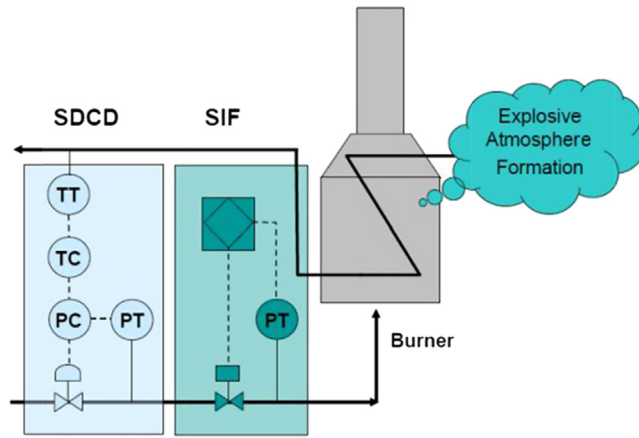
Time-dependent LOPA uses the frequency rate function for the initiating event at constant rate function. Even though layers of protection have constant probability, we have dynamic layers of protection because the incident rate frequency varies over time. In some cases there is no failure data available to model the layers of protection CDFs, and in some cases such probability is considered constant, as with human action, for example. An example of time-dependent LOPA is high pressure in a vessel. In this case, the worse consequence is vessel disruption and high material release with consequences that were described in the ETA example in Section 6.3.1 (toxic gas release, cloud explosion, fire ball). Before the accident occurs there are layers of protection that help prevent the



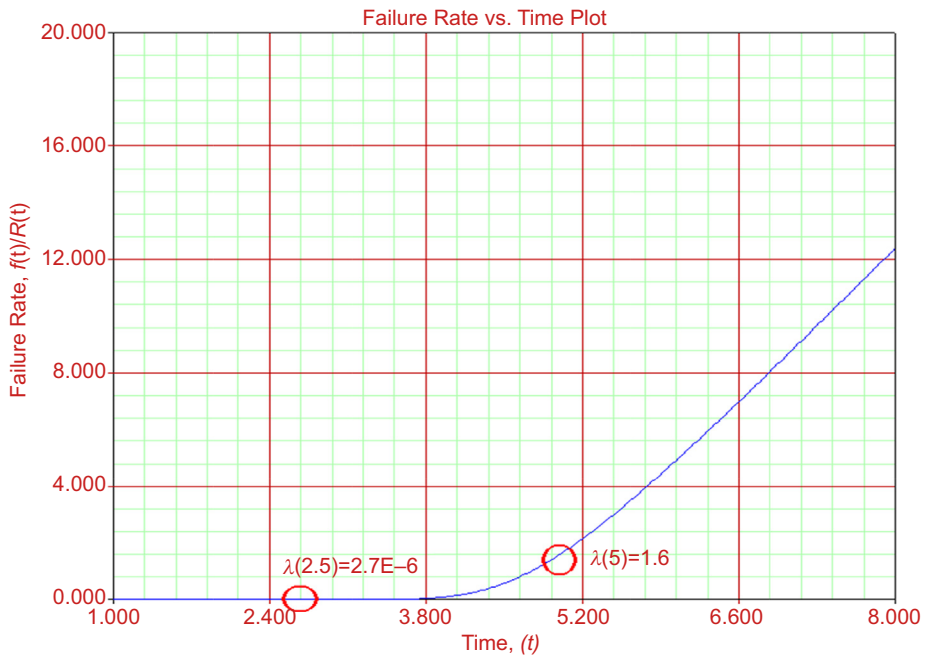
Scenario Number	Equipment	Scenario Description	
1	Furnace	Explosion of Furnace	
Data	Description	Probability	Frequency
xx/xx/xxxx			
Consequence Description	Furnace operator damage health and equipment loss		
Tolerable criterion	Tolerable risk level	M	NT
		4	5
Initiate event	Explosive atmospheric formation		
Conditions	Ignition probability	100%	
	Health damage	100%	
	Fatality probability	100%	
	Other		
Initiate event	Explosive atmospheric formation		$1 \times 10^{-2}$
Layer of protection	SDCD	$1 \times 10^{-1}$	
	Human action	$1 \times 10^{-1}$	
	SIF	$1 \times 10^{-2}$	
Total	Frequency of accident	$1 \times 10^{-5}$	
Tolerable risk	Yes	No	
	x		
other layer of protection required	No		
Tolerable risk	Yes	No	
Recommendation	No		

FIGURE 6.29

Layers of protection calculation.



**FIGURE 6.30**  
Furnace's explosive atmosphere formation.



**FIGURE 6.31**  
Furnace LOPA.

incident from turning into an accident. These layers of protection include SIF, relief valves, and operator actions. Thus the values of the initiating event and the layers of protection are:

- High pressure on vessel (PDF normal:  $\mu = 5$ ;  $\sigma = 0.5$ );
- Relief valve (PDF Gumbel:  $\mu = 10$ ;  $\sigma = 2$ );
- SIF failure ( $P = 1 \times 10^{-2}$ );
- Operator action ( $P = 1 \times 10^{-1}$ ).

The initiating event, high pressure on the vessel, is represented by a normal PDF because every 4.5 years there is preventive maintenance and after that the process is unstable. Thus dynamic LOPA is performed for two possibilities:

Case 1—2.5 years

$$f(\text{Vessel disrupt}) = f(\text{high pressure}) \times P(\text{Relief Valve}) \times P(\text{SIF}) \times P(\text{Operator human error})$$

$$f(\text{Vessel disrupt}) = (2.78 \times 10^{-6}) \times (0.0105) \times (1 \times 10^{-2}) \times (1 \times 10^{-1}) = 2.91 \times 10^{-11}$$

Case 2—5 years

$$f(\text{Vessel disrupt}) = f(\text{high pressure}) \times P(\text{Relief Valve}) \times P(\text{SIF}) \times P(\text{Operator human error})$$

$$f(\text{Vessel disrupt}) = (1.6) \times (0.046) \times (1 \times 10^{-2}) \times (1 \times 10^{-1}) = 0.73 \times 10^{-4}$$

The values of cumulative probability of failure are shown in Fig. 6.32. In the failure rate case, if you take a look at the risk matrix in Fig. 6.27, despite critical consequences, the risk is moderate (severity category IV and frequency category A) even though frequency increases from 2.5 to 5 years. In the case of maintenance in one of the layers of protection or even failure in 5 years the main question is: Is the risk tolerable without one of layers of protection? To answer this question it is necessary to calculate the frequency of gas release without one of the layers of protection. Unfortunately, in many cases LOPA is performed using qualitative risk analysis as the PRA and some actions are done without a tolerable risk level. Section 6.7.3 discusses this issue.

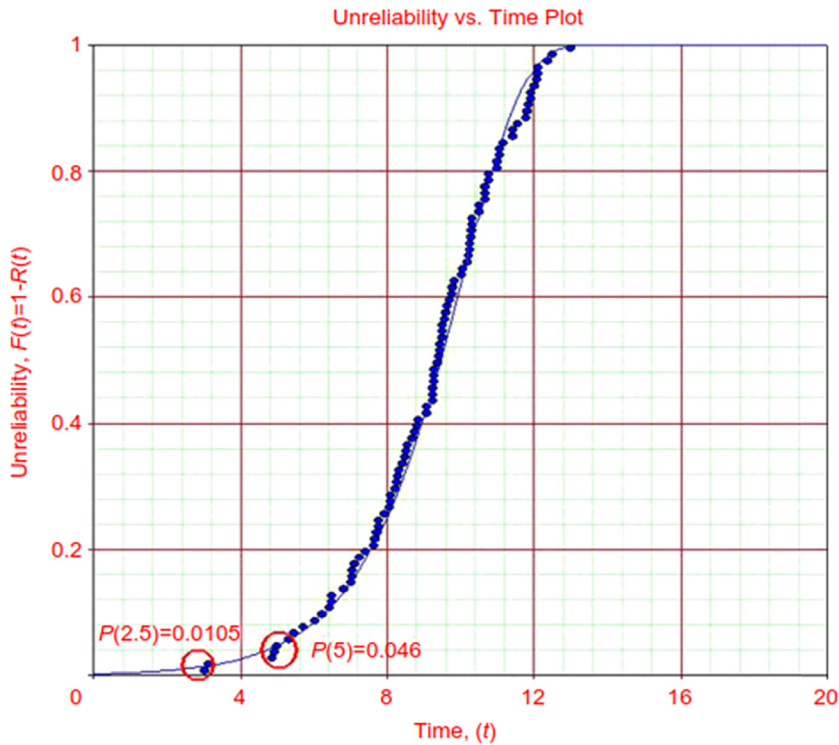
### 6.7.3 TIME-DEPENDENT LOPA AS QUALITATIVE RISK ANALYSIS SUPPORT

Time-dependent LOPA can be a powerful tool for supporting decisions in qualitative risk analysis to predict the real probability of failure. The values of cumulative probability of failure are shown in Fig. 6.32. In the failure rate case, if you take a look at the risk matrix in Fig. 6.27, despite critical consequence, risk is moderate (severity category IV and frequency category A), even though frequency increases from 2.5 to 5 years. Fig. 6.33 uses PRA of the gas release occurring when there is no SIF in the fifth year. The group decided to test the SIF of the vessel every 5 years and believe this is an acceptable risk.

Applying LOPA and regarding 5 years of life cycle, it is necessary to conduct SIF testing, and when the SIF is out of operation the frequency of gas release will be:

$$f(\text{gas release}) = f(\text{high pressure}) \times P(\text{Relief Valve}) \times P(\text{Operator human error})$$

$$f(\text{gas release}) = (1.6) \times (0.046) \times (1 \times 10^{-1}) = 0.73 \times 10^{-2}$$



**FIGURE 6.32**  
High pressure CDF.

Company: Oil & Gas		PRA (Preliminary Risk Analysis)		
Unit: U-22	System: Vessel V-076		Date: 06-01-2009	
Equipment: Vessel O-06			Draw N°: DE-XXXX.XX-XXXX Rev. A de 21/11/2008	
Hazard	Causes	Effects	Safeguards	Recommendations
High pressure on vessels	<ul style="list-style-type: none"> <li>- Loss of process control</li> <li>- Failure in control valve before vessel</li> <li>- Overflow</li> </ul>	<ul style="list-style-type: none"> <li>- Vessel collapse</li> <li>- Toxic gas release</li> <li>- Cloud explosion</li> <li>- Fire ball</li> </ul>	<ul style="list-style-type: none"> <li>- PSV</li> <li>- SIF-03</li> </ul>	R01) Inspect and test SIF in 5 years Action: Instrumentation Engineer

**FIGURE 6.33**  
Relief valve PDF.

Looking at the risk matrix in Fig. 6.27, the risk is not tolerable (severity category IV and frequency category B). This means the SIF must be tested before 5 years. If the SIF is tested in the fourth year the frequency of gas release will be:

$$f(\text{gas release}) = (0.11) \times (0.025) \times (1 \times 10^{-1}) = 2.75 \times 10^{-4}$$

In this case, looking at the risk matrix the risk is moderate (severity category IV and frequency category A). Thus it is better to test the SIF in the fourth year to keep risk at a tolerable level. In most cases such decisions do not take into account quantitative tools and reliability models. This analysis is most often conducted using a qualitative risk analysis such as preliminary risk analysis.

---

## 6.8 SAFETY INTEGRITY LEVEL ANALYSIS (SIL ANALYSIS)

SIL analysis began in the United States in the mechanical industry as a process management tool, being required to verify the integrity of an emergency control system. In 1996, the Instrumentation System and Automation Society on EUA published the ANSI/ISA-84.01 standard, and in Europe a similar standard, IEC 61508, was published to cover several industries.

SIL analysis is a semiquantitative methodology for defining if it is necessary to implement SIF as a layer of protection in a process and to guarantee that SIF has reliability enough, as a layer of protection, to help the system to achieve an acceptable risk level. Each SIL number is related to one SIF, and as discussed in Section 6.5.1, the SIF includes the initiating element (sensor), the logic element, and the final element (valve). SIF can include more than one of these elements, as shown in Fig. 6.15A. In the highest level of a safety system, there are SISs (safety instrumented systems) that are comprised for more than one SIF, as shown in Fig. 6.34.

Depending on the SIS configuration a single logic element can be used for more than one SIF, as shown in Fig. 6.34, which is a particular characteristic of each SIS project configuration that takes into account safety and cost.

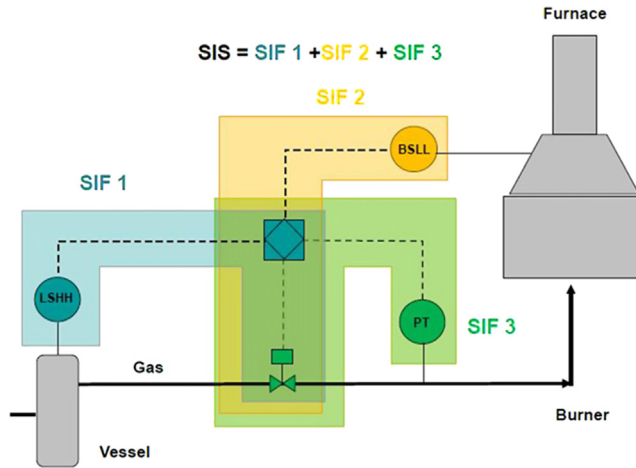
SIF is associated with hazards, and performing a qualitative hazard analysis, such as PHA, HAZOP, and FMEA, it is possible to identify hazards in a process. Despite good approaches for identifying hazards in a process when the main objective is to decide if it is necessary to implement SIF, to achieve a tolerable risk level other SIL methodologies are more appropriate. There are four SIL analysis methodologies:

- Hazard matrix
- Risk graph
- Frequency target
- Individual or societal risk

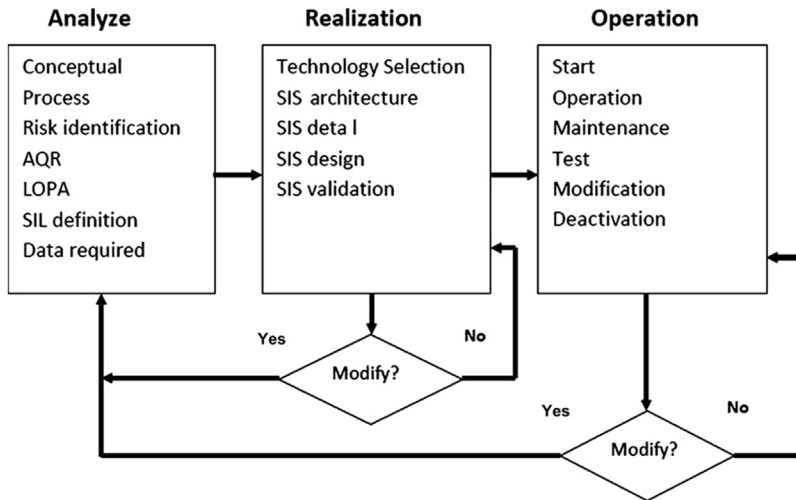
Using these methodologies it is possible to select the SIL for an SIF in process, but that is only part of an SIF project. The SIL definition is part of the analyze phase of the safety life cycle, as shown in Fig. 6.35.

Thus, after the SIL definition, it is necessary to define the SIS technology, which includes all SIFs, then begin the operation phases where there will be maintenance and testing during the process plant life cycle. The SIL reference values for SIF vary from 1 to 4, as shown in Table 6.4.

Depending on the SIL definition value when applying SIL methodologies (hazard matrix, risk graph, individual risk, societal risk) the risk must achieve an acceptable level. The risk criteria



**FIGURE 6.34**  
Safety instrumented system (SIS).



**FIGURE 6.35**  
Safety life cycle.

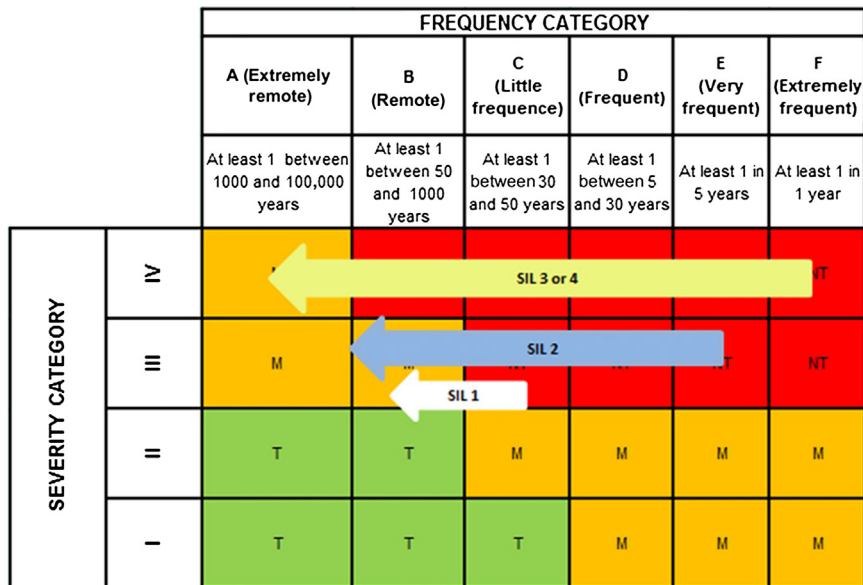
Source: Marzal, E.M., Scharpf, E., 2002. Safety Integration Level Selection: Systematics Methods Including Layer of Protection Analysis. The Instrumentation, Systems and Automation Society.

Safety Class	PFD	SIL
I	$10^1$	0
II	$10^1$	0
III	$10^2 < 10^1$	1
IV	$10^3 < 10^2$	2
V	$10^4 < 10^3$	3
VI	$10^4 < 10^3$	3
X	$10^5 < 10^4$	4

PFD, probability of failure on demand.  
 Source: Marzal, E.M., Scharpf, E., 2002. Safety Integration Level Selection: Systematics Methods Including Layer of Protection Analysis. The Instrumentation, Systems and Automation Society.

considered can be qualitative based on the risk matrix or quantitative based on individual or societal risk criteria depending on the SIL methodology adopted to assess the risk. The hazard matrix and risk graph are related to the qualitative risk approach and to the risk matrix, as shown in Fig. 6.36. Thus, depending on the risk level in the matrix, SIL 1, 2, 3, or 4 is required to keep the risk at an acceptable level in the matrix.

However, individual risk and societal risk are related to individual and societal risk concepts. Individual risk is a chance of death that an individual or group of people has when they are located in



**FIGURE 6.36**  
 The qualitative acceptable risk.

**FIGURE 6.37**

Acceptable individual risk (ISO—risk, vulnerable).

one vulnerable region and exposed to some hazard in the operational ground (industrial area) (Fig. 6.37). Individual risk is usually expressed in terms of the ISO—risk curve or ALARP region.

The ISO—risk curve is a graphical representation of the vulnerable area of individual risk. In many countries, there are different risk criteria. Thereby, different risk targets are defined as acceptable risk. Concerning individual risk for example, in case of  $1 \times 10^6$  deaths/year, the ISO risk contour cannot achieve the external region with presence of community. If the individual risk value is lower, it is acceptable that the ISO—risk contour achieves the community region. The SIL values verify that with SIF individual risk will reduce to an acceptable value, for example, reduce from  $1 \times 10^{-6}$  to  $1 \times 10^{-10}$  after SIF (SIL 3).

The ALARP region in individual risk is achieved when the SIL value of SIF is enough to mitigate risk from an unacceptable region to a tolerable region. Fig. 6.38 shows an example of a  $1 \times 10^{-4}$  risk that is mitigated to a tolerable region.

Societal risk is the chance of death that a group of people (community) outside the operational area have because of exposure to industrial hazard sources. Societal risk is usually represented by an F—N (frequency and number of deaths) curve that shows the expected number of fatalities at each frequency level. This curve is made up of all pairs of the expected number of deaths and frequency, a cumulative curve that uses all hazard scenarios from one or more than one specific hazard source (plants, tanks, vessels) the community is vulnerable to. In the F—N curve a tolerable region (ALARP) is defined, and whenever the curve is higher than the upper tolerable limit, mitigating actions are required. In this way it is possible to mitigate consequence or frequency. To mitigate consequence it is necessary to reduce the vulnerability area that accident scenarios create, and in doing so reduce the number of people exposed and consequently the expected number of deaths. The usual action to mitigate a consequence is to change the product or hazard source, change the location of the hazard source, or reduce the volume of product. To mitigate frequency it is necessary to reduce frequency values, and when SIF is implemented as a layer of protection it is possible to do so.



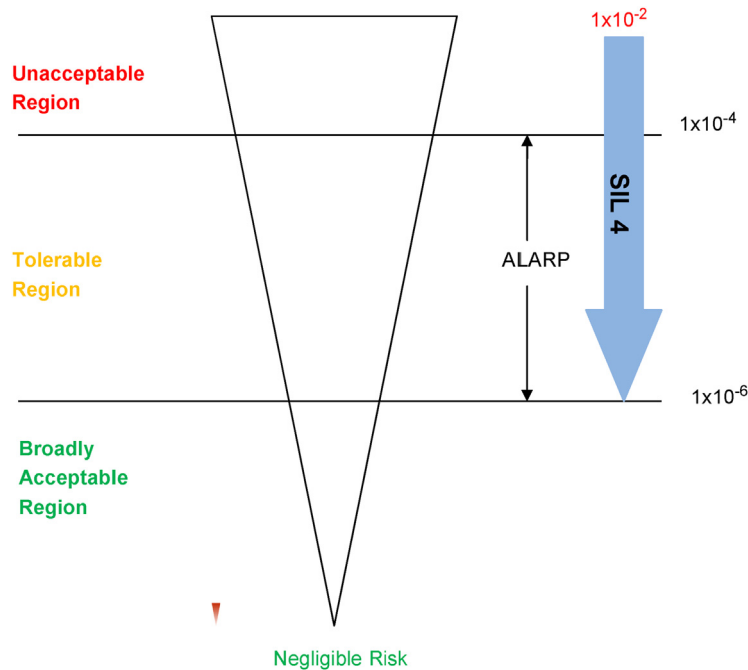


FIGURE 6.38

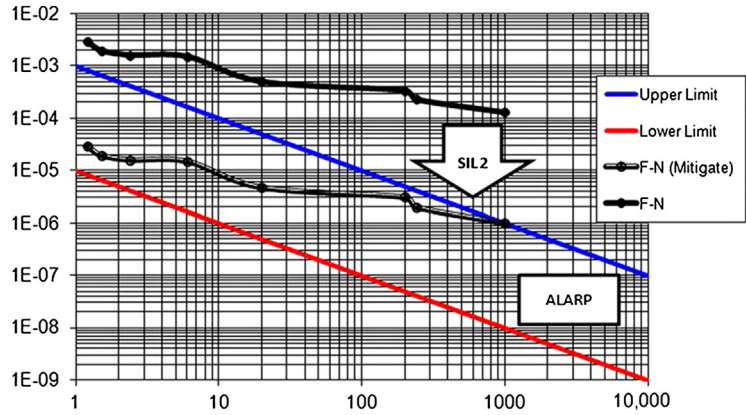
Acceptable individual risk (ALARP).

Fig. 6.39 shows the F–N curve mitigated when SIF (SIL 2) is implemented as a layer of protection. In this case, only one hazard source, such as a vessel, is being considered. The F–N curve is usually comprised of several hazard scenarios from different sources, and in this case, more than one SIF to mitigate the F–N curve to a tolerable region is necessary. As discussed in Section 6.4, each layer of protection has a probability of failure that reduces the frequency of the initiating event (incident) turning into an accident. Thus, by implementing SIF, the frequency is reduced because there is more than one probability value that must be multiplied by the frequency of the initiating event. The effect of SIF on the F–N curve is only in one point or in all of them depending on how SIF can mitigate risk related with the accident scenario.

The main question now is how to define the SIL (1, 2, 3, or 4) for each specific SIF, and the answer is through SIL selection methodologies, discussed in the following sections.

### 6.8.1 HAZARD MATRIX METHODOLOGY

A hazard matrix is the first qualitative SIL methodology that considers a qualitative risk matrix to select SIL for a specific SIF. Thus frequency and consequence are taken into account when the hazard is assessed. The combination of frequency of hazard and severity of consequence defines the SIL required for the SIF, that is, the number in the matrix, as shown in Fig. 6.40.



**FIGURE 6.39**  
Acceptable societal risk (F–N curve).

Probability	High	2	3b	3a
	Moderate	1	2	3b
	Low	Note C	1	3b
		Less	Serious	Extensive
		<b>Severity</b>		

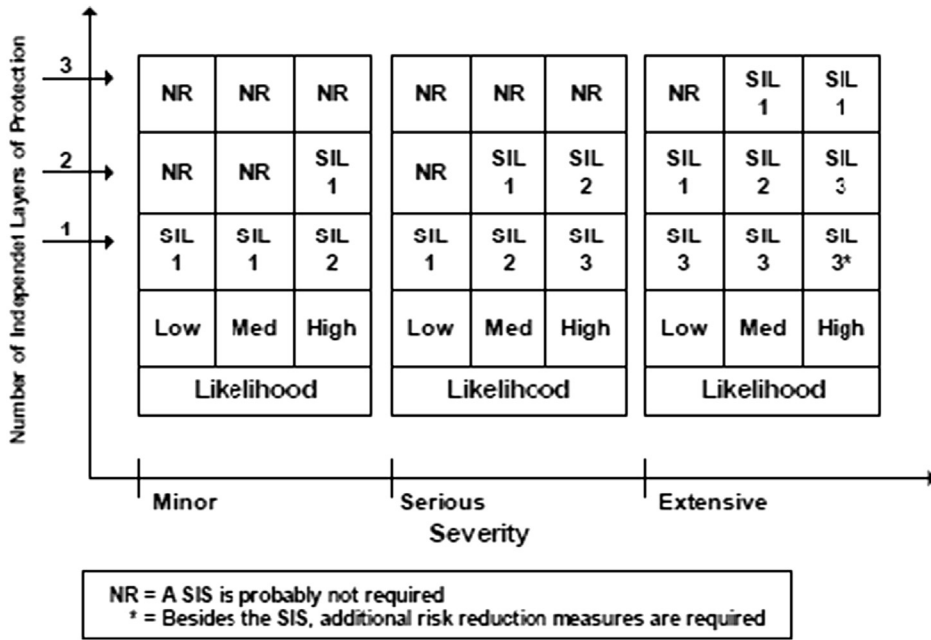
**FIGURE 6.40**  
Hazard matrix.

Some notes about hazard matrices:

In case of SIL 3, if SIF is not provided, a risk reduction is necessary to achieve tolerable risk level. Modifications are required.

In case of SIL 3, if SIF is not provided, a risk reduction is necessary to achieve tolerable risk level. This matrix does not select the SIL 4 condition.

When a hazard is assessed the layers of protection in place must be assessed to define the correct probability category. In the hazard matrix shown in Fig. 6.40 the layer of protection is not clear, and in this case the group of specialists who perform the SIL selection must take into account such layers of protection. On the other hand, there are some matrices that consider the SIL definition based on the number of layers of protection in place, as shown in Fig. 6.41. The risk matrix also has a category for probability and consequence and such criteria have qualitative definitions, as shown in Tables 6.5 and 6.6, respectively.



**FIGURE 6.41**  
 Hazard matrix with number of layers of protection.

An example of hazard matrix application can be considered to define if it is necessary to use an SIF to prevent, for example, an accident such as a toxic product leakage. This incident is expected to occur once every 1000 years, and if it happens 100 fatalities are expected. The vessel project engineer used one alarm to alert the operator and one SIF that is configured by a pressure sensor that sends a signal to a logic element that closes a valve to cut the vessel feed in case of high pressure. As shown in the consequence category in Table 6.5 the risk analysis group has classified the consequence as serious, and based on Table 6.6 they have classified the likelihood as moderate. Thus since there are two layers of protections, SIL 1 is selected, as shown in Fig. 6.42.

Table 6.5 Consequence Categories	
Severity Category	Description
Minor	Impact initially limited to local area of the event with potential for broader consequence if corrective action is taken
Serious	One that could cause any serious injury or fatality on-site or off-site, or property damage of \$1 million off-site or \$5 million on-site
Extensive	One that is more than five times worse than serious

Source: Marzal and Scharpf, 2002.

**Table 6.6 Frequency Categories**

Likelihood Category	Frequency (per year)	Description
Low	$<10^{-4}$	A failure or series of failures with a very low probability that is not expected to occur within the lifetime of the plant
Moderate	$10^{-2}-10^{-4}$	A failure or series of failures with a low probability that is not expected to occur within the lifetime of the plant
High	$>10^{-2}$	A failure can reasonably be expected within the lifetime of the plant

Source: Schwartz, 2002.

If a hazard matrix without the number of layers of protection was used as a reference, the SIL 2 would be selected, as shown in Fig. 6.43, even though using a hazard matrix regarding existing layers of protection the risk would be overestimated and a higher SIL classification can take place, as happens in many cases of qualitative risk analysis. While these methods are easy and can be applied quickly, caution is required, and whenever possible it is best to also use other SIL definition methodologies and compare results. However, this is a very good tool for an initiated specialist or even professionals who are not familiar with SIL methodologies and need to apply SIL analysis to make a decision.

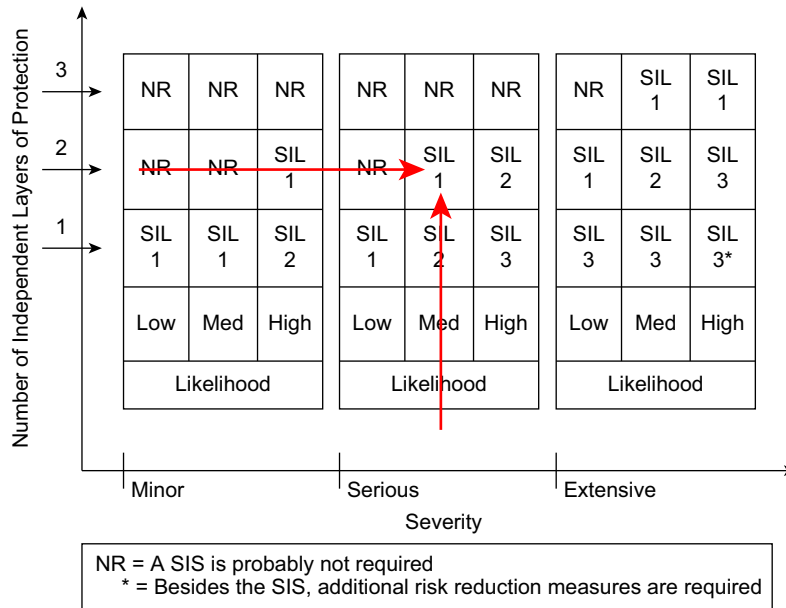


FIGURE 6.42

Hazard matrix with number of layers of protection (vessel example).

Probability	High	2	3b	3a
	Moderate	1	2	3b
	Low	Note C	1	3b
		Less	Serious	Extensive
		<b>Severity</b>		

FIGURE 6.43

Hazard matrix without number of layers of protection (vessel example).

## 6.8.2 RISK GRAPH METHODOLOGY

The risk graph methodology uses other criteria in addition to consequences and frequencies to select the SIL including:

- Consequence category
- Occupancy category
- Avoidance category
- Demand rate category

The consequence category uses the severity of the accident and is defined by the probable loss of life (PLL) number, with the following four classifications:

- Ca (minor injury)
- Cb ( $0.01 < PLL < 0.1$ )
- Cc ( $0.1 < PLL < 1$ )
- Cd ( $PLL > 1$ )

PLL is better defined by consequences and effects analysis, and even when qualitative analysis, such as PHA, is conducted, similar studies can be consulted to have a better idea of the PLL number.

The occupancy category uses the frequency that the vulnerable area of the hazard source is occupied by employees. Vulnerable area means if an accident happens, anyone in this area will be affected. The occupancy category has two classifications:

- Fa (rare to have exposure to the accident at the vulnerable area. The vulnerable area is occupied less than 10% of the time);
- Fb (frequent or permanent exposure to the accident at the vulnerable area. The vulnerable area is occupied more than 10% of the time);

The avoidance category uses the chance of the operator avoiding the accident, and there are two classifications:

- Pa (the facilities are provided with resources to avoid accidents, and they are independent, giving the operator time to escape from the vulnerable area. The operator will be alerted if the SIF has failed and will have enough time to take action to avoid an accident);
- Pb (if one of such conditions above is not satisfied).

The demand rate category uses the chance of the hazard event (incident) occurring, and there are three classifications:

- W1 (<0.03 times per year);
- W2 (0.3 < W2 < 0.03 times per year);
- W3 (3 < PLL < 0.3 times per year).

Thus the first step in the risk graph methodology is to define each category and then apply such values in the graph from left to right to select the SIL. Thus if, for example, we have Cc, Fa, Pb, and W3, the SIL selected is 3, as shown in Fig. 6.44.

An example similar to the hazard matrix example in Section 6.5.2 is an incident of a toxic product leak on a vessel, where the expected occurrence is once every 1000 years, and if it happens, 100 fatalities are expected. On the vessel, one alarm to alert the operator against high pressure was considered. In addition, there is one SIF that includes a pressure sensor that sends a signal to the logic element, which sends a command to the valve, which closes and cuts the vessel feed to avoid high pressure. Observing the consequence classification the risk analysis group classified the consequence

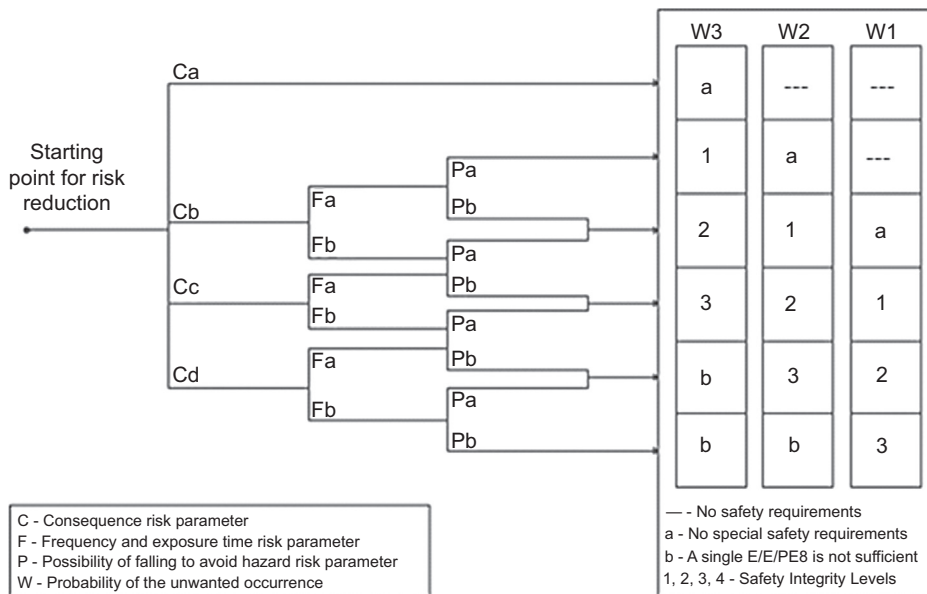


FIGURE 6.44

Risk graph methodology.

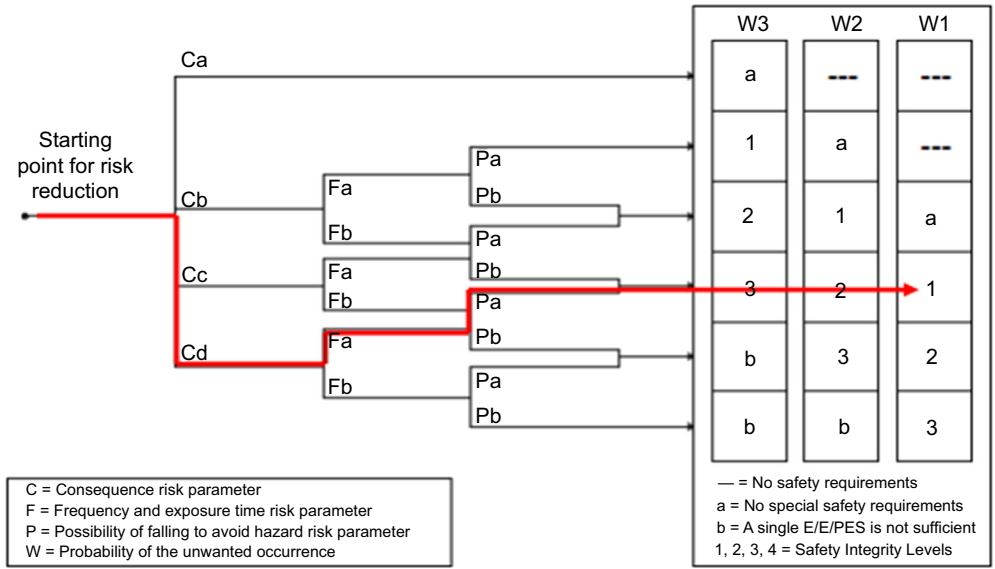


FIGURE 6.45

Risk graph methodology (toxic gas leak on vessel).

as Cd. The occupancy category was defined as Fa, the avoidance category was defined as Pa, and the demand rate category was defined as W1. Thus, based on risk graph methodology, the SIL 1 is selected, as shown in Fig. 6.45.

### 6.8.3 FREQUENCY TARGET METHODOLOGY

Frequency target methodology is based on risk reduction and can be described by:

$$RRF = \frac{F_{ac}}{F_t}$$

where RRF, risk reduction factor;  $F_{ac}$ , frequency of accident; and  $F_t$ , tolerable frequency.

So the RRF is based on accident frequency and tolerable frequency. Table 6.7 shows the RRF and SIL required and Table 6.8 defines the tolerable frequency, which depends on accident severity.

A similar example of hazard matrix and risk graph methodology is an incident of a toxic product leak on a vessel assessed by the risk analysis group during the project. This incident is expected to occur once every 1000 years, and if it does occur, 100 fatalities are expected. Based on Table 6.7, severity is considered serious and consequently the tolerable frequency is  $1 \times 10^{-4}$ , so the RRF will be:

$$RRF = \frac{1 \times 10^{-3}}{1 \times 10^{-4}} = 10$$

Thus, based on the RRF and using Table 6.7, SIL 1 is selected. In some cases, despite SIL selection defined by RRF, one level up from RRF is selected as a conservative approach. In the vessel analysis case it would be SIL 2.

**Table 6.7 Risk Reduction Factor**

SIL	Average PFD	Availability in %	RRF
1	10 <sup>2</sup> to <10 <sup>1</sup>	>90 to 99	>10 to 100
2	10 <sup>3</sup> to <10 <sup>2</sup>	>99 to 99.9	>100 to 1000
3	10 <sup>4</sup> to <10 <sup>3</sup>	>99.9 to 99.99	>1000 to 10,000
4	10 <sup>5</sup> to <10 <sup>4</sup>	>99.99 to 99.999	>10,000 to 100,000

**Table 6.8 Frequency Target**

Severity Rank	Impact	Frequency
Less	Low health disturbance and environmental impact. No process losses	1310 <sup>1.0</sup> × 10 <sup>-3</sup>
Serious	Equipment is damaged. Process shutdown. High environmental impact	1310 <sup>1.0</sup> × 10 <sup>-4</sup>
Extensive	High equipment damage. Long process shutdown and catastrophic health and environmental impact	1310 <sup>1.0</sup> × 10 <sup>-6</sup>

**6.8.4 INDIVIDUAL AND SOCIETAL RISK METHODOLOGY**

The individual risk methodology is similar to the frequency target, but requires the probable losses of life to calculate the tolerable frequency value. Thus the RRF is calculated as:

$$RRF = \frac{Fac}{Ft}$$

where RRF, risk reduction factor; Fac, frequency of accident; and Ft, tolerable frequency.

And:

$$Ft = Fc = PLL^a$$

where Fc, frequency criteria for individual or societal risk limit (frequency of deaths tolerable); PLL, probable loss of life; and a, risk aversion value (a > 0).

The risk aversion value is a weight defined by specialists to be input into the Ft equation when an accident or event is catastrophic.

Another example similar to the hazard matrix example is a risk graph and frequency target of an incident of a toxic product leak on a vessel assessed by the risk analysis group during the project. This incident is expected to occur every 1000 years, and the expected fatalities are 100. Based on individual risk criteria (Table 6.8), the individual risk is 1 × 10<sup>-4</sup>. The PLL is 100 deaths. The specialist team considered a = 1. Thus the first step is to calculate the tolerable frequency:

$$Ft = \frac{Fc}{PLL^a} = \frac{1 \times 10^{-4}}{100^1} = 1 \times 10^{-6}$$



The following step is to calculate the RRF:

$$\text{RRF} = \frac{\text{Fac}}{\text{Ft}} = \frac{1 \times 10^{-3}}{1 \times 10^{-6}} = 1 \times 10^3$$

Thus, based on Table 6.7, SIL 2 is selected for the SIF in this case.

An important remark about frequency criterion is that if societal risk is adopted to calculate Frequency tolerable value the societal risk related to one hundred deaths is 1E-5. Actually, in this case such deaths occur outside plant. In this case the Ft would be 1E-7 and consequently RRF would be and based on Table 6.7, SIL 3 is selected for SIF.

Another important note is that RRF is the inverse of the probability of failure on demand (PFD) as required for each SIL level, as shown in Table 6.7. If the table PFD is constant and if we assume we are considering the SIF PFD is constant over time, this is not correct because equipment ages and wears out over time. Thus, similar to the other quantitative risk analysis model, it is necessary to calculate the PFD over a long period of time based on historical failure data, as will be shown in the next section.

### 6.8.5 QUANTITATIVE APPROACH TO DEFINING PROBABILITY OF FAILURE ON DEMAND

As discussed with the other quantitative risk methodologies (FTA, ETA, and LOPA) the probability of failure of an event or a layer of protection varies over time, which means the probability of failure over time is not constant. The probability of failure for events and layers of protection such as SIF increase over time. In doing so, in SIF cases, as well as in other layers of protection, the most realistic approach is to define the CDF to predict the probability of failure on demand. Fig. 6.46 shows an example of an exponential CDF that represents the PFD of the SIF with a failure rate of  $1 \times 10^{-7}$ . Theoretically, the SIF will be an exponential CDF, but it is actually possible to use other types of CDFs depending on the historical data. When representing the PFD by CDF it is assumed that the equipment is degraded over time even when not operating. However, if equipment does not degrade when not operating, it is necessary to consider the usual failure on demands probability.

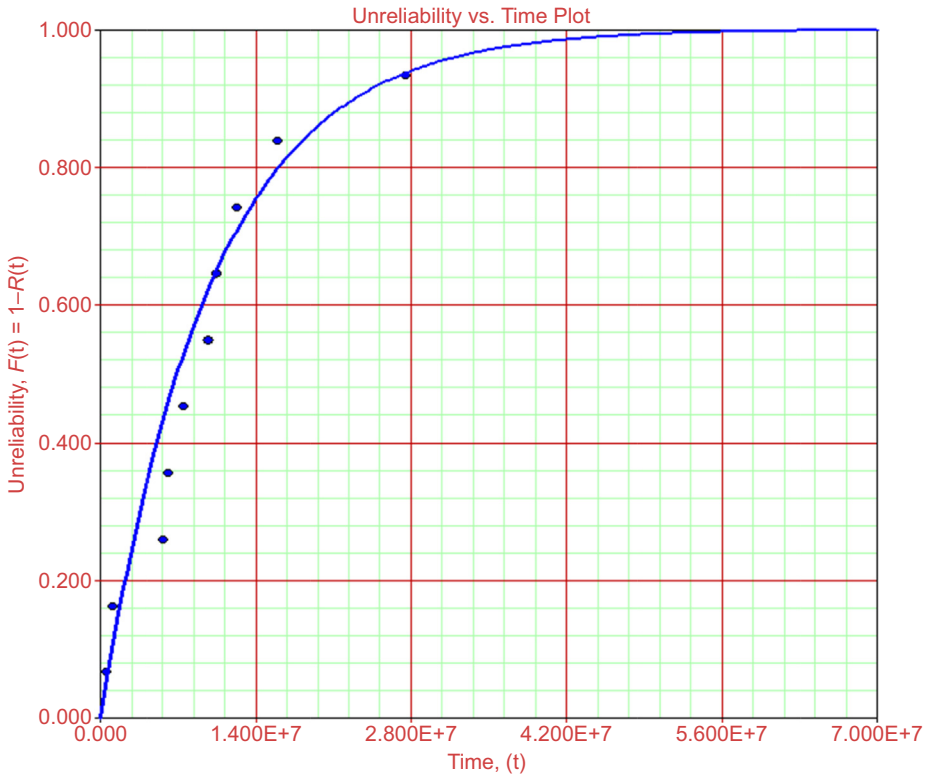
As Fig. 6.46 shows, the PFD increases over time. The SIF PFD is defined by:

$$\text{PFD}(t) = 1 - e^{-\lambda t}$$

where  $t$ , time and  $\lambda$ , failure rate.

Thus, by applying the SIF failure rate in the previous equation, we have different values of the SIF PFD over time, as shown in Table 6.9.

Based on the results of Table 6.9, the SIF decreased the SIL value after the first year, decreasing from SIL 3 to SIL 2, and after the 11th year, decreasing from SIL 2 to SIL 1 based on PFD values. This means if SIL 2 is selected to mitigate risk, the risk is mitigated until the 12th year when SIL 2 reduces to SIL 1. In this case, inspection must be conducted to reestablish SIL 2 values. Despite 11 years of the required failure on demand level, it is necessary to keep in mind that the longer inspection is delayed, the higher the chance of operating at an unacceptable level of risk. Thus inspections must be conducted to check the SIF. When establishing inspections to guarantee that SIF



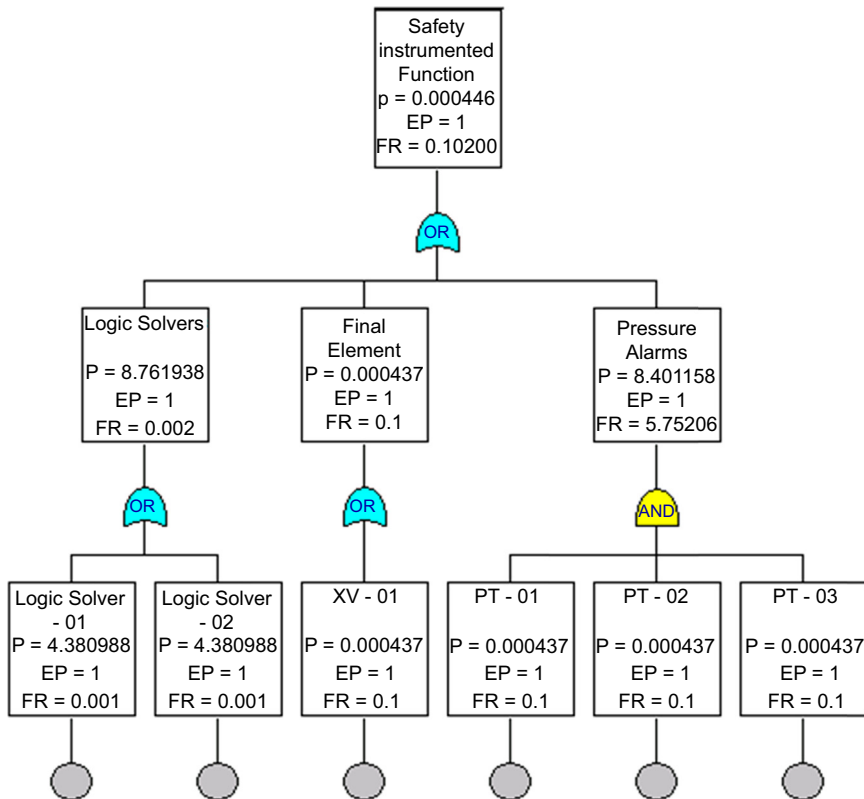
**FIGURE 6.46**  
Probability of failure on demand.

Table 6.9 SIL Variation Over Time			
Year	Hours	Probability of Failure on Demand	Safety Integrity Level
1	8760	$PFD(8760) = 1 - e^{-(110 \cdot 8760)} = 0.7 \cdot 10^3$	SIL 3 ( $10^4$ PFD $< 10^3$ )
2	17,520	$PFD(17,520) = 1 - e^{-(110 \cdot 17,520)} = 0.18 \cdot 10^2$	SIL 2 ( $10^3$ PFD $< 10^2$ )
3	26,280	$PFD(26,280) = 1 - e^{-(110 \cdot 26,280)} = 0.26 \cdot 10^2$	SIL 2 ( $10^3$ PFD $< 10^2$ )
4	35,040	$PFD(35,040) = 1 - e^{-(110 \cdot 35,040)} = 0.35 \cdot 10^2$	SIL 2 ( $10^3$ PFD $< 10^2$ )
5	43,800	$PFD(43,800) = 1 - e^{-(110 \cdot 43,800)} = 0.44 \cdot 10^2$	SIL 2 ( $10^3$ PFD $< 10^2$ )
6	52,560	$PFD(52,560) = 1 - e^{-(110 \cdot 52,560)} = 0.52 \cdot 10^2$	SIL 2 ( $10^3$ PFD $< 10^2$ )
7	61,320	$PFD(61,320) = 1 - e^{-(110 \cdot 61,320)} = 0.61 \cdot 10^2$	SIL 2 ( $10^3$ PFD $< 10^2$ )
8	70,080	$PFD(70,080) = 1 - e^{-(110 \cdot 70,080)} = 0.7 \cdot 10^2$	SIL 2 ( $10^3$ PFD $< 10^2$ )
9	78,840	$PFD(78,840) = 1 - e^{-(110 \cdot 78,840)} = 0.78 \cdot 10^2$	SIL 2 ( $10^3$ PFD $< 10^2$ )
10	87,600	$PFD(87,600) = 1 - e^{-(110 \cdot 87,600)} = 0.87 \cdot 10^2$	SIL 2 ( $10^3$ PFD $< 10^2$ )
11	96,360	$PFD(96,360) = 1 - e^{-(110 \cdot 96,360)} = 0.96 \cdot 10^2$	SIL 2 ( $10^3$ PFD $< 10^2$ )
12	105,120	$PFD(105,120) = 1 - e^{-(110 \cdot 105,120)} = 1.05 \cdot 10^2$	SIL 1 ( $10^2$ PFD $< 10^1$ )

remains at SIL 2 over time, there is always the possibility of human error, and in this case inspection, test, and replace might degrade the SIF sooner than expected. Thus, in addition to defining the inspection and test period to keep the SIL at the required SIL level, it is necessary to be aware of the human factors affecting inspection and test.

Further SIL analysis is the verification that is performed after the SIF configuration is defined to ensure that such configuration achieves the SIL target defined during SIL selection. Such assessment is usually carried out based on FTA analysis and historical failure data. Fig. 6.47 shows an example of SIF represented by FTA analysis after design configuration. The failure rates for the SIF components are:

- Pressure Alarms (PT-01, PT-02 and PT-03):  $\lambda = 0.1$
- Logic Solver (Logic Solver 1 and Logic Solver 2):  $\lambda = 0.01$
- Final Element (Valve XV-01):  $\lambda = 0.1$



**FIGURE 6.47**  
SIL verification FTA.

The software (BQR) considers also an inspection each 8760 h, which achieves the PDF of 4.46E-4. This PDF represents SIL level 3 over 10 years.

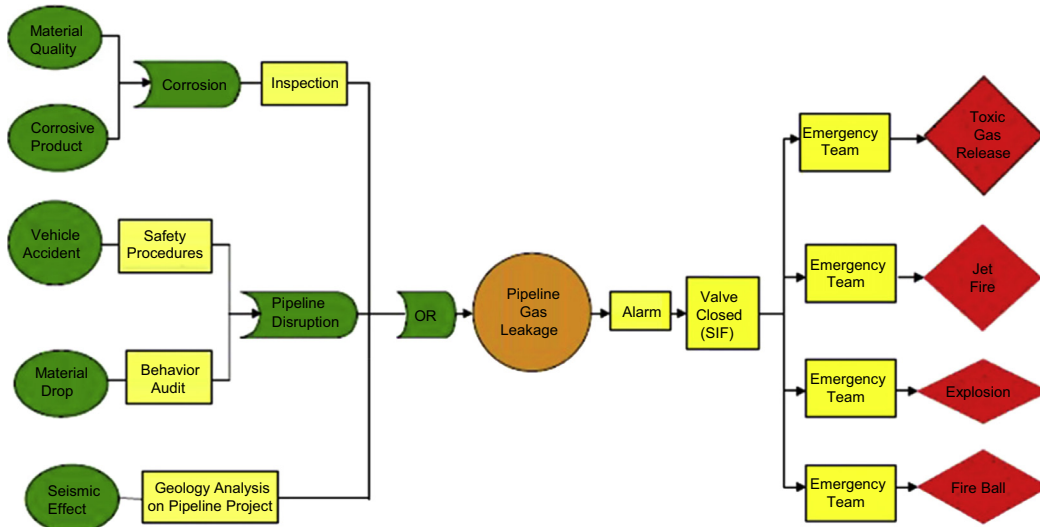
## 6.9 BOW TIE ANALYSIS

Bow tie analysis is the newest quantitative risk analysis and has been in use since the 1970s. It was incorporated by the Shell Oil Company into hazards management at the beginning of the 1990s.

Bow tie analysis includes FTA, ETA, and LOPA concepts and allows reliability engineers to assess all combinations of events from incident causes to incident consequences for the layers of protection that prevent accidents and mitigate consequences. Such methodology can be used to assess different types of problems, but in safety terms this type of analysis is used to assess and support accident analysis, process hazards, and perform risk management.

An example of bow tie analysis is an incident of gas release from a pipeline, as shown in Fig. 6.48. On the left side of the bow tie are all the causes of the incident and on the right side are all the consequences. In bow tie analysis, events are as follows:

- Potential causes (material quality, corrosive product, corrosion, vehicle accident, material drop, seismic effect, and pipeline disruption);
- Control measures (inspection, safety procedures, behavior audit, and geology analysis);
- Loss of control (pipeline gas leakage);
- Recovery measures (alarm, SIF, and emergency teams);
- Consequences (toxic gas release, jet fire, explosion, and fire ball).



**FIGURE 6.48**

Pipeline gas leak (bow tie).

As shown in Fig. 6.49, bow tie analysis can be a combination of FTA and ETA for layers of protection. In a pipeline gas leak, the potential causes are corrosion, pipeline disruption, and seismic effect.

Corrosion can be caused by inappropriate material quality in the pipeline or corrosive products in the pipeline, which do not meet pipeline specifications.

As a control measure to avoid corrosion, it is necessary to perform inspections periodically.

Pipeline disruption can be caused by vehicle accidents or material drops on the pipeline. As a control measure to avoid vehicle accidents it is necessary to follow traffic safety procedures. The control measure to avoid material drop on a pipeline when equipment or material are being moved around the pipeline area is to perform a behavior audit to verify that safety procedures are being conducted.

Seismic effect is another potential cause of accidents and the control measure is to perform geology analysis in the project phase to verify that the pipeline is in an area that is not subject to seismic effects.

If one of the main potential causes happens, that is, corrosion, pipeline disruption, or seismic effect of the pipeline, the incident of a pipeline gas leak may occur. If the incident occurs, there are four

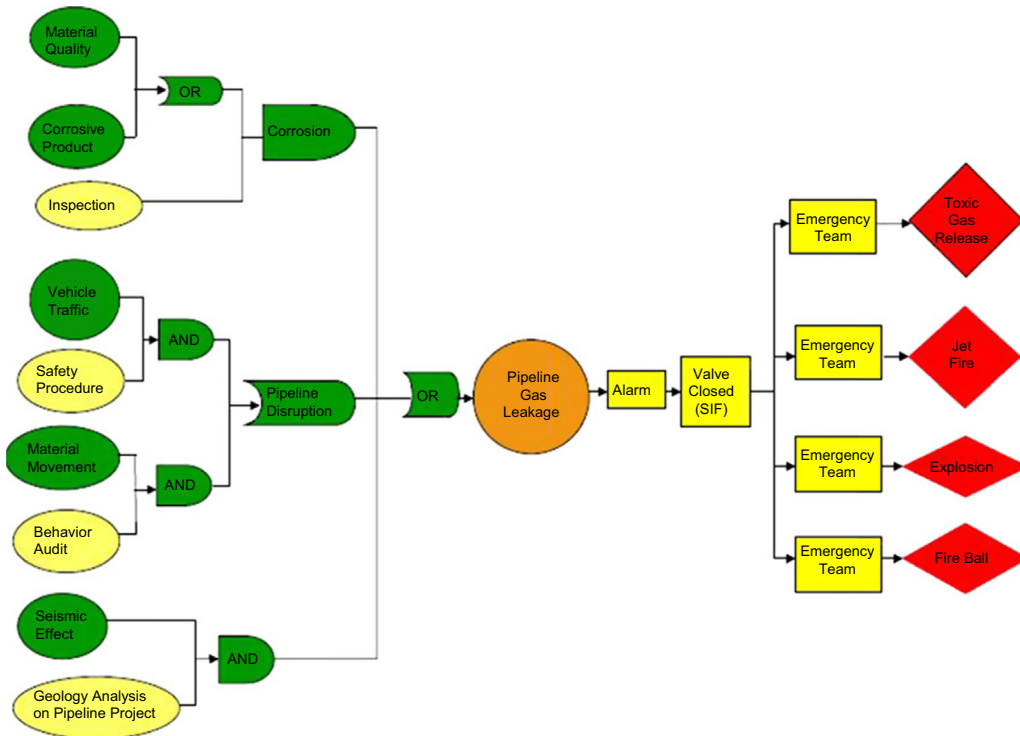


FIGURE 6.49

Pipeline gas leak (bow tie). Bow tie, FTA + ETA: Pipeline gas leakage.

probable consequences: toxic gas release, jet fire, explosion, or fire balls. Thus some recovery measures exist to avoid the accident, which are an alarm and SIF. With an alarm an operation emergency response is required, but if an SIF is used the valve will block the pipeline feed and reduce the amount of gas release.

To mitigate toxic gas release, jet fire, explosion, and fire ball consequences, emergency teams try to evacuate the vulnerable areas before some of the consequences occur. In addition, whenever possible the emergency team tries to eliminate ignition sources.

In most cases, bow tie analysis is performed qualitatively to assess an accident or incident, but when performing quantitatively it is a good tool because it includes most quantitative risk analysis methodology concepts and calculates the final event consequence probabilities.

In this case, depending on bow tie configuration, control measures can be taken into account in the fault tree logic when performing bow tie configuration, as shown in Fig. 6.49.

No matter what the bow tie configuration is in Fig. 6.48, the control measure probability of failure will be multiplied for fault tree logic gate results. For example, in the corrosion case in Fig. 6.48, the probability of corrosion will be:

$$\begin{aligned} P(\text{corrosion}) &= P(\text{Material Quality}) \cup P(\text{Corrosive product}) \\ &= P(\text{Material Quality}) + P(\text{Corrosive product}) - P(\text{Material Quality}) \\ &\quad \times P(\text{Corrosive product}) \end{aligned}$$

Actually, in this case the value of  $P(\text{corrosion})$  will be multiplied per  $P(\text{inspection})$  before calculating the logic gate “OR,” which gives the value of the pipeline gas leak.

In Fig. 6.49 the probability of corrosion is calculated by:

$$\begin{aligned} P(\text{corrosion}) &= P(\text{Material Quality}) \cup P(\text{Corrosive product}) \cap P(\text{Inspection}) \\ &= (P(\text{Material Quality}) + P(\text{Corrosive product}) - P(\text{Material Quality}) \\ &\quad \times P(\text{Corrosive product})) \times P(\text{Inspection}) \end{aligned}$$

### 6.9.1 TIME-INDEPENDENT BOW TIE ANALYSIS

If the final probability consequence results of the bow tie diagram are needed, it is necessary to consider the values of probability of potential causes, control measures, and recovery measures. To make this process easier it is best first to calculate the left side of the bow tie diagram and define the incident probability and then calculate the right side and define the consequence probability. For the bow tie diagram in Fig. 6.49 the values of probability for potential causes and control measures are:

$$P(\text{material quality}) = 0.1$$

$$P(\text{corrosive product}) = 0.2$$

$$P(\text{inspection}) = 0.01$$

$$P(\text{vehicle traffic}) = 0.3$$

$$P(\text{safety procedures}) = 0.01$$

$$P(\text{material movement}) = 0.1$$

$$P(\text{behavior audit}) = 0.005$$

$$P(\text{seismic effect}) = 0.005$$

$$P(\text{geology analysis on pipeline}) = 0.001$$

Thus the pipeline gas leak probability will be:

$$\begin{aligned} P(\text{Pipeline Gas Leakage}) &= (P(\text{Corrosion}) \cup P(\text{Pipeline Disruption}) \cup P(\text{Seismic effect})) \\ &= P(\text{Corrosion}) + P(\text{Pipeline Disruption}) + P(\text{Seismic effect}) \\ &\quad - (P(\text{Corrosion}) \times P(\text{Pipeline Disruption})) - (P(\text{Corrosion}) \times P(\text{Seismic effect})) \\ &\quad - (P(\text{Pipeline Disruption}) \times P(\text{Seismic effect})). \end{aligned}$$

To make the probability calculations easier, calculate each partial probability first and then substitute the probability values in the previous equation. Thus we have:

$$\begin{aligned} P(\text{Pipeline Gas Leakage}) &= (P(\text{Corrosion}) \cup P(\text{Pipeline Disruption}) \cup P(\text{Seismic effect})) \\ &= P(\text{Corrosion}) + P(\text{Pipeline Disruption}) + P(\text{Seismic effect}) - (P(\text{Corrosion}) \\ &\quad \times P(\text{Pipeline Disruption})) - (P(\text{Corrosion}) \times P(\text{Seismic effect})) - (P(\text{Pipeline Disruption}) \\ &\quad \times P(\text{Seismic effect})). \end{aligned}$$

To make the probability calculation easier it is necessary to calculate each partial probability first and after substitute probabilities values in the previous equation. Thus we have:

$$\begin{aligned} P(\text{Corrosion}) &= [P(\text{Material Quality}) \cup P(\text{Corrosive product})] \cap P(\text{Inspection}) \\ &= [P(\text{Material Quality}) + P(\text{Corrosive product}) - P(\text{Material Quality}) \times \\ &\quad P(\text{Corrosive product})] \times P(\text{Inspection}). \\ &= [(0.1 + 0.2) - (0.1 \times 0.2)] \times 0.01 = [(0.3) - (0.02)] \times 0.01 = 0.0028 \end{aligned}$$

$$P(\text{Corrosion}) = 0.0028$$

$$P(\text{Pipeline Disruption}) = [P(\text{Vehicle Traffic}) \cap P(\text{Safety procedures})] \cup [P(\text{Material Movement}) \cap P(\text{Behavior Audit})]$$

$$\begin{aligned} &= [P(\text{Vehicle Traffic}) \times P(\text{Safety procedures})] + [P(\text{Material Movement}) \times P(\text{Behavior Audit})] \\ &\quad - [P(\text{Vehicle Traffic}) \times P(\text{Safety procedures})] \times [P(\text{Material Movement}) \times P(\text{Behavior Audit})]. \\ &= [(0.3 \times 0.01) + (0.01 \times 0.005)] - [(0.3 \times 0.01) \times (0.01 \times 0.005)] \\ &= [0.003 + 0.00005] - [(0.003) \times (0.00005)] \\ &= 0.00305 - 0.00000015 = 0.00305 \end{aligned}$$

$$P(\text{Pipeline Disruption}) = 0.00305$$

$$\begin{aligned} P(\text{Seismic effect}) &= P(\text{Seismic Effect}) \cap P(\text{Geology Analysis on pipeline}) \\ &= P(\text{Seismic Effect}) \times P(\text{Geology Analysis on pipeline}) = 0.005 \times 0.01 = 0.00005 \end{aligned}$$

$$P(\text{Seismic effect}) = 0.00005$$

Finally, the pipeline gas leak probability is:

$$\begin{aligned} P(\text{Pipeline Gas Leakage}) &= (P(\text{Corrosion}) \cup P(\text{Pipeline Disruption}) \cup P(\text{Seismic effect})) \\ &= P(\text{Corrosion}) + P(\text{Pipeline Disruption}) + P(\text{Seismic effect}) - (P(\text{Corrosion}) \\ &\quad \times P(\text{Pipeline Disruption})) - (P(\text{Corrosion}) \times P(\text{Seismic effect})) - (P(\text{Pipeline Disruption}) \\ &\quad \times P(\text{Seismic effect})) \\ &= 0.0028 + 0.00305 + 0.00005 - (0.0028 \times 0.00305) - (0.0028 \times 0.00005) \\ &\quad - (0.00305 \times 0.00005) \\ &= 0.0059 - (0.00000854) - (0.00000014) - (0.0000001525) = 0.0058. \end{aligned}$$

$$P(\text{Pipeline Gas Leakage}) = 0.0058$$

The next step in the bow tie analysis is to calculate the consequences on the right side of the bow tie diagram. In this case, we consider the following probabilities:

- The probability of alarm failure is 10%.
- The probability of SIF failure is 0.1%.
- The probability the emergency team eliminates all ignition sources is an 80% chance of an accident being toxic gas release.
- If the emergency team is not able to eliminate the early ignition source the probability is a 10% chance of an accident scenario being a jet fire.
- When the emergency team is not able to eliminate the ignition source and a toxic cloud enters a confined place the probability is 1% of an accident scenario being an explosion.
- When the emergency team is not able to eliminate the late ignition source but avoids a toxic cloud entering a confined place, the probability is a 9% chance of an accident scenario being a fire ball.

In doing so, for the probability of a gas leak, the probabilities of toxic gas release, jet fire, explosion, and fire balls are:

$$\begin{aligned} P(\text{Toxic Gas Release}) &= P(\text{Pipeline Gas leakage}) \cap P(\text{Alarm}) \cap P(\text{SIF}) \cap P(\text{emergency team}) \\ &= P(\text{Pipeline Gas leakage}) \times P(\text{Alarm}) \times P(\text{SIF}) \times P(\text{emergency team}) \\ &= 0.0058 \times 0.1 \times 0.001 \times 0.8 = 0.000000464 \end{aligned}$$

$$P(\text{Toxic Gas Release}) = 0.000000464$$

$$\begin{aligned} P(\text{Jet Fire}) &= P(\text{Pipeline Gas leakage}) \cap P(\text{Alarm}) \times P(\text{SIF}) \cap P(\text{emergency team}) \\ &= P(\text{Pipeline Gas leakage}) \times P(\text{Alarm}) \times P(\text{SIF}) \times P(\text{emergency team}) \\ &= 0.0058 \times 0.1 \times 0.001 \times 0.1 = 0.000000058 \end{aligned}$$



$$P(\text{Jet Fire}) = 0.000000058$$

$$\begin{aligned} P(\text{Explosion}) &= P(\text{Pipeline Gas leakage}) \cap P(\text{Alarm}) \cap P(\text{SIF}) \cap P(\text{emergency team}) \\ &= P(\text{Pipeline Gas leakage}) \times P(\text{Alarm}) \times P(\text{SIF}) \times P(\text{emergency team}) \\ &= 0.0058 \times 0.1 \times 0.001 \times 0.01 = 0.000000058 \end{aligned}$$

$$P(\text{Explosion}) = 0.000000058$$

$$\begin{aligned} P(\text{Fire Ball}) &= P(\text{Pipeline Gas leakage}) \cap P(\text{Alarm}) \cap P(\text{SIF}) \cap P(\text{emergency team}) \\ &= P(\text{Pipeline Gas leakage}) \times P(\text{Alarm}) \times P(\text{SIF}) \times P(\text{emergency team}) \\ &= 0.0058 \times 0.1 \times 0.001 \times 0.09 = 0.0000000522 \end{aligned}$$

$$P(\text{Fire Ball}) = 0.0000000522$$

Such consequence probabilities can be used in the qualitative risk analysis, but as we discussed before, the probability of accidents occurring varies over time, which is the subject of the next section.

## 6.9.2 TIME-DEPENDENT BOW TIE ANALYSIS

As performed in other risk analysis methodologies, time-dependent bow tie analysis uses CDFs for events and consequently the probability of failure increases over time based on the CDF. In bow tie analysis, not all events are described by CDFs because the probability is really constant over time. A good example of a probability that is constant over time is an event such as emergency team intervention where there is one probability of success or failure based on the number of observations. Some potential causes, such as poor material quality and poor geology analysis, have similar concepts, that is, constant probability over time. However, other events or equipment are better represented by CDFs because of an increased chance of failure over time. Table 6.10 shows the failure rate for each potential cause, and the control measures and recovery measures related to the bow tie diagram are given in Fig. 6.49.

The probability of a poor quality of material is constant over time as well as the probability of failure in geology analysis and the probability of failure in emergency team actions. Thus such events have a similar probability in 1.5 years (13,140 h) and 5 years (43,800 h). However, the other events have different failure rates and consequently different probabilities over time based on the CDFs, which are described by an exponential function, having different values in 1.5 years and 5 years. The values of the probabilities in 1.5 years are similar to the values found in the static bow tie analysis example in Section 6.5.1. Thus dynamic bow tie analysis was conducted with probability values for 5 years and compared with values for 1.5 years.

The probability in 5 years (43,800 h) described in the sixth column is defined by:

$$P(\text{Inspection})(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00000001t} = 1 - e^{-0.00000001(43800)} = 0.04$$

$$P(\text{Vehicle} \cdot \text{Traffic})(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00000027t} = 1 - e^{-0.00000027(43800)} = 0.7$$

$$P(\text{Safety} \cdot \text{Procedure})(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00000001t} = 1 - e^{-0.00000001(43800)} = 0.04$$

$$P(\text{Material} \cdot \text{Movement})(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00000008t} = 1 - e^{-0.00000008(43800)} = 0.30$$

**Table 6.10 Probability Variation Over Time**

	<i>l</i> (oc/h)	<i>t</i> (h)	<i>P</i> (1.5 years)	<i>t</i> (h)	<i>P</i> (5 years)
<i>P</i> (material quality)	<i>x</i>	13,140	0.1	43,800	0.1
<i>P</i> (corrosive product)	1.7E-05	13,140	0.2	43,800	0.5
<i>P</i> (inspection)	1E-06	13,140	0.01	43,800	0.04
<i>P</i> (vehicle traffic)	2.7E-05	13,140	0.3	43,800	0.7
<i>P</i> (safety procedures)	1E-06	13,140	0.01	43,800	0.04
<i>P</i> (material movement)	8E-06	13,140	0.1	43,800	0.3
<i>P</i> (behavior audit)	3.8E-07	13,140	0.005	43,800	0.02
<i>P</i> (seismic effect)	3.8E-07	13,140	0.005	43,800	0.02
<i>P</i> (geology analysis on pipeline)	<i>x</i>	13,140	0.01	43,800	0.01
<i>P</i> (alarm)	8E-06	13,140	0.1	43,800	0.3
<i>P</i> (SIF)	1E-07	13,140	0.001	43,800	0.004
Emergency team(toxic gas leakage)	<i>x</i>	13,140	0.8	43,800	0.8
Emergency team(jet fire)	<i>x</i>	13,140	0.1	43,800	0.01
Emergency team(explosion)	<i>x</i>	13,140	0.01	43,800	0
Emergency team(fire ball)	<i>x</i>	13,140	0.9	43,800	0.9

$$P(\text{Behavior} \cdot \text{Audit})(t) = 1 - e^{-\lambda t} = 1 - e^{-0.0000000038t} = 1 - e^{-0.0000000038(43800)} = 0.02$$

$$P(\text{Seismic} \cdot \text{Effect})(t) = 1 - e^{-\lambda t} = 1 - e^{-0.0000000038t} = 1 - e^{-0.0000000038(43800)} = 0.02$$

$$P(\text{Alarm})(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00000008t} = 1 - e^{-0.00000008(43800)} = 0.3$$

$$P(\text{SIF})(t) = 1 - e^{-\lambda t} = 1 - e^{-0.000000001t} = 1 - e^{-0.000000001(43800)} = 0.004$$

The next step is to substitute the probabilities values from Table 6.10 in the following equations to find the probability of a pipeline gas leak in 5 years:

$$\begin{aligned} P(\text{Pipeline Gas Leakage}) &= (P(\text{Corrosion}) \cup P(\text{Pipeline Disruption}) \cup P(\text{Seismic effect})) \\ &= P(\text{Corrosion}) + P(\text{Pipeline Disruption}) + P(\text{Seismic effect}) - (P(\text{Corrosion}) \\ &\quad \times P(\text{Pipeline Disruption})) - (P(\text{Corrosion}) \times P(\text{Seismic effect})) \\ &\quad - (P(\text{Pipeline Disruption}) \times P(\text{Seismic effect})). \end{aligned}$$

As discussed it is necessary to calculate each partial probability first and then substitute the probability values in the previous equation. Thus we have:

$$\begin{aligned} P(\text{Corrosion}) &= [P(\text{Material Quality}) \cup P(\text{Corrosive product})] \cap P(\text{Inspection}) \\ &= [P(\text{Material Quality}) + P(\text{Corrosive product}) - P(\text{Material Quality}) \\ &\quad \times P(\text{Corrosive product})] \times P(\text{Inspection}). \\ &= [(0.1 + 0.5) - (0.1 \times 0.5)] \times 0.04 = [(0.6) - (0.05)] \times 0.04 = 0.022 \end{aligned}$$

$$P(\text{Corrosion}) = 0.022$$

$$P(\text{Pipeline Disruption}) = [P(\text{Vehicle Traffic}) \cap P(\text{Safety procedures})] \cup [P(\text{Material Movement}) \cap P(\text{Behavior Audit})]$$

$$= [P(\text{Vehicle Traffic}) \times P(\text{Safety procedures})] + [P(\text{Material Movement}) \times P(\text{Behavior Audit})] - [P(\text{Vehicle Traffic}) \times P(\text{Safety procedures})] \times [P(\text{Material Movement}) \times P(\text{Behavior Audit})].$$

$$= [(0.7 \times 0.04) + (0.3 \times 0.02)] - [(0.7 \times 0.04) \times (0.3 \times 0.02)]$$

$$= [0.028 + 0.006] - [(0.028) \times (0.006)] \\ = 0.034 - 0.000168 = 0.0338$$

$$P(\text{Pipeline Disruption}) = 0.0338$$

$$P(\text{Seismic effect}) = P(\text{Seismic Effect}) \cap P(\text{Geology Analysis on pipeline}) \\ = P(\text{Seismic Effect}) \times P(\text{Geology Analysis on pipeline}) = 0.02 \times 0.01 \\ = 0.0002$$

$$P(\text{Seismic effect}) = 0.0002$$

Finally, the pipeline gas leakage probability is:

$$P(\text{Pipeline Gas Leakage}) = (P(\text{Corrosion}) \cup P(\text{Pipeline Disruption}) \cup P(\text{Seismic effect})) \\ = P(\text{Corrosion}) + P(\text{Pipeline Disruption}) + P(\text{Seismic effect}) - (P(\text{Corrosion}) \\ \times P(\text{Pipeline Disruption})) - (P(\text{Corrosion}) \times P(\text{Seismic effect})) - (P(\text{Pipeline Disruption}) \\ \times P(\text{Seismic effect})). \\ = 0.022 + 0.0338 + 0.0002 - (0.022 \times 0.0338) - (0.022 \times 0.0002) - (0.0338 \times 0.0002). \\ = 0.056 - (0.0007436) - (0.0000044) - (0.00000676) = 0.00633.$$

$$P(\text{Pipeline Gas Leakage}) = 0.00633$$

The next step in bow tie analysis is calculating the consequences that are the right side of bow tie diagram. In doing so, regarding the probability of gas leakage and other events over 5 years, the probability of toxic gas release, jet fire, explosion, and fire ball are:

$$P(\text{Toxic Gas Release}) = P(\text{Pipeline Gas leakage}) \cap P(\text{Alarm}) \cap P(\text{SIF}) \cap P(\text{emergency team}) \\ = P(\text{Pipeline Gas leakage}) \times P(\text{Alarm}) \times P(\text{SIF}) \times P(\text{emergency team}) \\ = 0.055 \times 0.3 \times 0.004 \times 0.8 = 0.000528$$

$$P(\text{Toxic Gas Release}) = 0.000528$$

$$P(\text{Jet Fire}) = P(\text{Pipeline Gas leakage}) \cap P(\text{Alarm}) \cap P(\text{SIF}) \cap P(\text{emergency team}) \\ = P(\text{Pipeline Gas leakage}) \times P(\text{Alarm}) \times P(\text{SIF}) \times P(\text{emergency team}) \\ = 0.055 \times 0.3 \times 0.004 \times 0.1 = 0.0000066$$

$$P(\text{Jet Fire}) = 0.0000066$$

$$\begin{aligned}
P(\text{Explosion}) &= P(\text{Pipeline Gas leakage}) \cap P(\text{Alarm}) \cap P(\text{SIF}) \cap P(\text{emergency team}) \\
&= P(\text{Pipeline Gas leakage}) \times P(\text{Alarm}) \times P(\text{SIF}) \times P(\text{emergency team}) \\
&= 0.055 \times 0.3 \times 0.004 \times 0.01 = 0.00000066
\end{aligned}$$

$$P(\text{Explosion}) = 0.00000066$$

$$\begin{aligned}
P(\text{Fire Ball}) &= P(\text{Pipeline Gas leakage}) \cap P(\text{Alarm}) \cap P(\text{SIF}) \cap P(\text{emergency team}) \\
&= P(\text{Pipeline Gas leakage}) \times P(\text{Alarm}) \times P(\text{SIF}) \times P(\text{emergency team}) \\
&= 0.055 \times 0.3 \times 0.004 \times 0.09 = 0.00000594
\end{aligned}$$

$$P(\text{Fire Ball}) = 0.00000594$$

The probability of failure in 5 years is higher for all consequences and it is important to compare such values in the risk matrix to know if a new value of risk for each consequence is tolerable. To compare the risk matrix it is necessary to have probability values.

Remember that potential causes, control measures, and recovery measures can be represented in any kind of CDF (normal, Weibull, lognormal, loglogistic, logistic, Gumbel, gamma, and generalized gamma) depending on historical data. In this bow tie example, the exponential CDF was used to make it easier to understand.

Also note that such dynamic reliability analysis can be performed using software. One alternative to performing bow tie analysis is to use partial analysis starting from the left side of the bow tie to calculate the incident event by ETA and then go to the right side of the bow tie and calculate the consequences frequency.

In [Table 6.4](#), if we consider  $\lambda = 8 \times 10^{-6}$  for material quality and  $\lambda = 1 \times 10^{-6}$  for geology analysis of the pipeline, performing Monte Carlo simulation to define the pipeline gas leak we have  $\lambda = 4.8 \times 10^{-10}$  and  $R(43,800) = 100\%$ . Thus performing the calculation of the left side of the bow tie the frequency of consequences will be:

$$\begin{aligned}
F(\text{Toxic Gas Release}) &= F(\text{Pipeline Gas leakage}) \times P(\text{Alarm}) \times P(\text{SIF}) \times P(\text{emergency team}) \\
&= 4.8 \times 10^{-10} \times 0.3 \times 0.004 \times 0.8 = 4.6 \times 10^{-13}
\end{aligned}$$

$$F(\text{Toxic Gas Release}) = 4.6 \times 10^{-13}$$

$$\begin{aligned}
F(\text{Jet Fire}) &= F(\text{Pipeline Gas leakage}) \times P(\text{Alarm}) \times P(\text{SIF}) \times P(\text{emergency team}) \\
&= 4.8 \times 10^{-10} \times 0.3 \times 0.004 \times 0.1 = 5.76 \times 10^{-14}
\end{aligned}$$

$$F(\text{Jet Fire}) = 5.76 \times 10^{-14}$$

$$\begin{aligned}
F(\text{Explosion}) &= F(\text{Pipeline Gas leakage}) \times P(\text{Alarm}) \times P(\text{SIF}) \times P(\text{emergency team}) \\
&= 4.8 \times 10^{-10} \times 0.3 \times 0.004 \times 0.01 = 5.76 \times 10^{-15}
\end{aligned}$$

$$F(\text{Explosion}) = 5.76 \times 10^{-15}$$

$$\begin{aligned}
F(\text{Fire Ball}) &= P(\text{Pipeline Gas leakage}) \cap P(\text{Alarm}) \cap P(\text{SIF}) \cap P(\text{emergency team}) \\
&= P(\text{Pipeline Gas leakage}) \times P(\text{Alarm}) \times P(\text{SIF}) \times P(\text{emergency team})
\end{aligned}$$

$$= 4.8 \times 10^{-10} \times 0.3 \times 0.004 \times 0.09 = 5.2 \times 10^{-15}$$

$$F(\text{Fire Ball}) = 5.2 \times 10^{-15}$$

Fig. 6.50 shows the failure rate function of the pipeline gas leak as a result of simulation.

Each consequence has an individual risk. In the worst case (toxic gas leak) the risk is lower than  $1 \times 10^{-4}$ . Unless such consequence causes a higher number of deaths (more than 10,000,000) into operational ground, the individual risk will be intolerable.

Bow tie analysis is a good quantitative risk analysis tool to have a complete idea about potential incident causes, consequences, and control measures as a whole.

This methodology can qualitatively assess and identify the potential causes, control measures, recovery measures, and consequences to better understand accidents or even as a risk analysis tool to find out if a risk is tolerable. In addition, this method can also be used for risk management. In this case, potential causes, control measures, and recovery measures have to be updated constantly. In doing so the cut sets for incidents would be highlighted as well as control measures and recovery measures. As dynamic bow tie analysis gives different values for most events over time, if the bow tie is updated automatically by software, as shown in Fig. 6.51, it is possible to see the CDF of the incident and the consequences as well as the risk of each consequence over time to support decisions and better manage risk.

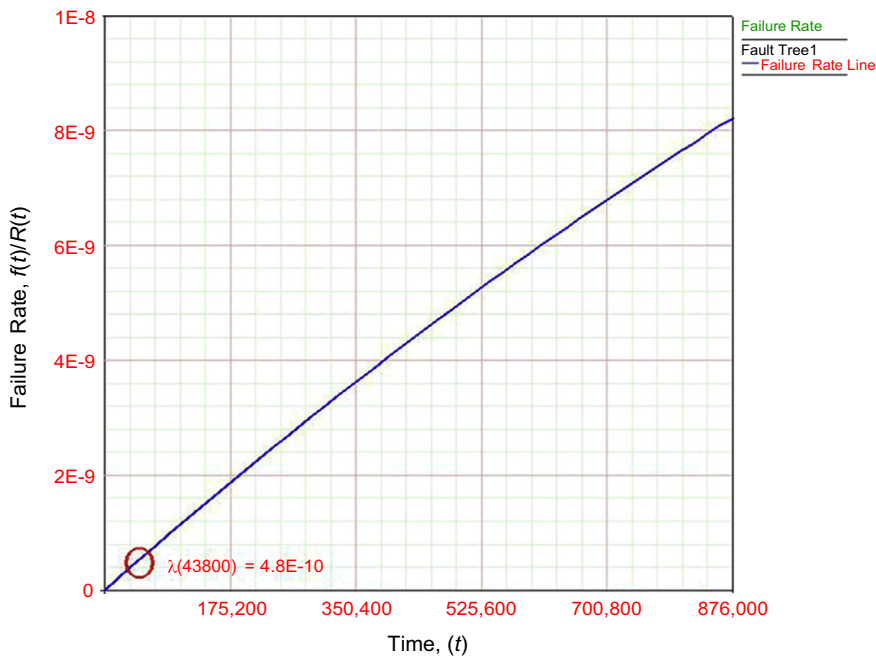


FIGURE 6.50

Pipeline gas leak failure rate.

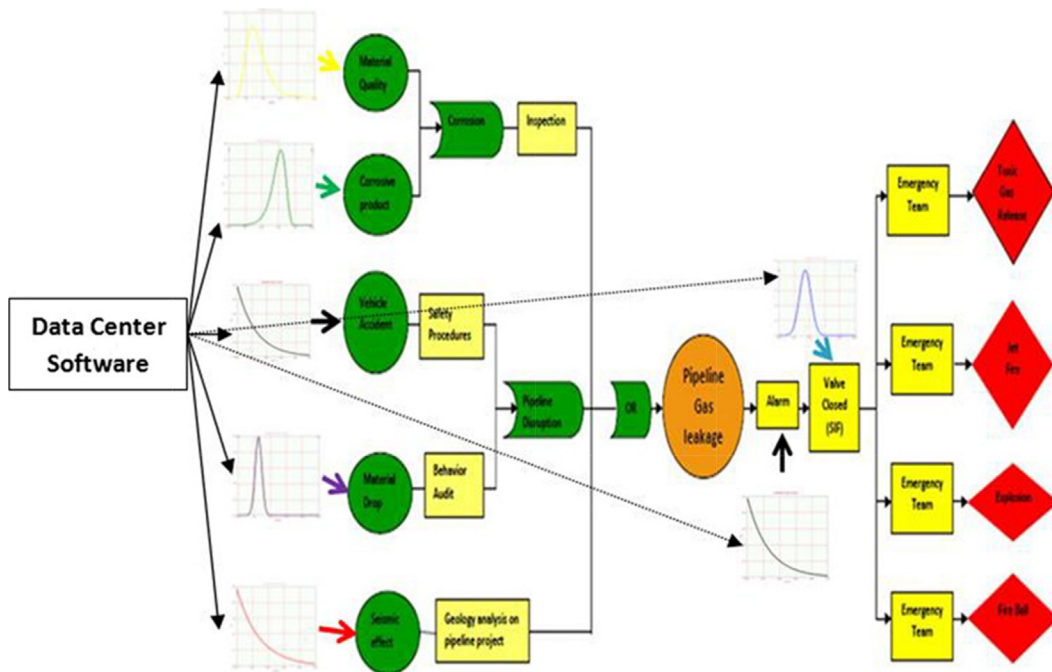


FIGURE 6.51

Dynamic bow tie analysis.

## 6.10 RISK ANALYSIS CASE STUDIES

To exemplify the application of risk analysis under a project or operational context to support a decision, different case studies will be used.

The first case study concerns the LOPA application to define the level of risk when safety critical equipment fails or a preventive maintenance is performed.

The second case study concerns the effect of the safety process on system performance. Therefore FTA based on HAZOP analysis will be integrated into an RBD to model and measure such safety effects on operational availability.

The third case study is a continuation of human reliability analysis carried out in Chapter 5, the objective of which was to predict the human error probability to shut down an emergency shutdown valve. In this particular case, FTA and bow tie analysis will be integrated to perform assessment of different consequences of human error.

The fourth case study describes a blowout accident and demonstrates bow tie methodology to support the accident assessment.

The final case study demonstrates the SIL analysis methodology, which will encompass SIL selection and SIL verification based on FTA.

### 6.10.1 CASE STUDY 1: APPLYING LOPA TO DECIDE WHETHER RISK IS ACCEPTABLE WHEN LAYERS OF PROTECTION ARE NOT AVAILABLE

Nowadays in the oil and gas industry, in most cases, the usual methodology applied to assess risk when the layers of protection are under corrective maintenance intervention because of failures or even preventive maintenance is PHA. PHA is an ideal risk analysis tool because employees are familiar with it, and it is easy to implement. However, it is not possible to know quantitatively if a risk is under control or when one or more layers of protection are unavailable.

In some cases the consequences are clear and in others they are not, but in some cases it is possible to check historical accident data or risk analysis reports. The real problem of estimating the probability of an unwanted event happening is that it is also necessary to estimate the probability of the initiating event combined with layer protection failures. Because of this, in most cases when initiating events, and layers of protection are not available, the analyst is conservative in decision making and overestimates risk. In this case the plant is shut down to avoid a catastrophic accident, but this was not necessary because a risk without a layer of protection is acceptable.

Indeed, LOPA should be applied to analyze the probability of an unwanted event occurring with and without a layer of protection. Once the data of the probability of an unwanted event and layers of protection is available it is possible to find the risk level and see if it is acceptable. The proposed preventive methodology supporting decisions when layers of protection are unavailable because of maintenance or failure is based on the following steps:

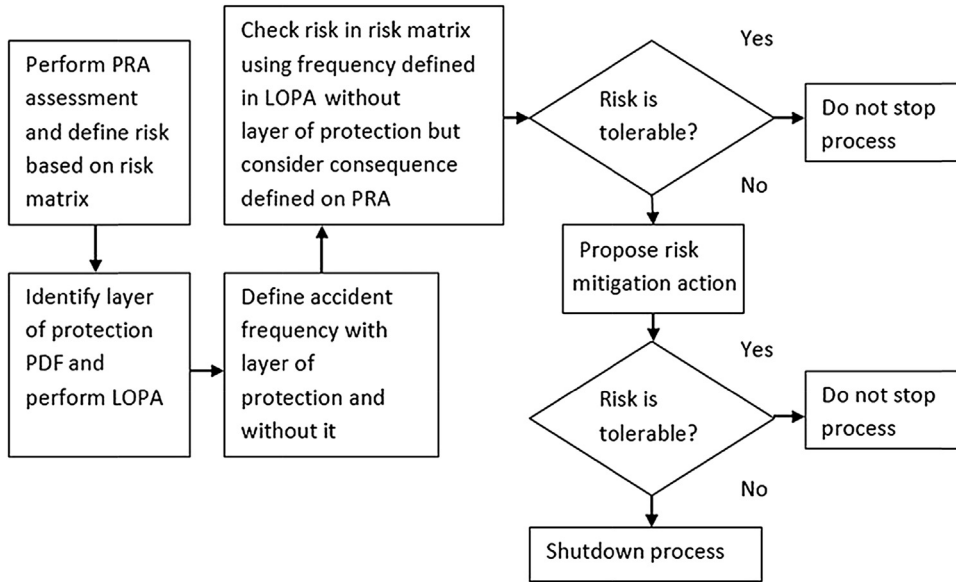
1. Conduct PRA of the system with a layer of protection to define the risk qualitatively.
2. Conduct LOPA to find the probability of an accident without a layer of protection.
3. See if the risk without a layer of protection is acceptable.
4. If the risk is unacceptable, propose some preventive action or new layer of protection to reduce risks to the acceptable region.
5. If it is not possible to reduce the risk to an acceptable condition, shut down the plant.

Based on these five steps, it is possible to make better decisions when layers of protection fail or when it is necessary to perform preventive maintenance in layers of protection. Fig. 6.52 shows the risk analysis methodology to support decisions when or if to shut down a plant.

There are two approaches to comparing risk when layers of protection are taken out of the process and to see if the risk is tolerable. The first approach is to analyze the frequency of accidents without layers of protection and combine it with the consequences based on the risk matrix. The second approach is to compare the final risk with the individual risk (ALARP) in cases where the consequence of death is estimated by consequences and effects analysis. Consequences and effects analysis measures the vulnerability of toxic releases, explosion, and jet fire, and predicts the number of deaths of people in the vulnerable area.

In the first case the first step is to conduct PRA based on the qualitative risk matrix and define the risk. Next, the probability of the unwanted event without a layer of protection is defined using LOPA and the risk matrix.

In the second case the frequency defined in LOPA is multiplied by the expected number of deaths estimated in the consequences and effects analysis and compared to the individual tolerable risk values. For example, if there is excess gas in a furnace, it is an unsafe condition, and to avoid furnace explosion a layer of protection such as a human action ( $P(f1) \frac{1}{4} 0.1$ ), manual valve ( $P(f2) = 0.01$ ), or



**FIGURE 6.52**

Risk analysis methodology to support a plant shutdown decision (LOPA).

basic process control system (BPCS)  $P(f_3) = 1 \times 10^{-4}$  is triggered. This incident (excess gas in a furnace) has a frequency of  $1 \times 10^{-1}$  per year. The frequency of the furnace explosion is:

$$f(\text{Furnace explosion}) = f(\text{excess of gas}) \times P(f_1) \times P(f_2) \times P(f_3)$$

$$f(\text{Furnace explosion}) = 1 \times 10^{-1} \times 0.1 \times 0.01 \times 1 \times 10^{-4} = 1 \times 10^{-8}$$

If this accident happened, at least 10 deaths in the plant are expected, so based on the risk matrix the risk is moderate, as shown in Fig. 6.53 (severity category III and frequency category A). Based on the individual risk criteria the risk is 10 (deaths)  $1 \times 10^{-8}$  (frequency), which is  $1 \times 10^{-7}$  (acceptable). For individual risk criteria this is acceptable because it is lower than  $1 \times 10^{-4}$ , as shown in Fig. 6.54.

In case of preventive maintenance or shutdown in the BPCS, for example, the furnace has to be stopped because the risk is not acceptable according to the individual risk criteria. In fact, without BPCS the frequency of accident is:

$$f(\text{Furnace explosion}) = f(\text{excess of gas}) \times P(f_1) \times P(f_2)$$

$$f(\text{Furnace explosion}) = 1 \times 10^{-1} \times 0.1 \times 0.01 = 1 \times 10^{-4}$$

$$\text{Individual Risk} = 10 \times 1 \times 10^{-4} = 1 \times 10^{-3}$$

This is in the unacceptable region, as shown in Fig. 6.54. However, if this value is used in the risk matrix the risk can be considered moderate (severity category III and frequency category A), as shown in Fig. 6.53. This shows that more than one risk criteria must be considered whenever possible to make better decisions.



		FREQUENCY CATEGORY					
		A (Extremely remote)	B (Remote)	C (Little frequency)	D (Frequent)	E (Very frequent)	F (Extremely frequent)
		At least 1 between 1000 and 100,000 years	At least 1 between 50 and 1000 years	At least 1 between 30 and 50 years	At least 1 between 5 and 30 years	At least 1 in 5 years	At least 1 in 1 year
SEVERITY CATEGORY	IV	M	NT	NT	NT	N	NT
	III	M	M	NT	NT	N	NT
	II	T	T	M	M	M	M
	I	T	T	T	M	M	M

FIGURE 6.53

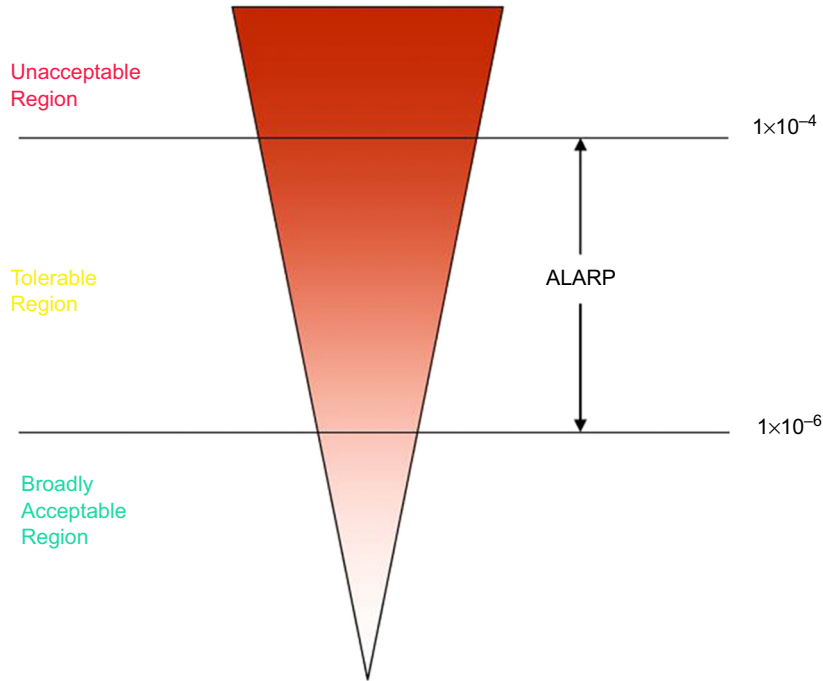
Risk matrix.

Whenever decisions are made based on the risk matrix it is possible to consider the tolerable risk to prevent plant shutdown. When LOPA is conducted the frequency is calculated, thus risk has a more realistic value.

In addition to preventive layers of protection, the contingency system can also influence the risk level to reduce consequence severity. If those systems are undergoing preventive maintenance or have failed, the consequence would be worse than expected if an accident occurred. This means the consequences without a contingency system would be worse in terms of risk level. Therefore when there is maintenance or a shutdown of the contingency system (sprinklers, fire system pumps, and chemical showers) it is necessary to see if the consequences are worse without it. Fig. 6.55 summarizes the steps applied to assess risk in case of preventive maintenance or corrective maintenance (failure) for the contingency system.

An example of the application of such methodology is in the preventive maintenance of a fire pump system in a refinery. This contingency system provides water to combat fire, and if it has failed or is undergoing maintenance when the fire occurred, the consequence will be worse; in other words, based on the matrix in Fig. 6.53 the consequence goes from critical to catastrophic. Aware of this fact the maintenance team will keep the system available during maintenance and take out only one pump for maintenance.

If the electric system shuts down, one fire protection pump stops. At least one pump is required to keep the fire pump system available. To define the fire pump system availability the dynamic FTA was



**FIGURE 6.54**

Individual risk tolerable region.

applied to find the fire pumps system's availability and the failure rate without one pump. To model the fire pump system's availability, the time-dependent FTA was used, as shown in Fig. 6.56.

The time-dependent FTA is a quantitative risk methodology applied in combinations of events that cause unwanted events, which in this case is fire pump system unavailability. In the top event, to make the system unavailable, failure in the electric energy supply and two others pumps (D and E) is necessary. Pump E is the redundancy of pump D. The failure pump rate is 0.5 per year and the electric system failure rate is 1 per year. The dynamic fault tree probability of failure is described by:

$$P(\text{Fire Pump System Out}) = \text{Top event failure probability};$$

$$P(\text{FES}) = \text{Failure Electric System probability};$$

$$P(\text{PD}) = \text{Pump D failure probability};$$

$$P(\text{PE}) = \text{Pump E failure probability}.$$

$$P(\text{FES})(t) = 1 - e^{-\lambda t} = 1 - e^{-0.0000014t} = 1 - e^{-0.0000014(43800)} = 0.059$$

$$P(\text{PD})(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00023t} = 1 - e^{-0.00023(43800)} = 0.9999$$

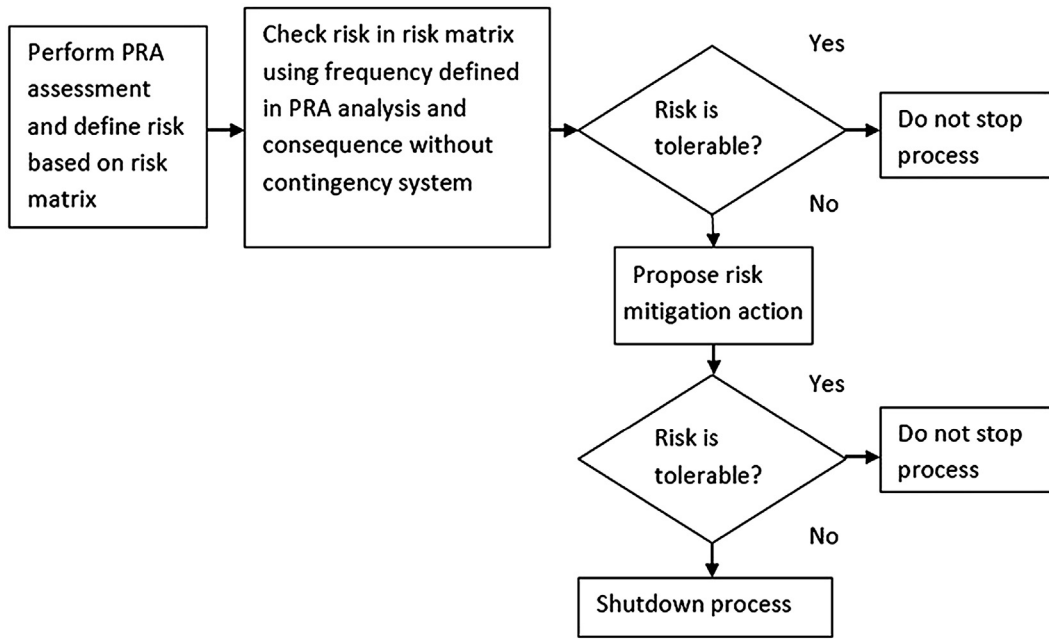


FIGURE 6.55

Risk analysis methodology to support plant shutdown decisions (contingency plan).

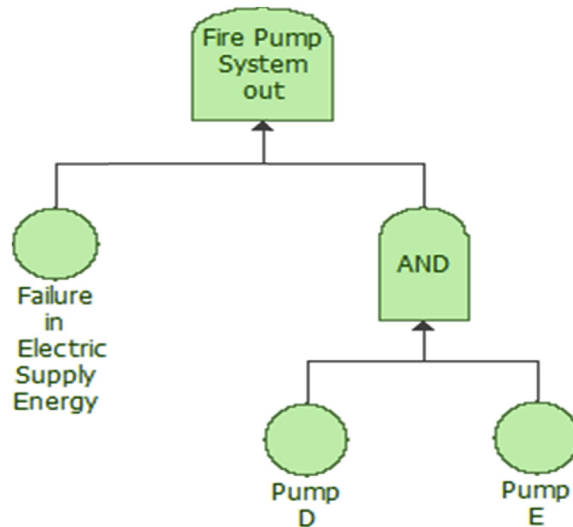


FIGURE 6.56

The fire pump system FTA.

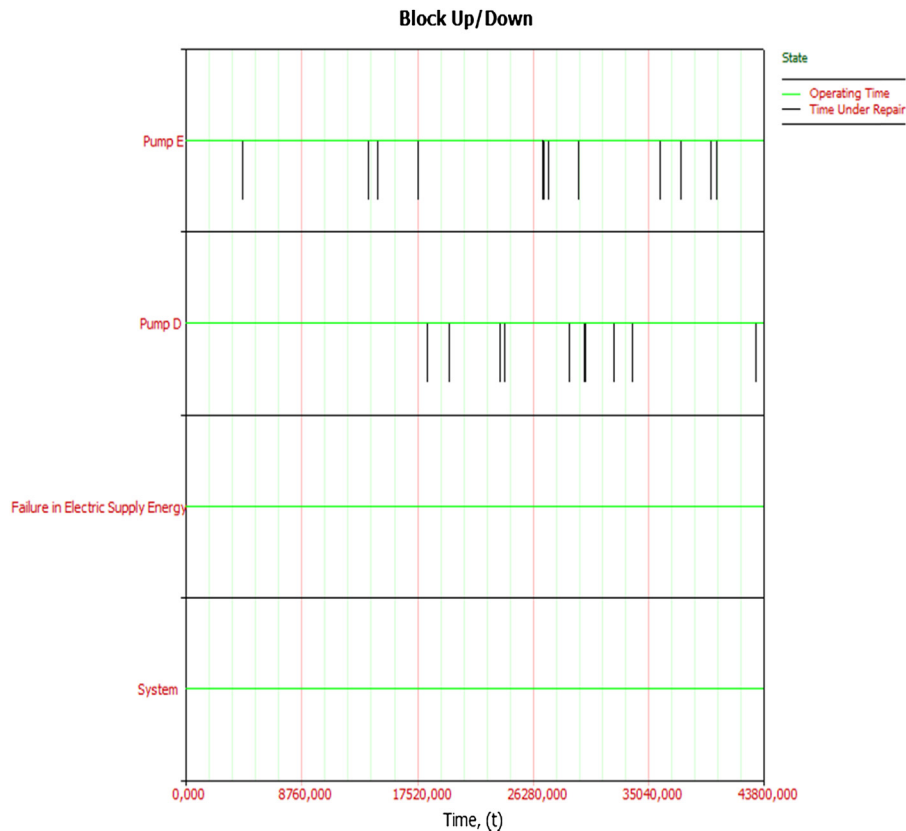
$$P(\text{PE})(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00023t} = 1 - e^{-0.00023(43800)} = 0.9999$$

$$P(\text{Fire} \cdot \text{Pump} \cdot \text{System} \cdot \text{Out}) = P(\text{FES}) \times P(\text{PD}) \times P(\text{PE}) = 0.059 \times 0.9999 \times 0.9999 = 0.06$$

where  $P(\text{fire pump system out})$ , top event failure probability;  $P(\text{FES})$ , failure electric system probability;  $P(\text{PD})$ , pump D failure probability; and  $P(\text{PE})$ , pump E failure probability.

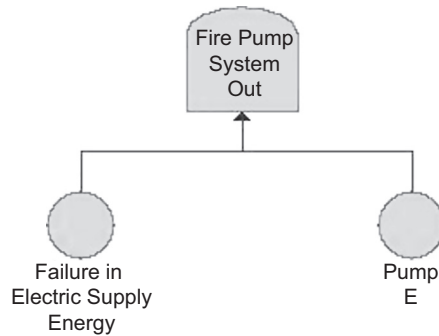
Whether 2 h are needed to reestablish the electric energy system and 8 h for each pump repair, the simulations in Fig. 6.57 show the system is 100% available until 5 years despite pump failures.

If the pump in maintenance (pump D) is out for 1 h (maintenance service time duration) in the fourth year and 11th month, for example, it is necessary to check the fire pump system availability and the probability of failure. Fig. 6.58 represents the fire pump system without pump D in maintenance.



**FIGURE 6.57**

The fire pump system simulation.



**FIGURE 6.58**

The fire pump system without pump D.

In this case the exponential function was used to represent PDF failure over time for both pumps and the electrical system. In this case the dynamic fault tree probability of failure is described by:

$$P(\text{Fire Pump System Out}) = P(\text{FES}) \times P(\text{PE})$$

where  $P(\text{fire pump system out})$ , top event failure probability;  $P(\text{FES})$ , failure electric system probability; and  $P(\text{PE})$ , pump E failure probability.

$$P(\text{FES})(t) = 1 - e^{-\lambda t} = 1 - e^{-0.0000014t} = 1 - e^{-0.0000014(43800)} = 0.059$$

$$P(\text{PE})(t) = 1 - e^{-\lambda t} = 1 - e^{-0.00023t} = 1 - e^{-0.00023(43800)} = 0.9999$$

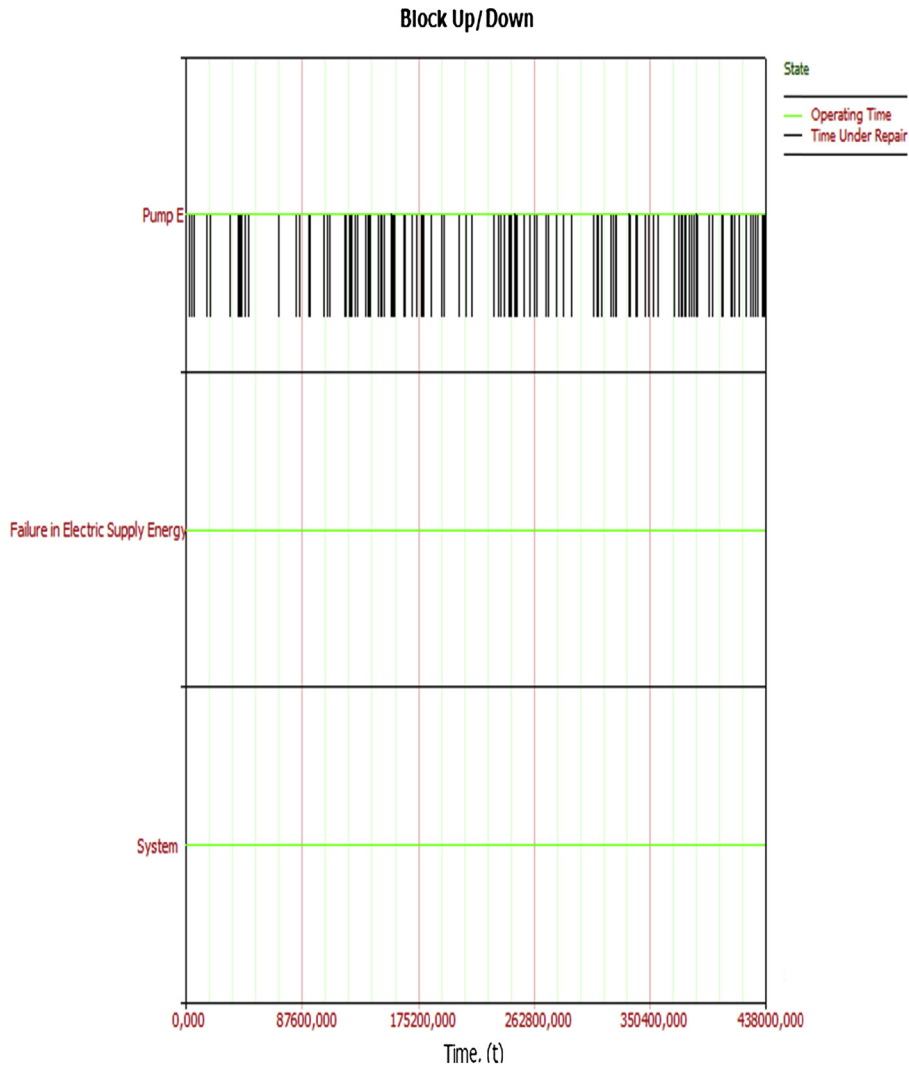
$$P(\text{Fire} \cdot \text{Pump} \cdot \text{System} \cdot \text{Out}) = P(\text{FES}) \times P(\text{PD}) \times P(\text{PE}) = 0.059 \times 0.9999 = 0.06$$

In terms of system probability of failure the situation will not worsen without pump D. Regarding maintenance, action on pump D is performed in the 11th month of the fourth year and takes only 1 h. The system will have 100% of availability as well without pump D, as shown in Fig. 6.59, and if some accident occurs the consequence will not be worse than expected because the fire pump system is available.

The conclusion is that maintenance in pump D is allowed because the whole fire pump system has 100% availability in 1 h (maintenance service duration) and probability of failure is similar with or without pump D (0.06). The simulation regards the system 4 years and 11 months older and operating without pump D.

The PRA methodology proposed is used to provide information to employees to make better decisions with respect to unsafe conditions when layers of protection or contingency systems fail or are out of operation for maintenance. A huge challenge today in the oil and gas industry is achieving safe behavior by employees for preventive action.

Despite difficulties at the beginning of the Brazilian offshore application cases discussed here, risk analysis tools such as LOPA are not widespread in the workforce, even though most employees recognize that it is a feasible methodology and a good approach to help keep processes under control. Whenever this methodology is applied the analysis should be formalized using forms and reports to supply future analysis with data to conduct a complete risk analysis.

**FIGURE 6.59**

Fire pump system simulation (without pump D).

### 6.10.2 CASE STUDY 2: RAMS ANALYSIS METHODOLOGY APPLIED TO MEASURE SAFETY PROCESS EFFECTS ON SYSTEM AVAILABILITY

RAMS (reliability, availability, maintainability, and safety) technology is a recognized management and engineering discipline for the purpose of guaranteeing the specified functionality of a product over its complete life cycle. This is used to keep the operation, maintenance, and disposal costs at a

predefined accepted level, by establishing the relevant performance characteristics at the beginning of the procurement cycle, as well as by monitoring and controlling their implementation throughout all project phases (Vozella et al., 2006).

The general definition of reliability used throughout industry and quoted in many engineering books published on this subject follows the example taken from MIL-STD-785:

- Reliability: The ability of an item to perform a required function under given conditions for a given time interval.
- Availability: The ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.
- Maintainability: A state in that it can perform a required function, when maintenance is performed under given conditions and using stated procedures and resources.
- Risk: An undesirable situation or circumstance that has both a likelihood of occurring and a potential negative consequence on a project.
- Safety: A system state with an acceptable level of risk with respect to:
  - Fatality
  - Injury or occupational illness
  - Damage to launcher hardware or launch site facilities
  - Pollution of the environment, atmosphere, or outer space
  - Damage to public or private property is not exceeded

Most safety processes and reliability are assessed separately for different approaches. To assess safety processes, HAZOP and PHA are most often conducted, and to assess system availability, RAM analysis is conducted. The usual procedures that establish how risk analysis and RAM analysis must be conducted have such analyses separate, even though both analyses drive risk to acceptable levels and the system to achieve the availability target.

Despite effectiveness, when safety and availability are performed apart, it is not possible to know how much safety processes affect system availability. Thus the RAMS analysis methodology proposed is described in Fig. 6.60.

RAMS methodology is similar to the RAM analysis in most steps, but steps 3 and 4 require assessing safety processes and modeling them. In normal RAMS analysis, safety process analysis is taken into account, but their events are not modeled together to know the impact such safety process events have on system availability.

### ***Safety Processes***

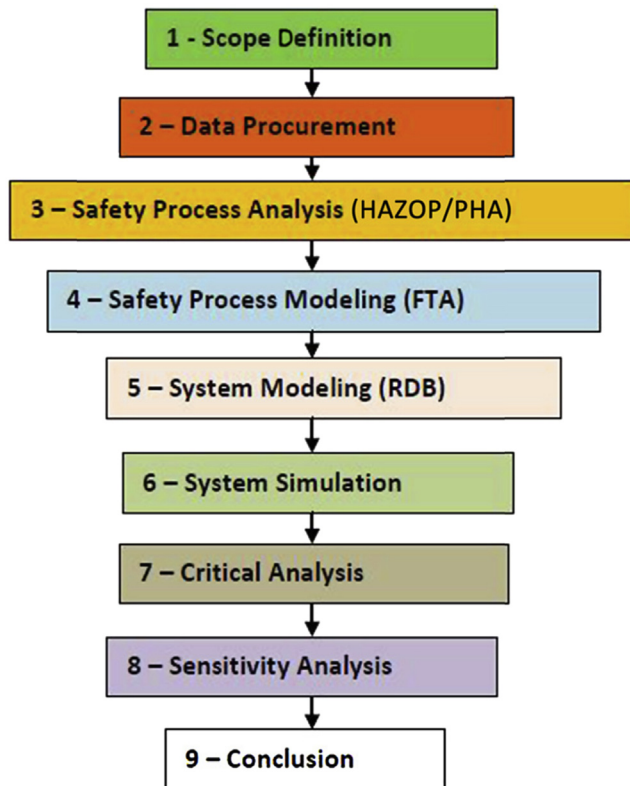
Today, the term safety includes hazard identification, technical evaluation, and the design of new engineering features to prevent loss. Safety, hazard, and risk are frequently used terms in safety processes and include (Crow and Louvar, 2002):

- Safety or loss prevention: The prevention of accidents through the use of appropriate technologies to identify the hazards and eliminate them before an accident occurs.
- Hazard: A chemical or physical condition that has the potential to cause damage to people, property, or the environment.

- Risk: A measure of human injury, environmental damage, or economic loss in terms of both the incident likelihood and the magnitude of the loss or injury.
- Safety process: The prevention of incidents in a process through the use of appropriate technologies to identify the hazards and eliminate them before an accident occurs.

In general, safety processes rely on multiple layers of protection. The first layer of protection is the process design features. Subsequent layers include control systems, interlocks, safety shutdown systems, protective systems, alarms, and emergency response plans. Inherent safety is a part of all layers of protection; however, it is especially directed toward process design features. The best approach to prevent accidents is to add process design features to prevent hazardous situations. An inherently safer plant is more tolerant of operator errors and abnormal conditions (Crow and Louvar, 2002).

Although a process or plant can be modified to increase inherent safety at any time in its life cycle, the potential for major improvements is the greatest at the earliest stages of process development. At these early stages process engineers and chemists have the maximum degree of freedom in the plant and process specifications, and they are free to consider basic process alternatives, such as changes to the fundamental chemistry and technology (Crow and Louvar, 2002).



**FIGURE 6.60**

RAMS analysis methodology.



The major approaches to inherently safer process designs are divided into the following categories (Crow and Louvar, 2002):

- Intensification
- Substitution
- Attenuation
- Simplification

Intensification means minimizing risk whenever possible with less hazardous equipment and products. Substitution means replacing equipment, whenever it is possible, with safer equipment and products. Attenuation means running processes under safer conditions to reduce incidents. Simplification means establishing process controls so that processes are controlled easily in the event of an incident.

Some process incidents are defined with one specific cause, such as a product spill caused by pipeline corrosion. Nevertheless, most process incidents occur as a result of event combinations where process variables (level, temperature, pressure, flow) are out of control. Therefore it is necessary to assess such events systematically, and the best approach to performing this analysis is HAZOP. However, HAZOP does not consider event combinations and such combinations can affect system availability or even trigger an accident. Thus to assess safety process combination events, dynamic FTA is a good tool and can be associated with blocks in system RBDs to find the safety processes impacting system availability.

### RAM Analysis Case Study

To illustrate RAMS methodology a refinery system case study is discussed. Thus for a system that operates for 3 years and then stops for maintenance and achieves 100% availability, such a system does not consider safety process effects.

Thus the main objective is to model such a system regarding safety process effects and find out how much the risk analysis recommendations impact system availability. Fig. 6.61 shows the system RBD without the safety process events.

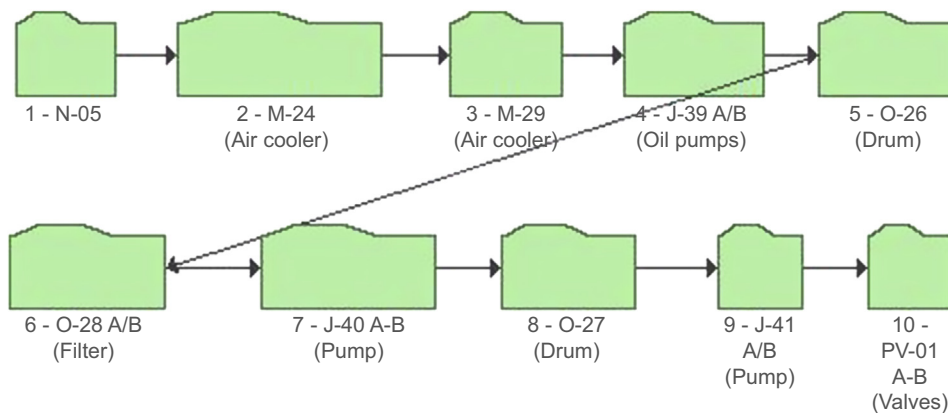


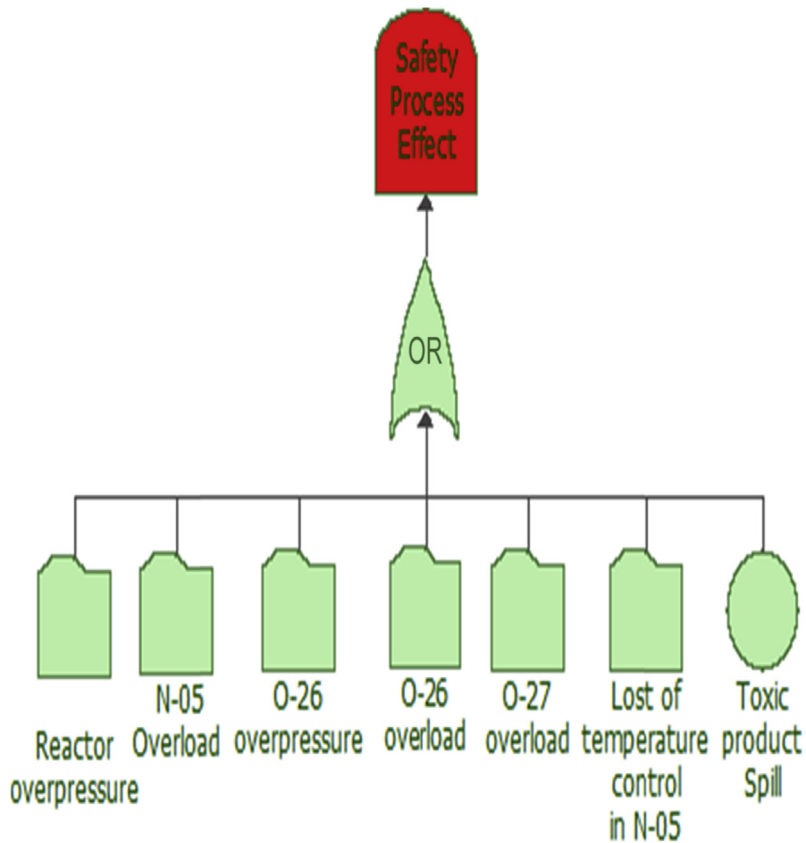
FIGURE 6.61

System RBD.

To identify safety process conditions that affect system availability a HAZOP analysis was conducted and six process deviations were identified:

- Reactor overpressure
- N-05 overload
- O-26 overload
- O-26 overpressure
- O-27 overload
- Loss of temperature control in N-05

In addition, toxic product spill was identified in the PHA and will be included in the FTA model. The next step is to model the safety process FTA, which includes the event combinations that trigger the process deviations and hazards that shut down the plant and impact system availability, as shown in Fig. 6.62.



**FIGURE 6.62**

Safety process effect.

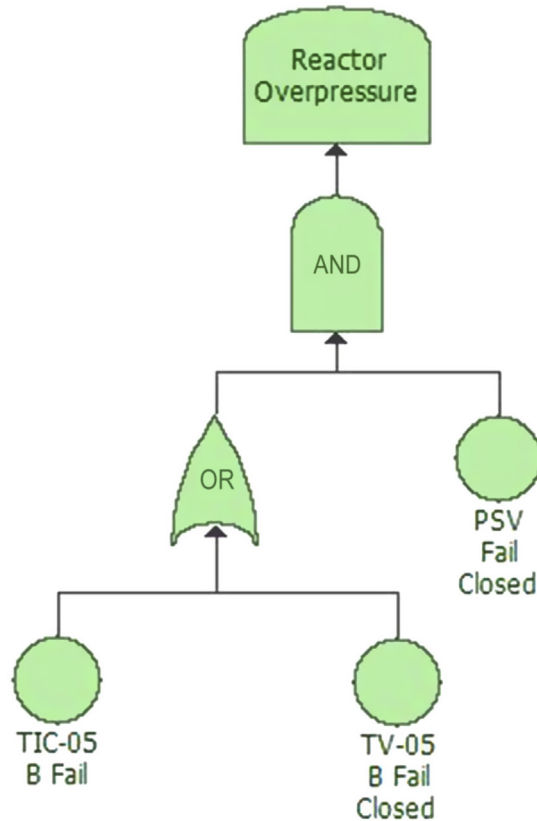


FIGURE 6.63

Reactor overpressure FTA.

Each basic event of the FTA has its own FTA, so in the first case, reactor overpressure occurs if TIC-05 B (temperature control SIF) or TV-05 (valve) fails and PSV (relief valve) also fails, as shown in Fig. 6.63.

In the second case, N-05 (tower) overload occurs if XV-05 B fails (fail closed), or there is an obstruction in the N-05 bottom outlet and also an omission error related to the operator not noticing LAH-12 (high-level alarm) and performing the corrective action, as shown in Fig. 6.64.

In the third case, O-26 (vessel) overpressure occurs if M-24 or PIC-06 or electric energy is unavailable and an operator omission error (PAH-76 or PAH-64), or PSV-05 or PSV-04, occurs. Omission error means that corrective action is not performed because alarms are not detected. The alarms are PAH-76 (high-pressure alarm) or PAH-64 (high-pressure alarm). In addition, if the PSV-64 (relief valve) or PSV-05 (relief valve) fail close together, this can also cause overpressure on O-26, as shown in Fig. 6.65.

In the fourth case, O-26 (vase) overload occurs if LIC-02 (level control SIF) fails or TV-05 (valve) fails to open or HV (valve) fails to open, as shown in Fig. 6.66.

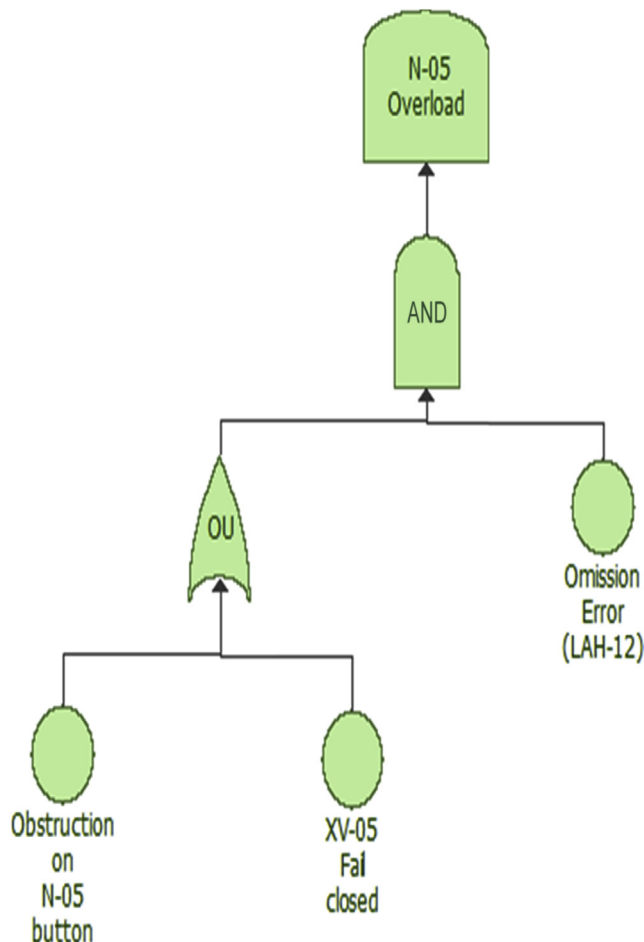
In the fifth case, O-27 (vase) overload occurs if LIC-03 (SIF level control) fails or LV-03 (valve) fails to open or FIC-04 (SIF flow control) fails and also there is an operator omission error (not realize LAH-23 [high-level alarm] and perform corrective action) as shown in Fig. 6.67.

In the sixth case, loss of temperature control in N-05 (tower) occurs if FIC-03 (SIF flow control) fails or TIC-10 (SIF temperature control) fails, and omission errors related to operators do not perceive TAH-08 (high-level alarm), TAH-09 (high-level alarm), and TAH-10 (high-level alarm), as shown in Fig. 6.68.

In addition, safety process effects are included in the FTA for the toxic product spill event. To perform simulation of the RBD for safety process effects failure, PDFs for each FTA basic events are used, as shown in Table 6.11.

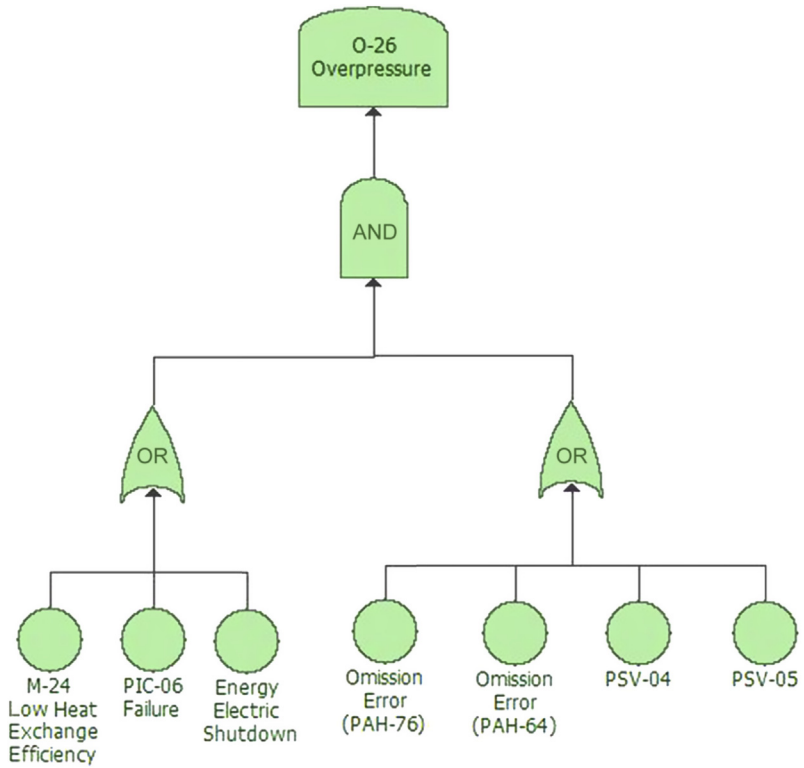
After including safety process effects in the RBD, the new RBD is as shown in Fig. 6.69.

Before the safety process effects the system achieved 100% availability and 99% reliability in 3 years. After the safety process effects, availability achieved 99.88% and 17.5% reliability in 3 years.



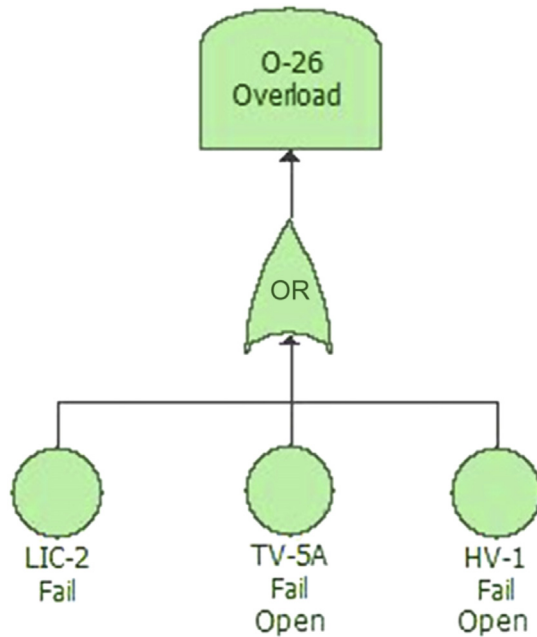
**FIGURE 6.64**

N-05 overload FTA.



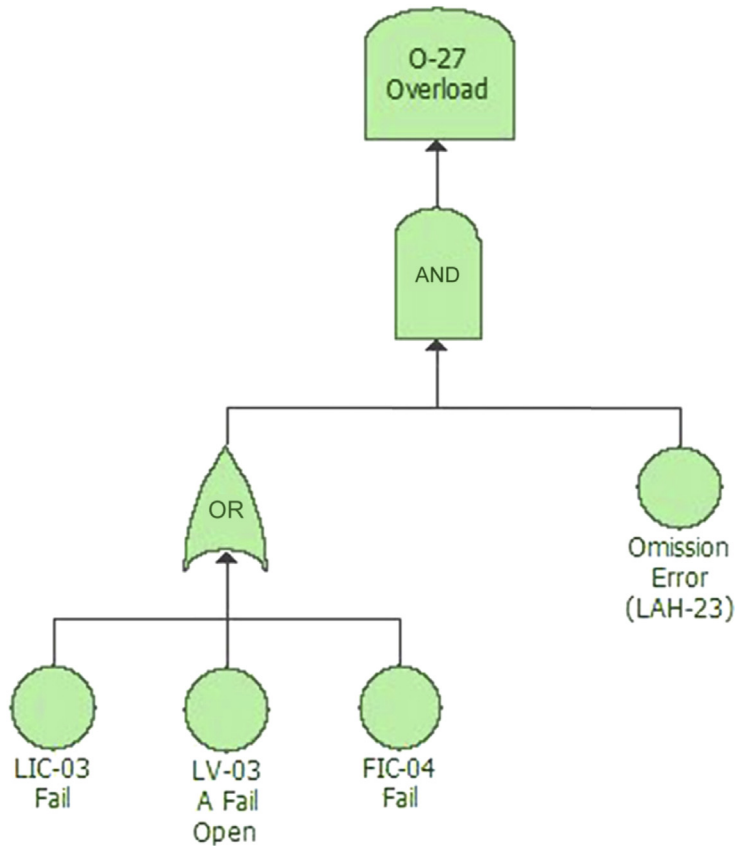
**FIGURE 6.65**

O-26 overpressure FTA.



**FIGURE 6.66**

O-26 overload FTA.

**FIGURE 6.67**

O-27 overload FTA.

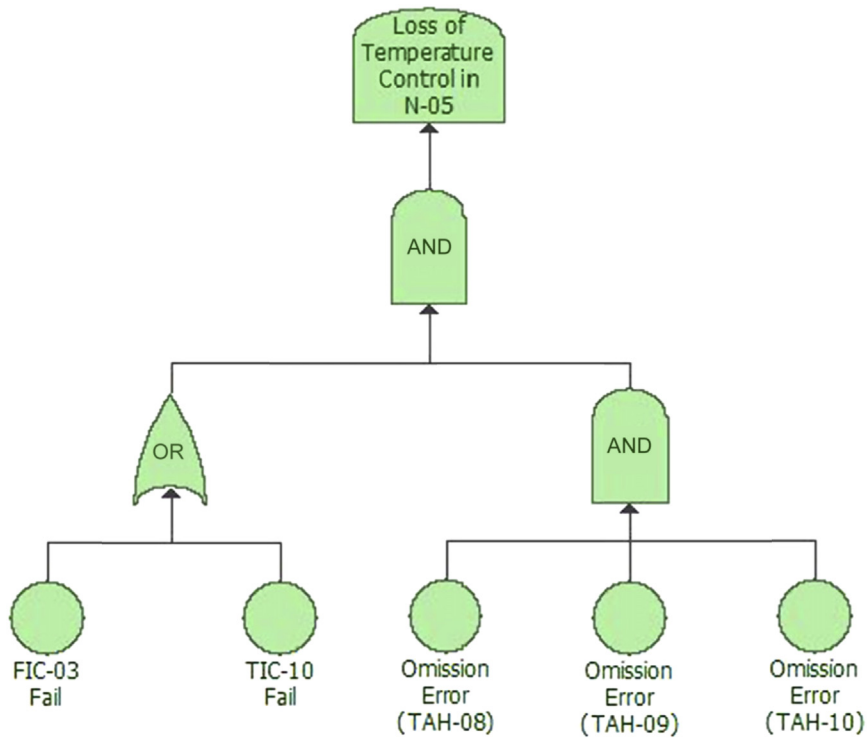
After including safety process effects, one shutdown is expected (expected number of system failures is equal to 1.3).

While availability was hardly affected, reliability reduced too much and the safety process impacts system reliability even more, as shown in Fig. 6.70 and represented by the upper line on the graph. The RI (reliability index) shows how much one subsystem or piece of equipment influences system reliability. In this way, using partial derivation it is possible to know how much it is necessary to increase subsystem or equipment reliability to improve the whole system reliability.

The following equation shows the relation:

$$\frac{\partial R(\text{System})}{\partial R(\text{Subsystem})} = \text{RI}$$

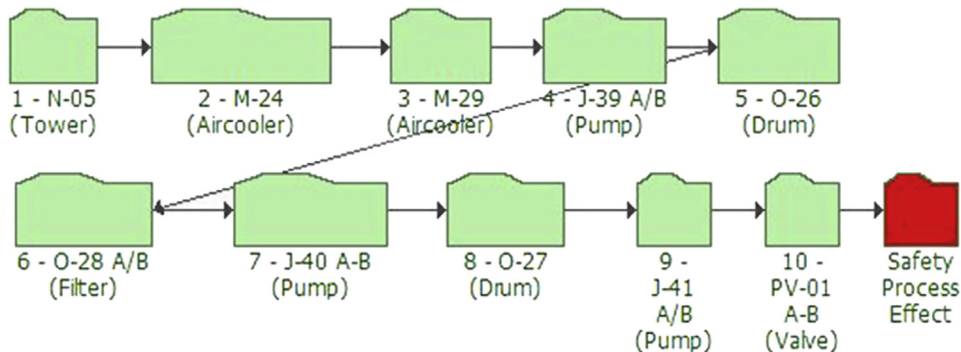
The most critical event in the safety process effects FTA is O-26 overload. In this way, implementing HAZOP recommendations to install alarms for operator effectiveness as the corrective



**FIGURE 6.68**

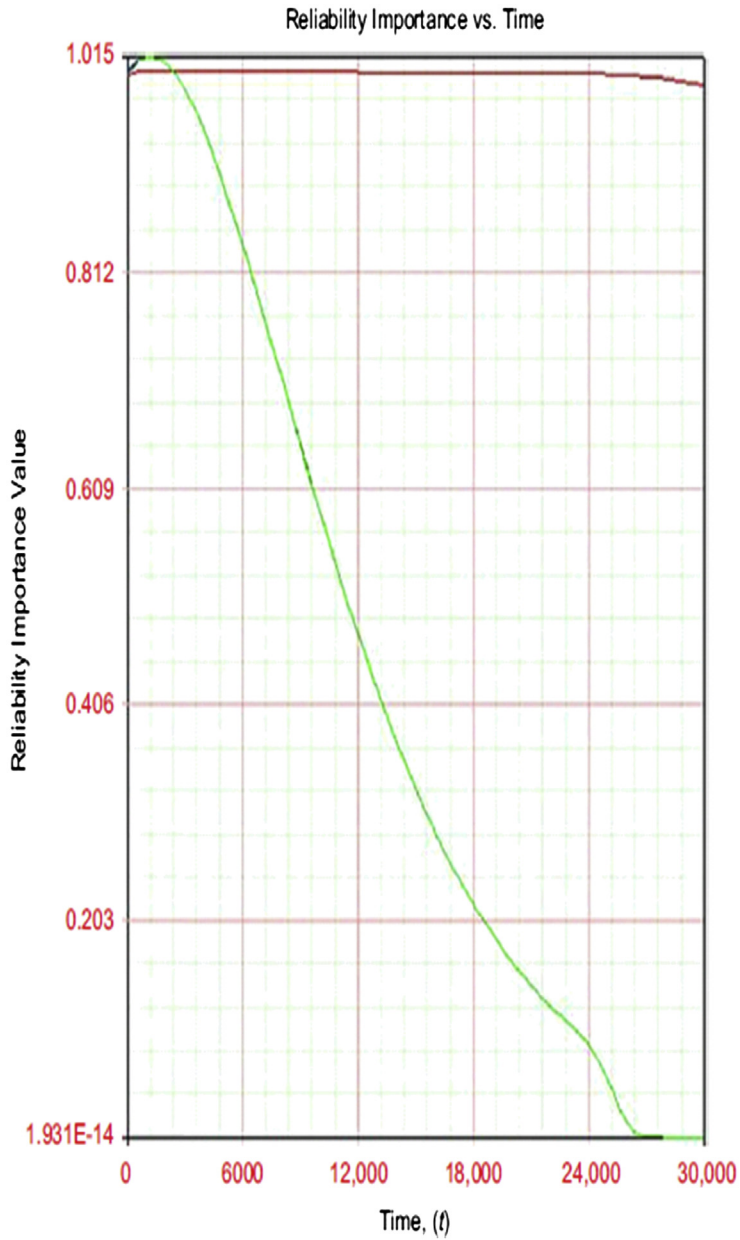
N-05 temperature loss control FTA.

Table 6.11 FTA PDF Parameters			
Equipment	PDF	Parameters	
SIF	Exponential	$\lambda = 0.000012$	
Heat exchanger	Normal	$\mu = 33,000$	$\sigma = 1000$
Valves	Normal	$\mu = 26,280$	$\sigma = 1000$
Human error	Exponential	$\lambda = 0.000038$	
Pipelines	Gumbel	$\mu = 175,200$	$\sigma = 175,200$



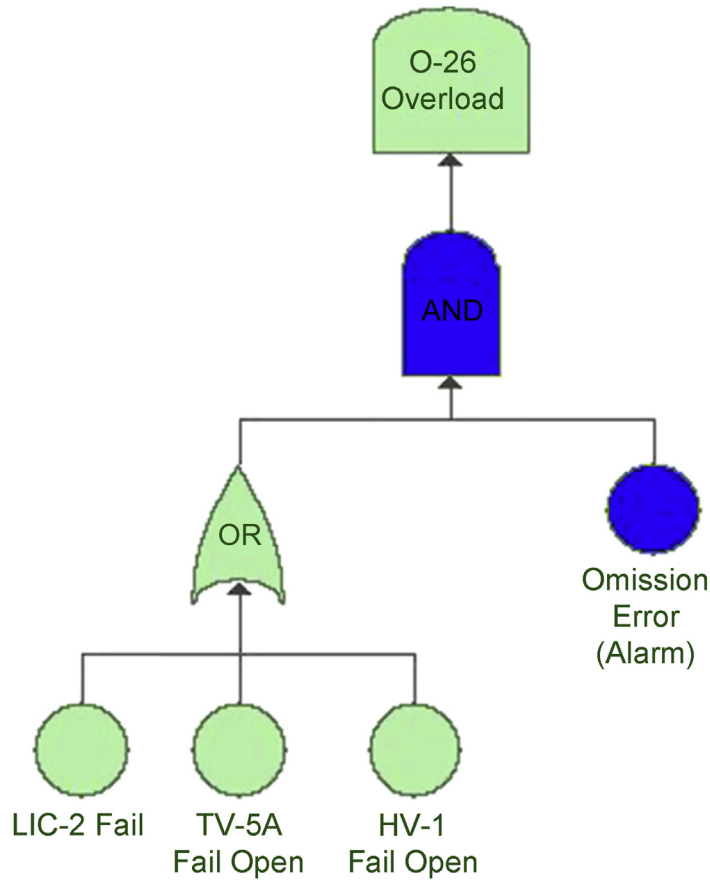
**FIGURE 6.69**

RAMS RBD.

**FIGURE 6.70**

RAMS operational availability and reliability result.





**FIGURE 6.71**  
O-26 overload FTA (a posteriori).

action, system availability achieved 100% in 3 years and reliability of 97.9% in 3 years, with no expected shutdowns in the plant. The new O-26 overload FTA is shown in Fig. 6.71 with the alarm implemented (on right side) with 100% availability and 99.9% reliability in 3 years. Before recommendations, availability and reliability were 99.88% and 17.4%, respectively, with one overload event expected in 3 years.

RAMS analysis methodology includes RAM analysis and risk assessment to find the safety events that impact system availability. While most analysis is complex to perform, the most important point is to model event combinations and put them in the RBD to find out how much the safety process affects system reliability and how much it is necessary to improve it to achieve the system availability target.

Normally in RAM analysis methodology, SIFs, alarms, and valves are not considered in the RBD because there is no historical data that shows that such data impacts system availability. However, the only way to find out how much a safety process impacts system availability is to model the event combinations. In addition, you can also see if it is necessary to implement all recommendations proposed in qualitative risk analysis such as HAZOP and PHA.

The case study shows only one recommendation was needed to reestablish system availability and reliability.

### 6.10.3 CASE STUDY 3: SHUTDOWN EMERGENCY VALVE RISK ANALYSIS: FTA, BOW TIE, AND HRA INTEGRATED APPROACH

The purpose of this case study is to demonstrate hybrid risk analysis, including human reliability analysis, bow tie, and fault tree analysis. Therefore the case study focuses on a shutdown caused by the spurious closure of an emergency shutdown valve (ESDV) on a transfer line leading to zero flow through that line. The purpose of the case study is to determine whether there is smooth operation following the trip of a single CRM (Condensate Rich MEG; MEG = ethylene glycol) line and identify any consequential process trips.

Fig. 6.72 shows that when ESDV closes, the mass flow through the east transfer line drops to zero. The total mass export rate also falls, before recovering to a flow rate of around 530,000 kg/h, which is lower than the initial total export flow of around 690,000 kg/h.

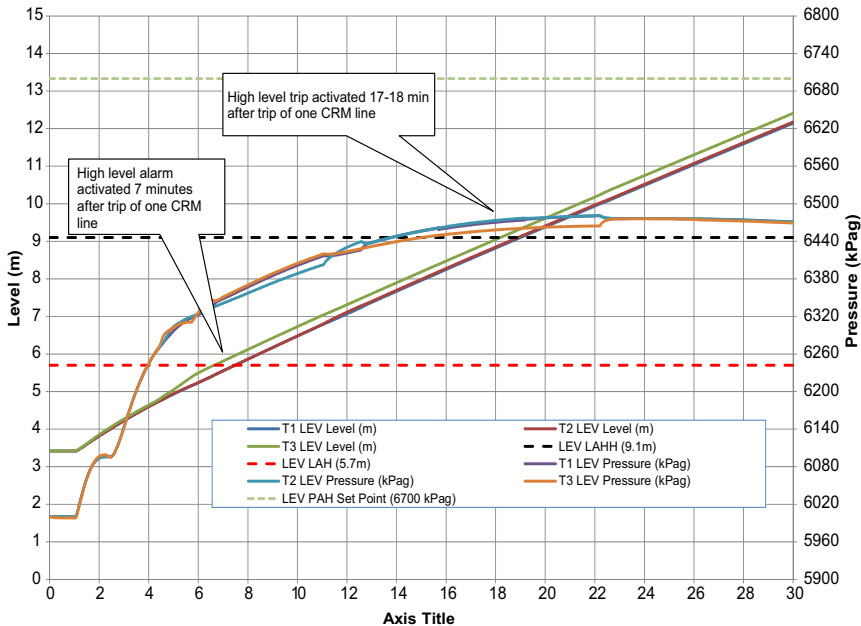


FIGURE 6.72

CRM transfer line flow and pressure.

Fig. 6.72 is a result of dynamic simulation, which considers the following sequence of events. At:

$T = 0$  min, initial conditions as above.

$T = 1$  min, ESDV at transfer line inlet close with a closure time of 12 s.

$T = 17$  min, liquid level in the three Liquid Export Vessels (LEVs) will reach the Level Trip High High (LZHH) trip set point with a single flow line operating. The trip actions were not simulated as part of this run.

$T = 30$  min, simulation ends.

### ***Human Reliability: Standardized Plant Analysis Risk-Human Reliability (SPAR-H) and Accident Sequence Evaluation Program (ASEP) Application***

Human reliability analysis qualifies the human intervention in terms of the probability of the operator making an error and consequently leading to a total plant shutdown. This section effectively calculates the frequency of total shutdowns incurred as a result of this scenario when relying on a specific operator action.

The error is effectively the operator either:

- Missing completely the first-out alarm that came up, that is, the high pressure at the inlet of the CRM, that is, an omission error (Appendix A); or
- Recognizing the alarm but not performing the correct action as per the procedure, that is, commission error (Appendix A).

Note that for the former omission error it takes a single operator, that is, the control room operator, to miss the alarm.

In addition, the latter commission error involves both the control room and the field operator. The scenario is as follows.

It is expected that by time  $t = 14$  min (10 min from the first alarm) the operator should be able to understand the issue and the root cause. In this time the operator has, however, been receiving continuous alarms since the incident that may either impede (distract) or enhance his judgment. He is expected to receive at least five alarms in that period, that is, the two high-pressure CRM alarms and the three high-level LEV alarms.

Internal procedures and system set up allows the operator 10 min to react to an alarm. So, by this time he will try to contact the field operator to fix the problem and open the valve.

The field operator, if he is close to the valve, can try to open it locally. If the valve does not open he will call the control room operator to explain the issue. It is assumed here that the valve cannot open or reset from the control room because it is a shutdown valve. It can only be opened or reset from the field.

If the field operator happens to be away from the valve, it is impossible to react to any instructions within 10 min.

The control room operator has to coordinate the actions of the field operator with his decision to trip or not the single train following the procedure. If the time since the alarm approaches 10 min, then he needs to trip the train.

Tripping the train involves pressing two physical emergency shutdown (ESD) pushbuttons that are located very close to the operator console. One for the LEP/LEV trains and one for the production train.

The commission error in steps (a) – (c) can be one of the following.

The control room operator forgetting that he needs to act within 10 min, that is, neglecting the procedure.

The control room operator does recognize the alarm long after it occurred, say 5 min. He does not realize that the time to act is less than 10 min, that is, only 5 min because the alarm activated long before he acknowledged it.

The field operator starts talking to the control room operator about other issues, which diverts his attention.

Another incident happens that also diverts the attention of the control room operator.

The control room operator does everything right, but presses the wrong ESD pushbutton and either does not trip any of the trains or he trips the whole plant.

Computation of the probability of error is as follows.

- Omission Error Probability

The omission error probability is computed using the ASEP method. Fig. 6.73 suggests that a 10-min response time leads to a 60% failure rate.

The same result can be obtained by using the SPAR-H method. Based on Tables 6.1 and 6.2, NHEP = 0.13 for a simple task performed rapidly (task type: D), which is recognition of the alarm and the action to trip one train in 10 min. The NHEP is 0.13, that is, the upper bound of category D. The task is not complex (pressing a single physical pushbutton), and there is no reason to suggest that

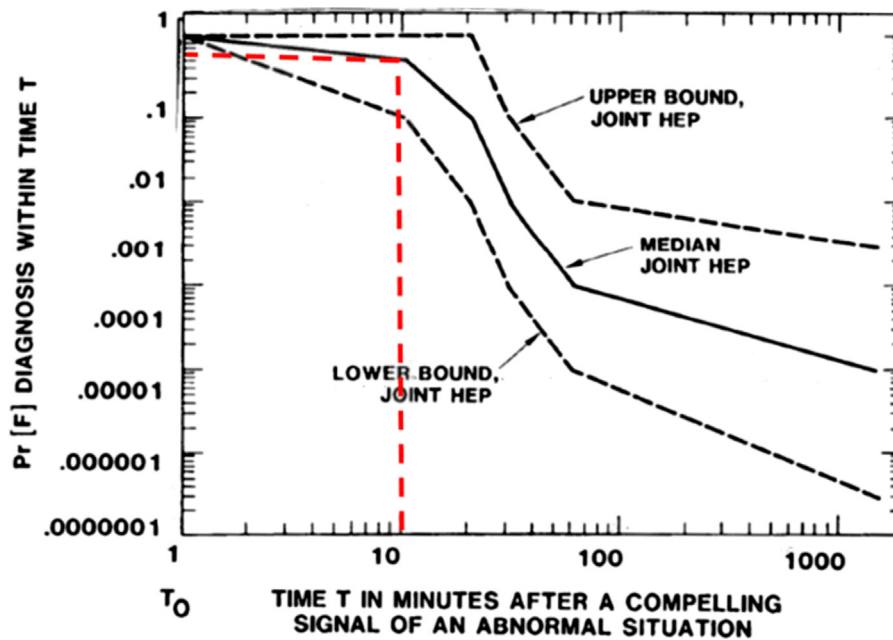


FIGURE 6.73

Nominal diagnosis model (estimate HEPs and UCBs for diagnoses within time). HEP, Human Error probability; UCBs, uncertainty bounds.

procedures, training, and ergonomics are not in place for such an activity. The available time is, however, the same as the required time if in 10 min we include the diagnosis. High stress is not considered, because prior to the CRM blockage it is assumed that there has not been any other incident.

### **SPAH-R: Commission Error Probability**

There are clearly two potential errors here, one for the field operator and one for the control room operator.

The rate of failure of the commission error is computed based on the SPAR-H method (Appendix A). The PFS values considered for the field operator error probability are shown in Table 6.15 along with the justification. The PFS composite is predicted as shown in the following equation:

$$\begin{aligned} \text{PFS}_{\text{composite}} &= \text{PFS}(\text{available time}) \times \text{PFS}(\text{Stress}) \times \text{PFS}(\text{complexity}) \\ &\quad \times \text{PFS}(\text{Experience/Training}) \times \text{PFS}(\text{Procedures}) \times \text{PFS}(\text{Ergonomics}) \\ &\quad \times \text{PFS}(\text{Fitness for duty}) \times \text{PFS}(\text{Work process}) \end{aligned}$$

$$\text{PFS}_{\text{composite}} = 1 \times 2 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 = 2 \quad [2]$$

For the control room operator error, Table 6.16 illustrates the PSF. The PFS composite predicted is:

$$\begin{aligned} \text{PFS}_{\text{composite}} &= \text{PFS}(\text{available time}) \times \text{PFS}(\text{Stress}) \times \text{PFS}(\text{complexity}) \\ &\quad \times \text{PFS}(\text{Experience/Training}) \times \text{PFS}(\text{Procedures}) \times \text{PFS}(\text{Ergonomics}) \\ &\quad \times \text{PFS}(\text{Fitness for duty}) \times \text{PFS}(\text{Work process}) \end{aligned}$$

$$\text{PFS}_{\text{composite}} = 10 \times 5 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 = 50$$

The next step is to calculate the HEP. To calculate the human error probability it is necessary to define the nominal human error probability. Based on current SPAR-H procedures, the NHEP for commission error is 0.001. In fact, this value defined by the standard is very low and will not reflect the human error during the early life phase. In the case of the operational phase, such value can be applied to predict the HEP. To define the NHEP, the early life phase will be applied based on the human error assessment reduction technique.

Based on the Human Error Assessment Reduction technique (HEART) nominal human error definition, the respective task and human probability error are:

$$\text{Field Operator Action} - \text{task B} - \text{NHEP} = 0.14$$

$$\text{Control room operator Action (commission error)} - \text{task F} - \text{NHEP} = 0.007$$

Thus the field operator action error and control room operator action error are:

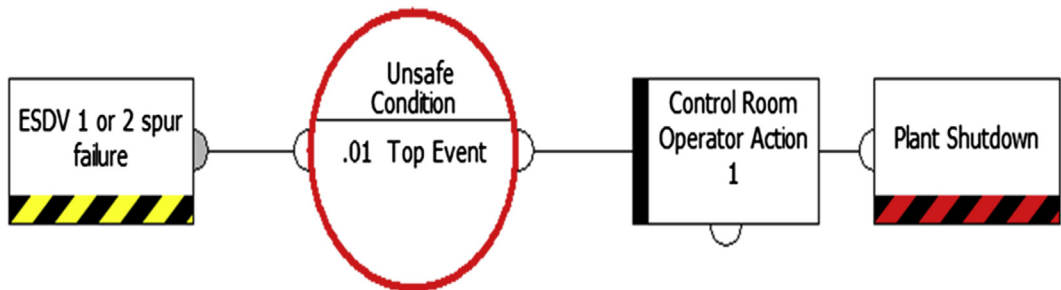
Field operator action error:

$$\text{HEP} = \frac{0.14 \times 2}{0.14 \times (2 - 1) + 1} = 0.25 = 25\% \quad [5]$$

Control room operator action (after field operator fails to recover):

$$\text{HEP} = \frac{0.007 \times 100}{0.007 \times (100 - 1) + 1} = 0.26 = 26\% \quad [6]$$

The decision whether to trip one train and perform it correctly is contingent on the control room operator. As a result, it is highly unlikely that the field operator error will influence the decision making



**FIGURE 6.74**

Scenario 1—Detection mistake (omission error).

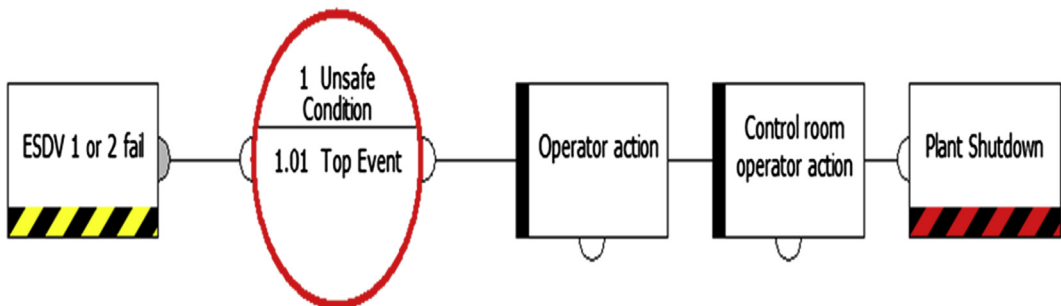
of the control room. As a result, for the frequency of shutdowns only control room operator (6) unreliability will be considered.

### ***Bow Tie Case Study Application***

The next step is to calculate the frequency of shutdowns caused by this scenario, that is, CRM inlet valve closure, while accounting for human reliability. Bow tie analysis will be applied in this SIF risk analysis. The main objective predicts the frequency of plant shutdown/year considering the human error of the operator and control room operator in different recovery action scenarios.

The frequency of ESDV failure is considered as one per year based on the internal company database. The failure rate of a single component is significantly lower than 1 per year ( $1 \times 10^{-2} - 1 \times 10^{-4}$ ) depending on the SIL level. However, when considering the combination of components and also the chance of human error, this rate can indeed be close to one failure per year. Note there are two identical trains, hence two of the CRM valves can fail closed. Such frequency can also be calculated based on real failure historical data. Consequently, once such data is available a lifetime data analysis is required.

The combined valve failure rate and operator reliability calculations are shown in [Figs. 6.74 and 6.75](#).



**FIGURE 6.75**

Scenario 2—Field operator not recovering and control room operator recovery action not successful.

$$\begin{aligned}
 F(\text{System Shutdown}) &= F(\text{ESDV Train 1 or Train 2 Fails}) \\
 &\quad \times P(\text{Control Room Operator action Fails}) \\
 &= 2 \times 0.6 = 1.2 \text{ Plant Shutdown/year} \quad [7]
 \end{aligned}$$

$$\begin{aligned}
 F(\text{System Shutdown}) &= F(\text{ESDV 1 or 2 Fails}) \times P(\text{Field Operator action Fails}) \\
 &\quad \times P(\text{Control Room Operator action Fails}) \\
 &= 2 \times 1 \times 0.26 = 0.52 \text{ Plant Shutdown/year} \quad [8]
 \end{aligned}$$

As the field operator action is a failure (did not manage to open the valve), it is considered as one contribution to the event failure rate.

The omission error is independent of the commission error. Hence the combination of the two needs to be considered to calculate the total failure rate.

Scenario 3—Detection mistake (omission, error) or operation recovery action mistake (commission error).

### ***FTA Case Application***

This analysis encompasses scenarios 1 and 2, which are best represented by an FTA. The FTA is a quantitative deductive method that identifies top events and incidents or accidents or the combination of events that trigger top events. Such combinations are defined by logic gates, based on Boolean logic, which define the combination of basic events. Such combinations can be represented by logic gate OR or by logic gate AND.

Case 1—Omission or commission error.

Scenario 4 will take into account scenario 1 (omission error) or scenario 2 (commission error) results (plant shutdown/year) for the FTA basic events. The final result is 1.12 shutdowns/year. The FTA is demonstrated in Fig. 6.76, which shows the combination and omission and commission error.

### ***Hybrid Method Case Application***

The complete hybrid diagram, which encompasses both FTA and bow tie, is represented in Fig. 6.77. This implies one shutdown every year because of CRM valve failure, which occurs once a year. However, given that there are two CRM lines and hence valves, the chance of any of them failing is once every year, that is, twice a year. Operator contribution manages to reduce the impact of the plant shutdown to once every year, that is, a twofold improvement. However, if the valve failure rate changes, the operator performance is expected to change. More frequent valve failures will render the operator more familiar with the procedure, which will minimize error. A rare valve failure may catch the operator unaware and oblivious to the procedure he has to follow if the adverse event occurs.

From this analysis it can be deduced that an automated system is required to prevent the plant-wide trip following the CRM inlet valve inadvertent closure. Relying on the operator will not reduce the shutdown rate significantly. The automated system can take a combination of measurements and with a time delay send a signal to trip train 1 LEV/LEP and train 1 of the gas production side (Inlet Surge Vessel (ISV), High pressure (HP) separator, etc.). The logic recommended is: If pressure at CRM is measured by PZT-109A/B/C (receiver B), the inlet is high (above alarm of 7500 kPag), and the CRM ESDV-094 or 078 (receiver B) is closed, then after a delay of 10 min trip train 1. The pressure transmitter is already wired in the ESD, while it has to be ensured that the ESDV limit switches are also wired to the ESD.

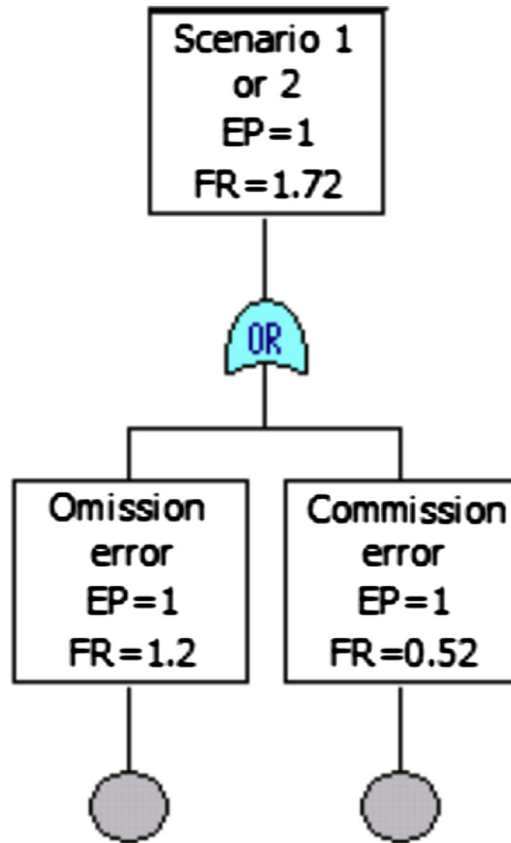


FIGURE 6.76

FTA for omission or commission error.

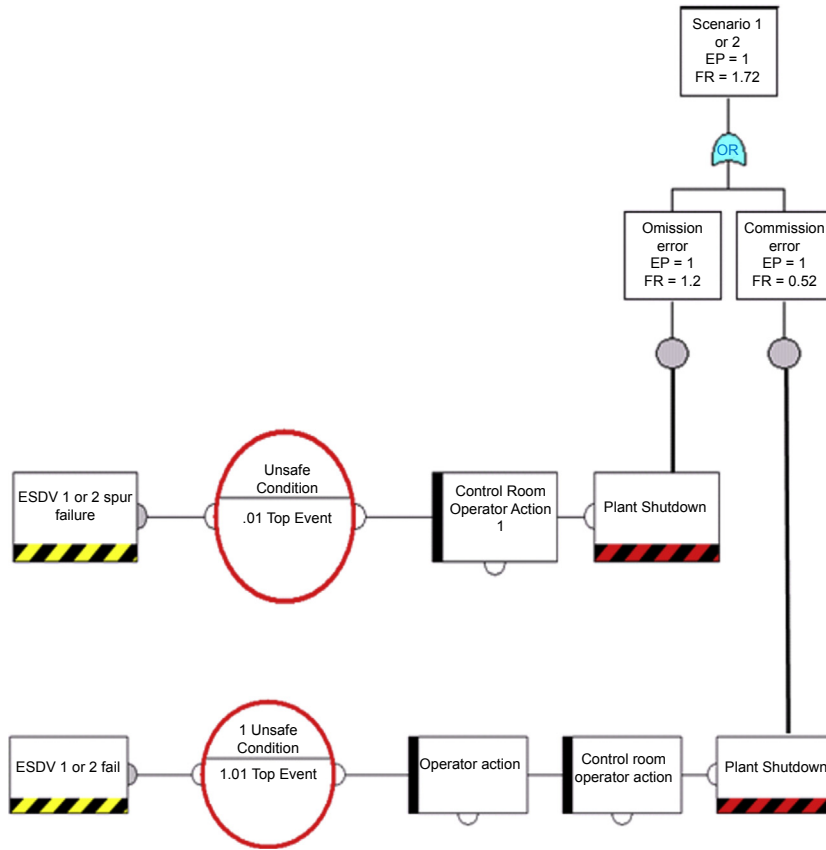
### Conclusions

Based on the sensitivity analysis to avoid cascade trips on all CPF trains following a CRM line inlet blockage, it is recommended to:

1. Reduce the high-pressure alarm setting at the inlet to the CRM from 7800 kPag to 6200 kPag in the low-pressure mode to alert the operator about the CRM blockage. Otherwise the response time becomes closer to the available time increasing 10-fold the probability of operator failure.
2. Make sure the operator knows that if a high-pressure alarm at the inlet of the CRMs is triggered there is no blockage in the CRM lines. If the blockage is confirmed and cannot be recovered, that is, unblock or reopen the failed valve, the operator has 20 min from the alarm activation to trip one of the trains to prevent multiple train trips.

By implementing recommendations 1 and 2 there is a 0.332 frequency of total plant shutdown following the upset, provided the single ESDV has a combined failure rate of one per year.





**FIGURE 6.77**  
Complete hybrid bow tie diagram.

Hybrid risk analysis performs a complete assessment, which encompasses equipment failures or incident events together with human error. The next step is to consider the dependency on time event when BTA and FTA are performed to mitigate risk over time.

#### 6.10.4 CASE STUDY 4: BLOWOUT ACCIDENT ANALYSIS BASED ON BOW TIE METHODOLOGY

On the evening of April 20, 2010, a gas release and subsequent explosion occurred on the Deepwater Horizon oil rig working on the Macondo exploration well for BP in the Gulf of Mexico. Eleven people died as a result of the accident and others were injured. We deeply regret this loss of life and recognize the tremendous loss suffered by the families, friends and co-workers of those who died.

The fire burned for 36 h before the rig sank, and hydrocarbons leaked into the Gulf of Mexico before the well was closed and sealed.

Based on the BP accident summary report (<http://www.bp.com/>), the eight key findings related to the causes of the accident are:

1. The annulus cement barrier did not isolate the hydrocarbons.  
The accident investigation team concluded that the migration of hydrocarbons happened because the cement was out of the design specification.
2. The shoe track barriers did not isolate the hydrocarbons:  
The accident investigation team concluded that the hydrocarbon ingress into the production casing happened because of functional failure in both shoe track cement and the float collar which allowed.
3. The negative-pressure test was accepted.  
During the negative-pressure test, the pressure readings and volume bled at the time of the negative-pressure test were indications of flow-path communication with the reservoir, showing that integrity had not been achieved.
4. Influx was not recognized until hydrocarbons were in the riser.  
The hydrocarbon influx was not detected and the team took preventive actions to control the well after hydrocarbons had passed through the BOP and into the riser.
5. Control response actions failed to regain control of the well.  
Despite the team closing the BOP and diverter, the fluids were not routed to the overboard diverter line.
6. Diversion to the mud gas separator resulted in gas venting onto the rig.  
The mud gas separator was diverted to the MGS and increased the chance of ignition.
7. The fire and gas system did not prevent hydrocarbon ignition.  
Hydrocarbons migrated to electrically classified areas with a high chance of ignition.
8. The BOP emergency mode did not seal the well.

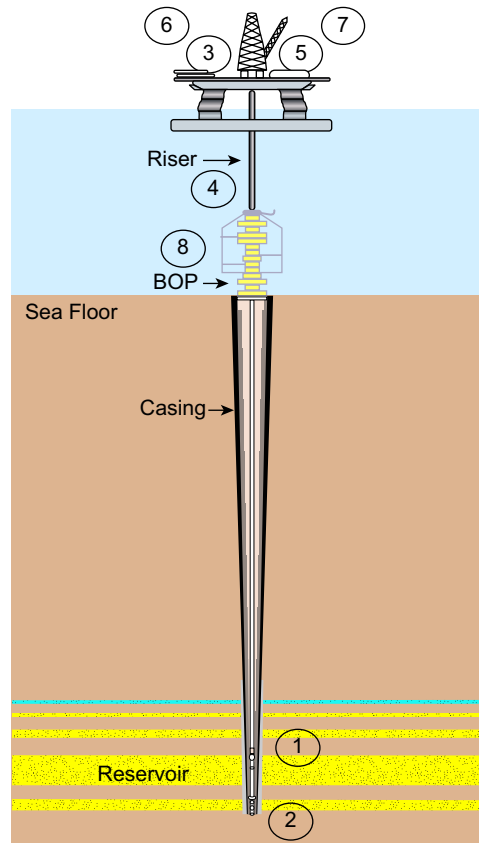
Three methods for operating the BOP in the emergency mode failed to seal the well.

The blowout accident took place on December 31, 2011 and demanded a huge contingency response, which involved government and local residents. Such contingency response cost \$14 billion, environmental impact, as well as employee deaths. Fig. 6.78 shows the Deepwater Horizon oil rig components that failed.

The accident method that was used to represent and understand the sequence of events that triggered the blowout was the Accident Sequence Analysis, as shown Fig. 6.79. Although the events that led to the accident are clear, it is also important to understand why such events happened, to prevent them happening in the future. In this way, each event can be considered as a top event and a combination of events that triggers such events can be assessed by FTA methodology, as defined in event 2 and 8 in Fig. 6.79.

The Accident Sequence Analysis can successfully represent the events that led to the blowout, as shown in Fig. 6.79.

We can conclude that even for a system that has a high level of layers of protection with an accident probability that is very low, it is always possible that such events will happen. In addition to safety systems the big challenge is to keep such a system at a high level of safety and this depends upon design, reliable equipment, reducing the chance of human error, as well as monitoring constantly the cut set event conditions. In the nuclear industry, such cut set conditions are monitored constantly, but



**FIGURE 6.78**

Events that triggered the accident.

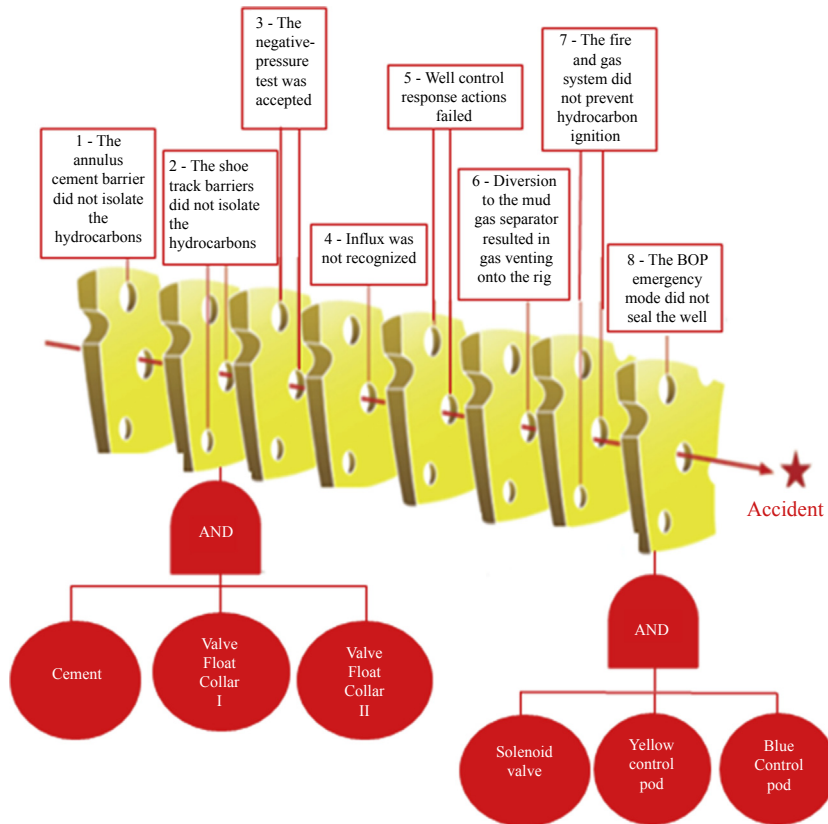
Source: [www.bp.com.br](http://www.bp.com.br).

even under such circumstances, external events like natural catastrophes can change the safety level and trigger an accident such as the one that happened at the Fukushima nuclear plant.

### 6.10.5 CASE STUDY 5: SAFETY INTEGRITY LEVEL RISK ASSESSMENT: SIL SELECTION AND VERIFICATION ANALYSIS

SIL analysis has the main objective of proposing a SIF as a layer of protection to mitigate risk. Therefore SIL analysis is part of risk assessment that takes place after hazard identification and risk analysis. In fact, SIL analysis is part of risk evaluation, which enables the best decisions to be made about the SIL of the SIF to mitigate the risk to tolerable levels.

The main discussion is about different alternatives between implementing SIF with an SIL level or alternative layers of protection to mitigate the risk.



**FIGURE 6.79**

Accident Sequence Analysis + FTA.

In fact, this all depends on safety system configuration and a layer of protection reliability over time. Therefore there is no standard solution, but different options that need to be discussed. To make the risk mitigation decision easier, it is necessary to identify all types of possible layers of protection as well as the PFD for each one.

This case study has the main objective of presenting a methodology that compares different solutions to mitigate the risk based on the concept of risk mitigation target, which can be achieved by implementing a single SIF with different layers of protection including SIF.

The risk mitigation target is a value defined by the difference between acceptable risk and current risk provided by risk analysis. Therefore different alternatives emerge that implement different types of layers of protection, which may include or not the SIF. Once again, such a decision depends not only on the risk mitigation target, but also on the layer of protection PFD as well as the layout, logistics, and technology in place.

The important fact is that the higher the SIL of SIF, the less alternative layer protection is required to achieve the risk mitigation target. However, the less the SIL of SIF, the more alternative layers of protection are required to achieve the risk mitigation target. The important issue to be considered in such a decision is the vulnerability of safety when relying on an individual layer of protection or small number of layers of protection. In addition to this is the necessity of performing preventive maintenance and tests to recover the layer of protection reliability and also verify device availability. Therefore the safety protection configuration needs to be sufficiently reliable to allow preventive maintenance or inspection intervention in one or more layers of protection without jeopardizing the risk mitigation target. Fig. 6.80 shows different safety protection alternatives concerning the combination of SIF with different SIL levels and alternative layers of protection.

The important step when performing SIL assessment is to identify the current layer of protection and its PFD. Therefore, based on remaining risk, it is possible to assess which SIL level is required to

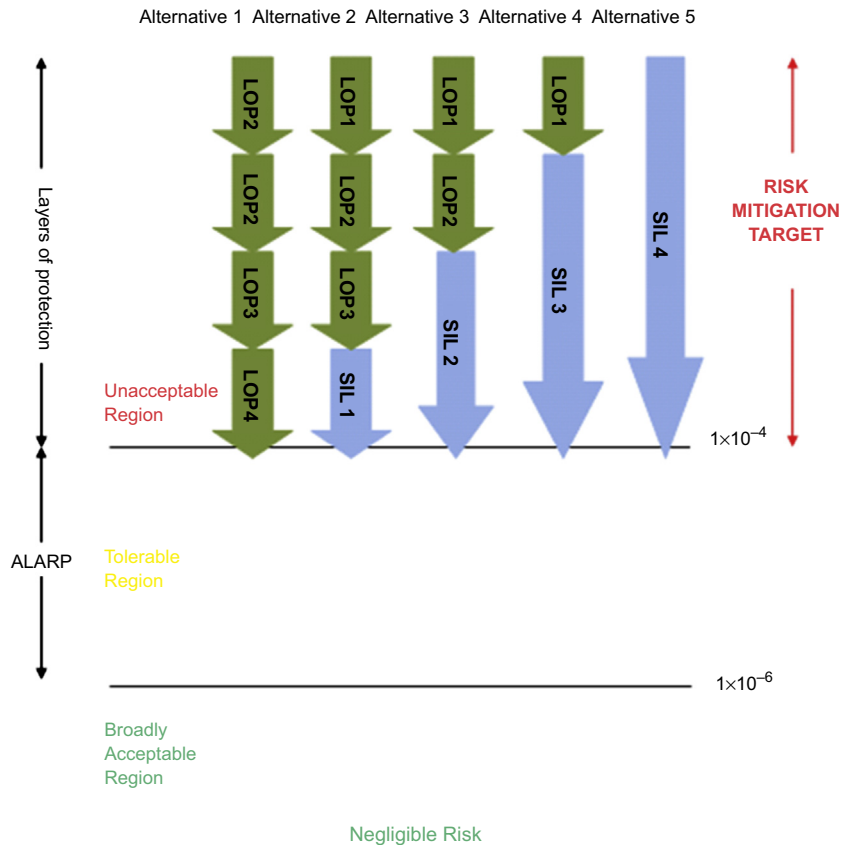


FIGURE 6.80

Risk mitigation target.



HAZARD IDENTIFICATION (HAZID)																						
System: Platform						HAZID Leader: Eduardo Calisto						DATE: 10/07/2013										
SUBSYSTEM: 1.1 - Separation			Node: From the Tie in to Separation Vessels, including Valve (PRV-01), pipelines, Pumps (P-5501) and vessels (V-5501 A/B)						Document: 551001-002-01 - A1 Rev-B DE													
HAZARD	CAUSES	CONSEQUENCE	PREVENTION	F	Safety		Asset		Env		Image		Recommendation	F	Safety		Asset		Env		Image	
					S	R	S	R	S	R	S	R			S	R	S	R	S	R	S	R
Huge gas Leakage	- Pipeline ruptures caused by external impact			D	IV	NT	IV	NT	IV	NT	IV	NT	R01) To monitor maintenance service on top of the platform. Action by: maintenance	A	IV	M	IV	M	IV	M	IV	M
	- Pipeline or vessel corrosion	- Explosion - Fire - Underground sea contamination	- Pipe and vessel Integrity - Process high pressure Alarm	C	IV	NT	IV	NT	IV	NT	IV	NT	R02) To implement NDT (Ultrasound test) to detect corrosion	A	IV	M	IV	M	IV	M	IV	M
	- Rupture caused by high pressure	- Heaths damage - Equipment Damage	- PCS - PRV	D	IV	NT	IV	NT	IV	NT	IV	NT	R03) To implement an additional layer of protection (SIF) to mitigate the risk.  R04) To implement SIL assessment (Selection and verification). Action by: Project	A	IV	M	IV	M	IV	M	IV	M

FIGURE 6.81 Separator vessel HAZID.

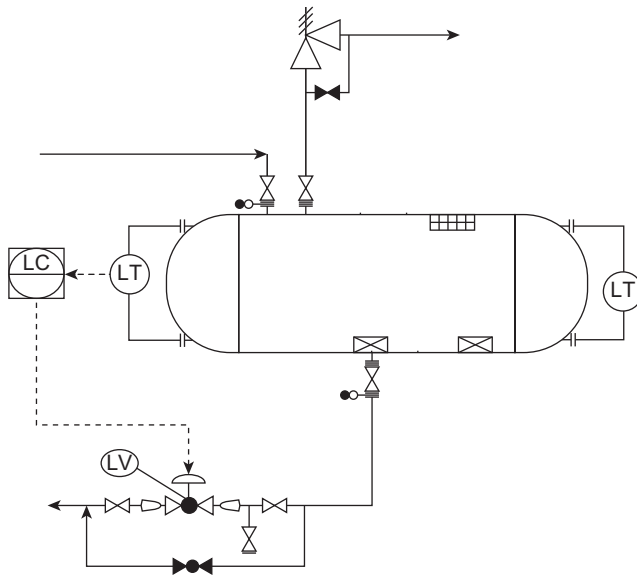
high flow frequency, which cause high pressure and layers of protection probability. Based on Fig. 6.83 the PFD are:

- High flow ( $f = 1$ );
- Process control system ( $PFD = 1 \times 10^{-1}$ );
- Relief valve ( $P = 1 \times 10^{-2}$ ).

Fig. 6.83 shows the layer of protection analysis to calculate the risk. The risk target is provided based on the risk matrix demonstrated in Fig. 6.84. A further step is to perform SIL analysis to select the SIL level. Based on LOPA, SIL 2 or SIL 3 ( $1 \times 10^{-3}$ ) is necessary to achieve the risk mitigation target.

### SIL Selection

As described in Section 6.8, SIL analysis has four different methods to perform SIL selection. The ideal situation is to perform more the one assessment based on the four SIL methods to assure

**FIGURE 6.82**

Separator vessel.

result consistency. Therefore the risk matrix and risk graph will be performed as part of SIL selection for the separator vessel hazard assessment.

### Risk Matrix

In case of SIL assessment the risk matrix method has a defined category for probability and consequence, and such criteria have qualitative definitions, as shown in [Tables 6.13 and 6.14](#), respectively. Such matrix definition is compared with the risk matrix defined in [Fig. 6.86](#).

The SIL value for the SIF related to the huge gas leakage caused by high pressure on the separator vessel can be assessed based on [Tables 6.13 and 6.14](#). The SIL value is defined based [Fig. 6.85](#), which defines the risk matrix with the number of layers of protection. Therefore SIL 2 is selected to mitigate the risk concerning the existence of two layers of protection as well as moderate likelihood and an extensive severity.

### Risk Graph Method

As discussed before in this chapter, this methodology selects SIL based on different accident scenario criteria such as consequence, occupancy, avoidance, and safety demand. Each one of such criteria has a different classification as described next. Such criteria are applied to a graph to define the SIL level, as demonstrated in [Fig. 6.86](#).

The consequence criterion takes into account the severity of health damage caused by an accident. The PLL is also a parameter to specify the consequence of the PLL. The consequence is classified into four levels:

- Ca (minor injury);
- Cb ( $0.01 < PLL < 0.1$ );



<b>Accident Scenario Number</b>	<b>Equipment</b>		
1	Separator Vessel		
<b>Date</b>			
15/07/2013			
<b>Consequence description</b>	Huge Gas leakage		
<b>Tolerable Risk Criterion</b>	<b>Tolerable Risk</b>	<b>Individual risk</b>	
		$1 \times 10^{-4} \geq IR \geq 1 \times 10^{-6}$	
<b>Trigger Event</b>	High product flow		
<b>LOPA events</b>	<b>Event</b>	<b>PFD</b>	<b>Frequency</b>
<b>Accident Condition</b>	N/A	N/A	N/A
<b>Initiate Event</b>	High flow	N/A	1
<b>Layer of protection</b>	SIF 1	$1 \times 10^{-1}$	N/A
	Relief Valve	$1 \times 10^{-1}$	N/A
<b>Total Frequency or probability of accident</b>		N/A	$1 \times 10^{-2}$
<b>Risk target</b>			$< 1 \times 10^{-4}$
<b>Is the risk tolerable ?</b>	Yes	No	
			X
<b>Other layer of protection is required ?</b>	What ?	Prob or Freq	
	SIF	?	
<b>Mitigation Action</b>		To proceed to SIL analysis	
<b>New Layer of protection</b>	SIF (SIL 2)		
<b>Previous frequency or probability of accident</b>	<b>Probability</b>	<b>Frequency</b>	
<b>New mitigated risk</b>			
<b>Is the risk target achieved ?</b>			
<b>Implementation Action</b>			

**FIGURE 6.83**  
Separator vessel LOPA.

		FREQUENCY CATEGORY					
		A (extremely remote)	B (remote)	C (Little frequency)	D (Frequent)	E (Very frequent)	F (Extremely frequent)
		At least 1 between 100 and 100,000 years	At least 1 between 50 and 1000	At least 1 between 30 and 50 years	At least 1 between 5 and 30 years	At least 1 in 5 years	At least 1 in 1 years
SEVERITY CATEGORY	∞	M	NT	NT	NT	NT	NT
	≡	M	M	NT	NT	NT	NT
	=	T	T	M	M	M	M
	-	T	T	T	M	M	M

FIGURE 6.84

Risk matrix.

Consequence Categories	
Severity Category	Description
Minor	Impact initially limited to local area of the event with potential for broader consequence if corrective action is not taken
Serious	One that could cause any serious injury or fatality on site or off site, or property damage of \$1 million off site or \$5 million on site
Extensive	One that is more than five times worse than serious

*Source: Schwartz, 2002.*

Likelihood Categories	Frequency (per year)	Description
Low	$<10^{-4}$	A failure or series of failures with a very low probability that is not expected to occur within the lifetime of the plant
Moderate	$10^{-2}-10^{-4}$	A failure or series of failures with a low probability that is not expected to occur within the lifetime of the plant
High	$>10^{-2}$	A failure can reasonably be expected within the lifetime of the plant

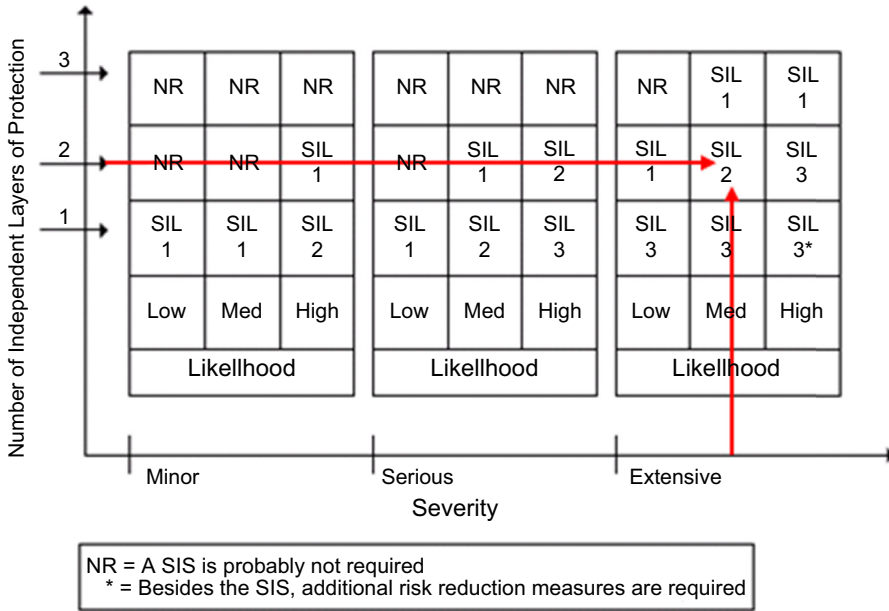


FIGURE 6.85

SIL selection based on the risk matrix method.

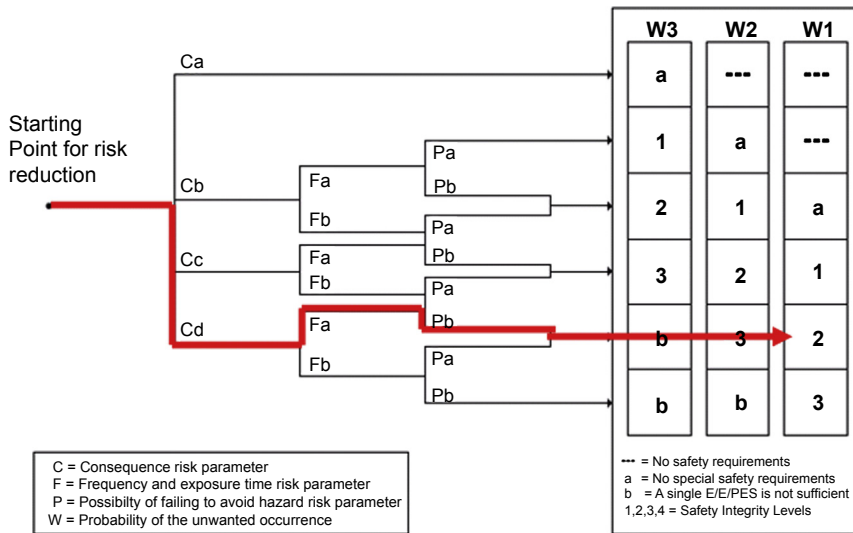


FIGURE 6.86

SIL selection based on the risk graph method.

- Cc ( $0.1 < PLL < 1$ );
- Cd ( $PLL > 1$ ).

The occupancies are classified into four levels:

- Fa (rare exposure to an accident in a vulnerable area. The vulnerable area is occupied less than 10% of the time);
- Fb (frequent or permanent exposure to an accident in a vulnerable area. The vulnerable area is occupied more than 10% of the time).

The third criterion to be assessed is avoidance and represents how feasible it is for the operator to avoid the accident. Basically, the avoidance is classified into two levels:

- Pa (the operator will be alerted if SIF has failed. Facilities with resources to prevent an accident are provided, and they are independent, enabling the operator to escape from the vulnerable area. There is sufficient time for the operator to be alerted about the incident and to take action to avoid it);
- Pb (if one of the conditions above is not satisfied).

The fourth criterion is the demand rate, which defines the frequency of incident which might trigger an accident if no layers of protection are able to avoid it. The demand rate is classified in three levels:

- W1 ( $< 0.03$  times per year);
- W2 ( $0.3 < W2 < 0.03$  times per year);
- W3 ( $3 < PLL < 0.3$  times per year).

Finally, concerning the separator vessel case, the classification is:

- Cd ( $PLL > 1$ );
- Fa (rare exposure to an accident in a vulnerable area. The vulnerable area is occupied less than 10% of the time);
- Pb (if one of the conditions above is not satisfied);
- W1 (less than 0.03 times per year).

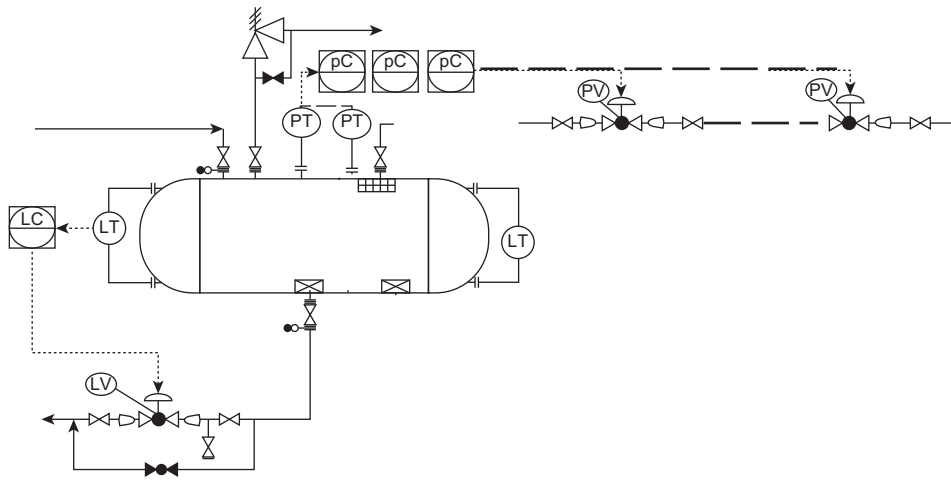
The demand rate took into account the two layers of protection already installed, which reduces the frequency of the hazard from W3 to W1. Therefore SIL 2 is selected based on risk graph criteria classification, as shown in [Fig. 6.86](#).

The result achieved with the risk matrix method and the risk graph method is similar, which indicates SIL 2. In case of different results the usual recommendation is to apply the more conservative value, in other words the higher SIL level.

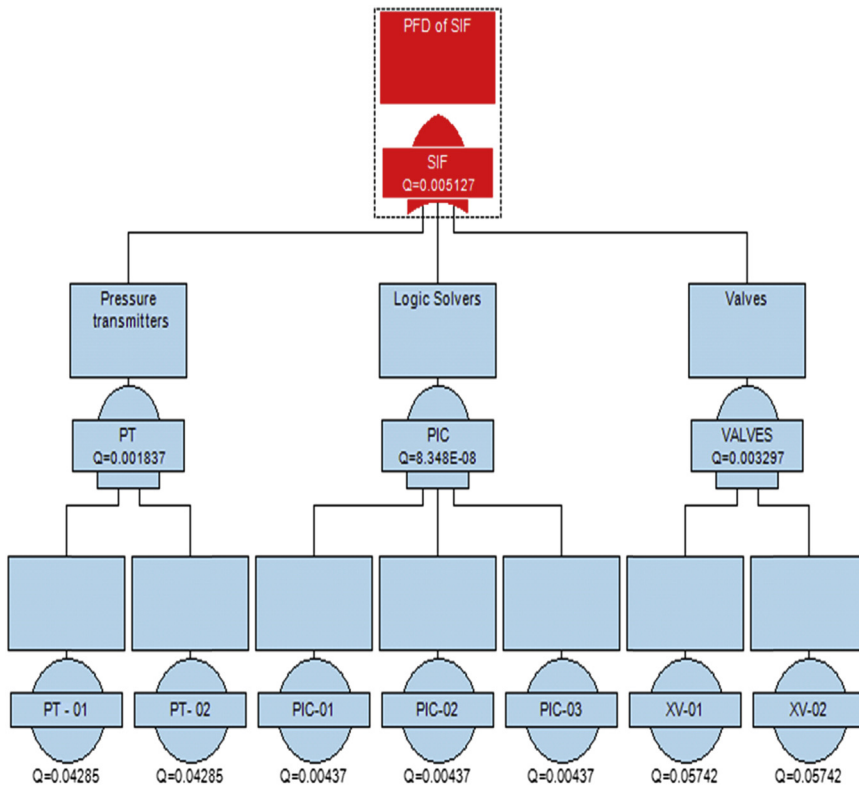
After SIL selection the SIF configuration is designed and it is required to check if such a design configuration achieves the SIL target.

### **SIL Verification**

The final step in SIL assessment is to verify if the SIF design configuration achieves the SIL target. Therefore different quantitative risk analysis methods such as RBD or FTA are applied to demonstrate the achievement of the SIL 2 target. [Fig. 6.87](#) demonstrates the SIF configuration to mitigate the high-pressure scenario caused by high flow.



**FIGURE 6.87**  
SIF configuration.



**FIGURE 6.88**  
SIF verification FTA.

Based on Fig. 6.87, the SIF configuration encompasses two pressure transmitter sensors, two control valves, and three logic solvers. To proceed, the SIL verification failure rate (hours) for each component must be defined such as:

- Pressure sensor transmitter ( $\lambda = 1 \times 10^{-6}$  failures/h);
- Logic solver ( $\lambda = 1 \times 10^{-7}$  failures/h);
- Valve (PFD =  $1.36 \times 10^{-6}$  failures/h).

Accident Scenario Number		Equipment	
1		Separator Vessel	
Date			
15/07/2013			
Consequence description		Huge Gas leakage	
Tolerable Risk Criterion	Tolerable Risk	Individual risk	
		1x E-4 ≥ IR ≥ 1x E-6	
Trigger Event		High product flow	
LOPA events	Event	PFD	Frequency
Accident Condition	N/A	N/A	N/A
Initiate Event	High flow	N/A	1
Layer of protection	SIF 1	$1 \times 10^{-1}$	N/A
	Relieve Valve	$1 \times 10^{-1}$	N/A
Total Frequency or probability of accident		N/A	$1 \times 10^{-2}$
Risk target			$< 1 \times 10^{-4}$
Is the risk tolerable ?		Yes	No
			X
Other layer of protection is required ?		What ?	Prob or Freq
		SIF	?
Mitigation Action		To proceed to SIL analysis	
New Layer of protection	SIF (SIL 2)	$5.125 \times 10^{-3}$	
Previous frequency or probability of accident		Probability	Frequency
		$1 \times 10^{-2}$	
New mitigated risk		$5.125 \times 10^{-5}$	
Is the risk target achieved ?		Yes	
Implementation Action		Implement SIF based on design configuration	

FIGURE 6.89

Final LOPA calculation.

Based on such values the FTA demonstrated in Fig. 6.88 shows that the SIF configuration achieves SIL level 2. The SIL level is required for 5-year operation (43,800 h).

The PFD of SIF in 5 years is  $5.125 \times 10^{-3}$ , which is considered SIL 2 ( $1 \times 10^{-2} < \text{PFD} < 1 \times 10^{-3}$ ).

Inspection and test on different SIF components can be carried out, but such test does not reestablish SIF reliability because preventive maintenance is not performed for electronic components. Concerning the valve, the most critical component that is considered in the FTA is the actuator, which has exponential PDF. The mechanical valve must have a guarantee to perform 5 years without wear-out. Therefore the SIL target will be achieved.

Verification assessment is based on theoretical data. To validate such values a test must be carried out to demonstrate that such SIF components will achieve the target for the specific time.

The final calculation is to input the PFD value on an LOPA template to prove that the risk mitigation target is achieved. Fig. 6.89 shows the final LOPA calculation including the SIF.

---

## REFERENCES

- Calixto, E., 2007a. The safety integrity level as hazop risk consistence. The Brazilian risk analysis case study. In: European Safety and Reliability Conference, Stavanger, Norway. Taylor & Francis Group, London, ISBN 978-0-415-44786.
- Calixto, E., 2007b. Integrated preliminary hazard analysis methodology for environment, safety and social issues: the platform risk analysis study. In: European Safety and Reliability Conference, Stavanger, Norway. Taylor & Francis Group, London, ISBN 978-0-415-44786.
- Calixto, E., 2011. The optimum replacement time considering reliability growth, life cycle and operational costs. In: ARS, Netherland, Amsterdam.
- Calixto, E., 2015. Safety Science: Methods to Prevent Incidents and Worker Health Damage at the Workplace. eISBN:978-1-60805-952-2, 2015, ISBN 978-1-60805-953-9. <http://dx.doi.org/10.2174/97816080595221150101> (bethamebook).
- Crow, D.A., Louvar, J.F., 2002. Chemical Process Safety Fundamentals with Applications. Prentice-Hall.
- Ericson, C., 1999. Fault tree analysis-A history. In: 17th International System Safety Conference, EUA, Orlando, FL.
- Marzal, E.M., Scharpf, E., 2002. Safety Integration Level Selection: Systematics Methods Including Layer of Protection Analysis. The Instrumentation, Systems and Automation Society.
- Vozella, A., Gigante, G., Travascio, L., Compare, M., 2006. RAMS for aerospace: better early or late than never. In: European Safety and Reliability Conference. Safety and Reliability for Managing Risk. Taylor & Francis Group.

## APPENDIX A

PFS	Level	Value	Explanation
Time	Nominal	1	Field operator's actions are independent of time. The time is controlled by the control room operator. If there is no time to reach or reopen the valve, the field operator has to advise the control room operator. If his time expires and he does not communicate with the control room, then the control room should trip train 1 to avoid cascade trips.
Stress	Extreme	2	Stress is high because the operator: <ul style="list-style-type: none"> <li>■ Is told that any error or delay will have an escalating effect that trips the whole facility.</li> <li>■ Senses the stress in the control room because of the implications of the fault.</li> </ul>
Complexity	Complexity	1	It is assumed that the field operator is close to the valve, otherwise the control room operator would not have contacted him given there are only 10 min available. The only task he has to do is press a manual pushbutton to open the valve. No complexity involved.
Experience/Training	Nominal	1	Nothing to suggest training will not be available; same with experience.
Procedures /Ergonomics/Fitness/ Work Process	Nominal	1	Nothing to suggest otherwise.

PFS	Level	Value	Explanation
Time	Nominal	10	Control room operator's combined acknowledgment and actions require at least 10 min. He has 10 min to react to the first alarm. So time available = time required.
Stress	Extreme	5	Stress is extreme because the operator: <ul style="list-style-type: none"> <li>• Knows that any error delay will have an escalating effect that trips the whole facility.</li> <li>• Has already been told by the field operator that the condition cannot be recovered.</li> <li>• Even if he does the task right, still has to trip one train, which will partially compromise production.</li> </ul>
Complexity	Complexity	1	The task of tripping one train is trivial. Given the time constraints before tripping the train, the tasks he allocates to the field operation and coordination are minimal.
Experience/Training	Nominal	1	Nothing to suggest training will not be available; same with experience.
Procedures /Ergonomics/Fitness/ Work Process	Nominal	1	Nothing to suggest otherwise.



## RELIABILITY MANAGEMENT

## 7

**CHAPTER OUTLINE**

<b>7.1 Reliability Management Over the Enterprise Life Cycle .....</b>	<b>667</b>
<b>7.2 Reliability Management Success Factors .....</b>	<b>669</b>
<b>7.3 The 10 Reliability Pitfalls for the Oil and Gas Industry .....</b>	<b>674</b>
7.3.1 Pitfall 1: Assume Exponential PDF for all Types of Equipment and Components .....	674
7.3.2 Pitfall 2: To Use MTBF and Failure Rate as a Performance Index .....	676
7.3.3 Pitfall 3: Do Not Consider the Preventive Maintenance Effect on Reliability and Operational Availability.....	679
7.3.4 Pitfall 4: Do Not Consider the Human Factor in Reliability Analysis .....	680
7.3.5 Pitfall 5: Do Not Consider Different Operation Condition Effects on Reliability Prediction.....	681
7.3.6 Pitfall 6: Do Not Consider ALT, HALT, and RGA When Necessary .....	682
7.3.7 Pitfall 7: To Apply Redundancy to Increase System Operational Availability for all Cases.....	683
7.3.8 Pitfall 8: Do Not Take Into Account Qualitative Methods Recommendation to Improve Reliability Performance.....	684
7.3.9 Pitfall 9: Do Not Consider Life Cycle Cost as Part of Reliability Engineering Analysis ...	685
7.3.10 Pitfall 10: Do Not Consider Reliability Engineering as Part of Asset Management .....	686
<b>7.4 Reliability Engineering: Implementation of Barriers to Successful Achievement.....</b>	<b>687</b>
7.4.1 The Decisor's Profile.....	687
7.4.2 The Organizational Fast Food Culture .....	689
7.4.3 The Standard Approach .....	690
<b>7.5 Reliability Management: Successful Cases .....</b>	<b>691</b>
7.5.1 Bayer .....	691
7.5.2 USNRC (United States Nuclear Regulatory Commission) .....	693
7.5.3 ESReDA (European Safety and Reliability and Data Association) .....	694
7.5.4 ESRA (European Safety and Reliability Association) .....	695
7.5.5 SINTEF (Stiftelsen for Industriell og Teknisk Forskning) .....	695
<b>7.6 Reliability Engineer Teaching and Research: Successful Universities and Research Center Cases.....</b>	<b>696</b>
7.6.1 Karlsruhe Institute of Technology.....	696
7.6.2 Indian Institute of Technology Kharagpur .....	698
7.6.3 University of Strathclyde Business School .....	699
7.6.4 University of Stavanger .....	699
<b>7.7 Reliability Management Final Thoughts.....</b>	<b>700</b>
<b>References .....</b>	<b>701</b>
<b>Further Reading .....</b>	<b>701</b>

This chapter covers the management of reliability engineering in the oil and gas industry. The previous six chapters presented different reliability engineering approaches, and the next step is to define how to manage reliability engineering and incorporate the methodologies into daily activities and processes. The second step is to understand the types of products and service reliability engineering supplies available during an enterprise's life cycle. Thus understanding the company's life cycle and in which phase the company or management operates is essential to have a clear idea of which reliability engineering methodology is best applied to get the best results. In this chapter, examples of companies from chemical industries that have been successful in managing reliability engineering and other organizations that have supported reliability engineering over many years will be given. Thus the first step is to understand the oil and gas industry, and the Five Forces methodology (Porter, 1998) is the simplest way to do so, as shown in Fig. 7.1.

The threat of "new entrants" is low because barriers to entry include high capital cost, economies of scale, distribution channels, proprietary technology, environmental regulation, geopolitical factors, and high levels of industry expertise needed to be competitive in the areas of exploration and extraction. In addition, fixed cost levels are high for upstream, downstream, and chemical products. Thus it is very hard for new players to enter the market.

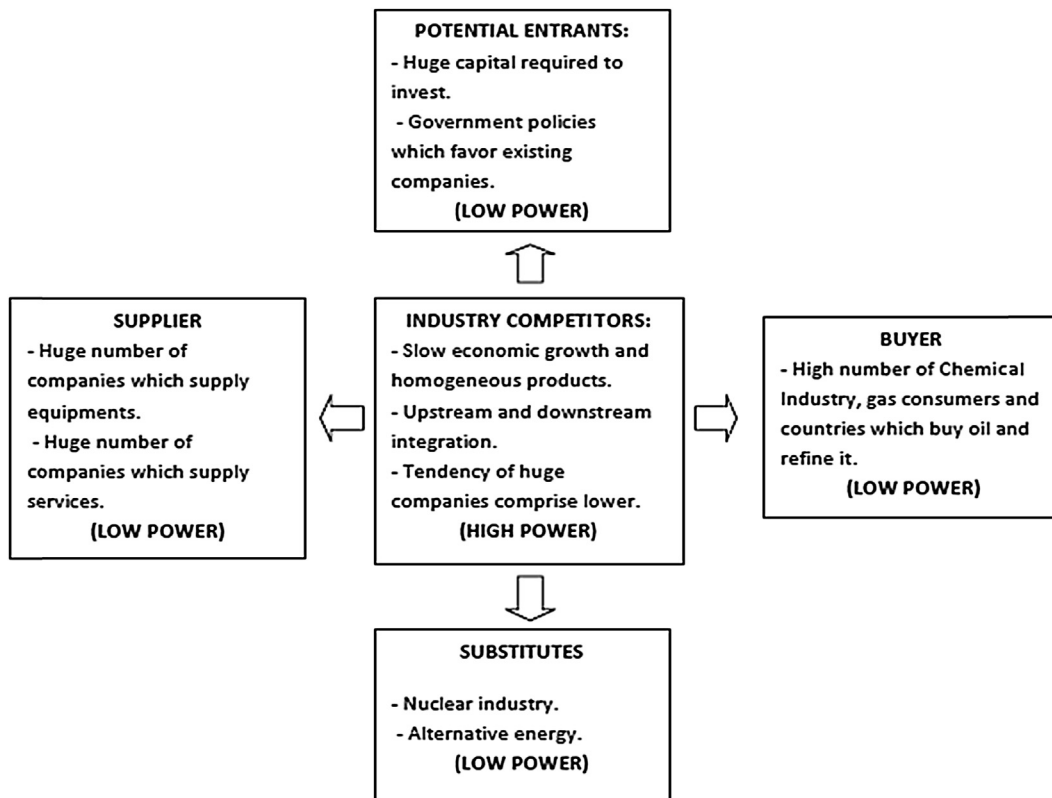


FIGURE 7.1

Oil and gas industry Five Forces methodology.

The “industry competitors” power is high because of the limited resources (oil and gas) and low number of companies (eg, ExxonMobil, BP, Chevron, ConocoPhillips, Royal Dutch Shell, Saudi Aramco, Kuwait Oil Company, etc.). The oil and gas industry is a commodity market and the competitive advantage is primarily derived from the ability to produce products at a lower cost via operational efficiencies.

The “buyer” is both industrial consumers and individual consumers. Industrial (ie, downstream) buyer power is low because upstream suppliers have an incentive to limit supply and keep prices high. The individual buyer power is low because of the high volume of demand.

The threat of “substitutes” is low and comes from nuclear power, hydroelectric, biomass, geothermal, solar, photovoltaic, and wind. Nuclear and hydroelectric energy sources are not a threat within the next decade because of government regulation, environmental concerns, and a high barrier to entry. Coal would be a threat to oil consumption as an energy source if there were technological advancements in coal liquefaction techniques that would provide clean, stable molecules from the largely abundant domestic coal reserves.

This explains why the oil and gas industry has such high profits. The oil and gas companies, equipment, and service suppliers require high processes and product performance that can translate to high reliability. In this way, we have two types of companies: equipment and service suppliers and big companies with downstream and upstream processes.

In the first case, companies that supply equipment will apply accelerated testing, reliability growth analysis, Design Failure Mode and Effect Analysis (DFMEA), and even life cycle analysis to assess their products and customer use.

In general terms, companies that supply services such as maintenance, operation, and construction will apply human reliability analysis to guarantee minimum human error and consequently high performance of their service. In the maintenance case, Reliability Centered Maintenance (RCM), Risk Based Inspection (RBI), Reliability Growth Based inspection (RGUI), Failure Mode and Effect Analysis (FMEA) and Failure Mode Effect and Criticality Analysis (FMECA) can also be applied to achieve high performance.

The big oil and gas companies with downstream and upstream processes will apply human reliability analysis, life cycle analysis, Reliability, Availability and Maintainability (RAM) analysis, RCM, RBI, RGUI, FMEA, FMECA, and quantitative risk analysis (Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Layer of Protection Analysis (LOPA), Safety Integrity Analysis (SIL), and bow tie analysis).

The main question is who is responsible for conducting such analysis and when does the analysis begin? These are the topics of the following sections.

---

## 7.1 RELIABILITY MANAGEMENT OVER THE ENTERPRISE LIFE CYCLE

To understand how to apply reliability engineering tools it is essential to understand what the term enterprise means over the life cycle of a product or service. The enterprise can be split into phases, including identification and assessment of opportunities, conceptual projects, basic projects, executive projects, assembly and construction, preoperation, operation, and deactivation. In general, these enterprise phases are comprised of planning, control, and learning phases. It is important to know which reliability engineering method to use to get the best results in each phase.

Depending on the company, some reliability engineering tools are more applicable than others. Thus for equipment suppliers in phase 2, accelerated testing, DFMEA, and reliability growth analysis are more applicable to verify if their products are achieving the reliability and availability

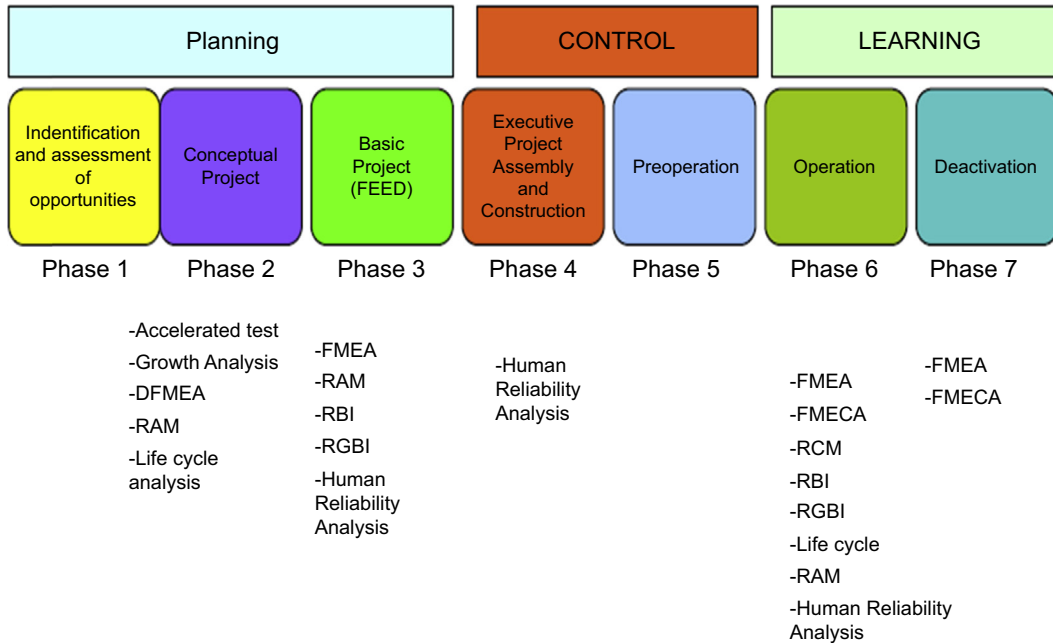
targets required by their customers. However, oil and gas companies with downstream or upstream processes apply mostly life cycle analysis and RAM analysis. In the first case, life cycle analysis is applied whenever similar equipment can be used as a reference for the new project and RAM analysis can be applied to check system availability, critical equipment, and avoid past mistakes. In addition, RAM analysis is a good opportunity to reduce costs, test redundancy policies, test different configurations, and even to predict the impact of other facilities on plant availability. RAM analysis in the project phase is also known as reliability VIP (value improving practice) based on IPA (independent project analysis) methodology. Such VIPs are also applied to other subjects, and other types of VIPs are the design of capacity, class of facility quality, processes simplification, waste minimization, predictive maintenance, constructability, energy optimization, value engineering, and 3D CAD design. The main objective is to improve project performance in terms of cost and project quality.

In phase 3, where projects have more detail, it is possible to apply FMEA, RBI, RGBI, RCM, and human reliability analysis. FMEA is applied to discuss failure modes, and it can also focus on safety. FMEA can be included in RCM analysis, and this tool predicts preventive maintenance and inspections, and in this case it is possible to estimate a maintenance budget for the first few operational years. RBI and RGBI can also be applied in a project to define inspection policies and tasks. Human reliability analysis can support risk analysis or even critical operations that influence safety or system availability.

Phase 4 is the last project phase, which means buildup plant time, and human reliability tools are very important when applied to revise procedures to reduce the chance of human error. In the equipment case, that is, assembly time, and even in this case, human reliability is important to avoid human error in assembly tasks. In phase 5, preoperation and plants and equipment are prepared for the operation phase. In phase 6, FMEA, FMECA, RCM, RBI, RGBI, life cycle analysis, RAM, and human reliability analysis can be applied to improve system performance based on improvements in critical equipment and operations. Maintenance plans and inspections can be constantly assessed using RCM, RBI, and RGBI. FMEA and FMECA can be included in RCM analysis or be used to assess specific equipment. Life cycle analysis can be conducted to support maintenance and inspection decisions and the time of such procedures, and even to support RAM analysis to define bad factors and prioritize improvements. Human reliability analysis can also be applied to reduce human errors in operation, maintenance, and safety procedures.

In phase 7, when the plant is deactivated, FMEA and FMECA can be applied to define unsafe failures of the deactivated equipment. While it is important to know which reliability engineering tool is best for which phases of the life cycle, the big challenge for oil and gas companies is working with different enterprises in different phases, which requires specialized teams and such teams must be managed efficiently to get the best results on time. Fig. 7.2 summarizes reliability engineering tools and their applications over the enterprise life cycle.

There are a number of points to consider regarding reliability engineering implementation over the enterprise life cycle. The first point is when to apply the correct reliability engineering methods throughout the asset life cycle. In order to define the correct method and the right time to apply, it is very important to be aware of the objective of the application or even the nature of asset problem. The second point is that over the enterprise life cycle other subjects and analyses are required, including risk analysis, environmental impact assessments, and VIPs, and often reliability engineering tools to compete for the resources to perform such analyses.



**FIGURE 7.2**

Reliability engineering applied over enterprise phases.

Lastly, establishing reliability engineering practices requires investment, time, and people, but can benefit a company for a long time. For some companies, even with the proper investment, time and people, is difficult to implement the reliability engineering program because the lack of cultural, organizational framework and leadership. The next section will discuss the factors that influence the success or failure in establishing reliability engineering program in company processes.

## 7.2 RELIABILITY MANAGEMENT SUCCESS FACTORS

As discussed, for reliability engineering to be successfully implemented within a company, the following factors must be considered:

- Culture
- Organizational framework
- Resources
- Work routine

The first factor is organizational culture, and culture can be defined by employees’ values, which are reflected in their attitude. In terms of organizational culture, to implement reliability engineering two values are important: “obtain economical results” and “make decisions based on facts, that is, based on quantitative data.” To make a decision based on quantitative data can be a strong barrier to implementing reliability engineering.

The main point of such a discussion is to be aware that some problems have a qualitative nature and must be solved with qualitative models, such as brainstorming, which requires assessment of the probable causes of the problem based on people's opinions.

However, some problems have a quantitative nature and must be solved using a quantitative model to define system availability, define equipment replacement time, define maintenance policy, and predict product reliability based on testing.

To apply reliability engineering tools it is essential to have failures and repair historical data. Data collection and failure data assessment must be part of maintenance and operation routines and must be recognized and reinforced by managers. The correct data collection must include the following information:

- Which equipment and components failed;
- Failure mode causes and consequences;
- Date when components and equipment failed and time needed for repairs;
- Specialist opinion and remarks about failure and repair.

As discussed in Chapter 1 (and shown in Fig. 1.2), when failure modes are standardized it is easier to assess failures and complete data collection. Additionally, reports are used by different specialists and not all of them understand the details of the equipment; standardization solves this problem as well.

The biggest challenge in data collection is maintaining reports and keeping them updated. There are some success cases where failure data reports were established and stocked, such as in a school library, and in this case there is a control of reports for who has read the books and a specific place on the shelves for books to be stored. Failures and repair data reports can be electronic or paper. Paper reports can be accessed by everyone, but that is not always the case with electronic reports. However, big companies in the oil and gas industry require in many cases access reports from other locations, which is more difficult with paper reports. The difficulty with electronic reports is that they have to be constantly updated. It is best to have both types of reports, but in practice it is hard to establish electronic data collection when there is not a routine for collecting data for paper reports. Today, however, there are technologies that allow data collection directly from the equipment or even from a data bank, such as SAP, Maximo, and Access, and such software also performs and updates reliability analysis.

What is most important, no matter the technology, is the data collection routine. It is best when maintenance and operational specialists complete the reports because details must be available in both data banks. In some companies this electronic data bank is not fulfilled by specialists and a lot of information is lost.

For a culture to “make decisions based on quantitative data” to solve problems of a quantitative nature requires maintaining a data collection routine. Other additional factors required are to successfully implement reliability engineering in current processes.

The organizational framework defines the product and service flow throughout companies and also who will be responsible for making decisions about processes, projects, product development, and so on. Oil and gas companies, despite their technical characteristics, are organized by specializations having in most cases a functional framework. This means there are several branches of management with different objectives such as project management, operation management, maintenance management, and safety management, and reliability engineering must support all of them. Training

specialists from the different areas of management to apply the specific reliability engineering tools is the first step in implementing reliability engineering methodologies, but in many cases it is not successful over a very long period because management often has its own agenda and there is not enough time to dedicate to reliability engineering. In other cases, specialists have forgotten key concepts or how to use software. In the maintenance case, FMEA, FMECA, and RCM are qualitative tools that are more related to maintenance routines than life cycle analysis and RAM analysis. Even though these methods are simpler than life cycle analysis and RAM analysis, it is necessary to practice them constantly. In project management where products from equipment supplier companies in the oil and gas industry are developed, reliability engineering is more common because accelerated testing, growth analysis, and DFMEA are part of the product development routine. However, in companies with downstream and upstream processes, project management may also have reliability engineers to conduct RAM analysis, FMEA, RCM, RBI, RGBI, and life cycle and support risk analysis. But in many cases, reliability engineers are moved to other activities such as risk analysis or project analysis.

Depending on requirements it is possible to have specific reliability management to support other management, such as project management, maintenance management, operational management, and safety management. At the beginning of implementation, if reliability engineers are free to perform their activities and have their own manager it is easier to establish a routine for reliability professionals.

There are also other factors that influence reliability management, including resources, that is, time, people, and money. Time is the most important resource, and in many cases there is not enough time for managers to perform reliability engineering analysis and for reliability engineers to perform it and give reliable results. In addition, justifying reliability, investment is hard because it will take some time to provide results because it is necessary to implement reliability engineering as a routine. At the beginning of the reliability engineering implementation, which can last more than 1 year, reliability is not very involved in the company's routines, which means that it is seldom related to operation, maintenance, and other management routines.

People are the second crucial resource for reliability engineering and today there are not enough reliability engineers available, in part because of the training and dedication required. Being a reliability engineer requires a good background in mathematics, statistics, and equipment, and it is also important that the engineer enjoys working with equipment, systems, and products. Also there are not many courses or specializations available as with other engineering specializations, even though reliability engineering requires practice to learn reliability tools. In other words, courses and specializations are not the only preparation needed for an engineer to be ready to apply reliability tools. Thus whenever there are dedicated reliability engineers willing to learn and apply reliability engineering tools, managers must support and reinforce them.

Money to invest in reliability engineering is also required, and depending on the objective it can require a significant investment, but in the long run this investment will pay for itself in results. In most cases, the oil and gas industry requires current reliability engineering applications to achieve high performance, and investment in software, training, and travel to conferences must be constant over time. Such investment includes a clear reliability specialist career definition with all aspect of any specialist career such as training, promotion, salary, bonus in order to keep such specialist professionals in company.

The reliability engineering specialist can have a background in different areas such as industrial, mechanical, electrical, electronic, material, and others. When creating a group of reliability specialists, it is important that engineers have different backgrounds in all types of equipment and processes. It is

also important to have experienced professionals with the skills needed to support analysis and solutions. In general, multidisciplinary reliability engineering management is better to perform analysis and support other management. This means having different engineers with different backgrounds (electrician, mechanic, production, metallurgic, etc.) dedicated to reliability.

Despite all these considerations, reliability professionals must have their own routine, since it is critical to the success of reliability engineering implementation. Actually, this is the most common mistake when companies try to implement reliability engineering in current processes: reliability professionals not being given enough time to commit to reliability engineering. This happens most often when management frequently asks a reliability specialist to perform other activities.

The reliability engineering routine includes working with data and performing analyses, requiring weeks or even months. The quality of a reliability specialist’s work depends on the time they dedicate to analysis and data collection. Fig. 7.3 summarizes the type of reliability engineering management can support with different types of analysis.

Having a formal “reliability management” to support other management as a project, maintenance, and operational is an ideal configuration that also provides a chance for reliability engineering to be successful. In this way, reliability is not treated as a side job of some professionals, but a formal activity within the organizational framework. Fig. 7.3 is easily applied to a functional organization but some organizations are matricial or organized per process. This means multidisciplinary teams work on different enterprise phases under supervision.

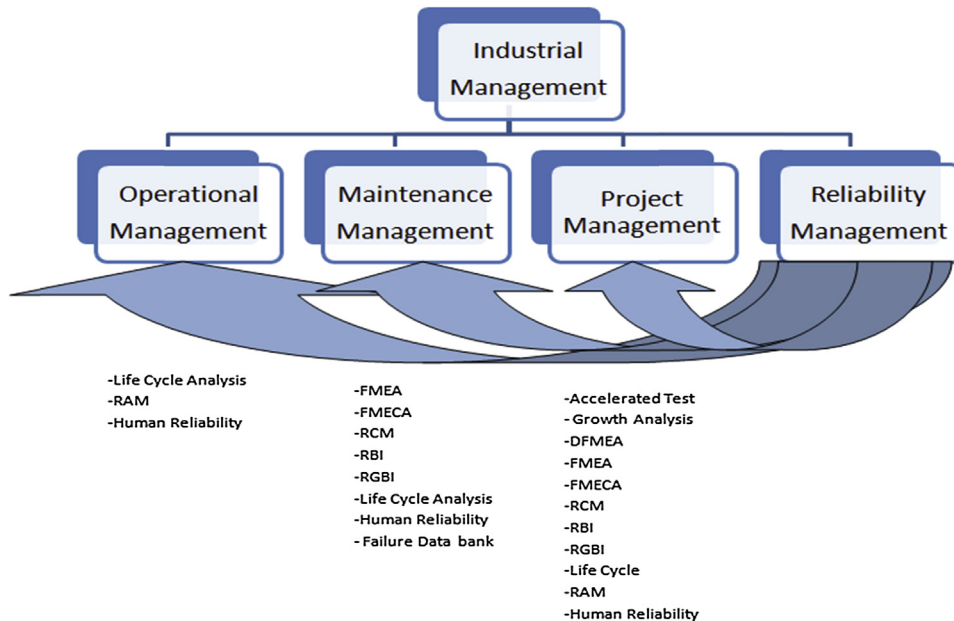
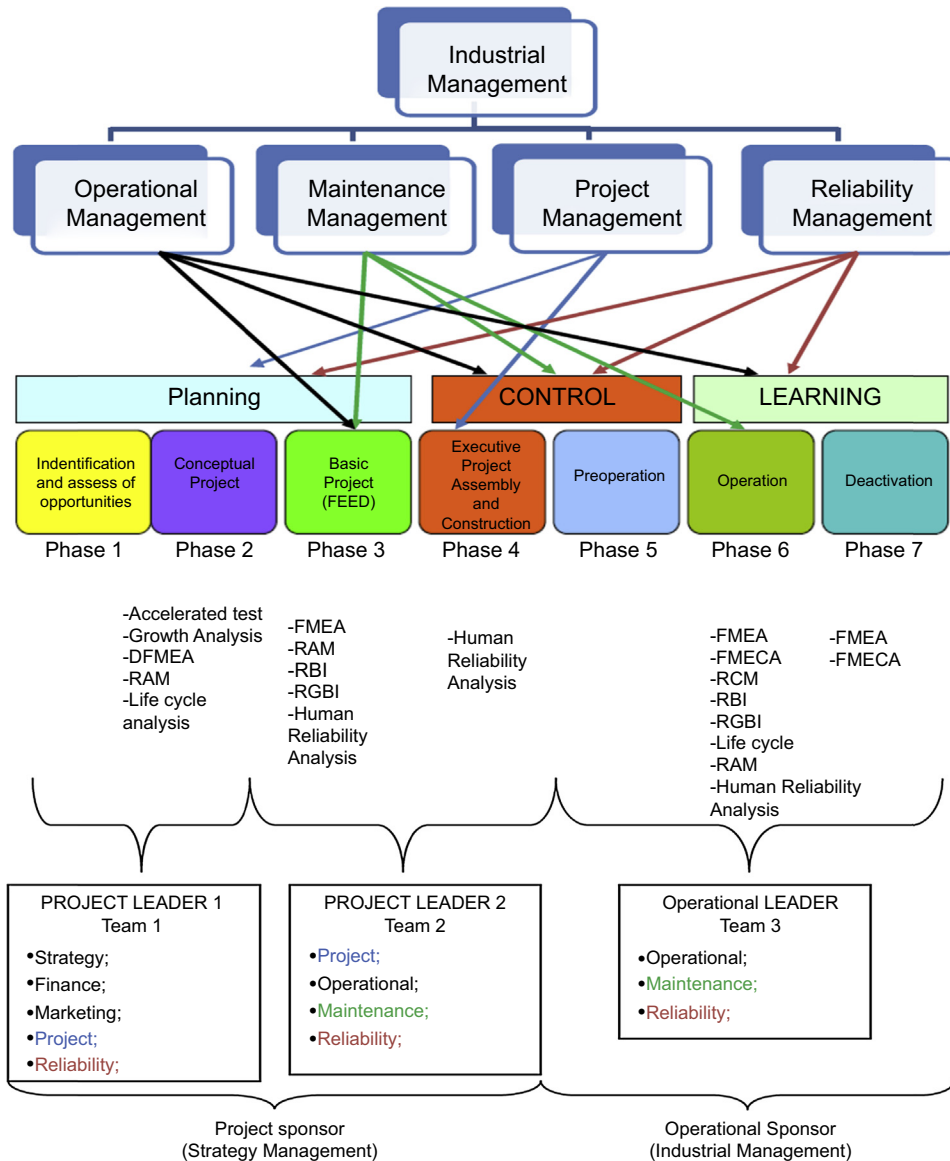


FIGURE 7.3

Reliability engineer management support (functional organization).



Fig. 7.4 represents the flow of professionals and services over enterprise phases. In this case, different professionals from different management teams work on different enterprise phases under project leaders and operational leaders, and management supports such leaders. In this configuration the manager defines which professionals will work in each enterprise phase and supplies resources to train such professionals to guarantee their service quality. The leader supervises and coordinates different professionals on their team with sufficient authority to guarantee that the requirements of the



**FIGURE 7.4**

Reliability engineer management support (matricial organization).

enterprise phases are under control. The project leader is under the project control and guarantees that the project control is meeting strategy objectives.

One such initiative taken into account is the four success factors (ie, culture, organizational framework, resources, and work routine), which means the organization recognizes results and decisions based on quantitative methods. A company that recognizes the value of reliability has a better chance of staying competitive. This type of organization creates reliability management and recognizes reliability engineering as a formal activity in the company. As a formal management, it is necessary to define which services and products will supply other management, and in doing so establish a work routine for the team of reliability specialists. Reliability managers must also be reliability specialists because it is not possible to prioritize analysis, assess the analysis quality, define training for the specialist team, or even analyze specialists' performance without understanding those principles.

Because of the importance of reliability management as well as maintenance management it is essential to integrate these areas of management with organizational business results. Asset management is a more integrated concept that comprises reliability and maintenance management and business management.

Asset management is simply the optimum way of managing assets to achieve a desired and sustainable outcome [BSI PAS 55:2008](#).

Asset management emphasizes an integrated approach in decision making and this means integrating asset development, operating assets, maintenance of assets, and disposal. Asset development covers a determination of asset options to be used, design and construction of production equipment in compliance with life cycle requirements, capacity, capability, flexibility, efficiency, and performance rate requirements as well as maintainability and reliability.

---

## 7.3 THE 10 RELIABILITY PITFALLS FOR THE OIL AND GAS INDUSTRY

As discussed previously, organizational factors such as culture, organizational framework, resources, and work routine are very important to have a successful reliability engineering program implementation.

In addition to such factors, it is necessary to avoid the 10 reliability engineering pitfalls that have been a barrier to reliability engineering success, even for an organization that accomplishes the four organizational factors.

Indeed, in some cases, to implement a structural reliability engineering program, many organizations try to standardize the reliability engineering department activities based on standards. Unfortunately, as reliability engineering is based on assessment of particular cases of asset performance and development, the standards do not cover many aspects and in some cases the wrong concepts as well as simple methods are used for complex asset assessment.

To understand the reason behind this, let us describe the 10 reliability engineering pitfalls.

### 7.3.1 PITFALL 1: ASSUME EXPONENTIAL PDF FOR ALL TYPES OF EQUIPMENT AND COMPONENTS

Based on Chapters 1 and 2, it is clearly understood that lifetime data analysis as well as different probabilistic accelerated test methods are the best approach to predict reliability based on historical data or even on accelerated test results.

To perform lifetime data analysis, it is necessary to have reliable historical data, which require time and in some cases a huge effort to be accomplished. Therefore an easier solution that many organizations

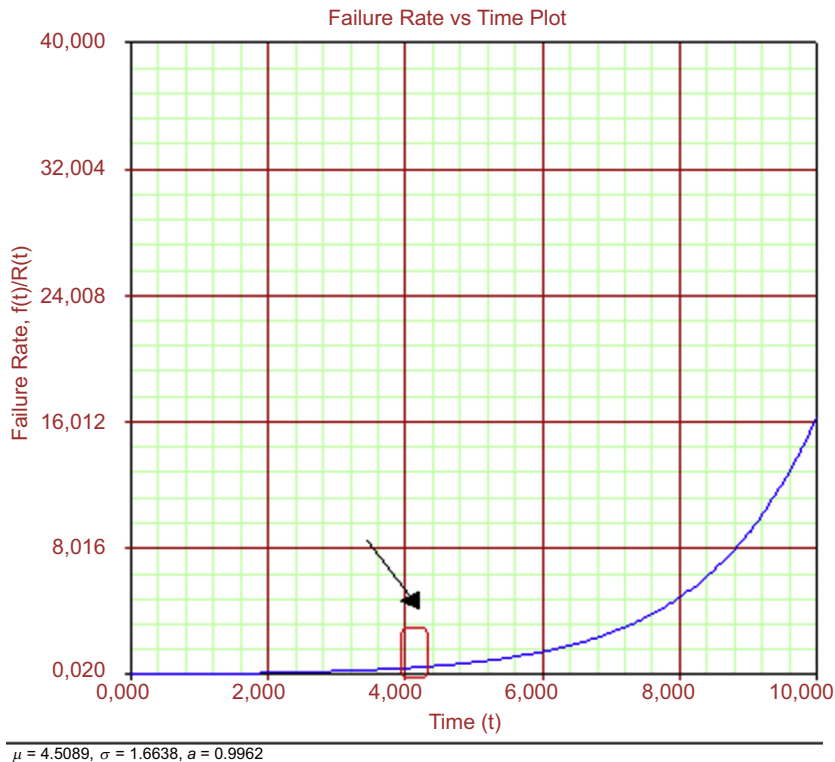
adopt to avoid the best and most robust approach is to use data from generic databases, which in most of cases are described in Expected time to failure (MTTF) and Expected time to repair (MTTR).

The first problem with a generic database such as OREDA is that the database represents equipment failures under certain operational conditions from northern Europe, which are totally different from the other asset operation conditions. In fact, the problem is not in the database.

The assumption of exponential PDF for all types of equipment is incorrect based on lifetime data analysis, and it is possible to prove that dynamic mechanical equipment such as valves, pumps, compressors, blowers and static mechanical equipment such as vessels, towers, and pipes has an increasing and not constant failure rate. Such increasing failure rate is minimized with preventive maintenance.

The second problem is that whenever the exponential PDF is applied the preventive maintenance will have no positive effect on reliability recovery. In fact, this does not happening for mechanical equipment in the real world. In such cases, preventive maintenance such as schedule and predictive are able to restore mechanical equipment and component reliability before the failure occurs.

However, during RAM analysis, if the exponential PDF is input in an RBD as well as preventive maintenance the result of operational availability or production efficiency will be impacted by preventive maintenance and corrective maintenance. This is not right, because in a proper RAM model, whenever preventive maintenance takes place before the most probable time of failure, the failure will be avoided if a PDF is applied, which represents the increasing failure rate such as normal and Gumbel, for instance. Fig. 7.5 shows the increasing failure rate time when preventive maintenance must take place.



**FIGURE 7.5**

Increasing failure rate.

It must be clear that an exponential PDF represents equipment failure, but it is necessary to prove that such PDF is the best fit for the failure historical data based on lifetime data analysis. However, it is also necessary to be careful because in a case where small amounts of historical failure data are available, the lifetime data analysis prediction indicates the exponential PDF as the best fit. Basically, this happens because the life cycle of such assessment is short and the increasing failure rate time has yet to be achieved.

### 7.3.2 PITFALL 2: TO USE MTBF AND FAILURE RATE AS A PERFORMANCE INDEX

Reliability engineering tools are mostly quantitative and predict different quantitative performance indexes such as reliability, operational availability, failure rate, and Expected time between failure (MTBF).

In many cases, constant failure rate and MTBF are defined as a performance index basically because of the simplicity of such index.

Despite its simplicity, such index does not describe the performance of equipment and components as reliably as reliability.

As described in Chapter 1, depending on the PDF, the MTBF can be dislocated to the right or to the left of the most probable time to failure.

In lognormal PDF cases, the MTBF is dislocated to the right of the most probable time to failure, as shown in Fig. 7.6 (Weibull PDF:  $\beta = 1.2$  and  $\eta = 17,520$  h). The consequence of taking decisions

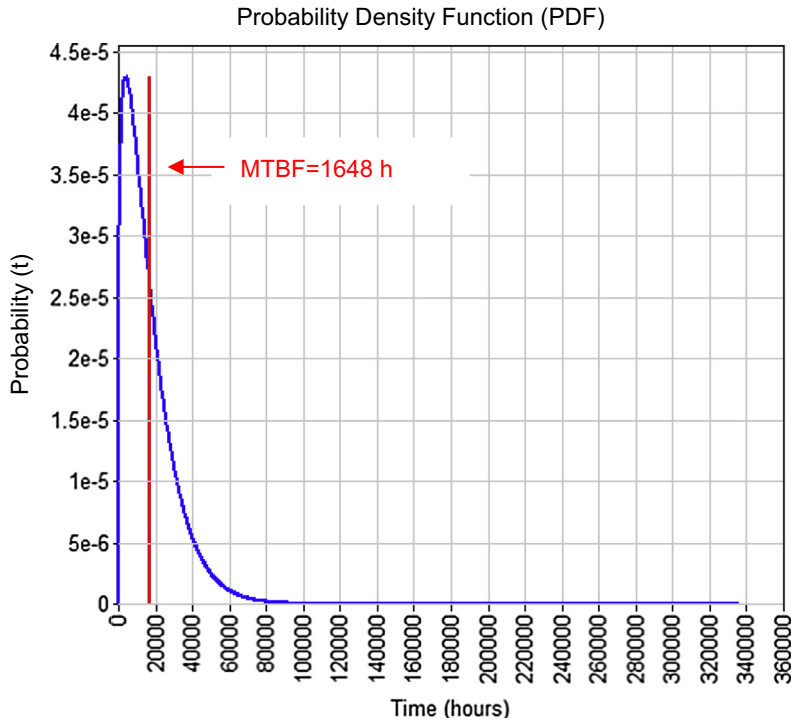


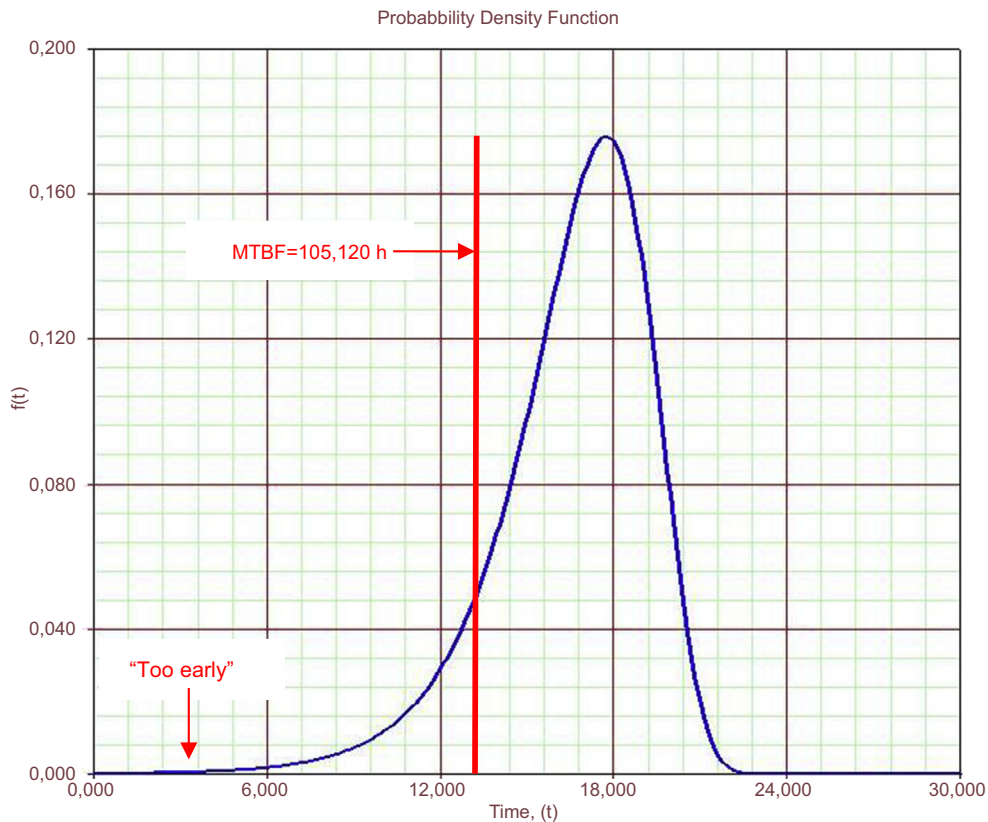
FIGURE 7.6

Lognormal PDF  $\times$  MTBF.

based on MTBF in this case is that the time to perform preventive action will be later than the failure time and most probably the failure will occur before the preventive maintenance. In this specific case, demonstrated in Fig. 7.6, reliability in 1648 h is 40%.

In Gumbel PDF cases, the MTBF is dislocated to the left of the most probable time to failure, as shown in Fig. 7.7 (Gumbel PDF:  $\mu = 15$  years and  $\sigma = 3$  years). The consequence of taking decisions based on MTBF in this case is that the time to perform preventive actions is too early. Therefore many preventive actions will be taking place and the cost of preventive maintenance will be higher than necessary. The other possibility is when preventive action is performed too early, such as inspection, the failure is not detected because the inspection time is out of the P–F interval.

In the case of normal PDF, the MTBF is equal to the most probable time to failure, as shown in Fig. 7.8 (normal PDF:  $\mu = 8760$  h and  $\sigma = 333$  h). However, it is necessary to know the standard deviation to mitigate the risk of taking a later decision or early decisions too early. The problem of taking earlier preventive action decisions is that again, in case of an inspection, the failure might not be

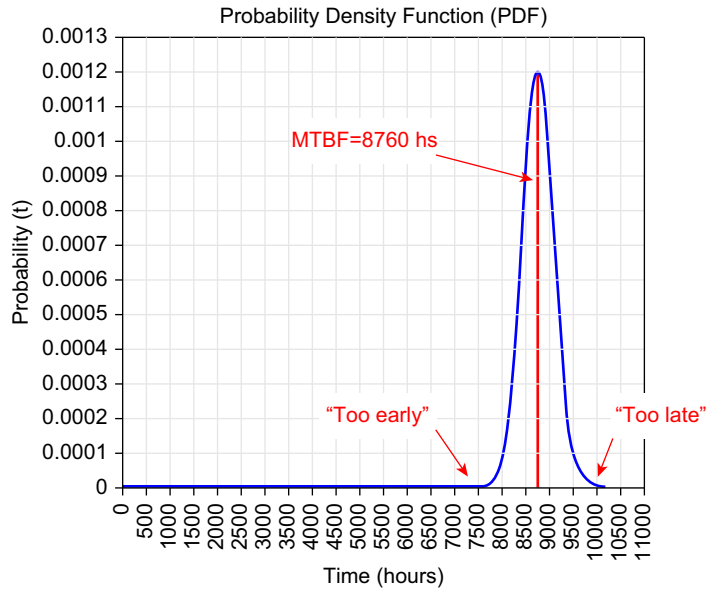


**FIGURE 7.7**

Gumbel PDF  $\times$  MTBF.

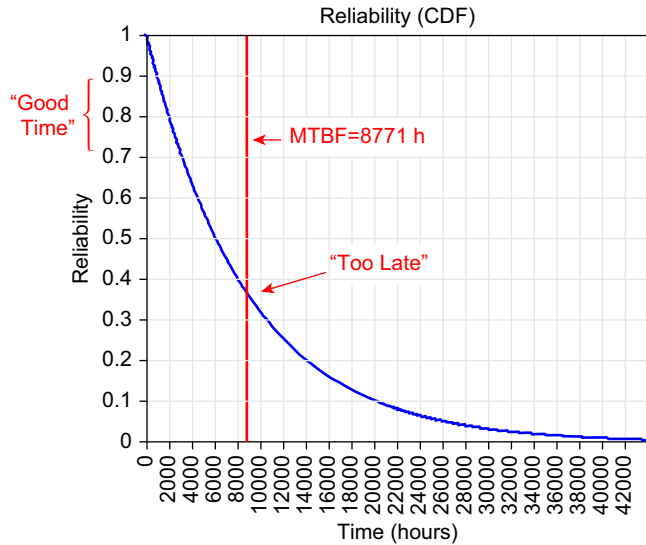
**FIGURE 7.8**

Normal PDF  $\times$  MTBF.



**FIGURE 7.9**

Normal PDF  $\times$  MTBF.



detected. In the case of later preventive action there will be a higher risk that failure happens before the preventive action.

In the case of exponential PDF, the MTBF is also a poorer reference because failure can happen at any time. In this case, the better option is to monitor the equipment condition, perform an inspection, or test to check if the component is available. In fact, based on reliability targets, to face a lower risk of failure will result in the situation shown in Fig. 7.9 (exponential PDF: MTTF = 8771 h).

In fact, for all cases, the most probable time to failure must be verified based on the shape of the PDF. In addition, reliability for a specific period of time is a better index because such performance is associated with a warranty term condition where a specific time without failure is expected.

Constant failure rate is also a problem when used as a performance index. First, such index does not show the risk of failure over time as does reliability. The reliability index shows the chance of equipment performing its function successfully over a period of time. This is to enable a better decision to be made on time rather than other indexes such as constant failure rate and MTBF, which are not related to time. Second, the failure rate in many cases increases in specific periods of time. Therefore preventive action must take place before the unwanted even occurs. Unfortunately, in many safety analyses, such increasing failure rates are not taken into account because the failure rate is considered constant. Maybe this explains why many preventive actions are not implemented to avoid incidents.

### **7.3.3 PITFALL 3: DO NOT CONSIDER THE PREVENTIVE MAINTENANCE EFFECT ON RELIABILITY AND OPERATIONAL AVAILABILITY**

Preventive maintenance is applied to most mechanical equipment. This means scheduled maintenance, inspection, and predictive maintenance. As described in Chapter 3, predictive maintenance has an important role by identifying the potential failure and defining an intervention time for preventive action to take place before the functional failure happens.

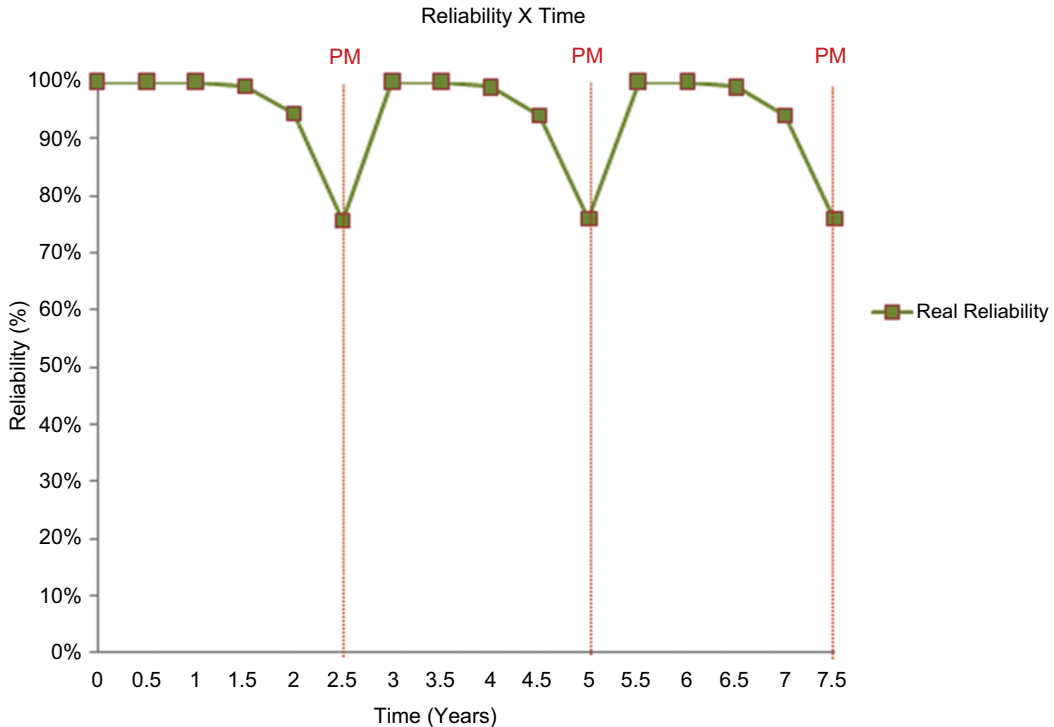
Unfortunately, many RAM analyses do not take into account the preventive maintenance effect on reliability and operational availability. Despite RAM analysis software enabling the possibility of input preventive maintenance, such assessment is not carried out in many cases. This happens because of lack of information about the preventive maintenance tasks and also because of the limitation of certain software to provide the effect of preventive maintenance on reliability and operational availability.

The error that must be avoided when accounting for preventive maintenance during RAM analysis is that the preventive maintenance and corrective maintenance downtime be applied to operational availability. Such errors can happen when the exponential PDF is applied together with preventive maintenance or when software does not perform the correct calculation, as demonstrated in Chapter 3.

In fact, there is a limit to representing online monitoring and other predictive maintenance on RAM software because all parameters are based on a time schedule. In this case, online monitoring and predictive maintenance are associated with a percentage of the equipment life cycle that the failure is expected to be detected.

Preventive maintenance tasks can be defined as a list of tasks for maintenance groups or a result of RCM and RBI analysis. In addition to including preventive maintenance task in RAM analysis, it is also necessary to optimize such a task to minimize the life cycle cost (LCC) and maximize operational availability, as described in Chapter 4. Fig. 7.10 shows the positive effect of preventive maintenance on reliability. Fig. 7.10 does not consider equipment degradation, as discussed in Chapter 4, because in this case the interval of preventive maintenance will reduce to reestablish reliability.

In addition to reestablishing reliability, the second effect is operational availability. As discussed in Chapter 3, such preventive maintenance is a better option if the downtime related to corrective maintenance is higher than the downtime caused by preventive maintenance. In this case, the higher downtime (corrective maintenance) is replaced by a lower downtime (preventive maintenance), which has a positive effect on operational availability.



**FIGURE 7.10**

Preventive maintenance effect on reliability.

The other issue that must be considered is the cost of corrective maintenance and preventive maintenance. In addition, the safety aspect is also important and is more relevant than downtime and cost. This means that preventive maintenance must take place to mitigate a risk even if downtime and cost are higher than corrective maintenance.

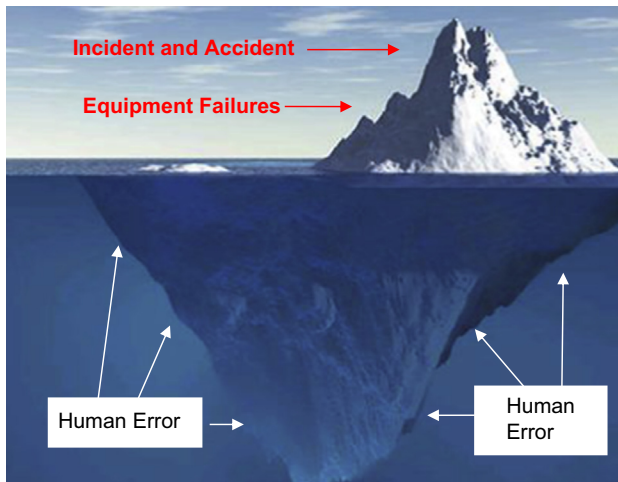
### 7.3.4 PITFALL 4: DO NOT CONSIDER THE HUMAN FACTOR IN RELIABILITY ANALYSIS

The assumption of no human error is a very common approach when qualitative or quantitative reliability analysis is being carried out. Despite the considerable influence on equipment failure root causes and accidents, human error is not taken into account in reliability and risk analysis. Equipment failure and accident root cause because of human error can be hidden, as shown in Fig. 7.11.

Inside organizations, in many cases dealing with human error is a big challenge because it may lead a punishment. However, in some organizations, because of competitiveness between employees to achieve high performance, it is not feasible to discuss human error.

These organizational aspects are huge barriers when trying to implement human reliability analysis together with other safety and reliability analyses.



**FIGURE 7.11**

Iceberg vision of human error.

In terms of methodology, as explained in Chapter 5, many methods can be applied to perform human error predictions and understand the effects of human performance factors. Such methods can be integrated with reliability analysis, such as RAM analysis as demonstrated in Chapter 5 (Section 5.12), risk analysis in Chapter 6 (Section 6.10.3), and FMEA, as demonstrated in Chapter 3.

### 7.3.5 PITFALL 5: DO NOT CONSIDER DIFFERENT OPERATION CONDITION EFFECTS ON RELIABILITY PREDICTION

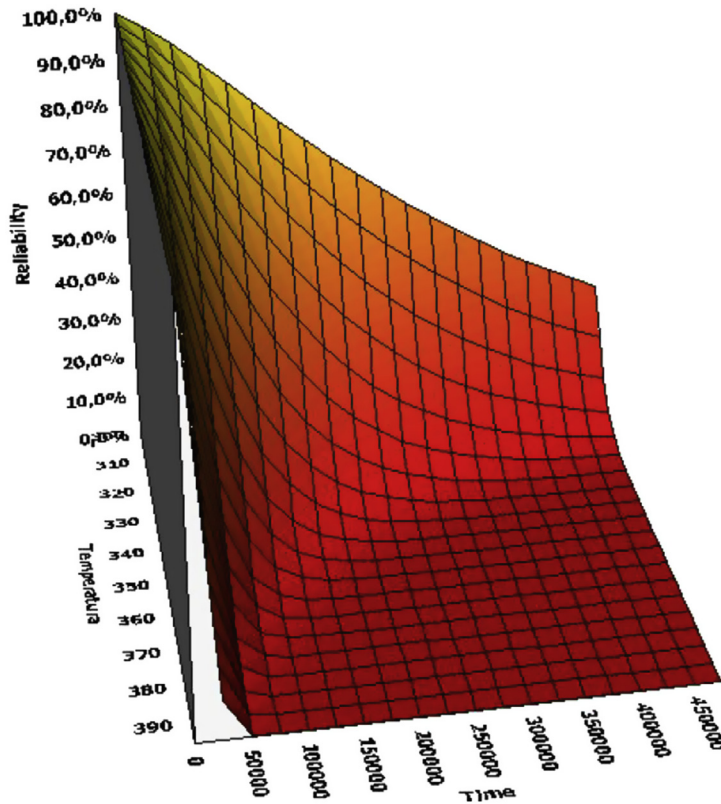
Whenever reliability prediction takes place, one of the most important issues to be taken into account is the operational conditions. The common error in this case is to apply reliability data from standard conditions or even historical data from different operational conditions.

In the case of using historical data from similar equipment, which operates in tougher conditions, reliability prediction will be more pessimistic, which can lead to spending more effort than necessary on improvement actions. However, whenever reliability prediction is based on equipment that operates in less extreme conditions the result will be overoptimistic reliability prediction, which leads to a lack of effort to implement necessary improvements.

Once the historical data for similar equipment is available it is necessary to check the operation conditions, and for each piece of equipment and components it is important to take into account the stress factor.

Chapter 2 has presented different methods to predict reliability based on accelerated test results. Such methods can also be used to predict reliability for different operating conditions, as shown in Fig. 7.12.

In fact, despite the robustness of such methods it is necessary to be aware that for all types of prediction, there's always a confidence level with an acceptable error. Therefore, in the case of unsafe failures or even when the consequence of failures leads to the high loss of production and profits, the strengths of the equipment and products need to be tested. In such cases, the HALT methods must be carried out whenever feasible, as described in Chapter 2.



**FIGURE 7.12**

Reliability based on different operational environmental conditions.

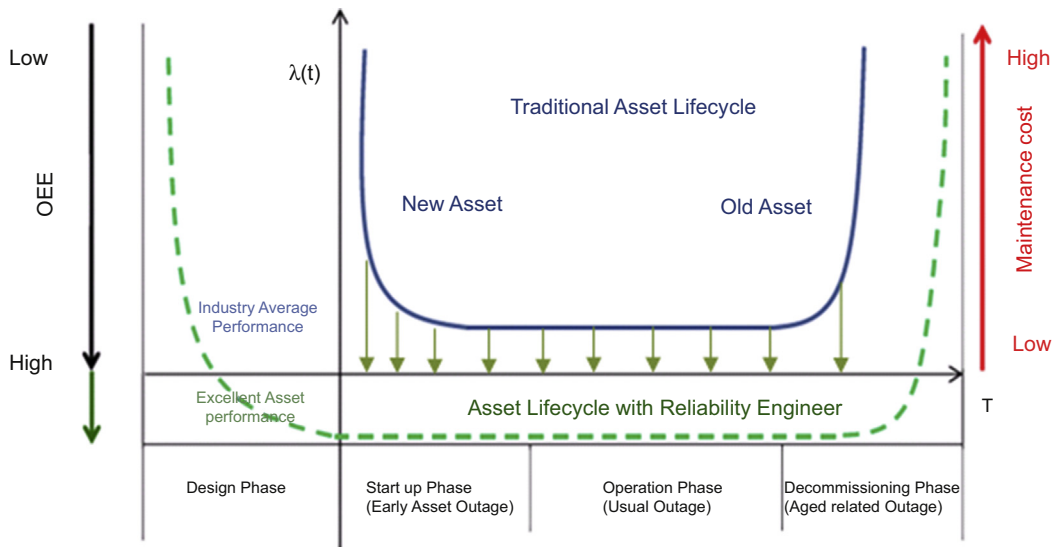
### 7.3.6 PITFALL 6: DO NOT CONSIDER ALT, HALT, AND RGA WHEN NECESSARY

The development of new equipment and components requires the application of reliability verification and validation. For electronics and electrical components, methods such as Accelerate Life Test (ALT), High Accelerate Life Test (HALT) and Reliability Growth Analysis (RGA) can predict component reliability, test product robustness, and also monitor the increase in reliability during improvement actions in the design phase.

Such methods are limited to the dimensions of equipment and also to the conditions that the equipment is intended to test. But even for huge equipment it is possible to test the critical parts and components separately, which enables a fair representation of equipment performance.

Unfortunately, such methods are not applied in many projects because of issues such as lack of time, money, investment, and also lack of requirement from clients for verification and validation of performance during design.

Many organizations still believe that it is better to improve equipment with lower performance during early life than during design. In fact, development during the design phase to eliminate early phase failures also avoids the loss of production during the operation phase.



**FIGURE 7.13**

Bathtub curve improvement based on better design.

The other situation that requires verification tests, such as ALT, HALT, and RGA, is when known equipment or components operate in new environmental conditions. In this case, it is also necessary to implement such tests rather than predict reliability based on standards, or assume that the commission acceptance test is a sufficient demonstration of equipment and component robustness.

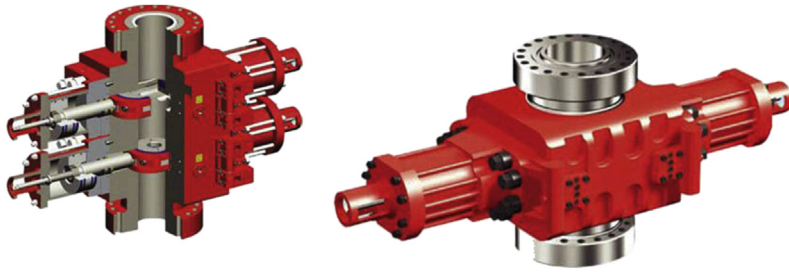
In fact, if no reliability target and warranty contract are defined, such verification tests and development do not make much sense. Unfortunately, many oil and gas companies have been facing problems during operations because of the low performance of equipment during early life. One classic example is safety instrumented functions (SIF) that cause shutdowns in operational plants because of spurious failures, which would have been tested and avoided during the design phase. In most cases, such shutdowns caused by SIF are short term but can happen many times, affecting the performance of other equipment because of the repetitiveness of startup and shutdown.

The application of the ALT, HALT, and RGA methods has the main objective of improving the bathtub curve performance by eliminating early life failures during the design phase as well as other phases of reliability performance, as demonstrated in [Fig. 7.13](#).

### 7.3.7 PITFALL 7: TO APPLY REDUNDANCY TO INCREASE SYSTEM OPERATIONAL AVAILABILITY FOR ALL CASES

Redundancy is an ideal solution in many cases to reduce asset vulnerability to external events and also to improve asset performance.

Nevertheless, it is not the best solution for all cases. In fact, in many projects there are standard solutions to apply redundancies for specific types of components such as pumps, compressors, valves and other equipment. Despite a good solution, it will not assure that the system will achieve high performance if each single equipment does not achieve the minimum level of reliability.



**FIGURE 7.14**

BOP configurations.

Source: [www.botta-equipment.com](http://www.botta-equipment.com).

Therefore, the first mistake concerning redundancy is not to define reliability targets for equipment with redundancies that cause a high operational cost of achieving the system performance target. However, in some cases the redundancies have lower reliability, which affects system performance.

The second important issue is to understand in which conditions the redundancies operate, because in some cases redundancy is not passive but active and has a similar degradation over time when compared with operative equipment.

Finally, unnecessary redundancies that contribute to high operational cost must be the concern of the design engineer. In Chapter 4, case studies 4.6.4, 4.6.7, and 4.6.9 demonstrated the assessment of redundancies.

A good example of redundancy applied to the oil and gas industry is the blowout preventer (BOP), the effectiveness of which relies not only on its configuration, but also on how reliable such layers are to prevent a blowout after a kick. Fig. 7.14 shows the BOP configuration example.

### 7.3.8 PITFALL 8: DO NOT TAKE INTO ACCOUNT QUALITATIVE METHODS RECOMMENDATION TO IMPROVE RELIABILITY PERFORMANCE

Quantitative and qualitative reliability have different objectives and both are important when applied to different asset phases.

The big mistake is to believe that only quantitative methods will be sufficient to support asset high performance. It is also a mistake to believe that qualitative methods will provide a solution.

In fact, quantitative methods such as Lifetime Data Analysis (LDA), RAM, Optimum Replace Time (ORT), ALT, and RGA are more appropriate when predicting and verifying asset performance, such as reliability, operational availability, production efficiency, and other indexes, as defined in Chapter 4 (Section 4.2.4).

Qualitative methods such as FMEA, RBI, RCM, Failure Report and Corrective Actions System (FRACAS), and Root cause Analysis (RCA) are more appropriate to understand failures and suggest actions to prevent such failures. Such information can be applied to improve critical equipment performance defined in quantitative methods (RAM), drive design improvement (DFMEA), and drive the reliability target achievement (RGA).

The main issue is to have a clear understanding of the problem and the type of solution needed to solve it to apply the appropriate method. Depending on the situation, more than one qualitative or quantitative method is required or even a combination of qualitative and quantitative methods, as is shown in Fig. 7.15.

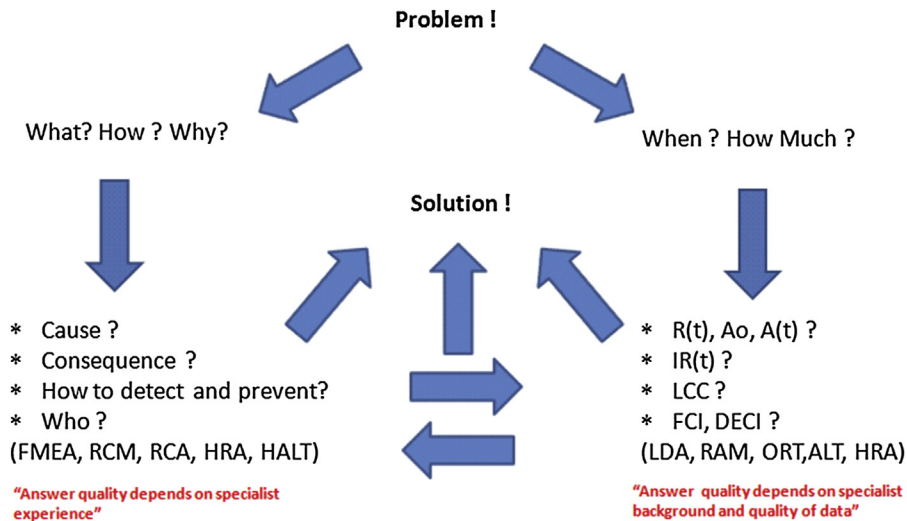


FIGURE 7.15

Qualitative and quantitative reliability engineering methods.

### 7.3.9 PITFALL 9: DO NOT CONSIDER LIFE CYCLE COST AS PART OF RELIABILITY ENGINEERING ANALYSIS

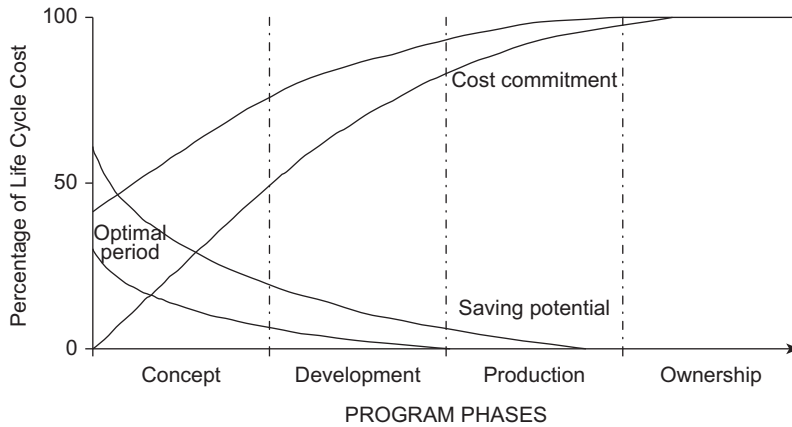
The additional pitfall when reliability engineering is being applied is not to consider the impact of solutions proposed on the LCC. Depending on the asset phase and the type of methods applied the impact on LCC can be easier or harder to predict. However, the necessity to demonstrate the impact on LCC is to get support from top-level leaders of organizations. In fact, this is a usual mistake that many engineers make when a technical solution is proposed. Indeed, in order to communicate technical solution to middle and high level managers, it is important to include the positive effect on LCC and organization profits. In order to get middle and high level managers support, the economic benefit of such technical solution must be demonstrated.

Indeed, different reliability methods such as LDA, RAM analysis, ALT, HALT, RGA, ORT, HRA, FMEA, and RCM have different objectives and depending on the cases, such LCC prediction may be obtained.

In the case of LDA, the LCC can be assessed when comparing the tradeoff between different suppliers of equipment by equating the LCC of higher reliability equipment with lower reliable equipment.

During RAM analysis, different solutions with respect to redundant equipment, system configuration impact of preventive maintenance, and also reduction of redundancy must take into account the impact on LCC.

During design, to demonstrate the reliability target achievement, ensure equipment reliability and robustness, or even improve equipment reliability to achieve targets, it is necessary to implement ALT, HALT, and RGA methods. The main issue in this case is to perform the assessment of the investment during the design phase (CAPEX), which compensates the reduction of operational cost (OPEX). Such assessment depending on a supplier's or customer's point of view might lead to a totally different conclusion. In fact, it is necessary that oil and gas companies define the reliability target for equipment



**FIGURE 7.16**

Early commitment of product life cycle cost.

Source: Michaels and Wood (1989).

and request the assurance of such target achievement from vendors. In many cases, such requirements do not exist or are unclear. In addition, the compensation cost in the case of the reliability requirement achievement not being attained must be clear and be stated in the warranty contract terms. From the supplier's point of view, it is necessary to understand that, more than direct cost, the company's reputation is also an indirect cost, which in many cases pays off the investment of all effort during the design phase to achieve the reliability target defined by the client.

Moreover, it is also important to identify the cost of recommendation defined in the qualitative reliability analysis, such as FMEA, RCM, and RBI. In fact, such methods can identify the cause and consequence of equipment problems as well as the recommendations to mitigate them. The recommendation of such methods focuses on project modifications, procedures, and task implementation, which also has an impact on LCC. Therefore the tradeoff analysis of such recommendation as well as different possible solutions must to be taken into account in terms of LCC impact.

However, it is necessary to be careful whenever safety issues are taken into account because LCC optimization does not mean the best solution in many cases. Finally, whenever it is possible, the result of solutions provided by qualitative or quantitative methods needs to consider the impact on LCC, as shown in Fig. 7.16.

### 7.3.10 PITFALL 10: DO NOT CONSIDER RELIABILITY ENGINEERING AS PART OF ASSET MANAGEMENT

In general terms, the main objective of asset management is to integrate the different organizational levels of the asset performance achievement, as will be explained in detail in the next chapter.

Reliability engineering has an important role in asset management because it enables the achievement of asset high performance of the different application methods. Therefore the reliability engineering program must be integrated with the asset management program to support and enable asset management success.

The common mistake is to keep the reliability program at a low level of organizations to solve and support asset performance achievement and not get higher level organization involvement.

Until the problems of solving asset performance are achieved, reliability will be realized by the top level of organizations as a tool to solve problems and not as a process that must be maintained to constantly achieve and maintain the asset high performance.

---

## 7.4 RELIABILITY ENGINEERING: IMPLEMENTATION OF BARRIERS TO SUCCESSFUL ACHIEVEMENT

The reliability engineering program faces some organizational barriers that have not allowed its full development. Such factors are related to the general organizational culture that is spreading all over the world nowadays, which awards the conservative decisors, standardize methods and procedures and priorities the fast rather the quality delivers. Such factors are organizational culture, leadership and standards procedures application.

- Decisors who face the risk of implementing new methods and approaches to deliver the best solution for their clients even in low demand services situations, which will not give a fast and cheap but certainly a robust result.
- The development of reliability professionals, which encompasses not only training and attractive salaries, but also organizational support and recognition.
- The application of the directives that define a general process and tolls to be applied, but also enable one to think outside the box, to give innovative solutions, and not just follow the standards.

### 7.4.1 THE DECISOR'S PROFILE

The decisor's profile influences all types of program implementation and is the same with reliability engineering. In fact, with regard to reliability engineering it is necessary to have the support of the organizational leaders because the results are available mostly in the medium and long terms. In addition, in some cases it is necessary to consider investment for a longer period of time without return, which is characterized as high-risk investment.

In fact, under different circumstances, different leaders have a different attitudes when facing risk situations. This requires a different approach to convince leaders to support reliability programs.

Basically, the types of decisor profile concerning risk are:

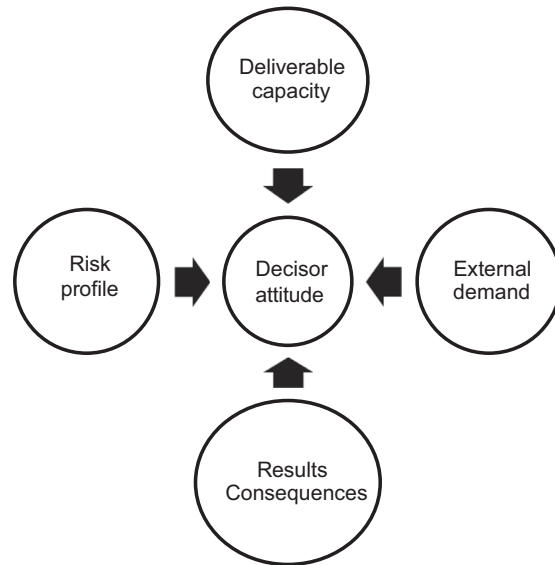
- Risk averse: The decisor who is willing to receive a lower compensation return and face a lower risk of being unsuccessful.
- Risk neutral: The decisor who is willing to receive whatever compensation return and is indifferent about facing a low or high risk of being unsuccessful.
- Risk seeking: The divisor who is willing to face a high risk to receive better compensation or even lower compensation.

Basically, there are four factors that influence the decisor's attitude such as decisor profile, external demand, deliverable capacity, and results, as shown in [Fig. 7.17](#). The decisor profile as previously defined is summarized in three types: risk averse, risk neutral, and risk seeking. The external demands



FIGURE 7.17

The decisor's attitude cycle.



are always related to some expectation of service or product quality and delivery time. Deliverable capacity is related to an individual's or a team's competency to fulfill the external demand expectation. The consequences are the results of positive or negative acceptance of deliverables.

Let us consider two extreme decisor profiles such as risk averse and risk seeking to understand their attitude and how to deal with this to implement reliability programs in the long term.

First, concerning the risk averse profile, whenever the external demand is higher than deliverable capacity, the risk of bad consequences is higher. In this case, the risk averse decisor tends to follow standards, apply a simple approach and methods, and does not support innovative solutions. Under such circumstances, qualitative methods are more easily applied than quantitative methods because quantitative methods require time, robust information, and knowledge. The problem here depends on external demands, and such quantitative methods must be applied, but to have a good result these methods are required more often than defined by external demands. Unfortunately, the risk averse leader usually avoids conflict and because of this avoids negotiating the external demand requirement, demanding more time to deliver with the expected quality of more resources to deliver on time.

It is necessary to understand that conflict is part of life and is different to confrontation. Conflict exists when two opposite ideas or objectives must be discussed to gain a consensus. Confrontation is when one idea or objective is imposed by force against other ideas and objectives without agreement.

The risk averse decisors are comfortable and supportive whenever the external demand is lower than the deliverable capacity. In this case the chance of obtaining a positive result is high.

During the reliability program implementation, mainly at the beginning, external demand is higher than deliverable capacity and this is required in investment technology and training. In this case it is necessary to convince the organization leader of the importance of such investment and clarify that the result is not short term. Unfortunately, because many organizations nowadays have a lack of future vision and focus on short-term results, the reliability program does not get the necessary investment and is unsuccessful.



In some particular situations when an external demand needs to be fulfilled, it is necessary to convince the risk averse decisor that to deliver with quality, more time is required. Unfortunately, because such decisors avoid conflict all the time they tend to prefer to deliver on time with lower quality rather than negotiate more time or resources to deliver with high quality. Such a situation is evident in economically difficult times where there is not enough economical recourses available and any kind of investment must be very well clarified to be approved.

The other decisor profile to be analyzed is the risk-seeking, which is the total opposite of the previous one. In this case, when external demand is higher than deliverable capacity the risk-seeking decisor accepts the risk of a bad result and tries to invest to improve the delivery capacity by training or employing more people to fulfill the demand. When such improvement in deliverable capacity is not possible, such a risk seeking decisor tends to negotiate external demand in terms of time and quality. In fact, such a dessert does not avoid the conflict, but uses conflict as a way to balance external demand with deliverable capacity. The problem with many risk-seeking decisors is that in many cases they turn the conflict into a confrontation and in the long term, starting to lose the other organizational leader's support.

However, when external demand is lower than deliverable capacity, the risk-seeking dessert is uncomfortable and tends to increase external demand or reduce deliverable capacity.

The demands of the reliability engineering program are not constant. Usually, it is more demanding during the design phase than during the operational phase. However, depending on the case, external demand for the project is low, but investment and development must be implemented if it is intended to have a reliability program that supports the whole asset life cycle. The big challenge is to convince risk-seeking decisors that investment and development are necessary for the reliability program during a low external demand situation.

### 7.4.2 THE ORGANIZATIONAL FAST FOOD CULTURE

The second huge barrier to implement a reliability engineering program is the fast food culture, which is widespread in many organizations. The fast food culture means fast delivery, according to a standard solution.

This is a big problem for reliability engineering, which bases its methods on solutions for assets with different characteristics. In fact, even clients have different requirements, which in many cases require a specific solution.

Concerning reliability engineering methods, the classic case is to use generic reliability databases to perform lifetime data analysis based on real historical data.

Unfortunately, the fast food culture prefers to deliver a standardized and rapid solution rather than a reliable and robust solution, which takes longer.

The effect of such a culture is that reliability engineering in the long term is poor because the results of any analysis do not represent reality when compared to the physical world, and the importance and credibility of the power of reliability engineering have been decreasing over time.

The second detrimental effect on reliability engineering is that once the simplest methods and calculations have taken place to ensure faster delivery, many professionals who are not reliability engineers are able to perform such simple calculations and perform reliability analysis based on incorrect concepts and assumptions. A classic example is the case of RAM analysis performed using Excel sheets, which considers constant failure rate and input constant interval of preventive maintenance and delivers an incorrect pessimist asset performance prediction.

The fast food culture encourages reliability engineering pitfalls such as do not implement ALT, HALT, and RGA when they are necessary, apply MTBF and constant failure rate as performance indexes, do not take into account preventive maintenance in reliability analysis, and do take into account different operational conditions when performing a reliability prediction.

In addition, in many projects the fast food culture does not support the implementation of different methods in different asset phases because it requires more time. The classic example is not to perform DFMEA, Process FMEA (PFMEA), System FMEA (SFMEA), and RCM during the project phase.

In fact, what is required is more resources to deliver the external demand with high quality in the expected time. In some cases, this means reducing project profitability, which is not allowed in companies in which economic drivers are to be followed.

### 7.4.3 THE STANDARD APPROACH

The standard approach is easily applied to regulate activities such as security, quality, and safety, which need to be done according to standards, regulations, and laws.

Reliability engineering methods are related to state-of-the-art methods to allow the asset a high performance achievement. This means that the standards are basic and lower limits in terms of reference.

In fact, the state of the art of some methods is rarely described in some standards because the standards are produced by a specialist working group that has a different level of knowledge, experience, and objectives. An additional point is that in many cases, despite understanding the state-of-the-art methods, it, and therefore, the standards are implemented because is faster and easier.

In fact, the state of the art is described in books and scientific papers and the usual approach is described in the standards. However, this is not to minimize the importance of standards as a guideline because in many situations it is not necessary to implement the state of the art.

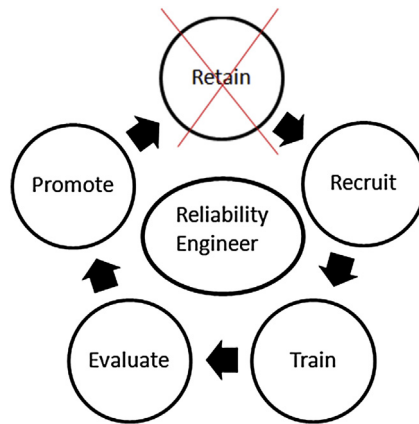
However, what needs to be understood is that standards used for reliability engineering are not legally enforceable and must be followed and never questioned. The standards are guidelines about a specific topic that may be followed or not, which depends on the objective of the application.

As mentioned previously, reliability engineering is supposed to address different solutions for different demands based on usual methods. The standards have a limitation not to address all possible cases, but the most common and usual ones. In fact, it is not the objective of any standard to address all possible cases, but just to give a guideline to initiate a solution.

There are many standards applied to reliability engineering, which are obsolete in terms of data and concepts and need to be updated. Standards can also be used as a reference. A reference does not mean a law or a directive to be followed. In fact, reliability engineering analysis is a clear responsibility of reliability engineers and not a responsibility of standards.

Unfortunately, in many organizations the fast food culture is well supported by standards, which provide simple solutions in less time. Therefore, usually, reliability training is based on standards that are simple to understand and supported by many leaders, which makes the development of reliability engineering professionals easier for the human resources department, which is based on the human resource cycle, as shown in [Fig. 7.18](#).

Reliability engineering encompasses standard knowledge, but the standards do not encompass the whole reliability engineering knowledge. In addition, reliability engineering requires experience and practice for a long period of time, which is not contained in any standard or procedure.

**FIGURE 7.18**

Human recourse cycle for reliability engineers.

Over the years the standard human resource approach for reliability engineers has been failing to support reliability engineering programs in some organizations because the fast food culture does not allow the long-term development of reliability professionals, development that should be based on theoretical knowledge as well as practical experience. Therefore, in many cases, the human resource cycle is not being completed and standardized organizations have been failing in to retain reliability engineers as shows Fig. 7.18.

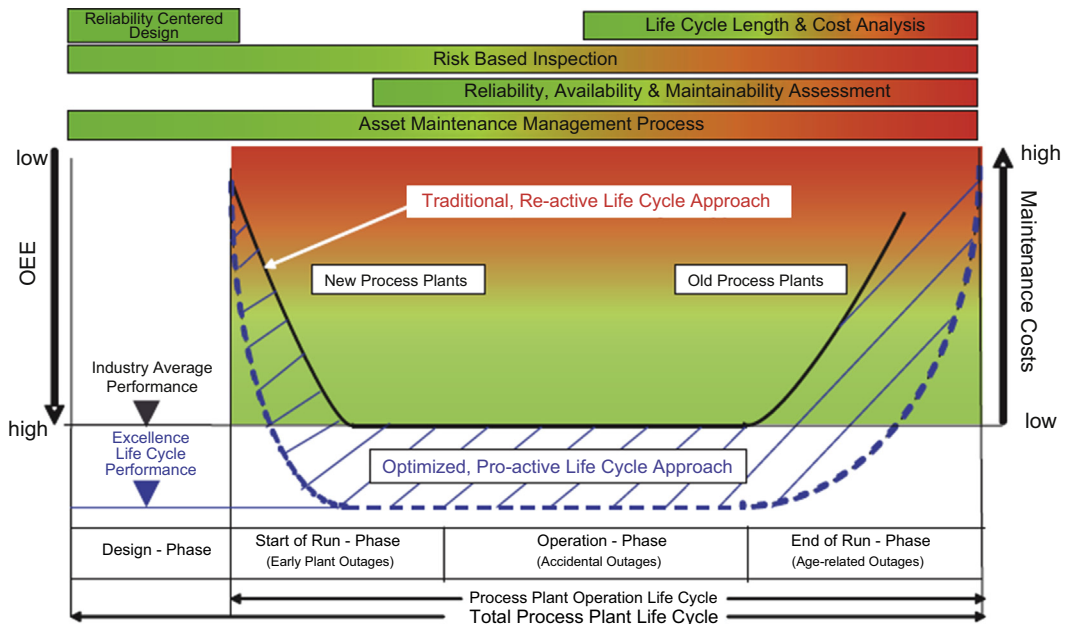
Unfortunately, standardized organizations have been reinforced by the fast food culture and this helps to explain why reliability engineering programs have failed in many organizations.

## 7.5 RELIABILITY MANAGEMENT: SUCCESSFUL CASES

Examples of successful reliability engineering implementation include many world-class companies such as NASA, Siemens, Lufthansa, Bayer, etc. The first example of reliability engineering applied over an enterprise life cycle is a methodology that was developed by Bayer, which uses reliability engineer methods throughout their processes and product life cycles as discussed.

### 7.5.1 BAYER

Facing a challenge of having plants with high availability and attending all customers' requirements is essential for Bayer to manage their assets effectively. Therefore asset life cycle management is "a comprehensive, fully integrated process, directed towards gaining greatest lifetime effectiveness, value and profitability from production and manufacturing asset" (<http://www.bayertechnology.com>). Asset life cycle management assures systematic implementation of processes, practices, and technical improvements to certain sustained compliance with health, safety, environment, and quality (HSEQ) targets, as well as availability and performance targets at the lowest possible cost under consideration of current and future operating and business requirements. Fig. 7.19 summarizes the asset life cycle



**FIGURE 7.19**

Bayer Technology Service asset life cycle management.

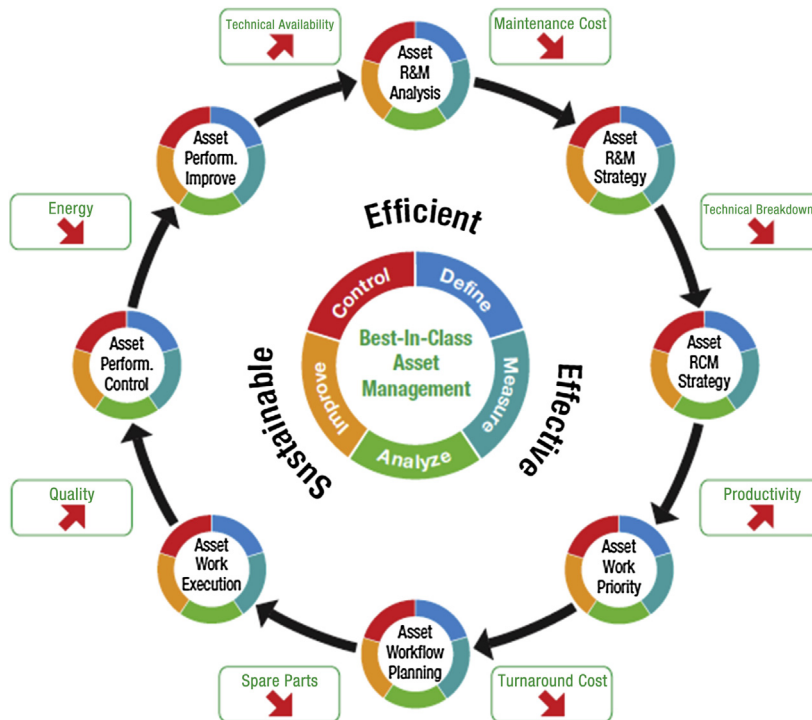
Source: <http://www.bayertechnology.com>.

process management. The main elements of the Bayer Technology Service asset life cycle management are:

- Reliability-centered design (RCD), which assures that reliability and maintenance issues are addressed appropriately during early engineering phases.
- Asset maintenance management processes, which is an integrated, risk-based loop process, ensuring that predefined availability, reliability, and maintainability targets are met without jeopardizing any HSEQ or commercial targets.
- RAM assessment, which addresses RAM topics at any point in time of the asset life cycle.
- Risk-based inspection focuses on the risk-based optimization of the inspection scope.
- LLC analysis is oriented toward determining how medium- to long-term targets can be met under consideration of RAM issues coming up as part of the aging processes of facilities.

In addition, to support asset life cycle management, the asset maintenance process is also used with the objective of optimization of maintenance and reliability at any point of operation utilizing state-of-the-art methodologies, techniques, and tools such as RCM, FMECA, root cause failure analysis, condition monitoring (CM), and bottom-up budgeting. Fig. 7.20 shows how such techniques are applied in asset maintenance processes.

In addition, some organizations, private and governmental, support reliability engineering by promoting events, conferences, meetings, and supporting standards. Such support has been essential



**FIGURE 7.20**

Asset maintenance processes.

Source: <http://www.bayertechnology.com>.

to developing reliability engineering over the years throughout the world. Such organizations include:

- USNRC (United States Nuclear Regulatory Commission)
- ESReDA (European Safety and Reliability and Data Association)
- ESRA (European Safety and Reliability Association)
- SINTEF (Stiftelsen for Industriell og Teknisk Forskning)

### 7.5.2 USNRC (UNITED STATES NUCLEAR REGULATORY COMMISSION)

The US Congress established the Atomic Energy Act of 1946 when regulation was the responsibility of the AEC (Atomic Energy Commission). Eight years later, Congress replaced that law with the Atomic Energy Act of 1954, which for the first time made the development of commercial nuclear power possible. The act assigned the AEC the functions of both encouraging the use of nuclear power and regulating its safety. By 1974, the AEC's regulatory programs had come under such strong attack that Congress decided to abolish the agency. The Energy Reorganization Act of 1974 created the NRC (Nuclear Regulatory Commission) that began operations on January 19, 1975.

On March 28, 1979, the debate over nuclear power safety moved from the hypothetical to reality. An accident at Unit 2 of the Three Mile Island plant in Pennsylvania melted about half of the reactor's core and for a time generated fear that widespread radioactive contamination would result. In the aftermath of the accident, the NRC placed much greater emphasis on operator training and "human factors" in plant performance, severe accidents that could occur as a result of small equipment failures (as occurred at Three Mile Island), emergency planning, plant operating histories, and other matters.

Today the NRC's regulatory activities are focused on reactor safety oversight and reactor license renewal of existing plants, materials safety oversight and materials licensing for a variety of purposes, and waste management of both high-level waste and low-level waste. In addition, the NRC is preparing to evaluate new applications for nuclear plants. Over the past decades, NRC has developed in numerous standards, some of which are related to reliability engineering, giving a great contribution mainly to human reliability analysis. Some standard examples are:

- NUREG-0492: Fault Tree Handbook (January 1981)
- NUREG/CR-2300: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants (December 1982)
- NUREG/CR-3518: SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment (1984)
- NUREG/CR-4772: Accident Sequence Evaluation Program Human Reliability Analysis Procedure (February 1987)
- NUREG-1624: Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA) (May 2000)
- NUREG-0711: Human Factors Engineering Program Review Model (February 2004)
- NUREG/CR-6869: A Reliability Physics Model for Aging of Cable Insulation Materials (March 2005)
- NUREG-1792: Good Practices for Implementing Human Reliability Analysis (HRA) (April 2005)
- NUREG/CR-6883: The SPAR-H Human Reliability Analysis Method (August 2005)
- NUREG/CR-6936: Probabilities of Failure and Uncertainty Estimate Information for Passive Components: A Literature Review (May 2007)
- NUREG/CR-6942: Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments (October 2007)
- NUREG/CR-6947: Human Factors Considerations with Respect to Emerging Technology in Nuclear Power Plants (October 2007)
- NUREG-1880: ATHEANA User's Guide (June 2008)
- NUREG-1921: EPRI/NRC-RES Fire Human Reliability Analysis Guidelines (November 2009)

### 7.5.3 ESReDA (EUROPEAN SAFETY AND RELIABILITY AND DATA ASSOCIATION)

When Swedish marine consultant Arne Ullman set up a forum to share information and risk expertise in October 1973, little did he know he was laying the foundations for one of the world's most significant safety and reliability organizations. It was this forum, the European Reliability Data Association (EUReDatA) that would form the beginnings of ESReDA.

The association was formally launched at the first European reliability Data Bank Conference in Stockholm, with the support of the Swedish Marine Ministry. A total of 11 pioneering associations

from France, Italy, the United Kingdom, Norway, Holland, and Sweden signed up and Ullman was elected as the first president. The ESReDA main objectives are to:

- Promote research and development, and the applications of RAMS techniques;
- Provide a forum to focus the resources and experience in safety and reliability dispersed throughout Europe;
- Foster the development and establishment of RAMS data and databases;
- Harmonize and facilitate European research and development efforts on scientific methods to assess, maintain, and improve RAMS in technical systems;
- Provide a source of specialist knowledge and expertise in RAMS to external bodies such as the European Union;
- Provide a centralized and extensive source of RAMS data;
- Further contribute to education in safety and reliability;
- Contribute to the development of European definitions, methods, and norms.

The successful ESReDA seminar that occurs nowadays twice per year with different topics has been promoting reliability engineering issues discussion and experience among participants.

#### **7.5.4 ESRA (EUROPEAN SAFETY AND RELIABILITY ASSOCIATION)**

ESRA is a nonprofit-making international association that abstains from all political activity. Its sole aim is to stimulate and favor the methodological advancement and practical application of safety and reliability in all areas of human endeavor by:

- Organizing the yearly European Safety and Reliability (ESREL) conference, one of the largest and most renowned in the field with participants from all over Europe and an increasing number from other continents;
- Organizing a number of technical committees, covering a variety of methodological areas (eg, reliability analysis, risk assessment, Monte Carlo simulation, human factors, accident modeling, occupational safety, risk management) and application areas (eg, nuclear, offshore, transportation, information, and communication technology);
- Promoting/organizing workshops and seminars on specific topics;
- Cooperating and exchanging information between national and international professional societies, standard setting organizations, industry, and equivalent groups.

By these means, ESRA provides an arena for peer contacts, dialogues, and information exchanges that foster the creation of collaborations and professional links in the field of reliability and safety. The technical committees, in particular, provide a visible framework for breeding such contacts and exchanges, through the organization of special sessions at the ESREL conferences and the publication of articles in the ESRA newsletter for information knowledge sharing.

#### **7.5.5 SINTEF (STIFTELSEN FOR INDUSTRIELL OG TEKNISK FORSKNING)**

SINTEF was established in 1950 by the Norwegian Institute of Technology, which now forms part of the Norwegian University of Science and Technology (NTNU). The main objectives of SINTEF are:

- To encourage technological and other types of industrially oriented research at the institute;
- To meet the need for research and development in the public and private sectors.



Today, SINTEF is the largest independent research organization in Scandinavia. They create value through knowledge generation, research, and innovation, and develop technological solutions that are brought into practical use. SINTEF operates in partnership with the NTNU in Trondheim, and collaborates with the University of Oslo. NTNU personnel work on SINTEF projects, while many SINTEF staff teaches at NTNU.

SINTEF has approximately 2100 employees, 1500 of whom are located in Trondheim and 420 in Oslo. They have offices in Bergen, Stavanger, and Tromsø, and in addition there are offices in Houston, Texas (USA), Rio de Janeiro (Brazil), and a laboratory in Hirtshals (Denmark). SINTEF's head office is in Trondheim.

Two of the greatest contributions to reliability engineering are the following publications:

- Offshore Reliability Data Handbook (OREDA Handbook);
- PDS Method Handbook and PDS Data Handbook.

The fifth edition of the OREDA Handbook gives data sources of failure rates, failure mode distribution, and repair times for equipment used in the petroleum, petrochemical, and natural gas industries.

The PDS handbooks are ideal when doing reliability analysis of safety instrumented systems. The reliability data in the handbooks are well suited for SIL analyses according to IEC 61508 and IEC 61511 and comprises devices (detectors, transmitters, valves, etc.) and control logic (electronics) failure data.

There are also several universities that have developed a curriculum for preparing reliability engineers all over the world with specializations and courses. Examples include: University of Maryland, University of Tennessee, Karlsruhe Institute of Technology, Indian Institute of Technology Kharagpur, University of Strathclyde Business School, and University of Stavanger. Some of these reliability engineering programs are described in the following sections.

---

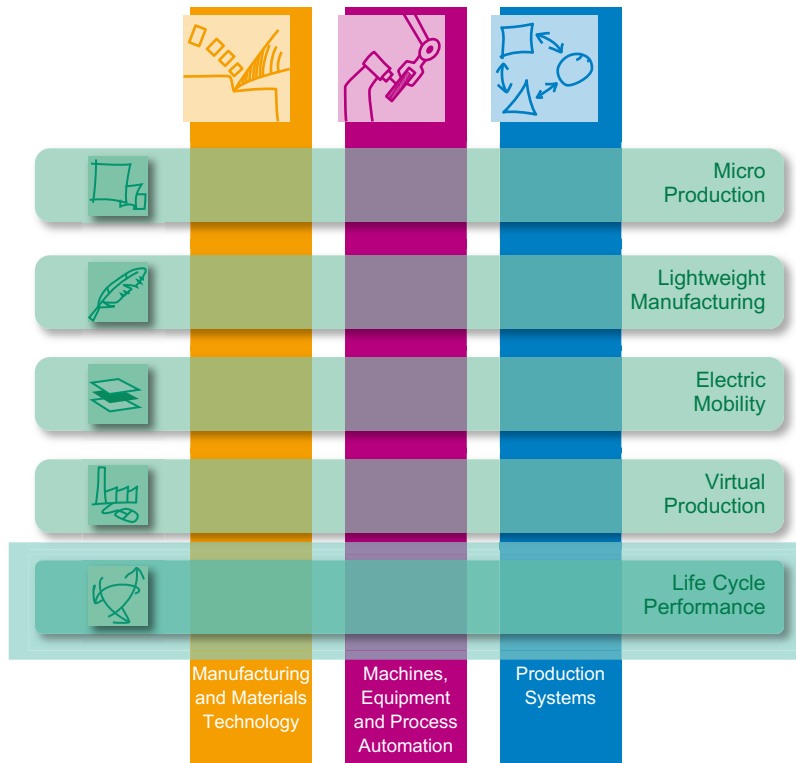
## 7.6 RELIABILITY ENGINEER TEACHING AND RESEARCH: SUCCESSFUL UNIVERSITIES AND RESEARCH CENTER CASES

### 7.6.1 KARLSRUHE INSTITUTE OF TECHNOLOGY

The wbk (Institute of Production Science) is a research institute at the Karlsruhe Institute of Technology (KIT), established October 2, 2009 with the merger of the University Karlsruhe and the Forschungszentrum Karlsruhe in Germany. KIT's main objectives are "positioning the institute as an institution of internationally outstanding research and teaching in the natural sciences and engineering that offers scientific excellence and world class performance in research, education and innovation." The wbk is one of the largest institutes within the department of mechanical engineering at KIT and has 50 scientists and 140 student assistants. The institute is organized into three research departments related to reliability engineering:

- Manufacturing and Materials Technology
- Machines, Equipment, and Processes Automation
- Production Systems





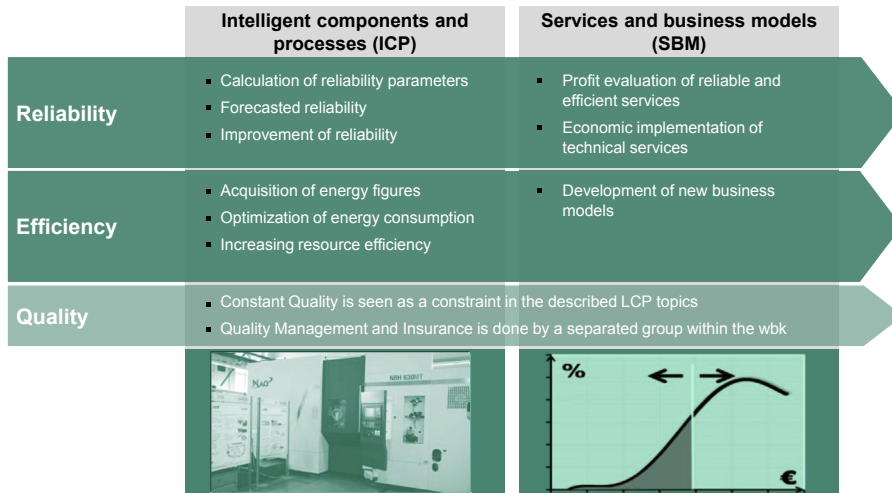
**FIGURE 7.21**

wbk organization.

All these research departments work on different super-ordinated focus areas of research. Besides the already established fields of life cycle performance (LCP), microproduction, and virtual production, new topics have been introduced such as lightweight manufacturing and production for electric mobility. In general, the wbk is matrix structured, as shown in Fig. 7.21.

LCP comprises the evaluation, optimization, and design of reliable and efficient systems throughout their life cycle. The main goals addressed are the reliability, the efficiency, and the quality of processes, machines, and production systems. This means analysis of life cycle costs, reliability and sustainability of technical systems, technical service costs and risk management, simulation and optimization of production systems, and a reliability-adapted spare parts provision. LCP focuses on reliability engineering and includes the following activities:

- Calculation of reliability parameters;
- Statistical failure analysis;
- Methods of durability and fatigue forecasted reliability;



**FIGURE 7.22**

LCP overview.

- Life cycle prediction based on statistical failure analysis;
- Stress tests and durability simulations improvement of reliability;
- Sensor technology and condition monitoring;
- Resilient components.

The LCP overview is shown in [Fig. 7.22](#).

### 7.6.2 INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

This center has been engaged in the areas of life testing, maintenance engineering, safety engineering, and system reliability studies. The technical facilities of this center include equipment such as drop test setup, durability test facilities, impact test facility, reliability analyzer, environmental chambers, and testing facilities including facilities for pump test, burn-in chamber, vibration exciter, switch test machines, corrosion test chamber, and thermal shock chamber. Some of the sponsored projects undertaken by the center include Design and Development of Computerized Condition Monitoring System, Design and Analysis of Protective Sensor Systems, and Safety Studies Information System for Safety and Accident Investigation. The main research areas are software reliability, system reliability analysis, probabilistic safety assessment, network reliability, accelerated life testing reliability, quality engineering, condition monitoring, system, simulation reliability, modeling, and analysis reliability, data analysis reliability, and safety engineering.

Some projects in reliability engineering carried out by Indian Institute of Technology Kharagpur are:

- Flood Probabilistic Safety Assessment of Kakrapara Nuclear Power Plant;
- Reliability Prediction, FMEA/FMECA, Modeling of LSS of Fighter Aircraft;
- Reliability Modeling and Analysis of Integrated Test Range;

- Reliability Work Package for Missile Project: Phase II;
- Reliability Improvement of Metering Products;
- Reliability Prediction, Modeling, and FMEA of Life Support System;
- Reliability Modeling and Analysis of Interim Test Range;
- Reliability and Maintenance Work Package for Generators/Motors;
- System Study on Remote Assessment of Residual Mission Reliability of Equipment Through Condition-Based Monitoring;
- Assessment of Residual Reliability of Armored Fighting Vehicles Through CBM.

### 7.6.3 UNIVERSITY OF STRATHCLYDE BUSINESS SCHOOL

The department of management science has led the formation of a University of Strathclyde Centre for Risk, Safety and Uncertainty Management. This is a collaboration between researchers in business, science, social science, and engineering and should provide a stimulating environment in which to work.

This MRes in risk and reliability started in 2004 and differs from conventional MSc qualifications in two ways. First, the split between taught courses and research projects is equal for the MRes compared with most conventional MScs where the split is two-thirds taught program and one-third project. Second, within the MRes there is a substantial emphasis on research training in the taught part of the course with the aim of producing graduates who can select appropriate methodologies with which to approach the industrial research problem at hand. The course aims to produce graduates with:

- In-depth understanding of the theory and practice of risk and reliability analysis;
- Sophisticated research skills relevant to modern industrial challenges.

The technical classes include subjects such as basic reliability theory and techniques, advanced system reliability modeling, modeling within reliability and maintainability, risk analysis and management, foundations of risk, and risk governance.

Some important projects conducted by the Centre for Risk, Safety, and Uncertainty Management are:

- Kenneth Hutchison project;
- Ashley Russell project;
- Mapping out the flows of information during the design and development of complex systems;
- MOD concerning the assessment of reliability cases at the procurement stage;
- Multicriteria risk assessment in the supply chain and the system dynamic risk assessment.

### 7.6.4 UNIVERSITY OF STAVANGER

Since its formation in 1998 the Center for Industrial Asset Management (CIAM), led by the University of Stavanger, has developed into a strong cluster of companies both land based as well as oil and gas related, together with other educational bodies and research institutions. The business concept of the center is toward the establishment of smart engineering assets with operational excellence and technology integration for increased competitiveness and value creation through collaboration on effective asset management principles and practices.

CIAM also offers research and educational opportunities for prospective students in offshore technology with a focus on industrial asset management. They receive advanced knowledge within engineering and management of advanced, complex, and integrated industrial assets and production facilities/systems.

The industrial asset management profile of CIAM comprises a number of disciplines, including operations and maintenance engineering, risk-based maintenance, human-technology-organizational issues, industrial service, decision engineering and performance management, investment analysis and life cycle costs/profits, project management, etc.

CIAM offers a number of value-creating activities for its partners inclusive of research and development projects, thematic seminars, professional conferences, workshops with leading experts, study visits to sites of specific industries, joint industry projects, technology demonstrations, education and competence development programs, etc.

---

## 7.7 RELIABILITY MANAGEMENT FINAL THOUGHTS

The main objective of this book is to give readers the main reliability engineering techniques with specific examples applied to the oil and gas and industry.

A big challenge is to clearly explain complex concepts to make daily reliability engineering applications easier. But to successfully implement reliability engineering in current processes, more knowledge is necessary.

As with other engineering specializations, reliability engineering offers an opportunity to learn and teach, as well as exchange ideas with other reliability specialists. Since the world of reliability engineering is vast, most reliability engineers will not have the chance to apply all the methods, but there is always something new to learn or update and that is what makes reliability engineering so interesting.

Understanding the mathematical models in this book is essential to practicing reliability engineering. Today software makes the mathematical processes easier, but it is still important to know and understand the fundamentals. Operational and maintenance experience is also very important and requires learning about the equipment and systems hands on in various industries. This includes listening to the experiences of operators and maintenance professionals and creating solutions with them, never forgetting that they are the ones who know the equipment best and the ones operating or performing maintenance.

Learning reliability engineering requires time and dedication. But more than this, you should also enjoy the process of analyzing and testing equipment.

There are not many universities or courses on reliability engineering offered today, especially when compared to other subjects, but the courses and programs that are available are excellent and will support you in your career goals.

We live in a competitive world, and reliability engineering offers the chance to be more competitive (in availability and reliability) in business. Some challenges in reliability engineering today include:

- Many companies nowadays do not have good failure data to support analysis and decision.
- Many industries like oil and gas need to develop common failure historical data reports to be used in reliability analysis.
- Many specialists nowadays do not consider the human factor in reliability analysis when it is relevant.

- Nowadays it is not so usual to use accelerated test results to predict equipment reliability and PDF parameters in RAM. The equipment supplier must carry on accelerated tests and supply their customers with such information.
- Risk analysis must be linked to life cycle analysis to have more accurate final results.

These aspects are good opportunities to apply reliability engineering in the years to come. Over the past 13 years in the oil and gas industry, reliability engineering has shown to be a successful application to support operational and maintenance decisions and drive plants to achieve high performance.

Reliability engineering must be applied more routinely, not only when there is a new project or when a plant is suffering from poor performance. Such concepts and applications will bring benefits for all oil and gas industry companies as well as for companies that supply equipment.

---

## REFERENCES

- Porter M.E., 1998. *Competitive Strategy: Techniques for Analyzing Industries and Competitors*. ISBN-13: 978-0684841489.
- Michaels, J., Wood, M., 1989. *Design to cost*. J Wiley & Sons Inc., 413 p.
- BSI PAS 55:2008, Institute of Asset Management.

---

## FURTHER READING

- Asset Maintenance Process. [www.bayertechnology.com](http://www.bayertechnology.com).
- Bayer Technology Services Asset Life Cycle Management. [www.bayertechnology.com](http://www.bayertechnology.com).
- <http://www.nrc.gov/>.
- <http://www.ieee.org>.
- <http://www.esreda.org>.
- <http://www.esrahomepage.org>.
- <http://www.sintef.no/home>.
- <http://www.enre.umd.edu/>.
- <http://www.rmc.utk.edu/index.php>.
- <http://www.wbk.kit.edu/english/124.php>.
- <http://iitkgp.ac.in/departments/home.php?deptcode=RE>.
- [http://www.sbs.strath.ac.uk/researchers/risk\\_and\\_reliability/](http://www.sbs.strath.ac.uk/researchers/risk_and_reliability/).
- [http://www.uis.no/research/industrial\\_asset\\_management/](http://www.uis.no/research/industrial_asset_management/).
- <http://www.mie.utoronto.ca/research/>.
- Motor Management Solution. <http://www.sea.siemens.com/us/Services>.
- Porter Michael, E., 1980. *Competitive Strategy. Technique to Analyzing Industry and Competitors*. Free Press, New York.
- R&M process. NASA-STD-8729-1. <http://www.hq.nasa.gov>.
- Reliability Management Process. [www.lufthansa-technik.com](http://www.lufthansa-technik.com).

## ASSET MANAGEMENT

## 8

**CHAPTER OUTLINE**

<b>8.1 Asset Management</b> .....	<b>703</b>
<b>8.2 Asset Integrity Management</b> .....	<b>719</b>
<b>8.3 Integrated Logistic Support</b> .....	<b>723</b>
<b>8.4 Asset Management Program Evaluation</b> .....	<b>727</b>
<b>8.5 Asset Management Case Studies</b> .....	<b>734</b>
8.5.1 Asset Integrity Management Implementation During the Design Phase:	
The Subsea Case Study.....	735
<i>Asset Integrity Management Phases</i> .....	735
<i>Asset Integrity Management: Flexible Riser</i> .....	736
8.5.2 Asset Integrity Management Implementation During the Predesign Phase:	
The Sulfur Recovery Plant Case .....	742
<i>Conclusions</i> .....	747
8.5.3 Integrated Logistic Support During the Design Phase: The Subsea Case Study.....	750
<i>Conclusion</i> .....	754
8.5.4 Asset Management Program Evaluation During the Design Phase:	
The Offshore Case Study .....	754
<i>Asset Management Aspects Evaluation</i> .....	756
<b>References</b> .....	<b>766</b>

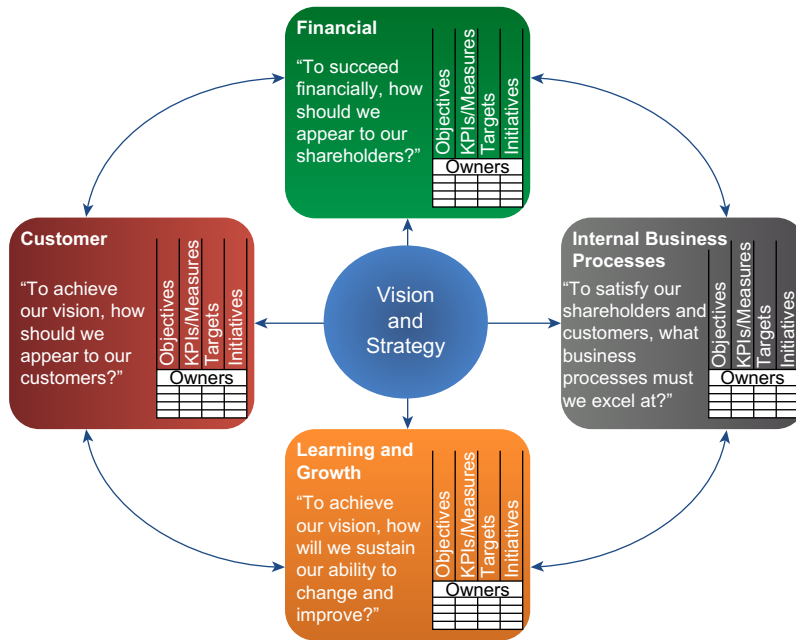
**8.1 ASSET MANAGEMENT**

Asset management is not a new concept for the oil and gas industry and other industries. Indeed, since an asset is part of the company's portfolio, some level of performance is expected for such asset.

In the oil and gas industry, plants and equipment have always had a target performance index that must be followed up.

In the 1990s, the famous balanced scorecard (BSC) management model brought a new concept of performance that was also applied by most oil and gas companies worldwide. Despite being a program not fully implemented by many companies, the BSC concept was a baseline performance management concept for different industries worldwide as well as oil and gas.

Basically, more than a process for performance index achievement, the BSC defines that it is also necessary to consider the financial, customer, and learning and growth perspectives as shown in



**FIGURE 8.1**

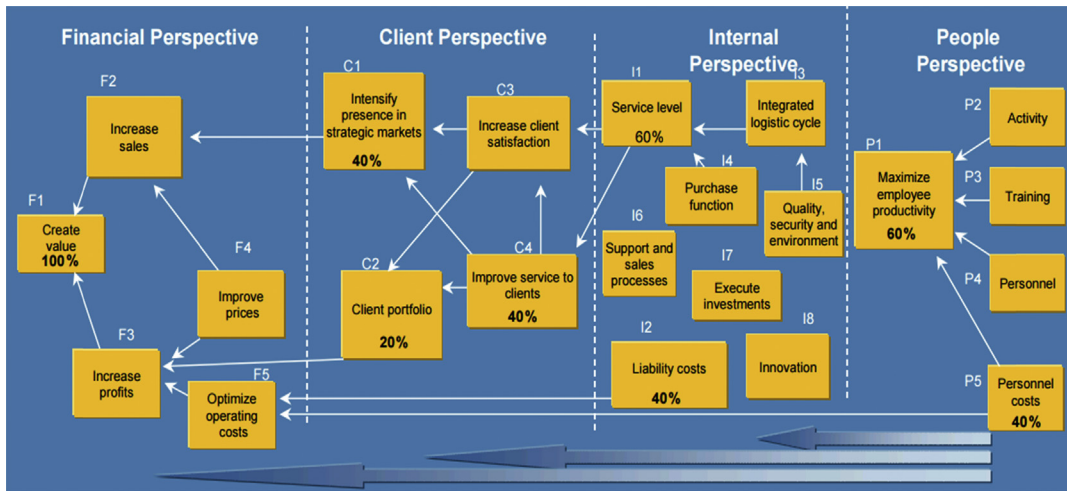
Balanced scored card.

Source: Kaplan, R.S., Norton, D.P., 1996. *The Balanced Scorecard: Translating Strategy into Action*. Boston, MA.: Harvard Business School Press, ISBN 978-0875846514.

Fig. 8.1. Such perspectives that concern the stakeholders and customer satisfaction achievement are based on performance results.

The financial factor links the internal financial result with the stakeholder's expectations. The customer factor links the product and service performance as well as the organization vision and mission to the stakeholder expectations. The internal business process is the basis for stakeholders and customer satisfaction by performance index achievement. Finally, to achieve high performance it is necessary to develop organizational learning and growth capacity, which gives organizations the ability to change and improve their internal processes to achieve high process performance and customer and client satisfaction.

One of the first successes of BSC implementation in the oil and gas industry was Repsol in 2001. The concept of BSC was implemented following the first step by strategic objective definition as well as the definition of the cause and effect of each initiative action to the strategic objectives, as shown in Fig. 8.2. Therefore for each BSC perspective the main objectives and weight have been defined for each one. The next step was to define the performance index to support the BSC. In the case of finance perspective, the main objective was to create value and to do that it is necessary to increase profits and sales. From the client's point of view, the main objectives are intensive presence in strategic markets, client portfolio, and improvement in client service. The internal process perspective focuses on service level and liability cost. The people perspective has the main objective of maximizing employee productivity and managing personal cost.



**FIGURE 8.2**

Balanced scorecard perspective objectives.

Source: Accenture, 2001. *Repsol YPF - A complete implementation model of balanced scorecards in the Oil and Gas sector.*

SeUGI 19. Florence. June 2001.

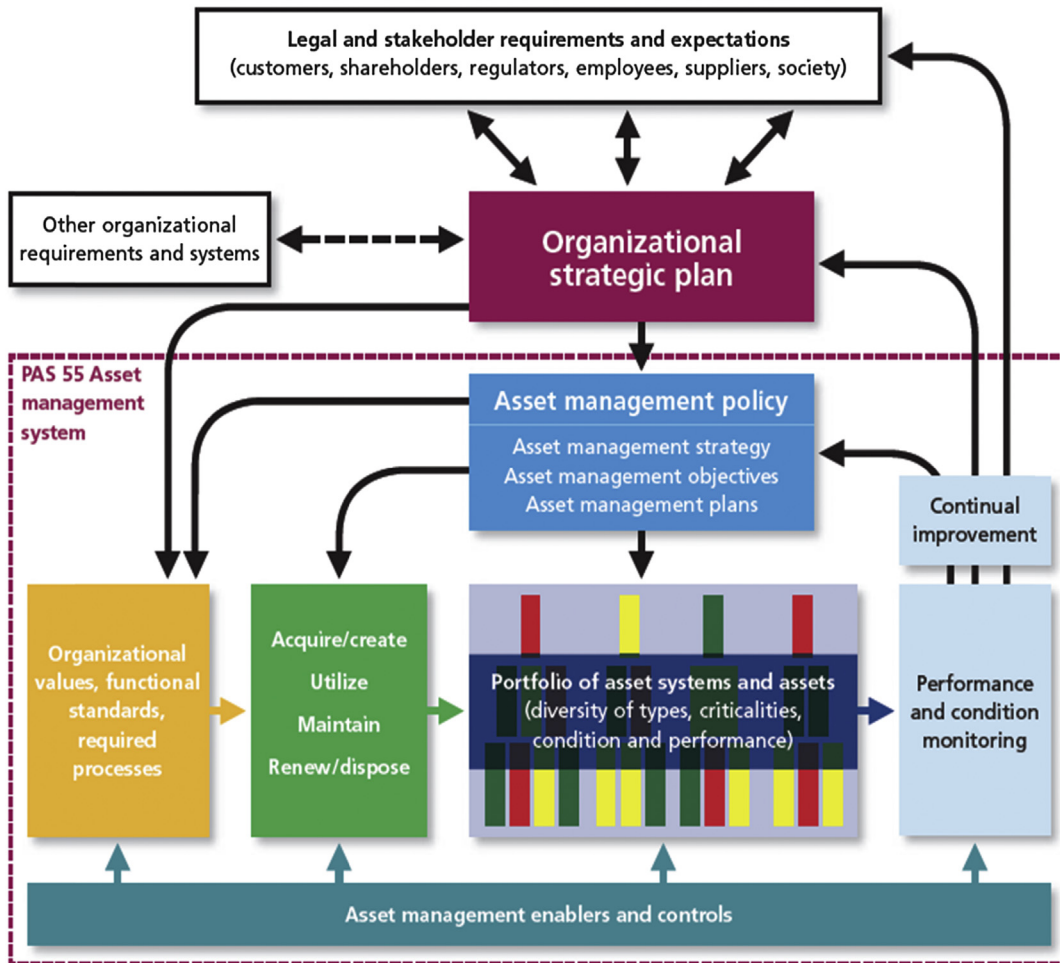
Based on such strategic objectives, the key performance index (KPI) for each perspective was defined and followed up. In the finance perspective, for example, the KPI “relative sales,” which measure the percentage of product sales relative to total sales, was established as a performance index.

In the oil and gas industry, the BSC has proved to be a successful management model, which enables the top organizational level to follow up the whole organization performance. Furthermore, the top-level index can be applied to different organization levels, which enables performance throughout the organization to be monitored. Such a model has been successfully implemented in different oil and gas companies such as Shell, Repsol, and Statoil.

Nevertheless, a particular aspect in the oil and gas industry is that performance is highly affected by the process perspective, which also includes safety and environmental effects as well as asset reliability. Because of the necessity of managing asset reliability and risk related to safety and the environment, a robust approach became necessary.

Asset management, similar to the BSC model, entails the development of business strategy, integrated to all organizational levels, as summarized in Fig. 8.3. The concept of asset management proposed by PAS 55 is: “to integrate legal and stakeholder requirement and expectation.” In this case, stakeholders are all agents affected by asset performance, such as customers, organizational stakeholders, regulators, suppliers, employees, and society. Therefore, based on such stakeholder requirement, the organization needs to define the strategy and a strategic plan, which includes an asset management policy, objectives, and performance index for each strategic objective. Such a strategy influences organizational values and is supported by standards, organizational culture, and organizational leaders at different levels.





**FIGURE 8.3**  
Asset management.

Source: PAS 55 standard, 2008. <http://www.bsigroup.com/en-GB/search-results/?q=PAS+55>.

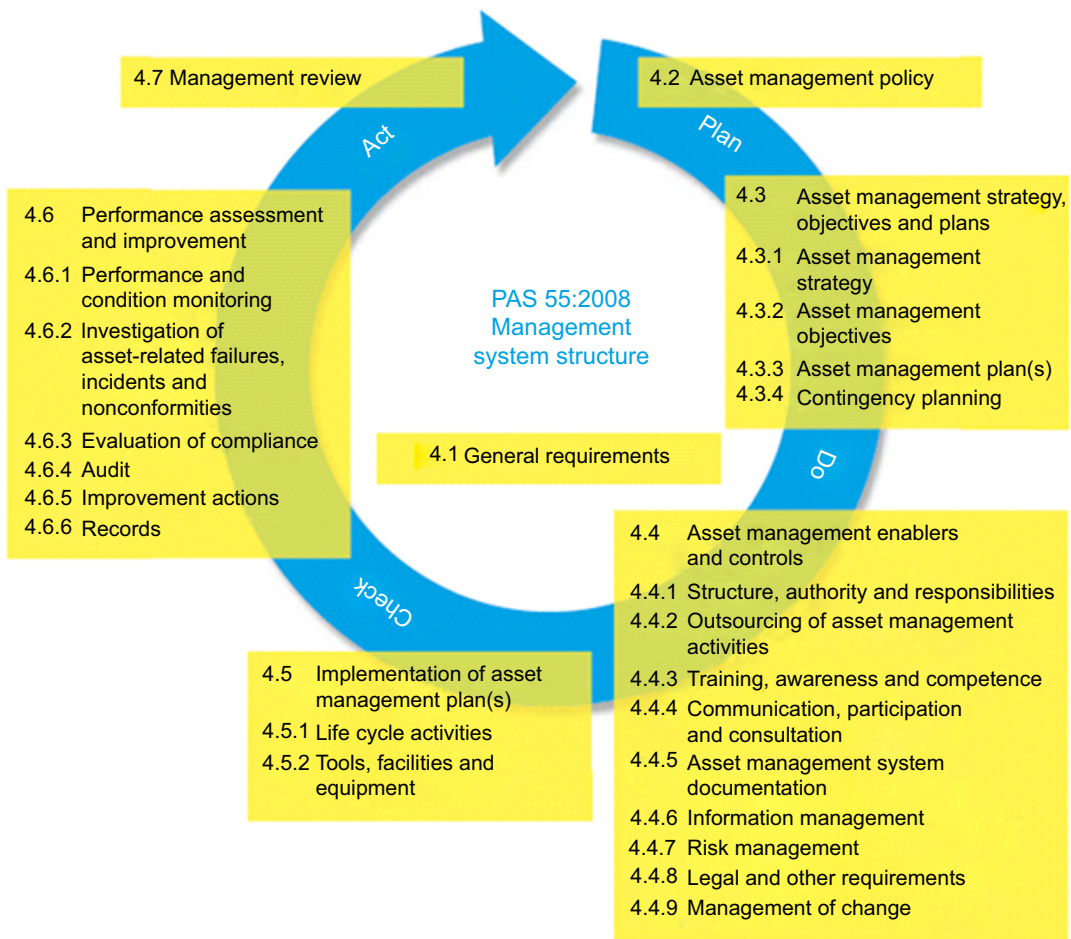
To monitor asset performance based on KPI, asset management enablers and controls are set up at different organizational levels. Therefore, based on KPI results, improvement actions may be implemented depending on necessity.

One of the most important expectations of asset management implementation is financial performance improvement and stakeholder satisfaction. These two objectives are not always easy to achieve together, but require a coordinated effort and clear understanding of all factors involved in the asset management process.

Return on capital employed may increase after asset management implementation because of the achievement of higher asset performance with lower cost. Such achievement is based on asset

optimization as discussed in Chapter 4. In fact, PAS 55 does not define how to achieve such optimal performance. Therefore the implementation of reliability engineering methods together with life cycle cost (LCC) and performance optimization enables the achievement of such optimal performance.

The concept of asset management proposed by PAS 55 is based on the Deming cycle, which encompass the phases planning, do, check, and act (PDCA), as shown in Fig. 8.4. During the planning phase, the asset management policy must be defined as well as the strategic plans and objectives. Further, the next step is to define the responsibilities, activities, communication, documentation, legal, and additional requirements. Furthermore, the plans' activities can be performed throughout the asset life cycle and during the verification phase; the KPIs as well as the audit process will indicate the necessity for improvement.



**FIGURE 8.4**

Asset management PDCA.

Source: PAS 55 standard, 2008. <http://www.bsigroup.com/en-GB/search-results?q=PAS+55>.

In fact, the asset management proposed by PAS 55 is not only a KPI monitoring process. It requires constant involvement of different leaders at different organizational levels as well as the structured management system to support such success achievement over the asset life cycle.

The PAS 55 has a similar structure when compared with other ISO standards, as shown in Fig. 8.5. Therefore, for most oil and gas companies who have already implemented ISO 9001, ISO 14001, and

PAS 55:2008	OHSAS 18001:2007	ISO 14001:2004	ISO 9001:2000
0 Introduction	0 Introduction	0 Introduction	0 Introduction
1 Scope	1 Scope	1 Scope	1 Scope
2 Normative references	2 Normative references	2 Normative references	2 Normative references
3 Terms and definitions	3 Terms and definitions	3 Terms and definitions	3 Terms and definitions
4 Asset management system requirements (title only)	4 OH&S management system elements (title only)	4 Environmental management system requirements (title only)	4 Quality management system (title only)
4.1 General requirements	4.1 General requirements	4.1 General requirements	4.1 General requirements
4.2 Asset management policy	4.2 OH&S policy	4.2 Environmental policy	5.1 Management commitment 5.3 Quality policy
4.3 Asset management strategy, objectives and plans (title only)	4.3 Planning (title only)	4.3 Planning (title only)	5.4 Planning (title only)
4.3.1 Asset management strategy	–	–	–
4.3.2 Asset management objectives	4.3.3 Objectives and programme(s)	4.3.3 Objectives, targets and programme(s)	5.4.1 Quality objectives
4.3.3 Asset management plan(s)	4.3.3 Objectives and programme(s)	4.3.3 Objectives, targets and programme(s)	5.4.2 Quality management system planning 7.1 Planning of product realization
4.3.4 Contingency planning	4.4.7 Emergency preparedness and response	4.4.7 Emergency preparedness and response	–
4.4 Asset management enablers and controls	–	–	–
4.4.1 Structure, authority and responsibilities	4.4.1 Resources, roles, responsibility, accountability and authority	4.4.1 Resources, roles, responsibility and authority	5.1 Management commitment 6.1 Provision of resources 6.3 Infrastructure
4.4.2 Outsourcing of asset management activities	–	–	–
4.4.3 Training, awareness and competence	4.4.2 Competence, training and awareness	4.4.2 Competence, training and awareness	6.2.1 (Human resources) General 6.2.2 Competence, awareness and training
4.4.4 Communication, participation and consultation	4.4.3 Communication, participation and consultation	4.4.3 Communication	5.5.3 Internal communication 7.2.3 Customer communication
4.4.5 Asset management system documentation	4.4.4 Documentation 4.4.5 Control of documents	4.4.4 Documentation 4.4.5 Control of documents	4.2.1 (Documentation requirements) General 4.2.3 Control of documents

FIGURE 8.5

PAS 55 items related to ISO standards.

OHSAS 18001, this is a similar system process that can be integrated with the other ISO standard systems and use all the common structures such as informatics technology, documentation structure, audit structure, procedures, and standards.

Nevertheless, the main objective of asset management is not to implement a new ISO standard and get the certificate but have a structured framework to support the asset management process throughout the asset life cycle. Therefore, oil and gas companies can also use the PAS 55 as a guideline to support their asset management.

The new asset management version is the standard series ISO 55000, which includes ISO 55000, ISO 55001, and ISO 55002. The ISO 55000 is related to the terms and definitions. The ISO 55001 is related to asset management requirements and the ISO 55002 is related to the guideline for the application of ISO 55001.

In general terms the series ISO 55000 encompasses similar aspects described in PAS 55 including the organizational context. Therefore the element of asset management based on ISO 55000 is described as follows (ISO 55001, 2014):

- Context of the organization
- Leadership
- Planning
- Support
- Operation
- Performance evaluation

Context of the organization includes internal and external contexts. The external context includes the social, cultural, economic, and physical environments, as well as regulatory, financial, and other constraints. The internal context includes organizational culture and environment, as well as the mission, vision, and values of the organization.

Leadership includes the top management who is responsible for developing the asset management policy and asset management objectives and for aligning them with the organizational objectives. Leaders at all levels are involved in the planning, implementation, and operation of the asset management system.

Planning and direction of the organization's activities includes its asset management activities. The organizational objectives are generally produced from the organization's strategic level planning activities and are documented in an organizational plan.

Support will require collaboration among many parts of the organization. This collaboration often involves the sharing of resources. Coordinating these resources and applying, verifying, and improving their use should be the objectives of the asset management system. It should also promote awareness of the asset management objectives across the whole organization.

Operation enables the directing, implementation, and control of its asset management activities, including those that have been outsourced. Functional policies, technical standards, plans, and processes for the implementation of the asset management plans should be fed back into the design and operation of the asset management system.

Performance evaluation can be direct or indirect, financial or nonfinancial. Effective asset data management and the transformation of data into information is a key to measuring asset performance. Monitoring, analysis, and evaluation of this information should be a continuous process. Asset

performance evaluations should be conducted on assets managed directly by the organization and on assets that are outsourced.

Fig. 8.6 describes the asset management element relationship based on ISO 55000.

Whenever the asset management discussion takes place, it is necessary to be careful as to what is meant by asset. The assets concept includes tangible assets such as production facilities, logistical assets and support systems, as well as intangible assets such as reputation and external relationships, work culture, and organizational knowledge.

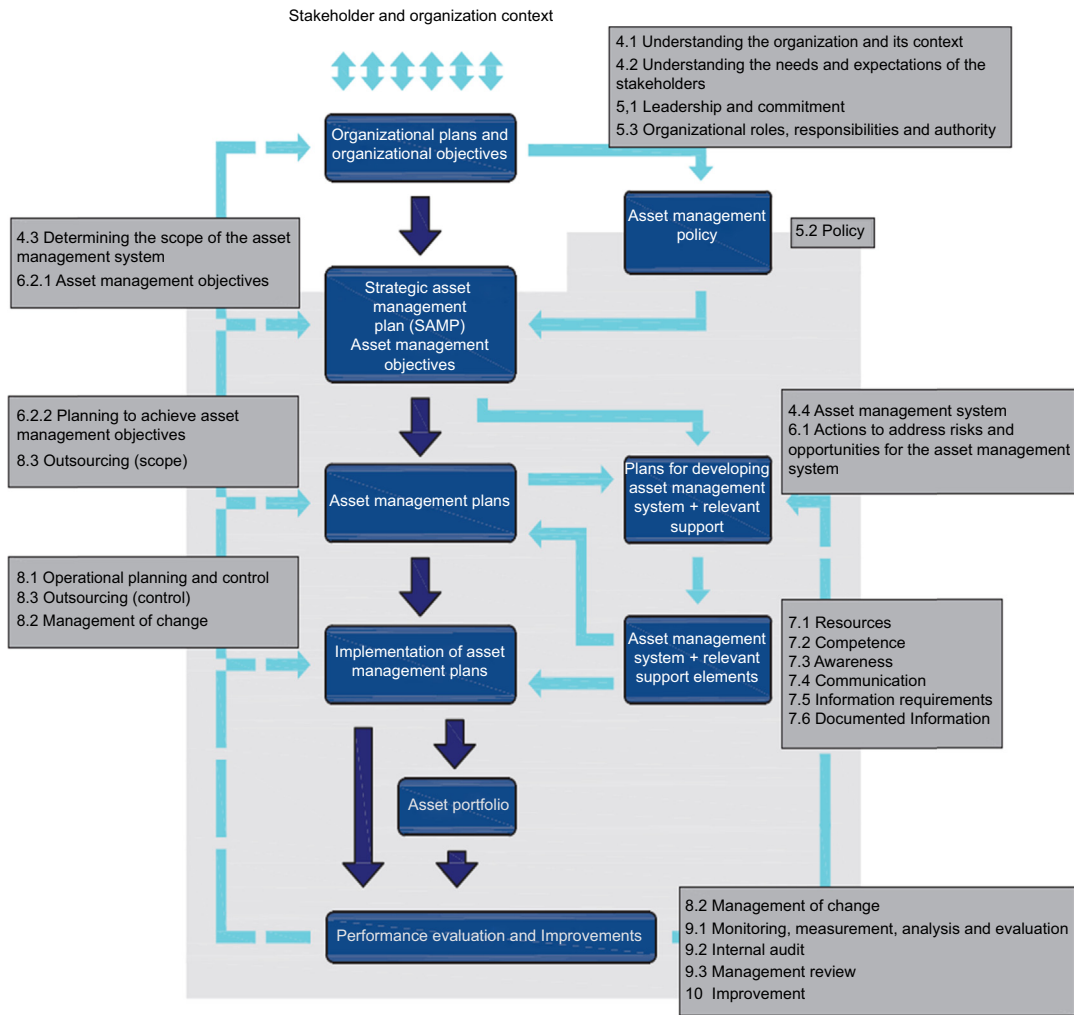


FIGURE 8.6

ISO 55000 element relationship.

Source: ISO 55002 standard (2014).

From now on, the asset concept discussed in this chapter is related to physical asset management. The physical asset is defined by the European Federation of National Maintenance Societies (EFNMS, 2009) as follows:

Physical asset management is the optimal life cycle management of the physical assets to sustainably achieve the stated business objectives.

Physical assets are tangible assets such as facilities and equipment. The main challenge concerning physical asset management is to define which one must be part of the physical asset management program and which one is not critical and will not be part of physical asset management. Basically, each physical asset that may influence positively or negatively on the business must be part of the physical asset management program. Such an effect must take into account all stakeholder expectations, which will not only be related to asset performance but also to safety and environmental risk. Moreover, an additional issue that relates to physical assets is resource allocation priority, which can be assessed by applying different reliability engineering methods as described in previous chapters.

Since the physical asset has the asset philosophy concept, top-down implementation is also applied. Therefore to achieve the business objective the first step is to understand the market. Chapter 7 has described market assessment concerning suppliers, customers, competitors, and regulation. Moreover, it is necessary to understand the impact of the market in the technology. Fig. 8.7 shows the specific features of asset management for different technology and market characteristics. Indeed, the technology can be defined basically as stable and dynamic. In the case of stable technology, the asset has a long life cycle. This is a common case for most physical assets in the oil and gas industry concerning process and facilities plants as well as static equipment. In the case of dynamic technology, the asset has a shorter life cycle. This is also applied to physical assets such as electronics and electrical components as well as rotating equipment. In addition, the market can also be characterized as stable and dynamic. Despite a stable market, as assessed in Chapter 7, the oil and gas industry is also part of the dynamic energy market, which demands constantly new technology and innovative development from the oil and gas industry.

Concerning the oil and gas industry as an oil, gas, and derivatives supplier, the technology and market are stable. Therefore it has a long life cycle, which requires asset performance optimization based on continuous improvement supported by reliability engineering, integrated logistic support (ILS), and LCC.

As mentioned previously, depending on equipment characteristics, different physical asset management approaches are required. In the case of most static equipment vendors, the market and technology are stable. Despite a long life cycle, which requires an LCC approach, some innovations are required, mostly related to materials being robust to different operational environmental conditions. Usually, these physical assets, such as pipes, vessels, towers, and tanks, are very reliable but require a very good maintenance and inspection plan to certify risk mitigation.

In the case of vendors who supply electronics and electrical components, the technology market is dynamic. Therefore physical asset management requires new asset concept development and a short life cycle, which implies a shorter payback time related to an economic life cycle. In this case, asset performance optimization must be achieved during the design phase, because any improvement during the operational phase will impact highly on payback and the profitability of such assets.



<b>Market</b>	<b>Dynamic</b>	<p><b>Specific features e.g.</b></p> <ul style="list-style-type: none"> <li>•Determine economic life time</li> <li>•Short economic life-time</li> <li>•LCP-approach required</li> <li>•Increase flexibility</li> <li>•New asset concepts</li> </ul>	<p><b>Specific features e.g.</b></p> <ul style="list-style-type: none"> <li>•Determine economic and technical life time</li> <li>•Short economic life-time</li> <li>•Short pay-back time required</li> <li>•LCP-approach required</li> <li>•Manage dynamics</li> <li>•New asset concepts</li> </ul>
	<b>Stable</b>	<p><b>Specific features e.g.</b></p> <ul style="list-style-type: none"> <li>•Long economic life-time</li> <li>•Long pay-back time</li> <li>•Increase life time</li> <li>•LCC-approach</li> <li>•Continuous improvements</li> </ul>	<p><b>Specific features e.g.</b></p> <ul style="list-style-type: none"> <li>•Short technical life-time</li> <li>•Determine technical life time</li> <li>•LCC-approach</li> <li>•New asset concepts</li> <li>•Improve technical performance</li> </ul>
		<b>Stable</b> Long life cycle	<b>Dynamic</b> Short life cycle
		<b>Technology</b>	

**FIGURE 8.7**

Organizational context.

*Source: EFNMS Asset Management Survey ESREDA Conference in Porto, May 2013.*

In the case of rotating equipment vendors, the market is dynamic and the technology is stable. This means that such assets have a long life cycle, but it is always necessary to develop new asset concepts because of competitiveness and also new customer requirements. In this particular case, the life cycle profit (LCP) approach is more appropriate than the LCC approach because each physical asset must be addressed to the customer, which requires a short economic life cycle related to the warranty period.

Technology and markets dictate the physical asset management characteristics for each individual company in the oil and gas industry. Nevertheless, all of them need to implement best practices to enable the asset high performance. Such an optimal solution requires not only the highest performance achievement, but also the logistical and LCC optimization integrated with such asset performance. Therefore, asset management in the oil and gas industry must be supported by the following programs:

- Reliability engineering program
- Asset integrity management program
- ILS program
- LCC/LCP program

All these topics will be discussed further in this chapter to clarify the concept and the relation between the programs.

Concerning the reliability engineering program, the high performance of physical assets is achieved by implementation of the best reliability engineering method throughout the asset life cycle phases. In this case, the best maintenance engineering practice such as Reliability Centred Maintenance (RCM), Risk Based Inspection (RBI) and Failure Mode and Effect Analysis (FMEA) are part of reliability engineering.

From a reliability engineering point of view, physical asset management can also be defined as:

The best practices applied along the physical asset life cycle to achieve the optimal asset performance result.

Therefore different reliability engineering methods in different asset life cycle phases must take place. The ideal physical asset performance is achieved when the majority of early life failures are eliminated in the design phase, which enables excellent performance not only in the early life period but also during the whole operational phase, which is represented by the green bathtub curve in Fig. 8.8. In fact, higher reliability means lower failure rate.

To achieve such performance it is necessary to implement different reliability engineering methods over the physical asset life cycle as described in previous chapters. Indeed, all effort starts at the design phase by applying different qualitative (Design Failure Mode and Effect Analysis (DFMEA), RCM, RBI, High Accelerated Life Test (HALT), Failure Report and Corrective Actions System (FRACAS), and human reliability) and quantitative (Reliability, Availability and Maintainability Analysis (RAM), Accelerated Life Test (ALT), reliability growth analysis and warranty analysis) methods. Such methods have the main objective of identifying the early life failure during design and eliminating them whenever possible. At the operational phase, different qualitative (PFMEA, RCM, RBI) and quantitative (lifetime data analysis (LDA) and RAM analysis) methods must be implemented to maintain asset performance targets until the end of asset life cycle. However, when decommissioning phase is achieved, the optimum replacement time (ORT), RAM analysis, and reliability growth analysis must be implemented to support the decision of replace or not the old assets.

Concerning the oil and gas life cycle, asset management must be developed in different phases such as:

- Asset management strategy
- Asset management development
- Asset management assurance
- Asset management warranty
- Asset management performance achievement

The asset management strategy phase is the first step, which defines the strategic objectives based on market and technology. The KPIs for a top-level system are also defined in this phase. In addition, the physical asset management support programs, policies, and strategic objectives are defined in this phase.



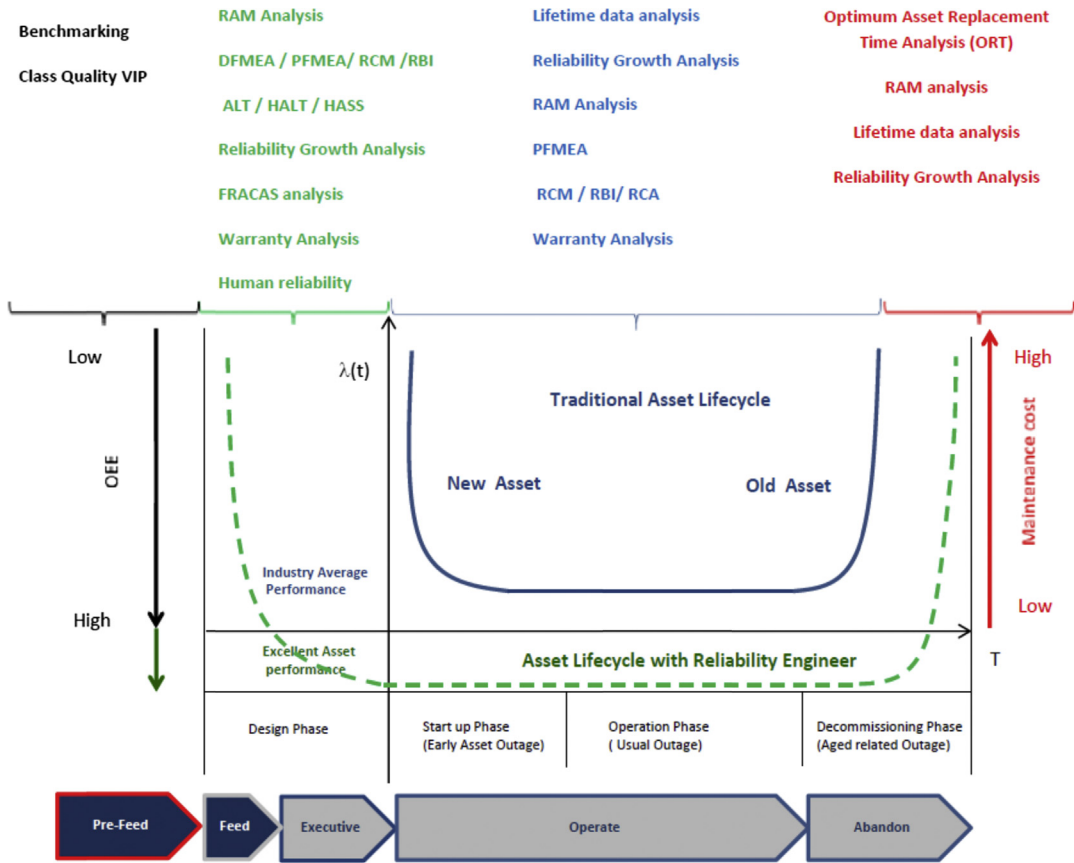


FIGURE 8.8

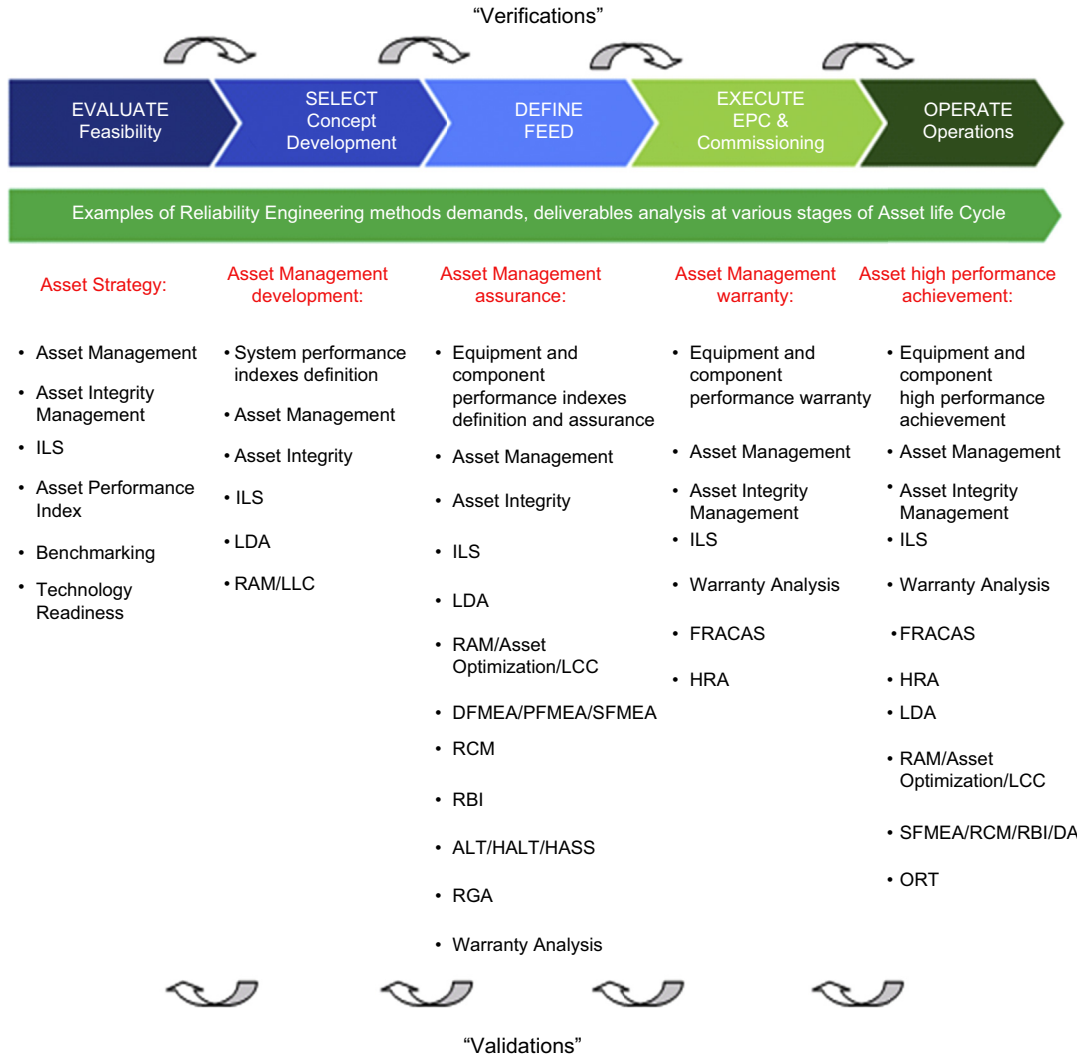
Asset management life cycle.

Source: Calixto, 2014. RAMS Analysis applied to decommissioning phase: Comparing and assess different methods to predict future failures. ESREL 2015, Wroclaw, Poland. © 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0.

The physical asset management development phase objective is the verification of the KPI defined in the previous phase, which is validated by top-level system assessment such as RAM/LCC analysis, ILS, and asset integrity analysis based on top-level risk analysis. In this phase, the LDA must be initiated based on similar previous project data to support the RAM analysis.

The asset management assurance objective is the verification of the KPI defined in the previous phase, which is validated by system equipment and component-level assessment based on different reliability engineering methods, as shown in Fig. 8.9. This is a critical phase because it defines the baseline to select the vendors based on the assurance of their assets.

The asset management warranty objective is the verification of the KPI defined in the previous phase, which is validated by the system, equipment, and component-level assessment based on a review of reliability engineering methods defined in Fig. 8.8 and a verification test. In this phase, the



**FIGURE 8.9**

Asset management phases and reliability methods.

Source: Calixto, E., 2015a. *Integrated Logistic Support. RAM, preventive maintenance, inspection, spare parts and life cycle cost optimization based on dynamic program.* In: ESREL 2015, Zürich, Switzerland. Taylor & Francis Group, London, ISBN:978-1-138-02879-1 and Calixto, E., 2015b. *Integrated asset integrity management: risk management, human factor, reliability and maintenance integrated methodology applied to subsea case.* In: ESREL 2015, Zürich, Switzerland. Taylor & Francis Group, London, ISBN:978-1-138-02879-1.

customer and vendors agree the warranty contract based on asset performance and the penalties in case of nonachievement of asset performance targets. This phase also establishes the performance monitoring system such as FRACAS to collect the asset performance data and in the case of failure to enable the root cause assessment. It is important to realize that some recommendation from previous phases must be addressed in this phase to avoid asset low performance because of error during installation.

Asset management performance achievement occurs during physical asset operation. In this phase, the verification of the KPI defined in the previous phase takes place and is validated based on physical asset performance. Since physical asset management is also based on the continuous improvement concept, reliability engineering methods support the whole operational phase to maintain asset high performance and improve such performance whenever necessary. Even if the physical asset achieves higher performance during the operational phase, a point will be reached where different equipment must be replaced to have a better asset economic result. Such a decision is supported by the ORT as described in Chapter 3.

Reliability engineering methods require investment, time, training, and planning to be executed on time to enable the physical asset to achieve better performance. In fact, depending on the asset it will be not necessary to implement all methods described in Fig. 8.9 and will depend on asset features as well as the knowledge and experience of the asset. In addition, two important issues related to physical asset management must be discussed, which are the asset management plan and the definition of the KPIs.

Concerning the necessary resources during different physical asset management phases, it is highly recommended to develop the asset management plan, which includes resources, methods, and delivery dates for all physical asset management phases to reduce the risk of delayed recommendation or wrong assumptions during the physical asset life cycle.

One of the most important advantages of linking the reliability engineering program to asset management is to integrate business and operational performance. In doing so the reliability engineering program receives top-level organizational support. In fact, this has not been happening for many reliability engineering programs in the oil and gas industry because such initiatives are local and operational efforts do not link to the business strategy. Therefore whenever companies face a hard market situation such programs are cut off and eliminated.

To give a proper performance assessment of the physical asset, the proper KPIs must be defined from the very beginning of an asset management strategy. As discussed in Chapter 7, one of the 10 reliability engineering mistakes is to use the MTBF and constant failure rate as a performance index. In fact, such an error must be avoided during the KPI definitions, otherwise all reliability engineering effort will not be realized properly during the operational phase. In addition, based on the wrong KPIs, preventive action can be performed too late or too early with regard to an unwanted event such as failure, which increases the asset LCC. The LCC can be divided in different verification index such as CAPEX and OPEX. In addition, the Opex for example can also be divided in different other index such as Maintenance cost (preventive, predictive and corrective cost). In fact, there are additional economic indexes such as ROI (return of investment) and EBITDA (earnings before interest, taxes, depreciation, and amortization) that's not described in the text because is not part of Reliability engineering focus.

As described in Chapters 3 and 4, some KPIs related to reliability are:

- Operational availability (OA)
- Production efficiency (PE)
- Utilization (Ut)
- Life Cycle Cost (LCC)

- Reliability (Re)
- Maintainability (Ma)
- Supportability (Su)
- Expected number of failures (ENF)
- Availability rank (AR)
- Availability importance (AI)
- Reliability importance (RI)
- Perceptual losses (PL)
- Failure rank (FR)
- Downtime criticality (DC)

The important issue related to the KPI concerns the KPI’s relevance to each organizational level, as defined in Fig. 8.10. The concept of target, control, and verification indexes helps to clarify such an issue and makes it easier for the KPIs achievement, control, and verification throughout different organizational levels. The target index is the primary objective for each individual organizational level. The control index is thus necessary to monitor the achievement of the target index and support improvement actions and recommendations when the target index is not achieved. The verification index is the basis for understanding the root cause of not achieving the control indexes.

The target index at each organizational level is always a control index for the above hierarchy level.

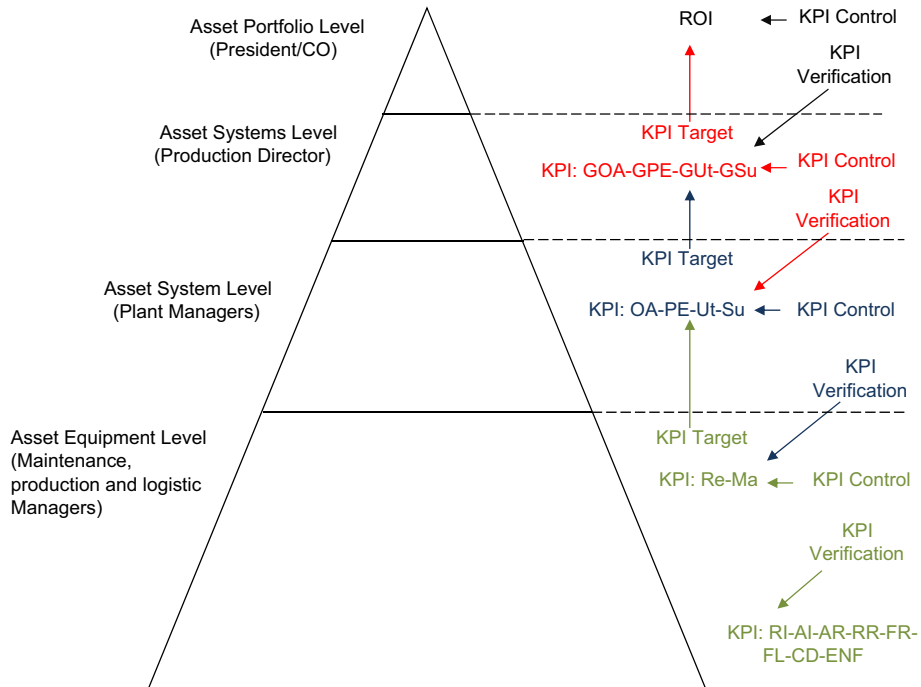


FIGURE 8.10

KPI hierarchy. G, general.

The control index for each organization level is the verification index for the above organizational level.

The verification index for each organizational level is always a control index of the lower hierarchy level.

Therefore concerning the KPI related to reliability, operational availability, production efficiency, utilization, and LCC are control indexes for a high intermediate organization level (production director), but the verification index for the top organization level (president/CEO). For the low intermediate organization level (plant managers) the verification indexes are reliability, maintainability, supportability, expected number of failures, failure rank, and downtime criticality. For the operational level, such as production and maintenance, these are the control indexes and such indexes are applied to all equipment and critical component levels.

Therefore, based on Fig. 8.10, whenever the return on investment (ROI) is not achieved the president/CEO can verify at the lower level the general indexes that encompass all physical assets at plant level, such as general operational availability, general efficiency production, general utilization, and general supportability. The case study in Section 4.6.8 in Chapter 4 demonstrates the RAM + L analysis applied to a refinery including different plants. Such a method is a good approach to define such performance indexes encompassing different physical assets.

Suppose that some of these indexes are not achieved and impact on ROI. At this level, this means that one specific plant does not achieve the target. In this case the production director is able to verify at a lower level which plant impacts on such performance and will receive justification and proposed improvement action from the specific plant manager who failed to achieve the target.

At the lower intermediate level the plant manager is able to verify which equipment has impacted on plant performance and will also verify if such low performance is related to equipment reliability, maintainability, or supportability. Therefore at the bottom organizational level the manager responsible for such low performance will look at equipment and component performance and will clarify the root cause of the failure as well as the solution for the problem.

A very important issue related to KPIs is to make the effort to be more preventive than reactive. To have a preventive performance index approach, different methods such as predictive maintenance and online monitoring as discussed in Chapter 3 must be applied to the equipment and components as well as RAM analysis, and asset optimization must be applied to the physical assets at the system level concerning equipment and component data together with preventive maintenance tasks, LCC, and logistics as defined in Chapter 4. Such methods and tools enable a more preventive approach when compared to the past when such tools, software, and methods were not available.

Finally, after the introductory explanation about asset management it is possible to realize some reasons why physical asset management has become a more essential part of oil and gas management, such as:

- Integration of the physical asset performance management throughout different organizational levels;
- Integration of reliability engineering and preventive maintenance methods as well as asset integrity management to support the physical asset performance achievement;
- A baseline to have an integrated optimization of physical asset management performance concerning logistics and LCC;

- Clear integration between business results and physical asset performance based on physical asset management KPIs related to strategic objectives;
- Support from the organization’s top-level leaders, in programs such as reliability engineering, asset integrity management, ILS, and LCC.

## 8.2 ASSET INTEGRITY MANAGEMENT

Asset integrity management is also part of asset management, but the main objective is to achieve physical asset high performance concerning safety and environmental aspects. In fact, risk management has been applied to all oil and gas companies all over the world, but in spite of this, major accidents have been not been avoided, notwithstanding a huge improvement in risk mitigation in the oil and gas industry worldwide. The residual risk of aging physical assets still concerns the asset manager, authorities, and society. Therefore a very important discussion in 2004 talked about the residual risk of aging physical assets.

The very beginning of asset integrity management started in July 2008 and marked the 20th anniversary of the Piper Alpha disaster. The UK Secretary of State for Work and Pensions afterward a parliamentary debate triggered a request for “key program asset management.”

The main program objective focused on offshore installations on the United Kingdom Continental Shelf, and revealed significant issues regarding the maintenance of safety critical systems used in major accidents concerning the period between 2004 and 2007.

Asset integrity is defined by the Health and Safety Executive (HSE) as:

The ability of an asset to perform its required function effectively and efficiently while protecting health, safety and the environment.

Based on such a definition the HSE’s Offshore Division undertook a review, with input and cooperation from key industry stakeholders, including trade unions and industry trade associations. The asset integrity program was comprised of the following:

- Asset integrity/process safety management;
- Physical state of plant;
- Safety-critical systems;
- Leadership;
- The engineering function;
- Corporate and cross-industry learning and communication;
- Human resources and competence;
- Safety culture;
- Workforce involvement in controlling major accident hazards;
- Existing mechanisms for workforce involvement.

Based on this case the first effort of “asset integrity/process safety management” had the objective of finding evidence of awareness of the need for effective process safety management and major hazard risk controls; in other words, risk management.

“Physical state of plant” had the objective of checking the general plant maintenance policy, regarding aging influences on asset failures and logistical issues that might influence asset integrity performance.

“Safety-critical systems” had the objective of finding evidence that safety-critical systems are identified and preventive action is being taken to avoid accidents, in addition to such preventive actions and improvements being sustained in the long term.

“Leadership” is an important aspect in any management program. In the KP3 program the main objective is to find out strong evidence that the role of leadership in integrity management has been effectively promoted throughout the industry. Moreover, an effort has been made to define and implement KPIs for asset integrity.

The “engineering function” objective is to check if it has adopted the enhancements to the technical authorities’ role uniformly across the sector.

“Corporate and cross-industry learning and communication” checks evidence that the culture in the industry is open to share information with other organizations. Indeed, its objective is also to verify if barriers are being broken down to provide more effective integration of the work of their independent verification bodies, and effective internal and external auditing processes.

“Human resources and competence” has the main objective of checking if resources are improving competence issues and training to prevent and avoid major hazards. Some issues, such as experienced staff and associated corporate knowledge, particularly in major hazard risk management, are important. In addition, it is important to highlight that the industry must maintain a focus on recruiting and retaining a fully competent workforce at all times.

The “safety culture” aspect checks evidence that progress has been made in key areas, which may produce a positive impact on safety culture offshore. This includes enhancing leadership knowledge and understanding, as well as workforces, to contribute to improved safety culture.

The “workforce involvement in controlling major accident hazards” main objective is to check if the risk controls and the role of installation integrity is now better understood by the offshore workforce. In addition, it is important to take into account how a high level of awareness is maintained in the long term.

To verify compliance with such elements, it is necessary to establish an audit process. This is required:

- To define the auditors qualified to check the asset compliance on such criterion as previously defined;
- To define the asset to be audited based on safety criticality;
- To define the evidence required in the audit process to ensure compliance with those asset integrity elements as well as how to obtain such evidence.

To precede with such an audit process a number of templates are defined by KP3, as shown in Fig. 8.11.

The first step to verify the compliance of critical factors for asset integrity management was successfully achieved. However, the additional and important steps were to implement the asset integrity management in oil and gas companies on a daily operational basis.

Integrity management, more than an audit process, must be established as an operational routine by an “operational integrity management program.” Such a program must take into account all aspects of integrity management as well as prepare employees in all organizational levels to implement integrity management as a work routine.

The success of such an implementation, like all programs, depends too much on leadership involvement and awareness as well as on the organizational culture in favor of integrity management.

Moreover, it is necessary to take into account other established programs like Six Sigma, ISO 14001, ISO 9001, OHSAS 18001, process safety management, and reliability engineering (reliability

Offshore D	<b>Maintenance of safety critical elements (SCE)</b>		
<ol style="list-style-type: none"> <li>1. Does the maintenance work order for a SCE contain a statement of or reference to the relevant SCE performance standard?</li> <li>2. Does the work order describe any tests to be conducted prior to re-commissioning, to demonstrate that the relevant performance standards has been met?</li> <li>3. How is the result of this test recorded (e.g. pass/fail/remedied)</li> <li>4. What do you do if the test doesn't meet the acceptance criteria?</li> </ol>			
<b>RELEVANT LEGISLATION</b> PFEER 5 Assessment - establish appropriate performance standards SCR 2 (5) SCEs remain in good repair and condition PFEER 19 Suitability and condition of plant PUWER 5 Maintenance			
NON COMPLIANCE / MAJOR FAILING	ISOLATED FAILURE / INCOMPLETE SYSTEM	IN COMPLIANCE / OK	NOT TESTED / NO EVIDENCE

**FIGURE 8.11**

KP3 audit guide.

Source: KP3 Audit Guide. Program Final Report. <http://www.hse.gov.uk/offshore/programmereports.htm>.

availability maintainability) to integrate the integrity management process to all of them, as shown in Fig. 8.12.

Indeed, this is a big challenge, but a good opportunity for the programs to prosper and drive organizations to achieve high asset integrity performance based on different aspects.

Operational integrity management encompasses risk management, reliability and maintenance, and human factors. Indeed, all elements discussed previously are comprised in these three pillars.

To achieve high performance it is always necessary to learn from experience and implement new ideas, otherwise there will be gaps in organizations.

Operational asset integrity management is a way to achieve operational excellence in the future, which means high asset integrity performance; in other words, low incidents, accidents, and environmental impacts.

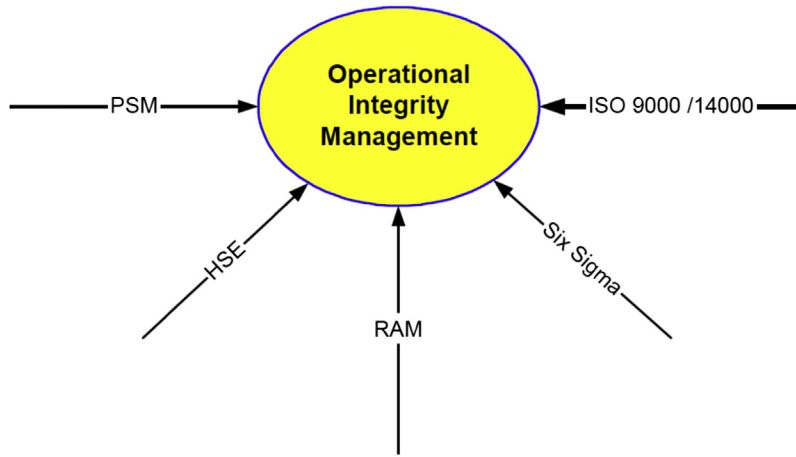
The operational excellence track started inside the occupational safety management in 19th century and then, standards, procedures, and methods were implemented, but there are still a lot of gaps that must be filled to achieve operational excellence, as shown in Fig. 8.13.

Since the first efforts to improve asset integrity performance, different methods have been applied to support asset integrity management.

Nowadays, the current asset integrity management programs are mostly based only on RBI analysis without considering the human factor assessment, which is a vulnerability that can be reduced based on proposed integrated asset integrity management. In addition, it is also important to integrate reliability and preventive maintenance into asset integrity management right from the very beginning of the life cycle phase as a way to achieve and maintain asset integrity. Therefore the asset integrity management pillars are “risk management”, “reliability,” and “human factor,” as shown in Fig. 8.14.

Risk management is intended to define a risk target, hazard identification, incident and accident investigation, risk assessment, risk evaluation, and risk mitigation, and to communicate the risk and

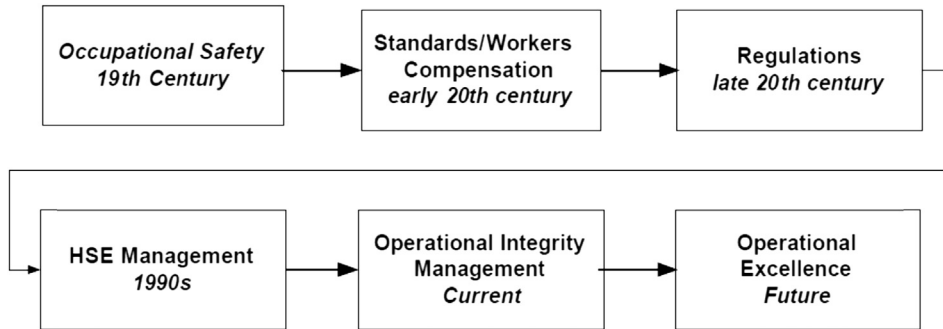




**FIGURE 8.12**

Operational integrity management.

Source: Sutton, I., 2010. *Process Risk and Reliability Management: Operational Integrity Management*, first ed. Elsevier. ISBN-13: 978-1437778052.



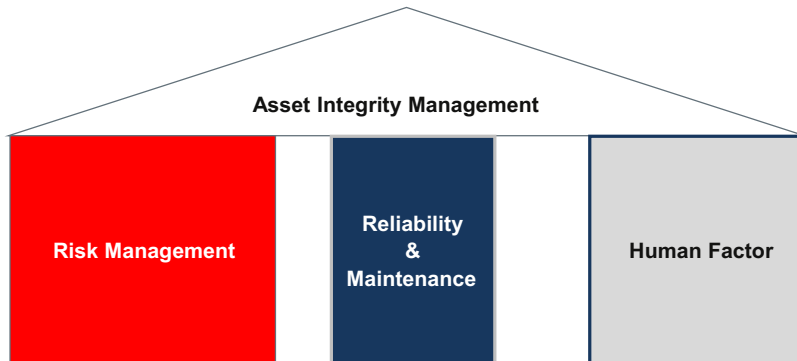
**FIGURE 8.13**

Operational excellence.

Source: Sutton, I., 2010. *Process Risk and Reliability Management: Operational Integrity Management*, first ed. Elsevier. ISBN-13: 978-1437778052.

prepare an emergency response plan. To identify hazards and assess the risk, different qualitative and quantitative methods can be applied such as Preliminary Hazard Analysis (PHA), Failure Mode And Effect Analysis (FMEA), Hazard Identification Analysis (HAZID), Hazard and Operability Analysis (HAZOP), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Safety Integrity Analysis (SIL), Layer of Protection Analysis (LOPA), Quantitative Risk Analysis (QRA or AQR), and bow tie, as discussed in Chapter 6.

The reliability and maintenance performance index is defined in the prefeed phase to be assured in the design phase of RAM analysis, LDA, accelerated life test, reliability growth analysis, DFMEA,



**FIGURE 8.14**

The house of asset integrity management.

RCM, and RBI. In addition, a long operational phase, LDA, and RAM analysis are carried out to support decisions as well as RBI and RCM, which will define maintenance and inspection policies to maintain asset availability and reliability during the operational phase.

The human factors as discussed in Chapter 5 are identified by human reliability analysis, which concerns all human performance factors related to all critical activities that can lead to an accident or environmental impact.

To implement integrated asset integrity management the following phases are proposed:

- **First phase:** Define the physical asset to be assessed concerning the consequence severity of unsafe failure or incident based on company or government authority risk criteria;
- **Second phase:** Define asset integrity performance targets concerning risk, reliability, maintenance, and human factors;
- **Third phase:** Perform risk analysis to identify the unsafe critical failures and incident event to mitigate the risk;
- **Fourth phase:** Identify potential human error related to unsafe critical failures and incident event and apply human reliability analysis to mitigate the risk;
- **Fifth phase:** Collect failure, incident, accident, and repair data, and perform LDA and also RAM analysis concerning inspections and maintenance policies to mitigate the risk;
- **Sixth phase:** Apply the integrated assessment of asset integrity management concerning all information related to risk, reliability, maintenance, and human factors and model based on the bow tie analysis method.

Asset integrity management cases applied to subsea and refinery assets will be demonstrated in [Section 8.5](#) to clarify concepts based on real applications.

## 8.3 INTEGRATED LOGISTIC SUPPORT

ILS has been applied to the military and aerospace industries worldwide, and has proved to be a successful methodology.

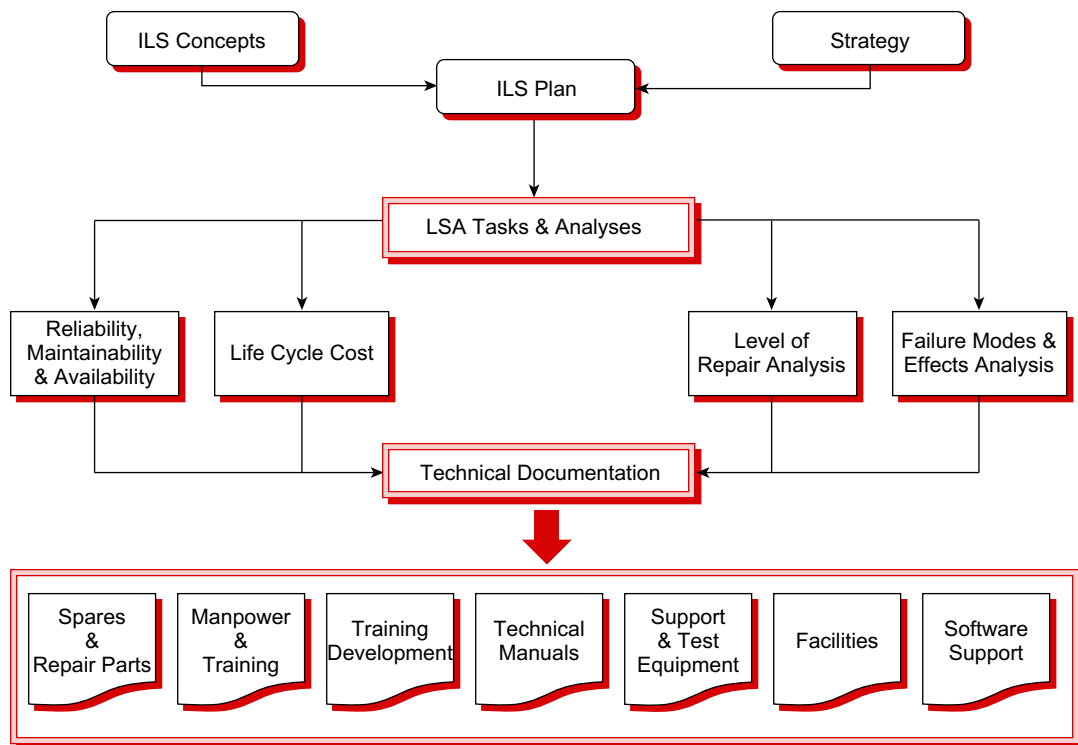
ILS encompasses all information from different reliability engineering methods and also includes important logistics issues such as delivery time and spare parts policies, which may affect asset performance.

To achieve the best result from ILS it is necessary to implement additional tools such as optimization modules, which minimize LCC and maximize operational availability and reliability.

The challenge in implementing such an approach is a lack of software, which would enable integrated logistics support optimization by taking into account the integration of different reliability methods.

The ILS strategy and policies are also defined at the very beginning of the asset life cycle and developed throughout the different asset life cycle phases. In fact, ILS enables the integration of all reliability engineering methods applied during the design phase to the commissioning and operational phases by delivering documents to be used during the operational phase, as shown in Fig. 8.15.

ILS is an integrated and iterative process for developing material, and a support and maintenance strategy that optimizes functional support, leverages existing resources, and guides the system engineering process to quantify and lower LCC and decrease the logistics footprint, making the system



**FIGURE 8.15**

ILS information flow.

Source: <http://www.mulkerin.com/images>.

easier to support. Although originally developed for military purposes, it is also widely used in commercial asset support. The primary objectives of the ILS study are as follows:

- Detailed reliability engineering, maintainability engineering, and maintenance (preventive, predictive, and corrective) operational planning;
- To supply (spare parts) support to acquire resources and LCC analysis;
- To support and test equipment/equipment support manpower and personnel;
- Training and training support;
- Technical data/publications;
- Computer resources support;
- Packaging, handling, storage, and transportation;
- Design interface.

ILS manages all information throughout the asset life cycle, integrating the design phase with the operational phase. In addition, based on ILS it is possible to influence the product design and develop the support solution to optimize supportability and LCC. ILS key principles based on standard [JP886 Defence Logistic Support Chain manual](#) are:

- **Influence on product design.** Ensure, where appropriate, that product design (including associated packaging), and the use of facilities, services, tools, spares, and manpower are optimized to maximize product availability at optimal Through Life Finance (TLF).
- **Design the support solution.** Create an integrated support solution to optimize TLF. Ensure that throughout life the use of facilities, services, tools, spares, and manpower is optimized to minimize whole life costs. Use of standard and/or common facilities, tools, spares, and manpower shall be encouraged where appropriate.
- **Deliver the initial support package.** Decide and procure the facilities, services, tools, spares, and manpower required to support the product for a given period. Ensure that the physical deliverables of the support solution are in a position to meet the logistic support date requirements. Ensure that life support is in place where appropriate.
- **Acquisition of product.** ILS applies to the acquisition of all products for the MOD including technology demonstrator programs, major upgrades, software projects, collaborative projects, and off-the-shelf procurement.
- **Supportability of product.** ILS will be applied to ensure that the product is designed to be supportable, that the necessary support infrastructure is put in place, and that TLF is optimized.
- **Requirement for ILS.** ILS is still required even when the product selected is already developed, is commercial off the shelf, or is military off the shelf, and designed.

To accomplish such a requirement it has been necessary to apply different reliability engineering methods and gather information as input data to ILS from the following sources:

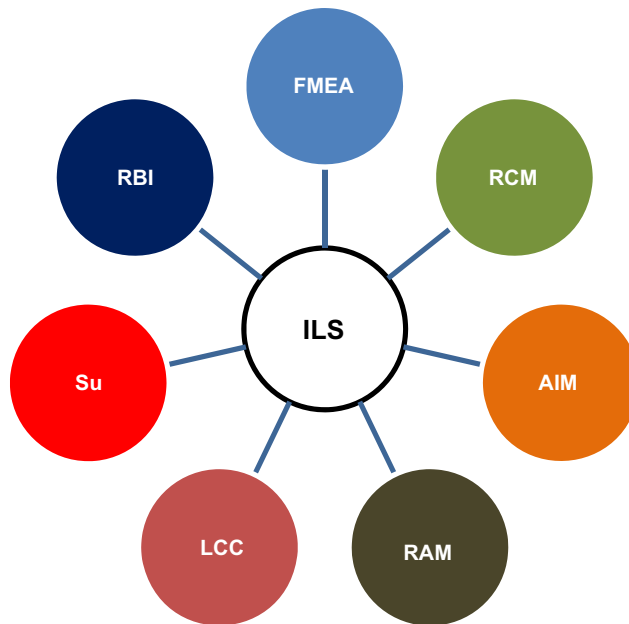
- Utility flow diagrams, process flow diagrams, piping and instrumentation diagrams (P&IDs), and descriptions;
- Discussions with project/operations personnel;
- FMEA;
- RCM analysis;
- RBI analysis;
- RAM analysis;

- Asset integrity management study (AIM);
- LCC;
- Supportability (Su)

Fig. 8.16 shows all methods that input information into ILS analysis.

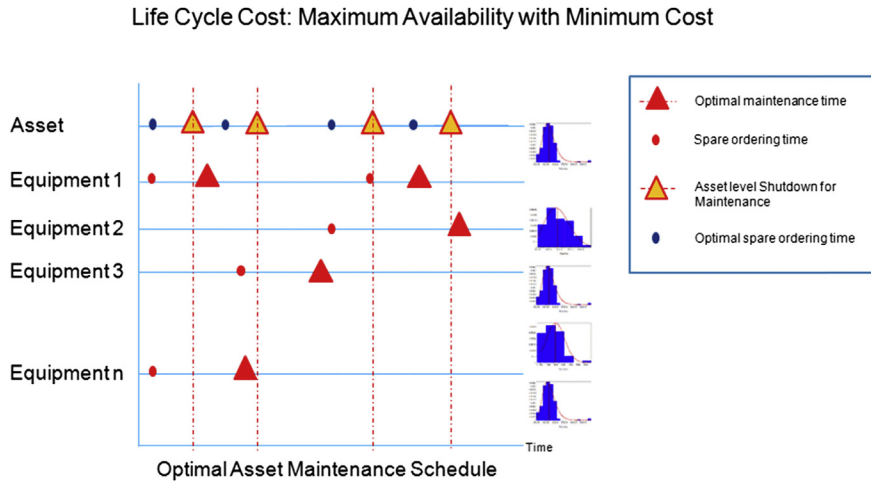
Despite all information, nowadays the main gap during ILS analysis is the lack of connection with LCC and physical asset performance such as operational availability and production efficiency. Such a gap requires an optimization approach, which will be discussed in the following section to enable minimization of the LCC while maximizing the operational availability and production efficiency.

The ILS optimization process starts with asset data collection based on different information systems such as Enterprise Risk Management (ERP), Enterprise asset management (EAM) and Computerized maintenance management system (CMMS). Furthermore, other databases providing information about asset reliability, maintenance, and procedures are also put together. Next, all information is assessed and reliability engineering analysis, such as RAM, LDA, and RCM, are carried out. The final step is to include the logistic issues such as delivery time and spare parts. Finally, all this information is put together to define which is the best time to perform preventive maintenance, inspection, and spare parts levels to maximize operational availability and minimize LCC. The ILS optimization cycle is demonstrated in Fig. 8.17. ILS optimization takes into account the spare parts and resources allocation for all types of maintenance as well as preventive maintenance and inspection, which allows lower LCC and maximum performance (operational availability, production efficiency, and reliability).



**FIGURE 8.16**

ILS input information.



**FIGURE 8.17**

ILS for system asset performance optimization.

*Source: Calixto, E., Bot, Y., 2015. RAM analysis applied to decommissioning phase: comparison and assessment of different methods predict future failures. In: ESREL 2014, Wroclaw, Poland. Taylor & Francis Group, London. ISBN:978-1-138-02681.*

ILS optimization theory will be demonstrated in [Section 8.5](#) based on a real subsea case study, which concerns different aspects of physical assets such as maintenance reliability, human factors, and LCC.

## 8.4 ASSET MANAGEMENT PROGRAM EVALUATION

The asset management program can be assessed based on PAS 55 aspects and also on the implementation of the best reliability engineering practice over the asset life cycle, which allows the achievement of asset high performance.

To perform asset integrity management program evaluation it is necessary to perform the audit process to confirm compliance by evidence. The traditional ISO audit process does not define at which level the asset management program is situated. Therefore criteria that classify the level of the asset management program must be defined. [Table 8.1](#) shows the different asset management level classifications based on best practices and defined criteria.

To perform asset management program evaluation at the classification level it is necessary to define the aspects to be assessed and the scores for each aspect based on specific scores. In addition, to perform such an audit process a set of questions, which requires demonstration of evidence, must be also defined.

A good example of management system implementation evaluation is based on the Malcolm Baldrige National Quality Award principles. In this case, audit process analysis is based on a set of questions that regards performance factors like leadership, strategy and planning, customers, society, information and knowledge, people, processes, and results.

Score Class	Score	Asset Management Characteristics	Asset Management Level Classification
A	9.6–10.00	The asset management program is adequate for all assets in the specific life cycle phase based on implementation of all the best reliability engineering, asset integrity management, and integrated logistic support program practices with compliance of all the defined criteria	State of the art
B	8.9–9.5	The asset management program is adequate for most of the assets in the specific life cycle phase based on implementation of most of the best reliability engineering, asset integrity management, and integrated logistic support program practices with compliance of most of the defined criteria	Excellent benchmarking
C	7.9–8.8	The asset management program is adequate for many assets in the specific life cycle phase based on the implementation of many of the best reliability engineering, asset integrity management, and integrated logistic support program practices with compliance of many of the defined criteria	Very good
D	5.1–7.8	The asset management program is adequate for many assets in the specific life cycle phase based on implementation of some of the best reliability engineering, asset integrity management, and integrated logistic support program practices with compliance of many of the defined criteria	Good
E	4.1–5.0	The asset management program is adequate for some assets in the specific life cycle phase based on implementation of some of the best reliability engineering, asset integrity management, and integrated logistic support program practices with compliance of many of the defined criteria	Intermediate
F	0–4.0	The asset management program is adequate for a low number of assets in the specific life cycle phase based on implementation of any of the best reliability engineering, asset integrity management, or integrated logistic support program practices with compliance of some of the defined criteria	Beginning

Asset management program evaluation will be based on similar principles to the Malcolm Baldrige National Quality Award but concern the aspect defined in PAS 55 as well as the asset life cycle phases. Therefore the aspects concerning asset management evaluation are strategy and planning, leadership, information and knowledge, processes, and results.

- Context of the organization
- Leadership
- Planning
- Support

- Operation
- Performance evaluation

“Context of the organization” encompasses all aspects related to the link between the external and internal environments defined by the business strategy that is defined in the asset strategy objectives and KPI definitions. In this case, it is necessary to demonstrate that all asset strategic objectives take into account the stakeholder requirements. The final compliance evidence is the definition of all critical assets that will take part in the asset management program based on business strategy.

“Leadership” must demonstrate the compliance of the leader’s involvement in communicating the asset management policies and objectives, and monitoring the KPIs, implementing improvement actions, as well as supporting the implementation of programs such as reliability, asset integrity, and ILS.

“Planning” focuses on the organization’s activities, including its asset management activities. The organizational objectives are generally produced from the organization’s strategic level planning activities and are documented in an organizational plan. Therefore it is necessary to define the asset management program plan, which defines all resources and methods that will be implemented during the asset life cycle. In this plan, all responsibilities and deliverables must be defined as well.

“Support” requires collaboration among many parts of the organization. In fact, the first step for employees to collaborate is to be prepared to perform their activity in the asset management program. Therefore training is an important issue and must demonstrate compliance as to how employees are qualified and trained to perform different tasks and implement different support program activities related to reliability, asset integrity, and ILS.

“Operation” encompasses the directing, implementation, and control of its asset management activities. Therefore all documents are related to asset management as well as to how the information is updated, stored, and linked to different asset life cycle phases.

In addition, the directing and implementation of asset management activities related to reliability engineering, asset integrity, and ILS must be demonstrated by compliance of the implementation of the PDCA cycle based on each phase and activity concerning the implementation of the asset management program plan in different asset life cycle phases.

“Performance” must demonstrate the evidence of the achievement of objectives for each asset life cycle based on the asset management program plan definition as well as the measurement and achievement of the KPI’s targets during the operational phase. Therefore the KPI’s monitoring, verification, and validation process throughout all asset life cycle phases as well as the improvement actions, lessons learned, and documentation and communications must be demonstrated.

The asset management evaluation is designed to encompass all asset life cycle phases, therefore it is necessary to implement the asset management program throughout the asset life cycle phases from the operational phase to achieve high evaluation classification. For each aspect, the specific weight is defined as:

- Context of the organization—weight 2
- Leadership—weight 1
- Planning—weight 1
- Support—weight 1
- Operation—weight 2
- Performance—weight 3



Such weights are multiplied by the total score for each aspect and must be applied to each asset life cycle phase, and the final evaluation will calculate the average of the total scores for each phase. This evaluates asset management program performance as a whole as well as for each individual phase.

The final issue to be defined are the questions that will be asked for each aspect as well as the score criteria based on presented evidence during the audit process.

For each question, compliance is scored based on the following criteria:

T—Total compliance (100%—employee knows company procedures or practices, has good procedures or practices implemented with more than 75% of the total possible evidence recorded).

H—High compliance (75%—employee knows company procedures or practices, has good procedures or practices implemented, but has higher than 75% of possible evidence recorded).

P—Partial compliance (50%—employee knows partially company procedures or practices, has partially good procedures or practices implemented, but has lower than 75% and higher than 50% of possible evidence recorded).

L—Low compliance (25%—employee knows company procedures or practices, has no procedures or practices implemented, and has lower than 50% of possible evidence recorded).

N—No compliance (0%—employee does not know company procedures or practices, has no procedures or practices implemented, and has no evidence recorded).

NA—Not applicable.

Such criteria consider that during the audit process the employees must demonstrate knowledge of asset management in their competence level and demonstrate evidence of such practices and the method's implementation.

The next step is to define the different questions based on ISO 55000 aspects and the best asset management practices described in this chapter.

Concerning the first aspect, “context of the organization” during the audit process the evidences must be demonstrated concerning the five required information such as:

1. The asset management policy contemplates the effort of physical asset performance achievement, including reliability, preventive maintenance, logistic integrated support asset integrity, and LCC aspects such as:
  - Spare parts policy;
  - Delay times and turnout;
  - Preventive maintenance;
  - Reliability and operational availability index definition;
  - Safety and environmental risk mitigation;
  - LCC optimization;
  - Continuous improvement and performance optimization;
  - Compliance with the law, safety, and environmental legal requirements;
  - Compliance with all stakeholder requirements.
2. The asset management policy communicates to all different levels throughout an organization.
3. The asset management policy relates to business strategy.
4. The strategic asset management objectives, goals, and KPIs are defined for all organizational levels.
5. The asset management strategy is updated regularly based on business's or stakeholder's needs.

Concerning the aspect, “Leadership,” during the audit process the evidences must be remonstrated concerning the five required information such as:

1. The leaders defined in the asset management plan communicate the asset strategy, strategic objectives, and asset policy at all organizational levels.
2. The leaders follow up the asset performance at all organizational levels.
3. The leaders defined in the asset management plan implement improvement actions based on the asset performance at all organizational levels.
4. The leaders defined in the asset management plan support the employees to achieve the KPIs at all organizational levels by addressing the necessary technological and financial management support.
5. The leaders defined in the asset management plan recognize and award the employees and team effort for the achievement of KPIs.

Concerning the aspect, “Planning,” during the audit process the evidences must be remonstrated concerning the five required information such as:

1. The asset management plan is derived and related to asset management strategic objectives, goals, and indexes.
2. The asset management plan defines the human resources, economic resources, the target time for each activity and deliverables, the methods, and technology based on the asset strategic objectives.
3. The necessary employee training is defined in the asset management plan for each asset life cycle.
4. The organizational structure, hierarchy, function, and responsibility for asset management is defined for each phase of the asset life cycle.
5. The asset management plan is updated during the asset life cycle phases and during the life cycle.

Concerning the aspect, “Support,” during the audit process the evidences must be remonstrated concerning the five required information such as:

1. The employees’ necessary competence related to their asset management activities is defined for organizational levels.
2. The employees’ necessary training related to asset management is defined for all organizational levels.
3. The employees’ activities related to asset management, such as reliability engineering, asset integrity, and ILS, are based on the procedures defined for all organizational levels.
4. The team activities are coordinated to support the asset management activities at all organizational levels based on asset management plan and procedures.
5. The employees have a channel to suggest new methods and approaches as well as asset management improvement based on the information technology that can be recorded and accessed at different organizational levels.

Concerning the aspect, “Operation,” during the audit process the evidences must be remonstrated concerning the five required information such as:

1. The asset management technology information, flow, and procedures defined in the asset management plan enable the KPIs to be accessed, recorded, and updated regularly throughout all organizational levels.
2. The asset management information technology and procedures defined in the asset management plan enable the KPIs to communicate, access, and record lessons learned to enhance the organizational improvement throughout all organizational levels.

3. The reliability engineering methods defined in the asset management plan are implemented in each asset management phase concerning the verification and validation of the tasks and KPIs defined in the previous phases.
4. The asset integrity management methods defined in the asset management plan are implemented in each asset management phase concerning the verification and validation of the tasks and KPIs defined in the previous phases.
5. The ILS methods defined in the asset management plan are implemented in each asset management phase concerning the verification and validation of the tasks and KPIs defined in the previous phases.

Concerning the aspect, “performance,” during the audit process the evidences must be remonstrated concerning the five required information such as:

1. The asset management strategic objectives are achieved.
2. The asset management KPIs are achieved concerning all organizational levels.
3. The activities and deliverables defined in the asset management plan are performed during the defined date in each asset life cycle phase.
4. The recommendation of the reliability engineering, asset integrity, and ILS methods are implemented on time.
5. The defined improvement action based on KPI results and deliverables is implemented on time.

Based on this set of issues, it is possible to evaluate the asset management program in each asset life cycle phase. Therefore during the audit process some usual questions arise such as:

- What is the required information to be supplied before the audit process.
- The result of the internal audit process and the previous audit process will be taken into account in the current audit process.
- Which is the acceptable evidence.

The answer to the first question depends on the auditors’ or the client’s point of view. In fact, for all types of audit process, information about the company and process is required as well as the history of the program implementation. Therefore the usual information about the company history, process, client, stakeholders, structure and departments, projects, products, and services is the first step. The second step is about asset management implementation and how the company implements all aspects defined in ISO 55000. The set of questions defined for each aspect is an ideal guideline to fulfill this information. It is important to remember that this audit process is quite different from the usual ISO standard audit process because it quantifies compliance with ISO 55000.

The answer to the second question depends also on the objective of the audit process. If the real objective is to improve the asset management program as best as possible, all information about the previous audit process will be helpful. In fact, the client can have support from a consultant company to fill the gaps of the asset management program based on the audit process results. Therefore, for each non compliance, the consulting company will advise the client on a solution and in some cases help the client to implement it to improve the asset quality management program.

The third question is about the evidence that can be accepted or not during the audit process. This is always a big issue during the audit process and, in many cases, evidence is produced only to demonstrate compliance during the audit process. In the asset management case, whenever best practice is not implemented the impact of the performance will be clear and will impact the asset management evaluation in the end.

It is important for the organizations that intend to implement the asset management program to be aware that the main objective of this process is to create a baseline to support the asset high performance throughout life cycle based on best practice. Such approach will help organizations to demonstrate the compliance during the audit process. Table 8.2 demonstrates the type of evidence that must be demonstrated during the audit process.

Based on Table 8.2, it is possible to perceive that the asset management plan has relevance for the asset management program because all organizational frameworks, hierarchies, functions,

	<b>Required Information</b>	<b>Compliance Evidence</b>
Context of the organization	1	Electronic and written policy
	2	Minutes of the meeting signed up and emails about the asset management policy communication
	3	Assessment of business strategy plan and asset management objectives, goals, and KPIs
	4	Written and electronics evidence of asset management strategic objectives, goals, and KPIs
	5	Minutes of the meeting and emails about the asset management strategic objectives, goals, and KPIs updated
Leadership	1	Electronic or written asset management plan
	2	Minutes of the meeting signed up and emails about asset performance follow-up
	3	Minutes of the meeting about improvement actions based on the asset performance signed up. Email and other electronic evidence can also be considered in a specific situation as well as physical evidence
	4	Minutes of the meeting about support for the employees to achieve the KPIs signed up. Email and other electronic evidence can also be considered in a specific situation as well as physical evidence
	5	Minutes of the meeting about recognizing and awarding the employees and team effort to KPI achievement signed up. Email and other electronic evidence can also be considered
Planning	1	Assessment of the electronic or written asset management plan based on asset management, strategic objectives, goals, and KPI definition
	2	Assessment of the written or electronic asset management plans
	3	Assessment of evidence of asset management training based on electronic or written list and asset management plans.
	4	Assessment of the written or electronic asset management plans
	5	Minutes of the meeting signed up and emails about the asset management plan update
Support	1	Human resource electronic or written document about competences and evidence of employee training
	2	Assessment of evidence of written or electronic training list and asset management plan definition.
	3	Written or electronic procedures
	4	Minutes of the meeting signed up and emails about asset management activity coordination and procedures
	5	Minutes of the meeting signed up and emails or written evidence

*Continued*

	<b>Required Information</b>	<b>Compliance Evidence</b>
Operation	1	Electronic or written evidence of KPIs accessed, recorded, and updated regularly throughout all organizational levels
	2	Electronic and written evidence of KPI communication, access, and record of lessons learned Minutes of the meeting signed up is also evidence of lessons learned
	3	Electronic and written evidence of engineering method's implementation based on asset management plan definition. Such evidence must demonstrate the verification and validation of the tasks and KPIs defined in the previous phases
	4	Electronic and written evidence of asset integrity method's implementation based on asset management plan definition. Such evidence must demonstrate the verification and validation of the tasks and KPIs defined in the previous phases
	5	Electronic and written evidence of ILS method's implementation based on asset management plan definition. Such evidence must demonstrate the verification and validation of the tasks and KPIs defined in the previous phases
Performance	1	Electronic or written evidence of asset management strategic objectives achievement
	2	Electronic or written evidence of asset management KPI achievement
	3	Electronic or written evidence of activities and deliverables final dates according to asset management plan definition
	4	Electronic or written evidence of recommendation plan related to each analysis and implementation
	5	Electronic or written evidence of improvement action implementation of KPI results

responsibilities, necessary procedures, information technology, activities, and deliverables for each phase of the asset life cycle are defined in this plan. Therefore to enable the efficiency of the audit process in evidence collection, the audit process must be carried out when the organization has the minimum of 6 months by releasing the asset management plan with at least one update. Such a requirement means that the minimum level of evidence is produced and at least one asset life cycle phase is assessed by the audit process. [Section 8.5](#) will demonstrate different methods discussed in this chapter and the case study in [Section 8.5.4](#) will demonstrate the audit process application.

## **8.5 ASSET MANAGEMENT CASE STUDIES**

The case studies will demonstrate the main program applications such as asset integrity management and ILS as well as asset management evaluation. Reliability engineering as well as risk analysis methods are part of such programs and will also be taken into account. The first case will show the application of the asset integrity method to a subsea project. The second case study will show the asset integrity concept applied to a refinery plant and will focus on environmental risk mitigation. The third case study is dedicated to the integrated logistics support applied to a subsea project. The final case study will demonstrate the asset management program evaluation process applied to a refinery project.

### 8.5.1 ASSET INTEGRITY MANAGEMENT IMPLEMENTATION DURING THE DESIGN PHASE: THE SUBSEA CASE STUDY

Asset integrity management methodology has the main objective of mitigating the asset risk of major accidents by applying an integrated approach, which encompasses risk management, reliability and maintenance, and human factors. The asset integrity program is very important to the oil and gas industry because it enables the risk mitigation of assets, such as platforms, subsea, refinery plants, onshore plants, storage facilities, and pipelines. This case study will exemplify the subsea case study applied in the sixth asset integrity management program step to demonstrate the integration of reliability and maintenance, risk assessment, and human reliability analysis.

#### ***Asset Integrity Management Phases***

To implement asset integrity management the following phases are necessary:

- **First phase:** Define the asset to be assessed.
- **Second phase:** Define the asset performance target.
- **Third phase:** Perform risk analysis.
- **Fourth phase:** Perform a human reliability assessment.
- **Fifth phase:** Collect failure, incident, accident, and repair data and perform performance LDA and RAM assessment including human error.
- **Sixth phase:** Apply the integrated assessment of asset integrity management.

The *first phase* is to define which are the assets that must be part of the asset integrity management program. Therefore different criteria can be applied to support such a decision. One of the most usual criteria is to include all assets with hazards that may cause consequences with high severity based on risk matrix assessment. Concerning subsea assets such as flowline, risers, and PLEM, most of them have an accident scenario classified with high severity (III and IV), based on a risk matrix, which requires being part of asset integrity management risk criteria, as shown in Fig. 8.18.

In the *second phase*, the asset performance target concerns risk, reliability, maintenance, and human factors based on companies' criteria or government definition.

In the *third phase*, risk analysis must be carried out to define hazards, assess risk, evaluate risk, and implement mitigation actions. Therefore different methods such as HAZOP, HAZID, FMEA, RBI, QRA are employed.

Considering subsoil assets, some examples of hazards with high severity are:

- Loss of containment;
- Ship collision.
- Dropped object;
- Extreme weather.

Therefore, based on the risk matrix criterion as shown in Fig. 8.18, all assets of a major accident with consequences classified as high severity (III or IV) must be part of asset integrity management. All information from the risk analysis assesses the risk and defines which assets must be part of asset integrity management. Fig. 8.19 summarizes the flow of asset integrity management decisions.

		FREQUENCY CATEGORY					
		A (extremely remote)	B (remote)	C (Little frequency)	D (Frequent)	E (Very frequent)	F (Extremely frequent)
		At least 1 between 1000 and 100,000 years	At least 1 between 50 and 1000	At least 1 between 30 and 50 years	At least 1 between 5 and 30 years	At least 1 in 5 years	At least 1 in 1 years
SEVERITY CATEGORY	IV	M	NT	NT	NT	NT	NT
	III	M	M	NT	NT	NT	NT
	II	T	T	M	M	M	M
	I	T	T	T	M	M	M

**FIGURE 8.18**  
Asset integrity management severity criteria.

In the *fourth phase*, all human factors defined during risk analysis must be assessed by a human reliability analysis method systematically and the recommendations must be implemented to mitigate the human error probability.

The *fifth phase* is dedicated to analyzing the failure, incident, accident, and repair data by performing LDA and RAM analysis, including inspections and maintenance policies defined on RBI and RCM and also human error defined in risk analysis such as FMEA.

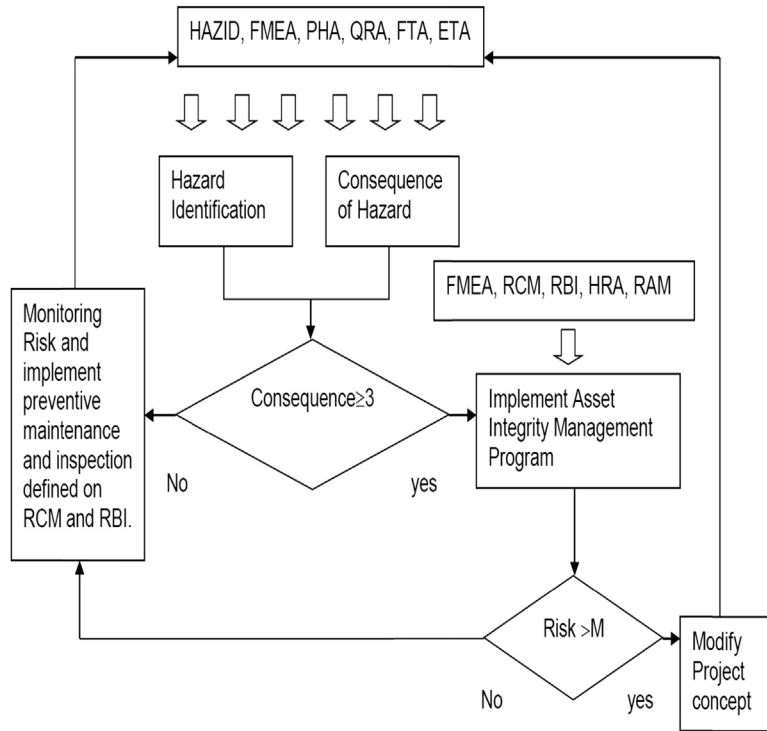
RAM analysis demonstrates that the flexible riser as well as the other subsea critical equipment including all preventive maintenance and inspection defined in RCM and RBI such as Remotely Operated Vehicle (ROV) inspection and NDT (nondestructive test), which allows the achievement of a reliability target of 100% in 30 years, is vulnerable to human error.

In the *sixth phase* the bow tie will be updated with the failure rate functions defined in the previous phase as well as the preventive actions, inspection and maintenance, and human factors that mitigate risk.

Bow tie analysis will be continually updated with all such information over the asset life cycle to help asset integrity management achieve high performance.

**Asset Integrity Management: Flexible Riser**

To exemplify integrated asset integrity management a subsea case study will be described based on the sixth phase of integrated asset integrity management methodology and will be applied to the flexible riser asset.



**FIGURE 8.19**

Asset integrity management decision flow.

Concerning the first phase the flexible riser is considered one of the most critical assets in terms of integrity based on the consequence of oil spill in cases of unsafe failures or external incidents. Therefore such equipment was selected to be part of the integrated asset integrity management approach.

The second phase defines the asset performance. Considering the flexible riser, it is expected to have no critical failure during a life cycle of 30 years; in other words, 100% of reliability in 30 years of operation, including all preventive maintenance and inspection defined in RCM and RBI, such as ROV inspection and NDT. The risk indexes were defined as tolerable with individual risk lower than  $1 \times E-4$ .

The third phase performs different risk analyses, which in this case was HAZOP, HAZID, FMEA, and RBI.

The fourth step takes into account the main human error that would trigger unsafe failures such as human error during installation. By applying human reliability analysis, it is estimated to reduce the human error probability (HEP) from 0.33 to 0.01. Similarly, the event of dropping an object was also assessed to reduce the HEP from 0.02 to 0.01.

The fifth step applies RAM analysis to predict the flexible riser performance, such as production efficiency and operational availability, as well as to verify if the flexible riser would achieve the reliability target of 100% in 30 years; however, it is vulnerable to human error.



The final sixth phase applies integrated asset integrity management based on bow tie analysis, as demonstrated on the next section.

### Sixth Phase: Integrated Asset Integrity Management

The sixth phase is to integrate all information from the previous phases by applying bow tie analysis. Therefore the main accident scenario is defined as follows:

- Loss of containment;
- Extreme weather.

**Loss of Containment.** Based on FMEA and HAZID analysis, the loss of containment and multiple fatalities is caused by leakage on a topside end fitting (top event). Fig. 8.20 shows the FMEA template and line 5 identifies the human error during installation that caused loss of containment. To mitigate such risk, human reliability analysis is performed and the recommendation is to define a procedure for installation.

The human reliability method applied in this case is the SPAH-R described in Chapter 5, one of the most applied Human Reliability Analysis (HRA), whose main objective is to define human error probability regarding the influence of human performance factors. Such methodology requires a specialist opinion to define the influence of human factors based on the PSF. Considering the human error during flexible riser installation, the Performance Shape Factor (PSF), which influences more on human error are low available time, high stress and low experience. To calculate the PSF composite, the following equation is applied:

$$PFS_{\text{composite}} = \prod_1^8 PFS$$

The NHEP (nominal human error probability) is based on specialist opinion or the SPAH-R procedure method, which establishes the value of HEP to omission error (0.01) and commission error (0.001). Thereafter the final step is to define the HEP by applying the following equation:

$$HEP = \frac{NHEP \cdot PSF_{\text{composite}}}{NHEP \cdot (PSF_{\text{composite}} - 1) + 1}$$

Therefore the PFS equation will be:

$$\begin{aligned} PFS_{\text{composite}} &= PFS (\text{available time}) \times PFS (\text{Stress}) \times PFS (\text{complexity}) \\ &\times PFS (\text{Experience/Training}) \times PFS (\text{Procedures}) \times PFS (\text{Ergonomics}) \times PFS (\text{Fitness for duty}) \\ &\times PFS (\text{Work process}) \\ PFS_{\text{composite}} &= 10 \times 1 \times 1 \times 1 \times 50 \times 1 \times 1 \times 1 = 500 \end{aligned}$$

The PFS values are defined based on the SPAH-R table defined in Chapter 5. The next step is to calculate the HEP and consider the commission error during flexible riser installation (NHEP = 0.001) and PFS<sub>composite</sub>. Therefore the final human error probability is:

$$HEP = \frac{0.001 \cdot 500}{0.001 \times (500 - 1) + 1} = 0.33$$

Failure Mode and Effect Analysis (FMEA)																								
FMEA Leader: Dr. Eduardo Calixto			Document: DE-100210-001 Rev01					Date: 25-05-2008																
System: Subsea			Subsystem: Subsea Flowline					Equipment: FL-01							Component: External sheath, Subsea End-fitting, Bend restrictor, Flowline									
No	Component	Failure mode	Phase	Cause	O	Conseq	S P	S I	S E	S S	R P	R I	R E	R S	Mitigate Action	O	S P	S I	S E	S S	R P	R I	R E	R S
1	External sheath	Tear	Op	Dropped objects	D	Ingress of seawater in annulus	I	III	I	I	DI	DIII	DI	DI	Define preventive maintenance	B	I	III	I	I	BI	BIII	BI	BI
2			Op	Human error during installation	E		I	III	II	I	EI	EIII	EI	EI	Define Installation procedure	B	I	III	I	I	BI	BIII	BI	BI
3		Overbending	Ins	Human error during installation	E	Damage of External Sheath	I	III	II	I	EI	EIII	EI	EI	Define Installation procedure	B	I	III	I	I	BI	BIII	BI	BI
4			Op	Barge Impact	E		I	III	II	I	EI	EIII	EI	EI	Monitoring vessel	B	I	III	I	I	BI	BIII	BI	BI
5	Subsea End-fitting	Leakage	Ins	Human error during installation	E	Loss of containment	I	III	II	I	EI	EIII	EIII	EIII	Define Installation procedure	B	I	III	I	I	BI	BIII	BIII	BIII
6		External corrosion	Op	Damage of coating	D	End-fitting	I	III	I	I	DI	DIII	DI	DI	Define preventive maintenance	B	I	III	I	I	BI	BIII	BI	BI
7	Bend restrictor	Early wear our	De/Ma	Material defect or design flaw	D	Low Flow and High pressure	I	II	I	I	DI	DII	DI	DI	N/A									
8	Flowline	Blockage	Op	Formation of Hydrates, Wax, Gel, Asphaltene		Low Flow and High pressure	I	III	I	I	DI	DIII	DI	DI	Define preventive maintenance	B	I	III	I	I	BI	BIII	BI	BI

**FIGURE 8.20**

Flexible riser FMEA.

Considering that the procedure will be executed well and the available time for installation is nominal to avoid human error, all PSF levels are classified as “1.” In this case the  $PFS_{\text{composite}}$  is reduced to 1 as shown in the following equation:

$$PFS_{\text{composite}} = 1 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 = 1$$

Therefore the HEP will be:

$$HEP = \frac{0.001 \times 1}{0.001 \times (10 - 1) + 1} = 0.001$$

Therefore, based on the bow tie analysis concept, the barrier against human error is to carry out human reliability analysis to identify the human performance factor, which has more influence on human error, and propose a recommendation to avoid it, as done previously.

The consequence of loss of containment, rather than environmental impact, will be leakage of the topside end fitting, and the recovery measure is to set up the emergency response (recovery measure) to mitigate the consequences, which are loss of containment in the sea and multiple fatalities (IV—safety). Fig. 8.21 shows the loss of containment bow tie diagram.

Based on RAM analysis results the frequency of leakage of the topside end fitting is  $2.5E-2$  in 20 years (exponential PDF – MTTF = 35 years).

The cost of loss of containment is valued between \$5 and \$10 million. In the worst case the financial risk is \$250,000.00 ( $2.5E-2 \times 10E-6$ ).

If human error during installation were avoided the frequency of leakage of the topside end fitting would be  $8.0E-8$  in 20 years (Gumbel PDF— $\mu = 35$  years,  $\sigma = 1$  year). In this case, the leakage is not expected during the design life (20 years).

The risk of multiple fatalities is  $4.0E-6$  ( $8.0E-8 \times 50$ ).

The cost of loss of containment is between \$1 and \$10 million. In the worst case the financial risk is \$0.08000 ( $8.0E-8 \times 10E-6$ ).

**Extreme Weather.** Based on RBI and HAZID analysis the extreme weather condition is a threat that causes severe damage in the flexible riser and the consequence is loss of containment. The barrier against extreme weather is robust design. In case of severe damage on the flexible riser the recovery

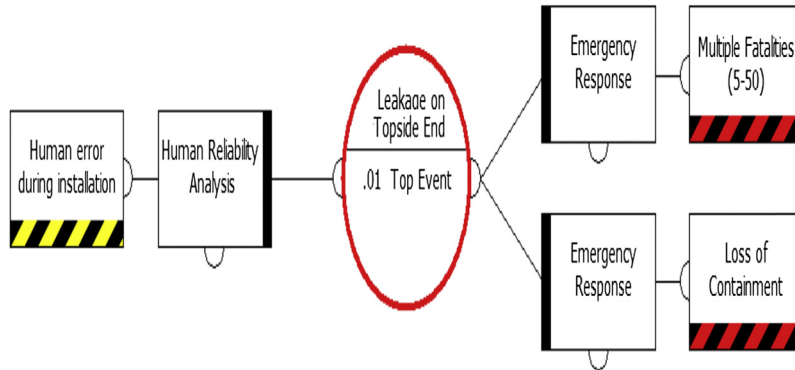
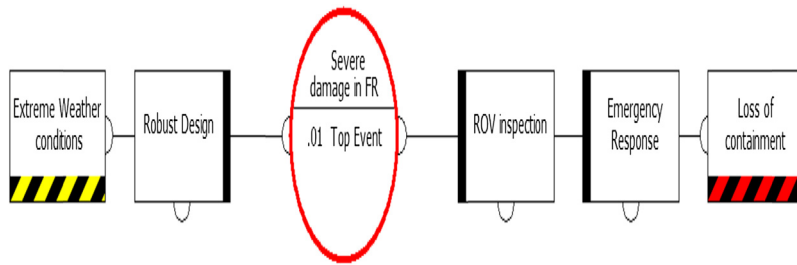


FIGURE 8.21

Loss of containment bow tie.



**FIGURE 8.22**

Extreme weather bow tie.

measure is ROV inspection and emergency response. Such recovery measures are able to avoid and mitigate the consequence, which is loss of containment. Fig. 8.22 shows the extreme weather bow tie diagram.

Based on RAM analysis, the frequency of severe damage in the flexible riser is  $2.5E-2$  in 20 years (exponential PDF –  $MTTF = 35$  years).

The cost of loss of containment is valued between \$50 and \$100 million. In the worst case the financial risk is \$250,000.00 ( $2.5E-2 \times 10E-7$ ).

If the robust design were able to support extreme weather conditions the frequency of severe damage in the flexible riser would be  $8.0E-8$  in 20 years (Gumbel PDF— $\mu = 35$  years,  $\sigma = 1$  year).

In this case the cost of loss of containment is between \$5 and \$100 million. In the worst case the financial risk is \$0.8000 ( $8.0E-8 \times 10E-7$ ).

**Conclusion.** The main objective of this case study was to demonstrate the integrated asset integrity management methodology based on a subsea case study (flexible riser), which encompassed risk management, reliability and maintenance, and also human reliability analysis. Nowadays, the lack of human factor assessment in risk management and asset integrity management is a vulnerability that is reduced based on proposed integrated asset integrity management. In addition, the proposed model integrates reliability and preventive maintenance into asset integrity management as a way of achieving and maintaining asset integrity.

Despite all the advantages, integrated asset integrity management requires a considerable effort in terms of dedicated time to perform all risks, reliability, and human factor analysis as well as integrate all results in a bow tie model to encompass the main issues that impact on asset integrity to mitigate risk.

The next step is to develop software tools that integrate all these different analyses and automatically produce the final result. Such effort is important to the integrated asset integrity management methodology proposed because it will build up a database that can be used in future analyses, reducing the time required to perform such a method.

The methodology proposed would achieve the following:

- To identify critical equipment and components based on risk criterion;
- To identify the layers of protection to avoid loss of containment and a critical accident;
- To identify the human error factor that can lead to loss of containment and a critical accident;

- To identify specific tests, inspection, and preventive maintenance required to mitigate failure identified from the FMEA, RCM, and RBI and propose scheduled tasks for critical equipment.

### 8.5.2 ASSET INTEGRITY MANAGEMENT IMPLEMENTATION DURING THE PREDESIGN PHASE: THE SULFUR RECOVERY PLANT CASE

The sulfur recovery plant has the main objective of reducing the sulfur component in refineries, plants, and products to mitigate the environmental impact caused by the sulfur component in the atmosphere.

Despite all efforts to avoid and control the emission of sulfur, in some cases, refineries that are located close to urban centers have a restricted sulfur emission allowance. Consequently, in the case of shutdown in sulfur recovery plants it is necessary to shut down other refinery plants to avoid environmental impacts caused by high levels of sulfur component emissions. In addition, loss of production is also associated with a poor consequence of such an event. The critical environmental impact caused by the sulfur component justifies the implementation of asset integrity management for the sulfur recovery plant to allow environmental high performance achievement.

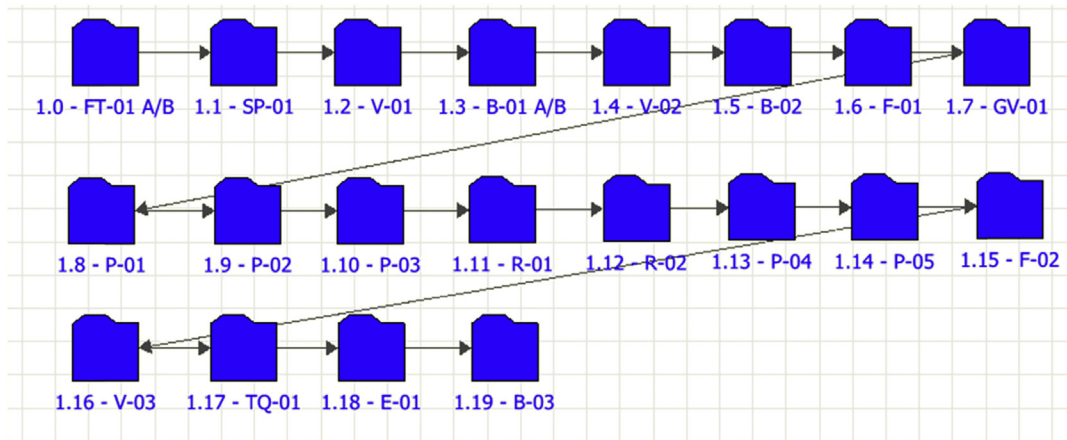
To implement asset integrity management the following phases are necessary:

- **First phase:** Define the asset to be assessed.
- **Second phase:** Define the asset performance target.
- **Third phase:** Perform risk analysis.
- **Fourth phase:** Perform a human reliability assessment.
- **Fifth phase:** Collect failure, incident, accident, and repair data and perform performance LDA and RAM assessment including human error.
- **Sixth phase:** Apply the integrated assessment of asset integrity management.

The first phase of asset integrity management is to define the asset to be assessed. This case study will focus on the sulfur recovery plant, which in case of shutdown causes a direct impact on loss of production as well as an associated environmental impact caused by the increasing level of sulfur component emissions.

The second phase is to define the performance index for such asset integrity. In this case study, based on company benchmarking as well as the environment target related to sulfur emission, it is required that the sulfur recovery plant achieves more than 99% of operational availability every 3 years.

The third phase is to apply quantitative methods to identify the hazards, assess the risk, verify the system performance, and propose recommendations. In this case, the undesirable event is associated with system outage. Therefore the main concern in this case is to achieve high operational availability over time in such a plant, which starts in the project phase with RAM analysis, RCM, and other reliability engineering methods. Once such methods are applied it is possible to define reliability requirements for critical equipment as well as preventive maintenance policies. The usual logic representation of a process plant in RAM analysis is an RBD (reliability block diagram), which describes the effect of each item of equipment in system operational availability in case of failure, as shown in Fig. 8.23. The pumps represented by the block 1.3–B-01 A/B and the filter represented by the block 1.0–FT-01 A/B are parallel blocks. This means that there is one active piece of equipment and another standby, the passive one. Such equipment causes impact on a system only when both are unavailable at the same time.



**FIGURE 8.23**

Sulfur recovery unit plant RBD.

The sulfur recovery plant operational availability as a result of RAM analysis shows that the system achieves an initial operational availability of 99.5% in 3 years. The critical equipment is the furnace, which has 99.9% of operational availability in 3 years. Such equipment is responsible for 40% of possible sulfur recovery plant outage. To avoid such downtime the following actions are proposed:

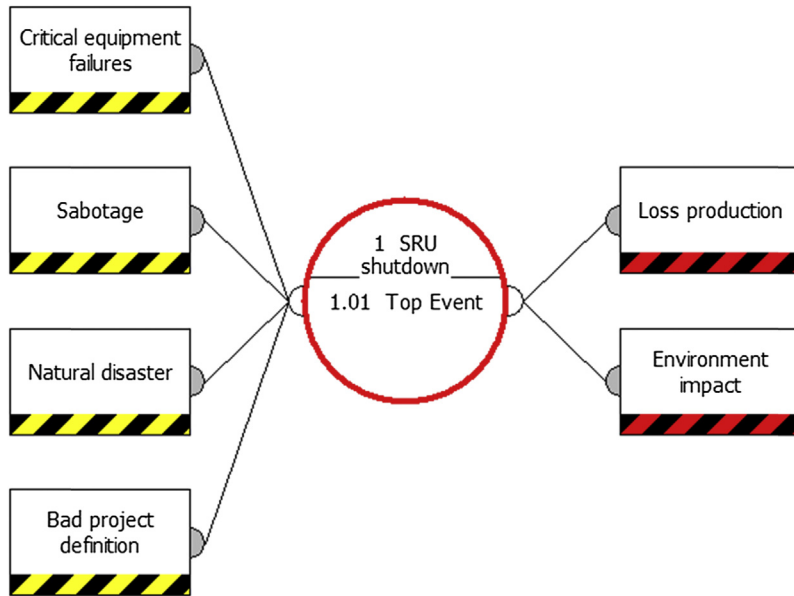
- Correct the burner's material specification;
- Operational procedure to avoid damage caused by high temperature during operation;
- Preventive maintenance policy.

Once such a recommendation is applied it is expected that the sulfur recovery plant achieves 99.7% of operational availability in 3 years.

After the project phase, once such recommendations are successfully achieved, high performance in the sulfur recovery plant is expected. Indeed, there will always be the chance of having some outage because of other equipment failures, despite low probability.

The fourth phase is to carry out bow tie analysis concerning the integrated asset integrity management vision of all threats and consequences. Indeed, concerning the sulfur recovery plant outage there are also other external events that might cause an impact on such plant and consequently outage, such as "bad project definition," "sabotage," and "natural disaster." The holistic vision about the possible threat that might cause the sulfur recovery plant outage as well as its consequence is well represented by the bow tie diagram, as shown in Fig. 8.24.

Despite RAM analysis, which shows that it is possible to achieve high performance, which means 99.5% in 3 years, external threats like sabotage, natural disaster, and bad project definition might impact on such performance. In this case it will be necessary to establish barriers to avoid such treats taking place as well as recovery action to avoid the loss of production and environmental impact once the sulfur recovery plant is shut down.



**FIGURE 8.24**

Sulfur recovery unit bow tie diagram.

Source: [http://www.risk-support.co.uk/risk\\_software.htm](http://www.risk-support.co.uk/risk_software.htm).

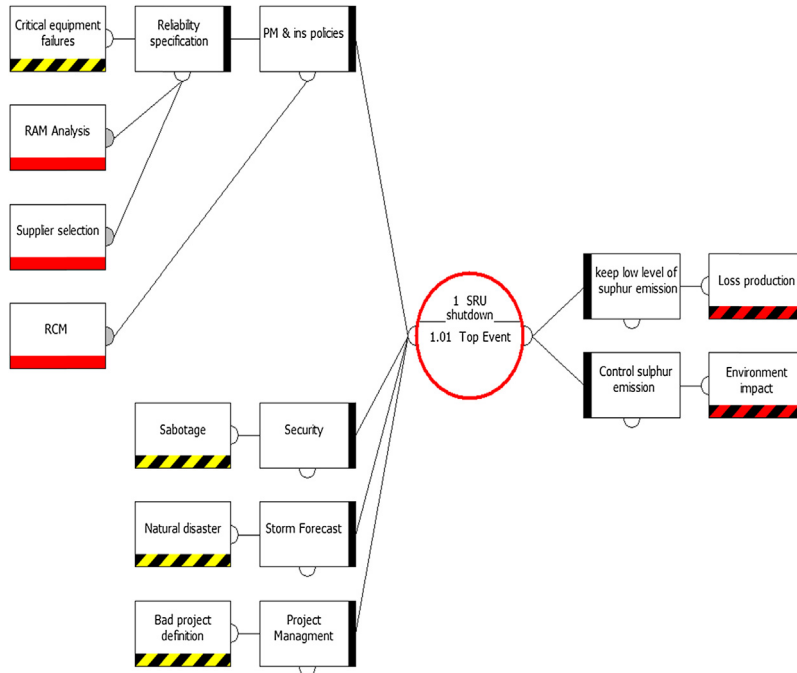
Considering the recovery action, once the sulfur plant is shut down there is little that can be done to avoid such consequences. Depending on the equipment that leads to shutdown of the plant there may not be enough time to maintain the refinery plants in operation. In case of shutdown, a furnace, for example, will require around 120 h to repair and consequently the whole refinery will be shut down.

Therefore barriers (the layer of protection) are very important to avoid triggering the TOP event (Incident), which means causing sulfur recovery plant outages. Fig. 8.25 shows the complete bow tie with the main barrier that must be used to avoid the top event.

Considering the threat “critical equipment failure” there are two barriers that must be used to avoid triggering a top event, that is, “reliability specification” and “preventive maintenance and inspection policies definition.” These barriers are successful when specific actions take place. In the first case, to define the reliability specification for critical equipment it is necessary to perform RAM analysis and select the equipment supplier based on reliability requirement predicted in RAM analysis. In the second case, to establish preventive maintenance and inspection policy it is necessary to perform RCM analysis. Indeed, such a preventive maintenance task must be applied in RAM analysis as well to predict the effects of each preventive maintenance on asset performance.

Considering the activity “RAM analysis” and the task “define reliability requirements for critical equipment” the final result is the reliability requirement definition for the critical equipment.

In addition, the activity “supplier selection” was defined as two main tasks such as “select supplier based on reliability requirement” and “critical equipment installation verification.” These tasks also have subtasks, as shown in Table 8.3.

**FIGURE 8.25**

Sulfur recovery plant complete bow tie diagram.

Source: [http://www.risk-support.co.uk/risk\\_software.htm](http://www.risk-support.co.uk/risk_software.htm).

Such similar steps must be carried out regarding the preventive and inspection policies defined in RCM. In addition, for the other threats such as “sabotage,” “natural disaster,” and “bad project definition” there will also be specific actions to be implemented over the asset life cycle. Indeed, a good risk project management program is able to identify the risk and provide an action plan to mitigate such risk. The big challenge is to integrate all risks and monitor them to mitigate action on time.

Such risk management philosophy is also a part of asset integrity management once the main objective is to maintain high performance of asset integrity by avoiding accidents and environmental impacts.

To monitor such action over the asset life cycle, the risk considered by the two bow tie consequences (loss of production and environmental impact) must be assessed and such risk will associate the probability that the threats take place once the layers of protection are not effective; in other words, the preventive actions were not implemented on time or were not effective enough.

Fig. 8.26 shows the risk assessment of the two bow ties’ final consequences (loss of production and environmental impact) based on the risk matrix concerning the consequences for people, environment, asset, and reputation.

The bow tie diagram risk assessment is performed with Active Bow Tie 1.7 software to have a single source of data and enable mitigation action implementation automatically. Therefore the risk assessment is also carried out by the software, which links the risk prediction to the bow tie diagram, as shown in Fig. 8.27.



**Table 8.3 Bow Tie Action Plan**

No.	Code	Activity/Task	Who	When
1	1.1	RAM analysis/define reliability requirement for critical equipment	Reliability engineer	Design phase
	1.1.1	Furnace (F-01)—99.7% in 3 years and 0.04 number of failures	Reliability engineer	Design phase
	1.1.2	Furnace (F-02)—99.7% in 3 years and 0.04 number of failures	Reliability engineer	Design phase
	1.1.3	Boiler (GV-01)—100% in 3 years and 0 number of failures	Reliability engineer	Design phase
2	2.1	Supplier selection/select supplier based on reliability requirement		
	2.1.1	Require lifetime data analysis or accelerated test from each supplier	Reliability engineer	Design phase
	2.1.2	Compare different supplier analyses	Reliability engineer	Design phase
	2.1.3	Chose supplier based on reliability assurance	Reliability engineer	Design phase
	2.1.4	Specify warranty contract for 3 years	Reliability engineer	Design phase
3	3.1	Supplier selection/critical equipment installation verification	Production engineer	Executive phase
	3.1.1	Verify critical task defined by supplier during furnace (F-01) installation	Production engineer	Executive phase
	3.1.2	Verify critical task defined by supplier during furnace (F-02) installation	Production engineer	Executive phase
	3.1.3	Verify critical task defined by supplier during boiler (GV-01) installation	Production engineer	Executive phase

		Frequency Category					
		A (Extremely Remote)	B (Remote)	C (Little Frequent)	D (Frequent)	E (Very frequent)	F (Extremely frequent)
		At least 1 between from 1000 to 100.000 years	At least 1 between from 50 to 1000 years	At least 1 between from 30 to 50 years	At least 1 between from 5 to 30 years	At least 1 between from 1 to 5 years	At least 1 in 1 years
Severity Category	IV	M	NT	NT	NT	NT	NT
	III	M	M	NT	NT	NT	NT
	II	T	T	M	M	M	M
	I	T	T	T	M	M	M

FIGURE 8.26

Risk matrix.

Hazard Code	Hazard Name	Top Event Code	Top Event Name
1	URE shutdown	1.01	Top Event

Code	Consequence	P	E	A	R
01	Loss production	B2	B3	B3	B2
02	Environment impact	B2	B3	B3	B3

FIGURE 8.27

Bow tie risk assessment. P, people; E, environment; A, asset; R, reputation.

As a result of risk assessment demonstrated in Fig. 8.27, the risk level for the environment (E) and asset (A) are moderate, which means that is not necessary additional actions to mitigate this risk level. Risk is calculated based on the following equation:

$$\begin{aligned} \text{Risk(Loss of production)} &= f_{\text{Loss of Production}} \times \text{Consequence} \\ \text{Risk(Loss of production)} &= (f_{\text{URE outage}} \times P_{\text{recovery}}) \times \text{Consequence} \\ f(\text{URE outage}) &= \sum_n^1 f_{\text{Threat}_n} \times \left( \prod_0^m P_{(\text{Barriers})_m} \right) \\ f(\text{URE outage}) &= \{0.33 \times (0.1 \times 0.1)\} + \{0.1 \times (0.1)\} + \{0.5 \times (0.01)\} \\ &\quad + \{0.33 \times (0.01)\} = 0.0193 \\ f(\text{Loss of production}) &= \{0.0193 \times (0.5)\} = 0.0097 \end{aligned}$$

A similar step was carried out for the risk assessment of environmental impact. Finally, the risk demonstrated in Table 8.4 calculates the frequency in the previous equation and classifies such frequency based on the risk matrix in Fig. 8.26 (0.097 → B). Therefore, concerning risk matrix consequence III, the final risk is “B III,” as shown in Table 8.4.

Indeed, different approaches can be applied to calculate the final risk. The consequence can also be expressed in monetary terms and consequently there will be a monetary risk measurement.

The importance of reliability and maintenance can be proved by Table 8.5 results where the risk level is intolerable if the reliability specification and preventive maintenance and inspection are not implemented. Such assumption is represented by 100% of failures in such layers of protection.

**Conclusions**

The main objective of this case study was to demonstrate the integrated asset integrity management methodology based on the sulfur recovery plant case study, which encompasses risk management and

**Table 8.4 Final Bow Tie Risk Assessment**

Threat	Frequency	Barriers	Probability	Top Event	Frequency	Recovery	Probability	Consequence	Frequency	Frequency Matrix	Consequence (Matrix)	Risk
Critical equipment failure	0.33	Reliability specification Preventive maintenance and inspection policies	0.1 0.1	URE outage	0.0193	Keep low level of sulfur emission	0.5	Loss of production	0.0097	B	III	B III
Sabotage	0.1	Security	0.1									
Natural disaster	0.5	Storm forecast	0.01			Control sulfur emission	0.5	Environmental impact	0.0097	B	III	B III
Bad project definition	0.1	Project management	0.01									

*URE = SRU = Sulfur Recovery Unit.*



reliability and maintenance methods implementation. Human reliability analysis was not implemented in this case because during the phase concept and development, FMEA was not carried out to identify human errors.

Asset integrity management must be updated in each asset life cycle phase and whenever necessary new methods such as FMEA, HAOP, HAZID, and human reliability analysis must be implemented according to each phase. In the next phase, define feed, the equipment is defined in component levels, therefore FMEA, RCM, and RBI can be carried out in detail and such information will be the input for RAM analysis as well as bow tie analysis.

The methodology proposed would achieve the following:

- To identify critical hazards based on semiquantitative risk analysis, which requires mitigation;
- To identify the layers of protection to avoid environmental impact and loss of production;
- To identify the important analysis that must be carried out in the next asset life cycle phase.

### 8.5.3 INTEGRATED LOGISTIC SUPPORT DURING THE DESIGN PHASE: THE SUBSEA CASE STUDY

To exemplify the advantages of ILS implementation during the design phase of the asset life cycle, a case study applied in the oil and gas industry will be presented in this section.

Concerning oil and gas assets, subsea equipment is the most critical in terms of investment, safety, and environmental criticality. Indeed, in the case of unsafe failures in flexible risers, flowlines, jumpers, and Pipeline End Manifold (PLEM) a major accident with catastrophic consequences may occur. In addition, loss of production may have huge economic consequences because of lack of proper spare parts or preventive maintenance and inspections. Fig. 8.28 shows the subsea system RBD, based on RAM analysis, which has achieved a lower performance than expected because of human errors during design installation and maintenance downtime.

System operational availability in the first 5 years is 90.34%. To improve subsea system performance it is necessary to mitigate the human error based on installation and maintenance procedure improvement and supervision follow-up. In addition, FMEA recommendations related to product specifications must be implemented during the design phase.

After all efforts have been made to achieve high performance by implementing the recommendations, system operational availability achieves 99.81% in 5 years. In fact, to achieve the lower LCC

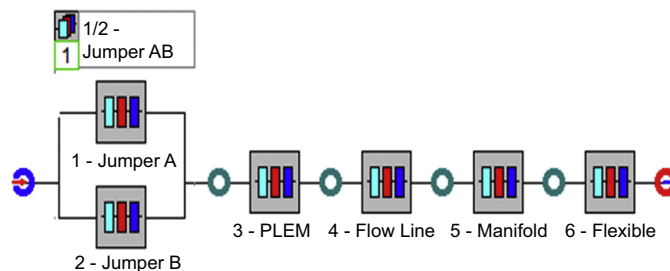


FIGURE 8.28

Subsea RBD (BQR apmOptimizer).

Source: <http://www.bqr.com>.

and higher operational availability it is necessary to take into account the cost of preventive maintenance, inspections, and spare parts optimization. In addition, logistic effects must be accounted for to have an integrated solution that the ILS methodology proposes.

To perform the ILS analysis the logistic times are very important. Table 8.6 considers the logistic times to deliver, test, and install critical subsea equipment.

In addition to logistic time, the LCC must be accounted for during ILS analysis and it is necessary to take into account the preventive maintenance and inspections of critical equipment, as shown in Table 8.7.

Concerning the logistics, all information is incorporated into the ILS model shown in Fig. 8.29, which considers all information deployed in Tables 8.6 and 8.7 as well as the RBD model described in Fig. 8.28. In addition, all preventive maintenance and inspection defined during RCM and RBI analysis is also incorporated into the logistic model. To optimize the preventive maintenance task such as the ROV inspection interval to minimize the LCC, optimization will be carried out. The ILS model was applied by using the apmOptimizer software, as shown in Fig. 8.29.

Concerning the flexible riser equipment, Table 8.8 shows the tradeoff analysis, which takes into account the initial annual inspection ROV and spare parts policy for the flexible riser and also the optimal inspection interval and spare parts policy for 5 years of operation.

In Table 8.8, the first column shows the different cases from A to F. The second column describes the scenarios A, B, C, D, and E, which consider human error for the first 5 years, and scenario F, which does not take into account human error (design, installation, and maintenance). The third

Item	Manufacturing Time (days)	Transportation Time (days)	Test and Installation Time (days)	Total Time (days)
Flexible riser	73	5	20	98
Flowline	73	5	20	98
Jumper	73	5	20	98
PLEM	73	5	20	98
Umbilical	73	5	20	98

Item	Equipment Cost (\$)	Test and Installation Time Cost (\$)	Repair Cost (\$)	ROV Cost (\$/day)
Flexible riser	440,000	200,000	640,000	50,000
Flowline	420,000	200,000	620,000	50,000
Jumper	105,000	150,000	550,000	50,000
PLEM	210,000	100,000	310,000	50,000
Umbilical	420,000	200,000	620,000	50,000

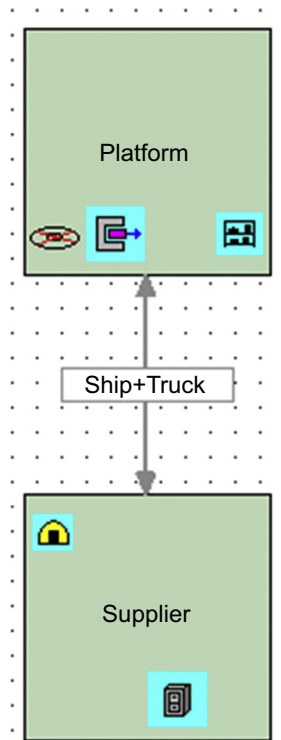


FIGURE 8.29

ILS model.

Cases	Scenario	Assumption	Inspection Interval (h)	Spare Number	Operational Availability (%)
A	With human errors accounted	Only corrective maintenance and spare parts	0	1 (Flexible riser)	99.80
B	With human errors accounted	Annual inspection without spare parts	8640	0	99.77
C	With human errors accounted	Optimal inspection without spare parts	8400	0	99.81
D	With human errors accounted	Optimal inspection and spare parts	8400	0	99.81
E	Without human errors accounted	Only corrective maintenance	0	0	100
F	Without human errors accounted	Only corrective maintenance and inspection	8640	0	100

column describes the assumptions that consider the type of maintenance and inspection and also the spare parts policy. The fourth column describes the inspection interval (ROV) based on RCM and RBI analysis on scenario B and optimal time based on the apmOptimizer solution described in scenarios C and D. The fifth column describes the spare parts (flexible riser) for different scenarios. In scenario A, one spare part is considered. For the other scenarios, a zero spare parts policy was implemented in the model.

The sixth column shows the operational availability achieved for each scenario based on each assumption.

Concerning operational availability, scenarios C, D, and F achieve the best operational availability in 5 years (99.81%).

Table 8.9 considers similar scenarios presented in Table 8.8 but shows the effect of inspection and spare parts policy on LCC for 5 years.

In Table 8.9, the first, second, and third columns are similar to Table 8.8. The fourth column describes the operating cost for each scenario. In this case, scenario A presents the highest cost, which is affected by the spare parts policy. Scenario D shows the lowest operating cost, which considers the optimal solution, which means the optimal inspection interval and spare parts. Scenario F shows the lowest operating cost considering no human error. The fifth column shows the consequence for assets that encompass the economic effect of loss of production based on expected number of failures. The sixth column encompasses the operational and asset consequence cost for each scenario. In this case, scenario A presents the worse result because the spare parts cost and lack of inspections will not prevent the failure and will increase the LCC. Scenarios D and F achieve the lowest LLC. In the first

Cases	Scenario	Assumption	Operational Cost (\$)	Consequence for Asset (\$)	LCC (\$)
A	With human errors accounted	Only corrective maintenance and spare	905,764.22	5,600,000.00 (10,000,000.00 × 0.56)	6505,764.22
B	With human errors accounted	Annual inspection without spare	1,256,566.34	80,000.00 (10,000,000.00 × 0.008)	1,336,566.34
C	With human errors accounted	Optimal inspection without spare	1,254,219.80	50,000.00 (10,000,000.00 × 0.005)	1,304,219.80
D	With human errors accounted	Optimal inspection and spare	1,254,219.80	50,000.00 (10,000,000.00 × 0.005)	1,304,219.80
E	Without human errors accounted	Only corrective maintenance	0	0	0
F	Without human errors accounted	Only corrective maintenance and inspection	1,250,000.00	0	1,250,000.00



case, scenario D is the optimal inspection interval, which avoids a higher number of failures and minimizes the consequence for the asset. Scenario F considers only the optimal inspection without any failures caused by human error.

The final solution applied a similar approach to other subsea critical equipment such as flowline, jumpers, and umbilical. Therefore the ILS model based on optimization minimizes the LCC and maximizes the operational availability.

### ***Conclusion***

The ILS model proposal optimizes asset performance and LCC including the logistics issues. To apply such methodology, plenty of failure, repair, maintenance, and logistic data are necessary.

The usual reliability engineering methods such as FMEA, RCM, RBI, RAM, and also asset integrity management are essential to perform the ILS optimization.

In many projects, to implement all methods requires time and investment, but more important is the culture of ILS as a key success factor to achieve high performance and lower LCC.

In many ILS applications, the optimal solution is not achieved because it requires an optimization model, which encompasses all information to define the best inspection and preventive maintenance interval, spare parts levels, and resource levels.

The case study presented was applied to a real subsea oil and gas project that successfully achieved the main objective: the logistic effect on system performance and also optimization of asset performance and LCC.

## **8.5.4 ASSET MANAGEMENT PROGRAM EVALUATION DURING THE DESIGN PHASE: THE OFFSHORE CASE STUDY**

To demonstrate asset management evaluation, this case study will present the offshore asset management process that encompasses the subsea and platform asset as a scope of asset management. The evaluation will be taken into account in the design phase.

To perform the audit process the company presented some basic information such as:

- Company features related to asset management, department, hierarchy, function, and asset characteristics;
- Asset management plan with all necessary definitions such as activities, responsibilities, resources, deliverables definition, and performance indexes;
- Procedures and standards related to the asset management program such as reliability engineering procedures, asset integrity procedures, and ILS procedures.

Based on this document the auditors, formed by a team with two specialists, planned the audit process, which was carried out during 2 days. The auditors' plan encompasses the following information:

- The managers will be part of the audit process based on the audit agenda.
- The documents, database, and procedures will be presented during the audit process.
- The audit process description will be provided with criteria about scores and required information for each ISO 55000 aspect.

The audit team delivers the audit plan to the client with additional adjustments in the audit agenda. In fact, during the audit the auditors must be sufficiently flexible to make a small adjustment so as not to cause any interference in the client normal work process.

It is very important that the auditors have experience in the ISO standard audit process and have an auditor certificate (ISO 9001, ISO 14001, OHSAS, or the ISO standards). In addition, the audit team must have specialists in all aspects covered by the asset management program, such as reliability engineering methods, risk management, preventive maintenance, risk analysis, human reliability, and ILS.

In many cases, there are discussions about asset integrity management and the integrated logistics support programs as part of asset management. In fact, all oil and gas companies take into account safety and the environment high performance achievement in their policies, which show the importance of the asset integrity high performance achievement for their processes. In addition, logistics always affect the asset performance and the integrated logistics support program is the state of the art of high performance logistic achievement over the asset life cycle.

The audit process results will be presented based on the evaluation template performed for each asset management aspect based on quantitative audit-defined criteria. No evidence will be presented in this test because of the confidential information. The asset performance aspects to be assessed during the audit process are:

- Context of the organization—weight 2
- Leadership—weight 1
- Planning—weight 1
- Support—weight 1
- Operation—weight 2
- Performance—weight 3

The weight of each aspect will be applied for the final core calculation based on weighted arithmetic average.

For each question, compliance is scored based on the following criteria:

T—Total compliance (100%—employee knows company procedures or practices, has good procedures or practices implemented with more than 75% of the total possible evidence recorded).

H—High compliance (75%—employee knows company procedures or practices, has good procedures or practices implemented, but has higher than 75% of possible evidence recorded).

P—Partial compliance (50%—employee knows partially company procedures or practices, has partially good procedures or practices implemented, but has lower than 75% and higher than 50% of possible evidence recorded).

L—Low compliance (25%—employee knows company procedures or practices, has no procedures or practices implemented, and has lower than 50% of possible evidence recorded).

N—No compliance (0%—employee does not know company procedures or practices, has no procedures or practices implemented, and has no evidence recorded).

NA—Not applicable.

Table 8.10 shows the asset management level classification.

<b>Score Class</b>	<b>Score</b>	<b>Asset Management Characteristics</b>	<b>Asset Management Level Classification</b>
A	9.6–10.00	The asset management program is adequate for all assets in the specific life cycle phase based on implementation of all the best reliability engineering, asset integrity management, and integrated logistic support program practices with compliance of all defined criteria	State of the art
B	8.9–9.5	The asset management program is adequate for most of the assets in the specific life cycle phase based on implementation of most of the best reliability engineering, asset integrity management, and integrated logistic support program practices with compliance of most of the defined criteria	Excellent benchmarking
C	7.9–8.8	The asset management program is adequate for many assets in the specific life cycle phase based on the implementation of many of the best reliability engineering, asset integrity management, and integrated logistic support program practices with compliance of many of the defined criteria	Very good
D	5.1–7.8	The asset management program is adequate for many assets in the specific life cycle phase based on implementation of some of the best reliability engineering, asset integrity management, and integrated logistic support program practices with compliance of many of the defined criteria	Good
E	4.1–5.0	The asset management program is adequate for some assets in the specific life cycle phase based on implementation of some of the best reliability engineering, asset integrity management, and integrated logistic support program practices with compliance of many of the defined criteria	Intermediate
F	0–4.0	The asset management program is adequate for a low number of assets in the specific life cycle phase based on implementation of any of the best reliability engineering, asset integrity management, or integrated logistic support program practices with compliance of some of the defined criteria	Beginning

### ***Asset Management Aspects Evaluation***

“Context of the organization” encompasses all aspects related to the link between the external and internal environments defined by the business strategy that is defined in the asset strategy objectives and KPI definitions. In this case, it is necessary to demonstrate that all asset strategic objectives take into account the stakeholder requirements based on the questions defined in [Table 8.11](#). [Table 8.11](#) encompasses the evaluation for this aspect with the columns questions, the evidence required, evidence presented, comment, score class, score, and punctuation.

The final punctuation for this aspect is calculated based on the arithmetic average of the questions punctuation. Concerning the context and organizational aspect, the asset management policy does not

**Table 8.11 Context of the Organization Aspect Evaluation**

	Required Information	Evidence Required	Evidence Presented	Comment	Score Class	Score	Punctuation
1	The asset management policy contemplates the effort of physical asset performance achievement, including reliability, preventive maintenance, logistic integrated support asset integrity, and LCC aspects such as: a. Spare part policy b. Delay times and turnout c. Preventive maintenance d. Reliability and operational availability index definition e. Safety and environmental risk mitigation f. Life cycle cost optimization g. Continuous improvement and performance optimization h. Compliance with the law, safety, and environment legal requirement i. Compliance with all stakeholder requirements	Electronic and written policy	Electronic and written policy	Not all aspects are covered in the policy explicitly such as ILC and LCC	H	0.75	0.75
2	The asset management policy communicates to all levels throughout an organization	Minutes of the meeting signed up and emails about the asset management policy communication	Email and report	N/A	T	1	1
3	The asset management policy relates to business strategy	Assessment of business strategy plan and asset management objectives, goals, and KPIs	Email and report	N/A	T	1	1

*Continued*

	<b>Required Information</b>	<b>Evidence Required</b>	<b>Evidence Presented</b>	<b>Comment</b>	<b>Score Class</b>	<b>Score</b>	<b>Punctuation</b>
4	The strategic asset management objectives, goals, and KPIs are defined for all organizational levels	Written and electronic evidence of asset management strategic objectives, goals, and KPIs	Email and RAM analysis report	N/A	T	1	1
5	The asset management strategy is updated regularly based on business or stakeholders' necessity	Minutes of the meeting and emails about the asset management strategic objectives, goals, and KPIs updated	Emails	N/A	T	1	1
	Final punctuation						9.5
	Final classification						B

contemplate 100% of aspects defined in question 1 such as ILS and LCC. Therefore total compliance was not achieved for such criteria.

“Leadership” must demonstrate the compliance of the leader’s involvement in communicating the asset management policies, objectives, and monitoring the KPIs, implement improvement actions, as well as support the implementation of the programs such as reliability, asset integrity, and ILS. [Table 8.12](#) shows all questions, evidence, and related score based on the evidence presented. In this case questions 2 and 3 did not achieve 100% compliance. The leadership does not follow up 100% of activities and performance by meeting, but in many cases there are email messages. In this case, meeting is difficult because the teams that work in the asset management program are located in different continents such as Asia, North America, and Europe.

However, a teleconference can be conducted, but because of lack of time, some participants find this option difficult in 100% of cases at all organizational levels. The improvement actions are, in many cases, communicated by emails, but for the same reason related to question 3 there is not 100% compliance.

“Planning” focuses on the organization’s activities, including its asset management activities. Therefore the asset management program plan is defined concerning all resources and methods that will be implemented during the asset life cycle. In this plan, all responsibilities and deliverables must be defined as well. [Table 8.13](#) shows all questions, evidence, and related score based on presenting evidence for the leadership aspect. Concerning the planning aspect the organization achieves state of the art. They demonstrate compliance for all five questions and very good practices of not only

**Table 8.12 Leadership Aspect Evaluation**

	Required Information	Evidence Required	Evidence Presented	Comment	Score Class	Score	Punctuation
1	The leaders defined in the asset management plan communicate the asset strategy, strategic objectives, and asset policy at all organizational levels	Electronic or written asset management plan	Email and procedures	N/A	T	1	1
2	The leaders follow up the asset performance at all organizational levels	Minutes of the meeting signed up and emails about asset performance followed up	Email and procedures	There is no meeting for 100% follow-up but in many cases there are email messages	H	0.75	0.75
3	The leaders defined in the asset management plan implement improvement actions based on the asset performance at all organizational levels	Minutes of the meeting about improvement actions based on the asset performance signed up. Email and other electronic evidence can also be considered in a specific situation as well as physical evidence	Email and procedures	There is no meeting, only email messages on most cases	P	0.5	0.5
4	The leaders defined in the asset management plan support the employees to achieve the KPIs at all organizational levels by addressing the necessary technological and financial management support	Minutes of the meeting about support for the employees to achieve the KPIs signed up. Email and other electronic evidence can also be considered in a specific situation as well as physical evidence	Email and procedures	N/A	T	1	1

*Continued*

**Table 8.12 Leadership Aspect Evaluation—cont'd**

	Required Information	Evidence Required	Evidence Presented	Comment	Score Class	Score	Punctuation
5	The leaders defined in the asset management plan recognize and award the employees and team effort for KPI achievement	Minutes of the meeting about recognizing and awarding the employees and team effort for KPI achievement signed up. Email and other electronic evidence can also be considered	Email and HR procedures	N/A	T	1	1
	Final punctuation Final classification						8.5 C

**Table 8.13 Planning Aspect Evaluation**

	Required Information	Evidence Required	Evidence Presented	Comment	Score Class	Score	Punctuation
1	The asset management plan is derived and related to asset management strategic objectives, goals, and indexes definition	Assessment of the electronic or written asset management plan based on asset management, strategic objectives, goals, and KPI definition	Emails and electronic evidence	N/A	T	1	1
2	The asset management plan defines the human resources, economic resources, the target time for each activity and deliverables, the methods, and technology based on the asset strategic objectives	Assessment of the written or electronic asset management plans	Emails and electronic evidence	N/A	T	1	1

**Table 8.13 Planning Aspect Evaluation—cont’d**

	Required Information	Evidence Required	Evidence Presented	Comment	Score Class	Score	Punctuation
3	The necessary employee training is defined in the asset management plan for each asset life cycle	Assessment of the asset management training electronic or written list based on asset management plans definition	Emails and electronic evidence	N/A	T	1	1
4	The organizational structure, hierarchy, function, and responsibility for the asset management is defined for each phase of the asset life cycle	Assessment of the written or electronic asset management plans	Emails and electronic evidence	N/A	T	1	1
5	The asset management plan is updated during the asset life cycle phases and during the life cycle Final punctuation Final classification	Minutes of the meeting signed up and emails about the asset management plan updated	Emails and electronic evidence	N/A	T	1	1
							10 T

planning the activities of asset management, but also considering the delivery time, requirements, as well as cost for each task.

“Support” requires collaboration among many groups of the organization. Therefore employees’ training and qualification are important issues in this item. Table 8.14 shows all questions, evidence, and related score based on presenting evidence for the support aspect. In this case the organization achieves partial compliance on questions 3 and 4. In fact, despite the high quality of the different analyses in all cases, there is no procedure for all of them such as RAM analysis, LDA, and ILS. In addition, in these cases employees are not qualified to perform such analyses, which require external support. The asset management team activities are highly coordinated at the top organizational level by project managers, but not at all organizational levels by discipline leaders.

“Operation” encompasses the directing, implementation, and control of asset management activities. Therefore all documents related to asset management as well as how the information is updated, stored, and linked to different asset life cycle phases must be demonstrated. Table 8.15 shows all questions, evidence, and related score based on presenting evidence for operational aspects. Questions 2 and 3 have not achieved total compliance. Concerning question 2 the KPI communication, access, and record of lessons learned to enhance the organizational improvement are not applied at all organizational levels. In addition, concerning verification and validation for KPIs, LDA implementation must be improved. In this case, there is a lack of data to perform such analysis, which influences the effectiveness of KPI prediction.



**Table 8.14 Support Aspect Evaluation**

	<b>Required Information</b>	<b>Evidence Required</b>	<b>Evidence Presented</b>	<b>Comment</b>	<b>Score Class</b>	<b>Score</b>	<b>Punctuation</b>
1	The employees' necessary competence related to their asset management activities is defined for organizational levels	Human resource electronic or written document about competences and evidence of employee training	Human resource electronic and written document	N/A	T	1	1
2	The employees' necessary training related to asset management is defined for all organizational levels	Assessment of the written or electronic train list based on asset management plans definition	Human resource electronic and written document	N/A	T	1	1
3	The employees' activities related to asset management, such as reliability engineering, asset integrity, and ILS, are based on the procedures defined for all organizational levels	Written or electronic procedures	Electronic procedures	There is no procedure for RAM analysis, LDA, and ILS	P	0.5	0.5
4	The team activities are coordinated to support the asset management activities at all organizational levels based on asset management plan and procedures	Minutes of the meeting signed up and emails about the asset management activities coordination and procedures	Emails and some meetings	There is no meeting for all organization levels only for the highest one	P	0.5	0.5
5	The employees have a channel to suggest new methods and approaches as well as asset management improvement based on the information technology that can be recorded and accessed at different organizational levels	Minutes of the meeting signed up and emails or written evidence	Email and meeting	N/A	T	1	1
	Final punctuation						8
	Final classification						C

**Table 8.15 Operation Aspect Evaluation**

	Required Information	Evidence Required	Evidence Presented	Comment	Score Class	Score	Punctuation
1	The asset management technology information, flow, and procedures defined in the asset management plan enable the KPIs to be assessed, recorded, and updated regularly at all organizational levels	Electronic and written evidence of KPIs accessed, recorded, and updated regularly at all organizational levels	Electronic and written evidence	N/A	T	1	1
2	The asset management, information technology, and procedures defined in the asset management plan enable KPI communication, access, and recording of lessons learned to enhance organizational improvement at all organizational levels	Electronic and written evidence of KPI communication, access, and recording of lessons learned. Minutes of the meeting signed up is also evidence of lessons learned	Electronic and written evidence	Not for all cases	H	0.75	0.75
3	The reliability engineering methods defined in the asset management plan are implemented in each asset management phase concerning the verification and validation of the tasks and KPIs defined in the previous phases	Electronic and written evidence of engineering method's implementation based on asset management plan definition. Such evidence must demonstrate the verification and validation of the tasks and KPIs defined in the previous phases	Electronic evidence (email, reports, and minutes of the meeting)	For most cases the LDA must be improved	H	0.75	0.75

*Continued*

	<b>Required Information</b>	<b>Evidence Required</b>	<b>Evidence Presented</b>	<b>Comment</b>	<b>Score Class</b>	<b>Score</b>	<b>Punctuation</b>
4	The asset integrity management methods defined in the asset management plan are implemented in each asset management phase concerning the verification and validation of the tasks and KPIs defined in the previous phases	Electronic and written evidence of asset integrity method's implementation based on asset management plan definition. Such evidence must demonstrate the verification and validation of the tasks and KPIs defined in the previous phases	Electronic and written evidence	N/A	T	1	1
5	The integrated logistic support methods defined in the asset management plan are implemented in each asset management phase concerning the verification and validation of the tasks and KPIs defined in the previous phases	Electronic and written evidence of ILS method's implementation based on asset management plan definition. Such evidence must demonstrate the verification and validation of the tasks and KPIs defined in the previous phases	Electronic and written evidence	N/A	T	1	1
	Final punctuation						9
	Final classification						B

“Performance” must demonstrate the evidence of the achievement of objectives for each asset life cycle based on asset management program plan definition as well as the measurement and achievement of the KPI’s targets during the operational phase. Therefore the KPI’s monitoring, verification, and validation process throughout all asset life cycle phases as well as the improvement actions and lessons learned, documentation, and communications must be demonstrated. Table 8.16 shows all questions, evidence, and related score based on presenting evidence for the performance aspect.

Questions 3, 4, and 5 did not achieve total compliance. In the case of question 3 the activities and deliverables defined in the asset management plan, for most of the cases, were performed during the defined date.

**Table 8.16 Performance Aspect Evaluation**

	Required Information	Evidence Required	Evidence Presented	Comment	Score Class	Score	Punctuation
1	The asset management strategic objectives are achieved	Electronic or written evidence of asset management strategic objectives achievement	Electronic or written evidence	N/A	T	1	1
2	The asset management KPIs are achieved concerning all organizational levels	Electronic or written evidence of asset management KPIs achievement	Electronic or written evidence	N/A	T	1	1
3	The activities and deliverables defined in the asset management plan are performed during the defined date in each asset life cycle phase	Electronic or written evidence of activities and deliverables final dates according to asset management plan definition	Electronic or written evidence	For most cases	H	0.75	0.75
4	The recommendation of the reliability engineering, asset integrity, and ILS methods are implemented on time	Electronic or written evidence of recommendation plan related to each analysis and implementation	Electronic or written evidence	For most cases	H	0.75	0.75
5	The defined improvement action based on KPI results and deliverables is implemented on time	Electronic or written evidence of improvement action implementation of KPI results	Electronic or written evidence	For most cases	H	0.75	0.75
	Final punctuation						8.5
	Final classification						C

Concerning question 4 the recommendation of the reliability engineering, asset integrity, and ILS methods, for most of the cases, were implemented on time.

Finally, concerning question 5, improvement actions based on KPI results and deliverable reports were implemented on time for most of the cases.

Based on individual aspects of asset management evaluation, the final evaluation takes place as demonstrated in [Table 8.17](#), which encompasses the aspects, score class, score, weight, punctuation, final punctuation, final evaluation and final score class. The final punctuation is calculated by the weighted arithmetic average.

	Aspect	Score Class	Score	Weight	Punctuation	Final Punctuation	Final Score Class
1	Context of the organization	B	9.5	2	19		
2	Leadership	C	8.5	1	8.5		
3	Planning	T	1	1	1		
4	Support	C	8	1	8		
5	Operation	B	9	2	18		
6	Performance evaluation	C	8.5	3	25.5		
	Total	C		10	80	8	Very good

### Conclusion

Based on [Table 8.17](#) results the asset management program achieves a very good score class classification, which means the asset management program is adequate for most of the assets in the specific life cycle phase. Such achievement was demonstrated based on compliance of the best reliability engineering, asset integrity management, and ILS program practices implementation.

Indeed, the different score class is achieved for different asset management aspects. Concerning the aspect planning the organization has achieved the total compliance, which means state of the art. In this case, different groups in the same companies, or even organizations in the same industry, can look at the learning aspect of such organizations to improve their own asset management performance. Similar to other aspects such as context of the organization and operation, high performance is achieved and minor improvement is required.

In the case of other aspects, it is clearly a necessary improvement to achieve the highest asset performance, but it is also necessary to consider the complexity of asset management program implementation and the available resources such as people, time, and money to invest in it.

The main advantage of such audit process implementation is that it enables continuous improvement over time and for the next asset life cycle phase. Additionally, the audit process results provide enough information to address the necessary improvement when necessary. Such improvement can be supported by internal or external specialists.

---

## REFERENCES

- Accenture, 2001. Repsol YPF - A complete implementation model of balanced scorecards in the Oil and Gas sector. SeUGI 19. Florence. June 2001.
- Calixto, E., Bot, Y., 2015. RAM analysis applied to decommissioning phase: comparison and assessment of different methods predict future failures. In: ESREL 2014, Wroclaw, Poland. Taylor & Francis Group, London. ISBN:978-1-138-02681.
- Calixto, E., 2014. RAMS Analysis applied to decommissioning phase: Comparing and assess different methods to predict future failures. ESREL 2015, Wroclaw, Poland. © 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0.

- Calixto, E., 2015a. Integrated Logistic Support. RAM, preventive maintenance, inspection, spare parts and life cycle cost optimization based on dynamic program. In: ESREL 2015, Zürich, Switzerland. Taylor & Francis Group, London, ISBN 978-1-138-02879-1.
- Calixto, E., 2015b. Integrated asset integrity management: risk management, human factor, reliability and maintenance integrated methodology applied to subsea case. In: ESREL 2015, Zürich, Switzerland. Taylor & Francis Group, London, ISBN 978-1-138-02879-1.
- EFNMS Asset Management Survey. ESREDA Conference, Porto, Portugal, May 2013. <http://www.efnms.org/mod/newsarchiv/view/cp-m10/newsmeldung-28>.
- <http://www.bqr.com>.
- [http://www.risk-support.co.uk/risk\\_software.htm](http://www.risk-support.co.uk/risk_software.htm).
- <http://blog.readytomanage.com/wp-content/uploads/2013/08/performance-management-diagram-kaplan-norton.jpg>.
- <http://www.mulkerin.com/images/>.
- ISO 55001:2014. Asset Management. BSI Group. Retrieved 10 February 2014.
- ISO 55002 standard, 2014. <http://www.bsigroup.com/en-GB/search-results/?q=ISO+55002>.
- JP886 Defence Logistic Support Chain manual. <https://www.gov.uk/government/collections/jsp-886-the-defence-logistics-support-chain>.
- Kaplan, R.S., Norton, D.P., 1996. The Balanced Scorecard: Translating Strategy into Action. Boston, MA.: Harvard Business School Press, ISBN 978-0875846514.
- KP3 Audit Guide. Program Final Report. <http://www.hse.gov.uk/offshore/programmereports.htm>.
- PAS 55 standard, 2008. <http://www.bsigroup.com/en-GB/search-results/?q=PAS+55>.
- Sutton, I., 2010. Process Risk and Reliability Management: Operational Integrity Management, first ed. Elsevier. ISBN-13: 978-1437778052.

# Index

*Note:* Page numbers followed by “f” indicate figures, “t” indicate tables.

## A

- Accelerated factor (AF), 97, 99, 102
- Accelerated life test (ALT), 79–80, 682–683
- Accelerated tests, 94
- Acceptable error, 52
- Accident Sequence Analysis, 649, 651f
- Accident Sequence Evaluation Program (ASEP), 485
  - event tree, 488f
  - post-accident analysis methodology, 491–495
  - pre-accident analysis methodology, 485–491
- Accident Sequence Precursor program (ASP program), 504
- Account qualitative methods, 684
- Achieved availability, 273
- Acid gas treatment plant (U-23), 432, 432f
- Acid water treatment plant (U-26), 433–434, 434f
- Acoustic method, 181
- Acquisition cost, 205
- Activation energy, 97
- Active redundancy, 306
- AEC. *See* Atomic Energy Commission (AEC)
- AF. *See* Accelerated factor (AF)
- Aggregated individual method, 6–7, 473
- AI index. *See* Availability importance index (AI index)
- AIM. *See* Asset integrity management (AIM)
- ALARP. *See* As low as reasonably practicable (ALARP)
- ALT. *See* Accelerated life test (ALT)
- ALTA PRO software (Reliasoft), 100
- American Petroleum Institute (API), 193
- API. *See* American Petroleum Institute (API)
- apmOptimizer software (BQR software), 332
- ARENA, 445
- Arithmetic average, 16
- Arrhenius life–stress model, 97–101
  - reliability  $\times$  time, 101f
  - sensor reliability curve
    - under different temperature conditions, 100f
    - under usual conditions, 99f
  - time to failures in accelerated test, 98t
- As low as reasonably practicable (ALARP), 555
  - individual risk, 558f
- ASEP. *See* Accident Sequence Evaluation Program (ASEP)
- ASL. *See* Average stock level (ASL)
- ASP program. *See* Accident Sequence Precursor program (ASP program)
- Asset integrity, 719
- Asset integrity management (AIM), 719–723, 726, 736
  - decision flow, 737f
  - flexible riser FMEA, 739f
  - phases, 735–736
    - sixth phase, 738–742
  - RAM analysis, 737
  - severity criteria, 736f
- Asset maintenance processes, 693f
- Asset management, 703, 706f. *See also* Reliability management
  - aspect evaluation, 756–766
    - context of organization, 757t–758t
    - final asset management evaluation, 766t
    - leadership aspect evaluation, 759t–760t
    - operation aspect evaluation, 763t–764t
    - performance aspect evaluation, 765t
    - planning aspect evaluation, 760t–761t
    - support aspect evaluation, 762t
  - asset integrity management, 719–723
  - BSC, 703, 704f, 705
    - perspective objectives, 705f
  - case studies, 734
    - asset integrity management, 736–742
    - asset integrity management phases, 735–736
    - bow tie action plan, 746t
    - bow tie risk assessment without mitigations, 749t
    - final bow tie risk assessment, 748t
    - ILS model, 752f
    - offshore case study, 754–766
    - risk matrix, 746f
    - subsea case study, 735–742, 750–754
    - sulfur recovery plant case, 742–750
  - evidence compliance with, 733t–734t
  - ILS, 723–727
  - internal business process, 704
  - ISO 55000, 709
    - element relationship, 710f
  - KP3 audit guide, 721f
  - KPI, 717
    - hierarchy, 717f
  - LCP approach, 712
  - level classification, 728t, 756t
  - life cycle, 714f
  - methodology, 174–176
  - oil and gas life cycle, 713
  - operational excellence, 722f
  - operational integrity management, 722f
  - organizational context, 712f

- Asset management (*Continued*)
    - by PAS 55, 707–709
    - items related to ISO standards, 708f
    - PDCA, 707f
    - performance evaluation, 709–710
    - phases and reliability methods, 715f
    - physical assets, 711
    - program evaluation, 727–734
    - reliability engineering, 686–687, 716
    - ROI, 718
    - warranty objective, 714–716
  - Asset performance optimization, ILS for system, 727f
  - Atmospheric and vacuum distillation plant (U-10), 429–430, 430f
  - Atmospheric distillation, 338–341, 341f
  - Atmospheric distillation plant (U-11), 429, 429f
  - Atomic Energy Commission (AEC), 693
  - ATTD. *See* Average time to deliver (ATTD)
  - Attenuation, 560
  - Availability, 445
    - average, 273
    - performance index, 299–305
      - AI index, 304–305
      - availability rank index, 302–303, 303f
      - downtime event critical index, 301, 302f
      - failure rank index, 300–301, 301f
      - percentage losses index, 299–300, 300f
      - RI index, 303–304, 304f
      - utilization index, 305
    - rank index, 302–303, 303f
  - Availability importance index (AI index), 304–305
  - Average, 25, 27–30
  - Average stock level (ASL), 318
  - Average time to deliver (ATTD), 409
  - Avoidance category, 605
- B**
- Balanced scorecard (BSC), 703, 704f
    - perspective objectives, 705f
  - Basic condition 1 (BC1), 486, 488
  - Basic condition 2 (BC2), 486, 488
  - Basic condition 3 (BC3), 486, 489
  - Basic condition 4 (BC4), 486, 489
  - Basic human error probability (BHEP), 486
  - Basic process control system (BPCS), 622–623
  - Bathtub curve, 16, 17f
  - Bayer case, 691–693
  - Bayes equation, 8
  - Bayesian inference methodology, 7–8
  - Bayesian network, 514–519, 517f
    - application, 535–537
    - casing drilling, 518f
    - results, 536f, 538f
    - startup turbine, 535f
  - BC1. *See* Basic condition 1 (BC1)
  - Bearing pump test, 103
  - Bernard equation, 43
  - Best platform offshore configuration, 460–469
  - Best time to replace equipment, 204–205
  - BHEP. *See* Basic human error probability (BHEP)
  - BLEVE. *See* Boiling liquid expanding vapor explosion (BLEVE)
  - BlockSim software, 312, 344, 350–351, 439
  - Blowout accident analysis, 648–650
  - Boiler optimum replacement time, 207, 207f
  - Boiler system, 456f
  - Boiling liquid expanding vapor explosion (BLEVE), 233
  - Bow tie analysis, 563, 611
    - Bow tie case study application, 645–646
    - pipeline gas leak, 611f–612f
    - probability variation over time, 617t
    - time-dependent bow tie analysis, 616–620
    - time-independent bow tie analysis, 613–616
  - Bow tie integrated approach, 641
    - bow tie case study application, 645–646
    - FTA case application, 646
    - human reliability, 642–644
    - hybrid method case application, 646–648
    - hybrid risk analysis, 648
    - sensitivity analysis, 647
  - BPCS. *See* Basic process control system (BPCS)
  - BQR software. *See* apmOptimizer software (BQR software)
  - BSC. *See* Balanced scorecard (BSC)
- C**
- C3 Separation, 362, 362f
  - CAFDE software, 41, 67, 80
  - Catalytic cracking plant (U-21), 434, 435f
  - CBM. *See* Condition-based monitoring (CBM)
  - CCR. *See* Cracking catalytic reform (CCR)
  - CD. *See* Complete dependence (CD)
  - CDF. *See* Cumulative density function (CDF)
  - CENPES II project reliability analysis, 372
    - conclusions, 384–385
    - data analysis, 373–375
      - diesel oil subsystem failure data, 375t
      - qualitative data analysis, 374t
    - efficiency cost analysis, 384
    - value analysis, 384t–385t
    - optimization, 379–383
    - system characteristics
      - cold water subsystem, 373
      - diesel oil subsystem, 373
      - electrical subsystem, 372
      - natural gas subsystem, 372–373
      - water-cooling subsystem, 373



- system modeling, 375–379, 376f
  - cold water subsystem modeling, 379, 381f
  - electric, 377–379, 378f
  - laboratories modeling, 379–383, 382f
  - simulation results, 377t
  - water cooling subsystem modeling, 379, 380f
- Center for Industrial Asset Management (CIAM), 699–700
- Center integrated processing data (CIPD), 372–373, 375
- Centrifugal compressor FMEA/RCM, 238–247, 246f–247f, 248t–252t
- Centrifugal pump FMEA/RCM, 225, 225f
  - bearing, 231t, 258t
  - equipment and component function, 226t
  - impeller and shaft, 228t, 255t
  - O-ring, casing, and coupling risk assessment, 227t, 253t–254t
  - packing, 232t, 259t
  - risk matrix, 233f
  - seal, 229t–230t, 256t–257t
  - severity classification, 234f
- Centroid test. *See* Laplace test
- Characteristic life parameter, 32, 102–103
- Chi square method, 52–54
  - chi square calculation, 54t
  - chi square critical values, 53t, 55t
  - compressor's sensor observed data, 53t
- CIAM. *See* Center for Industrial Asset Management (CIAM)
- CIPD. *See* Center integrated processing data (CIPD)
- Classic failure rate representation, 15–16
- Cleaning, 420, 420f
- CM. *See* Condition monitoring (CM); Corrective maintenance (CM)
- Coffin–Manson relationship, 100–101
- Cold Area, 419, 419f
- Cold water subsystem, 373
  - modeling, 379, 381f
- COMAH system. *See* Control of Major Accident Hazards system (COMAH system)
- Commission error, 474
  - probability, 550–551
- Commissioning phase, human error assessment during, 540
- Common cause failure, 161
- Complete dependence (CD), 491
- Component, 222
  - function, 222
- Compression subsystem, 388, 390f
- Compressor's optimum replacement time
  - conclusion, 426–427
  - critical analysis, 421
    - downing event criticality index, 423f
    - reliability importance, 422f
- failure and repair data analysis, 416
  - furnace failure and repair PDF parameters, 417f
- modeling, 416–420
  - cleaning, 420, 420f
  - cold area, 419, 419f
  - conversion, 418, 418f
  - DEA subsystem, 419–420, 420f
  - fluid catalytic cracking system RBD, 418f
  - warming subsystem, 416–418, 418f
- sensitivity analysis, 422–426
  - compressor A life cycle analysis, 426f
  - compressor A lifetime data analysis failure rate functions, 425f
    - optimum replacement time, 424f
    - optimum replacement time methodology, 424f
    - System phase diagram, 427f
  - simulation, 421
- Condition monitoring (CM), 692
- Condition-based monitoring (CBM), 187–188
- Confidence limits, 59–60
- Consensus group method, 7–8, 8f, 473
- Consequence
  - analysis, 513
    - and effects analysis, 584–585
- Control meshes (MC2), 375
- Control of Major Accident Hazards system (COMAH system), 194
  - Conversion, 418, 418f
- Cooling subsystem, 379
- Corrective actions system, 209, 213f
- Corrective maintenance (CM), 179
  - downtime, 299
- Correlation, 49
- Corrosion, 95, 612
- Cracking catalytic reform (CCR), 441
- Cracking thermal (CTB), 441
- Cramer–von Mises tests, 57–58, 58t–59t
- Creep, 96
- Critical analysis, 174–179
  - compressor's optimum replacement time, 421
    - downing event criticality index, 423f
    - reliability importance, 422f
  - criticality matrix, 176t
  - design phase, RAM analysis during, 465
    - critical equipment, 466t
    - operational availability rank, 466t
  - distillation plant study case, 345–347
    - EC index, 345, 346f
    - equipment RI, 345, 347f
    - RI, 345, 346f
  - equipment criticality assessment, 177t

- Critical analysis (*Continued*)  
 RAM + L analysis, 441–442  
   macrosystem RBD configuration, 442f  
   system efficiency improvement, 442t  
 refinery plant availability optimization, 363–365  
 thermal cracking plant ram analysis, 392–397  
   downtime event criticality index, 395f  
   percentage failure index, 395f  
   reliability importance, 393f–394f  
   system operating and system not operating, 396f
- Critical equipment list, 174–179
- Criticality analysis. *See* Critical analysis
- Crow extended model, 138–140  
   reliability  $\times$  time stages, 141f  
   sensor improvement test result, 140t
- Crow-AMSAA model, 124–131, 446, 448–449, 453, 460  
   compressor MTBF  $\times$  time, 130f  
   failure intensity  $\times$  time, 128f  
   pumps Crow–AMSAA parameters, 129t  
   seal pump failure intensity  $\times$  time, 129f
- CTB. *See* Cracking thermal (CTB)
- Cumulative density function (CDF), 18, 477–478, 557
- Cumulative failure rate, 142
- Cumulative number of failure function, 202
- Cumulative risk model, 116–118  
   reliability  $\times$  time  $\times$  voltage, 119f  
   stress level over test time, 118f  
   time to failures in two stress levels, 118t  
   varying stress levels, 120f
- Cut set events, 577
- Cyclic strain-controlled test, 97
- D**
- Data analysis, CENPES II project reliability analysis, 373–375  
   diesel oil subsystem failure data, 375t  
   qualitative data analysis, 374t
- Data characteristics, 9
- Data failure, 275–277  
   maintenance activities steps on vessel, 277t  
   quantitative failure and repair data, 276t
- Data monitoring, 208f
- DEA system. *See* Diethylamine system (DEA system)
- DECI. *See* Downing event criticality index (DECI)
- Decisor's profile, 687–689, 688f
- Decommissioning phase, RAM analysis in, 445–448, 448f.  
   *See also* Design phase, RAM analysis during  
   asset management, 447f  
   boiler system, 456f  
   case study, 454–457  
   comparing different methods, 453  
   conclusion, 457–460  
   GRM, 449–450, 450f  
   hot water boiler subsystem, 457f  
   hot water distribution subsystem, 458f  
   LDA, 450–453, 452f  
   loss of production during winter, 459f  
   optimum replacement time, 460f  
   reliability database, 455t  
   RGA, 448–449, 454f  
   RGA  $\times$  MC, 456t  
   Deethanizer, 361–362, 362f  
   Degradation, 143–145  
     limit, 145  
     in stock, 409–410  
   Degrees of freedom, 52  
   Delphi method, 6–7, 473  
   Dependent duration, 95  
   Depropanizer, 361, 361f  
   Design failure mode effects analysis (DFMEA), 95, 160,  
     163–167  
     detection, 165t  
     frequency of failure, 164t  
     seal pump, 166t  
     severity effect, 165t  
   Design phase, RAM analysis during, 460–461. *See also*  
     Decommissioning phase, RAM analysis in  
     conclusion, 469  
     criticality analysis, 465  
       critical equipment, 466t  
       operational availability rank, 466t  
     LDA, 461–462, 462t  
     methodology, 461, 462f  
     modeling, 462–464  
     sensitivity analysis, 465–468  
       asset performance after preventive maintenance,  
         468f, 468t  
       asset performance by year, 467t  
     simulation, 465  
       asset performance prediction, 465t  
   Deviation, 23, 25, 27–30  
   DFMEA. *See* Design failure mode effects analysis (DFMEA);  
     Drive design improvement (DFMEA)  
   Diesel drying subsystem, 342, 342f  
   Diesel hydrodesulfurization plant (U-13), 430–431, 431f  
   Diesel oil subsystem, 373  
   Diethylamine system (DEA system), 286f, 287–288  
     plant RBD, 433f  
     subsystem, 419–420, 420f  
     treatment system, 172–174, 174f  
   Dynamic Program (DP), 330  
   Distillation plant study case in Brazilian oil and gas industry,  
     334–335  
     conclusion, 348

- critical analysis, 345–347
    - EC index, 345, 346f
    - equipment RI, 345, 347f
    - RI, 345, 346f
  - failure and repair data analysis, 335
    - fan PDF, 336f
    - quantitative failure and repair data, 336f
  - modeling, 335–344
    - atmospheric distillation, 338–341, 341f
    - diesel drying subsystem, 342, 342f
    - distillation subsystem RBD, 337f
    - heating, 338, 339f
    - merox subsystem, 344, 344f
    - prefractioning subsystem, 338, 340f
    - preheating, 337, 337f
    - salt treatment, 337, 338f
    - vacuum distillation subsystem, 342, 343f
    - water treatment subsystem, 342, 342f
  - sensitivity analysis, 347–348
  - simulation subsystem, 344–345
  - Downing event criticality index (DECI), 301, 302f, 392–393, 421, 423f
  - Downtime event criticality index, 395f
  - DP. *See* Dinamic Program (DP)
  - Drawwork, 402f
  - Drill facility system, 399
    - conclusions, 415–416
    - introduction, 399
    - partial availability, 399–403
      - case study, 404–415
      - drawwork, 402f
      - PDF parameters discounted time, 400f
      - timeline, 403f
  - Drive design improvement (DFMEA), 684
  - Duane model, 123–124
- E**
- EC index. *See* Event criticality index (EC index)
  - ECOM. *See* Error commission (ECOM)
  - Effectiveness factor, 139
  - Efficiency cost analysis, 384
    - value analysis, 384t–385t
  - Electric motor failure
    - data, 51–52
    - histogram, 42, 43f
  - Electric system modeling, 377–379, 378f
  - Electrical current, 96
  - Electrical subsystem, 372
  - Electrical system, 170, 170f, 171t
  - Electrochemical process, 96
  - Electromigration, 96
  - Electronic failure reports, 4
  - Emergency plan, 561
  - Emergency shutdown valve (ESDV), 641
    - NHEP values, 551t
    - PSF values, 549t
    - shutdown case study, 545–546
    - SPAH-R, 550–551
    - SPAR-H, 547–550
  - Energy system shutdown, 161
  - Engineering function, 720
  - EOM. *See* Error omission (EOM)
  - Equipment
    - configuration, 222
    - description, 222
    - failure rate, 15–16
    - function, 222
    - reliability
      - index, 347f, 366f
      - performance, 186–187
  - Error commission (ECOM), 486
  - Error omission (EOM), 486
  - Error-producing conditions, 495, 496t–497t, 525t
  - ESDV. *See* Emergency shutdown valve (ESDV)
  - ESRA. *See* European Safety and Reliability Association (ESRA)
  - ESReDA. *See* European Safety and Reliability and Data Association (ESReDA)
  - ESREL. *See* European Safety and Reliability (ESREL)
  - ETA. *See* Event tree analysis (ETA)
  - European Reliability Data Association (EURData), 694
  - European Safety and Reliability (ESREL), 695
  - European Safety and Reliability and Data Association (ESReDA), 693–695
  - European Safety and Reliability Association (ESRA), 693, 695
  - Event criticality index (EC index), 301, 345, 346f, 363, 365f
  - Event tree analysis (ETA), 562, 584. *See also* Fault tree analysis (FTA)
    - event tree, 585f
    - hybrid risk analysis, 586f
    - static event tree, 585f
    - time-dependent, 587–589
    - time-independent, 585–587
  - Expected number of failures, 299
  - Exponential model, 148. *See also* Linear model; Phase exponential model
    - vessel corrosion
      - failure time prediction, 150t
      - PDF, 151f
    - vessel degradation
      - prediction, 150f
      - over time, 149t

- Exponential PDF, 13, 17–20, 18f
  - failure rate, 19f
  - gas compressor and component failure rates, 20f
- Exponential reliability function, 18
- Extreme weather, 740–741
  - bow tie, 741f
- Eyring life–stress model, 101–102
- F**
- Failure
  - data reports, 3, 5f
  - on demand, 161
  - intensity parameters, 126
  - rank index, 300–301, 301f
- Failure and repair data analysis
  - compressor's optimum replacement time, 416
  - furnace failure and repair PDF parameters, 417f
  - distillation plant study case, 335
  - fan PDF, 336f
  - quantitative failure and repair data, 336t
- RAM + L analysis, 428
  - failures and repair data, 428t
- refinery hydrotreating unit, 349
  - qualitative failure and repair data, 349t
- refinery plant availability optimization, 359
  - exchanger PDF, 360f
  - quantitative failure and repair data, 360t
- thermal cracking plant ram analysis, 385–386
  - furnace failure and repair PDF parameters, 386f
- Failure mode, 3, 4f, 222
  - analysis, 167–174
    - diethylamine treatment system, 172–174, 174f
    - electrical system, 170, 170f, 171t
    - load movement system, 172, 172f, 173t, 175t
    - water supply system, 167–170, 168f, 169t
  - causes, 222
- Failure mode, effects, and criticality analysis (FMECA), 161, 163
- Failure mode and effects analysis (FMEA), 160–179, 221–267, 221f, 272, 562
  - criticality analysis, 174–179
  - DFMEA, 163–167
  - effective FMEA process, 162f
  - failure mode analysis, 167–174
- Failure mode event analysis. *See* Failure mode and effects analysis (FMEA)
- Failure rate, 16, 18–19, 19f, 113–114
  - function, 114–115
  - analysis, 15–16
  - as performance index, 676–679
- Failure report analysis and corrective action system analysis (FRACAS analysis), 207–219
  - critical failure modes, 214f
  - critical root causes, 215f
  - data monitoring, 208f
  - failure report analysis, 210t
  - fault tree analysis applied to root cause analysis, 211f
  - 5 WHY test, 212f
  - pump critical component failure, 214f
  - warranty analysis, 212–219
- Fatigue tests, 97
- Fault tree analysis (FTA), 562, 572. *See also* Event tree analysis (ETA)
  - case application, 646
  - fault tree, 582f–583f
    - RBD, 574f, 576f
  - furnace explosion, 578f
  - integrated approach, 641
    - bow tie case study application, 645–646
    - human reliability, 642–644
    - hybrid method case application, 646–648
    - hybrid risk analysis, 648
    - sensitivity analysis, 647
  - preliminary risk analysis, 581f
  - as qualitative risk analysis support, 580–583
  - as root cause analysis tool, 583–584
  - static, 573
  - time-dependent, 577–580
  - time-independent, 573–577
- Fault tree RBD, 574f, 576f
- FCC. *See* Fluid catalytic cracking (FCC)
- Feed subsystem, 387, 387f
- Fisher matrix, 61–62
- “5Why Test”, 209, 212f
- Floating liquefied natural gas (FLNG), 461
- Floating production, storage and offloading units (FPSO units), 460–461
- Floating production systems (FPSs), 460–461
- Floating storage and offloading system (FSO system), 461
- Floating storage unit (FSU), 461
- Flowline FMEA/RBI, 248–267, 261t, 262f, 263t–266t
- Fluid catalytic cracking (FCC), 416
- FMEA. *See* Failure mode and effects analysis (FMEA)
- FMECA. *See* Failure mode, effects, and criticality analysis (FMECA)
- F–N curve, 557
- FPSO units. *See* Floating production, storage and offloading units (FPSO units)
- FPSs. *See* Floating production systems (FPSs)
- FRACAS analysis. *See* Failure report analysis and corrective action system analysis (FRACAS analysis)
- Fractioning plant (U-20), 435–436, 436f

Fractioning subsystem, 388, 389f  
 Frequency, 52, 223  
 Frequency target methodology, 606  
 FSO system. *See* Floating storage and offloading system (FSO system)  
 FSU. *See* Floating storage unit (FSU)  
 FTA. *See* Fault tree analysis (FTA)  
 Furnace explosion, 577  
   FTA, 578f  
 Furnace lifetime data analysis cases, 87–91, 89t, 90f

## G

Gamma PDF, 35–37  
   with different shape, 35f  
   energy shutdown in compressor, 37f  
   failure rate  $\times$  time, 36f  
 General critical equipment assessment methodology, 177–179  
 General loglinear (GLL), 97  
   life–stress model, 110–113  
     reliability  $\times$  temperature  $\times$  voltage, 115f  
     sensor reliability curve under operational conditions, 114f  
     time to failures in accelerated test, 113t  
 General Renewal Model (GRM), 445, 449–450, 450f, 453  
 Generalized gamma PDF, 37–39  
   turbine blade damage failure rate function, 40f  
   turbine blade damage PDF, 38f  
 Generic error probability (GEP), 495  
 Generic operational cost function over time, 204–205  
 Generic PDFs, 42  
 GEP. *See* Generic error probability (GEP)  
 GLL. *See* General loglinear (GLL)  
 Gompertz model, 133–136. *See also* Lloyd–Lipow model  
   pump bearing improvement test result, 134t  
   reliability time stages, 135f  
 “Good as new” assumption, 9  
 Goodness of fit methods, 41–58  
   chi square method, 52–54  
   Cramer–von Mises tests, 57–58  
   K–S method, 54–56, 55f, 56t  
   maximum likelihood methods, 50–52  
   plot method, 42–47  
   rank regression, 47–50  
 GRM. *See* General Renewal Model (GRM)  
 Gumbel PDF, 13, 25, 29–31, 538  
   furnace corrosion failure rate  $\times$  time, 31f  
   furnace external corrosion Gumbel PDF, 30f  
 Gumbel reliability function, 30

## H

HALT. *See* Highly accelerated life test (HALT)  
 HASS. *See* Highly accelerated stress screening test (HASS)

Hazard, 564–565  
   matrix methodology, 600–603  
 Hazard and operability analysis (HAZOP analysis), 223,  
   567–572, 581–583, 582f  
   Coke plant HAZOP example, 570f  
   flexible riser HAZID example, 571f  
   guide words, 569t  
   steps, 569f  
 Hazard identification (HAZID), 223, 562  
 Hazard operability study (HAZOP), 562  
 HAZID. *See* Hazard identification (HAZID)  
 HAZOP. *See* Hazard operability study (HAZOP)  
 HAZOP analysis. *See* Hazard and operability analysis (HAZOP analysis)  
 HD. *See* High dependence (HD)  
 HDS  
   first-stage optimization, 355–356  
   second-stage optimization, 356–357  
 HDT optimization, 357  
 Health, safety, environment, and quality (HSEQ),  
   691–692  
 Health and Safety Executive (HSE), 719  
 HEART. *See* Human Error Assessment Reduction Technique (HEART)  
 Heat exchanger lifetime data analysis cases, 80–83, 84t,  
   85f–86f  
 Heating, 338, 339f  
 HEP. *See* Human error probability (HEP)  
 Hierarchical task analysis (HTA), 512–513  
 High accelerated test. *See* Highly accelerated life test (HALT)  
 High dependence (HD), 491  
 High voltage, 96  
 High-frequency detection, 185  
 High-performance system, 416–427  
 Higher vibration, 96  
 Highly accelerated life test (HALT), 79–80, 94, 119,  
   682–683  
 Highly accelerated stress screening test (HASS), 119  
 Historical data, 2–3  
 Hot water  
   boiler subsystem, 457f  
   distribution subsystem, 458f  
 HRA integrated approach, 641  
   bow tie case study application, 645–646  
   FTA case application, 646  
   human reliability, 642–644  
   hybrid method case application, 646–648  
   hybrid risk analysis, 648  
   sensitivity analysis, 647  
 HSE. *See* Health and Safety Executive (HSE)  
 HSEQ. *See* Health, safety, environment, and quality (HSEQ)  
 HTA. *See* Hierarchical task analysis (HTA)

- Human error, 473–474, 680  
 assessment during commissioning phase, 540  
 effect on platform system operational availability, 540–545  
 identification, 513  
 impact on platform operational availability, 540–545  
   human error, 545  
   human error block diagram simulation, 543f  
   NHEP values, 542t  
   platform system diagram block, 544f  
   PSF values, 541t  
   relative downtime loss, 545f  
 influence factors in, 475f  
 probability, 478f
- Human Error Assessment Reduction Technique (HEART), 495–500  
 case study application, 525–527  
 error-producing conditions, 496t–497t  
 generic tasks and nominal human unreliability, 496t  
 human error probability, 499t, 501t
- Human error probability (HEP), 473–474, 495, 508, 518, 737
- Human factors, 723  
 in reliability analysis, 680–681
- Human performance factor, 476, 502, 504, 510, 548
- Human reliability, 473–476, 642–644
- Human reliability analysis, 472–476, 668. *See also*  
 Reliability growth analysis (RGA)
- ASEP, 485–495
- Bayesian network, 514–519  
 case study, 519–520  
   Bayesian network application, 535–537  
   error-producing conditions, 525t  
   HEART case study application, 525–527  
   human error probability results, 539  
   methodologies comparison, 538  
   OAT case study application, 521–522  
   SLIM-MAUD case study application, 532–534  
   SPAR-H case study application, 523–525  
   STahr case study application, 527–532  
   THERP case study application, 520–521
- ESDV, 545–551
- first-generation methods, 476t
- HEART, 495–500
- human error impact on platform operational availability, 540–545
- OAT, 482–485
- second generation of human reliability methods, 473
- second-and third-generation methods, 477t
- SHERPA, 512–514
- SLIM-MAUD, 510–512
- SPAR-H model, 504–510
- STahr method, 500–504
- THERP, 476–482
- Human resources and competence, 720
- Humidity, 96
- Hybrid method case application, 646–648
- Hybrid risk analysis, 648
- Hydrodesulfurization process, 350
- Hypothesis null test, 53
- I**
- IEEE. *See* Institute of Electrical and Electronics Engineers (IEEE)
- ILS. *See* Integrated logistic support (ILS)
- Improvement allocation based on availability, 324–328
- Independent duration, 95
- Independent project analysis (IPA), 667–668
- Independent time LOPA, 591
- Indian Institute of Technology Kharagpur, 698–699
- Individual and societal risk methodology, 607–608
- Individual data, 3
- Individual risk, 558f  
 acceptable, 599f–600f
- Information security, 4
- Infrared methods, 180–181
- Inherent availability, 273
- Initial failure rate, 142
- Inspection  
 based on reliability growth, 410–415, 414f, 415t  
 downtime, 299
- Inspection optimization (PIO), 332
- Institute of Electrical and Electronics Engineers (IEEE), 472
- Insulator, 96
- Integrated asset integrity management, 738–742
- Integrated logistic support (ILS), 723–727  
 during design phase, 750–754  
 information flow, 724f  
 input information, 726f  
 for system asset performance optimization, 727f
- Intensification, 560
- Intensity failure, 142
- Intentional error, 474
- Interdiffusion, 96
- Internal business process, 704
- Interval data, 6, 7f
- Inverse power law life–stress model, 103–104  
 bearing reliability  $\times$  time under operational conditions, 105f  
 bearing reliability curve under different rotation conditions, 106f  
 time to failures in accelerated test, 104t
- IPA. *See* Independent project analysis (IPA)
- ISO 55000, 709  
 element relationship, 710f
- ISO–risk curve, 555, 557f, 599

**K**

Karlsruhe Institute of Technology (KIT), 696–698  
 Key performance index (KPI), 705  
   for top-level system, 713  
 Kijima factor, 87  
 Kijima I and II model, 313–317, 410, 449  
 KIT. *See* Karlsruhe Institute of Technology (KIT)  
 Kolmogorov–Smirnov method (K–S method), 54–56, 55f,  
   56t, 57f, 57t  
 KPI. *See* Key performance index (KPI)  
 K–S method. *See* Kolmogorov–Smirnov method (K–S  
   method)

**L**

Laboratories modeling, 379–383, 382f  
 Laplace test, 9–10  
 Layers of protection analysis (LOPA), 562, 590  
   to deciding risk, 622–628  
   furnace, 593f  
     explosive atmosphere formation, 593f  
   high pressure CDF, 595f  
   independent time, 591  
   layers of protection, 590f, 592f  
   relief valve PDF, 595f  
   time-dependent, 591–594  
     as qualitative risk analysis support, 594–596  
 LCC. *See* Life cycle cost (LCC)  
 LCP. *See* Life cycle performance (LCP)  
 LDA. *See* Lifetime data analysis (LDA)  
 Leadership, 720  
   aspect evaluation, 759t–760t  
   leaders, 673–674, 687–689  
 Level of repair (LORO), 332  
 Life cycle cost (LCC), 679, 706–707  
   as part of reliability engineering analysis, 685–686  
 Life cycle performance (LCP), 697–698, 698f, 712  
 Life cycle profit approach. *See* Life cycle performance (LCP)  
 Lifetime data analysis (LDA), 64–91, 65f, 207, 328,  
   450–453, 452f, 461–462, 713  
   bearing failure rate function, 71f  
   bearing reliability function, 70f  
   furnace lifetime data analysis cases, 87–91  
   goodness of fit methods, 41–58  
   heat exchanger lifetime data analysis cases, 80–83  
   joint failure  
     PDF, 90f  
     rate function, 92f  
   joint reliability function, 91f  
   PDF, 11–41  
   pipeline lifetime data analysis cases, 83–87  
   pump bearing lifetime data analysis, 69f  
   pump failure historical data, 66t, 68t, 69f

  pump lifetime data analysis, 64–67  
   pump seal lifetime data analysis, 70f  
   quantitative failure data analysis, 2–11  
   reliability, 59–63  
   safety instrumented function, 81t  
   screw compressor lifetime data analysis case, 67–71  
   sensor lifetime data analysis case, 76–80  
   valve lifetime data analysis case, 75–76  
 Light SESA, 372  
 Likelihood assessment, 222  
 Linear model, 145–147. *See also* Exponential model  
   tank pitting degradation over time, 146t  
   tank pitting thickness degradation, 147f  
     prediction, 147t  
   tank pitting thickness failure PDF, 148f  
 Liquefied natural gas (LNG), 461  
 Liquefied petroleum gas (LPG), 487  
 Lloyd–Lipow model, 131–132. *See also* Gompertz model  
   pump bearing improvement test result, 132t  
   reliability  $\times$  time stages, 133f  
 LNG. *See* Liquefied natural gas (LNG)  
 Load movement system, 172, 172f, 173t, 175t  
 Logarithmic model, 151–156  
   heat exchanger erosion degradation over time, 154t  
   heat exchanger tube erosion  
     prediction, 155t  
     PDF, 156f  
     thickness, 155f  
 Logistic(s), 320–324. *See also* Maintenance policies;  
   Redundancy policies; Renovation process; Stock  
   policy  
   energy supply  $\times$  cogeneration supply, 321f  
   model, 136–137  
   pump shafts improvement test result, 137t  
   reliability  $\times$  time stages, 138f  
 PDF, 13, 23–24  
   pump seal failure rate, 24f  
   pump seal leakage, 23f  
 RBD, 322f–324f  
   resources, 436–438  
   outside U-12 impacts, 438f  
   tank feed distillation plants, 437f  
   time, 214  
 Loglogistic PDF, 27–29  
   furnace corrosion failure rate  $\times$  time, 29f  
   furnace corrosion loglogistic PDF, 28f  
 Loglogistic reliability function, 28  
 Lognormal PDF, 25–27  
   furnace corrosion failure rate  $\times$  time, 27f  
   furnace corrosion lognormal PDF, 26f  
   valve repair time PDF, 26f  
 Lognormal reliability function, 25



LOPA. *See* Layers of protection analysis (LOPA)

LORO. *See* Level of repair (LORO)

Loss of containment, 738–740  
bow tie, 740f

LPG. *See* Liquefied petroleum gas (LPG)

## M

Maintainability, 445

Maintainability, Availability, Reliability, and Operability Simulator (MAROS), 344, 439

Maintenance

cost, 205, 223

strategy, 179–188, 179f

task, 223

Maintenance policies, 309–313. *See also* Logistic(s);

Redundancy policies; Renovation process; Stock policy

air cooler preventive maintenance RBD, 313f–314f

reliability not recovered by preventive maintenance, 311f

reliability recovered by preventive maintenance, 310f

Maintenance requirements (MR), 483

Major Hazard Incident Data Analysis Service (MHIDAS), 473

Malcolm Baldrige National Quality Award, 728–729

Markov chain methodology, 288–291, 290f

MAROS. *See* Maintainability, Availability, Reliability, and Operability Simulator (MAROS)

Mathematic life–stress models, 97

Maximum discrepancy, 54

Maximum likelihood estimation (MLE), 50–52

MC simulations. *See* Monte Carlo simulations (MC simulations)

MC2. *See* Control meshes (MC2)

Mean, 23

Mean availability, 299

Mean availability standard deviation, 299

Mean availability with inspection, 299

Mean time before failure. *See* Mean time between failure (MTBF)

Mean time between failure (MTBF), 16, 123, 217, 311  
as performance index, 676–679

Mean time to failure (MTTF), 2, 16, 98, 217, 219f, 348, 355, 357

Mean time to first failure (MTTFF), 299

Mean time to repair (MTTR), 349, 355, 357

Median rank equation, 42

Merox subsystem, 344, 344f

Method comparison and assessment of RAM analysis, 445–460

MHIDAS. *See* Major Hazard Incident Data Analysis Service (MHIDAS)

MIL-P-1629 procedure, 160

Minimum availability target, 349–350

Mixed Weibull probability density function, 33, 34f

MLE. *See* Maximum likelihood estimation (MLE)

Modeling, 277–280, 283

block availability, 281f

CENPES II project reliability analysis, 375–379, 376f

cold water subsystem modeling, 379, 381f

electric, 377–379, 378f

laboratories modeling, 379–383, 382f

simulation results, 377t

water cooling subsystem modeling, 379, 380f

compressor's optimum replacement time, 416–420

cleaning, 420, 420f

cold area, 419, 419f

conversion, 418, 418f

DEA subsystem, 419–420, 420f

fluid catalytic cracking system RBD, 418f

warming subsystem, 416–418, 418f

design phase, RAM analysis during, 462–464

flare system, 464f

instrument air, 464f

medium heating, 464f

recompression train, 463f

separation train, 463f

water treatment, 464f

distillation plant study case, 335–344

drill facility system, 404–406, 404f

availability rank, 406t

availability rank index, 406t

reliability importance index, 405f, 407f

Markov chain methodology, 288–291, 290f

RAM + L analysis, 429

acid gas treatment plant, 432, 432f

acid water treatment plant, 433–434, 434f

atmospheric and vacuum distillation plant, 429–430, 430f

atmospheric distillation plant, 429, 429f

catalytic cracking plant, 434, 435f

DEA plant RBD, 433f

diesel hydrodesulfurization plant, 430–431, 431f

fractioning plant, 435–436, 436f

Naphtha hydrodesulfurization plant, 432, 432f

reforming catalytic cracking plant, 435, 435f

thermal catalytic cracking plant, 430, 431f

RBD, 283–288

refinery hydrotreating unit, 350–351

reliability block, 351f

refinery plant availability optimization, 359–362

deethanizer, 361–362, 362f

depropanizer, 361, 361f

propane subsystem RBD, 361f

reliability and availability performance index, 299–305

system block diagram, 278f



- thermal cracking plant ram analysis, 386–391
    - compression subsystem, 388, 390f
    - feed and preheating subsystem, 387, 387f
    - fractioning subsystem, 388, 389f
    - stabilization, 391, 391f
    - thermal cracking subsystem, 387f–388f, 388
  - Monitoring methods, 180
  - Monte Carlo simulations (MC simulations), 280, 352, 399, 453
    - in RAM analysis, 399–400
  - Most likely time (MP), 349, 375
  - MP. *See* Most likely time (MP)
  - MR. *See* Maintenance requirements (MR)
  - MTBF. *See* Mean time between failure (MTBF)
  - MTTF. *See* Mean time to failure (MTTF)
  - MTTFF. *See* Mean time to first failure (MTTFF)
  - MTTR. *See* Mean time to repair (MTTR)
- N**
- Naphtha hydrodesulfurization plant (U-12), 432, 432f
  - Natural gas subsystem, 372–373
  - NDT. *See* Nondestructive test (NDT)
  - Negative correlation, 49
  - NHEP. *See* Nominal human error probability (NHEP)
  - Nominal group technique, 7, 473
  - Nominal human error probability (NHEP), 738
  - Nondestructive test (NDT), 180, 736
  - Nonhomogeneous Poisson process, 410
  - Nonlinear model transformation, 327
  - Nonlinear optimization methodology model, 359–372
  - Nonproportional hazard model, 116
  - Nonrepairable equipment availability, 283
  - Normal PDF, 13, 20–22
    - pump seal leakage, 21f
    - seal pump failure rate, 22f
  - Normal reliability function, 21
  - Norwegian University of Science and Technology (NTNU), 695
  - Null hypothesis, 54, 56, 58
- O**
- OAT. *See* Operator action tree (OAT)
  - OC1. *See* Optimum condition 1 (OC1)
  - Occult failure, 161
  - Occupancy category, 604–605
  - Offline monitoring, 185, 187f
  - Offshore case study, 754–766
  - Offshore Reliability Data Handbook (OREDA Handbook), 373–374, 696
  - Oil and gas industry, 473, 705
    - reliability pitfalls for, 674
      - account qualitative methods, 684
      - ALT, HALT, and RGA, 682–683
      - BOP configurations, 684f
      - exponential PDF for equipment and components, 674–676
      - human factor in reliability analysis, 680–681
      - life cycle cost, 685–686
      - using MTBF and failure rate as performance index, 676–679
    - operation condition effects on reliability prediction, 681
    - preventive maintenance effect, 679–680
    - redundancy to increasing system operational availability, 683–684
    - reliability engineering as part of asset management, 686–687
  - Oil lubricant analysis, 185
  - Omission error, 474
    - probability, 643
  - Operate to failure approach (OTF approach), 187–188
  - Operation(al)
    - aspect evaluation, 763t–764t
    - asset integrity management, 721
    - availability, 273, 401
    - cost function, 205
    - effects in availability, 385–398
    - excellence, 722f
    - integrity management, 722f
  - Operator action tree (OAT), 482–485, 522f
    - case study application, 521–522
    - tube and shell maintenance, 483f
  - Optimistic time (O), 349, 375
  - Optimization, 351–357
    - availability of subsystems, 352t
    - CENPES II project reliability analysis, 379–383
    - equipment optimization proposal, 358t
    - HDS first-stage optimization, 355–356
    - HDS second-stage optimization, 356–357
    - refinery hydrotreating unit, 349–357
      - availability of subsystems, 352t
      - HDS first-stage optimization, 355–356
      - HDS second-stage optimization, 356–357
      - selective hydrogenation section optimization, 353–354
    - refinery plant availability optimization, 365–371
      - EC, 363, 365f
      - equipment RI, 366f
      - RI, 363, 364f
      - selective hydrogenation section optimization, 353–354
  - Optimum condition 1 (OC1), 486, 489
  - Optimum condition 2 (OC2), 486, 489
  - Optimum condition 3 (OC3), 486, 489
  - Optimum condition 4 (OC4), 486, 489
  - Optimum replacement time (ORT), 179, 713
    - analysis, 203–207, 206f, 206t
  - OREDA Handbook. *See* Offshore Reliability Data Handbook (OREDA Handbook)
  - Organizational fast food culture, 689–690

Organizational framework, 670–671  
 ORT. *See* Optimum replacement time (ORT)  
 OTF approach. *See* Operate to failure approach (OTF approach)

## P

- P*(HE). *See* Human error probability (HEP)  
 Partial availability, 399–403  
   based on system age, 399–416  
   drawwork, 402f  
   general renovation process, 409–410  
     pump operation, 411f–412f  
   inspection based on reliability growth, 410–415, 414f, 415t  
   modeling and simulation, 404–406  
     availability rank, 406t  
     availability rank index, 406t  
     drill facility subsystem, 404f  
     reliability importance index, 405f, 407f  
 PDF parameters discounted time, 400f  
 stock policy, 406–409  
   optimum stock policy, 408t–409t  
 timeline, 403f  
 PAS 55, 706–709  
   items related to ISO standards, 708f  
 Passive redundancies, 306  
 PC test. *See* Post-calibration test (PC test)  
 PDA. *See* Probabilistic degradation analysis (PDA)  
 PDF. *See* Probability density function (PDF)  
 PdM. *See* Predictive maintenance (PdM)  
 Penetrant liquid test, 184, 184f  
 Percentage failure index, 395f  
 Percentage losses index, 299–300, 300f  
 Performance  
   aspect evaluation, 765t  
   evaluation, 709–710  
   index using MTBF and failure rate as, 676–679  
   optimization, 328–332  
     asset, 329f  
     equipment, 330f  
     fan component parts, 333f  
     fan preventive maintenance, 333f  
     system asset, 331f  
 Performance-shaping factors (PSFs), 473  
   workplace environment, 478  
 Permanent regime availability, 273  
 Pessimistic time (P), 349, 375  
 PFD. *See* Probability of failure on demand (PFD)  
 PFMEA. *See* Process failure mode and effects analysis (PFMEA)  
 PHA. *See* Preliminary hazard analysis (PHA)  
 Phase, 222  
   analysis, 185  
   Phase exponential model, 156–158. *See also* Exponential model  
     tank corrosion thickness, 157f  
     tank floor corrosion  
       failure prediction, 157t  
       PDF, 158f  
 Physical assets, 711  
 PIO. *See* Inspection optimization (PIO)  
 Pipeline disruption, 612  
 Pipeline FMEA/RBI, 233, 239t–240t  
   pipeline equipment FMEA function, 238t  
   pipeline equipment list hierarchy, 238f  
 Pipeline lifetime data analysis cases, 83–87, 86t–87t, 88f  
 Planning aspect evaluation, 760t–761t  
 Planning strategy, 162  
 Platform applicability, 461  
 Platform operational availability, human error impact on  
   human error, 545  
     assessment during commissioning phase, 540  
     block diagram simulation, 543f  
     effect on platform system operational availability, 540–545  
   NHEP values, 542t  
   platform system diagram block, 544f  
   PSF values, 541t  
   relative downtime loss, 545f  
 PLL. *See* Probable loss of life (PLL)  
 Plot method, 42–47  
   cumulative probability of failure, 44f  
   electric motor failure histogram, 42, 43f  
   plotted exponential CFD and parameter, 46f  
   plotted Weibull  
     2P CFD and parameters, 45f  
     3P CFD and parameters, 44f  
 PM. *See* Preventive maintenance (PM)  
 PM test. *See* Post-maintenance test (PM test)  
 PMO. *See* Preventive maintenance optimization (PMO)  
 Point availability, 299  
 Position parameter, 17, 20–21, 23, 25, 27–30, 32, 43–44  
 Positive correlation, 49  
 Post-accident analysis methodology, 491–495  
   diagnosis of human error probability, 493t  
 Post-accident tasks, 485  
 Post-calibration test (PC test), 486  
 Post-maintenance test (PM test), 486  
 Posteriori knowledge, 8–9  
 Potential failure phase, 180  
 Potential reliability growth, 139  
 Potential–functional interval, 180, 180f  
 Power model, 150–151  
   law model, 141–143, 144f

- turbine blade crack
    - degradation over time, 152t
    - PDF, 153f
    - prediction, 153f, 153t
  - Pre-accident analysis methodology, 485–491
  - Pre-accident tasks, 485
  - Predictive maintenance (PdM), 180
    - methods, 145
  - Prefractioning subsystem, 338, 340f
  - Preheating, 337, 337f
    - subsystem, 387, 387f
  - Preliminary hazard analysis (PHA), 223, 562, 564–566, 568f
    - to naphtha feed to hydrogen generation plant, 566f
    - platform production, 567f
  - Pressure swing absorption (PSA), 438
  - Preventive maintenance (PM), 179–180, 186–187, 299, 718, 721, 737, 751
    - downtime, 299
    - effect, 679–680
      - on reliability, 680f
  - Preventive maintenance optimization (PMO), 332
  - Priority rank, 177
  - Probabilistic degradation analysis (PDA), 143–158. *See also* Reliability growth analysis (RGA)
    - exponential model, 148
    - linear model, 145–147
    - logarithmic model, 151–156
    - phase exponential model, 156–158
    - power model, 150–151
  - Probability density function (PDF), 2–3, 11–41, 14f, 97, 179, 275, 450, 557, 676f
    - cumulative density function, 14f–15f
      - and equipment, 12f
      - exchanger, 360f
    - exponential, 17–20, 18f, 289
    - furnace, 6f, 275f
    - gamma, 35–37
    - generalized gamma, 37–39
    - Gumbel, 29–31
    - logistic, 23–24
    - loglogistic, 27–29
    - lognormal, 25–27
    - normal, 20–22
    - oil and gas equipment, 451f
    - parameters discounted time, 400f
    - pressure swing adsorption system valve actuator, 12f
    - Rayleigh, 39–41
    - Weibull, 31–34
      - wrong vs. correct approach, 11f
  - Probability of failure, 194
  - Probability of failure on demand (PFD), 608, 609f
  - Probable loss of life (PLL), 604
  - Process failure mode and effects analysis (PFMEA), 167
  - Programmed maintenance, 180
  - Proportional hazard model, 113–116
    - failure × temperature, 116t
    - failure rate under operational conditions, 117f
  - Proposal DP method, 331
  - PSA. *See* Pressure swing absorption (PSA)
  - PSFs. *See* Performance-shaping factors (PSFs)
  - Pump lifetime data analysis, 64–67
  - Punctual availability, 272
- ## Q
- Qualitative accelerated test, 119–122
    - life test, 94
      - stress limits, 121f
    - temperature × vibration × time, 121f
    - temperature chamber, 122f
  - Qualitative reliability approaches, 561
  - Qualitative risk analysis support
    - FTA as, 580–583
      - time-dependent LOPA as, 594–596
  - Quantitative accelerated test, 94–118
    - Arrhenius life–stress model, 97–101
    - cumulative risk model, 116–118
    - Eyring life–stress model, 101–102
    - GLL life–stress model, 110–113
    - inverse power law life–stress model, 103–104
    - life test, 94
      - proportional hazard model, 113–116
      - T–H life–stress model, 104–107
      - T–NT life–stress model, 109–110
  - Quantitative approach, 608–611
  - Quantitative failure data analysis, 2–11
  - Quantitative reliability approaches, 561
- ## R
- Radiography method, 182, 183f
  - RAM + L analysis, 427, 428f
    - conclusions, 443–445
      - critical analysis and improvement actions, 441–442
        - macrosystem RBD configuration, 442f
        - system efficiency improvement, 442t
    - failure and repair data analysis, 428
      - failures and repair data, 428t
    - logistic resources, 436–438
      - outside U-12 impacts, 438f
      - tank feed distillation plants, 437f
    - simulation, 443
      - actual refinery, 443f–444f
      - system modeling, 429–436
      - system simulation, 439–441
        - system efficiency, 441t

- RAM analysis. *See* Reliability, availability, and maintainability analysis (RAM analysis)
- RAMS technology. *See* Reliability, availability, maintainability, and safety technology (RAMS technology)
- Random test, 96
- Rank regression, 47–50
  - to electric motor failure data, 48t, 50t
- Rayleigh CDF function, 39
- Rayleigh function, 39
- Rayleigh PDF, 39–41, 40f–41f
- RBD. *See* Reliability block diagram (RBD)
- RBD BQR software, 456
- RBI analysis. *See* Risk-based inspection analysis (RBI analysis)
- RCD. *See* Reliability-centered design (RCD)
- RCM. *See* Reliability-centered maintenance (RCM)
- RCM analysis. *See* Reliability centered maintenance analysis (RCM analysis)
- ReBI analysis. *See* Reliability-based inspection analysis (ReBI analysis)
- Recovery analysis, 513
- Recovery factor (RF), 486
- Redesign out maintenance (ROM), 187–188
- Redundancy policies, 306–309. *See also* Logistic(s); Maintenance policies; Renovation process; Stock policy
  - one standby pump for two operating pumps, 307f
  - reducing electrical energy redundancies, 308f
  - reducing hydrogen generation unit plant feed redundancy, 309f
- Redundancy to increasing system operational availability, 683–684
- Refinery case study, 427–445
- Refinery hydrotreating unit, 348
  - conclusions, 357–359
  - failure and repair data analysis, 349
    - qualitative failure and repair data, 349t
  - hydrodesulfurization process, 350
  - modeling, 350–351
    - reliability block, 351f
  - optimization, 349–350
    - equipment optimization proposal, 358t
    - of HDT, 357
  - simulation and optimization, 351–357
    - availability of subsystems, 352t
    - HDS first-stage optimization, 355–356
    - HDS second-stage optimization, 356–357
    - selective hydrogenation section optimization, 353–354
- Refinery plant availability optimization, 359
  - conclusion, 371–372
  - critical analysis, 363–365
  - failure and repair data analysis, 359
    - exchanger PDF, 360f
    - quantitative failure and repair data, 360t
  - modeling, 359–362
    - deethanizer, 361–362, 362f
    - depropanizer, 361, 361f
    - propane subsystem RBD, 361f
  - optimization, 365–371
    - EC, 363, 365f
    - equipment RI, 366f
    - RI, 363, 364f
    - simulation, 363
- Reforming catalytic cracking plant (U-22), 435, 435f
- ReGBI analysis. *See* Reliability growth-based inspection analysis (ReGBI analysis)
- Reliability, 13–15, 59–63, 159–160, 299, 445, 557
  - concept, 2
  - confident limits to reliability function, 63f
  - engineer teaching and research
    - Indian Institute of Technology Kharagpur, 698–699
    - KIT, 696–698
    - University of Stavanger, 699–700
    - University of Strathclyde Business School, 699
    - wbk organization, 697f
  - FMEA, 160–179
  - FRACAS analysis, 207–219
  - growth index, 131
  - human factor in reliability analysis, 680–681
  - logistic PDF, 23–24
  - ORT analysis, 204–207
  - performance index, 299–305
    - downtime event critical index, 301, 302f
    - failure rank index, 300–301, 301f
    - percentage losses index, 299–300, 300f
    - RI index, 303–304, 304f
    - utilization index, 305
  - programmed/schedule maintenance based on, 188f
  - RBI analysis, 193–198
  - RCM analysis, 189–193
  - ReBI analysis, 199–201
  - ReGBI analysis, 202–204
  - repair time confidence bounds, 61t
  - seal pump reliability, 60f
- Reliability, availability, and maintainability analysis (RAM analysis), 64, 130–131, 160, 176, 272–283, 632–641, 667–668, 675
  - applied to decommissioning phase, 445–460
  - CENPES II project reliability analysis, 372–385
  - conclusion and reports, 281–283
  - data failure and repair analysis, 275–277
    - maintenance activities steps on vessel, 277t
    - quantitative failure and repair data, 276t

- during design phase, 460–469
- high-performance system, 416–427
- improvement allocation based on availability, 324–328
- methodology steps, 274f
- modeling and simulation, 277–280, 283
  - block availability, 281f
  - Markov chain methodology, 288–291, 290f
  - RBD, 283–288
  - reliability and availability performance index, 299–305
  - simulation, 291–299, 297f
  - system block diagram, 278f
- nonlinear optimization methodology model, 359–372
- operational effects in availability, 385–398
- partial availability based on system age, 399–416
- performance optimization, 328–332
- RAM + L analysis, 427–445
  - and risk assessment, 640
  - scope definition, 274
- sensitivity analysis, 280–281, 305
  - in critical equipment, 334–348
    - general renovation process, 313–317
    - logistics, 320–324
    - maintenance policies, 309–313
    - redundancy policies, 306–309
    - stock policy, 318–319
- systems availability enhancement methodology, 348–359
- Reliability, availability, maintainability, and safety technology (RAMS technology), 629–630
  - FTA PDF parameters, 638t
  - methodology, 629–641
  - N-05 overload FTA, 635f
  - N-05 temperature loss control FTA, 638f
  - O-26 overload FTA, 636f, 640f
  - O-26 overpressure FTA, 636f
  - O-27 overload FTA, 637f
  - RBD, 638f–639f
  - safety processes, 630–632
    - effect, 633f
  - SIFs, 641
  - system RBD, 632f
- Reliability and safety processes
  - ALARP individual risk, 558f
  - bow tie analysis, 611–620
  - ETA, 584–589
  - FTA, 572–584
  - HAZOP analysis, 567–572
  - ISO–risk curve, 555, 557f
  - LOPA, 590–596
  - PHA, 564–566
  - risk analysis
    - and management, 554
    - cases studies, 621–662
    - methods, 561–563
  - risk communication, 561
  - risk management process, 559, 560f
  - risk matrix, 555f
  - severity category, 556t
  - SIL analysis, 596–611
  - societal risk, 557
- Reliability block diagram (RBD), 273–274, 277, 283–288, 324–325, 540–542, 573, 742
  - atmospheric distillation plant, 283f
  - data center utilities system, 285f
  - diethylamine system, 286f, 287–288
  - heat subsystem in distillation plant, 284f
  - in logistics, 322f–324f
- Reliability centered maintenance analysis (RCM analysis), 160, 189–193, 221–267, 223f
  - load movement, 191t
  - water supply, 190t
  - water system RCM, 192f
- Reliability engineering
  - over enterprise phases, 669f
  - implementation of barriers, 687
    - decisor's profile, 687–689, 688f
    - organizational fast food culture, 689–690
    - standard approach, 690–691
  - management support, 672f–673f
  - methods, 716
  - as part of asset management, 686–687
  - pitfalls, 674
    - account qualitative methods, 684
    - ALT, HALT, and RGA, 682–683
    - BOP configurations, 684f
    - exponential PDF for types of equipment and components, 674–676
    - human factor in reliability analysis, 680–681
    - life cycle cost, 685–686
    - using MTBF and failure rate as performance index, 676–679
  - operation condition effects on reliability prediction, 681
  - preventive maintenance effect, 679–680
  - redundancy to increasing system operational availability, 683–684
  - reliability engineering as part of asset management, 686–687
  - program, 674, 686–687, 689, 713
  - reliability engineer teaching and research, 696–700

- Reliability growth analysis (RGA), 79–80, 122–143, 410, 448–449, 454f, 682–683. *See also* Human reliability analysis
    - accumulated MTBF  $\times$  time, 125f
    - Crow extended model, 138–140
    - Crow–AMSAA model, 124–131
    - Duane model, 123–124
    - Gompertz model, 133–136
    - Lloyd–Lipow model, 131–132
    - logistic model, 136–137
    - methodology, 104
    - power law model, 141–143
  - Reliability growth-based inspection analysis (ReGBI analysis), 198, 202–204, 204f, 410
  - Reliability importance, 303–304, 304f, 393f–394f
  - Reliability index (RI), 2–3, 345, 346f, 363, 364f, 379, 637
    - equipment, 347f, 366f
  - Reliability management. *See also* Asset management; Human reliability analysis
    - over enterprise life cycle, 667–669
    - “industry competitors” power, 667
    - in oil and gas industry, 666
    - oil and gas industry five forces methodology, 666f
    - reliability pitfalls for oil and gas industry, 674–687
    - success factors, 669–674
    - successful cases, 691
      - asset maintenance processes, 693f
      - Bayer case, 691–693
      - ESRA, 695
      - ESReDA, 694–695
      - SINTEF, 695–696
      - USNRC, 693–694
  - Reliability prediction, operation condition effects on, 681
  - Reliability superior limit (RSL), 59–60
  - Reliability target achievement (RGA), 684
  - Reliability-based inspection analysis (ReBI analysis), 198–201, 200t–201t
  - Reliability-centered design (RCD), 692
  - Reliability-centered maintenance (RCM), 272
  - Renovation process, 313–317. *See also* Logistic(s); Maintenance policies; Redundancy policies; Stock policy
    - independent and identically distributed equipment failure pattern, 315f
    - partial availability, 409–410
      - pump operation, 411f–412f
    - pump operations
      - as-bad-as-old, 317f
      - as-good-as-new, 316f
  - Repair analysis, 275–277
    - maintenance activities steps on vessel, 277t
    - quantitative failure and repair data, 276t
  - Responsible, 223
  - Return on investment (ROI), 718
  - RF. *See* Recovery factor (RF)
  - RGA. *See* Reliability growth analysis (RGA); Reliability target achievement (RGA)
  - RGBI method. *See* Reliability growth-based inspection analysis (ReGBI analysis)
  - RI. *See* Reliability index (RI)
  - Risk
    - of failure, 194–195
      - graph methodology, 604–606, 605f–606f, 655–659
      - management, 721–722
      - matrix, 655, 657f
      - mitigation target, 651, 652f
  - Risk analysis, 221–222
    - case studies, 621
      - applying LOPA, 622–628
      - blowout accident analysis, 648–650
      - fire pump system FTA, 626f
      - fire pump system simulation, 627f
      - individual risk tolerable region, 625f
      - methodology to supporting plant shutdown decision, 623f, 626f
      - RAMS analysis methodology, 629–641
      - risk matrix, 624f
      - safety integrity level risk assessment, 650–662
      - shutdown emergency valve risk analysis, 641–648
    - and management, 554
    - methods, 561–563
      - risk analysis throughout asset phases, 563t
  - Risk assessment. *See also* Risk analysis
  - Risk priority number (RPN), 163
  - Risk-based inspection analysis (RBI analysis), 193–198, 221–267, 224f
    - diethylamine system RBI, 197f
    - evolution of inspection and maintenance plan strategies, 194f
    - frequency rank, 195f
    - risk matrix, 195f
    - severity rank, 196f
  - Risk-seeking dessert, 689
  - ROI. *See* Return on investment (ROI)
  - ROM. *See* Redesign out maintenance (ROM)
  - Root cause analysis, 208
    - FTA as tool, 583–584
  - RPN. *See* Risk priority number (RPN)
  - RSL. *See* Reliability superior limit (RSL)
- ## S
- Safety
    - culture, 720
    - dialogue, 560–561

- integrity function sensor, 76
- safety-critical systems, 720
- Safety instrumented function (SIF), 161, 563, 683
- Safety instrumented systems (SISs), 596, 597f
- Safety integrity level (SIL), 562–563, 596
  - acceptable individual risk, 599f–600f
  - classification, 598t
  - consequence categories, 602t
  - frequency categories, 603t
  - frequency target methodology, 606
  - hazard matrix methodology, 600–603
  - individual and societal risk methodology, 607–608
  - ISO–risk curve, 599
  - methodologies, 596–598
  - qualitative acceptable risk, 598f
  - quantitative approach, 608–611
  - risk assessment, 650
    - final LOPA calculation, 661f
    - frequency categories, 657t
    - HAZID, 653
    - layers of protection PFD, 653t
    - LOPA, 653–654
    - risk mitigation target, 651, 652f
    - separator vessel HAZID, 654f
    - separator vessel LOPA, 656f
    - SIF configuration, 660f
    - SIL selection, 654–659
    - SIL verification, 659–662, 660f
  - risk graph methodology, 604–606, 605f–606f
  - safety life cycle, 597f
  - SISs, 597f
  - variation over time, 609t
  - verification FTA, 610f
- Salt treatment, 337, 338f
- Scale parameters, 20–21, 23, 25, 27–30
- Scope definition, 274
- Screw compressor lifetime data analysis case, 67–71, 72t, 73f–76f
- SDT infrared detector, 180–181, 181f
- SDT ultrasound detector, 181, 182f
- Second generation of human reliability methods, 473
- Seismic effect, 612
- Selective hydrogenation section optimization, 353–354
- Sensitivity analysis, 280–281, 305, 647
  - compressor's optimum replacement time, 422–426
    - compressor A life cycle analysis, 426f
    - compressor A lifetime data analysis failure rate functions, 425f
  - optimum replacement time, 424f
  - optimum replacement time methodology, 424f
  - system phase diagram, 427f
- in critical equipment, 334–348
  - design phase, RAM analysis during, 465–468
    - asset performance after preventive maintenance, 468f, 468t
    - asset performance by year, 467t
  - distillation plant study case, 347–348
  - general renovation process, 313–317
  - logistics, 320–324
  - maintenance policies, 309–313
  - redundancy policies, 306–309
  - stock policy, 318–319
  - thermal cracking plant ram analysis, 397–398
    - optimum stock level, 397t
    - reducing standby pumps, 398f
- Sensor lifetime data analysis case, 76–80, 82f–83f
- Serially modeled systems and equipment, 375
- SFMEA. *See* System failure mode and effects analysis (SFMEA)
- Shape parameter, 31–33, 43–44
- SHERPA. *See* Systematic Human Error Reduction and Prediction Approach (SHERPA)
- Shutdown emergency valve risk analysis, 641
  - bow tie case study application, 645–646
  - FTA case application, 646
  - human reliability, 642–644
  - hybrid method case application, 646–648
  - hybrid risk analysis, 648
  - sensitivity analysis, 647
- SIF. *See* Safety instrumented function (SIF)
- SIL. *See* Safety integrity level (SIL)
- Simplification, 560
- Simulation, 277–280, 283, 291–299, 297f
  - block availability, 281f
  - case studies, 293–299
  - compressor's optimum replacement time, 421
  - design phase, RAM analysis during, 465
    - asset performance prediction, 465t
  - distillation plant study case, 344–345
  - drill facility system, 404–406, 404f
    - availability rank, 406t
      - availability rank index, 406t
      - reliability importance index, 405f, 407f
  - Markov chain methodology, 288–291, 290f
  - RAM + L analysis, 439–441, 443
    - actual refinery, 443f–444f
    - system efficiency, 441t
  - RBD, 283–288
  - refinery hydrotreating unit, 351–357
    - availability of subsystems, 352t
    - HDS first-stage optimization, 355–356
    - HDS second-stage optimization, 356–357
    - selective hydrogenation section optimization, 353–354
  - refinery plant availability optimization, 363
  - reliability and availability performance index, 299–305

- Simulation (*Continued*)
    - result, 298t
    - system block diagram, 278f
    - thermal cracking plant ram analysis, 392
  - Sine tests, 96
  - SINTEF. *See* Stiftelsen for Industriell og Teknisk Forskning (SINTEF)
  - SISs. *See* Safety instrumented systems (SISs)
  - SLI. *See* Success likelihood index (SLI)
  - SLIM-MAUD. *See* Success Likelihood Index Methodology-Multi-Attribute Utility Decomposition (SLIM-MAUD)
  - Smallest extreme value PDF. *See* Gumbel PDF
  - Societal risk, 557, 558f, 599
  - Sociotechnical Analysis of Human Reliability method (STahr method), 500–504
    - case study application, 527–532
    - procedure weights, 528t
    - supervision weights, 529t
    - training weights, 528t
    - turbine STahr, 530t–531t
    - human error probability, 503t
    - human reliability tree, 502f
    - procedure weight, 503t
    - training weight, 502t
  - SPAR-H model. *See* Standardized Plant Analysis Risk Retain Human Reliability model (SPAR-H model)
  - Spare parts, 223, 328, 332
    - cost, 223
  - Stabilization, 391, 391f
  - STahr method. *See* Sociotechnical Analysis of Human Reliability method (STahr method)
  - Standard approach, 690–691
  - Standardized Plant Analysis Risk Retain Human Reliability model (SPAR-H model), 504–510
    - case study application, 523–525
    - path diagram, 506f
    - PSF values, 505t
      - posteriori, 509t
      - priori, 507t
  - Static FTA, 573
  - Status, 223
  - Stiftelsen for Industriell og Teknisk Forskning (SINTEF), 693, 695–696
  - Stock policy, 318–319. *See also* Logistic(s); Maintenance policies; Redundancy policies; Renovation process
    - optimum stock level, 319t
    - turbine stock level, 320t
  - Stock policy, 406–409
    - optimum, 408t–409t
  - Strain-controlled cyclic loading, 97
  - Stress factor, 95
  - Stressors, 95, 96f
    - factor, 278–279
  - Subsea case study, 735–742, 750–754
  - Substitution, 560
  - Success likelihood index (SLI), 510
  - Success Likelihood Index Methodology-Multi-Attribute Utility Decomposition (SLIM-MAUD), 510–512
    - case study application, 532–534
    - score and weights, 511t
    - SLI values, 512t
  - Sulfur recovery plant case, 742–750
  - Support aspect evaluation, 762t
  - Supportability (Su), 726
  - Switch effect, 279–280
  - System availability, 351
  - System failure mode and effects analysis (SFMEA), 167
  - System operational availability, redundancy to increasing, 683–684
  - System optimal maintenance policy, 332
  - System reliability, 278
  - Systematic Human Error Reduction and Prediction Approach (SHERPA), 512–514, 516t
    - risk matrix, 514t
    - severity, 515t
    - tabulation, 516t
    - task classification, 513t
  - Systems availability enhancement methodology, 348–359
- ## T
- T statistic, 57–58
  - Tabulation, 513
    - SHERPA, 516t
  - Tank components (T1), 375
  - Tank FMEA/RBI, 233–238, 242t–244t
    - tank equipment FMEA function, 241t
    - tank equipment list hierarchy, 241f
  - Tank output valves (VS1), 375
  - Taro, 445
  - Technique for human error rate prediction (THERP), 476–482
    - case study application, 520–521
    - drilling phase tasks, 481f–482f
    - event tree, 480f
    - human error probability, 478f
    - tube and shell heat exchanger, 479f
  - Temperature–humidity stress model (T–H stress model), 97, 104–107
    - logic element PDF curve under temperature conditions, 108f
    - logic element reliability curve under operational conditions, 108f
    - time to failures in accelerated test, 107t
  - Test condition, 97
  - Test duration, 95



- Test qualitative analysis, 159–160
  - Test–fix–find test approach, 122–123
  - Test–fix–test approach, 122–123
  - T–H stress model. *See* Temperature–humidity stress model (T–H stress model)
  - Thermal catalytic cracking plant (U-211), 430, 431f
  - Thermal cracking plant RAM analysis, 385
    - conclusion, 398
    - critical analysis, 392–397
      - downtime event criticality index, 395f
      - percentage failure index, 395f
      - reliability importance, 393f–394f
      - system operating and system not operating, 396f
    - failure and repair data analysis, 385–386
      - furnace failure and repair PDF parameters, 386f
    - modeling, 386–391
      - compression subsystem, 388, 390f
      - feed and preheating subsystem, 387, 387f
      - fractioning subsystem, 388, 389f
      - stabilization, 391, 391f
      - thermal cracking subsystem, 387f–388f, 388
    - sensibility analysis, 397–398
      - optimum stock level, 397t
      - reducing standby pumps, 398f
    - simulation, 392
  - Thermal cracking subsystem, 387f–388f, 388
  - Thermal–nonthermal stress model (T–NT stress model), 97, 109–110
    - failure rate under temperature conditions, 112f
    - sensor reliability curve under operational conditions, 111f
    - time to failures in accelerated test, 110t
  - THERP. *See* Technique for human error rate prediction (THERP)
  - 3D reliability time rotation graph, 104
  - Throughput, 299
  - Time, 186–187
    - to failure, 10–11, 10t
  - Time-dependent
    - bow tie analysis, 616–620
    - ETA, 587–589, 625–627
    - FTA, 577–580
    - LOPA, 591–594
      - as qualitative risk analysis support, 594–596
  - Time-independent
    - bow tie analysis, 613–616
    - ETA, 585–587
    - FTA, 573–577
  - Timeline, 403f
  - T–NT stress model. *See* Thermal–nonthermal stress model (T–NT stress model)
  - Total cost, 223, 299
  - Total downtime, 299
  - Total number of failures, 299
  - Total repair time, 214, 349, 374
  - Turbine blade damage, 38
    - failure rate function, 40f
    - PDF, 38f
  - Turbine failures in interval data, 6, 7f
  - Turnout, 214
- ## U
- United States Nuclear Regulatory Commission (USNRC), 693–694
  - University of Stavanger, 699–700
  - University of Strathclyde Business School, 699
  - Unreported failures equipment life cycle, 4–6
  - Unsafe failure, 162
  - Uptime, 299
  - US Congress established the Atomic Energy Act (1946), 693
  - US Nuclear Regulatory Commission (USNRC), 472
  - Used oil analysis, 185
  - USNRC. *See* United States Nuclear Regulatory Commission (USNRC); US Nuclear Regulatory Commission (USNRC)
  - Utilization index, 305
- ## V
- Vacuum distillation subsystem, 342, 343f
  - Value improving practice (VIP), 667–668
  - Valve FMEA/RCM, 226, 236t–237t
    - equipment and component function, 235t
    - globe valve hierarchy, 235f
  - Valve lifetime data analysis case, 75–76, 77t, 78f–80f
  - Valve repair time PDF, 25, 26f
  - Vendor equipment performance, 208
  - Vibration
    - analysis, 185, 186f
    - monitoring, 185
    - tests, 96
  - VIP. *See* Value improving practice (VIP)
- ## W
- Warming subsystem, 416–418, 418f
  - Warranty analysis, 212–219
    - MTTF, 219f
    - real reliability  $\times$  target reliability, 215f, 217f
    - warranty  $\times$  time, 216f
    - warranty performance index, 218t
  - Water
    - cooling subsystem modeling, 379, 380f
    - supply system, 167–170, 168f, 169t
    - treatment subsystem, 342, 342f
    - water-cooling subsystem, 373

Wear debris monitoring techniques, 185  
Wear inline monitoring, 185, 187f  
Wear online monitoring, 185, 187f  
Wear particle analysis, 185  
Weibull 2P parameters, 45  
Weibull 3P parameters, 45, 47  
Weibull failure rate function, 33–34  
Weibull PDF, 13, 31–34  
    furnace burner damage, 32f  
    mixed Weibull probability density function, 33, 34f

Weibull reliability function, 33  
Work routine, 674  
Wrong versus correct approach PDF, 11f

## X

X-ray generator source, 182

## Z

Zero dependence (ZD), 491

Second Edition

# GAS and OIL RELIABILITY ENGINEERING

## Modeling and Analysis

Eduardo Calixto

Reliability engineering should be systematically applied in the oil and gas industry to support the assets to achieve and maintain high performance. *Gas and Oil Reliability Engineering: Modeling and Analysis, Second Edition*, provides the latest tactics and processes that can be used in oil and gas markets to improve reliability knowledge, reduce costs to stay competitive, and support decisions for achieving and maintaining high performance in plants' facilities and equipment. Updated with relevant analysis and case studies covering equipment for both onshore and offshore operations, this reference provides the engineer and manager with more information on lifetime data analysis (LDA), safety integrity levels (SILs), and asset management. New chapters on safety, more coverage on the latest software, quantitative and qualitative techniques such as ReBI (Reliability-Based Inspection), ReGBI (Reliability Growth-Based Inspection), RCM (Reliability Centered Maintenance), LDA (Lifetime Data Analysis), and asset integrity management make the book a critical resource that will arm engineers and managers with the basic reliability principles and standard concepts that are necessary to explain the need for reliability assurance in the oil and gas industry.

### Key Features

- Provides the latest tactics and processes that can be used in oil and gas markets to improve reliability knowledge and reduce costs
- Presents practical knowledge with over 20 new internationally based case studies covering blowout preventers, offshore platforms, pipelines, valves, and subsea equipment from various locations, such as Australia, the Middle East, and Asia
- Contains expanded explanations of reliability skills with a new chapter on asset integrity management, relevant software, and techniques training, such as THERP, ASEP, RBI, FMEA, and RAMS

### About the Author

**Eduardo Calixto** is currently a RAMS expert, performing different reliability engineering and safety engineering analyses for Philotech GmbH in Germany. Eduardo has over 15 years of experience working in reliability engineering and safety for the oil and gas, railway, and mining industries. Previously, he has worked with many companies internationally as a reliability engineer, such as Petrobras, Genesis Oil and Gas, and Reliasoft, along with collaborating on projects with multiple major oil operators such as Chevron, Shell, and Kuwait Oil Company. Eduardo received his BA in Industrial Engineering and his MSc in Safety Management, both from Federal Fluminense University in Brazil, and his DSc in Energy and Environmental Engineering from the Federal University of Rio de Janeiro.

### Related Titles

*Designing for Human Reliability* by Ron McLeod / 978-0-12-802421-8

*Process Risk and Reliability Management, Second Edition* by Ian Sutton / 978-0-12-801653-4

*Reliable Maintenance Planning, Estimating, and Scheduling* by Ralph Peters / 978-0-12-397042-8

Engineering



**Gulf Professional Publishing**  
An imprint of Elsevier  
elsevier.com

ISBN 978-0-12-805427-7



9 780128 054277