University of Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/ Specialization: **Industrial Asset Management**	Spring semester, 2020 ~~Open~~ / **Restricted access**
Author: **Anar Ahadov**	(Author's signature)

Faculty supervisor: **Idriss El-Thalji** (UiS)
External supervisor: **Martin Lauritzsen** (TechnipFMC Norway)
Program coordinator: **Jayantha P. Liyanage** (UiS)

Thesis title:

Requirements Elicitation for Barrier Monitoring System

Credits (ECTS): **30**

Key words: Requirements Elicitation Barrier Monitoring Subsea Industry Safety Integrity Level Production Master Valve (PMV) Production Wing Valve (PWV) Down-hole Safety Valve (DHSV)	Total Page Number: 141 Stavanger, July 10th,2020 Date/year

Requirements Elicitation for Barrier Monitoring System

by

Anar Ahadov

University of
Stavanger

In fullfillment of the requirements for the degree of
Master of Science (MSC).Industrial Asst Management
Department of Mechanical and Strucutural Engineering and Material Science
Faculty of Science and Technolgy
University of Stavanger

Stavanger,NO - July 2020

Abstract

The activities undertaken by operator companies in the Norwegian Continental Shelf pose a very high risk to human life and the environment. Leading causes of accidents are poor maintenance, inadequate risk assessment and failure of barrier safety valves. A combination of all the listed accident causes are investigated with a focus on barrier valves (PMV, PWV, DHSV). Despite the fact that PSA has defined regulations and recommended standards related to barriers managements, operators in the Norwegian continental shelf still fail to implement the regulatory requirements regarding safety barriers. This stems from challenges related to interpretation and uncertainty of barrier testing requirements.

Challenges related to interpreting barrier requirements arise from terminological inconsistencies or the use of non-standard syntax in documenting requirements. The purpose of this study was to illuminate the challenges encountered by operator companies in adhering to standards recommended by Petroleum Safety Authority of Norway. There will be a focus on clarity of testing requirements from standards, technical challenges which prevent standard adherence and technical capabilities of current condition monitoring systems.

To understand how these requirements and generate primary data, semi-structured interviews (with customers or via representative) were performed to get specific clarification and standard based requirements, customer-based requirements are analyzed and verified. Secondary data was also collected and analyzed from different case studies.

The requirements elicitation discovered that companies preferred to follow NORSOK D-10 as opposed to PSAN recommendation of NOG 070, since NOG 070 gives little weight to uncertainties during PFD calculation. Commonest failure modes cited during valve failure were mechanical failure due to leakage, general mechanical failure and corrosion. Findings also suggested that operator companies did not follow the maintenance procedure strictly. Also, condition monitoring systems provided by monitoring service providers did not could not detect certain failure modes that operators faced.

Keywords: Requirements Elicitation, Barrier Monitoring, Subsea Industry, Safety Barriers, Safety Integrity Level, Production Master Valve, Production Wing Valve, Down-hole Safety Valve.

Acknowledgements

I would like to express my gratitude to TechnipFMC for providing me with the opportunity of writing this thesis and contributing with the development of new technologies that will allow the company to be more competitive in these times of rapid growth in the subsea arena.

I would like to thank my company supervisor Martin Lauritzsen and Bent Helge Nystad for their continuous support during the past months. Also, to the engineering department in TechnipFMC Norway who provided me with valuable data for my research.

Last, but by no means least, I thank my academic supervisor Idriss El-Thalji for his support and great guidance. He nurtured my curiosity for subsea technology and provided me with knowledge in a very interesting way.

Contents

List of Tables

List of Figures

Acronyms

CM Condition Monitoring. 25

DD Dangerous Detected. 23

DU Dangerous Undetectable. 20

EPU Electric Power Unit. 37

ESD Emergency Shutdown. 3, 20

FMECA Failure Mode and Criticality Analysis. 59

FST Full Stroke Test. 21

HPU Hyrdaulic Power Unit. 37

HSE Health Safety Environment. 12

PFD Probability Failure on Demand. 21

PMV Production Master Valve. 19

PST Partial Stroke Test. 21

PWV Production Wing Valve. 19

ROV Remotely Operated Vechicle. 10, 31

SCM Subsea Control Module. 36

SCSSV Surface Controlled Subsarface Safety Valve. 10

SIF Safety instrumented Function. 23

SIL Safety Integrity Level. 23, 30

SOK Strength of Knowledge. 61

TCI Tecnical Condition Index. 27

XT Christmas Tree. 32

Chapter 1

Introduction

1.1 Problem and Background

The petroleum industry is the main driver for the Norwegian economy. It is the country's largest industry. The country has a mature market for the oil and gas sector as it has been producing oil and gas from the North sea for decades. Norway has made several significant oil and gas discoveries in the past few years, including the giant Johan Sverdrup field, which will require major investments and create new jobs in the industry. Demand for oil and gas continues to grow, so the search for hydrocarbons begins to move into deeper regions of the sea. Today, there are more than 1140 wells in Norway and their number will continue to grow as demand will increase [40].

As the oil and gas industry grows gradually in Norway, production has to be reliable, cost-efficient and safe. Thus, to ensure safe operation of the facilities, safety barriers like emergency shutdown valves (ESD), e.g., (DHSV), (PMW), and (PWV), are in place. These valves will shut down affected processes, areas, or equipment should an unwanted incident occur. The shutdown can range from a single valve to a complete shutdown and evacuation of the facility. One of the most critical pieces of equipment in a safety instrumented system (SIS) is the emergency a shutdown valves, which has strict requirements regarding performance and reliability. For safety instrumented systems, the PSAN specifically recommends International Electrochemical Commission (IEC) standards 61508 and 61511, as well as the Norwegian Oil and Gas Guideline 070 (NOG 070) [16], to be used as a basis to achieve this requirement. The NOG 070 guideline specifies minimum performance requirements (minimum SIL requirements) to the reliability of selected safety instrumented functions in wells that are required by national and international standards adopted in the Norwegian Petroleum sector. In the operational phase of the facility, it must be verified through maintenance and condition monitoring that the observed SIL of the safety instrumented functions meets the SIL requirement.

Even though the petroleum industry is mature in the Norwegian continental shelf, there are some challenges related to the understanding of barrier requirements and key stakeholder's needs. This problem is caused by the use non- standard syntax and ambiguous or inconsistent terms for documenting requirements. Therefore, the purpose of this thesis is to perform an elicitation of requirements related to barrier monitoring systems for ESD valves using the process of systems engineering.This thesis will explicitly outline key stakeholders' needs and help stakeholders to understand barrier requirements.

In order to present targeted status, the key stakeholders' needs for this thesis will be collected, analyzed and translated into requirements. Moreover, the requirements form standard,guidline (NOG 070 and Norsok-D10), and best practices will be extracted and analyzed to cover the thesis purpose. This study will help stakeholders to develop barrier monitoring system in the future work.

1.2 Objectives and Research questions

The objective of this thesis is to develop a barrier monitoring system for emergency shutdown valves by elicitation key stakeholders' needs and translate it to the technical requirements. The stakeholders are considered for this work are operator companies and service companies.. This study will help stakeholders to understand barrier requirements and match their interests. The thesis will cover three main issues related to stakeholders.

- How much barrier testing requirements are clear for stakeholders as specified in the local standards and guidelines (Norsok-D 010 and NOG 070) and if they follow these standards?
- To identify the main problems that operator companies meet and what should be detected by monitoring systems?
- To determine which failure modes can detect monitoring service providers's requirements in accordance with customer needs.?

1.3 Scope Limitations

There are several limitations encountered in this thesis. And these are listed as followings:

- The studies carried out for this report are only addressing the hydrocarbon industry and particularly the Subsea emergency shutdown valves. Even though knowledge for some of the presented concepts is very generic, it may also be relevant for topside oil and gas industry.
- The national standard and guideline such as Norsok D-10 and NOG-070 are the prime sources for this report. Besides technical papers, literature and secondary data within-subject are have been used to support discussions.
- The writer of this report had limited experience and knowledge about actual offshore settings and work practices on the NCS. This limitation will influence the requirements elicitation process made in this report and because of it certain scenarios will be simplified in order to provide an easy understanding to the readers.
- Due to the time and scope limitation of this master thesis, the translated customer requirements have not been tested and verified. Hence, it can be worked upon in the future and employed on an industrial lelvel as well.

- The requirements elicitation process should have been done with the operator companies representatives. However, for case study 1 and 2 data have been gathered from Kvaeven Anna and Shaipov Moslim study due to unexpected circumstances.

- It is essential that while extending the condition monitoring system to take failure mode, failure causes, and failure symptoms into consideration as they are main inputs for descriptors development. Thus, these three main inputs have been described in the literature review section. Besides, the failure mode and symptoms analysis table have been developed, see Appendix C. However, due to time limitation, scope limitation and lack of data, failure causes were the discussion topic.

1.4 Methodology

The requirement elicitation process is implemented in this thesis. The national standards (NOG 070, Norsok -D 010), Industrial guidelines, best practices, and customers' needs were the main sources for the requirements used in the requirement elicitation. A literature review of the relevant standards and white papers were done prior to the requirement elicitation task. First and foremost, elicited requirements from standards required additional analysis steps to translate them into a specific level of detail. That required semi-structured interviews with experts to extract the practical meaning of how these requirements are implemented in the real world. Second, collecting customer needs to be required semi-structured interviews (with customers or via representatives) to get specific clarification related to capabilities and/or characteristics. However, In some parts of the thesis, secondary sources have been used as input for this thesis. These sources have been gathered from various case studies that performed with companies such as ConocoPhillips, Equinor, AkerBp, Spirit Energy and Maersk. Later on, the gathered data translated into technical requirements. Third, the standard/based requirements and customer-based requirements were analyzed (classified, traced to technical functions). Finally, the requirements were reported.

1.5 Thesis structure

The thesis report is structured as follows:

- **Chapter 1:** Provides general problem background information that occurs in Norwegian continental shelf and concerns the project scope, purpose and limitations;
- **Chapter 2:** Introduces theoretical overview about System Engineering and Requirements Elicitation. Later, subsea well barriers are introduces along with different testing methods used in their ESD valves;
- **Chapter 3:** describes current monitoring system that implemented for monitoring subsea valves barrier valves and gives brief information which barrier valves claimed by monitoring service providers to be improved;
- **Chapter 4:** analysis ESD system, how related valves are tested,operated and

monitored. Moreover, the chapter gives knowledge about observed failure mechanisms, failure modes and symptoms that mostly occurs in the valves, later on, the chapter will be proceeded with data collection from different case studies to determine stakeholders needs related to barrier valves;
• **Chapter 5:** discuses elicited requirements and this will be splitted in three stages where in the first stage requirements from standards such as Norsok D- 010 and NOG 070 are interpreted, additionally it will discuss how often required company do testing and how the ConocoPhilips follows the procedure.In the second stage failure modes and failure mechanisms are elicited from gathered data. In the final stage of this chapter TechnipFmc's and Valvewacth's monitoring requirements elicited;
• **Appendix A :** describes testing integrity requirements in the standards such as Norsok D-10 and NOG-070.
• **Appendix B :**introduces the questions that have been asked from industry representative by primary source.
• **Appendix C :** provides recommendation based on Failure mode and Symptom analysis to develop condition monitoring.

Chapter 2

Theoretical Background and Literature Review

2.1 System Engineering Process

2.1.1 System Engineering

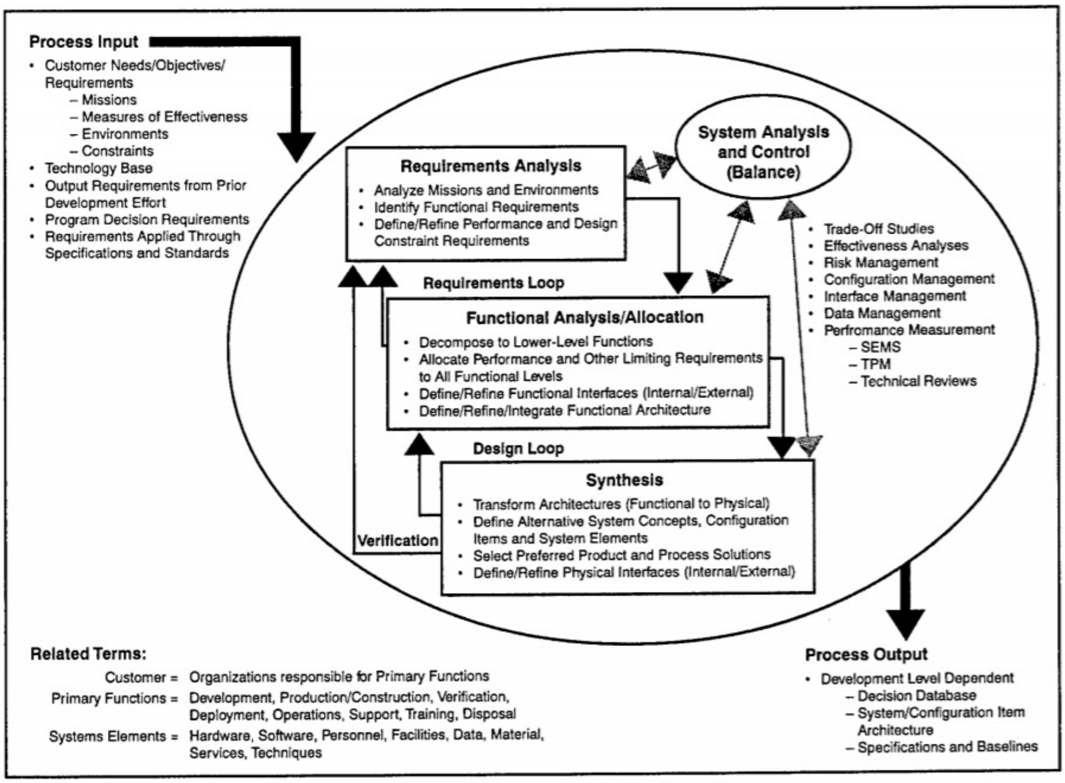

Process Input
• Customer Needs/Objectives/ Requirements
– Missions
– Measures of Effectiveness
– Environments
– Constraints
• Technology Base
• Output Requirements from Prior Development Effort
• Program Decision Requirements
• Requirements Applied Through Specifications and Standards
System Analysis and Control (Balance)
Requirements Analysis
• Analyze Missions and Environments
• Identify Functional Requirements
• Define/Refine Performance and Design Constraint Requirements
Requirements Loop
Functional Analysis/Allocation
• Decompose to Lower-Level Functions
• Allocate Performance and Other Limiting Requirements to All Functional Levels
• Define/Refine Functional Interfaces (Internal/External)
• Define/Refine/Integrate Functional Architecture
• Trade-Off Studies
• Effectiveness Analyses
• Risk Management
• Configuration Management
• Interface Management
• Data Management
• Perfromance Measurement
– SEMS
– TPM
– Technical Reviews
Design Loop
Synthesis
• Transform Architectures (Functional to Physical)
• Define Alternative System Concepts, Configuration Items and System Elements
• Select Preferred Product and Process Solutions
• Define/Refine Physical Interfaces (Internal/External)
Verification
Related Terms:
Customer = Organizations responsible for Primary Functions
Primary Functions = Development, Production/Construction, Verification, Deployment, Operations, Support, Training, Disposal
Systems Elements = Hardware, Software, Personnel, Facilities, Data, Material, Services, Techniques
Process Output
• Development Level Dependent
– Decision Database
– System/Configuration Item Architecture
– Specifications and Baselines

Figure 2.1: The System Engineering Process [33]

The system engineering is important discipline,which takes key role in the scientific and engineering area. Because of the system are more and more complicated.

The system engineering it transforms needs and requirements into a set of system product and generate information for decision makers, and provides input for next level development [33]. Therefore, the requirements engineering inputs takes very important role in the system engineering.

System engineering process inputs - Inputs consist primarily of the customer's needs, objectives,requirements and project constraints. The system engineering process is illustrated in Figure 2.1.

2.1.2 Requirement Engineering

Requirements engineering is a subdivision of system engineering, and using it, the system boundaries and the system characteristics can be analyzed. The requirements engineering embraces requirements elicitation, documentation, and maintenance of the requirements. Requirements engineering is a repeatable and systematic technique. In every phase of the requirements engineering lifecycle, the requirements are analyzed and evaluated to find consistency and completeness. Thus, the requirements that are collected for this process are applicable to the whole system and not only for a single component [23].

" The cost of the requirement engineering depends on the magnitude and the type of the system that is being designed or developed.For big systems it will costs 15% of the total budget only for formal requirement specification, for narrow systems it fluctuates from 8 to 10 percent " [30] [39].

Occasionally, the problems occur in the industries due to the usage of inappropriate requirements [23]. They are such as followings:

1. Delayed and over budget projects
2. The product does not reach the intended target. The customer, who are actually paying for the system, are not satisfied.
3. The errors faced in the development of the system, is the reason for the problems in using the system.
4. The continuous use of such system makes it error prone, and thus enhances the cost of maintenance.

Fixing an error resulted by the wrong requirement is much difficult than correcting the errors occured in the later stages of project.

"Fixing the requirements errors requires the rework on system design, implementation and testing. The cost of fixing the requirements errors is 100 times more than the cost of the simple errors that occurred in the later stages of the project " [30].

2.1.3 Requirement Elicitation

Requirement elicitation is the process of gathering requirements [23]. One of the most important targets of elicitation process is to explore what problem needs to be solved, and hence identify system boundaries. These boundaries define, at a high level, where the final delivered system will fit into the current operational environment. Identifying and agreeing a system's boundaries affects all subsequent elicitation efforts. The identification of stakeholders and user classes, of goals and tasks, and of scenarios and use cases all depend on how the boundaries are chosen [39].

Identifying stakeholders– Stakeholders embrace customers or clients (who pay for the system), developers (who design, construct and maintain the system), and users (who interact with the system to get their work done).

Goals denote the targets a system must meet. Eliciting high level goals early in the development process is important . Eliciting goals focuses the requirements engineer on the problem domain and the needs of the stakeholders, rather than on possible solutions to those problems [39].

The requirements elicitation process embraces a chain of processes that interact with each other to generate requirements documentation. The lifecycle of requirements elicitation process is showed in the figure below.

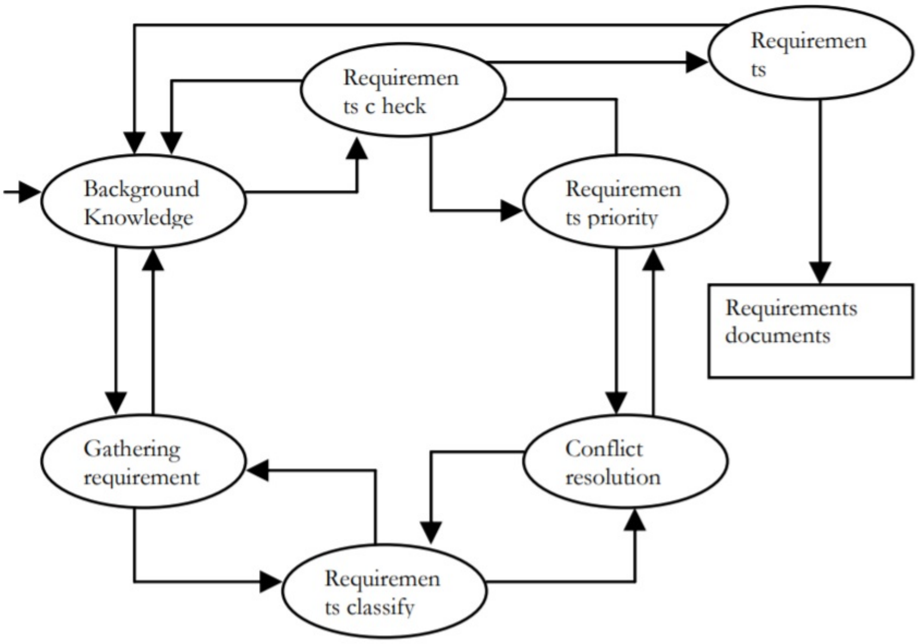


Figure 2.2: Requirements Elicitation Process [23]

Back ground Knowledge - The analyst should understand the back ground and domain knowledge of the application that is being developed.

Gathering the requirements- This is the activity discovering by involving with the stakeholders and users.

Requirements Classification- This activity includes the organizing of the requirements gathered from different sources.

Requirements Conflict - This activity embraces with the stakeholders and requirements engineers. This is used to solve problems in the requirements that disagree the organization and business rules.

Requirements Prioritization - Recognizing the important requirements by interacting with the stakeholders and organize them in to most priority number.

Requirements Check - This activity embraces checking stakeholder's expectations.

The requirements elicitation process must be maintained precisely during elicitation requirements. This process not only helps the organization to collect requirements, but it also analyses the requirements and business procedures of the organization. The requirements elicitation and analysis is a tough activity in requirements engineering because of the following reasons.

1. Lack of technical knowledge and unawareness of technical aspects from stakeholder's side.

2. Sometimes Stakeholders demand unrealistic things and even they do not know what exactly expecting from system.

3. Stakeholders express their requirements in general terms so that It is difficult to find technical aspects of the system from general terms and translate it to requirements.

2.1.4 Requirement Analysis

The first step of the Systems Engineering process is to analyze the process inputs. Requirements analysis is used to enhance functional and performance requirements. Thus, customer requirements are translated into a set of requirements that determine what the system must do and how well it must perform.The system engineer must ensure that system requirements are understandable, unambiguous, comprehensive, complete, and concise [33].

Requirements analysis should clarify and define functional requirements and design constraints. Functional requirements determine (how far), time lines (when and how long), and availability (how often). Design constraints determine those factors that limit design flexibility, such as: environmental conditions or limits; defense against internal or external threats; and contract ,customer or regulatory standards.

2.1.5 Classical Requirement Elicitation Techniques

The classical techniques have been used for a long time, and these are as follows.

2.1.5.1 Interviews

The most popular method for requirements elicitation is to interview stakeholders. In this method, the analyst and the engineers of the requirements engineering process discuss with the different types of stakeholders to understand the requirements of the system and the targets they have to fulfill in the system [39] [23] [28].

1. **Closed Interview** - In this interview the requirement engineer prepares predefined questions and tries to get answers for these questions from stakeholders.

2. **Open Interview** - In this interview the requirement engineer does not prepare any predefined questions,but he/she tries to get information from stakeholders from open discussion.They mostly try to concentrate on the expectation of stakeholders on the system

2.1.5.2 Questionnaire

Questionnaires are one of the methods collecting requirements in less cost [23]. Questionnaires is the simplest among the technique and may bring remarkable results if constructed properly. There is some measure that should be taken off while preparing the questions about a topic [28].

- The questions must be to the point.
- There should not any repetition.
- The ambiguous statements should be avoided.
- The questions should be arranged in a reasonable manner
- These should be relevant to the domain of the system.

There are dual forms of questions:

1. **Open-Ended Questions**- The open-ended question allows the user to talk normally and tell in his/her own words what the requirements are. They are not bound to answer in a specific format. It is a user centered approach to know the requirements.
2. **Closed-Ended Questions**-This is a pre-defined structure of questionnaires to be asked in a strict manner. It cannot vary form one person to the other. Every person intermingles with the it in a similar way.It does not allow user to speak of his/her mind. These types of questions are easy to judge and generate reports.

A well organized and effective questionnaire can be used to decide the user's requirements, objectives, and constraints. Thus, it can influence people to answer honestly and makes it possible to collect reliable results from stakeholders.

2.2 Barrier Philosophy

2.2.1 Classification and Characteristics of Barrier Types

ISO 13628-1 is the general standard which provides safety requirements and recommendations during the development of the subsea production system. It provides guidelines for the development of a barrier philosophy for planned or existing subsea production system, [7]. According to the standard, a barrier can be classified into one of three basic types, and they are as following:

- Passive
- Active
- Temporary

The standard defines passive barriers as permanent that are not actuated or routinely disturbed once they are in place, such as the following:

- cement (and competent underground start);
- downhole packers (including seal-bore extensions);
- downhole components, such as mandrels and valves for gas lift and chemical injection;
- subsea wellheads (including wellhead gaskets);
- casing and tubing strings (including hangers and seal assemblies);
- subsea tree bodies and valve blocks (including interfacing gaskets);
- pipeline systems (including jumpers, connector bodies, gaskets and pipe);
- tree and manifold piping;
- pressure -sealing caps (including gaskets);

The active barriers are designed to be actuated routinely in one of three ways:

- manually (e.g., by a diver or ROV)
- some from a remote control (e.g., via the production control system)
- by reverse flow (e.g., check valves) and they are as following:
  - downhole SCSSVand SSCSV;
  - Subsea tree valves (including valves in the production and annulus flow paths, as well as valves in hydraulic and chemical injection lines);
  - manifold valves (including hydraulically actuated and ROV- operated valves);
  - flowline isolation valves (including those on a manifold, as well as at the top riser);
  - check valves (including those in downhole gas-lift valves and chemical injection lines).

Temporary barriers are designed to be used for limited time during a specific activity which may require ongoing attention to ensure their effectiveness. These activities include:

- kill weight fluid,e.g. in the tubing or in the tubing/production casing annulus;
- installing downhole tubing plugs which do not remain in the well.

The distinction between passive and active barriers that passive does not take action for it to achieve its function, while active ones take action in response to a measurement or human action. All barriers listed above are used during operation in the subsea production system, and their main objective is to prevent a hazardous event from occurring or reduce the consequences of a hazardous event.

2.2.2 Well Barriers

In risk management, barriers prevent the occurrence of a sequences of events, limit the harm, and inconveniences accidents. Figure below illustrates role of barriers in risk management context.

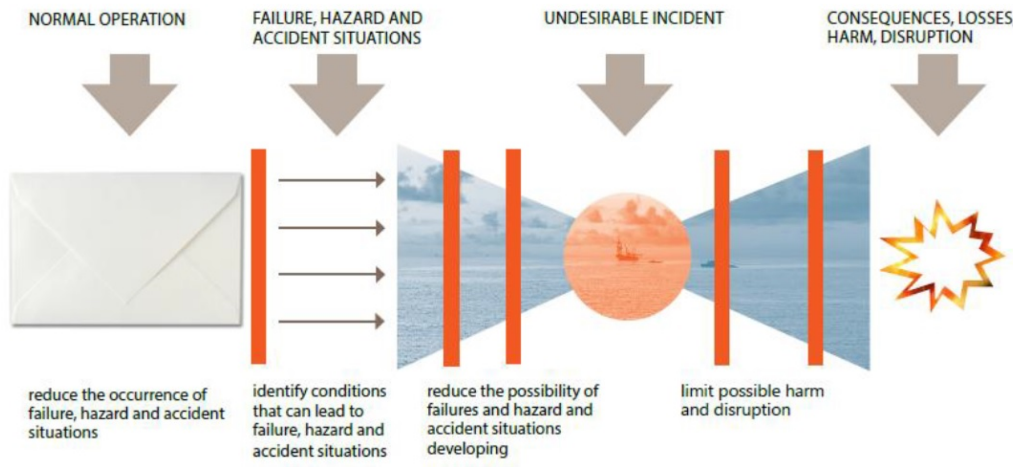
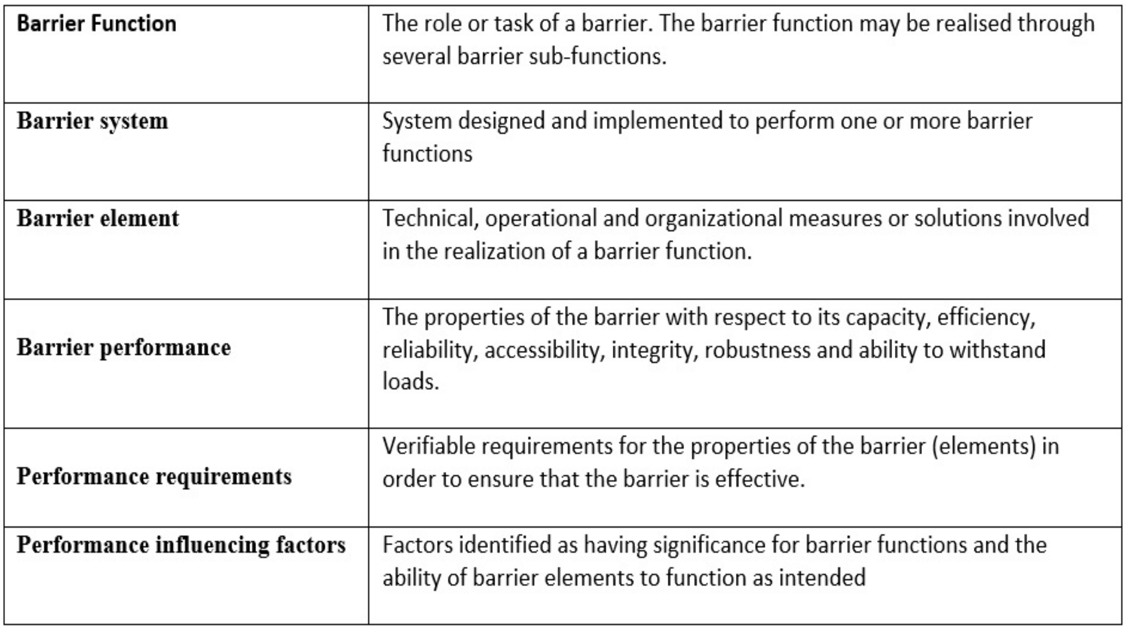

NORMAL OPERATION
FAILURE, HAZARD AND ACCIDENT SITUATIONS
UNDESIRABLE INCIDENT
CONSEQUENCES, LOSSES, HARM, DISRUPTION
reduce the occurrence of failure, hazard and accident situations
identify conditions that can lead to failure, hazard and accident situations
reduce the possibility of failures and hazard and accident situations developing
limit possible harm and disruption

Figure 2.3: The role of barriers in a risk management context. Normal operation: Risk reduction, safe and robust solutions. Failure, hazard and accident situations [31]

2.2.2.1 Key Concepts and Definition

A barrier can be classified according to its function, its system and elements that make up the barrier. Moreover, it is important to be aware of its performance requirements, and performance influencing factors that may affect them.



Barrier Function	The role or task of a barrier. The barrier function may be realised through several barrier sub-functions.
Barrier system	System designed and implemented to perform one or more barrier functions
Barrier element	Technical, operational and organizational measures or solutions involved in the realization of a barrier function.
Barrier performance	The properties of the barrier with respect to its capacity, efficiency, reliability, accessibility, integrity, robustness and ability to withstand loads.
Performance requirements	Verifiable requirements for the properties of the barrier (elements) in order to ensure that the barrier is effective.
Performance influencing factors	Factors identified as having significance for barrier functions and the ability of barrier elements to function as intended

Table 2.1: Barrier system and its function

In oil and gas industry, a critical hazard shall be always be evaluated to prevent blowout events and well releases [15]. In this case, well barriers play a critical role. Well barriers are determined according to Norsok D-010 [20].

2.2.2.2 Governing Regulations and Documentation

Well barriers are controlled and monitored according to the following regulations and associated guidelines:

- The framework regulations §11 (Risk reduction principles) [4]
- The management regulations §4 (Risk reduction)[4]
- The management regulations §5 (Barriers) [5]
- The facilities regulation §48 (Well Barriers) [2]
- The facilities regulations §8 (Safety functions)[3]
- The activities regulations §47 (Maintenance programme) [1]

To attain the requirements to well barriers, the regulation guidelines recommend the standard NORSOK D-010 Chapters 4, 5, 6 and 15 to be used in the matters ofHSE [31]. Maintenance activities to be performed in accordance with well barrier management include inspection, trial, testing, repair and monitoring.

> ***"Failure modes that may constitute a health,safety or environment risk shall be systematically prevented through a maintenance programme... The programme shall include activities for monitoring performance and technical conditions... "***

The activities regulations §47 describes that maintenance programme can include sub- programmes for testing and preventive maintenance. For well control and intervention,Norsok D-10 should be used as basis for maintenance activities.

2.2.3 Well Integrity

Norsok D-010 is a functional standard that sets minimum requirements for the equipment/solutions to be used in a well. However, oil marketing companies choose solutions by themselves, and they have full responsibilities to meet the requirements of the standard. According to this definition, the personnel planning the drilling and completion of wells will have to identify the solutions that give safe well life cycle designs that meet the minimum requirements of the standard.

The responsibilities of operating companies and service providers are to ensure that they adequately meet all requirements of the standard. Also, the equipment that planned to be used must be according to standard. If not, the equipment will need to be improved and qualified before use. Deviations from the standard can be made in some cases when the standard allows this. The performance of the solution implemented should be equivalent to, or better than the stipulated requirement.Thus, it is important to properly define equipment specifications and requirements for well barriers to ensure the well integrity is maintained throughout the well life.

In accordance with Norsok D-010, there shall be two well barriers available throughout all well activities and operations. This also applies to including suspended or abandoned wells, where a pressure differential exists. It may cause uncontrolled outflow from the borehole/well to the external environment. This sets the foundation for how to operate wells and keep the wells safe in all phases of the development. Thereby, the operators have to adhere to the two well barrier philosophies in all phases of their operations.

Planning
Execution
Operation
Intervention
Plug & abandonment

Figure 2.4: Well barrier life cycle [21]

2.2.4 Well Barrier Function

While analyzing the well barriers, it is crucial to understand the barrier functions and their possible failure modes.

Norsok D 010 differs between primary and secondary well barriers. The primary barrier is the closest barrier to the pressurized hydrocarbons. A properly functioning well barrier can contain the pressurized hydrocarbons. However, if the primary well barrier fails (e.g., by leakage or a valve that fails to close), the secondary barrier will prevent outflow from the well. If the secondary well barrier is not able to function, there may, or may not, be a tertiary barrier available that can stop the flow of hydrocarbons.

The figure below contains schematic representations showing the respective locations of both of primary and secondary barriers.

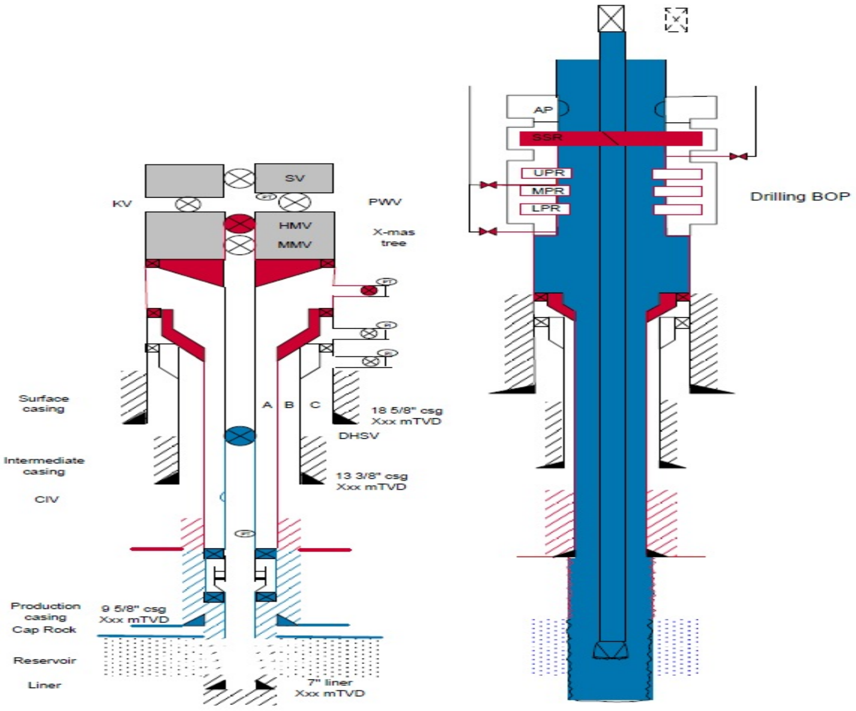
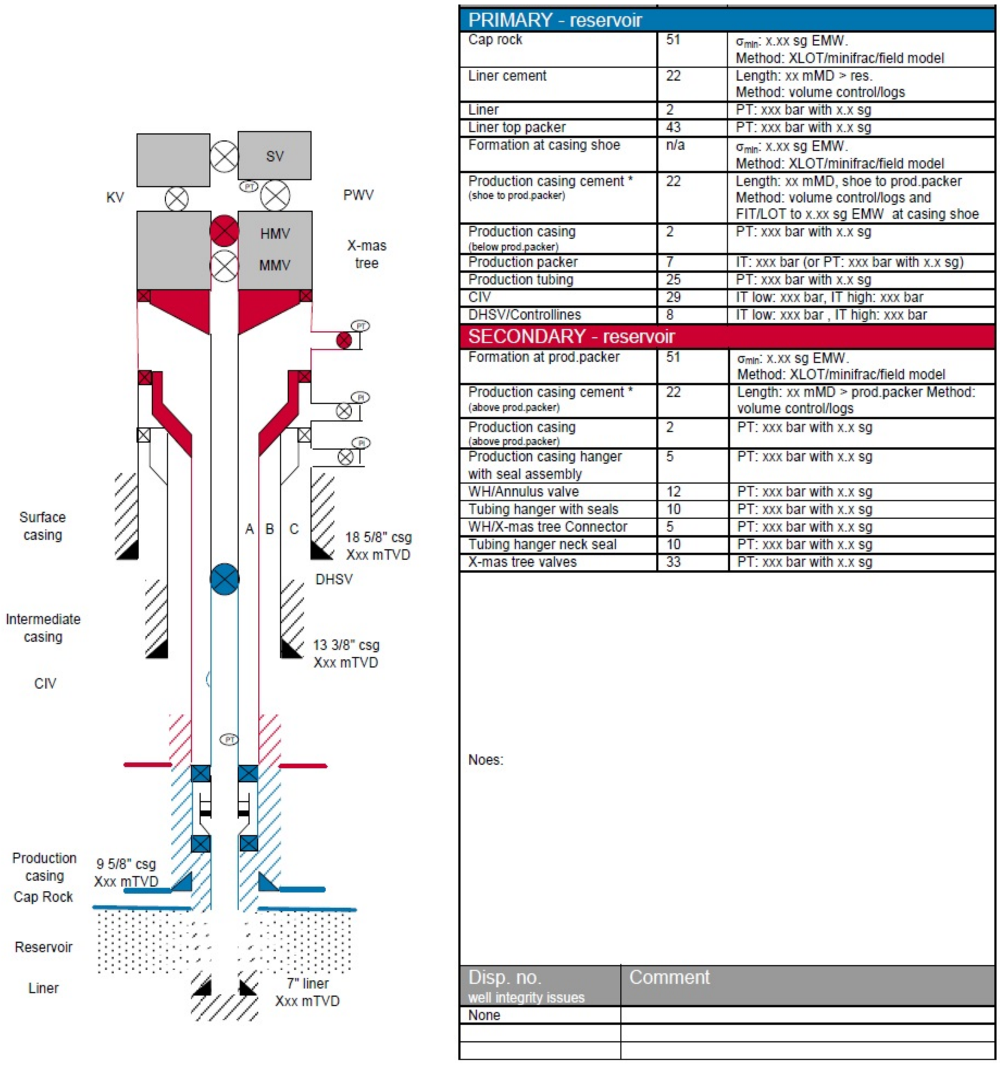


Figure 2.5: Primary and secondary barriers in production and drilling mode [37]

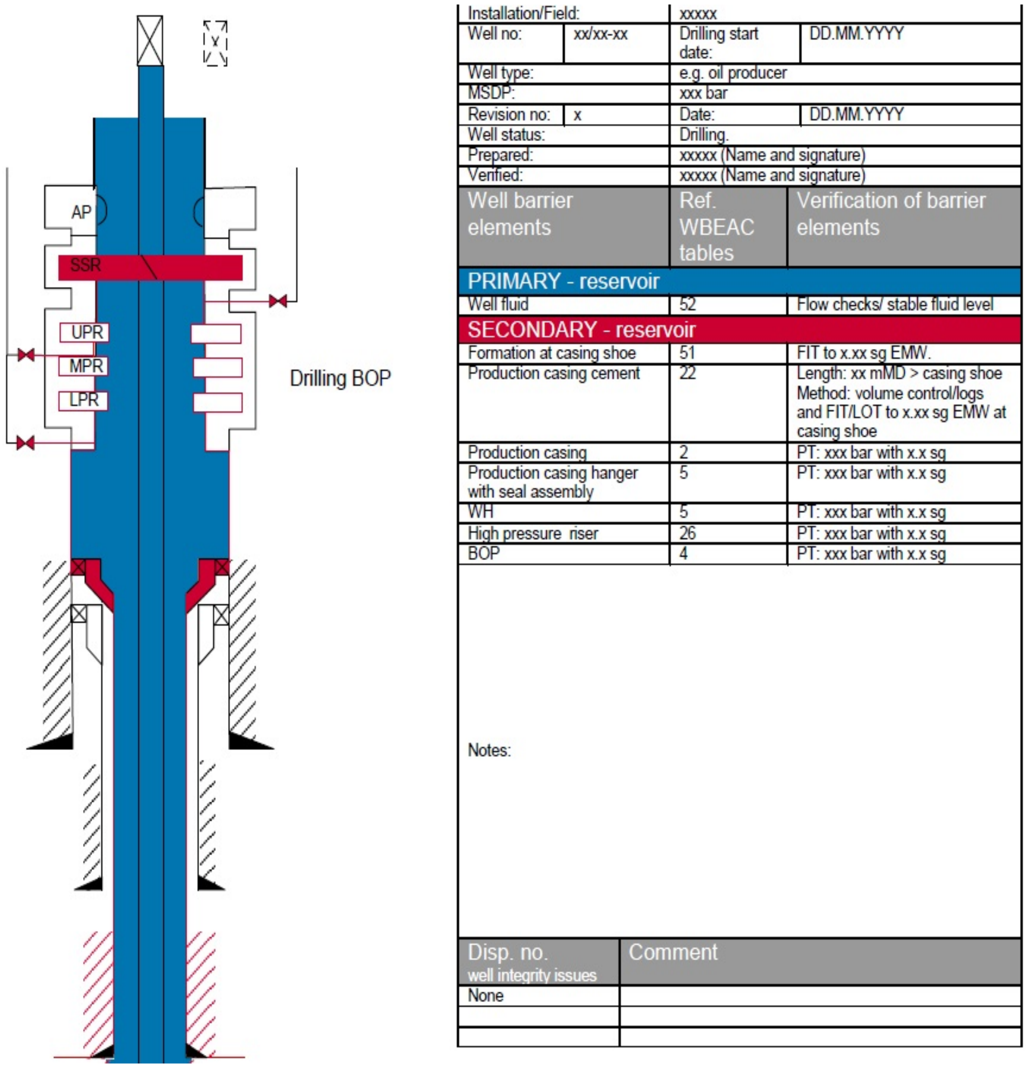


PRIMARY - reservoir		
Cap rock	51	σ_{min}: x.xx sg EMW. Method: XLOT/minifrac/field model
Liner cement	22	Length: xx mMD > res. Method: volume control/logs
Liner	2	PT: xxx bar with x.x sg
Liner top packer	43	PT: xxx bar with x.x sg
Formation at casing shoe	n/a	σ_{min}: x.xx sg EMW. Method: XLOT/minifrac/field model
Production casing cement * (shoe to prod.packer)	22	Length: xx mMD, shoe to prod.packer Method: volume control/logs and FIT/LOT to x.xx sg EMW at casing shoe
Production casing (below prod.packer)	2	PT: xxx bar with x.x sg
Production packer	7	IT: xxx bar (or PT: xxx bar with x.x sg)
Production tubing	25	PT: xxx bar with x.x sg
CIV	29	IT low: xxx bar, IT high: xxx bar
DHSV/Controllines	8	IT low: xxx bar , IT high: xxx bar
SECONDARY - reservoir		
Formation at prod.packer	51	σ_{min}: x.xx sg EMW. Method: XLOT/minifrac/field model
Production casing cement * (above prod.packer)	22	Length: xx mMD > prod.packer Method: volume control/logs
Production casing (above prod.packer)	2	PT: xxx bar with x.x sg
Production casing hanger with seal assembly	5	PT: xxx bar with x.x sg
WH/Annulus valve	12	PT: xxx bar with x.x sg
Tubing hanger with seals	10	PT: xxx bar with x.x sg
WH/X-mas tree Connector	5	PT: xxx bar with x.x sg
Tubing hanger neck seal	10	PT: xxx bar with x.x sg
X-mas tree valves	33	PT: xxx bar with x.x sg

Noes:

Disp. no. well integrity issues	Comment
None	

Figure 2.6: Well barrier production Schematic illustration [20]



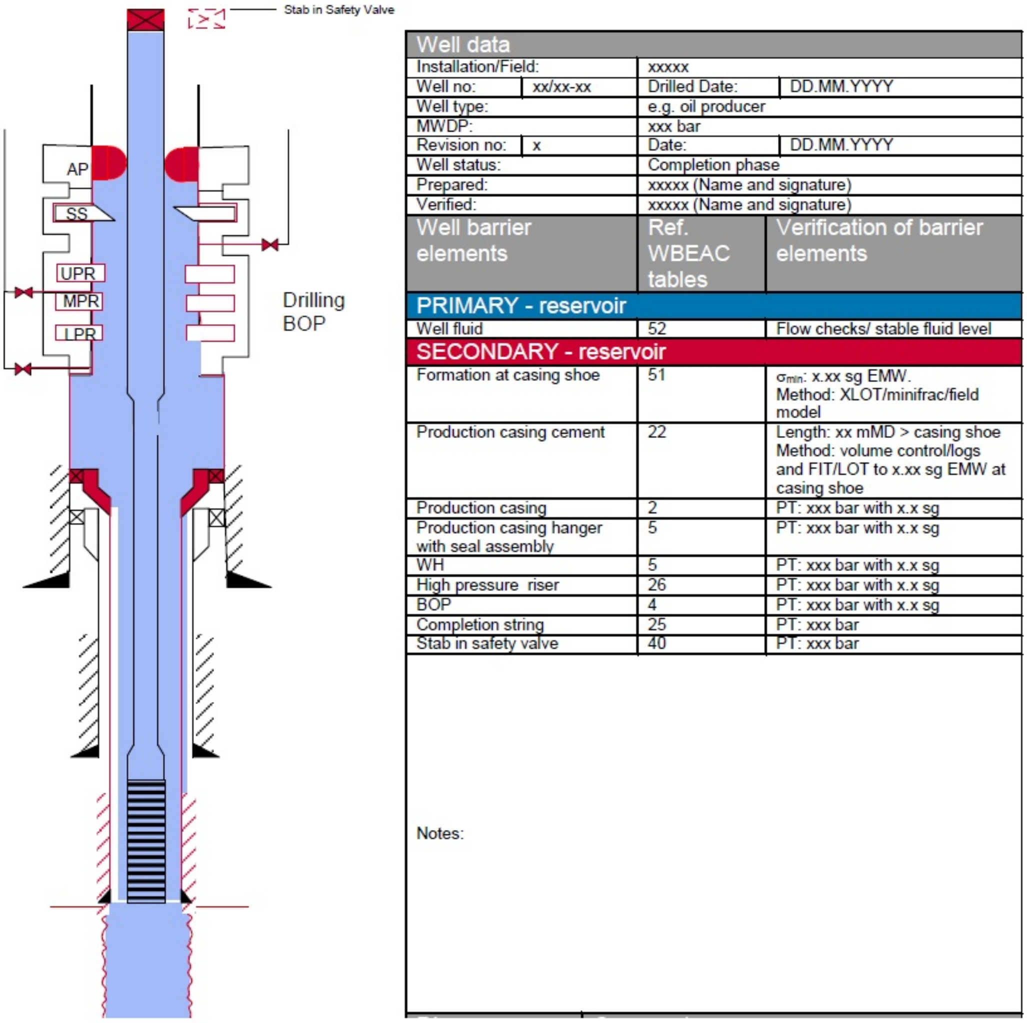
Installation/Field:		xxxxx	
Well no:	xx/xx-xx	Drilling start date:	DD.MM.YYYY
Well type:		e.g. oil producer	
MSDP:		xxx bar	
Revision no:	x	Date:	DD.MM.YYYY
Well status:		Drilling.	
Prepared:		xxxxx (Name and signature)	
Verified:		xxxxx (Name and signature)	

Well barrier elements	Ref. WBEAC tables	Verification of barrier elements
PRIMARY - reservoir		
Well fluid	52	Flow checks/ stable fluid level
SECONDARY - reservoir		
Formation at casing shoe	51	FIT to x.xx sg EMW.
Production casing cement	22	Length: xx mMD > casing shoe Method: volume control/logs and FIT/LOT to x.xx sg EMW at casing shoe
Production casing	2	PT: xxx bar with x.x sg
Production casing hanger with seal assembly	5	PT: xxx bar with x.x sg
WH	5	PT: xxx bar with x.x sg
High pressure riser	26	PT: xxx bar with x.x sg
BOP	4	PT: xxx bar with x.x sg

Notes:

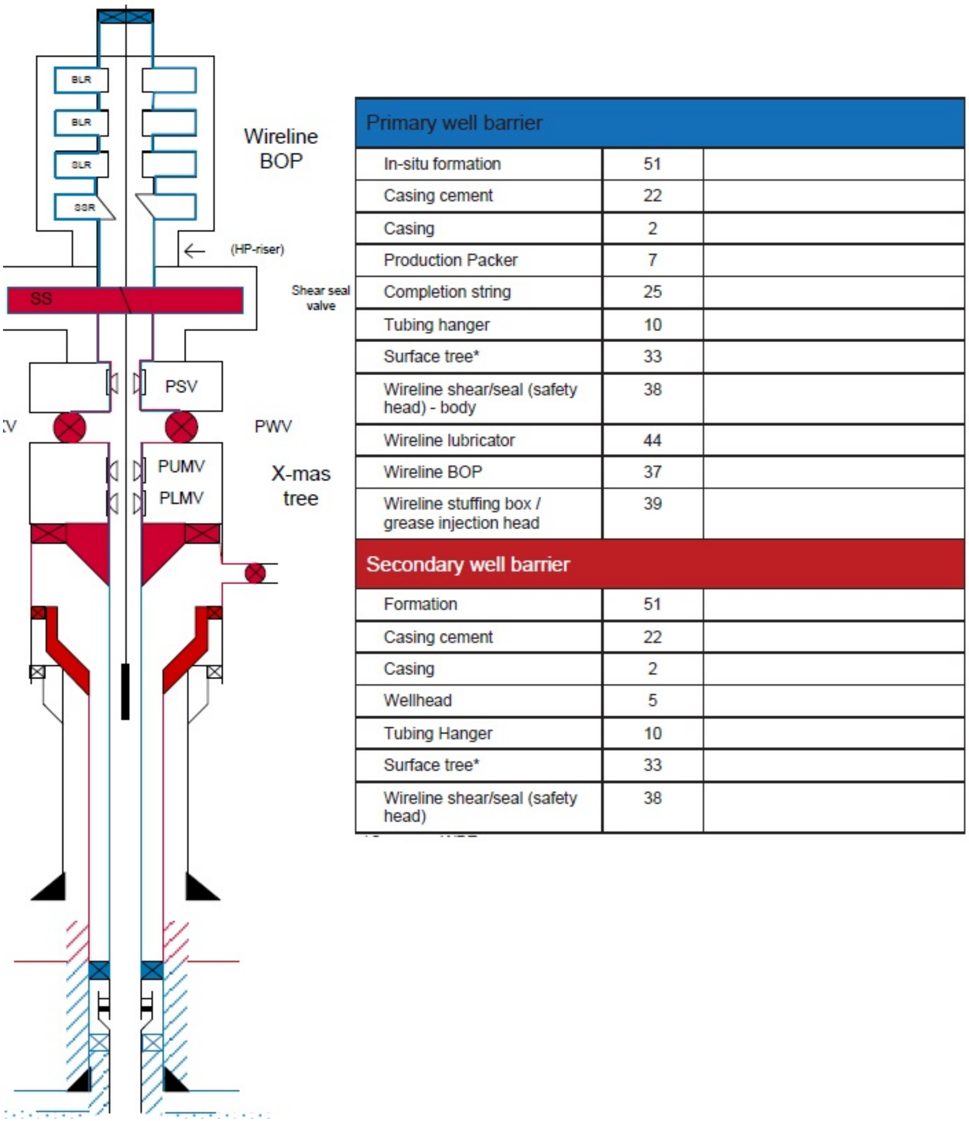
Disp. no. well integrity issues	Comment
None	

Figure 2.7: Well Barrier Schematic illustration for Drilling Phase [20]



Well data			
Installation/Field:		xxxxx	
Well no:	xx/xx-xx	Drilled Date:	DD.MM.YYYY
Well type:		e.g. oil producer	
MWDP:		xxx bar	
Revision no:	x	Date:	DD.MM.YYYY
Well status:		Completion phase	
Prepared:		xxxxx (Name and signature)	
Verified:		xxxxx (Name and signature)	
Well barrier elements		Ref. WBEAC tables	Verification of barrier elements
PRIMARY - reservoir			
Well fluid		52	Flow checks/ stable fluid level
SECONDARY - reservoir			
Formation at casing shoe		51	σ_{min}: x.xx sg EMW. Method: XLOT/minifrac/field model
Production casing cement		22	Length: xx mMD > casing shoe Method: volume control/logs and FIT/LOT to x.xx sg EMW at casing shoe
Production casing		2	PT: xxx bar with x.x sg
Production casing hanger with seal assembly		5	PT: xxx bar with x.x sg
WH		5	PT: xxx bar with x.x sg
High pressure riser		26	PT: xxx bar with x.x sg
BOP		4	PT: xxx bar with x.x sg
Completion string		25	PT: xxx bar
Stab in safety valve		40	PT: xxx bar
Notes:			

Figure 2.8: Well Barrier Schematic illustration for Completion Phase [20]



Primary well barrier		
In-situ formation	51	
Casing cement	22	
Casing	2	
Production Packer	7	
Completion string	25	
Tubing hanger	10	
Surface tree*	33	
Wireline shear/seal (safety head) - body	38	
Wireline lubricator	44	
Wireline BOP	37	
Wireline stuffing box / grease injection head	39	
Secondary well barrier		
Formation	51	
Casing cement	22	
Casing	2	
Wellhead	5	
Tubing Hanger	10	
Surface tree*	33	
Wireline shear/seal (safety head)	38	

Figure 2.9: Well Barrier Schematic illustration for Intervention Phase [20]

2.2.5 Technical Well Barriers

The general philosophy of the wells is to be equipped with sufficient mechanical well barriers that prevent uncontrolled flow from the reservoir. Additionally, it is a general rule that no single failure of components should lead to unacceptable consequences.

In practice, wells are equipped with two well barriers against the reservoir. and these barriers need to be as independent of each other as possible. In addition, it is required to have sufficient barriers in place against limited volumes. e.g. against outflow from annulus A in gas lifted wells.

For wells in operation and plugged wells, two independent well barriers need to be in place. For wells undergoing drilling or intervention, it is not always possible to assure complete independence. In this case, operators must implement measures to improve reliability of the common well barrier elements. In addition, operators must develop stronger emergency response plans.

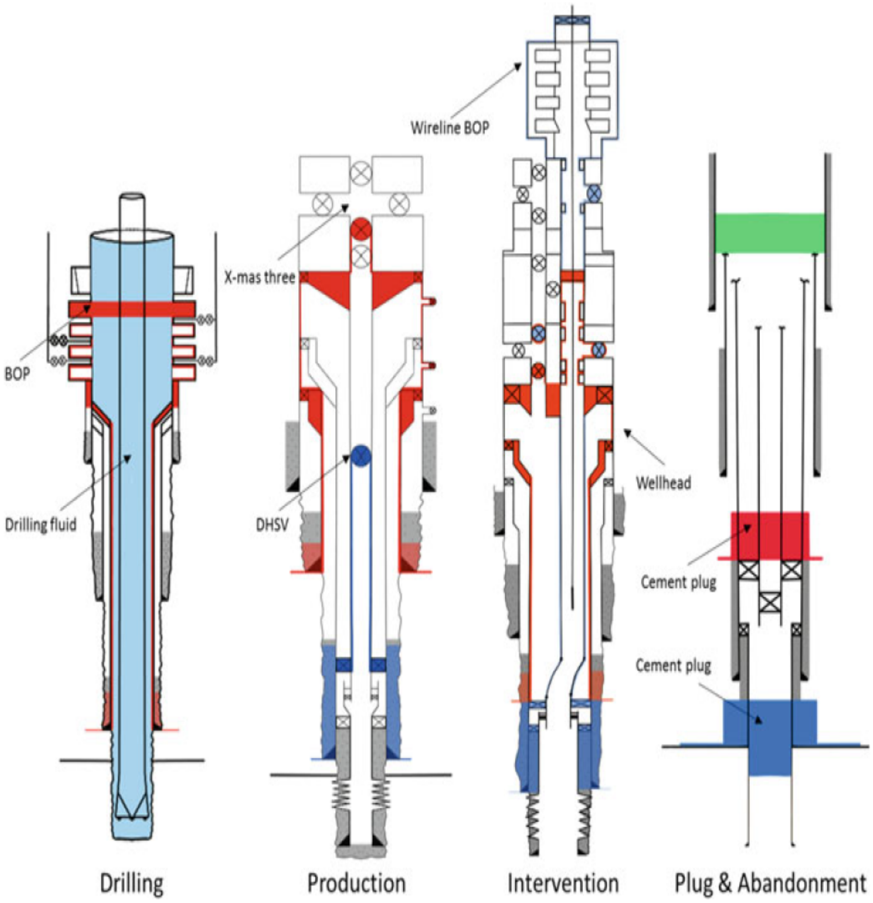
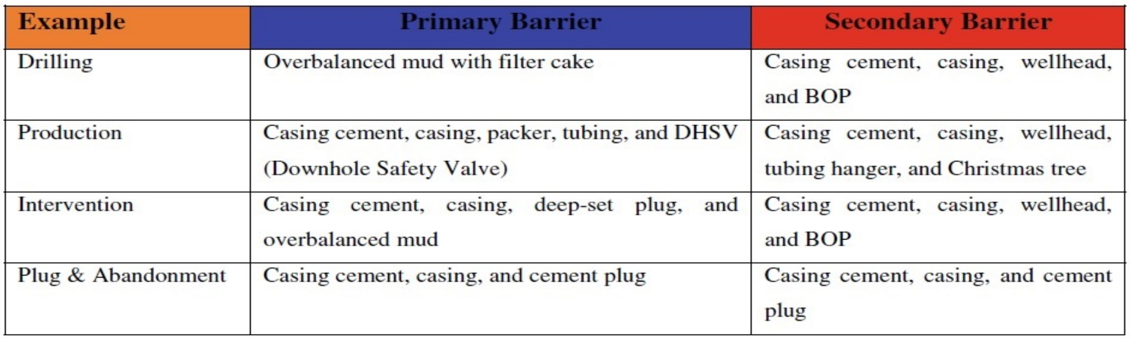


Figure 2.10: Illustration of the two-barrier philosphy throughout a well's lifecycle [14]



Example	Primary Barrier	Secondary Barrier
Drilling	Overbalanced mud with filter cake	Casing cement, casing, wellhead, and BOP
Production	Casing cement, casing, packer, tubing, and DHSV (Downhole Safety Valve)	Casing cement, casing, wellhead, tubing hanger, and Christmas tree
Intervention	Casing cement, casing, deep-set plug, and overbalanced mud	Casing cement, casing, wellhead, and BOP
Plug & Abandonment	Casing cement, casing, and cement plug	Casing cement, casing, and cement plug

Table 2.2: Examples of barrier system through the life-cycle of the well given in Fig. 2.4 [29]

2.2.6 Well Barrier elements (Valves)

Barrier elements that comprise electrical, electronic, and/or programmable electronic technology are referred to as safety – instrumented functions (SIF). They belong to a class of systems called safety instrumented systems . SIS are responsible for ensuring that safe operating conditions are not exceeded. There are several SIS in the oil and gas industry, with names related to their essential function: emergency shutdown systems, process shutdown systems, fire and gas detection systems, and so on. SIS consist of three main sub-systems:

- Input elements; sensors (for automatic activation) or push-buttons (for manual
- Logic solver(s); an electronic or non-electronic device that process the signal(s) from the input elements and sends signals to the relevant final elements
- Final elements; physical items that interact with the well, for example, valves, such that loss of containment is stopped or avoided.

SIF are the final element in the SIS. Several SIF may be built into the same SIS. The same logic solver may, for instance, be used to activate several isolation valves. Nevertheless, there are some essential design considerations: Functions that respond to the same event (e.g., well kick or choke collapse) should not share components. This means that if the primary and secondary barriers have SIF, they need to be placed in two different (and independent) SIS to avoid a failure of the logic solver that causes simultaneous failure of the primary and the secondary barrier. Examples of these safety instrumented functions are DHSV, PMV, PWV. These elements are activated upon manual pushbuttons or a signal from sensors, which the logic solver deems excessive.

2.2.7 Failsafe Functions

For a well in operation some barrier elements need to be in an open position to enable production. These are typically the DHSV (SCSSV), PMV and PWV. It is therefore critical that these valves automatically close in the event of a fire, power outage or loss of hydraulic supply. It is a general requirement that these valves are fail-safe, meaning that the valve is designed to move to the safe position when such a failure occurs.

To ensure the fail-safe function, it is critical that correct design calculations are done. An example is for instance that a DHSV needs to have strong enough spring ensuring the valve will close with the highest possible pressure on the control line after control line failure.

Typically, the barriers that mounted on the Xmas tree and wellhead are active, and they have fail-safe functions. These barriers control fluid that flows through the wellbore, and in case of the problem in the well, primary and secondary barriers must function. If the primary barrier valve (DHSV or SCSSV) fails to close, secondary one (PMV, PWV) must shut uncontrolled flow, instead. The location of valves are shown in the figure 2.5 below.

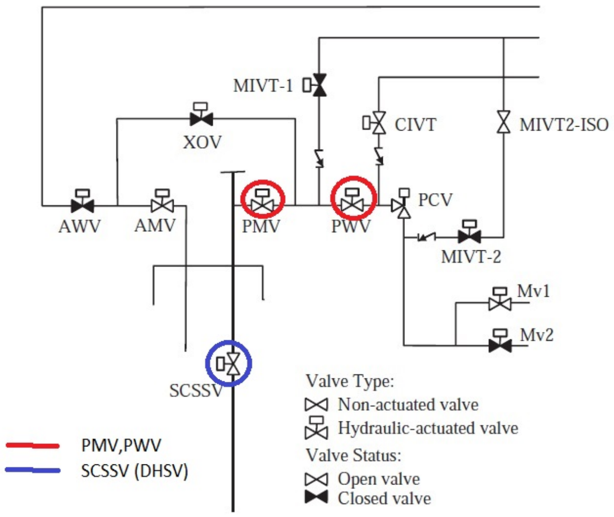


Figure 2.11: Xmass tree and Welhead Barrier Valves, adapted [17]

2.3 Testing Barrier Valves

The Emergency shutdown (ESD) system, is Safety Instrumented system (SIS). To ensure that the required safety integrity level (SIL) of each safety instrumented function complies with IEC 61508, IEC 61511, NOG 070 and Norsok D-010, testing must be performed to correct performance and to confirm correct behavior in response to specific fault conditions, such as power loss. In the operational phase, the tests split into the following categories:(i) Partial Stroke (ii) Full stroke Test, (iii) Internal leak Test.

2.3.1 Partial Stroke Testing

Emergency shutdown valves are normally operated in *low demand mode of operation* [10].This means that the frequency of demands for operation of the valves is no greater than one per year. The ESD valves are kept in open position for long period of time and designed to close the valves in case a demand should occur [36].These valves usually have hydraulic or pneumatic *fail-safe close* actuators. Failure in the ESD valves may occur while they are in open position and may cause the valves to *"fail to close"* or to *"leak"* in situation when demand occurs. Such failures are called *dangerous undetected* (DU) failures and may stay a long period of time. Thereby functional testing is required to reveal *dangerous undected* failures,which constitutes partial stroke testing and full stroke testing. In recent years, partial stroke testing has been supplemented to functional testing [36].

Example: *Emergency Shutdown Valve*

Emergency shutdown valve is installed on a gas Xmas tree and Wellhead production system. If an emergency occurs in the production system, the valve should close and stop the fluid flow. The valve is a hydraulically operated gate valve. The actual open/close function is performed by sliding a rectangular gate, having a bore equal to the bore of the conduct. The gate is moved by a hydraulic piston connected to the gate by a stem. The gate valve has a‘*fail-safe* actuator. The valve is automatically closed by the spring force when the hydraulic pressure is bled off.

Partial Stroke Testing of Valves. Partial stroke testing is similar concept as imperfect test, but it is not exactly same. A common application partial proof testing is *partial stroke testing of valves.*The PST of emergency down valve is a good solution to maintain the probability of failure on demand (PFD) for safe plant operation.This method may result in savings for both plant initial cost and running cost verses other methods of achieving the plant safety integrity level.

During *partial stroke testing of valves* , the emergency shutdown valve is only subject to partial movements. The valve movements are so small that any impact on the process flow or pressure is negligible; thus,it does not require any stop of production[41].The movement may for example be from 0-15% (of a total of 100% travel distance); that is long enough to (hopefully) identify whether or not the valve is stuck, and short enough to avoid process disturbances.When full stroke testing is not practical, Partial stroke testing is provided. The new version of ISA-TR 96.05.01 refers that partial stroke testing can detect earlier detection of certain dangerous undetectable failures and improve the system reliability level,though full stroke testing cannot be avoided entirely [27].

2.3.2 Full Stroke Testing

Full Stroke Testing of Valves. The objective full stroke testing is to reveal hidden failures and to verify that the system is able to perform when demand occur. FST contains stroking the valves from fully open to fully closed position (if fail-close), and opposite for a fail- open ESD valves , and requires a planned shutdown. It is sometimes is not feasible to carry out full stroke test, because it may not be technically feasible or be very time consuming.Another reason may be that the test itself may be truly dangerous for operational safety [26].

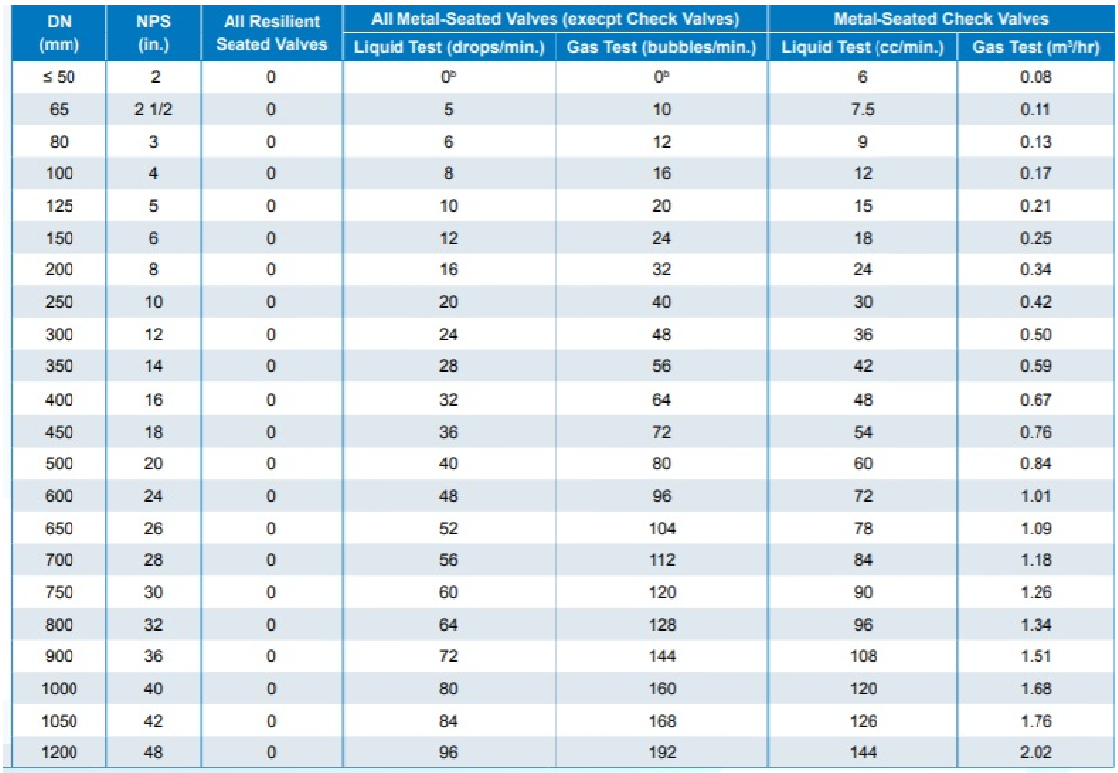
FST is used to test subsea barrier valves as partial stroke testing. However, the difference in that, while FST is executed, the system needs to be studown - if no bypass availabe. The NOG 070 guidline states that Subsea barrier valves shall be tested at leas once a year, to demonsrate that barrier valves (i.e., PMV, PWV, and DHSV) can achieve the specified safe state when a process demand occurs [6]. These valves are typical ESD valves, are located in Subsea X mass tree's production bore and wellhead, and play a vital role as safety valves during production. Subsea X mass tree and wellhead barrier valves do not have any bypass valves, in that case, the production needs to stop, whereas full stroke testing is executed.

The table 2.3 provides a listing dangerous failures and failure modes for Subsea gate valve and wellhead Flap valve. The test strategy indicates whether failure mode can be detected by partial stroke testing or only by full testing. Based on OREDA data, the typical percentage of the failures that can be detected by PST is 70% for many process isolation valves types and services . Supplementary analysis can be performed to justify a higher percentage a detected failures. However , it is very difficult to demonsrate a percentage greater than 85% for subsea valves applications. Those failures that are not detected during the PST are tested using an FST [34].

Failures	Failure Modes	Test Strategy
Actuator sizing is insufficient to actuate valve in emergency conditions	Valve fails to close (or open)	Not tested
Valve packing is seized	Valve fails to close (or open)	Partial or full stroke
Valve packing is tight	Valve is slow to move to closed or open position	Partial or full stroke, if speed of closure or resistance to closure is monitored
Airline to actuator crimped	Valve is slow to move to closed or open position	Partial or full stroke, if speed of closure or resistance to closure is monitored, Physical inspection
Airline to actuator blocked	Valve is slow to move to closed or open position	Partial or full stroke
Valve stem sticks	Valve fails to close (or open)	Partial or full stroke
Valve seat is scarred	Valve fails to seal off	Full stroke with leak test
Valve seat contains debris	Valve fails to seal off	Full stroke test
Valve seat plugged due to deposition or polymerization	Valve fails to seal off	Full stroke test

Table 2.3: Dangerous Failure,Failure Modes, and Test Strategy [34]

2.3.3 Internal Leak Testing



DN (mm)	NPS (in.)	All Resilient Seated Valves	All Metal-Seated Valves (execpt Check Valves)		Metal-Seated Check Valves	
			Liquid Test (drops/min.)	Gas Test (bubbles/min.)	Liquid Test (cc/min.)	Gas Test (m^3/hr)
≤ 50	2	0	0^b	0^b	6	0.08
65	2 1/2	0	5	10	7.5	0.11
80	3	0	6	12	9	0.13
100	4	0	8	16	12	0.17
125	5	0	10	20	15	0.21
150	6	0	12	24	18	0.25
200	8	0	16	32	24	0.34
250	10	0	20	40	30	0.42
300	12	0	24	48	36	0.50
350	14	0	28	56	42	0.59
400	16	0	32	64	48	0.67
450	18	0	36	72	54	0.76
500	20	0	40	80	60	0.84
600	24	0	48	96	72	1.01
650	26	0	52	104	78	1.09
700	28	0	56	112	84	1.18
750	30	0	60	120	90	1.26
800	32	0	64	128	96	1.34
900	36	0	72	144	108	1.51
1000	40	0	80	160	120	1.68
1050	42	0	84	168	126	1.76
1200	48	0	96	192	144	2.02

Figure 2.12: API 598 (9th edition 2009) Valve Seats Leakages Rates [12]

To ensure fluids or gas will not pass through ESD valves while demand occurs, the leak test must be executed. Leaks occur when a gas or liquid fluid flows from higher pressure side to a lower pressure side of a part and are caused by holes, cracks, weak seals, or permeable areas in a product. In the Subsea Xmass tree and wellhead, leakage of the Barrier (DHSV, PMV, PWV) can pose serious risks. Therefore, it is important to conduct regular leak testing to ensure leaks are revealed before they cause damage or harm.

Leak testing is conducted, by closing the valve, pressurized one side of the valve, and monitor leakage rate on the opposite valve side during a specified time. The leakage depends on valves size and range from 0.15 to 11.5 ml per minute for valve sizes 1 through to 12 inches [12]. The test duration and leakage acceptance criteria are dependent on valve size, valve design, valve pressure, and seat type. It is described in the standards, such as ISO 5208, API 6D, API 598. Figure 2.12 depicts leakage acceptance criteria defined in API 598 standard.

2.3.4 Dangerous Detectable and Dangerous Undetectable Failures

ESD valves on the Subsea X mass tree and wellhead usually are remained open and activated only when demand occurs. Therefore, failures may occur and remain hidden until the emergency occurs or testing is performed. Failures are classified into Dangerous undetected (DU) and Dangerous detected (DD) [13]. Proof testing and Diagnostic testing are the techniques used to classify failures [35].

Proof testing . This test verifies that a SIS is able to perform its SIF. The time interval between two consecutive proof test is often called proof test interval. DU failures are revealed only through proof testing

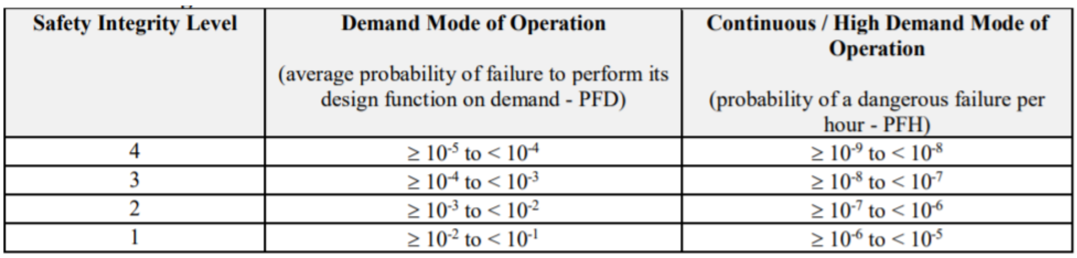
Diagnostic testing .The test uses built-in is automatic partial test that uses built in self-test features to detect almost immediately failures.The failures that are detected announced as alarms in the control room. DD failures are revealed by diagnostic testing.

2.3.5 SIL requirements

SIL is a numerical benchmark and related to probability failure on demand (PFD). The IEC 61508 and IEC 61511 are a risk based approach standards for setting the SIF performance levels by assigning a SIL. In the IEC standards, a safety function is considered as a function to be implemented to achieve a specified risk reduction related to a hazardous event. A safety function is thus specified in terms of the action to be taken and the required probability to successfully carry out this action [24]. This probability is also referred to as safety integrity, and in the context of IEC standards safety integrity is classified according to the discrete level as indicated in figure 7.2 below. Even though, IEC 61508 does not specify detailed, it divides requirements in four Safety integrity level, SIL 1,SIL 2, SIL 3 and SIL 4, lited in order of increasing reliability.[41]. 70

SIL is important because it represents how well a SIS performs. SIL can be affected by design robustness, e.g. device integrity, voting, and common cause faults. It can also be affected by operation and maintenance strategy, e.g., diagnostics and testing intervals [45].

Final element (especially barrier valve) testing is the most challenging part of SIL compliance for production companies. HSE management advocates that barrier valves should be tested frequently to detect DU failures to ensure that barrier valves are able to operate when demand occurs. During testing, the valves are checked to ensure SIL compliance with requirements. However, maintenance engineers claim that testing barriers often to collect additional data can cause extra degradation of the valves, and this can reduce Safety integrity level. Therefore,this implies that there should be balance between testing and data collection [48].



Safety Integrity Level	**Demand Mode of Operation** (average probability of failure to perform its design function on demand - PFD)	**Continuous / High Demand Mode of Operation** (probability of a dangerous failure per hour - PFH)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

Figure 2.13: Safety integrity level [6]

Chapter 3

Barrier Valve Condition Monitoring

3.1 Condition monitoring in subsea equipment

Subsea systems have existed for more than 50 years. It was just a few years ago that Oil and Gas companies have considered Condition Monitoring (CM) for subsea equipment as an essential part of their asset management strategies. Thus, Original Equipment Manufacturers (OEMs) have taken different approaches, but all of them have the same goals, such as reducing reliability, reduce NPT, maximize production, and minimize Life Cycle Cost (LCC). The section below describes what Subsea OEMs are doing with respect to CM. It also presents latest developments made by researchers and instrumentation manufacturers.

3.1.1 Condition monitoring providers approach

In recent years, General Electric (GE) released the Subsea Monitoring and Remote technology Center (SMART Center). The operation center is located in the UK where they remotely monitor subsea production systems around the world. The center performs remote fault diagnosis, equipment performance trending and provides recommendation for maintenance intervention and valuable information to flow assurance engineers. Additionally, The SMART center is connected to other GE's center around the globe, and allows collaboration between GE experts in the UK and maintenance engineers other locations. The benefits of this center are quicker response to issues with equipment failures. Some of the parameters monitored by GE are:

- Hydraulic Leakage
- Umbilical resistance degradation
- Choke erosion
- Valve signature
- Communication and Power

Schlumberger also provides subsea monitoring solutions. The company provides downhole sensors and subsea control modules among with many other products.

Their system offers a parallel surveillance system that allows to monitor and control SPS together with wellbore equipment. The figure 5.1 below, is includes a subsea control module that monitors and operates the XT and an additional control module and communication hub (subCnet) for the downhole sensors and valves [18]. This system allows for integration of sensors used in different applications from different vendors, for further processing by the CMS and transmission to an onshore operation center.

Other CM services supplied by Schlumberger are integrity surveillance of risers, flowlines and jumpers as well as detection of leaks and distributed temperatures measurements for hydrate prediction.

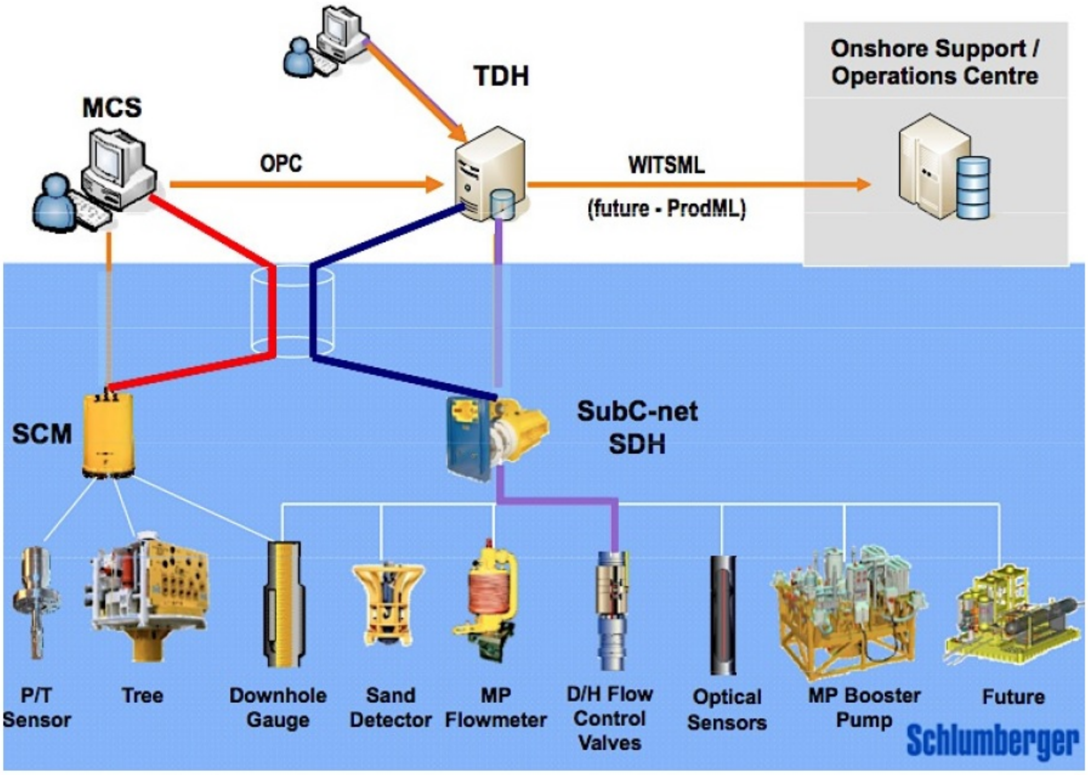


Figure 3.1: Schlumberger parallel surveillance system [18]

Aker solutions has also made some developments in their CM of subsea equipment. The company has an e-field program, which is based on instrumentation surveillance, data analysis, operational optimization, and advanced control through real-time intervention , and remote operations. The information about CM of subsea equipment is not available publicly and therefore cannot be discussed in detail in this report.

TechnipFMC has CM program as well. Its *Condition and Perfomance Monitoring* (CPM) system monitors electrical and mechanical components continuously and provides real-time processing to determine current operating conditions and early detection of degradation and-or reduced efficiency [46]. The CPM program, which uses the Technical Condition Index (TCI) explained in section 2.3.1 as the main tool for asset diagnosis, is divided in 4 main process areas:

Monitor and report: the equipment is monitored; abnormal trends are identified (TCI) and reported in-real time to TechnipFMC onshore operation center and customer.

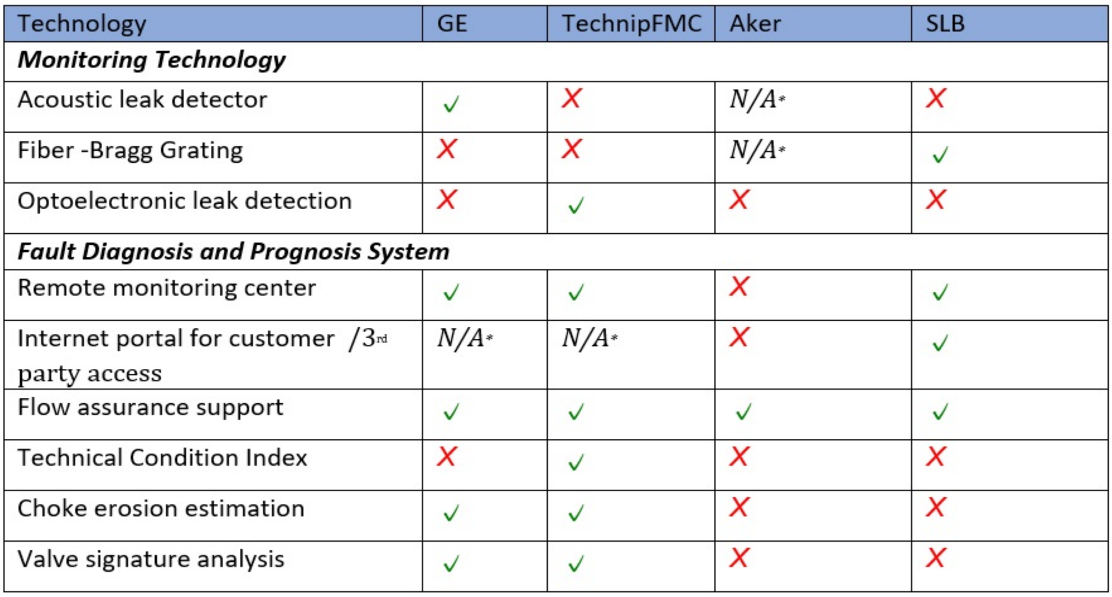
Diagnose, advice and alert: a full diagnostic tool is developed by TechnipFMC with possible assistance from the end user and/or experts located remotely. After installation of the tool, appropriate maintenance action is suggested.

Recover and maintain: the maintenance activities are carried out and related information is entered in a database for future reference.

Knowledge Management: condition and defects on the equipment are compared to the initial failure analysis to corroborate the prediction and then the TCI model is updated based on the findings.

TechnipFMC uses advanced technologies for equipment surveillance such as, opto-electronic leak detection based on fluorescence spectroscopy. This system is based on the principle that different substances absorb more or less light depending on their composition. The main aim of this system is to determine whether any other substances other than seawater are present in the periphery of the equipment.An arrange of LED lamps emit light, record the light reflected and determine if the there are any substances other than seawater around the instrument. The hydrocarbons and hydraulic fluid have specific fluorescence signatures. The detection system can be calibrated for the liquids present in the particular equipment monitored, which allows the senors to detect very small leaks. The monitoring of subsea trees, templates and manifolds can be detected up to 5m. As an option, the system can be fitted with a digital camera that allows confirming the presence of a leak detected by the sensors,without the need to use ROVs for this purpose [38].

The below table 3.1 depicts a summary of the sensor technologies and prognosis/diagnosis systems used by the main subsea equipment providers is presented in.



Technology	GE	TechnipFMC	Aker	SLB
Monitoring Technology				
Acoustic leak detector	✓	✗	*N/A**	✗
Fiber -Bragg Grating	✗	✗	*N/A**	✓
Optoelectronic leak detection	✗	✓	✗	✗
Fault Diagnosis and Prognosis System				
Remote monitoring center	✓	✓	✗	✓
Internet portal for customer /3rd party access	*N/A**	*N/A**	✗	✓
Flow assurance support	✓	✓	✓	✓
Technical Condition Index	✗	✓	✗	✗
Choke erosion estimation	✓	✓	✗	✗
Valve signature analysis	✓	✓	✗	✗

Table 3.1: Subsea Condition monitoring Suppliers [18]

3.2 Existing Condition Monitoring

Certain subsea production equipment like the Xmass tree and Wellhead include vital components. In the event of a failure of a vital component, significant damage to the environment could occur. It is therefore it is crucial to monitor the operation of such components.

The barrier valves are located on the Xmass tree and Wellhead. Generally, these valves hydraulically operated valves. A known, conventional method for measuring the position of such valves is by using at least one pressure transducer, which is connected at least to one hydraulic supply or return line of the valve. The output signal from the transducer is passed to control means at the topside control station via an umbilical cable. The actual measured pressure indicates the state of opening and closing of the valve, thus enabling it to be controlled from the topside control station.

Despite the information provided by the pressure transducer monitors the position of the valve , it enables a limited assessment to be made of the condition and performance of the valve. It has been found out that the use of known pressure transducer monitoring arrangements provide insufficient information to enable a full analysis of barrier valves. Such valves are considered using condition monitoring techniques [25].

3.3 Recommended Condition Monitoring

There exist different aspects that claim which barrier valves might be improved by mounting the acoustic and accelerometer. The first and second claim is schematically shown in the figure 4.2. The first claim describes that the valves that being monitored are the production master valve, production wing valve, and downhole safety valve located on a subsea tree and wellhead. An acoustic sensor, in this example a hydrophone, is fitted to these valves. The valves are controlled by operating signals received from a subsea control module. The valves may be hydraulically or electrically operated. The hydrophone is electrically connected to a subsea electronics module (SEM), housed in the SCM. The SCM and SEM are in communication with a topside control system, which is provided at a surface location, for example, onshore or at a vessel via an umbilical cable[25].

The hydrophone is adapted to capture the acoustic signature of the production master valve, production wing valve and downhole safety valve and convert the data to an associated electrical signal. The term ”acoustic signature” as used herein, refers to the frequency response as measured over a period of time associated with the operation of the valve. The electrical signal is passed via the cable to SEM. The SEM, in turn, transfers this via an umbilical cable to the topside control system for data analysis. The data analysis performed within the topside control system utilizes pattern recognition algorithms to com pare the received data against a database that contains historical data. Typically the historical data related to valve position as well as fault condition acoustic signatures. By suitable comparison, the position of the valve may be determined. In addition, the processing may recognise whether there is any abnormal situation [25].

The second claim has many similarities to the first claim. However, in the second claim, the sensor used to monitor the valve operation is an accelerometer. Which is connected to SEM via cable. The accelerometer can capture signals caused by the physical actuation of the valve. The information sent by the accelerometer may be compared with known acceleration signatures of the valve states and also be used to determine the opening and closing condition of the valve.

Once an acoustic and or accelerometer is mounted on the valve, it needs to capable of continuously capturing acoustic/acceleration signals and the associated acoustic/acceleration frequency spectrum. These can then relay to the surface location where captured data is compared with known data for the related equipment.

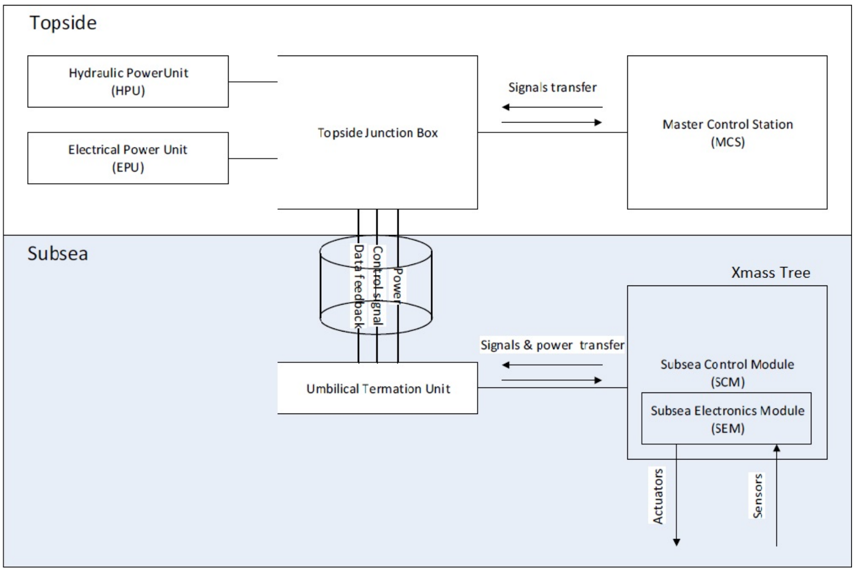


Figure 3.2: Barrier valves Monitoring [19]

Chapter 4

System Analysis and Data Collection

4.1 System Analysis

4.1.1 Emergency Shutdown System

In the oil and gas industry, the ESD is a safety-critical system.The ESD system is designed to minimize the consequences of emergencies related to the escape of hydrocarbons and the outbreak of fire in hydrocarbon carrying areas. The main objectives of the ESD system are to prevent plant, personnel and environmental damage in response to hydrocarbon escape [32]. ESD system can be designed differently, such as fail-to-close and fail-to-open; it depends on its application area [49].

The ESD system in itself is a Safety instrumented System (SIS) and brings the system to a safe state if any violations are predefined. Such systems are designed to be initiated automatically when certain demand occurs. As mentioned earlier, the system is operated on demand, the measurement of the system based on the calculation of probability failure on demand, which expresses that the likelihood the safety function does not work when required.To ensure that system will work when demand occur then the ESD system needs of high Safety integrity level, typically SIL 2 or 3.

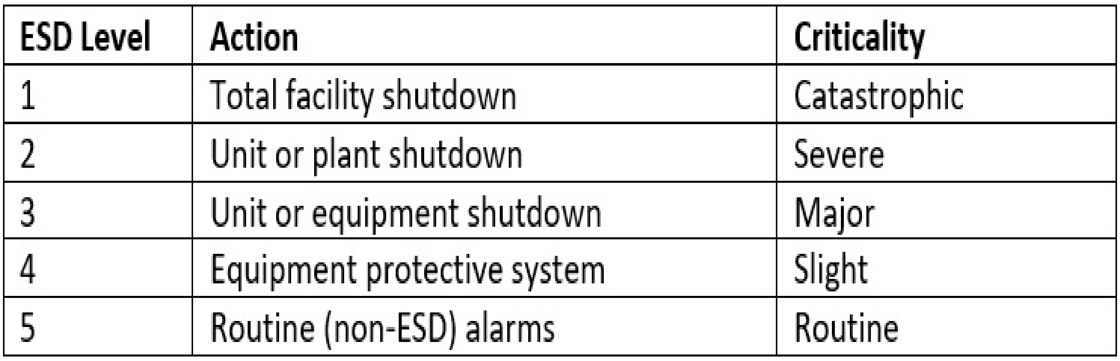
The typical ESD system is different from other systems. This means that the system needs respond to threats to entire facility. Therefore, It is considered one of the most important safety systems that can be provided for any facility. Without an ESD system, facility can be exposed to an incident by leaking ”unlimited ” fuel which can destroy environment .That’s why, an ESD system is designed to respond minimum requirements:

- Shutdown of parts systems and equipment
- Isolate hydrocarbon inventories
- Stop hydrocarbon flow

ESD systems are designed with several mechanisms which initiate shutdown. In the Subsea X mass tree and wellhead ,these systems can be initiate automatically or mechanically.These mechanisms are as following:

- Automatic activation caused by process instrumentation system
- Automatic activation from a confirmed fire and gas detection alarm
- Manual activation with ROV

Usually, there are certain levels of ESD activations. These levels activate emergency measures with increasing amounts. For example, low hazards or small area would require a shutdown of individual equipment, while major incidents would require a plant shutdown. The isolated part of the facility should not put on a threat to another portion of the plant. If it occurs, then the facility should be shut down. The table below illustrates typical ESD levels used in the oil and gas industry.



ESD Level	Action	Criticality
1	Total facility shutdown	Catastrophic
2	Unit or plant shutdown	Severe
3	Unit or equipment shutdown	Major
4	Equipment protective system	Slight
5	Routine (non-ESD) alarms	Routine

Table 4.1: Typical ESD levels [32]

4.1.2 ESD Valves in Subsea X mass Tree

Two valves located in the Subsea Christmas tree are the main ESD Valves, are important in production hydrocarbons:

- PMV is the primary and the most important valve in the Christmas Tree. It provides insulation between the borehole and the production tubing, wherein the hydrocarbons flow from the Christmas Tree to the manifold. During the exploitation of the lode, the valve is in the fully open position. The PMV must be strong enough to withstand the pressure prevailing in the well and prevent an uncontrolled leakage of hydrocarbons from the well.
- PWV is used for closing and opening the XT under normal operating conditions. Just like the PMV, it is responsible for securing the flow of hydrocarbons from the well.

These valves are fail-safe gate valves. It is a very popular type of valves used in Xmass Tree.This type of valves not only meets the safety function in the event of failure, but also allows for the closure of the valves in the Xmass tree without injecting heavy drilling mud into the well in order to eliminate flow from the reservoir into the hole. Closing the valves may be necessary, for example, during pressure and function tests.

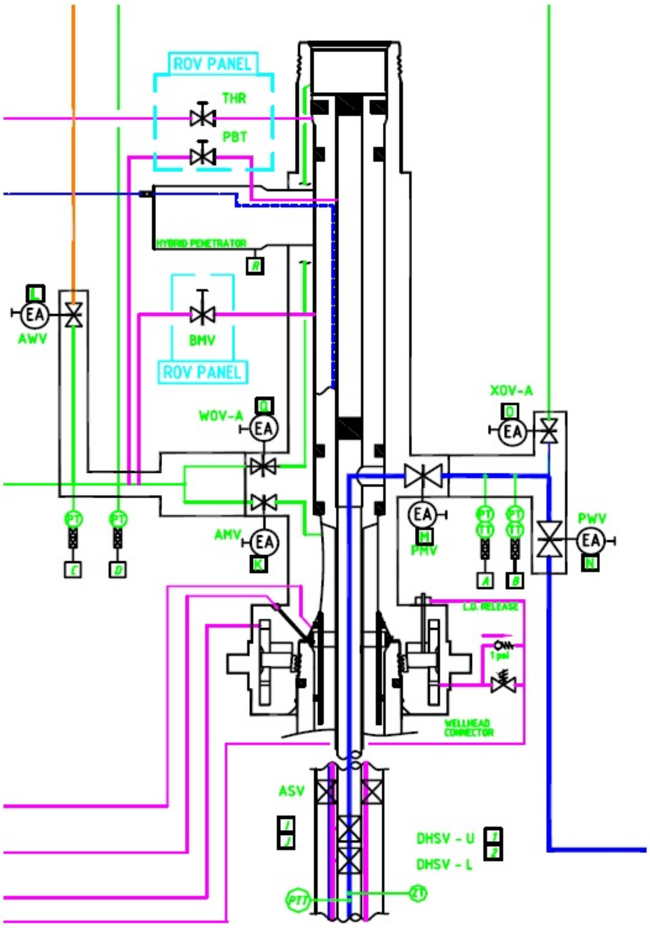


Figure 4.1: Subsea Christmas Tree Schematic Diagram [47]

The valves in the Xmass Tree are controlled via a subsea control module mounted directly on the XT. The subsea control module contains the electronics, hydraulics and instrumentation needed for the safe and effective control of valves in the Xmass tree and the DHSV, usually referred to Surface Controlled Subsurface Safety Valve (SCSSV) [17]. In addition, the subsea control module is responsible for the distribution of the electric current monitoring signal and for communication with the surface. Modern subsea control modules must have reliability for water depths of up to 3000 meters and pressures of 20,000 psi (138 MPa). In order to allow for the closing or opening of valves directly and independently of the control system, Xmass trees are equipped with a panel, which allows for the direct control valve to use the remotely operated vehicle (ROV). Direct control of valves may be necessary for the assembly or disassembly of the Xmass tree of maintenance or failure of the control system [11].

PMV and PWV Gate Valves with Hydraulic Actuators

In this section, gate valves and hydraulic actuators used in the Xmass tree will be studied. The purpose of these valves is to isolate the flow of hydrocarbons or injection fluids which pass through the bore. The valves are located on the Xmass tree majority are gate valves, and they function either fully open or fully closed. These valves are fail - closed type, meaning that, in the case of system failure (e.g., loss of power), the valves move automatically to the closed position to avoid flow through the system. An example of valves arrangement in a subsea Xmass tree is shown in Figure 4.2.

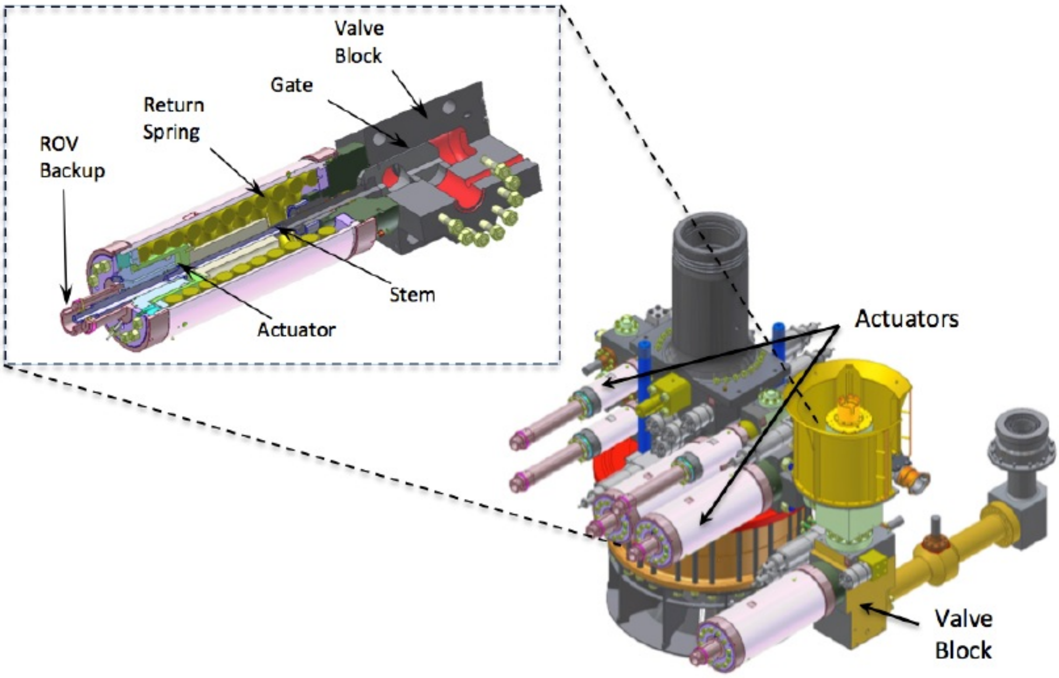


Figure 4.2: Hydrulic gate valves installed on Xmass tree [18]

The valves and actuators showed herein function in the following manner: If the valve needs to be opened, then pressurized hydraulic fluid is sent into the chamber to push the actuator. Once the force exerted by the actuator on the return spring overcomes the opposing forces, the stem moves inside the valve, exposing an opening in the gate that matches the opening in the valve block, letting the fluid go through. To close the valve, the hydraulic pressure is released, and the spring force moves the actuator to its original position.

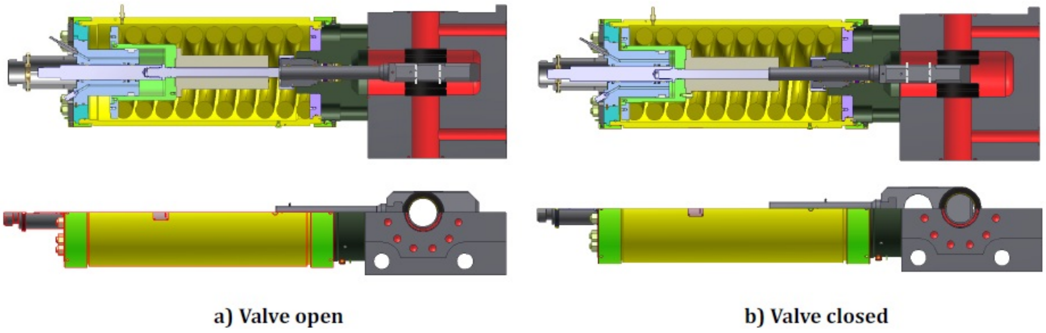


Figure 4.3: Hydrulic gate valves installed on Xmass tree [18]

4.1.3 ESD Valve in Wellhead

A very important valve, which is primary barrier valve, is not located in the Xmass tree, but it is controlled by it, is the DHSV (DHSV). The DHSV is mounted in a completed wellbore at a depth ranging from 100 to 500 meters below seabed. It is a flap-type valve and it is intended to prevent the uncontrolled release of hydrocarbons from the lode in the event of an emergency when other valves have failed. The DHSV is controlled with hydraulic fluid by the Christmas Tree [11].

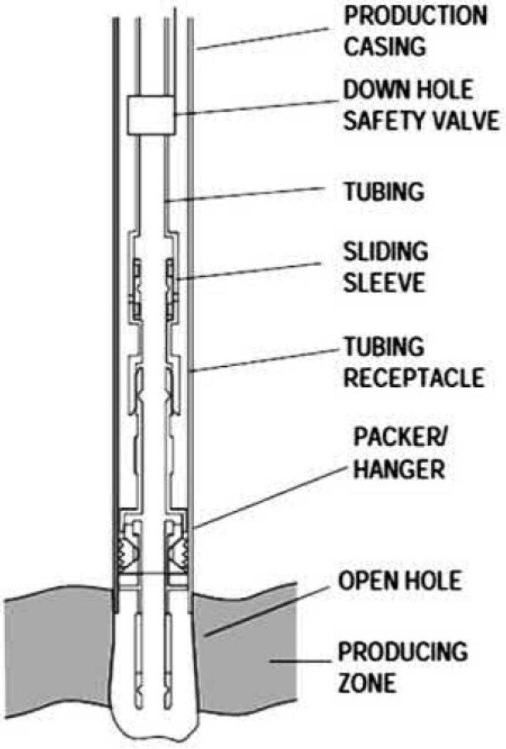


Figure 4.4: Wellhead Configuration [17]

Wellhead Flap Valve with Hydraulic Actuator

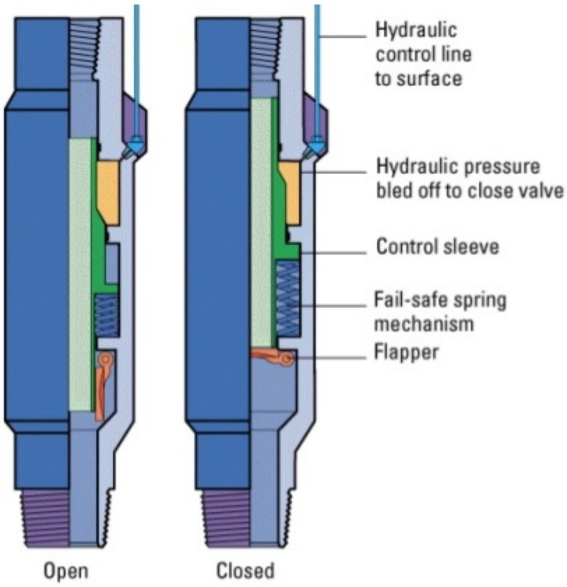

Hydraulic control line to surface
Hydraulic pressure bled off to close valve
Control sleeve
Fail-safe spring mechanism
Flapper
Open
Closed

Figure 4.5: Hydrulic flape valve installed on wellhead [42]

A very vital valve that is not located on Xmass tree, but it is controlled by it, is a DHSV. It is mounted on the completed wellbore on the depth from 100 to 500 below seabed.The valve is operated remotely through a control line that hydraulically connects the safety valve, up and through the wellhead, to an ESD system with hydraulic-pressure supply. The design is fail-safe: through the control line, hydraulic pressure is applied to keep the valve open during production. If the hydraulic pressure is lost, the safety valve closes automatically through the action of an internal power- spring system- a normally closed fail-safe design.

4.1.4 System Context of Barrier Valves

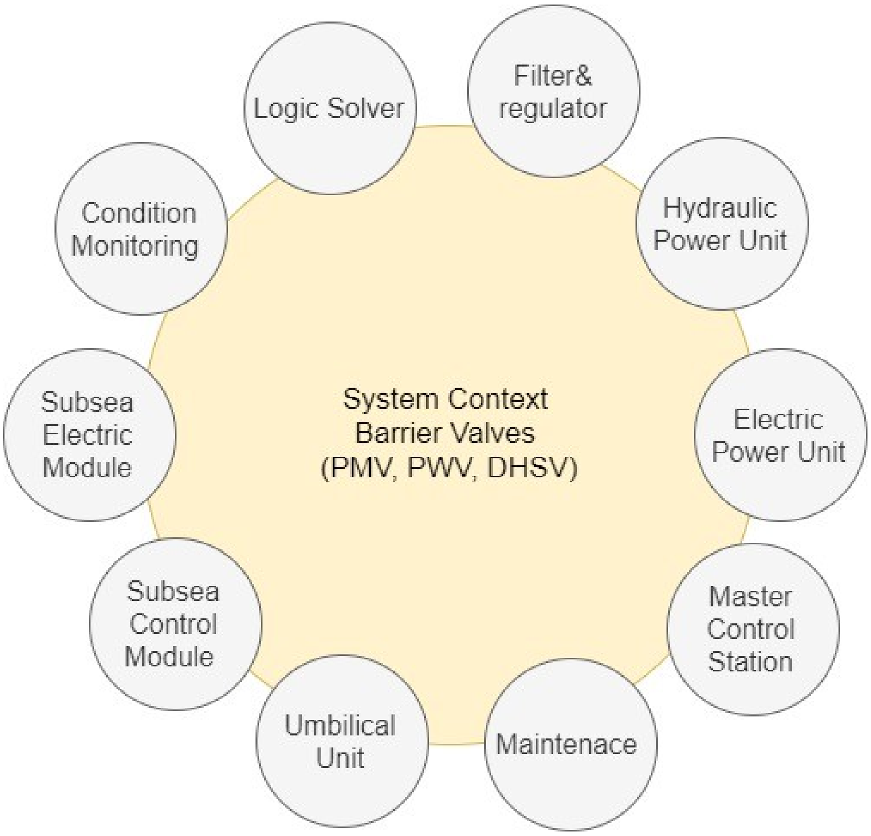


Figure 4.6: System Context of Barrier Valves

A system is composed of different components and conditions which are essential for the proper functioning to obtain the desired objective and goals, as shown above in Fig 4.6, such as Subsea Control Module, Hydraulic Power Unit, Master control Station ,Umbilical, Logic solver, Condition monitoring and Filter regulator. However, Some parts of the system, such as Maintenance, are not directly interacted with it, and their absence may bring improper functioning or dis-utility of the system. Therefore, the support infrastructures are considered as the main element in the system context.

4.1.5 System Hierarchy

Figure 4.7 below provides illustrative information regarding the System of the System, which is addressing the ESD valve. The main objective of the figure to show

how system activities start from the top-level and descents until the components level. The end of the figure depicts the components which are essential for the functioning of the valve. But it is included other part of the system which controls the valves, such as SCM and MCS.

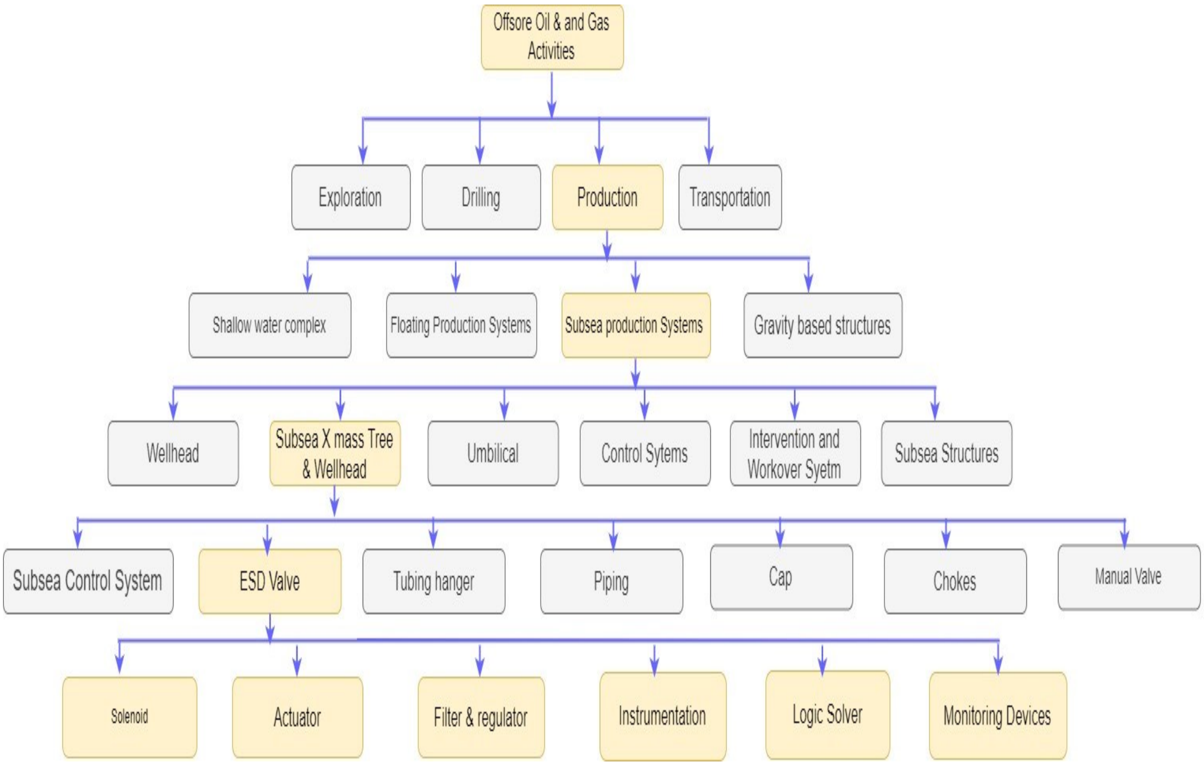


Figure 4.7: Hierarchy of the Complete System

4.1.6 Operating Use Case Scenario of Barrier Valves

Considering the operating use case scenario, the operator requests the first prerequisites for operation. After that, the system permissiveness is checked to ensure that the valves can operate when demand occurs. The checking permissiveness is maintained to be sure that; Actuator pressure level is Ok, the Supply flow level is Ok, the Return pressure level is Ok, Return flow level is Ok. Additional Hydraulic flow is checked from HPU, where hydraulic flow supply begins from, to ensure that will not be any issues related to flow supply during demands required. The received data from the system is displayed on the screen in the control room. Subsequently, the valve is turned on and sending the signal to the Subsea control module to activate a valve. While the system operates, all mentioned parameters monitored consequently. This scenario depicts with the help of a sequential diagram, as shown in Figure 4.8.

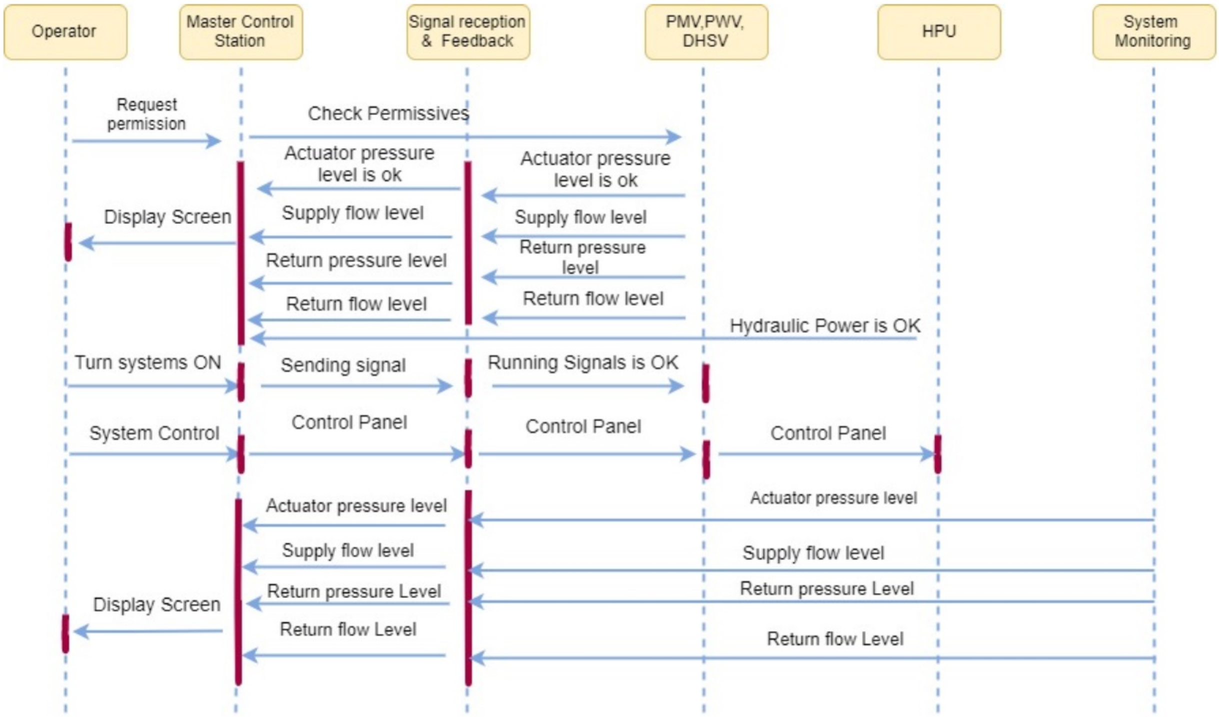


Figure 4.8: Operating Use Case Scenario Sequential Diagram

The same process is explained below with the inter-relationship, identifying the inputs and outputs with supporting mechanism and controls.

The Barrier valves' control system is divided into two, the Topside control system and the Subsea control system. The Topside has main subsystems, such as MCS, HPU, EPU. But the Subsea system is different from Topside and covers the main subsystem as the Subsea control module (SCM). Such System is operated from Topside by an operator.

The topside control system controls the barrier valves on the Xmass tree and Wellhead. The system starts with inputs from the Operator ”open or close the valve” and sends signals to the Master control station that provides complete control and monitoring of Barrier valves.The received signal is sent to further, to the Electronic power unit that empowers the Subsea control module with power supply. All gathered data (e.g., Actuator pressure level, Supply flow level, Return pressure level, Return flow level) from different sensors are collected in the Subsea control module. That is later transforming gathered data to the Master control station. The system is supported by different Auxiliary components controlled by the Subsea control module. While the overall system is being monitored through inputs from different packages, including Condition Monitoring, etc. The loop is finally closed with inputs from these functions to Main Control. Figure 4.9 depicts system inputs and outputs.

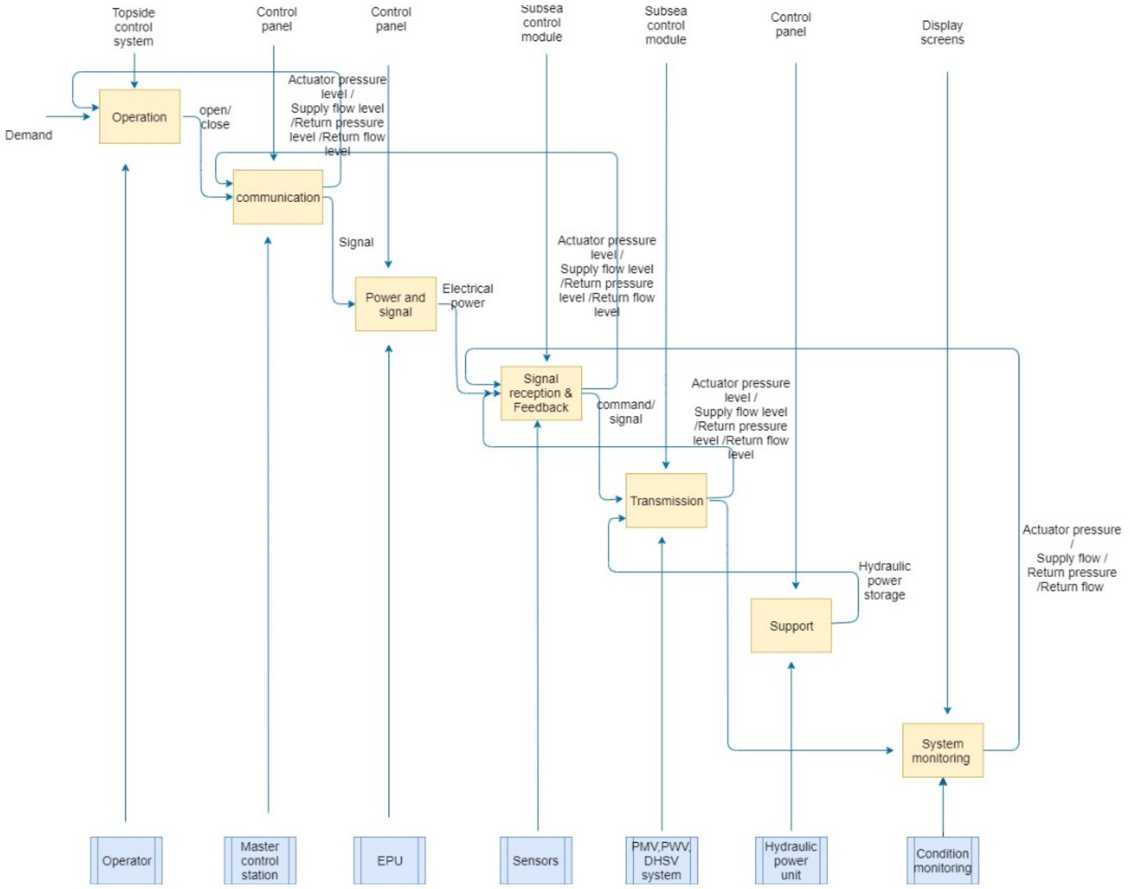


Figure 4.9: IDEF-Operating Use Case Scenario Working Conditions of Barrier Valves

4.1.7 Monitoring Use Case Scenario of Barrier Valves

Below described is the monitoring use-case scenario for PMV, PWV, and DHSV; it deals with the continuous monitoring of PMV, PWV, and DHSV. In the starting , the operator inputs reference data/ values to the control system, that monitors different valves parameters (like Supply flow level, Actuator pressure and Return pressure level, etc.) and analyze. The system continues iteratively as long as the values fall within the prescribed limits and notify an alarm or initiate tripping for necessary checks, which means that the operator needs additional check the data warehouse to be sure; if the system within limits when any abnormality is detected.

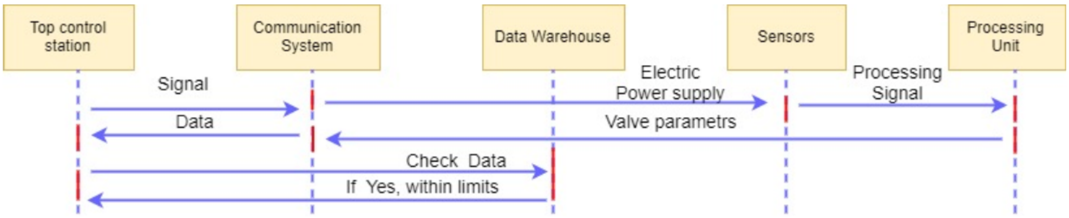


Figure 4.10: Monitoring Use Case Scenario Sequential Diagram Barrier Valves

The same process is explained below with the inter-relationship, identifying the inputs and outputs with supporting mechanism and controls.

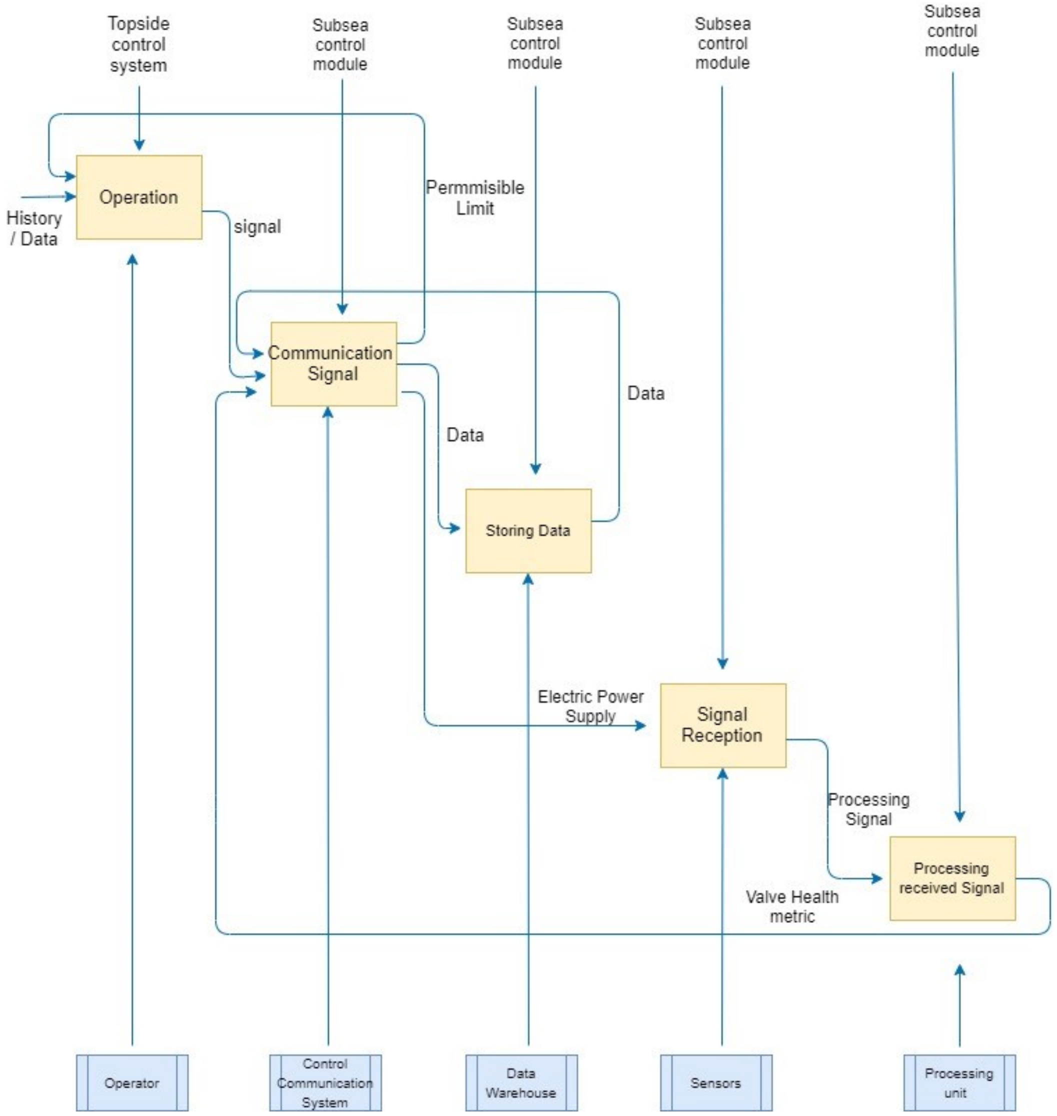


Figure 4.11: IDEF -Monitoring Diagram Barrier Valves

The below IDEF diagram describes the Monitoring Use Case that deals with Operation based on respective controls from different Sensors. The valve Control (Subsea control module) receives these signals from various sensors, and then the signal processes further to Topside control via the control communication system station. The valve performance is monitored based on pre-defined parameters, and these are then continuously analyzed against set limits generating specific alarm and trips. The operation personnel may access the data warehouse to gather additional information regarding the particular condition that gave rise to the alarm condition. If the valve parameters are out of setpoint, then maintenance action should be taken into consideration.

4.1.8 Testing Use Case Scenario of Barrier Valves

Below describes the Testing use case scenario of Barrier valves; It starts with a notification from Condition monitoring for planned testing, that is carried out by testing personnel. If the results are satisfactory, the systems update/notified;whereas, for any abnormalities, a work order is created for maintenance. Then the maintenance is performed after ordering necessary spares (as required), and the testing team is informed of the repair, who again re-tests and verifies the repair for satisfaction and closes work order accordingly.

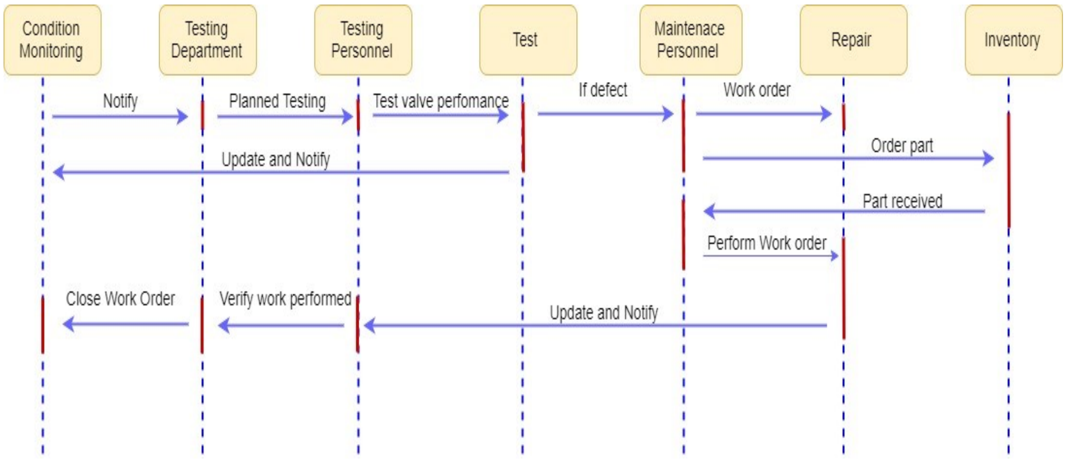


Figure 4.12: Testing Use Case Scenario Sequential Diagram Barrier valves

The same process is explained below with the inter-relationship, identifying the inputs and outputs with supporting mechanism and controls.

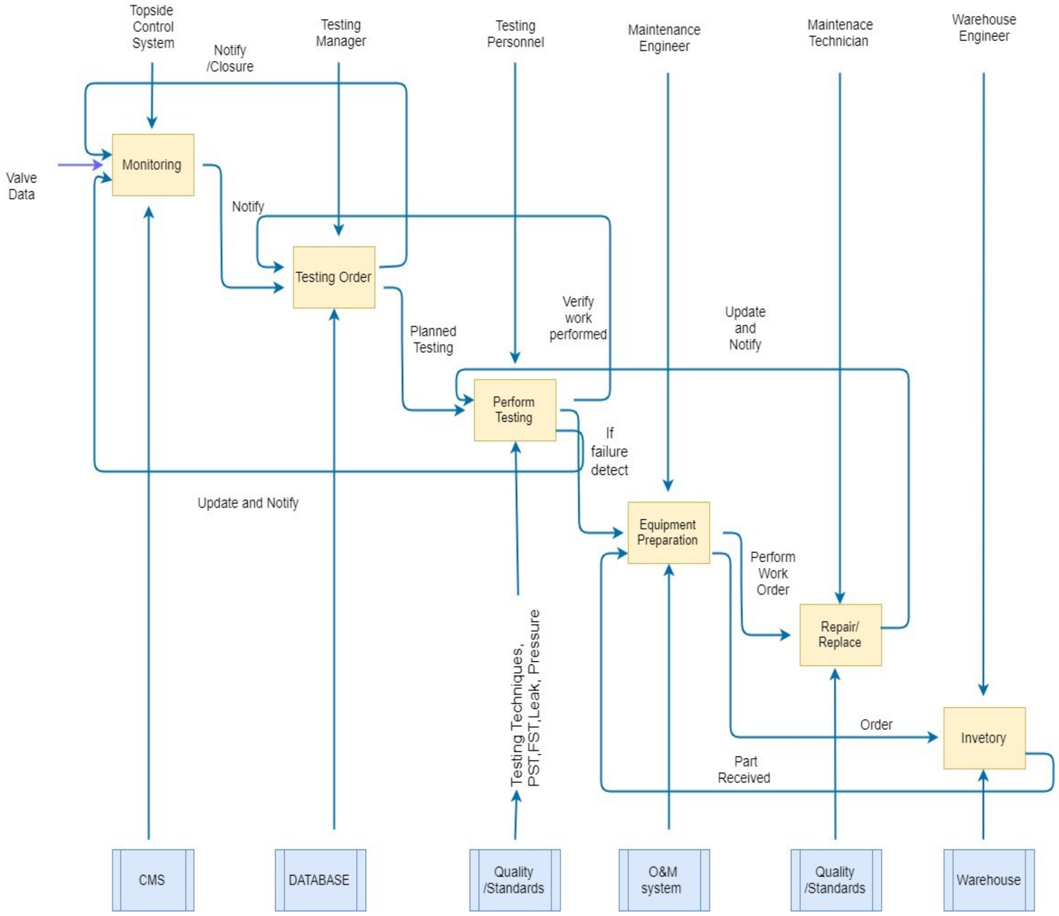
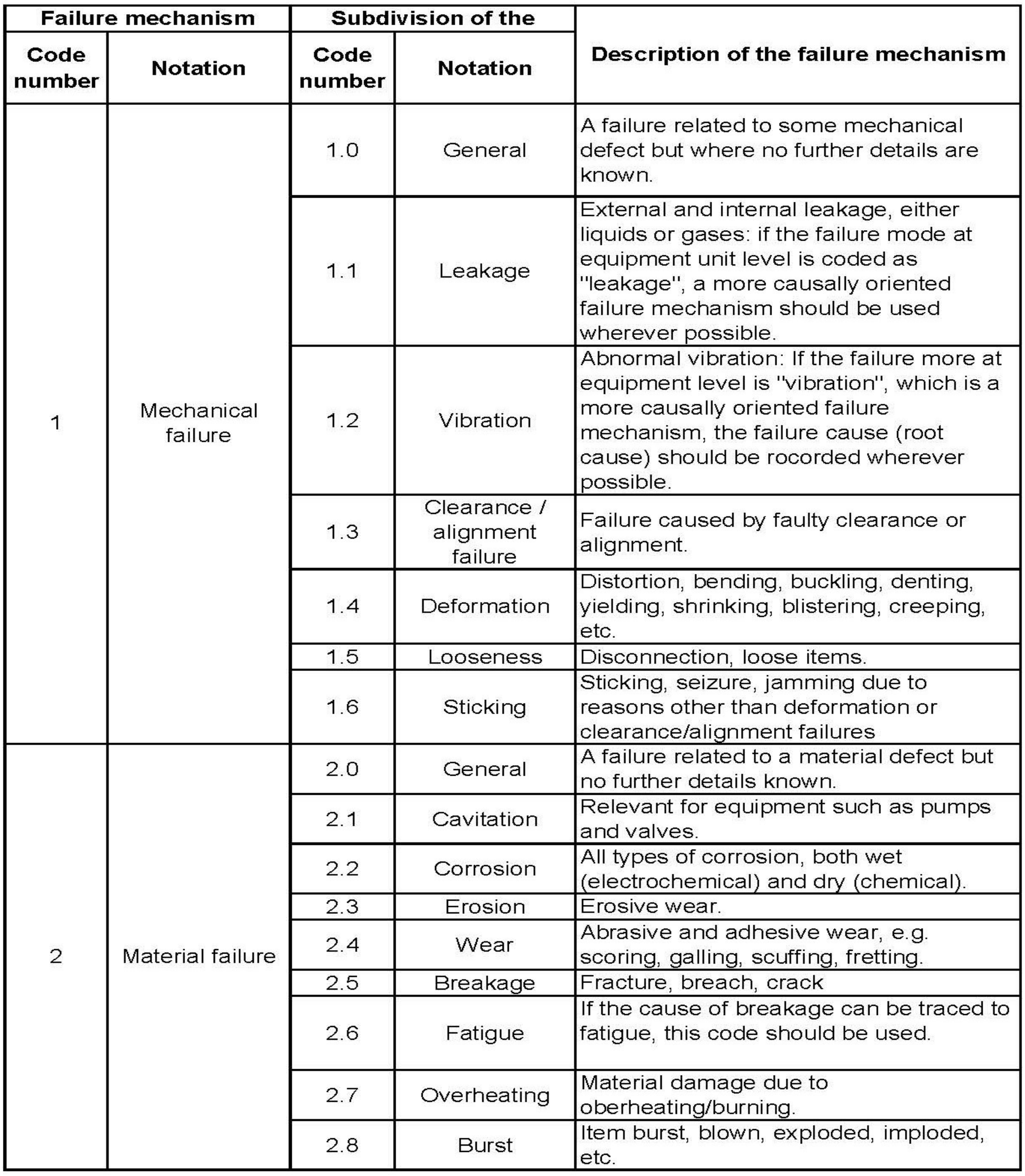


Figure 4.13: IDEF- Testing Diagram Barrier valves

The system is being continuously monitored through a CMS; and notifications are generated as per Database for Planned testing, followed by respective Testing as per implied techniques. With the results under limits, the same is notified back and closed in the system; while, in event of any abnormalities, the trail is followed by respective maintenance works as per Standards, after possible ordering of Inventory. That is further Tested for verification and appropriate closure at the end.

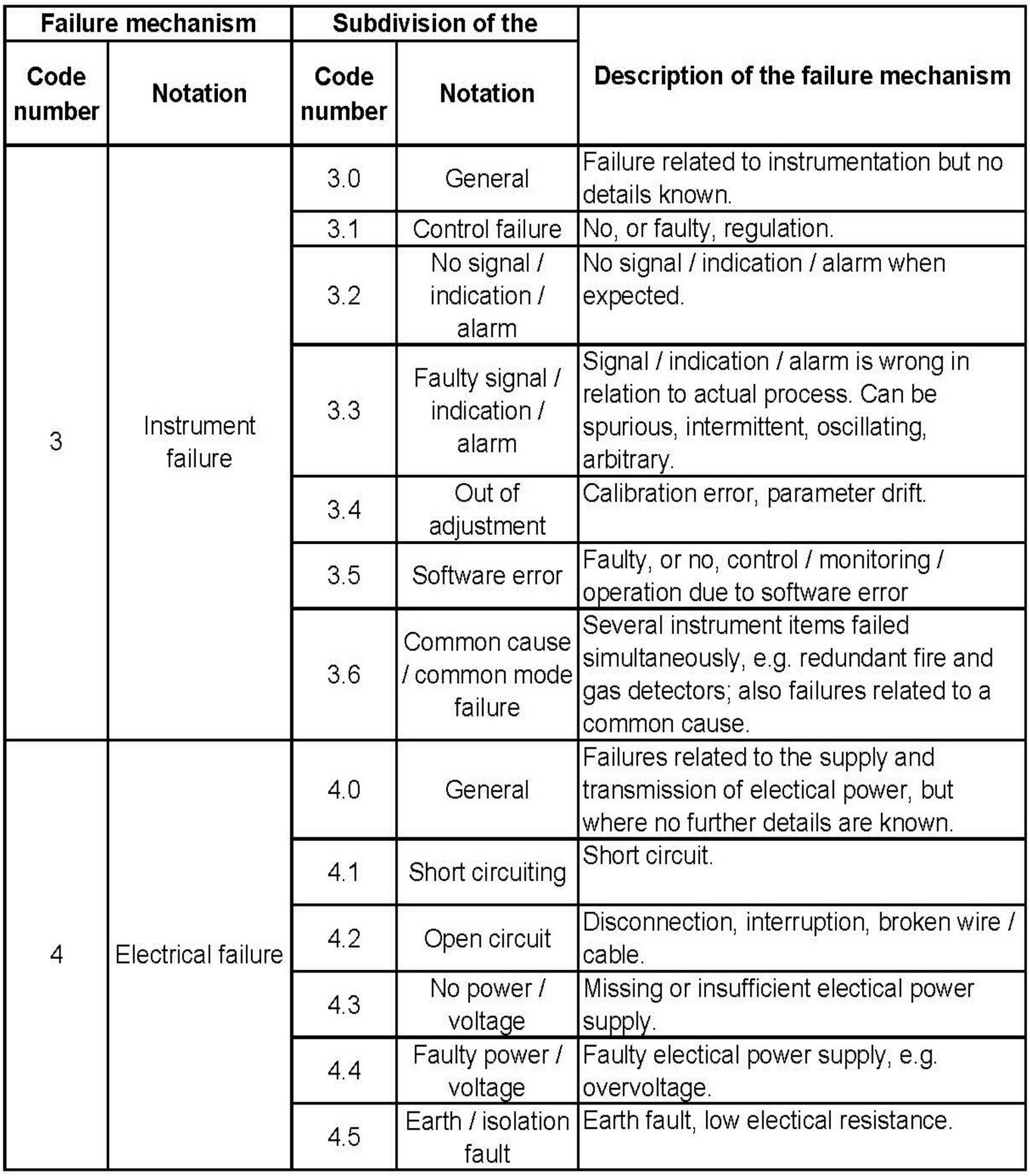
4.1.9 System Failure Mechanism

The data table of Failure Mechanisms shows the main causes of failure of ESD valves. The table will give us information according to its code number, which failure mechanism encountered on the valve mostly. This table is main the primary source for analyzing failure mechanisms according to interviewed engineers inputs from case study 2. Consequently ,elicited requirements will be presented in subsection 5.2 with respect to this table.



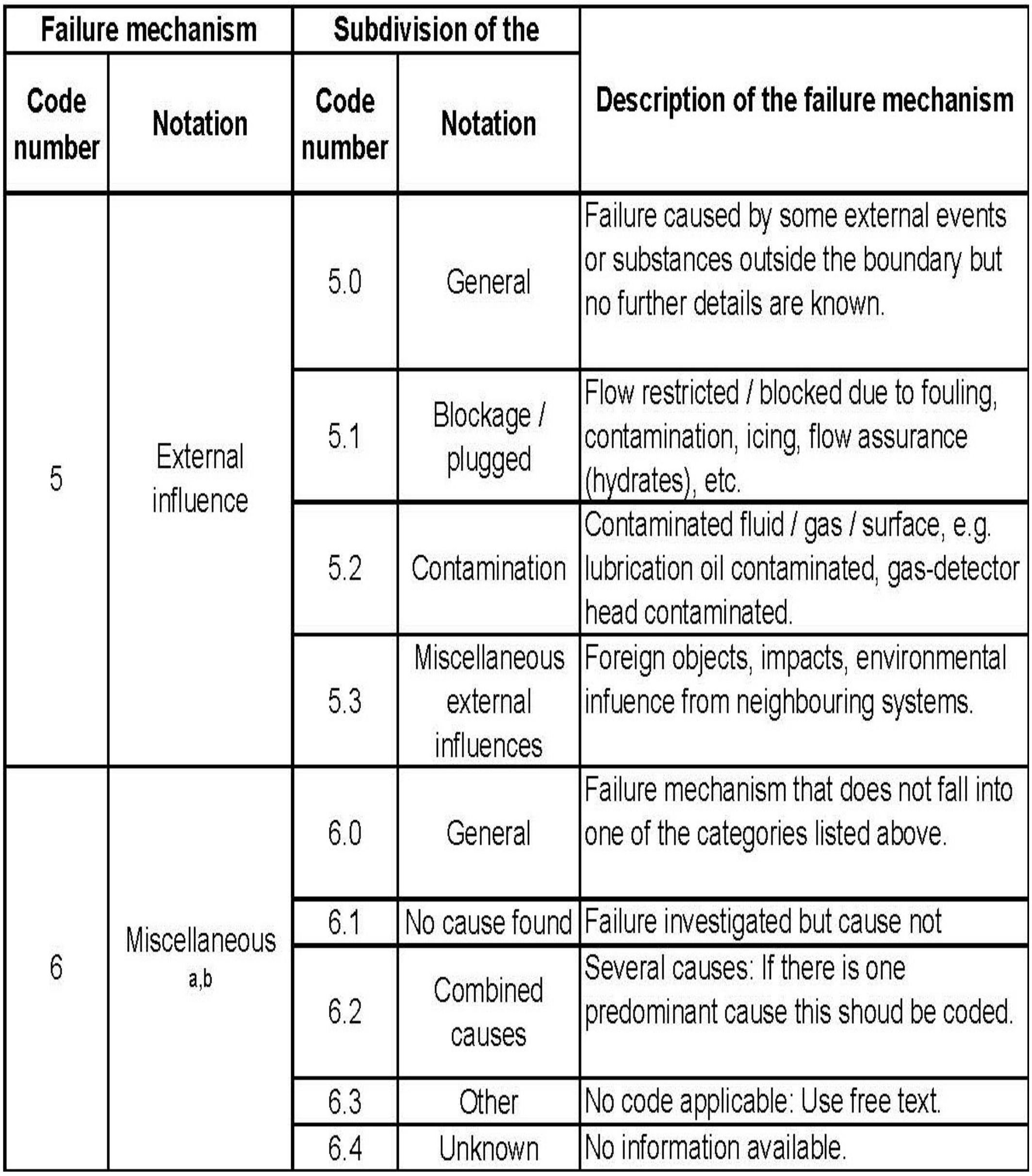
Failure mechanism		Subdivision of the		Description of the failure mechanism
Code number	Notation	Code number	Notation	
1	Mechanical failure	1.0	General	A failure related to some mechanical defect but where no further details are known.
		1.1	Leakage	External and internal leakage, either liquids or gases: if the failure mode at equipment unit level is coded as "leakage", a more causally oriented failure mechanism should be used wherever possible.
		1.2	Vibration	Abnormal vibration: If the failure more at equipment level is "vibration", which is a more causally oriented failure mechanism, the failure cause (root cause) should be rocorded wherever possible.
		1.3	Clearance / alignment failure	Failure caused by faulty clearance or alignment.
		1.4	Deformation	Distortion, bending, buckling, denting, yielding, shrinking, blistering, creeping, etc.
		1.5	Looseness	Disconnection, loose items.
		1.6	Sticking	Sticking, seizure, jamming due to reasons other than deformation or clearance/alignment failures
2	Material failure	2.0	General	A failure related to a material defect but no further details known.
		2.1	Cavitation	Relevant for equipment such as pumps and valves.
		2.2	Corrosion	All types of corrosion, both wet (electrochemical) and dry (chemical).
		2.3	Erosion	Erosive wear.
		2.4	Wear	Abrasive and adhesive wear, e.g. scoring, galling, scuffing, fretting.
		2.5	Breakage	Fracture, breach, crack
		2.6	Fatigue	If the cause of breakage can be traced to fatigue, this code should be used.
		2.7	Overheating	Material damage due to oberheating/burning.
		2.8	Burst	Item burst, blown, exploded, imploded, etc.

Table 4.2: Failure Mechanism [9]



Failure mechanism		Subdivision of the		Description of the failure mechanism
Code number	Notation	Code number	Notation	
3	Instrument failure	3.0	General	Failure related to instrumentation but no details known.
		3.1	Control failure	No, or faulty, regulation.
		3.2	No signal / indication / alarm	No signal / indication / alarm when expected.
		3.3	Faulty signal / indication / alarm	Signal / indication / alarm is wrong in relation to actual process. Can be spurious, intermittent, oscillating, arbitrary.
		3.4	Out of adjustment	Calibration error, parameter drift.
		3.5	Software error	Faulty, or no, control / monitoring / operation due to software error
		3.6	Common cause / common mode failure	Several instrument items failed simultaneously, e.g. redundant fire and gas detectors; also failures related to a common cause.
4	Electrical failure	4.0	General	Failures related to the supply and transmission of electical power, but where no further details are known.
		4.1	Short circuiting	Short circuit.
		4.2	Open circuit	Disconnection, interruption, broken wire / cable.
		4.3	No power / voltage	Missing or insufficient electical power supply.
		4.4	Faulty power / voltage	Faulty electical power supply, e.g. overvoltage.
		4.5	Earth / isolation fault	Earth fault, low electical resistance.

Table 4.3: Failure Mechanism (continued), [9]

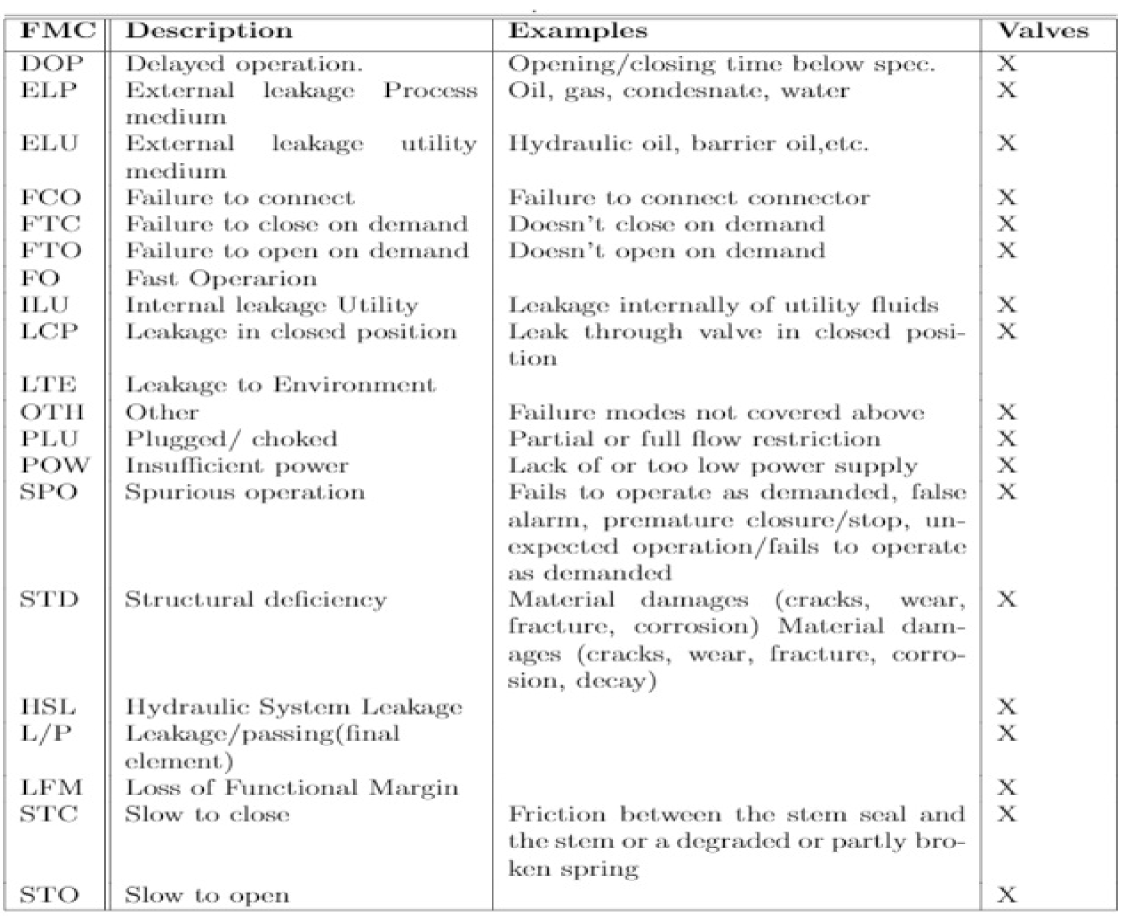


Failure mechanism		Subdivision of the		Description of the failure mechanism
Code number	Notation	Code number	Notation	
5	External influence	5.0	General	Failure caused by some external events or substances outside the boundary but no further details are known.
		5.1	Blockage / plugged	Flow restricted / blocked due to fouling, contamination, icing, flow assurance (hydrates), etc.
		5.2	Contamination	Contaminated fluid / gas / surface, e.g. lubrication oil contaminated, gas-detector head contaminated.
		5.3	Miscellaneous external influences	Foreign objects, impacts, environmental infuence from neighbouring systems.
6	Miscellaneous a,b	6.0	General	Failure mechanism that does not fall into one of the categories listed above.
		6.1	No cause found	Failure investigated but cause not
		6.2	Combined causes	Several causes: If there is one predominant cause this shoud be coded.
		6.3	Other	No code applicable: Use free text.
		6.4	Unknown	No information available.

Table 4.4: Failure Mechanism (continued), [9]

4.1.10 System Failure Modes

The ESD valves can fail in various ways in the subsea Xmass tree and Wellhead. For instance, the valve can function spuriously (also known as spurious trip), or it can fail to function etc. Table 4.5 below describes all possible failure modes of ESD valves. The furnished data was gathered from different sources, such as OREDA, BS EN ISO 14224, and SA-TR96.05.01.



FMC	Description	Examples	Valves
DOP	Delayed operation.	Opening/closing time below spec.	X
ELP	External leakage Process medium	Oil, gas, condesnate, water	X
ELU	External leakage utility medium	Hydraulic oil, barrier oil,etc.	X
FCO	Failure to connect	Failure to connect connector	X
FTC	Failure to close on demand	Doesn't close on demand	X
FTO	Failure to open on demand	Doesn't open on demand	X
FO	Fast Operarion		
ILU	Internal leakage Utility	Leakage internally of utility fluids	X
LCP	Leakage in closed position	Leak through valve in closed position	X
LTE	Leakage to Environment		
OTH	Other	Failure modes not covered above	X
PLU	Plugged/ choked	Partial or full flow restriction	X
POW	Insufficient power	Lack of or too low power supply	X
SPO	Spurious operation	Fails to operate as demanded, false alarm, premature closure/stop, unexpected operation/fails to operate as demanded	X
STD	Structural deficiency	Material damages (cracks, wear, fracture, corrosion) Material damages (cracks, wear, fracture, corrosion, decay)	X
HSL	Hydraulic System Leakage		X
L/P	Leakage/passing(final element)		X
LFM	Loss of Functional Margin		X
STC	Slow to close	Friction between the stem seal and the stem or a degraded or partly broken spring	X
STO	Slow to open		X

Table 4.5: Subsea Barrier Valves Failure Mode, from [8][27][44]

Although all possible failure modes are furnished in table 5.2, only some of them are considered as vital failure modes for Safety shutdown valves in the Subsea Xmas tree and Wellhead [41]. And these main failure modes are as following:

-*Failure to close on command* (FTC): This failure mode may be caused by a broken spring, blocked return line for the hydraulic fluid, too high friction between the stem and the stem seal, too high friction between the gate and the seats, or by sand, debris, or hydrates in the valve cavity.

-*Fail to open on command* (FTO): When the valve is closed, it may fail to reopen. Possible causes may be leakage in the control line, excessive high friction between the stem seals and the stem, high friction between the gate and the seats, and sand, debris, or hydrates in the valve cavity.

-*Leakage (through the valve) in closed position* (LCP): This failure mode is mainly caused by corrosion and/or erosion on the gate or the seat. It may also be caused by misalignment between the gate and the seat.

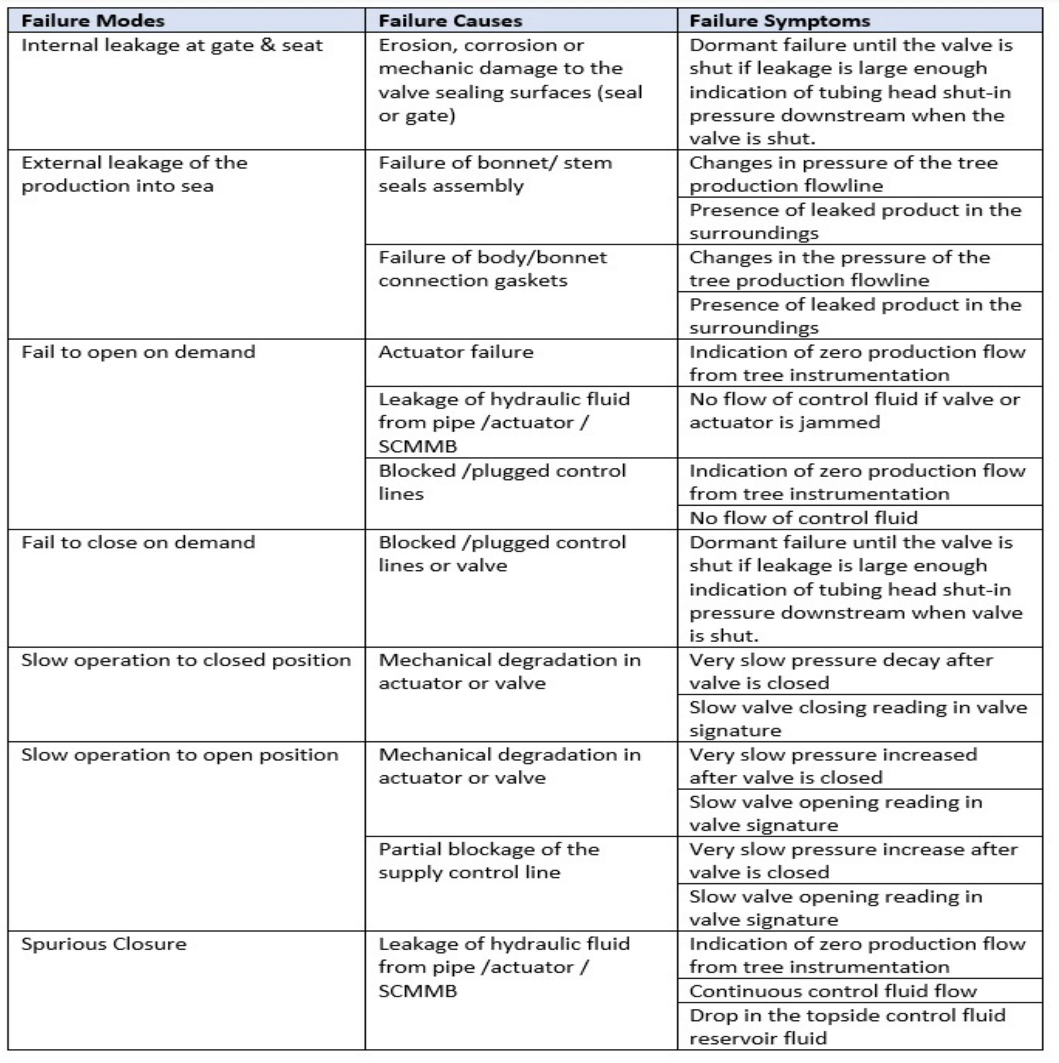
-*Spurious trip* (ST). This failure mode occurs when the valve closes without a closing signal. It is caused by a failure in the hydraulic system or a leakage in the supply line from the control system to the valve.

-*Closing too slowly* (CTS). The process may require the valve to close within a certain time interval (e.g., 10 seconds) after the ESD signal has been given. Possible causes may be friction between the stem seal and the stem or a degraded or partly broken spring.

4.1.11 System Failure Symptoms

In Subsea, failing valve can cause catastrophic damage to the environment. However, identification first failure symptoms and preventing a failing valve can help to avoid these types of situations. Failing valves will express signs at the first hint of trouble. For example, failing PMV will start with notification very slow pressure decay after the valve is closed. The situation is referred to as “ Slow operation to closed position “ and is caused by mechanical degradation in actuator or valve. Slow to close can lead to severe damage if the intervention will not be done on time. Generally speaking, it is essential to consider all possible failure symptoms to mitigate catastrophic damage. For this reason, all possible symptoms of PMV, PWV, and DHSV are furnished in table 4.6.

Sometimes it is not so obvious to identify the symptoms that reflect failure modes. Designers of the CM system have to think “outside the box” to determine those measurements that will provide the information needed about the health of the system



Failure Modes	Failure Causes	Failure Symptoms
Internal leakage at gate & seat	Erosion, corrosion or mechanic damage to the valve sealing surfaces (seal or gate)	Dormant failure until the valve is shut if leakage is large enough indication of tubing head shut-in pressure downstream when the valve is shut.
External leakage of the production into sea	Failure of bonnet/ stem seals assembly	Changes in pressure of the tree production flowline
		Presence of leaked product in the surroundings
	Failure of body/bonnet connection gaskets	Changes in the pressure of the tree production flowline
		Presence of leaked product in the surroundings
Fail to open on demand	Actuator failure	Indication of zero production flow from tree instrumentation
	Leakage of hydraulic fluid from pipe /actuator / SCMMB	No flow of control fluid if valve or actuator is jammed
	Blocked /plugged control lines	Indication of zero production flow from tree instrumentation
		No flow of control fluid
Fail to close on demand	Blocked /plugged control lines or valve	Dormant failure until the valve is shut if leakage is large enough indication of tubing head shut-in pressure downstream when valve is shut.
Slow operation to closed position	Mechanical degradation in actuator or valve	Very slow pressure decay after valve is closed
		Slow valve closing reading in valve signature
Slow operation to open position	Mechanical degradation in actuator or valve	Very slow pressure increased after valve is closed
		Slow valve opening reading in valve signature
	Partial blockage of the supply control line	Very slow pressure increase after valve is closed
		Slow valve opening reading in valve signature
Spurious Closure	Leakage of hydraulic fluid from pipe /actuator / SCMMB	Indication of zero production flow from tree instrumentation
		Continuous control fluid flow
		Drop in the topside control fluid reservoir fluid

Table 4.6: Subsea Barrier Valves Failure Symptoms

4.2 Data Collection

4.2.1 Case Study 1: ConocoPhillips

This section provides testing requirements and data for this section have gathered from Kvaeven Anna's case study [31] that conducted with ConocoPhillips. The study was performed in Greater Ekofisk Area that mainly operated by ConocoPhillips.

Additionally,the primary testing requirements for this thesis have been elicitated from local standards (NOG 070 and Norsok D010). Besides the standards, the operator requirements have been elicitated from a case study that was performed with ConocoPhillips. The elicitated requirement from standard and Conocophilihs are the main inputs to define how much barrier testing requirements are clear for the company, and if they comply with standards. The testing requirements from standards have furnished in the Appendix A , and they are the main discussion topics of this thesis.

The Greater Ekofisk Area

The Greater Ekofisk Area (GEA) is located in the southern North Sea, 300 km southwest of Stavanger. The sea depth in the area is 70 – 80 meters. There are several producing fields within the GEA, see figure below. Component operational data for the case study SIF's final elements are gathered by Kvaevan Anna from wells on installations producing from the Ekofisk (Mike, Zulu) and Eldfisk (Sierra) fields.

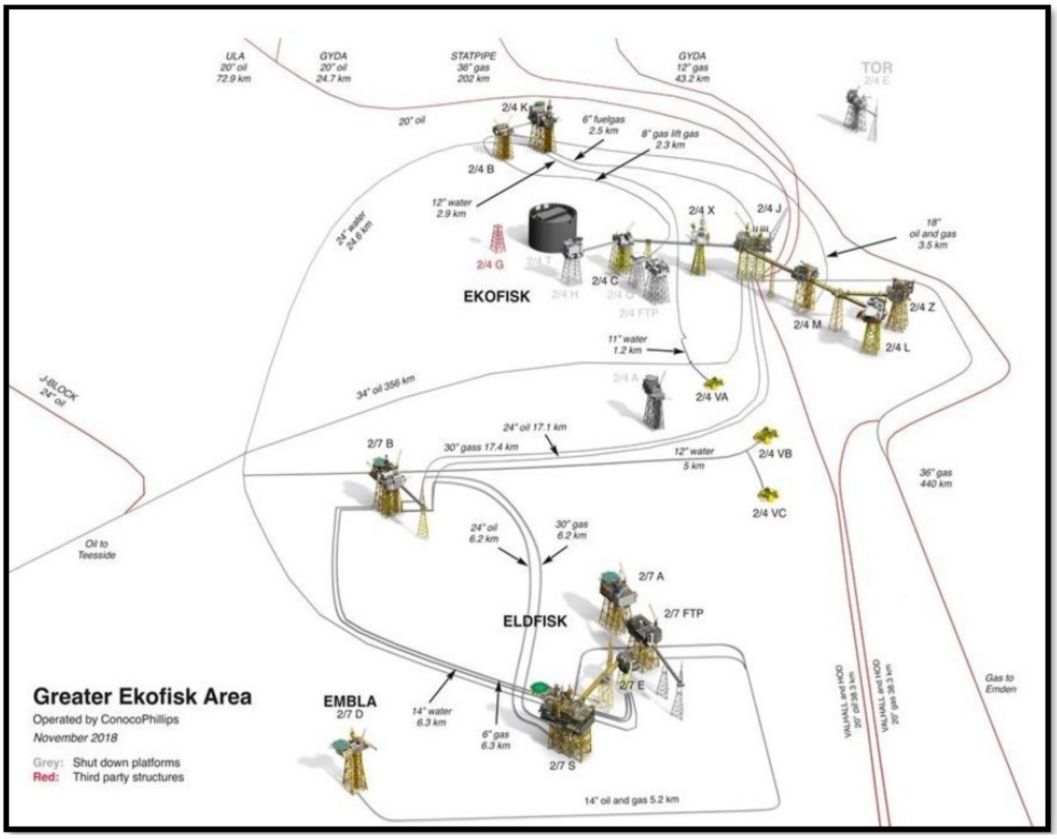


Figure 4.14: The Greater Ekofisk Area [31]

The EKOFISK FIELD

The Ekofisk field was explored in 1969 and started production in 1971, as the first field in Norwegian history. The reservoir is located at 3000m below sea level and produces both oil and gas [31].

The Mike and Zulu installations embraced in this study are part of The Ekofisk Complex, see figure below, on the central Ekofisk field[31]. Eko - Mike is a united production and process installation and was installed in 2005. Eko - Zulu is a united production and injection installation and was installed in 2013. Production wells on Mike produce mainly oil, whereas production wells on Zulu produce both oil and gas [31].

Figure 4.15: The Ekofisk complex [31]

The ElDFISK FIELD

The Eldfisk field is located in the North Sea approximately 10km south of the Ekofisk field and entered into production in 1979 [31]. The reservoir is located at 2700 – 2900m below sea level and produces mainly oil. The Eld - Sierra installation embraced in this study is part of the Eldfisk Complex in the Eldfisk field, see figure below. The Sierra entered into production in 2015. The wells on Sierra included in this study are oil production wells.

Figure 4.16: The ElDFISK Complex [31]

Several factors can affect can affect operd temperature (PT), well fluid content (Oil-Gas-Water), souring potential and scale potential. Consequently, these factors may also affect the lifespan of components.

According to Kvaevan [31], scale formation is a common problem in oil and gas production. As reservoir fluids move up the wellbore to the surface, pressure depletion and temperature changes in the well cause salts dissolved in the produced fluids, in particular water, to precipitate. This phenomenon is known as scale formation. As scale deposits on valves and other components in the well, it can affect their ability to function as intended, and high scale potential in wells is found out to shorten the lifetime of components. Issues with scale formation are found out in some wells on all three installations that included in this study, but mainly on Eko - Mike due to early water break through from waterflooding.

Moreover, souring in the produced fluids can also reduce component lifetime. Souring is related to the content of hydrogen sulphide and other acidic substances, and as these substances are corrosive, it can cause components in the well to degrade earlier in their lifetime. In recent years, increased souring has been observed in both the Ekofisk and Eldfisk fields. As these substances are water – soluble, the increase is related to the onset of water injection in these fields. The highest contents of hydrogen sulphide are registered in the wells where waterflooding is most mature. Although all necessary actions have been taken by COPNO to keep corrosion under control, Souring yet remains the main issue that influences the reliability of components.

Because water breakthrough also increases the likelihood of scale, it can be hypothesised that some wells are more prone to both scale and corrosive environments. For example, on Eko – Mike, where particular scale issues are reportedly experienced due to early water break through, the operating environment may also be particularly corrosive, which will cause components in these wells to be subject to an overall higher degree of wear and tear than in "good wells", where these issues are not experienced.

Survivability of Components Data Provided by COPNO

The survivability plots below are preliminary reliability analyses of well barrier components in production that indicate COPNO's high component reliability for the PMW, PWV and DHSV of SIF. The data that was collected by Kvaeven and have been adapted for this thesis is according to the general impression of professionals at COPNO in terms of high reliability of components.

Survivability plots were provided by the COPNO Norway team. These plots were generated based on data collected from production wells on the Mike, Zulu and Sierra installations can be seen below in Figure 4.17 and Figure 4.18.

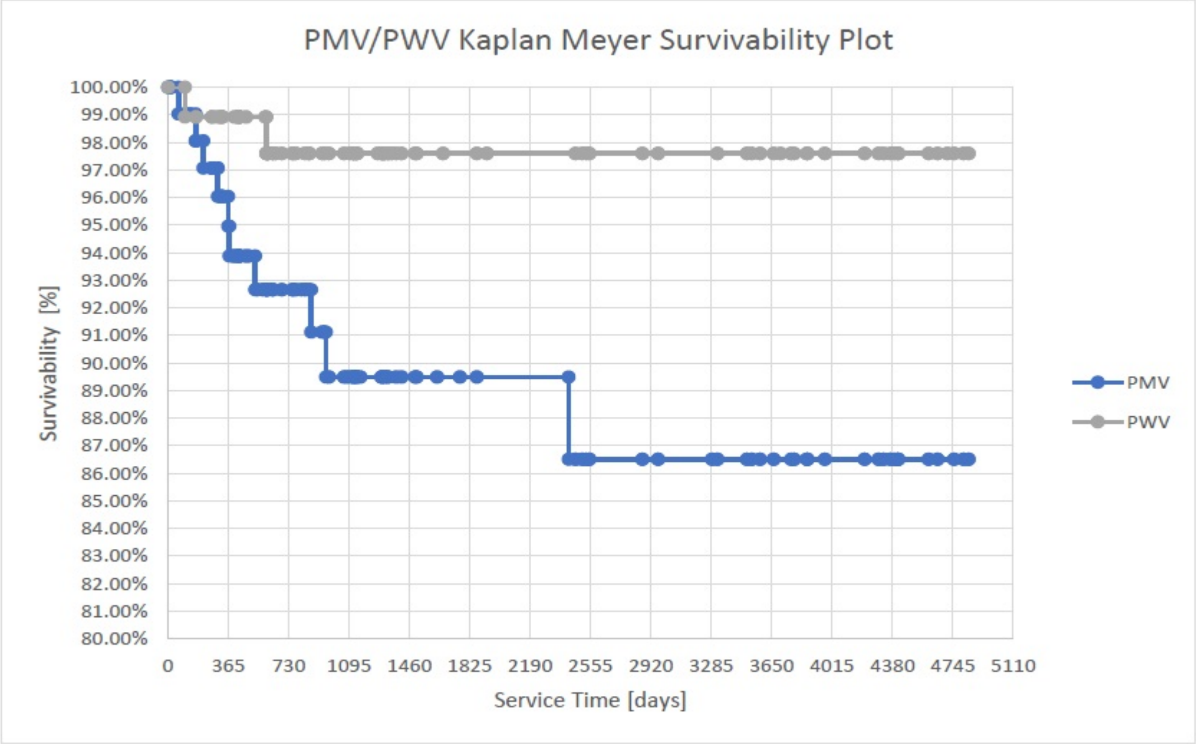


Figure 4.17: Kaplan Meyer Survivability plot of the PMV and PWV final elements of the SIF "Isolation of production bore in one topside well from the production manifold/flowline (ESD)". Courtesy of COPNO [31]

Figure 4.17 above describes the reliability of PMV and PWV. As can be seen from the plot, the reliability of the PMV does not fall below 98% until 214 days, whereas the PWV does not fall below 98% until after 598 days. From another Figure 4.18 below can be seen that earlier and frequent failure is experienced for DHSVs. But even for DHSV, the reliability of the component after six months is still at 80%.

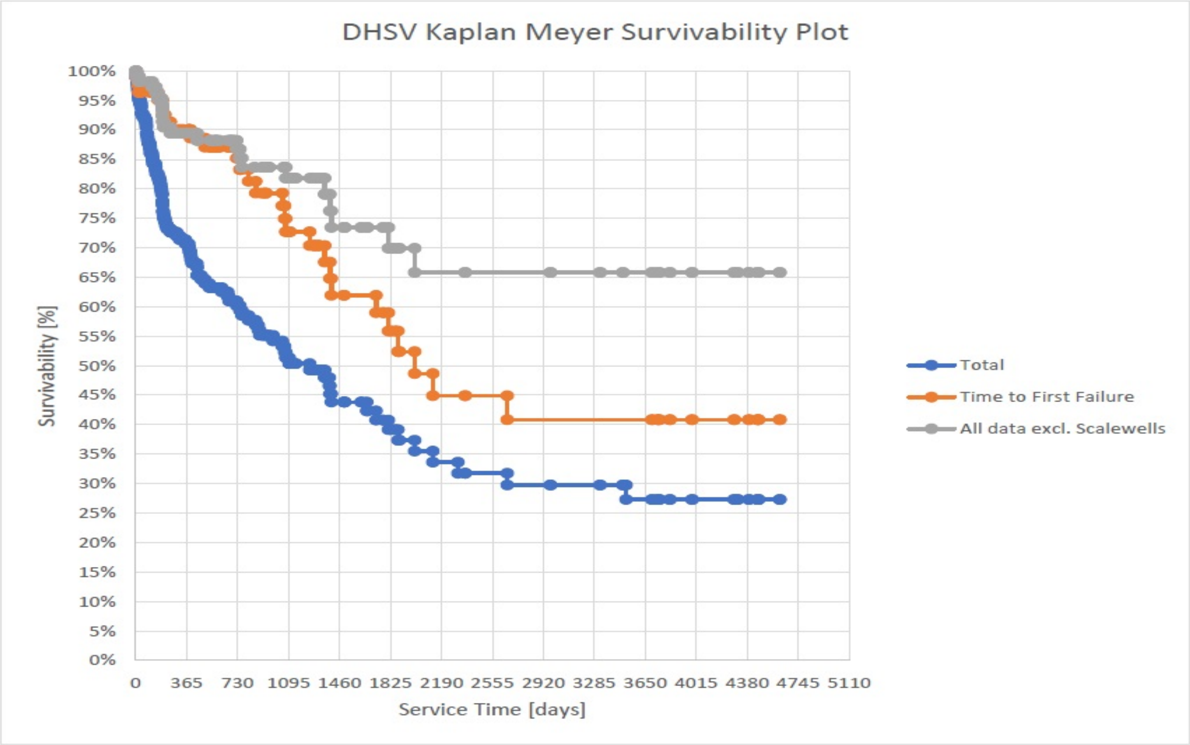


Figure 4.18: Kaplan Meyer survivability plot of the DHSV final element in the SIF “Isolation of production bore in one topside well from the production/manifold flowline (ESD)”. Courtesy of COPNO [31]

Thus, For testing these components at intervals of 1 month, lasting up to three and six months, is called into question based on the demonstrated reliability of the components during operation. As the proof tests require a significant investment of time and resources. It is in the interest of many operator companies as well as COPNO to find out whether it is possible to increase the planned proof test intervals in the maintenance program for the barrier components for wells, including PMV, PWV and DHSV.

Installed Component

The data was gathered from wells that were drilled between 2004 and 2008. Components were installed and used from 2005 to 2018. Test data recorded during this period of approximately 13.5 years.

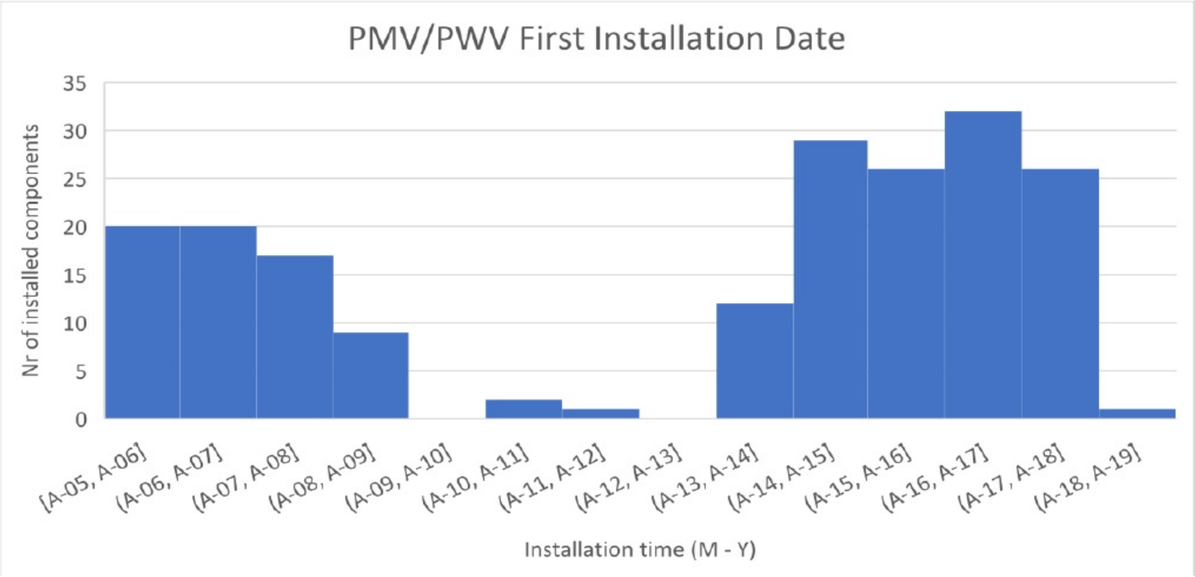


Figure 4.19: PMV and PWV installation dates [31]

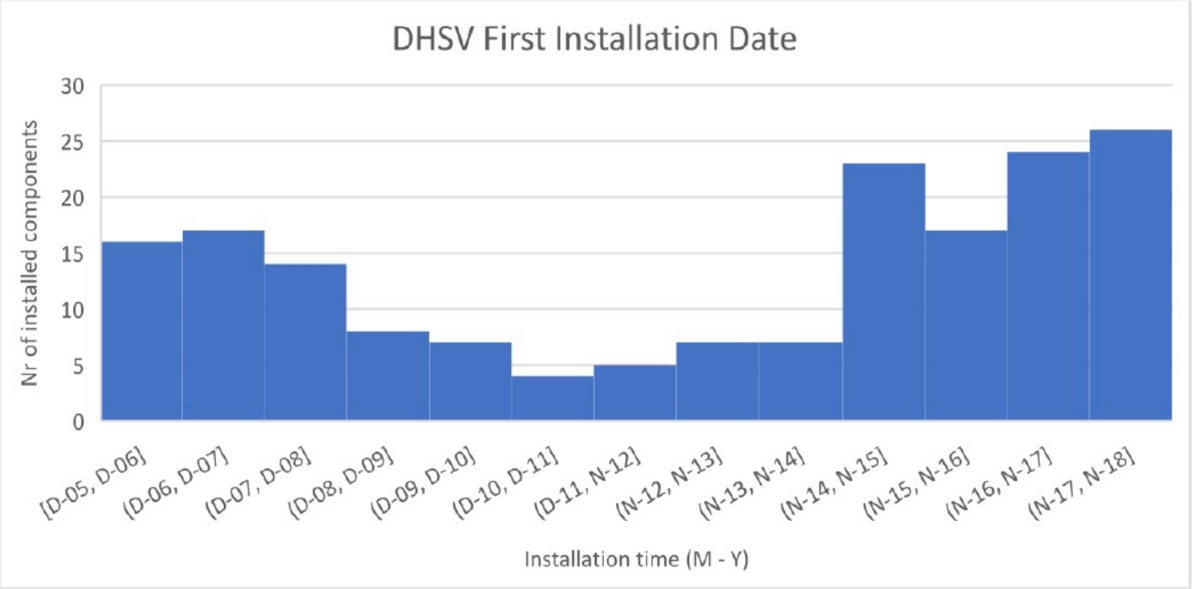


Figure 4.20: DHSV installation (first installation, no replacement [31]

NUMBER OF DU FAILURES

During the total observation period, the following number of DU component failures are registered:

- PMV : 9
- PWV : 2
- DHSV: 88

The registered number of DU failures for the DHSV compared to the PMV and PWV is striking. However, it is generally expected to be more operational problems and failures for the DHSV than valves further up the well, because DHSVs are subject to much harsher environments, with high pressures and temperatures, and abrupt pressure/temperature drops. These factors also increase the likelihood of well problems such as scale formation, which is generally a bigger problem for components further down the well than components higher up.

4.2.2 Case Study 2: Equinor, AkerBp, Spirit Energy and Maersk

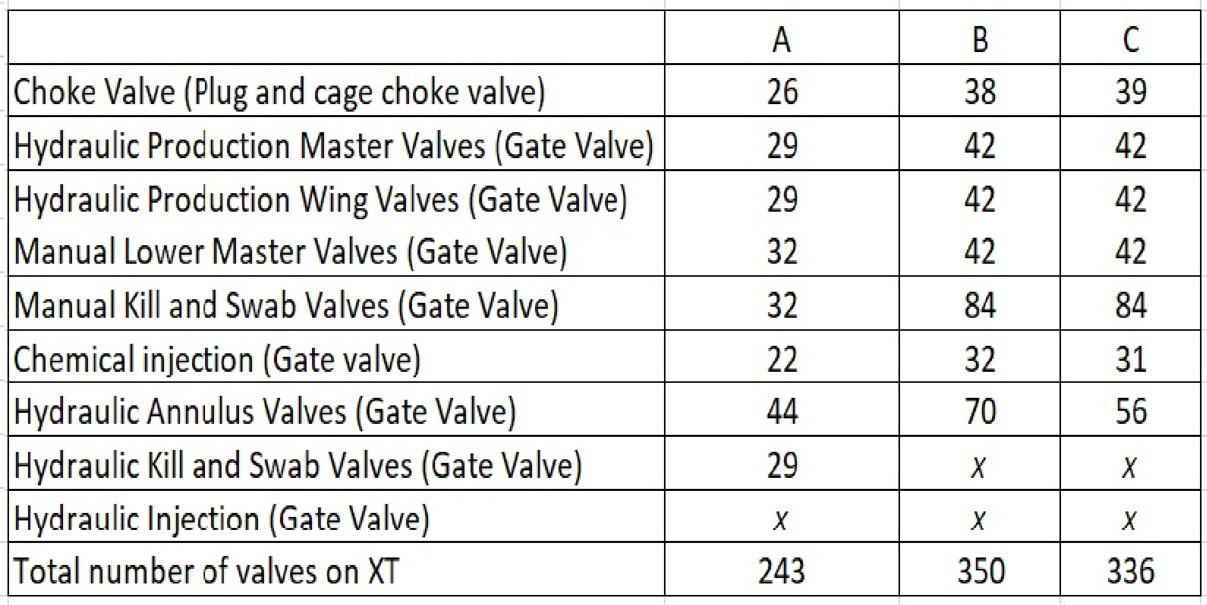
In this section, data was obtained from Shaipov case studies. These case studies were conducted as a series of interview-styled dialogues with OIMs, Drilling Supervisors, Well Intervention Supervisors, Maintenance Engineers, Wellhead operators, Drillers and Assistant drillers both on production platforms and drilling rigs. His data gives us an illustration of the failure trend for each valve type, specifically about barrier valves, such as PMV and PWV, that are located on XT. The data depicts the frequency of barrier valve failure over the past five years (2013-2018) along with their leading causes. Interviews were conducted the following drilling rigs/platforms:

- Island Innovator (Semi-Sub Drilling rig), Spirit Energy
- Gullfaks B (Production platform), Equinor
- Valhall DP (Production platform), AkerBP
- Maersk Invincible (Jack-up Drilling rig), Maersk

However, the names of the fields will remain anonymous in this thesis. This is because identification of fields was not performed in the reference text due to confidentiality agreements. Alphabetical placeholders are used in place of field names. These are:

- Field A
- Field B
- Field C

The table below depicts the number of functional locations of each valve in the Field A, B and C.



	A	B	C
Choke Valve (Plug and cage choke valve)	26	38	39
Hydraulic Production Master Valves (Gate Valve)	29	42	42
Hydraulic Production Wing Valves (Gate Valve)	29	42	42
Manual Lower Master Valves (Gate Valve)	32	42	42
Manual Kill and Swab Valves (Gate Valve)	32	84	84
Chemical injection (Gate valve)	22	32	31
Hydraulic Annulus Valves (Gate Valve)	44	70	56
Hydraulic Kill and Swab Valves (Gate Valve)	29	x	x
Hydraulic Injection (Gate Valve)	x	x	x
Total number of valves on XT	243	350	336

Table 4.7: Total installed valve comparison in Field A, B,C (2013-2018)

NUMBER OF FAILURES

Figure 4.21, 4.22 and 4.23 illustrate the number of failures of the in their respective fields between 2013 and 2018.

Field A

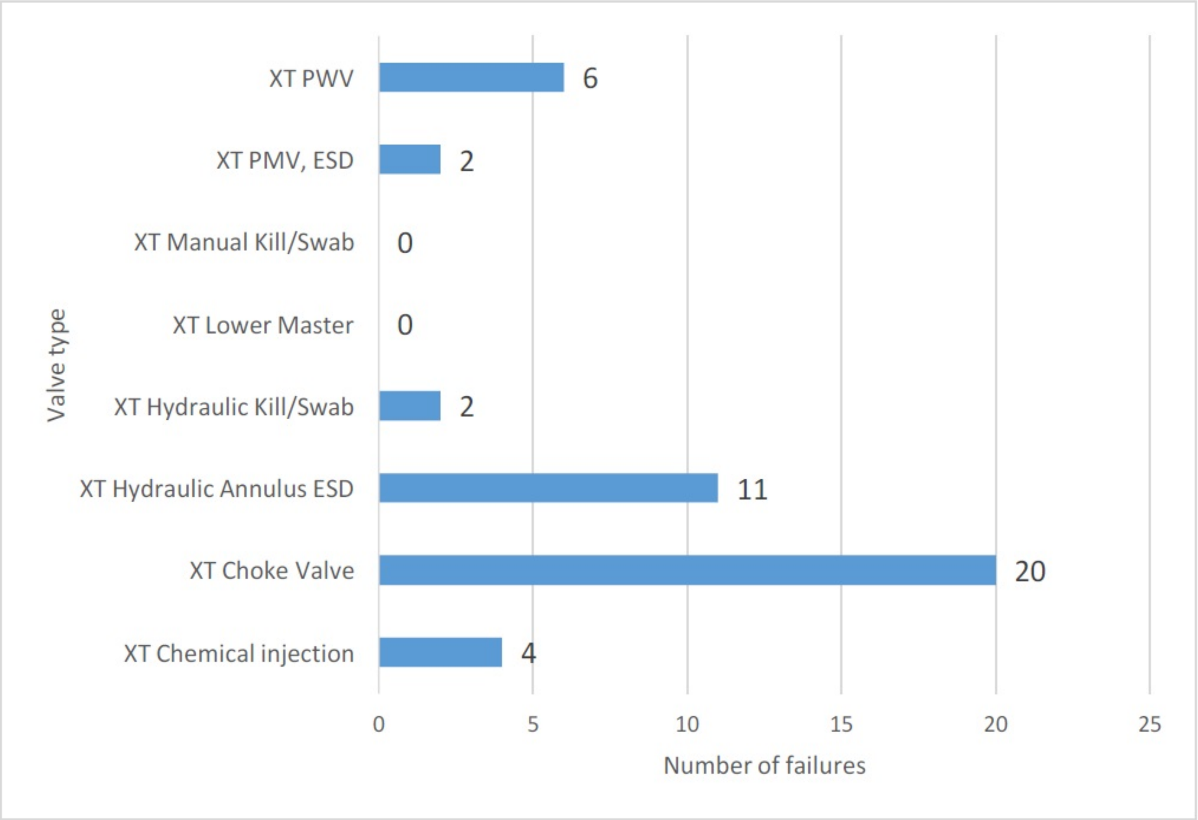


Figure 4.21: Number of valve failures on Field A (2013-2018) [43]

FIELD B

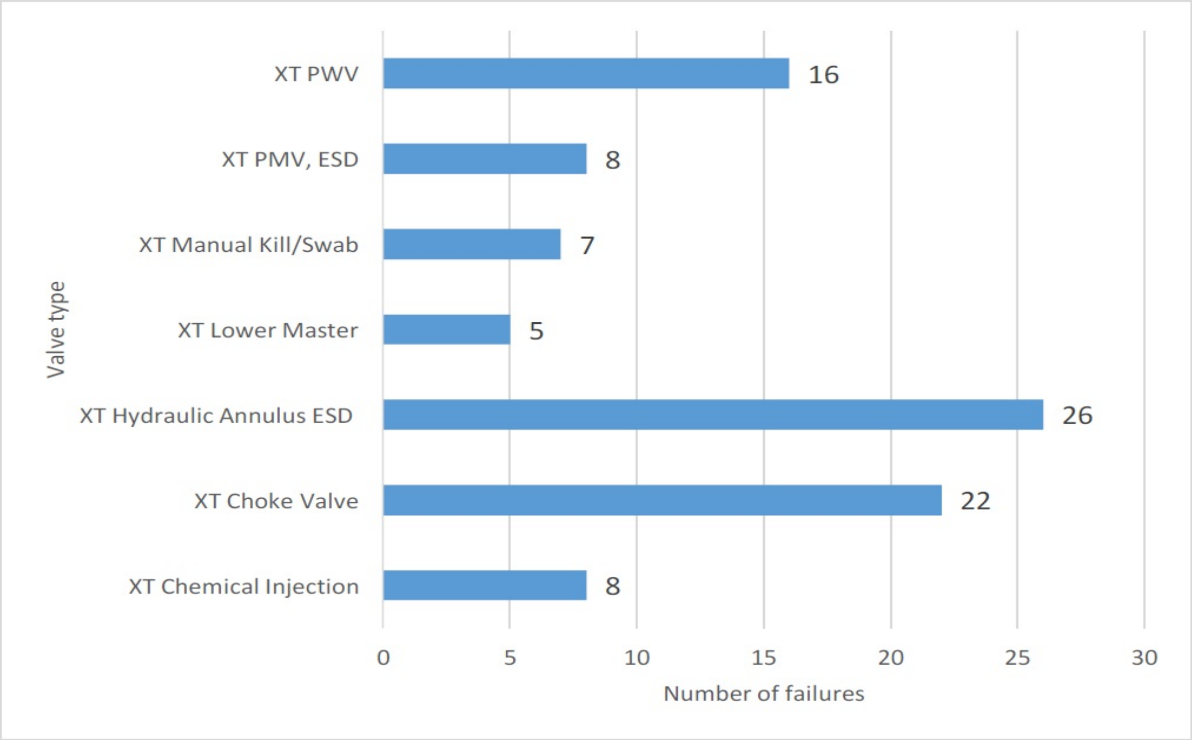


Figure 4.22: Number of valve failures on Field B (2013-2018) [43]

FIELD C

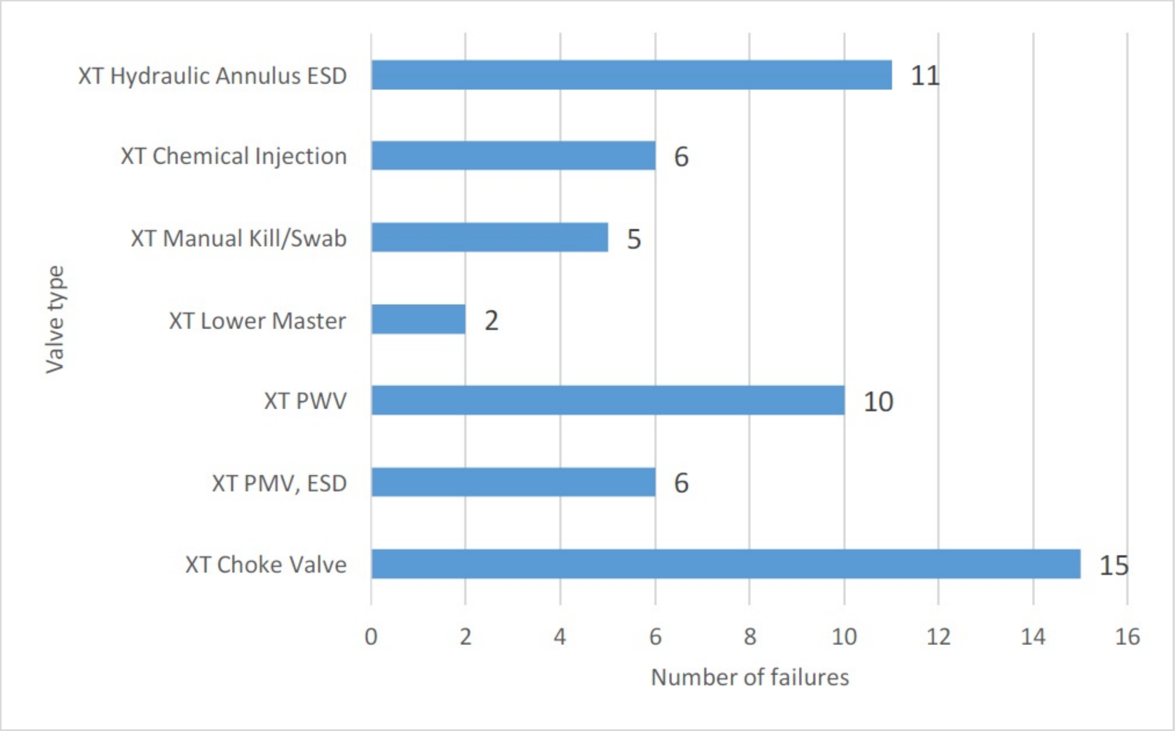


Figure 4.23: Number of XT valve failures on Field C (2013-2018) [43]

In field A and C choke valves show the highest frequency of failures and are closely followed by Hydraulic Annulus valves. In field B, Hydraulic Annulus valves fail the most with Choke valves coming in second. However, PMV and PWV valves are the focus of this thesis as these are the primary safety barriers on XT. In all three fields, PWV valves have the third highest number of failures. PMV valves have the third highest in field A and B, but the fourth in field C.

FAILURE RATE

Figure 4.24, 4.25 and 4.26 illustrate the failure rates of the aforementioned valves in their respective fields.

Field A

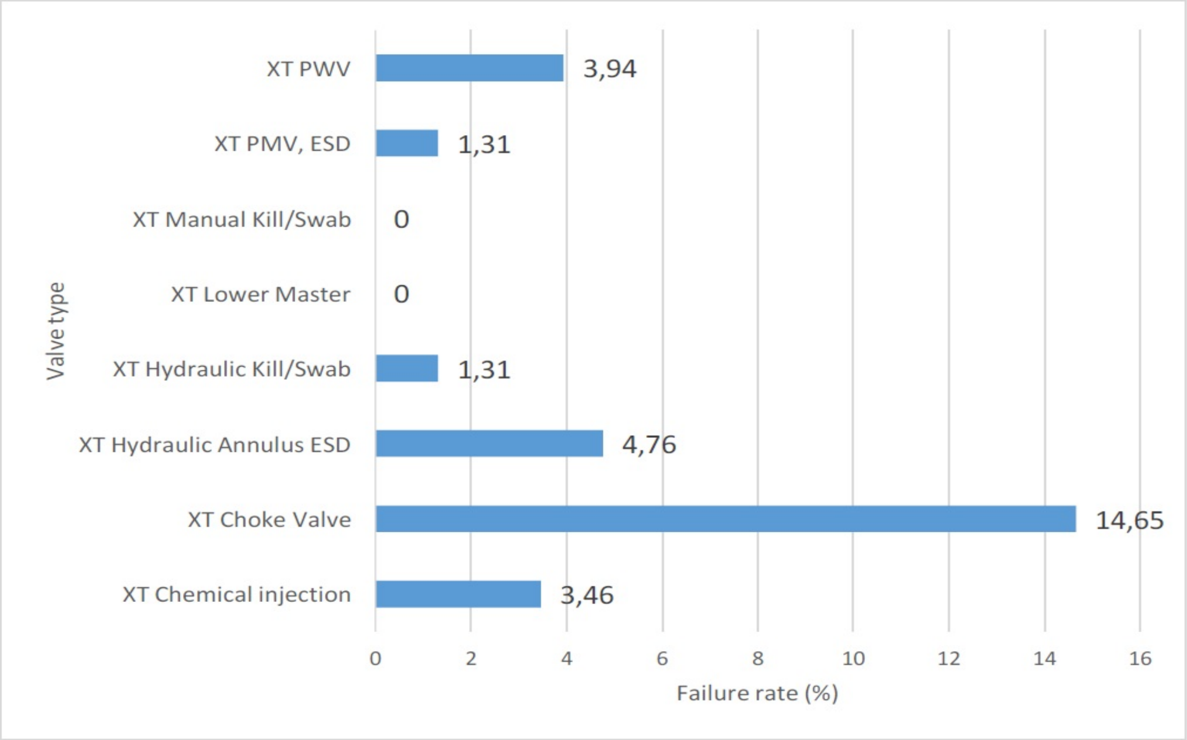


Figure 4.24: Failure rate on Field A (2013-2018) [43]

Field B

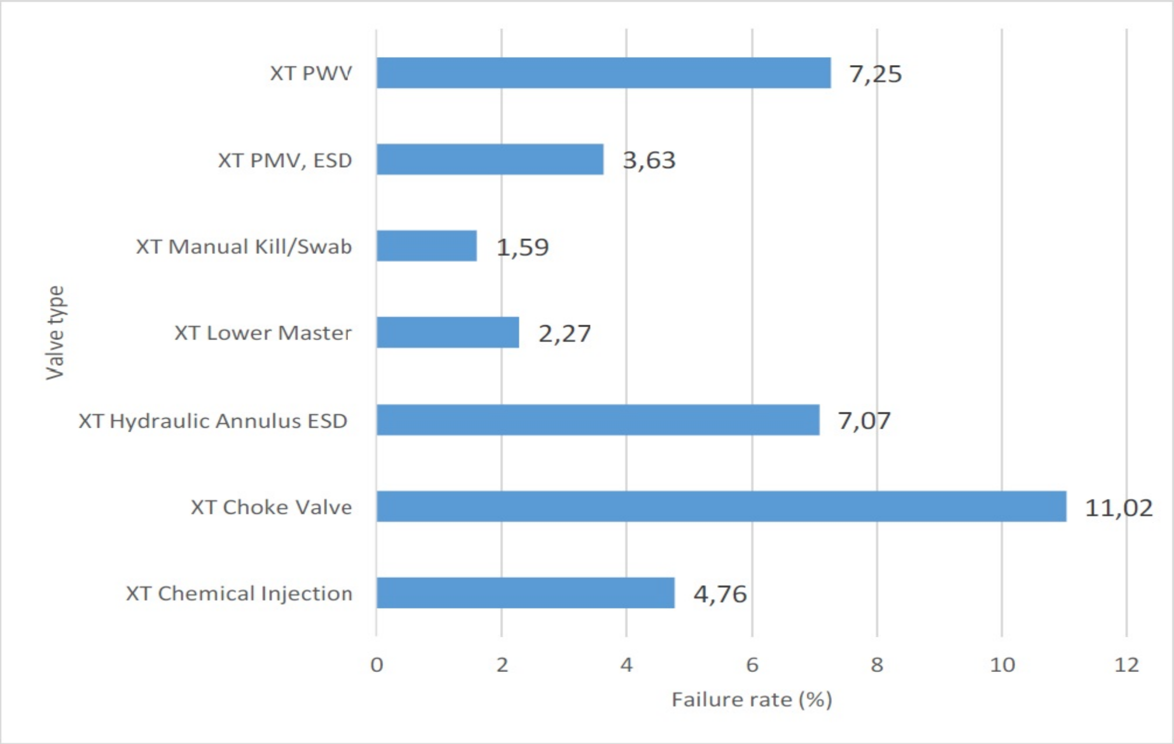


Figure 4.25: Failure rate on Field B (2013-2018) [43]

FIELD C

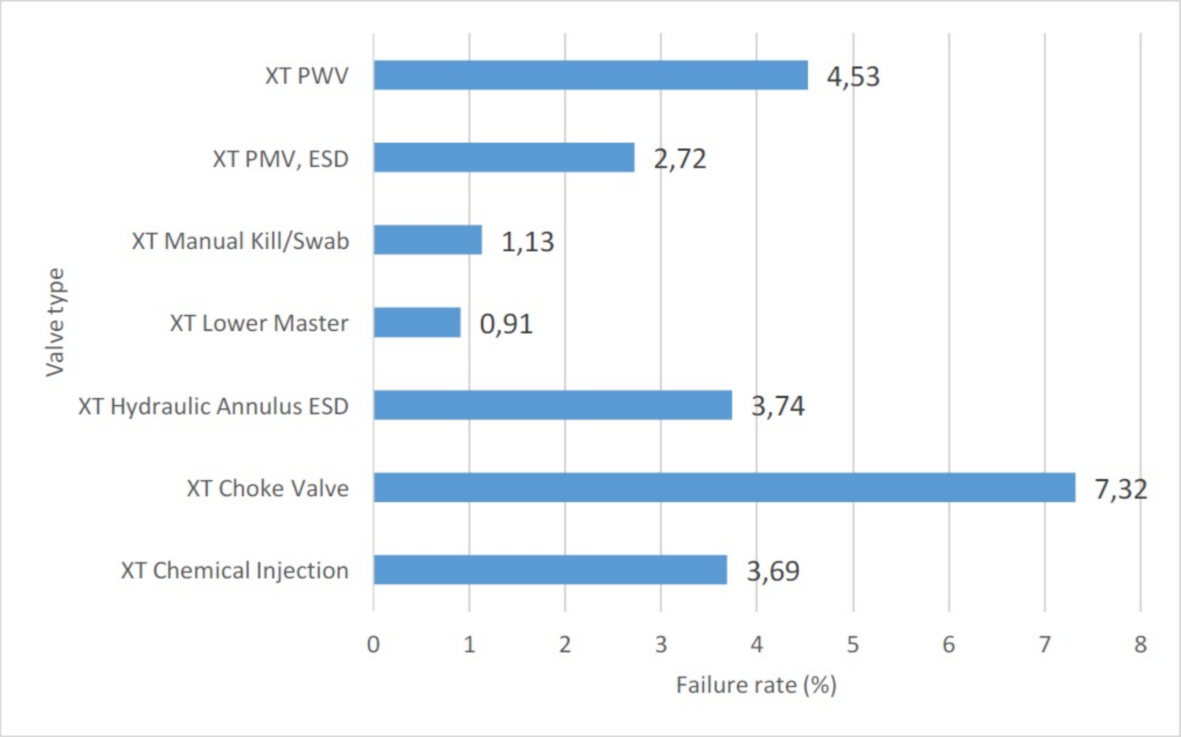


Figure 4.26: Failure rate on Field C (2013-2018) [43]

Choke valves have the highest failure rate in all fields. In fields A, Hydraulic Annulus valves have the second highest failure rate. However, PWV have the second highest failure rate in fields B and C. PWV have the third highest failure rates in field A, whereas Hydraulic Annulus valves have the third highest failure rates in field C. Regarding PWV and PMV valves, failure rates increases in the sequence: Field A, Field C, Field B. Generally, there are difference in the failure rates across fields. These differences difference could be due to valve design, valve maintenance procedures, age and behaviour of the field, etc. A generalized trend can be obtained by calcfulating failure rate for each valve type as illustrated in Figure 4.27.

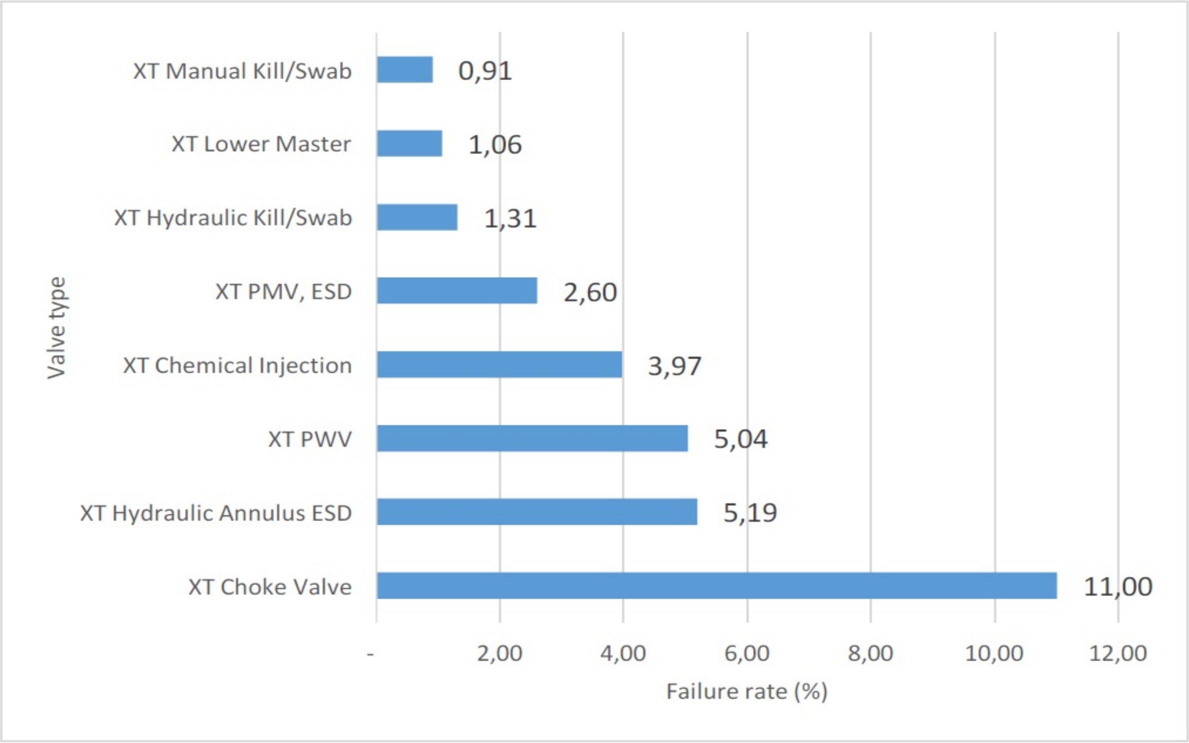


Figure 4.27: Total average Failure rate (%)from Field A, B and C in (2013-2018) [43]

Figures, which are illustrated above, show the failure trend of XT valves, especially barrier valves. As we can see from the figure above 4.27, Choke valve failure has the highest failure rate among XTs valves. Howver, as our focus on this thesis is on barrier valves, we should look at the failure rates of PMV and PWV in particular. Engineers of their respective companies attribute high rate of PMV and PWV failure to a few factors. Some engineers believed that well fluid behaviour and high frequency of use during normal operations are the causes of high failure rate. Others engineers believed that corrosion, erosion and poor maintenance related issues were the cause of high PMV and PWV failure rate. Also, the most common failure mechanism stated was corrosion. Each engineer also had a slightly different interpretation of best maintenance practices on valves (and other equipment in general). A count of the unique failure mechanism attributed to valve failure by engineers is illustrated in Figure 4.28.

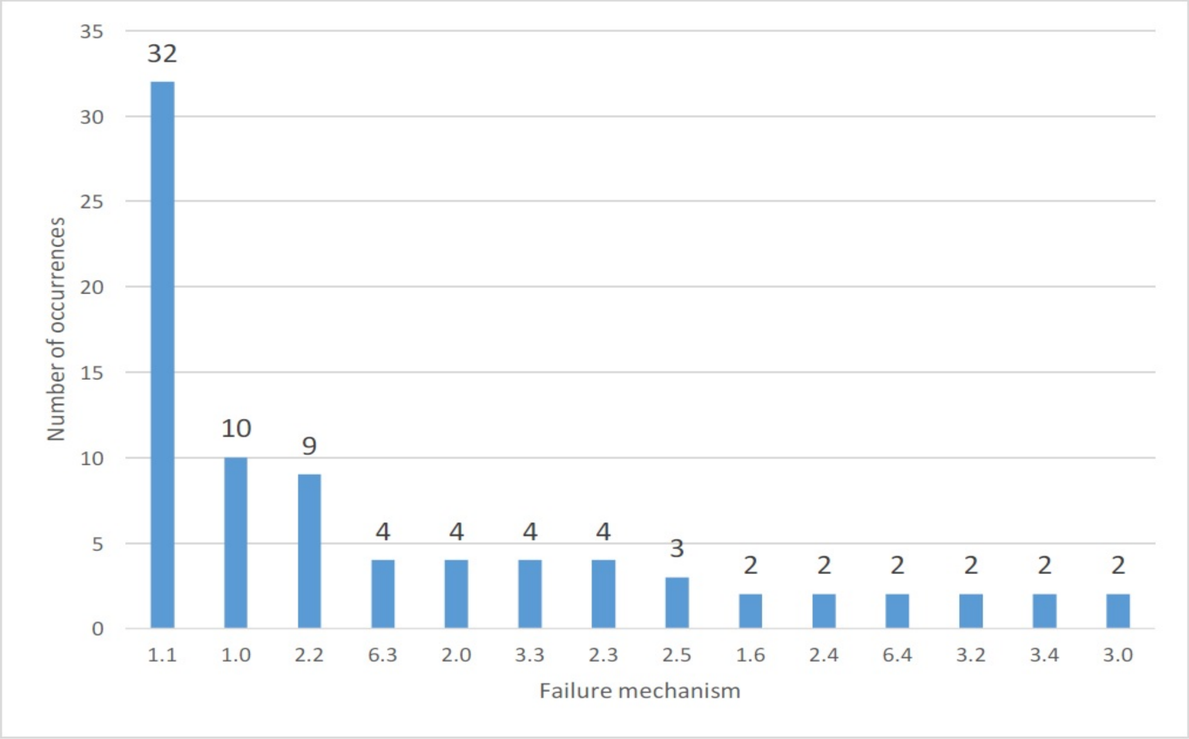


Figure 4.28: Number of failure mechanism detected in the fields in years (2013-2018) [43]

According to the interviewed engineers, three main failure mechanisms occurred very frequently. Approximately 62% of engineers attributed valve failure to these three mechanisms. They are coded by ISO 14224 as follows: 1.1, 1.0, 2.2. Descriptions of these failure mechanisms are given in Section 4.1.9. These failure mechanisms are as followings:

- 1.1 : Mechanical failure due to leakage - External or internal leakage, either liquids or gases was cited 32 times.
- 1.0 : Mechanical failure due to general- A failure related to some mechanical detect but where no further details are known. Mechanical failure was cited 10 times.
- 2.2 : Material failure due to corrosion - All types of corrosion, both wet (electrochemical) and dry (chemical) was cited 9 times.

The main reason for conducting an interview was to explore what main problem needs to be solved and transfer these needs to the specific requirements. In section 5.2.1, the table is showed customer needs that have been translated to the technical requirements.

4.2.3 Case Study 3 : TechnipFMC

The source for this thesis has been gathered from TechnipFMC's condition monitoring team. The relevant information regarding the Xmass tree and wellhead valves were collected during a structured interview. Condition monitoring and valve monitoring systems were presented by personnel.The structured interview with condition monitoring engineers helped to clarify condition monitoring system and how valves are monitored. Additionally, to get exact information related to the Hydraulic valves monitoring system, monitoring requirements were gathered from FMECA and CPM reports. Structured interview with engineers and company reports provided an overview of condition monitoring requirements. The gathered requirements are furnished in table 5.2 and it will be discussed in section 5.3.1.

4.2.4 Case Study 4: MRC Global Norway

The monitoring requirements and data related to MRC Global's condition monitoring system (Valvewatch) has been gathered from MRC Global Norway's website. This company is the supplier of monitoring equipment and technology associated with ESD valves on the Equinor topside project. Their brand Valvewatch includes sensors, software and system package. Unfortunately, a structured interview could not be conducted. However, the information gathered from their website provided descriptions of Valvewatch monitoring systems used in the Norwegian Oil and Gas industry. The table in section 5.3.2 describes Valvewatch monitoring requirements.

Chapter 5

Requirements Elicitation and Discussion

5.1 Case Study: Conoco-Phillips

5.1.1 Testing Requirements

Even though the specific requirements and guidelines are available in the NOG 070 regarding the reliability-based maintenance strategy for barrier valves, it has not been applied by ConocoPhillips Norway yet. However, the common proof testing policy of the COPNO is the according to the time- based requirements for well barrier components as defined in the Norsok D-010 standard. According to COPNO, for example, the Downhole safety valve (DHSV) should be tested every month until three consecutive tests have successfully run, as outlined in Appendix A. Henceforth, for referential simplicity, this testing interval shall be referred to in this document as the 1-3-6 test model. However, PSAN recommends to operators to use NOG 070 guidelines to update testing intervals based on component reliability.

Primarily, Norsok -D10 states that the testing frequency for ESD functions should be defined according to the following criteria:

1. changes in the well flow composition which increase the risk of scale, deposits, corrosion, erosion as well as high production and injection
2. experience data rates.

NOG-070 states that the method to be used for updating test intervals is outlined in the SINTEF PDS report "Guidelines for follow-up Safety Instrumented Systems (SIS) in the operating phase". It consists of the following steps:

1. Determine updated DU failure rate from operational experience and generic failure rate.
2. Determine the 90% confidence interval for DU (updated)
3. Update test intervals based on the following criteria
   (a) If DU (updated) is less than half of DU (assumed), double the testing interval.

(b) DU (updated) is more than half of DU (assumed), halve the testing interval.

In section 15 of the NORSOK D-10 standard, a comparison can be made between the monitoring requirements of DHSV (subsection 8) and PMV/PWV (subsection 33). The standard stipulates that DHSV should be leak tested. No such test specification is given for PMV/PWV. However, the given acceptance criteria is leak-related. This could imply leak testing or functioanl testing. In theory, operator companies are only required by NORSOK D-10 to perform ESD (proof) testing for DHSV, PMV and PWV once per year. However, in practice, operator companies follow the 1-3-6 interval. This approach involves a few disadvantages. It introduces the potential for valve degradation because leak tests only require the valve to be closed once whereas full stroke testing requires that the valve is operated (opened and closed) multiple times. Also, proof testing is an end-to-end test in relation to the subsystems involved. It is also designed to detect all failures modes in Section 4.1.10, which are FTO, FTC, LCP, ST and CTS. This is a more time-consuming process since testing involves verifying the functionality of each SIF's sensor, logic-solver and final control element, as well as their associated interfaces. This increases test duration and contributes to higher downtime.

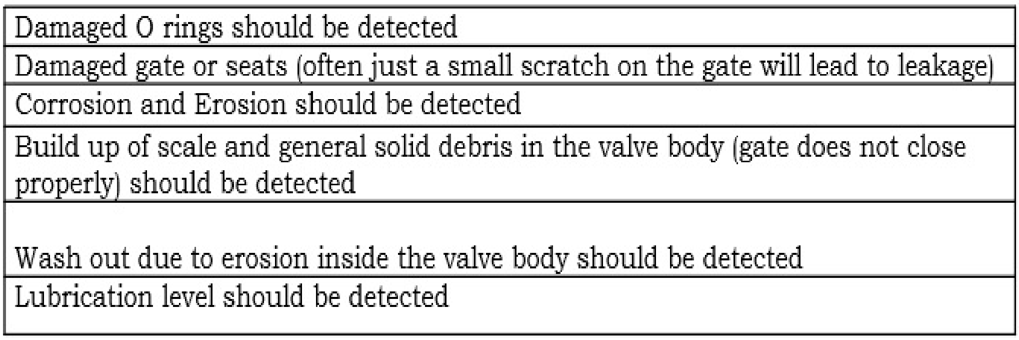
It can be observed from Chapter 4, Subsection 4.2.1 that the total number of failures in DHSV over the period of observation is 8 times higher than the combined number of failures of the PMV and PWV. As a result, the optimal test duration for DHSV and PMV/PWV valves are 6 months and 12 months respectively. An alternative method of updating test intervals which does not depend on doubling or halving may exist. Considering that test period is dependent or SIL, an argument could be made for setting an SIL with a respective SIL margin and optimizing test durations to the nearest month. Since SIL is not exceeded, safe operation is assured. This also allows for smaller improvements to be made, in cases where the DU is significantly greater than or less than DU but not up to a factor of 2.

One of the main drawbacks of using the NOG 070 method for updating test intervals is based on the low importance given to uncertainty management. Updating NOG 070 is complicated by the use of PDFavg within the 90% confidence interval. PDFavg has a qualitative element which manifests in the strength of knowledge used to determine its value. SoK may be high or low. PDFavg is then used to compute SIL. Due to propagation of uncertainty, calculated may not reflect the true reliability of the system in question. Flage and Aven [22] argues that PDVavg is based particular background knowledge and if the background knowledge changes, it might be that assigned probability also change. Hence, Flage and Aven [22] proposed simple method to take into cosideration before a conclusion is made on SIL. According to their evaluation, perfomance influencing factors are not predicted by PFDavg,could be evaluated by SOK.

5.2 Case Study: Equinor, AkerBp, Spirit Energy and Maersk

5.2.1 Monitoring Requirements

The furnished table below is elicitation result from case study 2 detailing issues which operated company mainly encountered. The table highlights common issues that offshore personnel experience. This data was translated into technical requirements.Going through the TechnipFMC hydraulic valve monitoring system, the author could not determine if the monitoring system can define such issues. However, discussion with engineers exposed the main causes of valve failures such as corrosion, erosion, damaged- O -rings, and general mechanical failure. Hence, all interpretation of what TechnipFMC and Valve-watch can monitor is stated in the following section and it was interpreted according to customer requirements.



Damaged O rings should be detected
Damaged gate or seats (often just a small scratch on the gate will lead to leakage)
Corrosion and Erosion should be detected
Build up of scale and general solid debris in the valve body (gate does not close properly) should be detected
Wash out due to erosion inside the valve body should be detected
Lubrication level should be detected

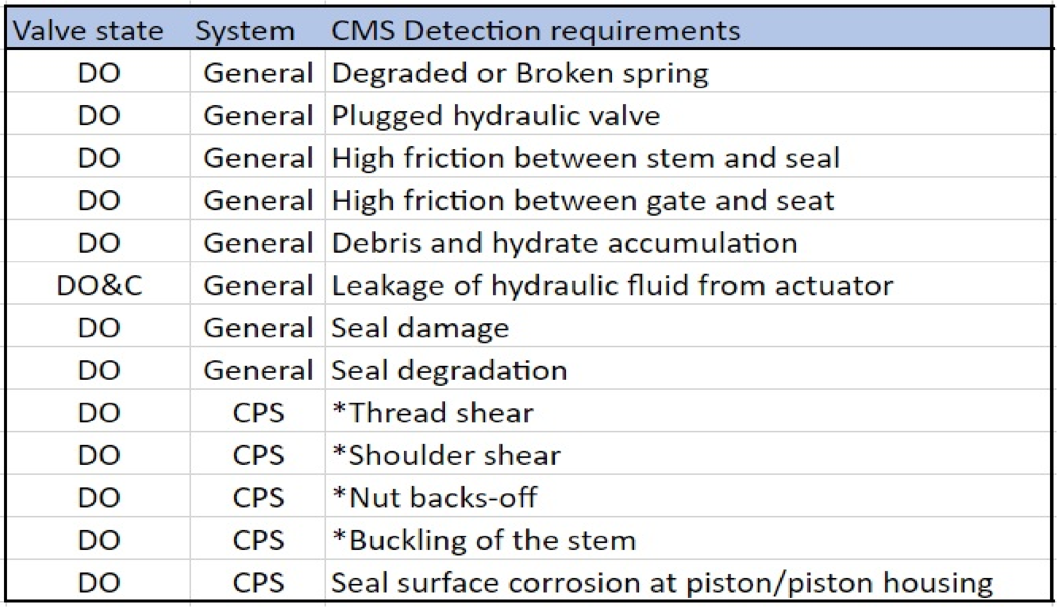
Table 5.1: Operator Company's CMS Improvement Requirements

5.3 Monitoring Service Provider Requirements

The section below compares the monitoring capabilities of the interviewed service companies to the monitoring requirements of operator companies. Deficiencies in monitoring services provided by service companies are highlighted and potential solutions to these deficiencies are outlined.

5.3.1 TechnipFMC

The valve state column describes which valve state is required before detection of the failure mechanism can be made. One valve state is "during operation" meaning the valve has been actuated and is in motion. The other is "continuously" and this means that the valve remains static in the open or closed state. TechnipFMC further describes which system of their CMS takes the responsibility of detecting a certain failure mechanism. These are placed in the System column of Table 5.2.



Valve state	System	CMS Detection requirements
DO	General	Degraded or Broken spring
DO	General	Plugged hydraulic valve
DO	General	High friction between stem and seal
DO	General	High friction between gate and seat
DO	General	Debris and hydrate accumulation
DO&C	General	Leakage of hydraulic fluid from actuator
DO	General	Seal damage
DO	General	Seal degradation
DO	CPS	*Thread shear
DO	CPS	*Shoulder shear
DO	CPS	*Nut backs-off
DO	CPS	*Buckling of the stem
DO	CPS	Seal surface corrosion at piston/piston housing

Table 5.2: TechnipFMC Hydraulic Valve Monitoring Requirements

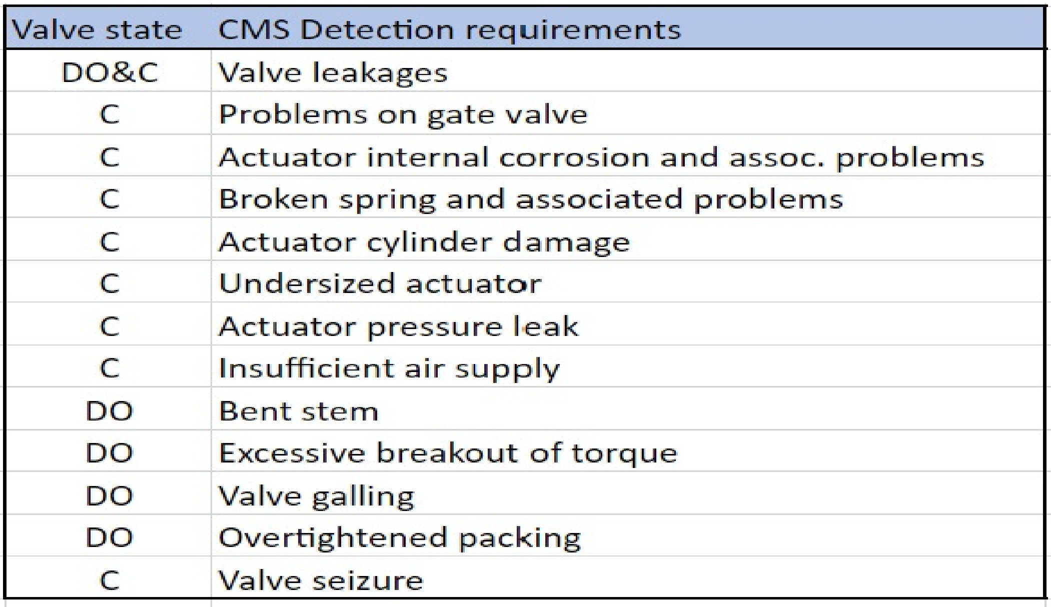
"DO - during operation, C-Continuously *These failure modes are associated with loose nuts and bolts. As a result, they are very unlikely to occur"

A few observations can be made from TechnipFMC's condition monitoring system. Firstly, all requirements extracted from their monitoring system require the valve to be in operation. TechnipFMC's system is able to detect all of the monitoring requirements from Case Study 2 except for detection of damaged O-rings and detection of washout due to erosion. In addition, corrosion erosion are partially detected since only seal surface and piston housing components are addressed. Interviewed engineers stated their monitoring system can only detect lubrication level when the valve is in operation. This means that it is not possible to predict failure from low lubrication level before demand occurs.

Also the results Case Study 2 indicate that the most common failure mechanisms are mechanical failure due to leakage, general mechanical failure and material failure due to corrosion. Mechanical failure due to leakage was by far the most predominant failure mechanism.TechnipFMC's condition monitoring system is unable to detect mechanical failure due to leakage during online diagnostic. However, mechanical failure due to leakage can be detected during proof testing. In order to maintain high SIL with such a CMS, a short testing interval should be maintained. However, with a CMS capable of detecting mechanical failure due to leakage, testing interval can be lengthened, thereby reducing operating costs.

5.3.2 ValveWatch

In relation to Case Study 2 requirements, the Valvewatch CMS does not detect damaged gates or seats, damaged O-rings, lubrication level or scale and debris formation. However, Valvewatch's CMS is able to detect broken springs and internal corrosion of actuators, but not gates,stems and pistons. This CMS was designed to detect internal leakage in both open and closed position. This gives their CMS an edge over Technip FMC's CMS.



Valve state	CMS Detection requirements
DO&C	Valve leakages
C	Problems on gate valve
C	Actuator internal corrosion and assoc. problems
C	Broken spring and associated problems
C	Actuator cylinder damage
C	Undersized actuator
C	Actuator pressure leak
C	Insufficient air supply
DO	Bent stem
DO	Excessive breakout of torque
DO	Valve galling
DO	Overtightened packing
C	Valve seizure

Table 5.3: Valve-watch Monitoring Requirements

"DO - during operation, C-Continuously *These failure modes are associated with loose nuts and bolts. As a result, they are very unlikely to occur"

However, during usage, the verracity of their claim should be verified. This function does not distinguish Valvewatch's CMS from Technip FMC's CMS in terms of DU detection. This is because the DU specified in NORSOK D-10 standard is the detection of leakage when the valve is in the closed position. The absence of a detection in the open position does not necessarily translate to the absence of a leak if the valve were to be in the closed position. For instance, damage to the gate of a valve may lead to the modification of its shape. This may lead to incomplete closure and ultimately allow for leakage when the function is demanded. However, in the open position, no such leakage will be detected since Valvewatch does not detect damaged gate. In this regard, neither company's CMS can convert this DU failure into a DD failure. However, a correlation could exist between failure in the open position to failure in the closed position and this hypothesis may need to be further investigated.

General mechanical failure was the most reported failure mechanism reported by interviewed engineers in case study 2. This translates to the inability of practitioners to classify the cause for the mechanical failure due to insufficient information from monitoring system and insufficient evidence from inspection. In practice, this could result from instrument error, calibration error and more. This classification problem should be addressed by service providers to ensure that a greater portion of failures are classified to a specific failure mechanism. These specific failure mechanisms can then be addressed, thereby reducing the total number of dangerous undetectable failures.

At the moment, classification of failure mechanisms is based on descriptor-based analysis during testing and simple SIF continuous monitoring applications. However, a CMS that employed more complex algorithms like stationary and time series anomaly detection systems could be used to improve failure classification. In this case, failures which were classified under general mechanical failure could be identified under a known failure mechanism which could then be addressed in the maintenance procedure. However, more research will have to be performed regarding methods to train and test such algorithms in order to minimize false positive and false negative classifications.

Corrosion was the third most reported failure mechanism. Corrosion occurs when two metals with different electropositivity remain in contact with each other in the presence of an electrolyte. This difference in electropositivity is directly proportional to redox potential. In these situations, operator companies should inform service providers of the predicted souring potential of the well. Service companies should work to select valve components with the lowest redox potential. Maximizing the use of stainless steel-based materials is ideal. Components with different redox potentials should also be avoided as this leads to redox reactions within the valve. Using stainless steel, however, increases the fixed capital investment operators will spend on their valves. Nevertheless, their maintenance costs will reduce and in-turn, their valve lifespan will potentially increase. Generally, this will lead to greater reliability and survivability. Consequently, SIL margin is likely to improve. This could ultimately allow for operating companies to increase their component testing intervals as stipulated by the NORSOK D-10 standard.

Chapter 6

Conclusion & Recommendation

Operator company should revise its testing policy and forward to condition monitoring

From case study 1, it was found that the operator company on the Norwegian continental shelf are still unsure which standards they should follow. Thus, the standard should describe more specifically about testing intervals and frequency. As the author of this thesis, I could not find specific requirements that state how long testing intervals should be. So, such kinds of requirements confuse the stakeholders, and instead of extending test intervals, they can reduce it, which can cause degradation of the system. As we can see that from section 4.2.1 survivability of the valve is high. This means that there are possibilities to extend testing intervals, as NORSOK D-10 states in Appendix A.1. However, the associated company finds it difficult to implement it. As stated earlier, PSAN recommends applying NOG 070, though PF-Davg is used as a quantitative justification. Also, the calculated PFDavg for safety instrumented function is based on all available background knowledge [PFDavg K]. As the background knowledge might differ between analysts, the calculated PFDavg can vary greatly.

Thus, the elicited requirement from the COPNO shows that the company is interested in extending their testing intervals according to their computed reliability as illustrated in figure 4.17 and 4.18. However, there are still uncertainties to extending testing. Thus, to extend testing policy in the future, the COPNO company should revise its testing policy as its experienced operational data is reliable enough, as stated in NORSOK D10, and following implementation procedure, as stated in NOG 070. Additionally, the company should develop its strength of knowledge in line with PFDavg to provide appropriate decision support for decision making under uncertainty in a safety context with the combination (PFDavg, SoK).

Valve suppliers should develop reliabilty of barrier valves

During the requirements elicitation, it was discovered that certain barrier valves were not designed for use in their respective fields. Barrier valve design must also consider the same immutable factors used in ESD testing time duration such as well flow composition and experience data. High quality valves can then be designed by performing proper materials selection to prevent corrosion. The author of this thesis determined most poor valve and reported it. Moreover, findings show that certain valve components have a greater tendency to fail, and it may not be possible to monitor these components until the valve is operated. These could lead to catastrophic results. According to interviewved engineers

Maintenance strategy should be revised as most valve failures come from poor maintenance strategy

Poor maintenance was sited as another major reason for barriers valve failure. Bad interpretations of maintenance procedures and general flauting are two major modes that lead to poor maintenance. According to my observations and interviewed engineers, individuals had preferred ways of performing maintenance operations. These operations could deviate sometimes from the technical requirement and guidelines related to maintenance strategy. And it is no secret that a poorly maintained valve does not last as long as it should.

In the subsea industry, there exist a variety of different types of valves, so the operator companies should become familiar with them, so they will know how they operate. This is a vital factor in designing a personalized valve maintenance program. Thus, maintenance personnel should be familiar with what types of valves they possess along with the physical properties of these valves. Moreover, as long as most valve failure comes from a poor maintenance system, the operator should revise their maintenance frequency or perform predictive maintenance. Hence, it can lead to safe maintenance, higher predictability, and increase the availability of the system.

Bibliography

[1] Petroleum Safety Authority Norway (PSAN). *The activities regulations §47 Maintenance programme. 2018:* URL: `https://www.ptil.no/en/regulations/all-acts/the-activities-regulations3/IX/47/`. (accessed: 03.07.2020).

[2] Petroleum Safety Authority Norway (PSAN). *The facilities regulations §48 Well barriers:* URL: `https://www.ptil.no/en/regulations/all-acts/the-activities-regulations3/IX/47/`. (accessed: 03.07.2020).

[3] Petroleum Safety Authority Norway (PSAN). *The facilities regulations §8 Safety functions:* URL: `https://www.ptil.no/en/regulations/all-acts/the-activities-regulations3/IX/47/`. (accessed: 03.07.2020).

[4] Petroleum Safety Authority Norway (PSAN). *The framework regulations §11 Risk reduction measures.* URL: `https://www.ptil.no/en/regulations/all-acts/the-activities-regulations3/IX/47/`. (accessed: 03.07.2020).

[5] Petroleum Safety Authority Norway (PSAN). *The management regulations §5 Barriers:* URL: `https://www.ptil.no/en/regulations/all-acts/the-activities-regulations3/IX/47/`. (accessed: 03.07.2020).

[6] NOG 070. *Norwegian Oil and Gas Association;Application of IEC 61508 AND IEC 61511 in the Norweigan Petroleum Industry.* NOG. 2018.

[7] ISO 13628-1. *Petroleum and Natural gas Industries- Design and Operation Subsea Production Systems-Part 1: General requirements and recommendations.* ISO. 2005.

[8] BS EN ISO 14224. *Petroleum, petrochemical and natural gas industries - Collection and exchange of reliability and maintenance data for equipment (ISO 14224:2016).* BS EN ISO. 2016.

[9] NS-ES ISO 14224. *Petroleum,petrochemical and natural gas Industries- Collection and exchange of reliability and maintenance data for equipment (ISO 14224:2016.* NS-ES ISO. 2016.

[10] IEC 61508. *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements.* IEC. 2010.

[11] Katarzyna Adamowicz, Piotr Sarna, and Wiesław Szatko. “Safety in subsea petroleum production systems: subsea christmas tree case study”. In: *Czasopismo Techniczne* (2016).

[12] Adelaide, Brisbane, and Perth. “Leakage Acceptance Rates Comparison Metal Soft Seated Valves ISO 5208/API 598/API 6D/MSS SP-61/FCI 70-2”. In: *Global Supplyline* (2019).

[13] Borhanuddin Ahmad, Norhaliza Abdul Wahab, and Amirah A Rahman. “Emergency Shutdown Valve Reliability Function Test by Automated Partial Stroke Testing System”. In: *Jurnal Teknologi* 78.7-4 (2016).

[14] Joe Anders et al. "Implementation of Well Barrier Schematic Workflows". In: *SPE Digital Energy Conference and Exhibition*. Society of Petroleum Engineers. 2015.

[15] Norwegian Oil Industry Association et al. *Risk and Emergency Preparedness Assessment, NORSOK Standard Z-013, Rev. 3*. 2010.

[16] Norwegian Petroleum Safety Authority. *Norwegian's Petroleum Histrory*. URL: `https:https://www.ptil.no/en/search-complete-website/?q=Barrier+safety+valve+testing`. (accessed: 03.05.2020).

[17] Yong Bai and Qiang Bai. *Subsea engineering handbook*. Gulf Professional Publishing, 2018.

[18] Alejandro Bencomo. "Applications of condition monitoring for the subsea industry". MA thesis. University of Stavanger, Norway, 2012.

[19] Jon Berven. "Subsea control system for all-electric Xmas trees". MA thesis. University of Stavanger, Norway, 2013.

[20] Norsok D-010. "Well Integrity in Drilling and Well Operations". In: *Standards Norway* (2013).

[21] Tore FJågesund. "Illustrating Well Barriers". In: (215).

[22] Roger Flage and Terje Aven. "Expressing and communicating uncertainty in relation to quantitative risk analysis". In: *Reliability: Theory & Applications* 4.2-1 (13) (2009).

[23] Sai Ganesh Gunda. *Requirements engineering: elicitation techniques*. 2008.

[24] Stein Hauge, Per Hokstad, and Tor Onshus. "The introduction of IEC 61511 in Norwegian offshore industry". In: *Proceedings of the European Safety & Reliability International Conference (ESREL'01)*. 2001, pp. 483–490.

[25] Stuart Guy Holley. *Valve condition monitoring*. US Patent App. 13/194,509. Mar. 2012.

[26] Arnljot Høyland and Marvin Rausand. *System reliability theory: models and statistical methods*. Vol. 420. John Wiley & Sons, 2009.

[27] ISA-TR96.05.01-2017. *Partial Stroke Testing of Automated Valves*. ISA. 2017.

[28] Affifa Kanwal. "Requirements Engineering: Elicitation Techniques". In: ().

[29] Mahmoud Khalifeh and Arild Saasen. "Introduction to Permanent Plug and Abandonment of Wells". In: (2020).

[30] Gerald Kotonya and Ian Sommerville. *Requirements engineering: processes and techniques*. Wiley Publishing, 1998.

[31] Anna Kvæven. "Optimisation of Test Intervals for Well Barriers". MA thesis. University of Stavanger, Norway, 2019.

[32] Anders Lemme and Helene Jakobsen Furseth. *Expansion of the Condition Monitoring Strategy for ESD and PSD valves on Johan Sverdrup:A case study in Equinor ASA*. 4036 Stavanger, Norway, 2019.

[33] Bob Lightsey. *Systems engineering fundamentals*. Tech. rep. DEFENSE ACQUISITION UNIV FT BELVOIR VA, 2001.

[34] Bela G Liptak. *Instrument Engineers' Handbook, Volume Two: Process Control and Optimization*. CRC press, 2018.

[35] Yiliu Liu and Marvin Rausand. "Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems". In: *Reliability Engineering & System Safety* 145 (2016), pp. 366–372.

[36] Mary Ann Lundteigen and Marvin Rausand. "Partial stroke testing of process shutdown valves: How to determine the test coverage". In: *Journal of Loss Prevention in the Process Industries* 21.6 (2008), pp. 579–588.

[37] Lundeteigen Marvin et al. "An Introduction to Well Integrity". In: (2012).

[38] D Moodie, L Costello, D McStay, et al. "Optoelectronic leak detection system for monitoring subsea structures". In: *Subsea Control and Data Acquisition (SCADA) Conference*. Society of Underwater Technology. 2010.

[39] Bashar Nuseibeh and Steve Easterbrook. "Requirements engineering: a roadmap". In: *Proceedings of the Conference on the Future of Software Engineering*. 2000, pp. 35–46.

[40] Norwegian Petroleum. *Norwegian's Petroleum Histrory*. URL: `https:https://www.norskpetroleum.no/en/framework/norways-petroleum-history/`. (accessed: 03.07.2020).

[41] Marvin Rausand. *Reliability of safety-critical systems: theory and applications*. John Wiley & Sons, 2014.

[42] Schlumberger. *Subsurface Safety Valve (SSSV)*. URL: `https:https://www.glossary.oilfield.slb.com/en/Terms/s/subsurface_safety_valve_sssv.aspx?r=1&l=ri&fst=0&p=1`. (accessed: 03.07.2020).

[43] Moslim Shaipov. "Drilling and Well-Valve usage in changing environment". MA thesis. University of Stavanger, Norway, 2018.

[44] NTNU Sintef. "Offshore and onshore Reliability Data". In: *OREDA Handbook, 6th ed, DNV, Oslo* (2015).

[45] Angela E Summers. *Partial Stroke Testing of Block Valves*. Houston, Texas, 2001.

[46] TecnipFMC. "Specification, Subsea - Production Perfomance Services, CPM 2.0, Hydraulic Actuator module,- Internal Documentation". In: (2017).

[47] Einar H Winther-Larssen. "Design of an electric X-mas tree gate valve actuator". MA thesis. Institutt for teknisk kybernetikk, 2007.

[48] Pengyu Zhu and Jayantha P Liyanage. "Application of prognostics and health management to low demand systems: Use of condition data to help determine function test interval". In: *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*. IEEE. 2018, pp. 242–246.

[49] Pengyu Zhu et al. "Review of workflows of emergency shutdown systems in the Norwegian oil and gas industry". In: *Safety science* 121 (2020), pp. 594–602.

Appendix A

Appendix: (Integrity Requirements and Verification of Well Barrier Components)

A.1 Norsok D-10

The standard NORSOK D-010 defines requirements and guidlines relating to well integrity in drilling and well activities[20]. According to NORSOK D-010 subsection 8.7.1:

All valves, available testable seals and lines which are part of the primary or secondary well barriers shall have a maintenance program and be periodically tested to verify its function and integrity according to section 15

A.1.1 Integrity Requirements

Requirement related to the integrity of well barriers are provided in section 8.7.1:

If a safety critical valve type has a failure rate on the installation which exceeds 2% within a 12 month period, measures shall be taken to improve the reliability of the valve type in general.

A.1.2 Integrity Verification-Component Test Programmes

Verification and minimum test frequency is defined for the PMW, PWV and DHSV in section 15. The standard define that test frequency should be regulated according to section 15:

PMV/PWV

Initial Test and verification:The valves shall be tested with both low and high maximum differential pressure in the direction of flow. The low-pressure test shall be maximum 35 bar.

Monitoring

1) The automatic valves shall be tested at regular intervals as follows:

- Monthly, until three consecutive qualified tests have been performed; thereafter
- Every three months, until three consecutive tests have been performed; hereafter
- Every six months

2) The emergency shutdown function shall be tested yearly.It shall be verified acceptable shut down time and that the valve closes on signal.

DHSV

Initial Test and verification: It shall be tested with both low and high differential pressure in the direction of flow. The low-pressure test shall be maximum 70bar.

Monitoring

1) The valve shall be leak tested at specified regular intervals as follows:

- Monthly, until three consecutive tests have been performed; thereafter
- Every three months, until three consecutive qualified tests have been performed; thereafter
- Every six months

2) The emergency shutdown function shall be tested yearly. It shall be verified acceptable shut down time and that the valve closes on signal.

It is noted that if a valve fails, the test procedure starts over again with one – month test intervals, extending to three and six months.

A.1.3 Updating Component Test Intervals

In the standard, for updating the prescribed test intervals based on component re liabilities are provided in section 8.7.1 and test frequency should regulate based on:

a) experience data;

b) changes of the well flow composition increasing risk of deposits, scale, corrosion, erosion and high production and injection rates.

The historic performance and reliability data used to justify a change in the test frequency shall be documented.

A.2 NOG 070

The NOG 070 guideline performs predefined performance requirements.The guideline presents minimum SIL requirements to the integrity of specified global and local SIFs that are already required in standards adopted by the Norwegian Petroleum Sector. The minimum SIL requirements have been set based on analysis of generic reliability data gathered from the industry, e.g. provided in The PDS data handbook [33].

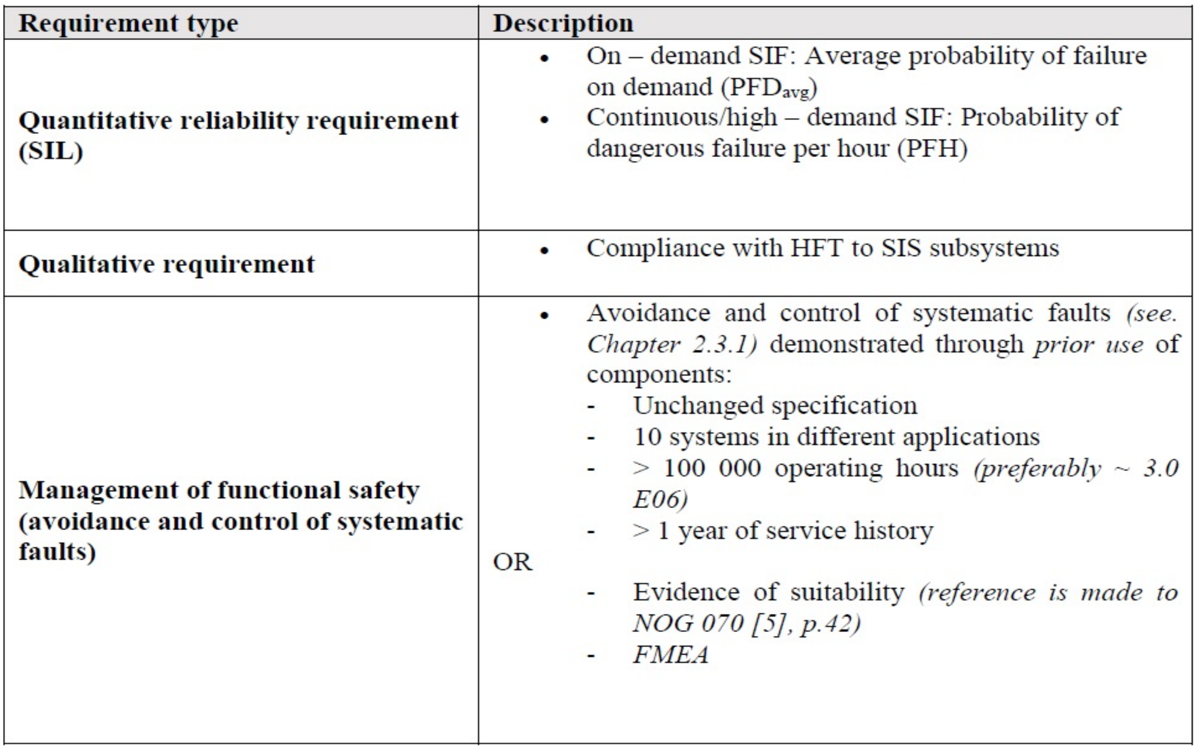
NOG 070 refers [6] that SIL must be verified through maintenance and monitoring to present that SIL meets the required SIL for the SIF. According to the standard section 10.5:

> ***"The SIS shall be proof tested and maintained regularly during operation in order to ensure that the functional integrity is maintained... SIL classified safety functions and associated equipment shall be tested according to predefined proof test procedures scheduled in a PM programme as part of the maintenance system"***

A.2.1 SIL Requirements

Minimum SIL requirements to selected SIFs are presented in NOG 070 [6], section. 7.5. According to NOG 070, based on IEC 61508 and IEC 61511 [3, 4], there are three main requirement types that shall be fulfilled by a SIF implemented through SIS-technology in order to achieve a given SIL; a quantitative requirement to the SIFs reliability, and qualitative requirements to hardware fault tolerance and management of functional safety.

The requirement types are presented below in figure A.1



Requirement type	Description
Quantitative reliability requirement (SIL)	• On – demand SIF: Average probability of failure on demand (PFD_{avg}) • Continuous/high – demand SIF: Probability of dangerous failure per hour (PFH)
Qualitative requirement	• Compliance with HFT to SIS subsystems
Management of functional safety (avoidance and control of systematic faults)	• Avoidance and control of systematic faults *(see. Chapter 2.3.1)* demonstrated through *prior use* of components: - Unchanged specification - 10 systems in different applications - > 100 000 operating hours *(preferably ~ 3.0 E06)* - > 1 year of service history OR - Evidence of suitability *(reference is made to NOG 070 [5], p.42)* - *FMEA*

Figure A.1: SIF requirements to achieve a given SIL [6]

In addition, IEC 61508/IEC61511/NOG 070 also make recommendations to [6]:

The quality of failure rate data : If sufficient data is available, it is recommended to use historical field data as a basis for calculations of the quantitative requirement. To evaluate whether field data is qualified for use in calculations, NOG 070 presents considerations to the data collection approach, detailing level and failure registration.

Independence between safety systems: Measures shall be implemented to avoid adverse effects between SIS and non-SIS systems and applications, and between SIS nodes.

Documentation from the design phase: All requirements, assumptions and prerequisites from the design phase that may affect the operation and maintenance of SISs should be transferred in a consistent and complete manner to operation.

Focus on deviation from the list of assumptions underbuilding the SIL requirements set to typical SIFs in NOG 070: Assumptions are listed to design, process conditions etc. these must be met by the operator for the minimum SIL requirements to be applicable to identified SIFs on the installation.

A.2.2 SIL Verification

NOG 070 Section F.1 recommends the establishment of a performance target criteria to verify SIL requirements during operation.

"The number of registered DU failures during operation will be the main integrity performance indicator during operation. The associated integrity target criteria can be calculated from the generic DU failure rate, since in design this parameter is used to show that the predicted PFDavg meets the required PFDavg."

A.2.3 Updating Component Test Intervals

According to NOG 070, if the SIF's operation experience can prove that components are significantly more or less reliable than what was presumed in the design phase, then it recommends that the SIF should be considered to update the test interval. To update components test intervals, NOG 070 refers to the SINTEF PDF report "Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase." In short, the method presented in the PDS report is as follows:

1. Calculate updated failure rates for dangerous undetected failures (DU) based on operational experience, or by combining operational experience with generic failure rate data

2. Establish a 90% confidence interval for DU

3. Based on the 90% confidence interval, the following criteria is proposed for updating the test intervals by comparing with the originally assumed (generic) rate of dangerous undetected failures (DU):

If the updated failure rate is less than half assumed failure rate and entire estimated 90% confidence interval for updated failure rate is below assumed failure rate, then functional test interval can be considered doubled.

if the updated failure rate is more than twice and etire estimated 90% confidence interval for updated failure rate is above assumed, then functional test interval must be halved

Moreover, The guideline states that qualitative evaluations on factors such as the quality, confidence and relevance in collected data, quality of testing, number of operational hours, types of failures, benefits are practicalities of changing test intervals.

Appendix B

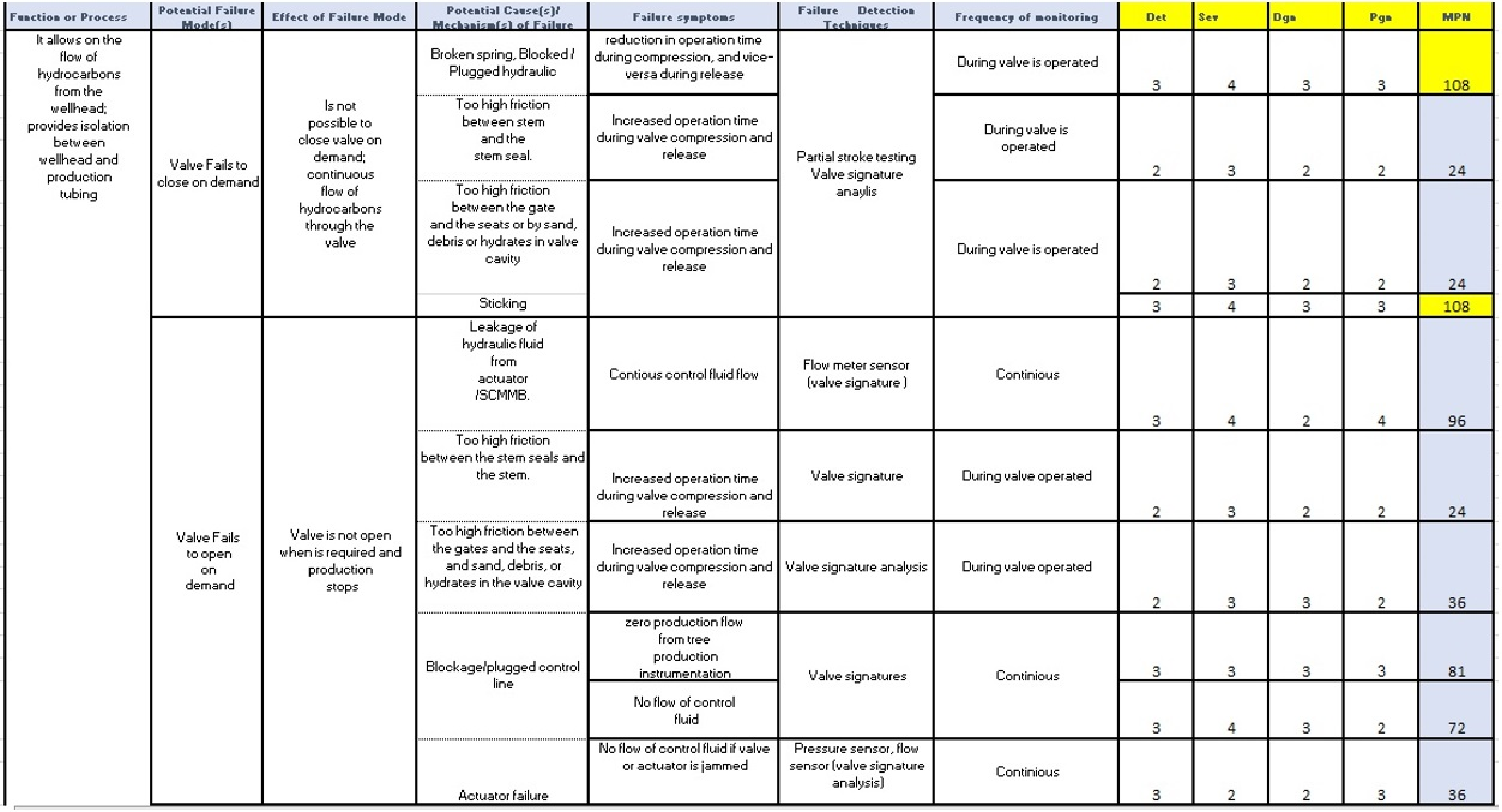
Appendix: (Interview Questions Asked by Primary Source)

- In your experience, how often do these valves (in particular gate valves and choke valves) on XT fail?
- How often do you perform preventive/corrective maintenance on these valves?
- In your opinion, are the current maintenance procedures good enough for you to always follow them?
- What are the most common failure causes for these valves?
- Are your company willing to look at any potential improvements that can be done to reduce the cost of these valves?

Appendix C

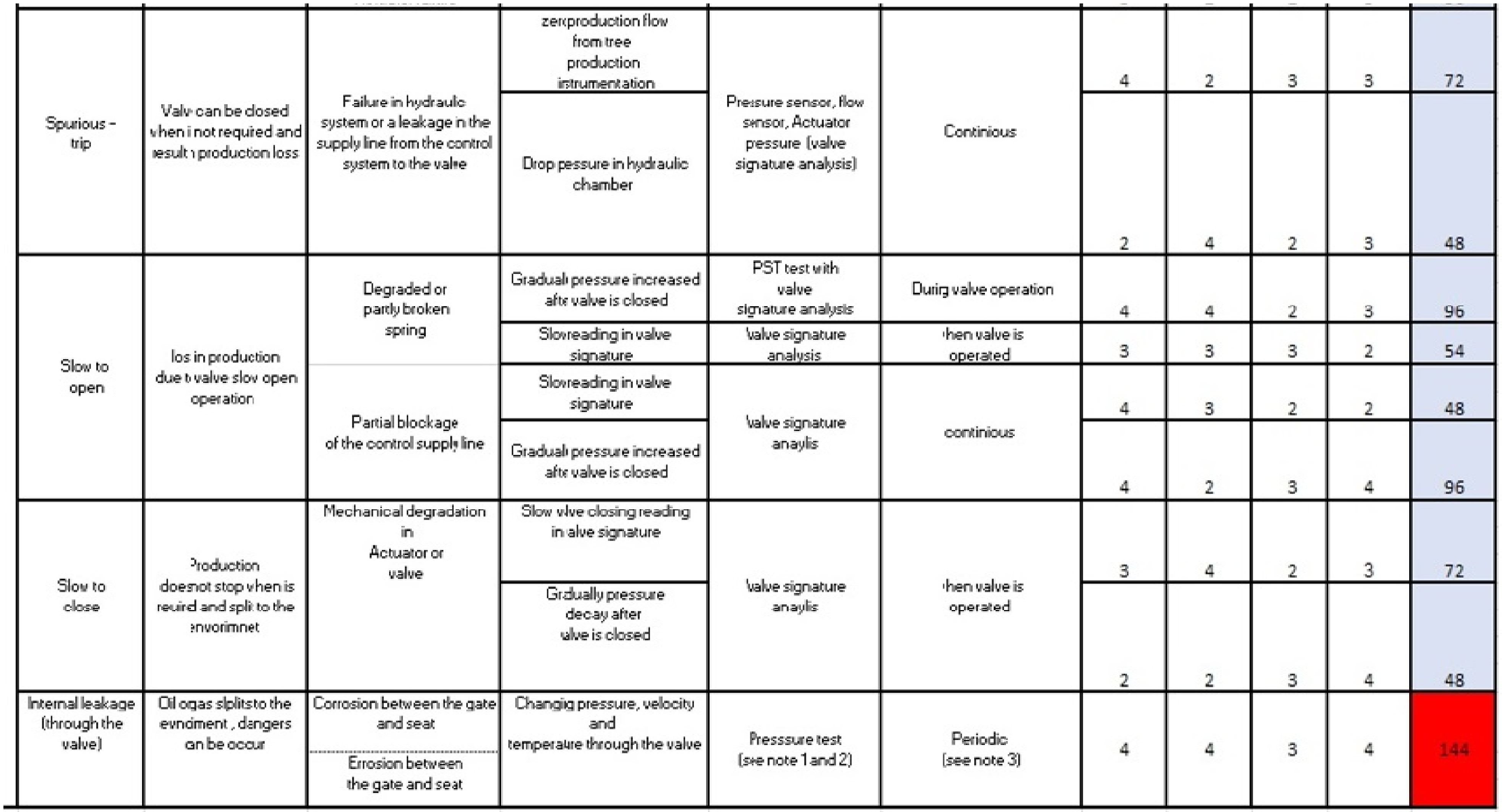
Appendix: (Failure Mode and Symptom Analysis)

The table below illustrates Failure mode and Symptoms analysis for the production master valve and production wing valve. The table gives us information about which symptom can detect the critical failure modes in barrier valves. Failure mode that is marked with red color has been taken from TechnipFMC's FMECA report. As this failure mode is most vital, it is analyzed and recommended, which symptom can detect this failure mode.



Function or Process	Potential Failure Mode(s)	Effect of Failure Mode	Potential Cause(s)/ Mechanism(s) of Failure	Failure symptoms	Failure Detection Techniques	Frequency of monitoring	Det	Sev	Dga	Pga	MPN
It allows on the flow of hydrocarbons from the wellhead; provides isolation between wellhead and production tubing	Valve Fails to close on demand	Is not possible to close valve on demand; continuous flow of hydrocarbons through the valve	Broken spring, Blocked / Plugged hydraulic	reduction in operation time during compression, and vice-versa during release	Partial stroke testing Valve signature anaylis	During valve is operated	3	4	3	3	108
			Too high friction between stem and the stem seal.	Increased operation time during valve compression and release		During valve is operated	2	3	2	2	24
			Too high friction between the gate and the seats or by sand, debris or hydrates in valve cavity	Increased operation time during valve compression and release		During valve is operated	2	3	2	2	24
			Sticking				3	4	3	3	108
	Valve Fails to open on demand	Valve is not open when is required and production stops	Leakage of hydraulic fluid from actuator /SCMMB.	Contious control fluid flow	Flow meter sensor (valve signature)	Continious	3	4	2	4	96
			Too high friction between the stem seals and the stem.	Increased operation time during valve compression and release	Valve signature	During valve operated	2	3	2	2	24
			Too high friction between the gates and the seats, and sand, debris, or hydrates in the valve cavity	Increased operation time during valve compression and release	Valve signature analysis	During valve operated	2	3	3	2	36
			Blockage/plugged control line	zero production flow from tree production instrumentation	Valve signatures	Continious	3	3	3	3	81
				No flow of control fluid			3	4	3	2	72
			Actuator failure	No flow of control fluid if valve or actuator is jammed	Pressure sensor, flow sensor (valve signature analysis)	Continious	3	2	2	3	36

Table C.1: Failure Mode Symptom Analysis for PMV,PWV and DHSV



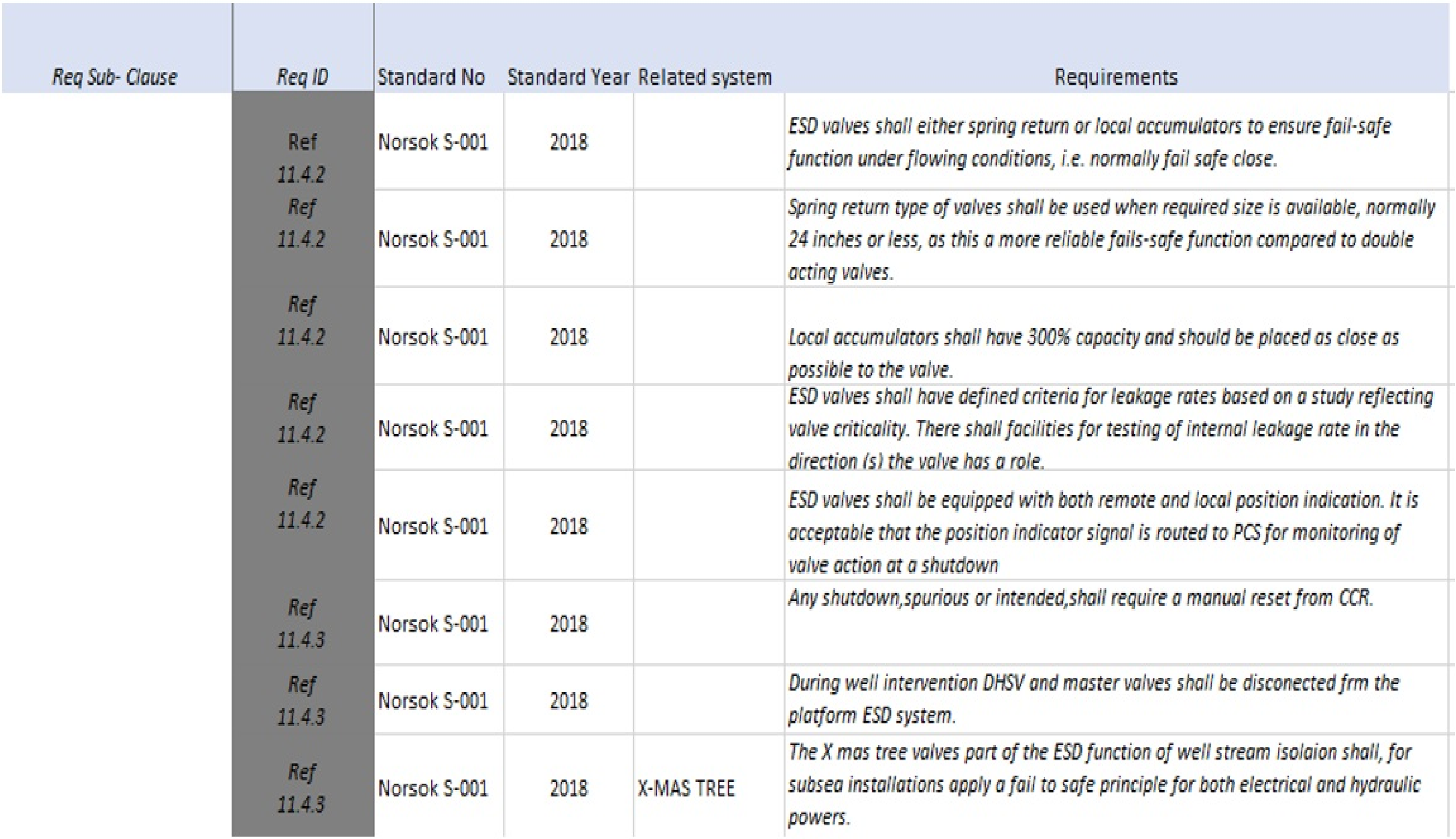
Spurious - trip	Valv can be dosed vhen i not required and esult 1 production loss	Failure in hydraulic system or a leakage n the supply line from the control system to the valve	zerproduction flow from tree production istrumentation	Presure sensor, flow sensor, Actuator pessure (valve signature analysis)	Continious	4	2	3	3	72
			Drop pessure in hydraulic chamber			2	4	2	3	48
Slow to open	los in production due t valve slov open operation	Degraded or partly broken spring	Graduali pressure increased aftr valve is closed	PST test with valve signature analysis	Durig valve operation	4	4	2	3	96
			Slowreading in valve signature	Valve signature analysis	'hen valve is operated	3	3	3	2	54
		Partial blockage of the control supply line	Slowreading in valve signature	Valve signature anaylis	continious	4	3	2	2	48
			Graduali pressure increased aftr valve is closed			4	2	3	4	96
Slow to close	Production doesnot stop vhen is reuird and split to the envorimnet	Mechanical degradation in Actuator or valve	Slow vlve closing reading in alve signature	Valve signature anaylis	'hen valve is operated	3	4	2	3	72
			Grdually pressure decay after valve is closed			2	2	3	4	48
Internal leakage (through the valve)	Oil ogas slplits to the evndiment , dangers an be occur	Corrosion between the gate and seat Erosion between the gate and seat	Changig pressure, velocity and temperatue through the valve	Presssure test (see note 1 and 2)	Periodic (see note 3)	4	4	3	4	144

Table C.2: Failure Mode Symptom Analysis for PMV,PWV and DHSV (Continued)

Appendix D

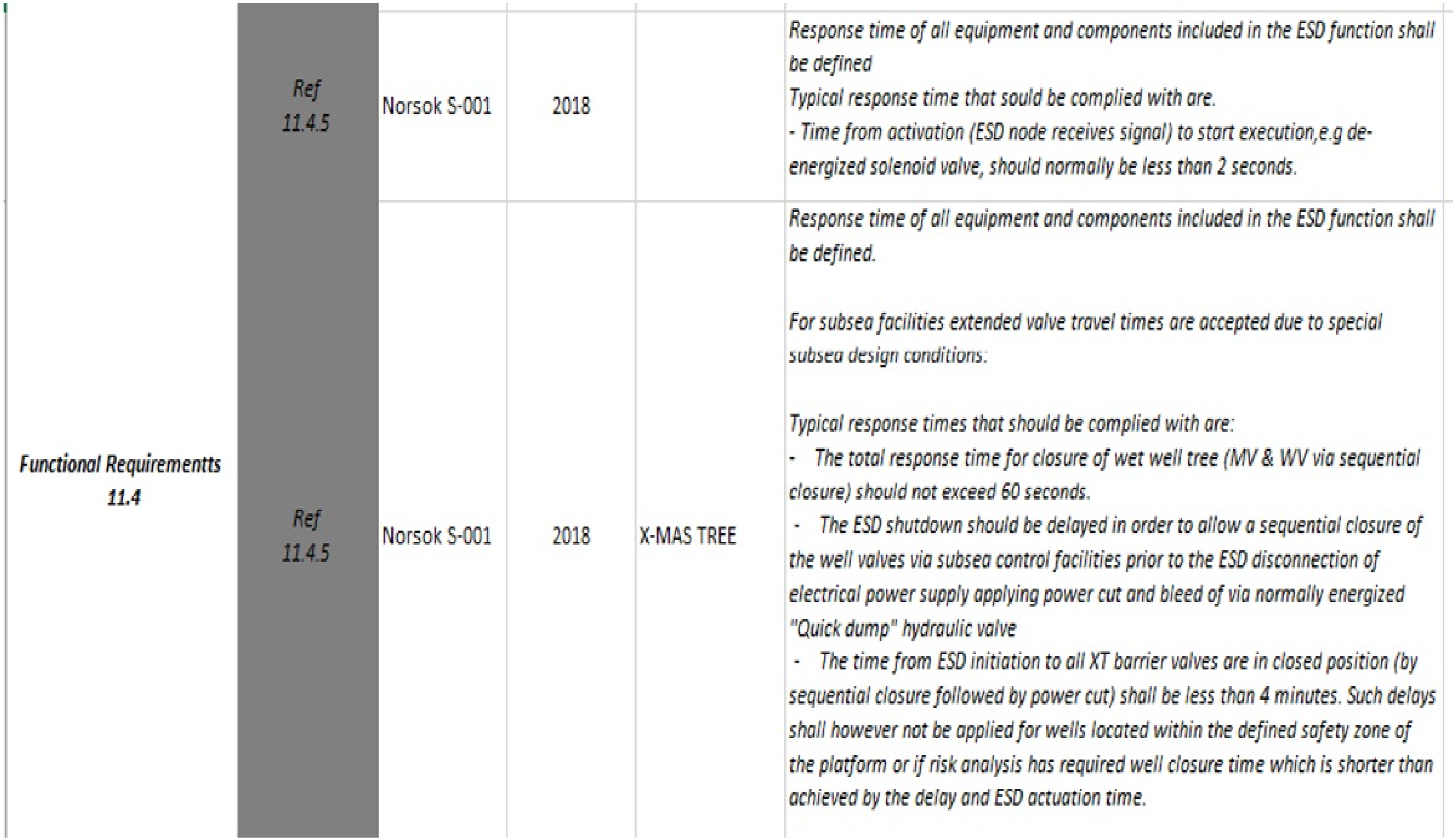
Appendix: (General Requirements for Barrier Valves)

The table below illustrates elicited requirements for barrier valves from standards such as Norsok S001, Norsok Z008, IEC 61511, IEC 61508 and NOG-070.

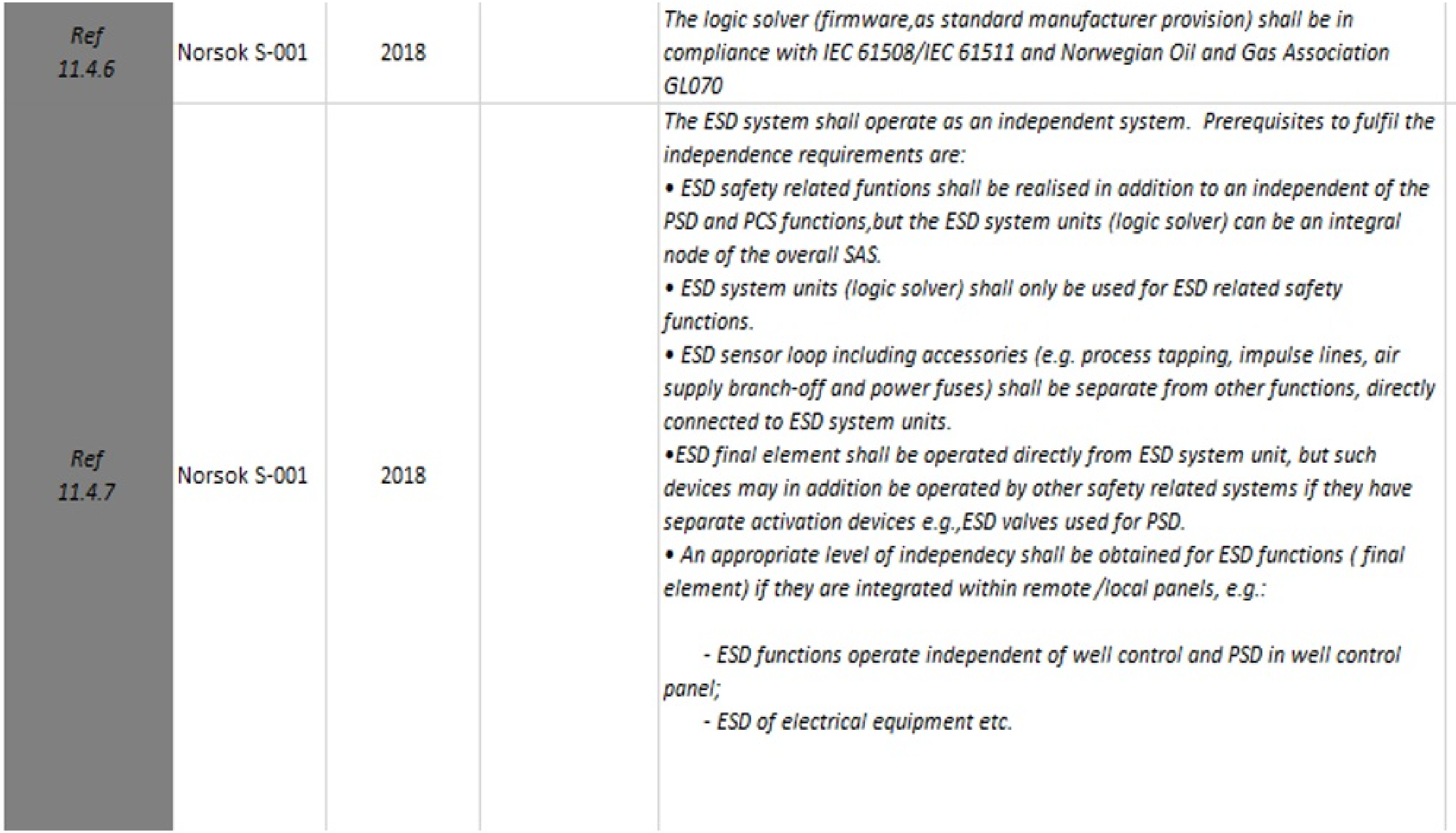


Req Sub- Clause	Req ID	Standard No	Standard Year	Related system	Requirements
	Ref 11.4.2	Norsok S-001	2018		ESD valves shall either spring return or local accumulators to ensure fail-safe function under flowing conditions, i.e. normally fail safe close.
	Ref 11.4.2	Norsok S-001	2018		Spring return type of valves shall be used when required size is available, normally 24 inches or less, as this a more reliable fails-safe function compared to double acting valves.
	Ref 11.4.2	Norsok S-001	2018		Local accumulators shall have 300% capacity and should be placed as close as possible to the valve.
	Ref 11.4.2	Norsok S-001	2018		ESD valves shall have defined criteria for leakage rates based on a study reflecting valve criticality. There shall facilities for testing of internal leakage rate in the direction (s) the valve has a role.
	Ref 11.4.2	Norsok S-001	2018		ESD valves shall be equipped with both remote and local position indication. It is acceptable that the position indicator signal is routed to PCS for monitoring of valve action at a shutdown
	Ref 11.4.3	Norsok S-001	2018		Any shutdown,spurious or intended,shall require a manual reset from CCR.
	Ref 11.4.3	Norsok S-001	2018		During well intervention DHSV and master valves shall be disconected frm the platform ESD system.
	Ref 11.4.3	Norsok S-001	2018	X-MAS TREE	The X mas tree valves part of the ESD function of well stream isolaion shall, for subsea installations apply a fail to safe principle for both electrical and hydraulic powers.

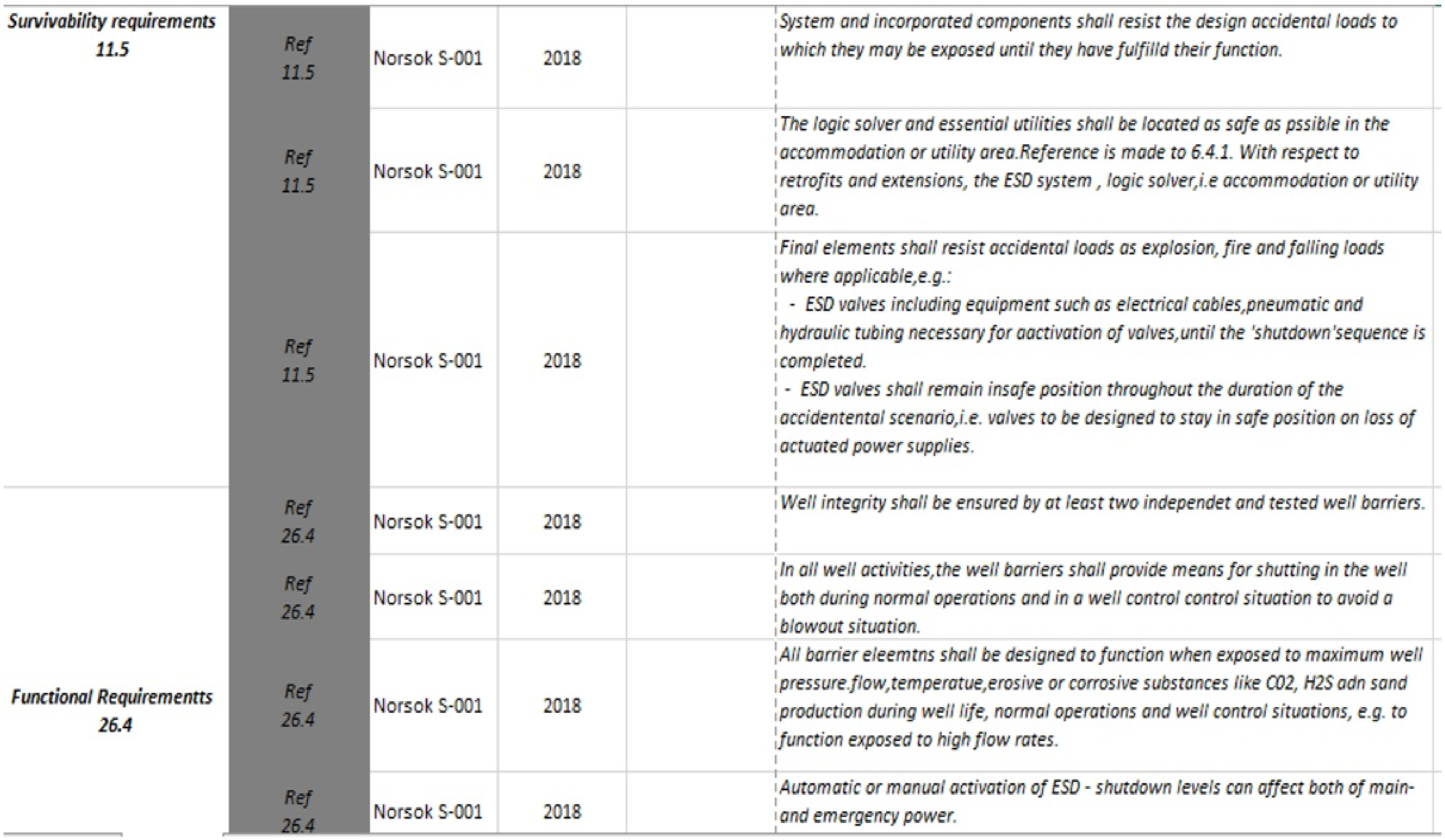
Table D.1: Failure Mode Symptom Analysis for PMV and PWV (Continued)



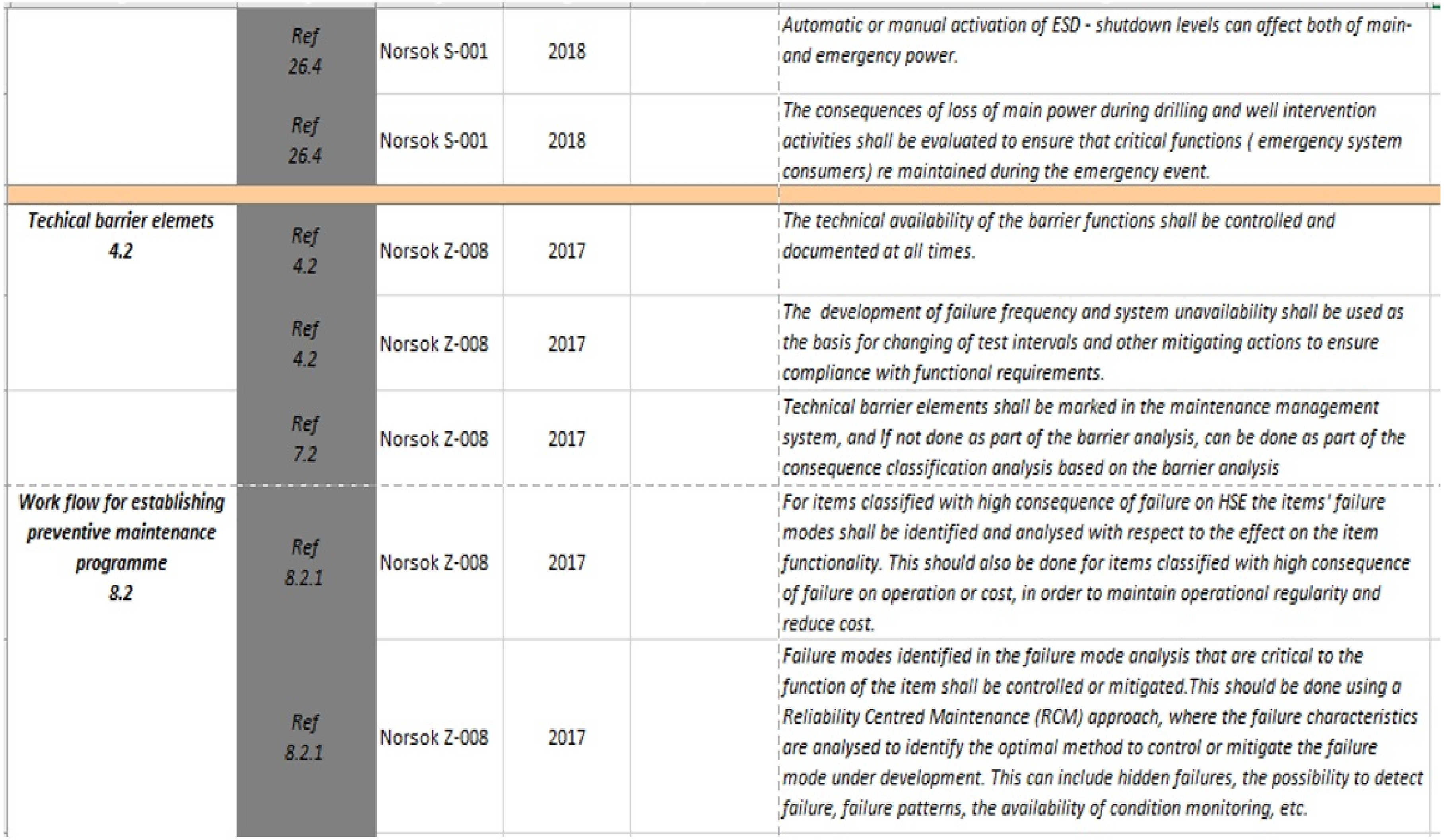
Functional Requirementts 11.4	*Ref 11.4.5*	Norsok S-001	2018		*Response time of all equipment and components included in the ESD function shall be defined* *Typical response time that sould be complied with are.* *- Time from activation (ESD node receives signal) to start execution,e.g de-energized solenoid valve, should normally be less than 2 seconds.*
	Ref 11.4.5	Norsok S-001	2018	X-MAS TREE	*Response time of all equipment and components included in the ESD function shall be defined.* *For subsea facilities extended valve travel times are accepted due to special subsea design conditions:* *Typical response times that should be complied with are:* *- The total response time for closure of wet well tree (MV & WV via sequential closure) should not exceed 60 seconds.* *- The ESD shutdown should be delayed in order to allow a sequential closure of the well valves via subsea control facilities prior to the ESD disconnection of electrical power supply applying power cut and bleed of via normally energized "Quick dump" hydraulic valve* *- The time from ESD initiation to all XT barrier valves are in closed position (by sequential closure followed by power cut) shall be less than 4 minutes. Such delays shall however not be applied for wells located within the defined safety zone of the platform or if risk analysis has required well closure time which is shorter than achieved by the delay and ESD actuation time.*



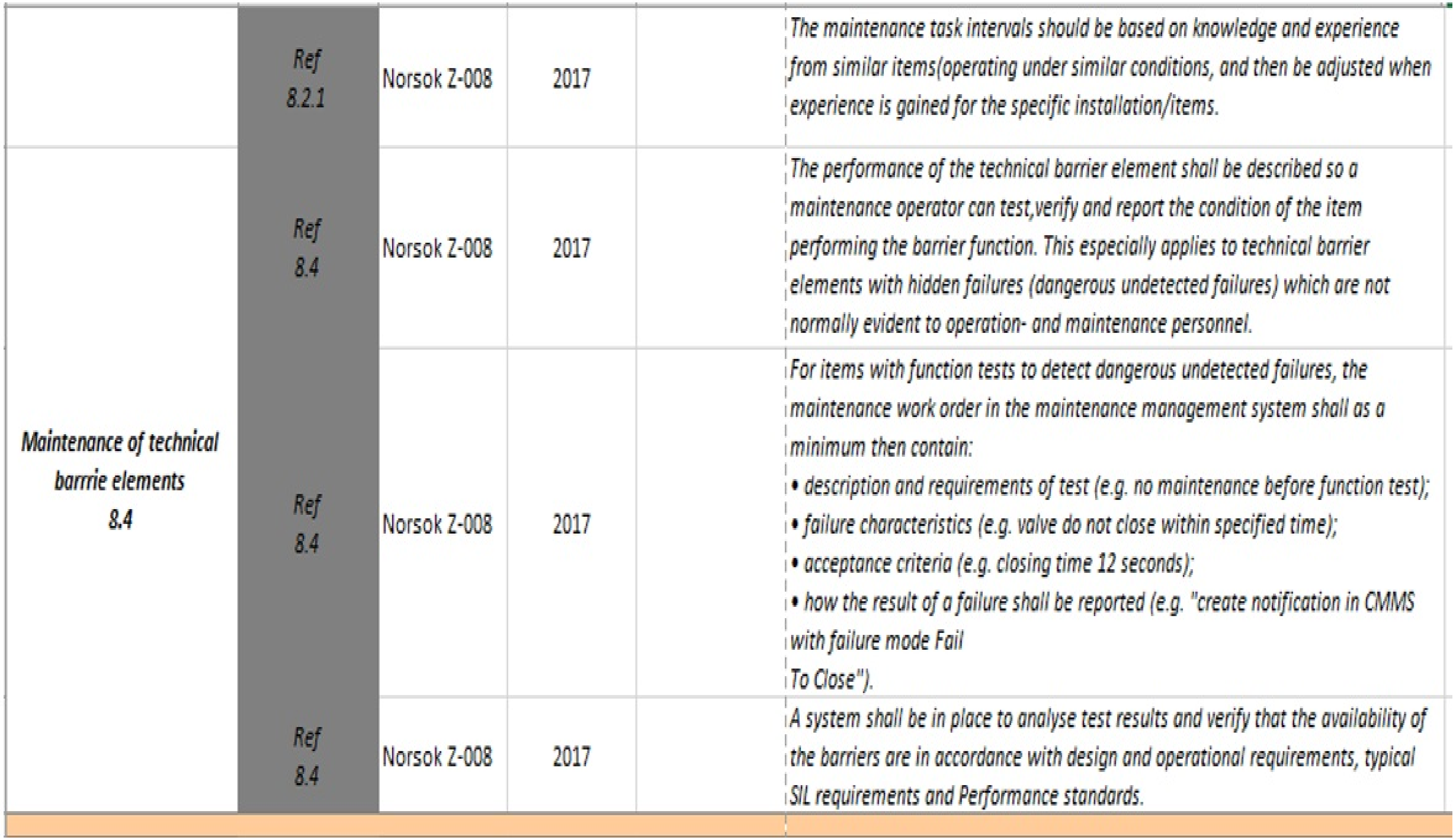
Ref 11.4.6	Norsok S-001	2018		*The logic solver (firmware,as standard manufacturer provision) shall be in compliance with IEC 61508/IEC 61511 and Norwegian Oil and Gas Association GL070*
Ref 11.4.7	Norsok S-001	2018		*The ESD system shall operate as an independent system. Prerequisites to fulfil the independence requirements are:* *• ESD safety related funtions shall be realised in addition to an independent of the PSD and PCS functions,but the ESD system units (logic solver) can be an integral node of the overall SAS.* *• ESD system units (logic solver) shall only be used for ESD related safety functions.* *• ESD sensor loop including accessories (e.g. process tapping, impulse lines, air supply branch-off and power fuses) shall be separate from other functions, directly connected to ESD system units.* *•ESD final element shall be operated directly from ESD system unit, but such devices may in addition be operated by other safety related systems if they have separate activation devices e.g.,ESD valves used for PSD.* *• An appropriate level of independecy shall be obtained for ESD functions (final element) if they are integrated within remote /local panels, e.g.:* *- ESD functions operate independent of well control and PSD in well control panel;* *- ESD of electrical equipment etc.*



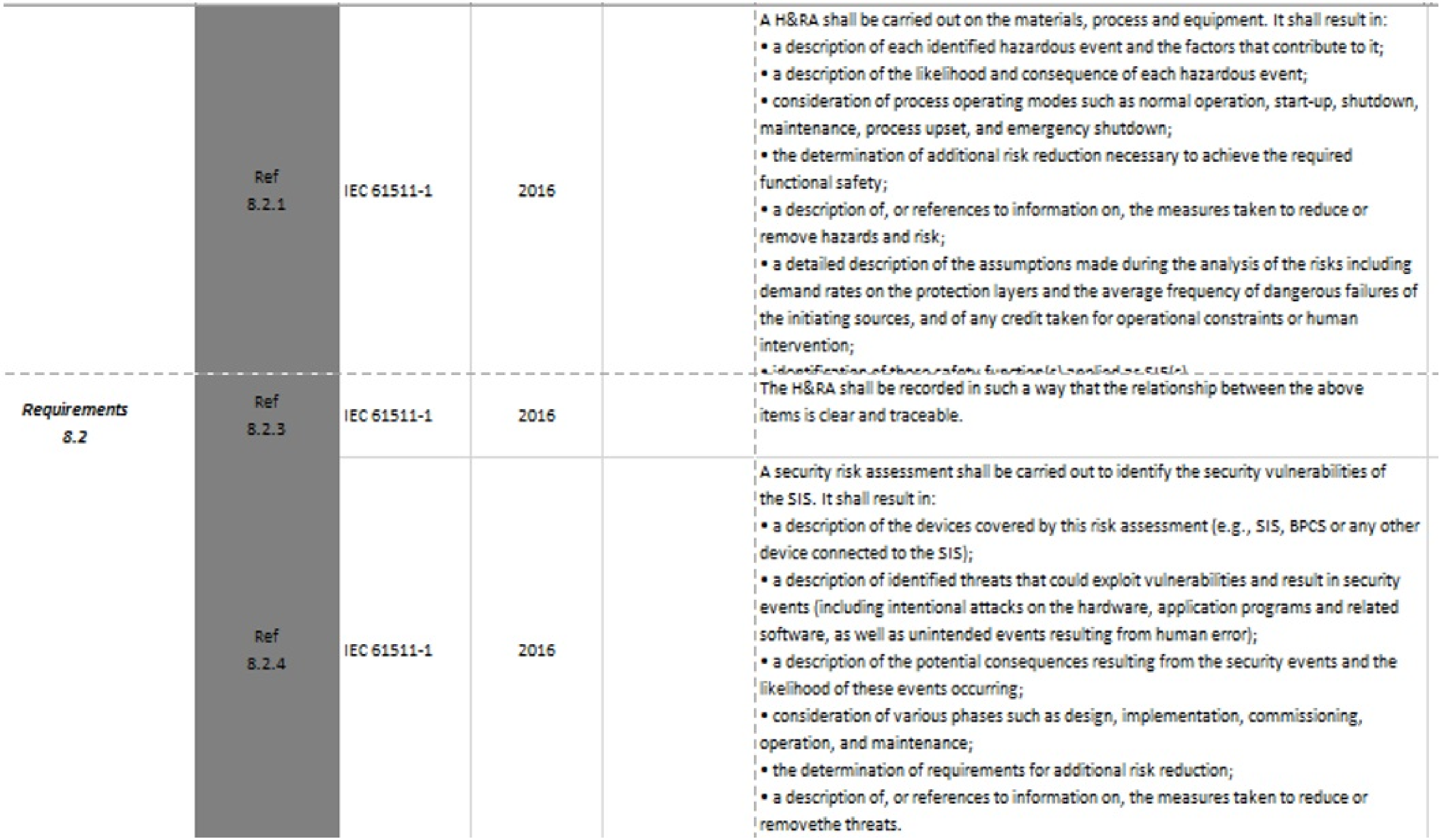
Survivability requirements 11.5	*Ref 11.5*	Norsok S-001	2018		*System and incorporated components shall resist the design accidental loads to which they may be exposed until they have fulfilld their function.*
	Ref 11.5	Norsok S-001	2018		*The logic solver and essential utilities shall be located as safe as pssible in the accommodation or utility area.Reference is made to 6.4.1. With respect to retrofits and extensions, the ESD system , logic solver,i.e accommodation or utility area.*
	Ref 11.5	Norsok S-001	2018		*Final elements shall resist accidental loads as explosion, fire and falling loads where applicable,e.g.:* *- ESD valves including equipment such as electrical cables,pneumatic and hydraulic tubing necessary for aactivation of valves,until the 'shutdown'sequence is completed.* *- ESD valves shall remain insafe position throughout the duration of the accidentental scenario,i.e. valves to be designed to stay in safe position on loss of actuated power supplies.*
Functional Requirementts 26.4	*Ref 26.4*	Norsok S-001	2018		*Well integrity shall be ensured by at least two independet and tested well barriers.*
	Ref 26.4	Norsok S-001	2018		*In all well activities,the well barriers shall provide means for shutting in the well both during normal operations and in a well control control situation to avoid a blowout situation.*
	Ref 26.4	Norsok S-001	2018		*All barrier eleemtns shall be designed to function when exposed to maximum well pressure.flow,temperatue,erosive or corrosive substances like C02, H2S adn sand production during well life, normal operations and well control situations, e.g. to function exposed to high flow rates.*
	Ref 26.4	Norsok S-001	2018		*Automatic or manual activation of ESD - shutdown levels can affect both of main- and emergency power.*



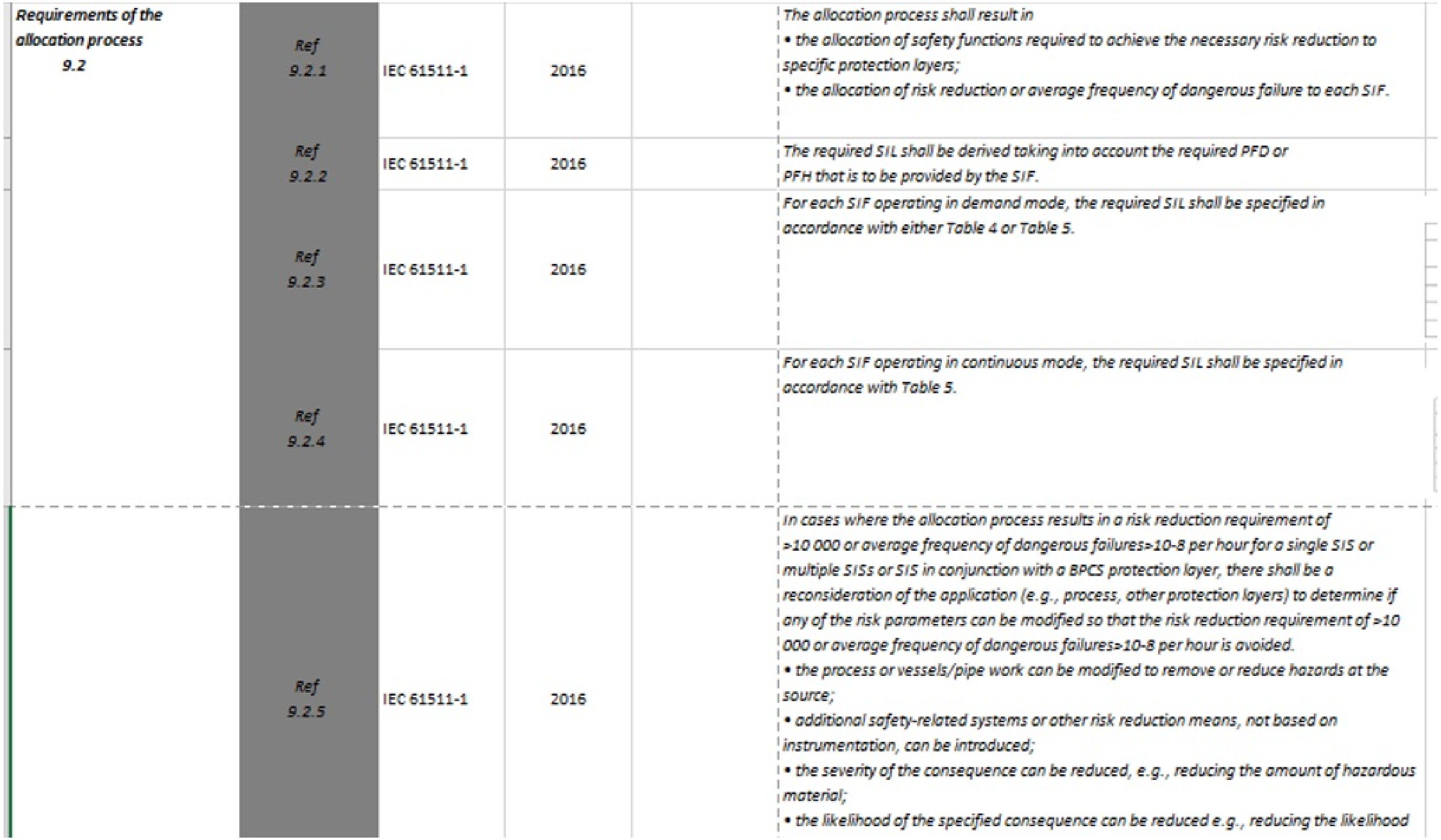
	Ref 26.4	Norsok S-001	2018		Automatic or manual activation of ESD - shutdown levels can affect both of main- and emergency power.
	Ref 26.4	Norsok S-001	2018		The consequences of loss of main power during drilling and well intervention activities shall be evaluated to ensure that critical functions (emergency system consumers) re maintained during the emergency event.
Techical barrier elemets **4.2**	Ref 4.2	Norsok Z-008	2017		The technical availability of the barrier functions shall be controlled and documented at all times.
	Ref 4.2	Norsok Z-008	2017		The development of failure frequency and system unavailability shall be used as the basis for changing of test intervals and other mitigating actions to ensure compliance with functional requirements.
	Ref 7.2	Norsok Z-008	2017		Technical barrier elements shall be marked in the maintenance management system, and If not done as part of the barrier analysis, can be done as part of the consequence classification analysis based on the barrier analysis
Work flow for establishing preventive maintenance programme **8.2**	Ref 8.2.1	Norsok Z-008	2017		For items classified with high consequence of failure on HSE the items' failure modes shall be identified and analysed with respect to the effect on the item functionality. This should also be done for items classified with high consequence of failure on operation or cost, in order to maintain operational regularity and reduce cost.
	Ref 8.2.1	Norsok Z-008	2017		Failure modes identified in the failure mode analysis that are critical to the function of the item shall be controlled or mitigated.This should be done using a Reliability Centred Maintenance (RCM) approach, where the failure characteristics are analysed to identify the optimal method to control or mitigate the failure mode under development. This can include hidden failures, the possibility to detect failure, failure patterns, the availability of condition monitoring, etc.



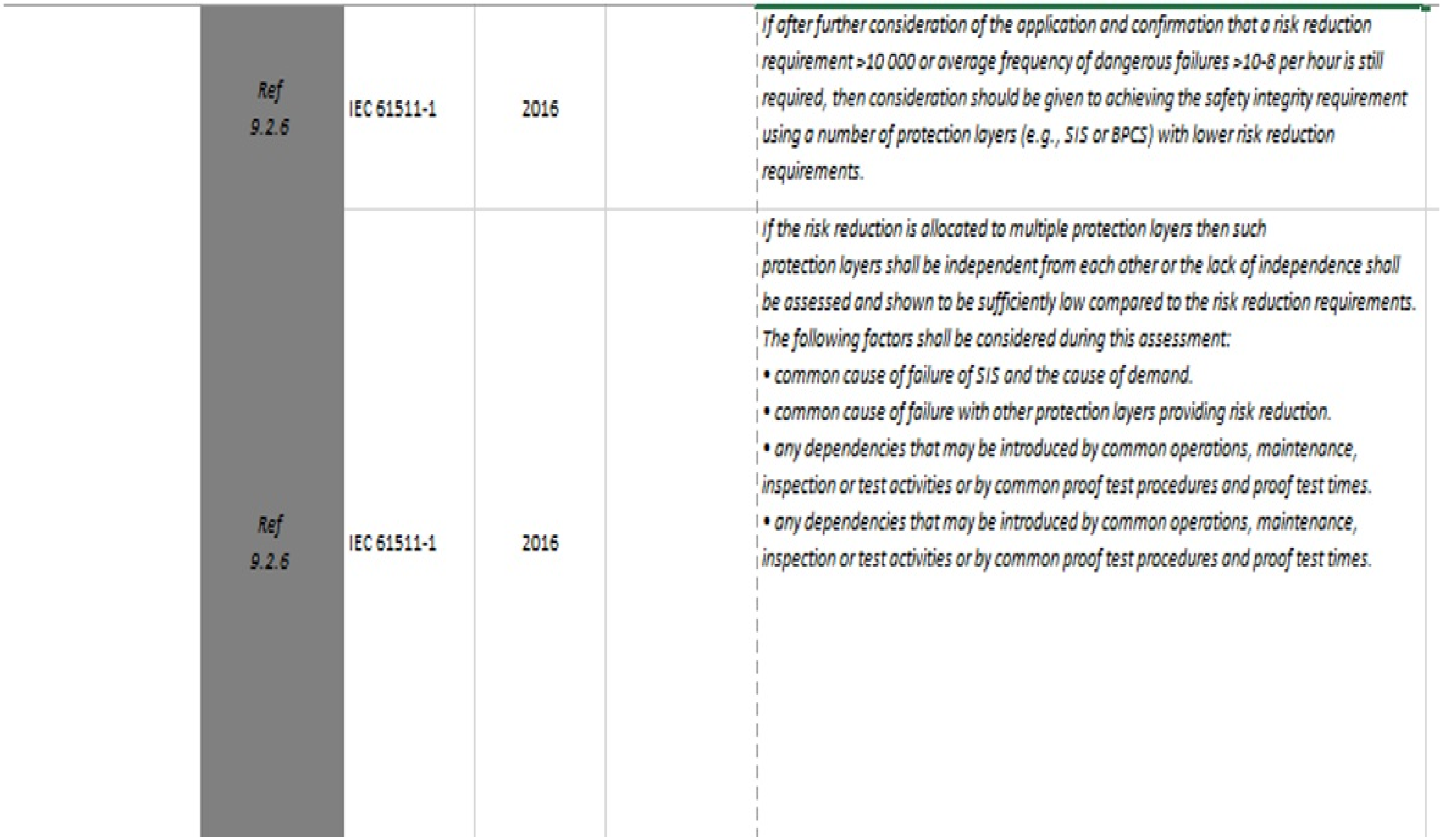
	Ref *8.2.1*	Norsok Z-008	2017		*The maintenance task intervals should be based on knowledge and experience from similar items(operating under similar conditions, and then be adjusted when experience is gained for the specific installation/items.*
Maintenance of technical barrie elements 8.4	*Ref* *8.4*	Norsok Z-008	2017		*The performance of the technical barrier element shall be described so a maintenance operator can test,verify and report the condition of the item performing the barrier function. This especially applies to technical barrier elements with hidden failures (dangerous undetected failures) which are not normally evident to operation- and maintenance personnel.*
	Ref *8.4*	Norsok Z-008	2017		*For items with function tests to detect dangerous undetected failures, the maintenance work order in the maintenance management system shall as a minimum then contain:* • *description and requirements of test (e.g. no maintenance before function test);* • *failure characteristics (e.g. valve do not close within specified time);* • *acceptance criteria (e.g. closing time 12 seconds);* • *how the result of a failure shall be reported (e.g. "create notification in CMMS with failure mode Fail* *To Close").*
	Ref *8.4*	Norsok Z-008	2017		*A system shall be in place to analyse test results and verify that the availability of the barriers are in accordance with design and operational requirements, typical SIL requirements and Performance standards.*



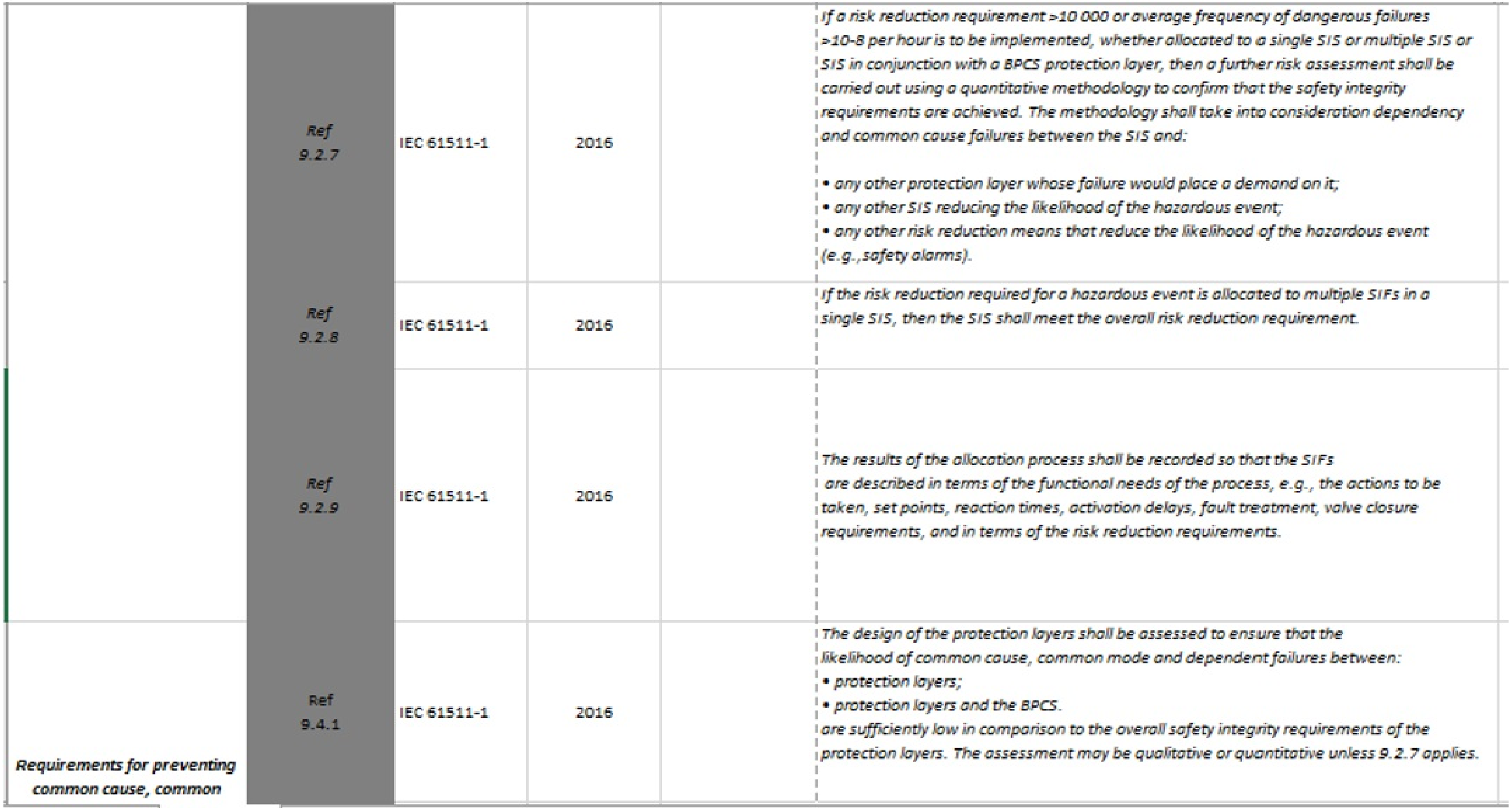
Requirements 8.2	Ref 8.2.1	IEC 61511-1	2016		A H&RA shall be carried out on the materials, process and equipment. It shall result in: • a description of each identified hazardous event and the factors that contribute to it; • a description of the likelihood and consequence of each hazardous event; • consideration of process operating modes such as normal operation, start-up, shutdown, maintenance, process upset, and emergency shutdown; • the determination of additional risk reduction necessary to achieve the required functional safety; • a description of, or references to information on, the measures taken to reduce or remove hazards and risk; • a detailed description of the assumptions made during the analysis of the risks including demand rates on the protection layers and the average frequency of dangerous failures of the initiating sources, and of any credit taken for operational constraints or human intervention; • identification of those safety function(s) applied as SIS(s)
	Ref 8.2.3	IEC 61511-1	2016		The H&RA shall be recorded in such a way that the relationship between the above items is clear and traceable.
	Ref 8.2.4	IEC 61511-1	2016		A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. It shall result in: • a description of the devices covered by this risk assessment (e.g., SIS, BPCS or any other device connected to the SIS); • a description of identified threats that could exploit vulnerabilities and result in security events (including intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error); • a description of the potential consequences resulting from the security events and the likelihood of these events occurring; • consideration of various phases such as design, implementation, commissioning, operation, and maintenance; • the determination of requirements for additional risk reduction; • a description of, or references to information on, the measures taken to reduce or removethe threats.



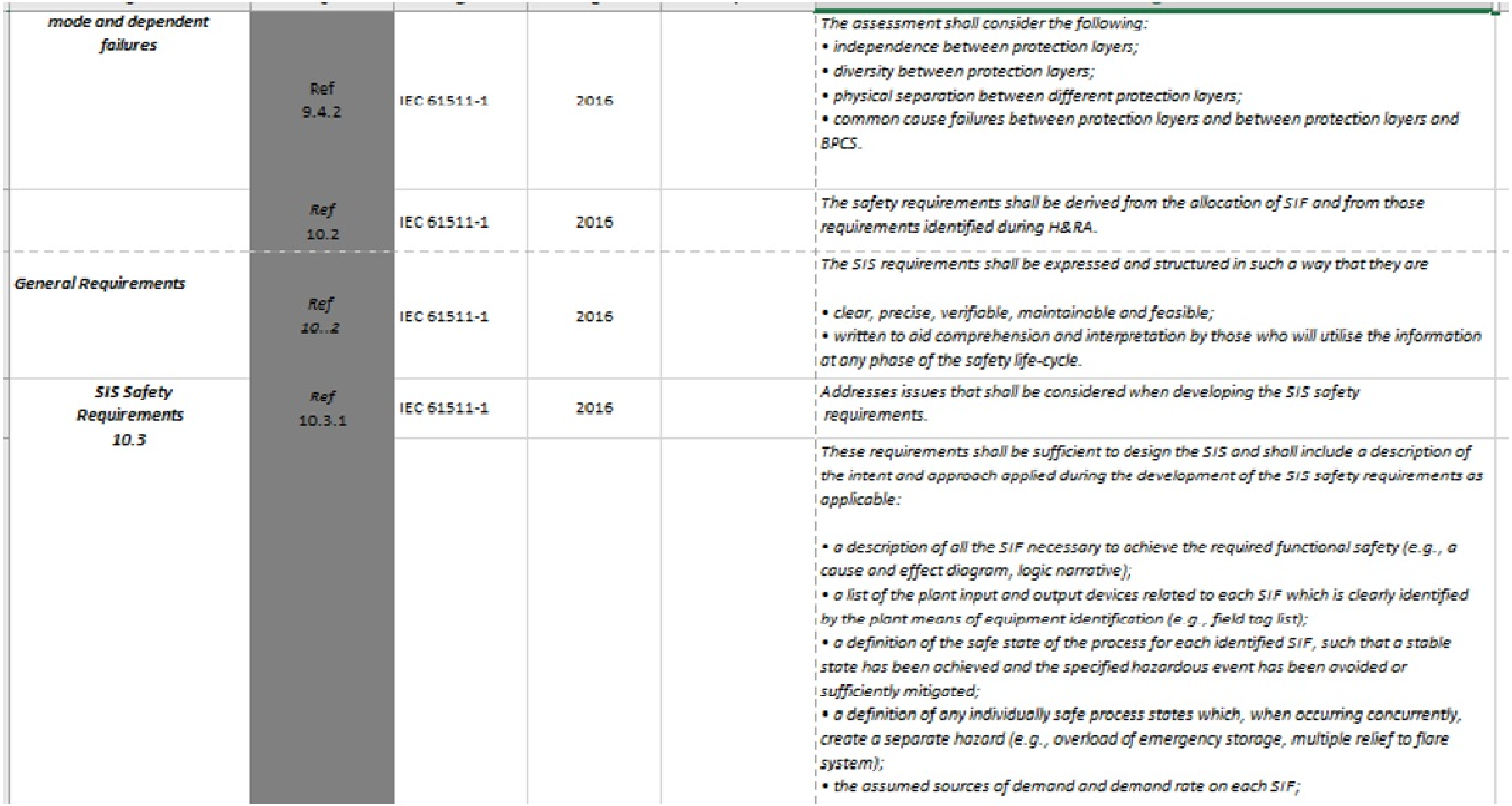
Requirements of the allocation process ***9.2***	*Ref* *9.2.1*	IEC 61511-1	2016		*The allocation process shall result in* *• the allocation of safety functions required to achieve the necessary risk reduction to specific protection layers;* *• the allocation of risk reduction or average frequency of dangerous failure to each SIF.*
	Ref *9.2.2*	IEC 61511-1	2016		*The required SIL shall be derived taking into account the required PFD or PFH that is to be provided by the SIF.*
	Ref *9.2.3*	IEC 61511-1	2016		*For each SIF operating in demand mode, the required SIL shall be specified in accordance with either Table 4 or Table 5.*
	Ref *9.2.4*	IEC 61511-1	2016		*For each SIF operating in continuous mode, the required SIL shall be specified in accordance with Table 5.*
	Ref *9.2.5*	IEC 61511-1	2016		*In cases where the allocation process results in a risk reduction requirement of >10 000 or average frequency of dangerous failures>10-8 per hour for a single SIS or multiple SISs or SIS in conjunction with a BPCS protection layer, there shall be a reconsideration of the application (e.g., process, other protection layers) to determine if any of the risk parameters can be modified so that the risk reduction requirement of >10 000 or average frequency of dangerous failures>10-8 per hour is avoided.* *• the process or vessels/pipe work can be modified to remove or reduce hazards at the source;* *• additional safety-related systems or other risk reduction means, not based on instrumentation, can be introduced;* *• the severity of the consequence can be reduced, e.g., reducing the amount of hazardous material;* *• the likelihood of the specified consequence can be reduced e.g., reducing the likelihood*



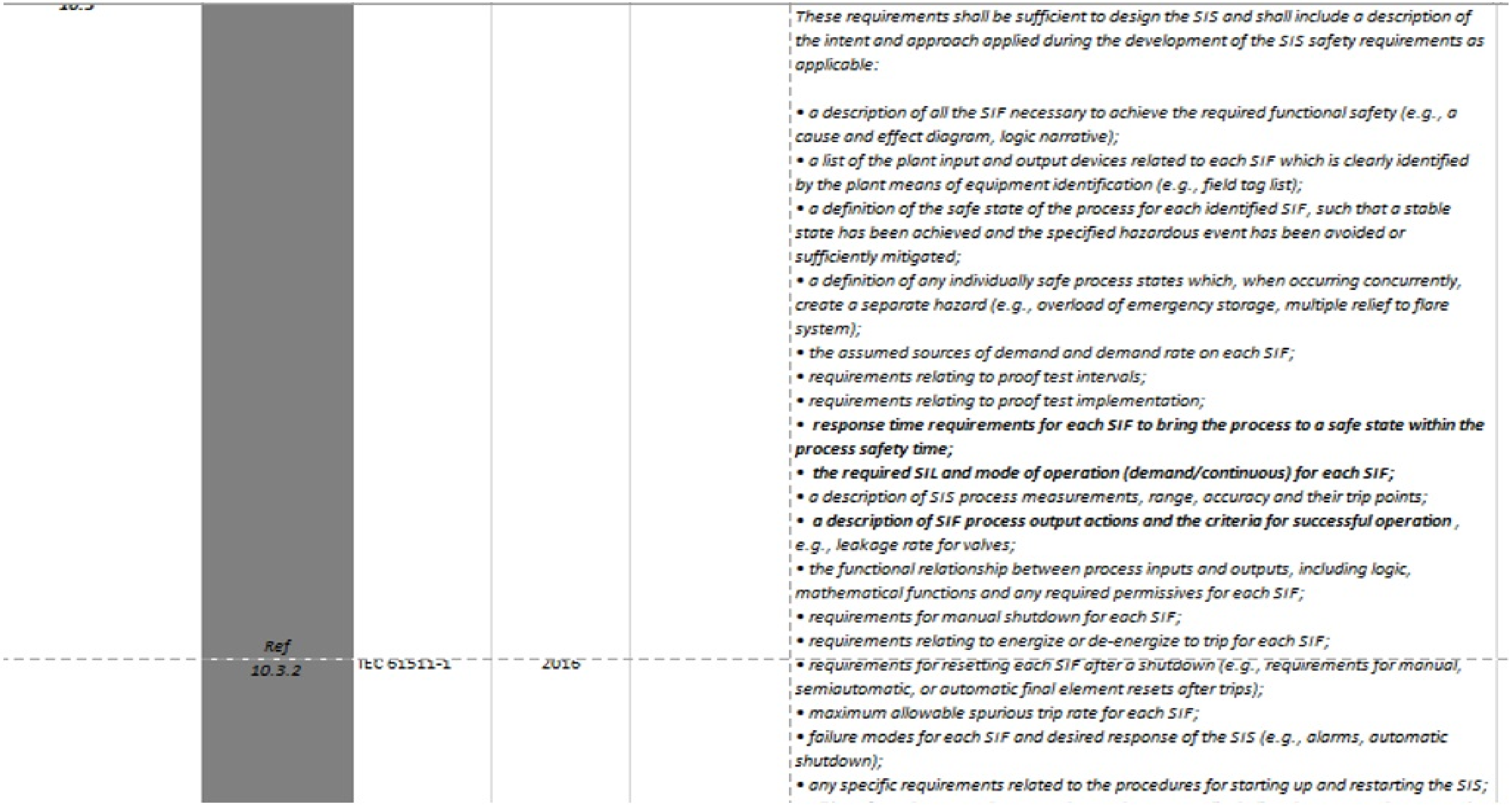
Ref *9.2.6*	IEC 61511-1	2016		*If after further consideration of the application and confirmation that a risk reduction requirement >10 000 or average frequency of dangerous failures >10-8 per hour is still required, then consideration should be given to achieving the safety integrity requirement using a number of protection layers (e.g., SIS or BPCS) with lower risk reduction requirements.*
Ref *9.2.6*	IEC 61511-1	2016		*If the risk reduction is allocated to multiple protection layers then such protection layers shall be independent from each other or the lack of independence shall be assessed and shown to be sufficiently low compared to the risk reduction requirements.* *The following factors shall be considered during this assessment:* *• common cause of failure of SIS and the cause of demand.* *• common cause of failure with other protection layers providing risk reduction.* *• any dependencies that may be introduced by common operations, maintenance, inspection or test activities or by common proof test procedures and proof test times.* *• any dependencies that may be introduced by common operations, maintenance, inspection or test activities or by common proof test procedures and proof test times.*



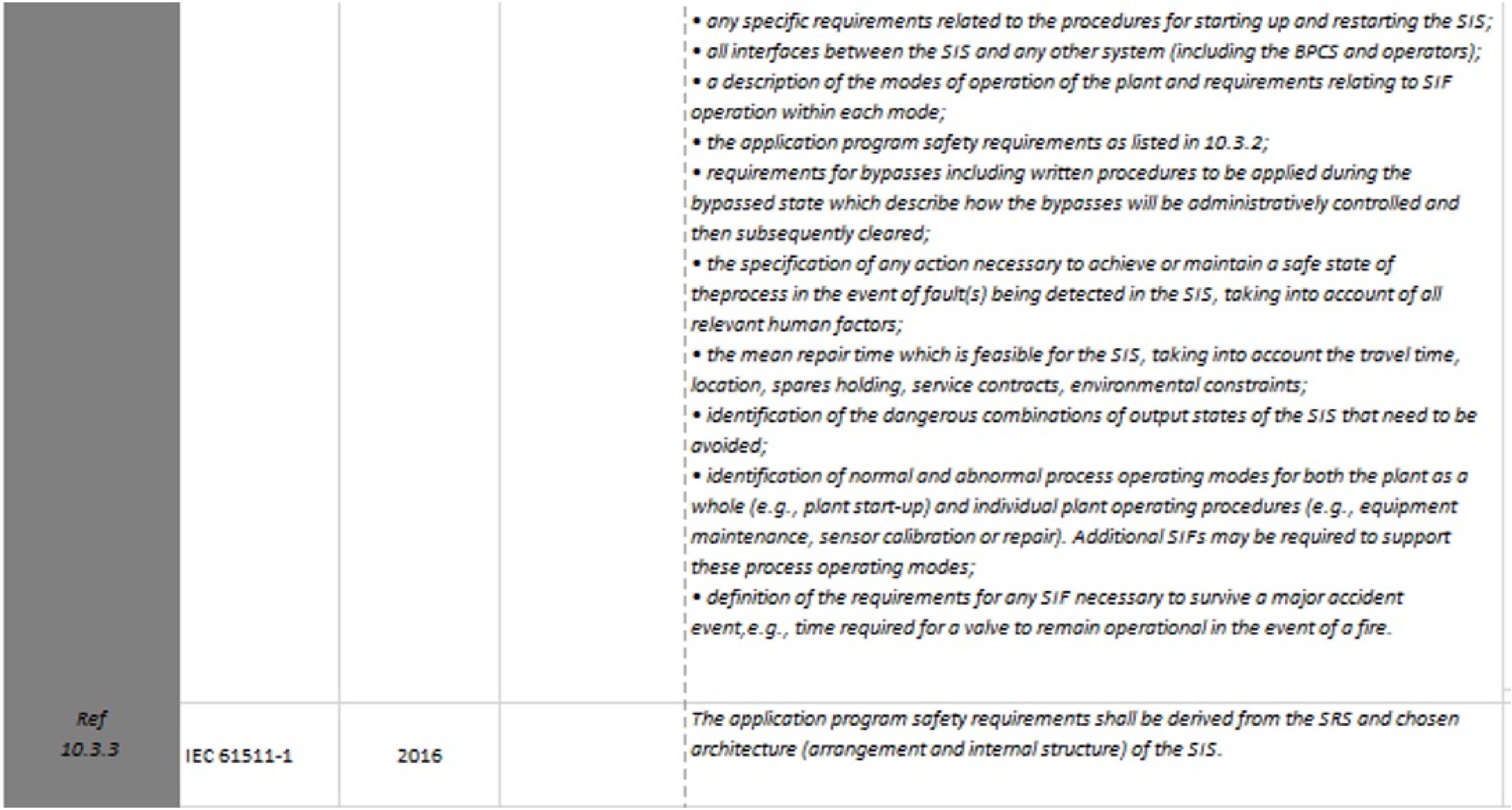
	Ref *9.2.7*	IEC 61511-1	2016		*If a risk reduction requirement >10 000 or average frequency of dangerous failures >10-8 per hour is to be implemented, whether allocated to a single SIS or multiple SIS or SIS in conjunction with a BPCS protection layer, then a further risk assessment shall be carried out using a quantitative methodology to confirm that the safety integrity requirements are achieved. The methodology shall take into consideration dependency and common cause failures between the SIS and:* *• any other protection layer whose failure would place a demand on it;* *• any other SIS reducing the likelihood of the hazardous event;* *• any other risk reduction means that reduce the likelihood of the hazardous event (e.g.,safety alarms).*
	Ref *9.2.8*	IEC 61511-1	2016		*If the risk reduction required for a hazardous event is allocated to multiple SIFs in a single SIS, then the SIS shall meet the overall risk reduction requirement.*
	Ref *9.2.9*	IEC 61511-1	2016		*The results of the allocation process shall be recorded so that the SIFs are described in terms of the functional needs of the process, e.g., the actions to be taken, set points, reaction times, activation delays, fault treatment, valve closure requirements, and in terms of the risk reduction requirements.*
Requirements for preventing common cause, common	Ref 9.4.1	IEC 61511-1	2016		*The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode and dependent failures between:* *• protection layers;* *• protection layers and the BPCS.* *are sufficiently low in comparison to the overall safety integrity requirements of the protection layers. The assessment may be qualitative or quantitative unless 9.2.7 applies.*



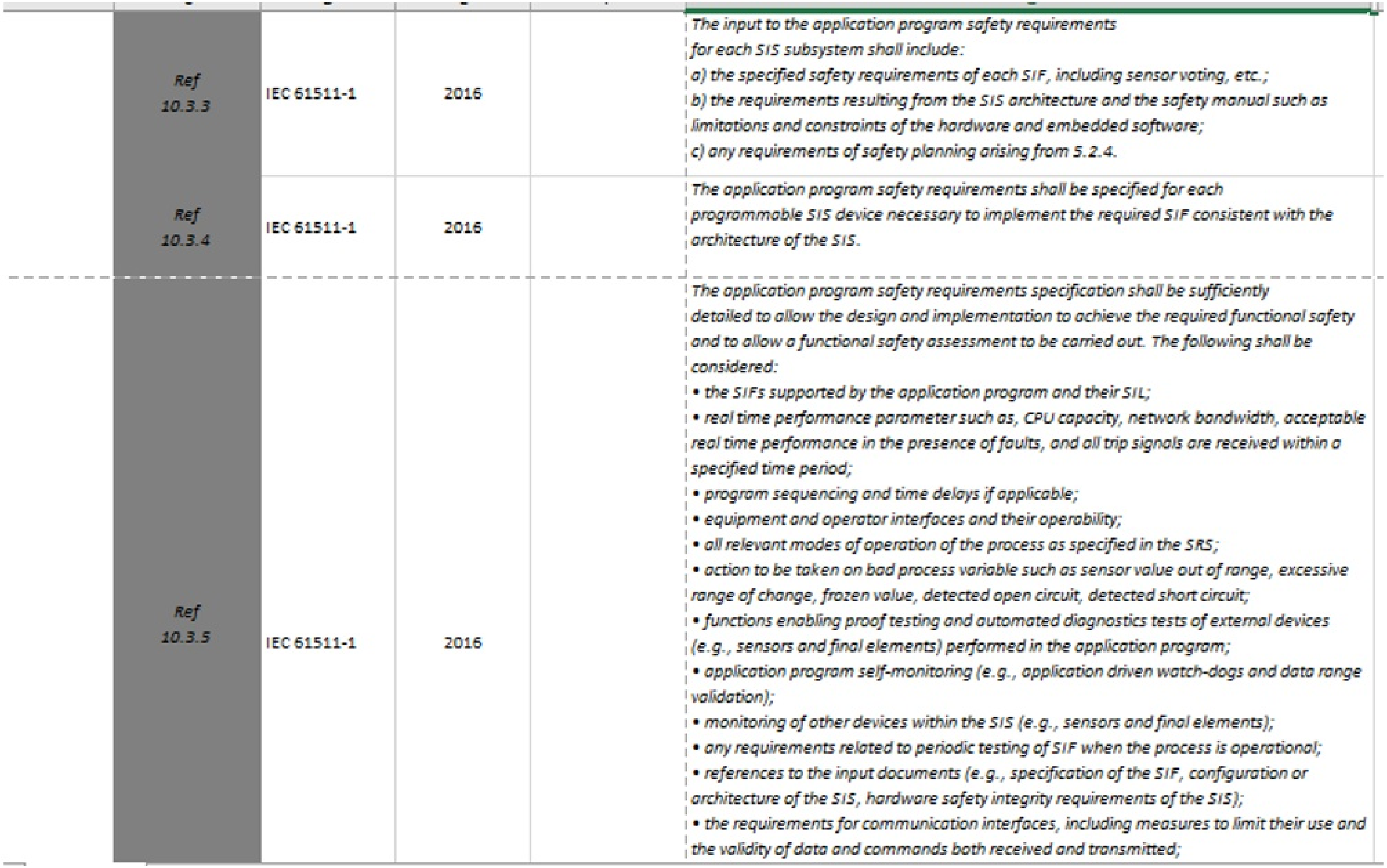
mode and dependent failures	Ref 9.4.2	IEC 61511-1	2016		*The assessment shall consider the following:* *• independence between protection layers;* *• diversity between protection layers;* *• physical separation between different protection layers;* *• common cause failures between protection layers and between protection layers and BPCS.*
	Ref 10.2	IEC 61511-1	2016		*The safety requirements shall be derived from the allocation of SIF and from those requirements identified during H&RA.*
General Requirements	*Ref* *10..2*	IEC 61511-1	2016		*The SIS requirements shall be expressed and structured in such a way that they are* *• clear, precise, verifiable, maintainable and feasible;* *• written to aid comprehension and interpretation by those who will utilise the information at any phase of the safety life-cycle.*
SIS Safety Requirements 10.3	*Ref* 10.3.1	IEC 61511-1	2016		*Addresses issues that shall be considered when developing the SIS safety requirements.*
					These requirements shall be sufficient to design the SIS and shall include a description of the intent and approach applied during the development of the SIS safety requirements as applicable: *• a description of all the SIF necessary to achieve the required functional safety (e.g., a cause and effect diagram, logic narrative);* *• a list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification (e.g., field tag list);* *• a definition of the safe state of the process for each identified SIF, such that a stable state has been achieved and the specified hazardous event has been avoided or sufficiently mitigated;* *• a definition of any individually safe process states which, when occuring concurrently, create a separate hazard (e.g., overload of emergency storage, multiple relief to flare system);* *• the assumed sources of demand and demand rate on each SIF;*



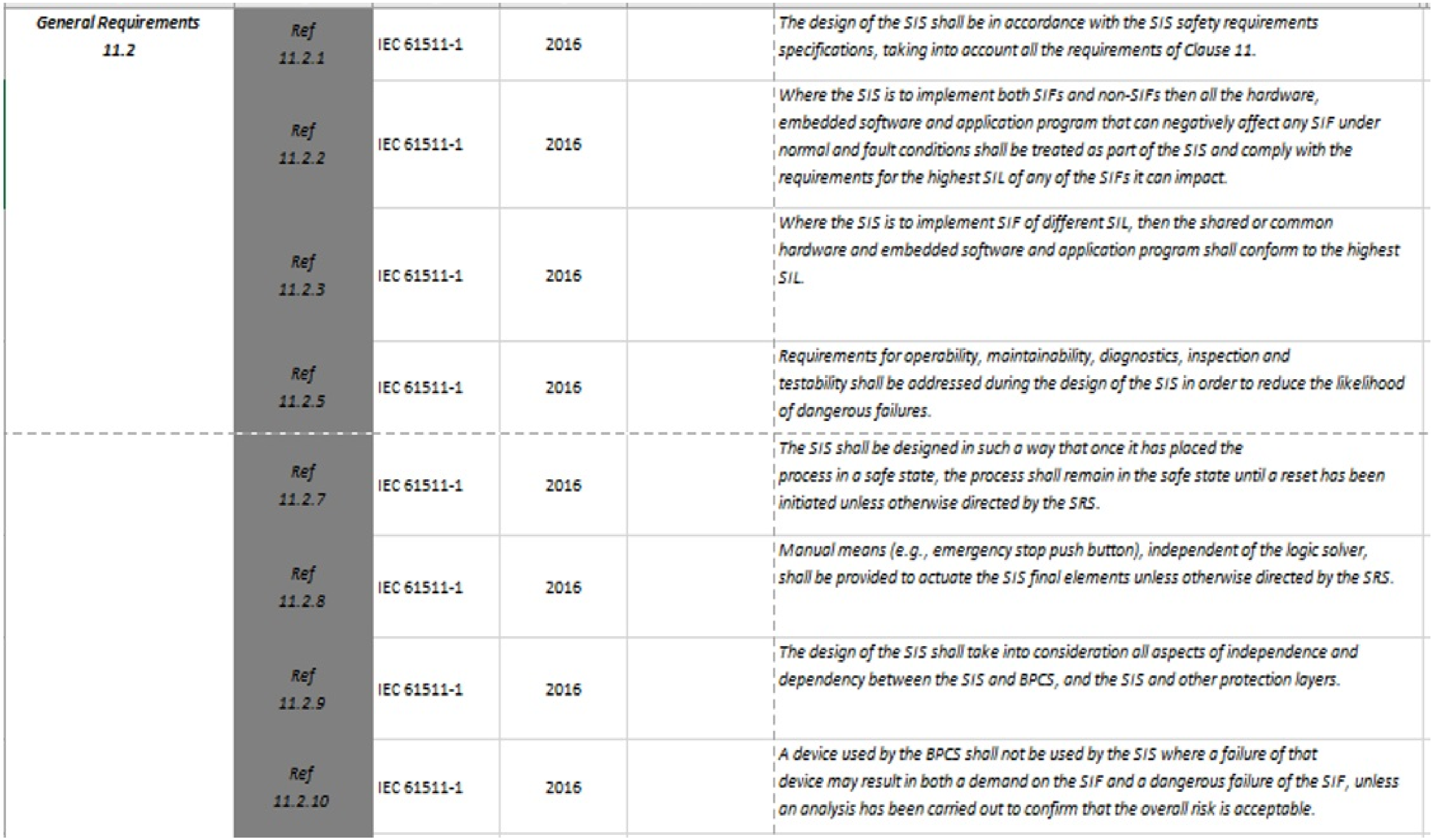
10.3	Ref 10.3.2	IEC 61511-1	2016		*These requirements shall be sufficient to design the SIS and shall include a description of the intent and approach applied during the development of the SIS safety requirements as applicable:* *• a description of all the SIF necessary to achieve the required functional safety (e.g., a cause and effect diagram, logic narrative);* *• a list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification (e.g., field tag list);* *• a definition of the safe state of the process for each identified SIF, such that a stable state has been achieved and the specified hazardous event has been avoided or sufficiently mitigated;* *• a definition of any individually safe process states which, when occurring concurrently, create a separate hazard (e.g., overload of emergency storage, multiple relief to flare system);* *• the assumed sources of demand and demand rate on each SIF;* *• requirements relating to proof test intervals;* *• requirements relating to proof test implementation;* ***• response time requirements for each SIF to bring the process to a safe state within the process safety time;*** ***• the required SIL and mode of operation (demand/continuous) for each SIF;*** *• a description of SIS process measurements, range, accuracy and their trip points;* ***• a description of SIF process output actions and the criteria for successful operation**, e.g., leakage rate for valves;* *• the functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissives for each SIF;* *• requirements for manual shutdown for each SIF;* *• requirements relating to energize or de-energize to trip for each SIF;* *• requirements for resetting each SIF after a shutdown (e.g., requirements for manual, semiautomatic, or automatic final element resets after trips);* *• maximum allowable spurious trip rate for each SIF;* *• failure modes for each SIF and desired response of the SIS (e.g., alarms, automatic shutdown);* *• any specific requirements related to the procedures for starting up and restarting the SIS;*



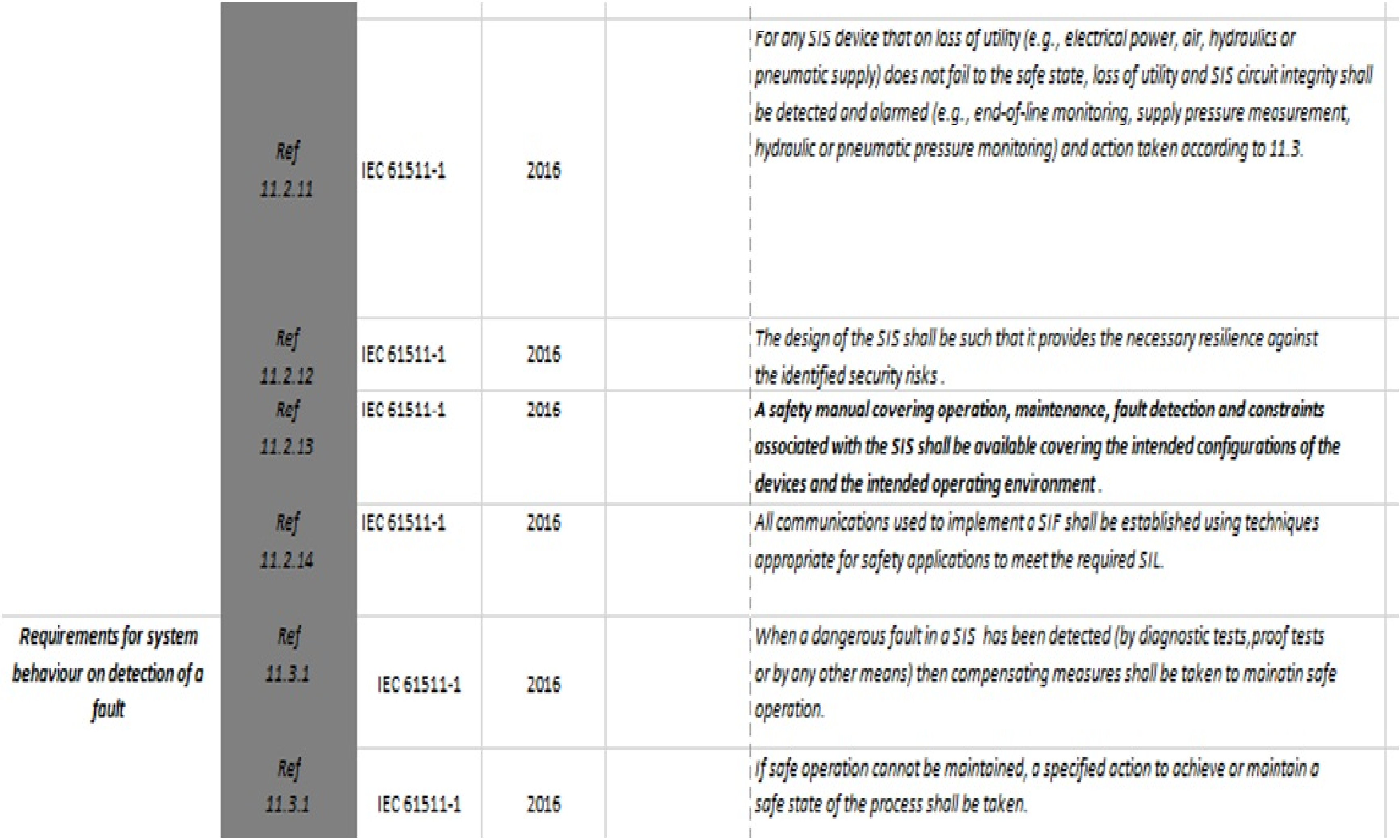
				• any specific requirements related to the procedures for starting up and restarting the SIS; • all interfaces between the SIS and any other system (including the BPCS and operators); • a description of the modes of operation of the plant and requirements relating to SIF operation within each mode; • the application program safety requirements as listed in 10.3.2; • requirements for bypasses including written procedures to be applied during the bypassed state which describe how the bypasses will be administratively controlled and then subsequently cleared; • the specification of any action necessary to achieve or maintain a safe state of theprocess in the event of fault(s) being detected in the SIS, taking into account of all relevant human factors; • the mean repair time which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints; • identification of the dangerous combinations of output states of the SIS that need to be avoided; • identification of normal and abnormal process operating modes for both the plant as a whole (e.g., plant start-up) and individual plant operating procedures (e.g., equipment maintenance, sensor calibration or repair). Additional SIFs may be required to support these process operating modes; • definition of the requirements for any SIF necessary to survive a major accident event,e.g., time required for a valve to remain operational in the event of a fire.
Ref *10.3.3*	IEC 61511-1	2016		The application program safety requirements shall be derived from the SRS and chosen architecture (arrangement and internal structure) of the SIS.



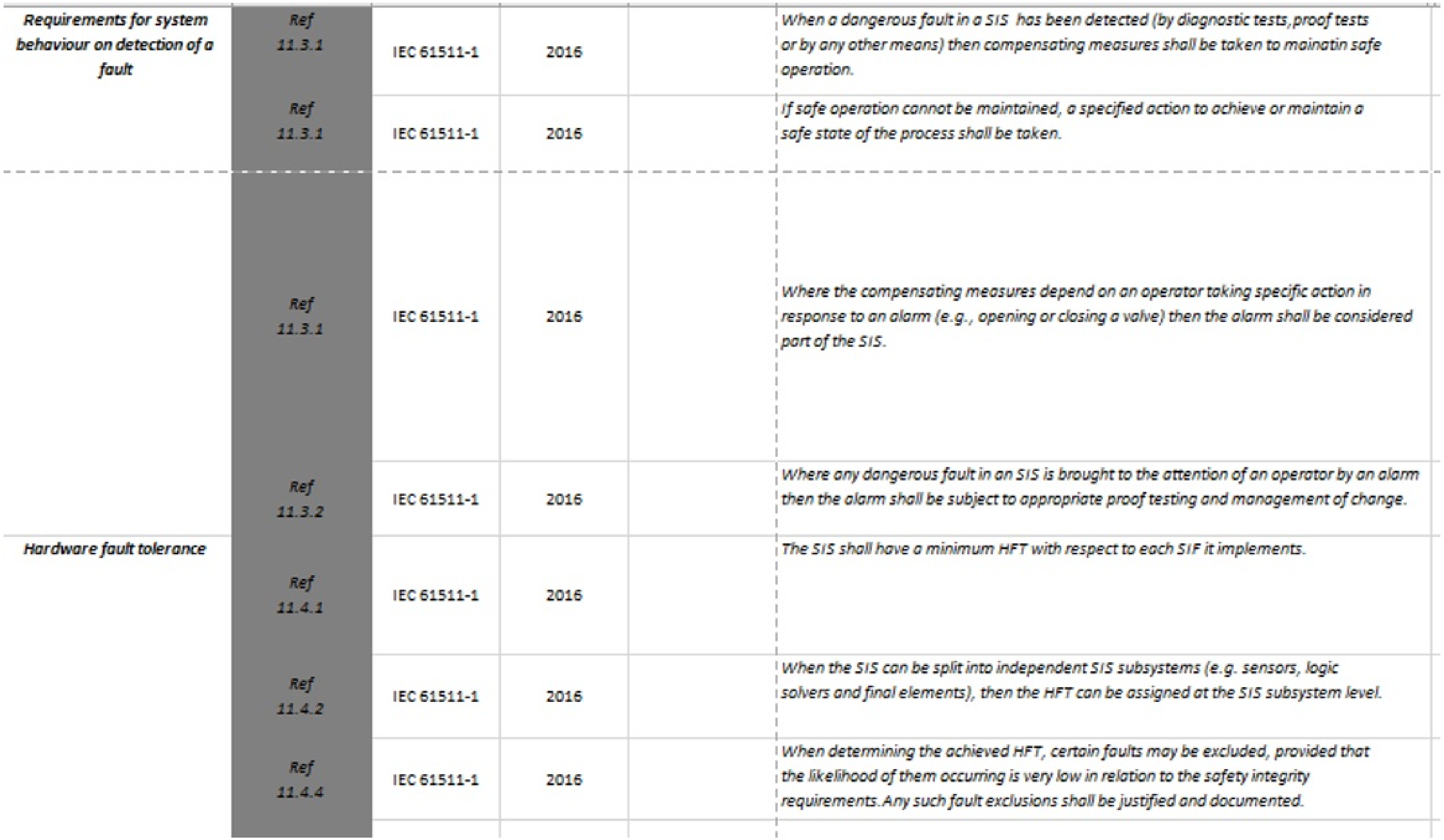
	Ref *10.3.3*	IEC 61511-1	2016		*The input to the application program safety requirements* *for each SIS subsystem shall include:* *a) the specified safety requirements of each SIF, including sensor voting, etc.;* *b) the requirements resulting from the SIS architecture and the safety manual such as limitations and constraints of the hardware and embedded software;* *c) any requirements of safety planning arising from 5.2.4.*
	Ref *10.3.4*	IEC 61511-1	2016		*The application program safety requirements shall be specified for each programmable SIS device necessary to implement the required SIF consistent with the architecture of the SIS.*
	Ref *10.3.5*	IEC 61511-1	2016		*The application program safety requirements specification shall be sufficiently detailed to allow the design and implementation to achieve the required functional safety and to allow a functional safety assessment to be carried out. The following shall be considered:* *• the SIFs supported by the application program and their SIL;* *• real time performance parameter such as, CPU capacity, network bandwidth, acceptable real time performance in the presence of faults, and all trip signals are received within a specified time period;* *• program sequencing and time delays if applicable;* *• equipment and operator interfaces and their operability;* *• all relevant modes of operation of the process as specified in the SRS;* *• action to be taken on bad process variable such as sensor value out of range, excessive range of change, frozen value, detected open circuit, detected short circuit;* *• functions enabling proof testing and automated diagnostics tests of external devices (e.g., sensors and final elements) performed in the application program;* *• application program self-monitoring (e.g., application driven watch-dogs and data range validation);* *• monitoring of other devices within the SIS (e.g., sensors and final elements);* *• any requirements related to periodic testing of SIF when the process is operational;* *• references to the input documents (e.g., specification of the SIF, configuration or architecture of the SIS, hardware safety integrity requirements of the SIS);* *• the requirements for communication interfaces, including measures to limit their use and the validity of data and commands both received and transmitted;*



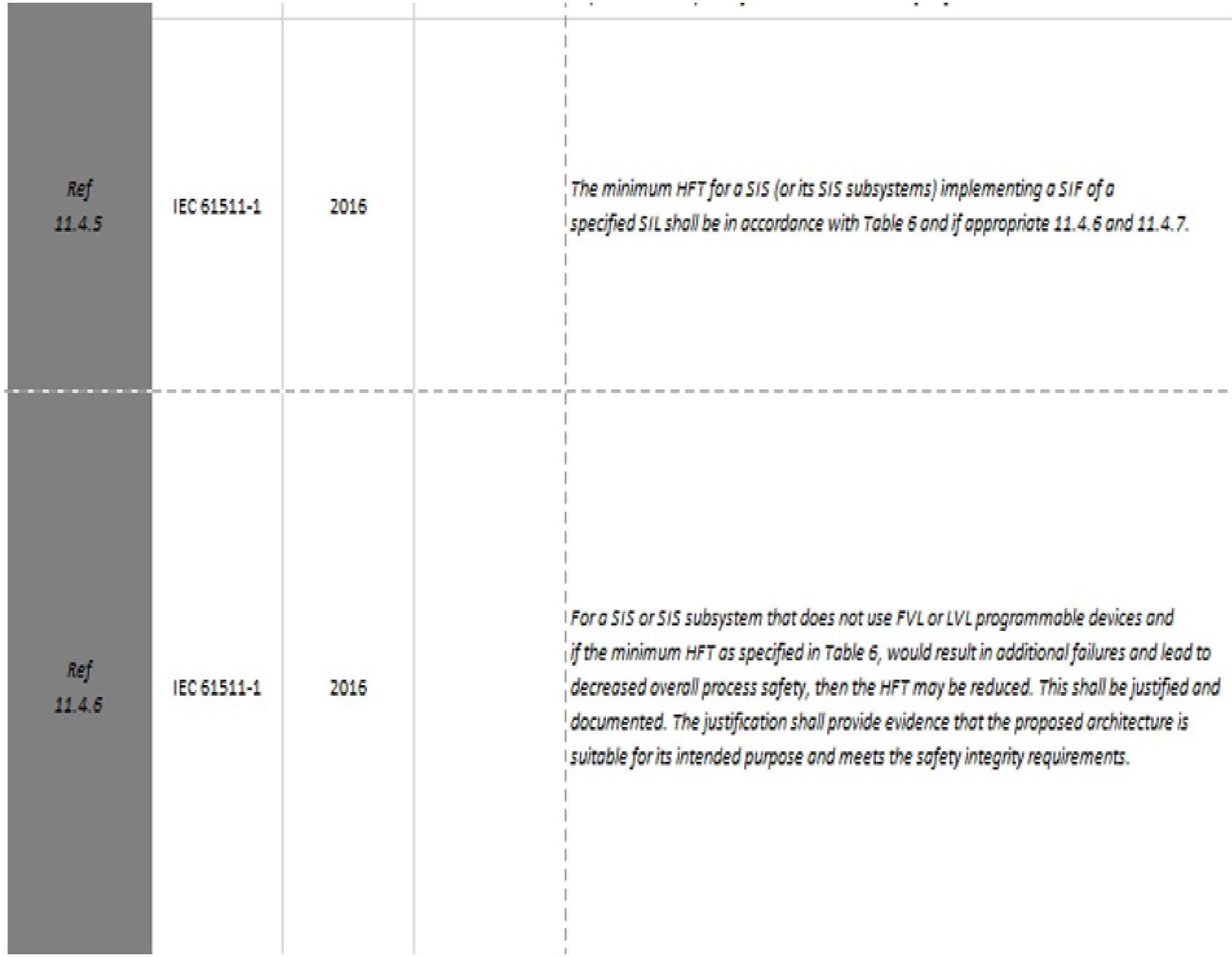
General Requirements ***11.2***	***Ref*** ***11.2.1***	IEC 61511-1	2016		*The design of the SIS shall be in accordance with the SIS safety requirements specifications, taking into account all the requirements of Clause 11.*
	Ref ***11.2.2***	IEC 61511-1	2016		*Where the SIS is to implement both SIFs and non-SIFs then all the hardware, embedded software and application program that can negatively affect any SIF under normal and fault conditions shall be treated as part of the SIS and comply with the requirements for the highest SIL of any of the SIFs it can impact.*
	Ref ***11.2.3***	IEC 61511-1	2016		*Where the SIS is to implement SIF of different SIL, then the shared or common hardware and embedded software and application program shall conform to the highest SIL.*
	Ref ***11.2.5***	IEC 61511-1	2016		*Requirements for operability, maintainability, diagnostics, inspection and testability shall be addressed during the design of the SIS in order to reduce the likelihood of dangerous failures.*
	Ref ***11.2.7***	IEC 61511-1	2016		*The SIS shall be designed in such a way that once it has placed the process in a safe state, the process shall remain in the safe state until a reset has been initiated unless otherwise directed by the SRS.*
	Ref ***11.2.8***	IEC 61511-1	2016		*Manual means (e.g., emergency stop push button), independent of the logic solver, shall be provided to actuate the SIS final elements unless otherwise directed by the SRS.*
	Ref ***11.2.9***	IEC 61511-1	2016		*The design of the SIS shall take into consideration all aspects of independence and dependency between the SIS and BPCS, and the SIS and other protection layers.*
	Ref ***11.2.10***	IEC 61511-1	2016		*A device used by the BPCS shall not be used by the SIS where a failure of that device may result in both a demand on the SIF and a dangerous failure of the SIF, unless an analysis has been carried out to confirm that the overall risk is acceptable.*



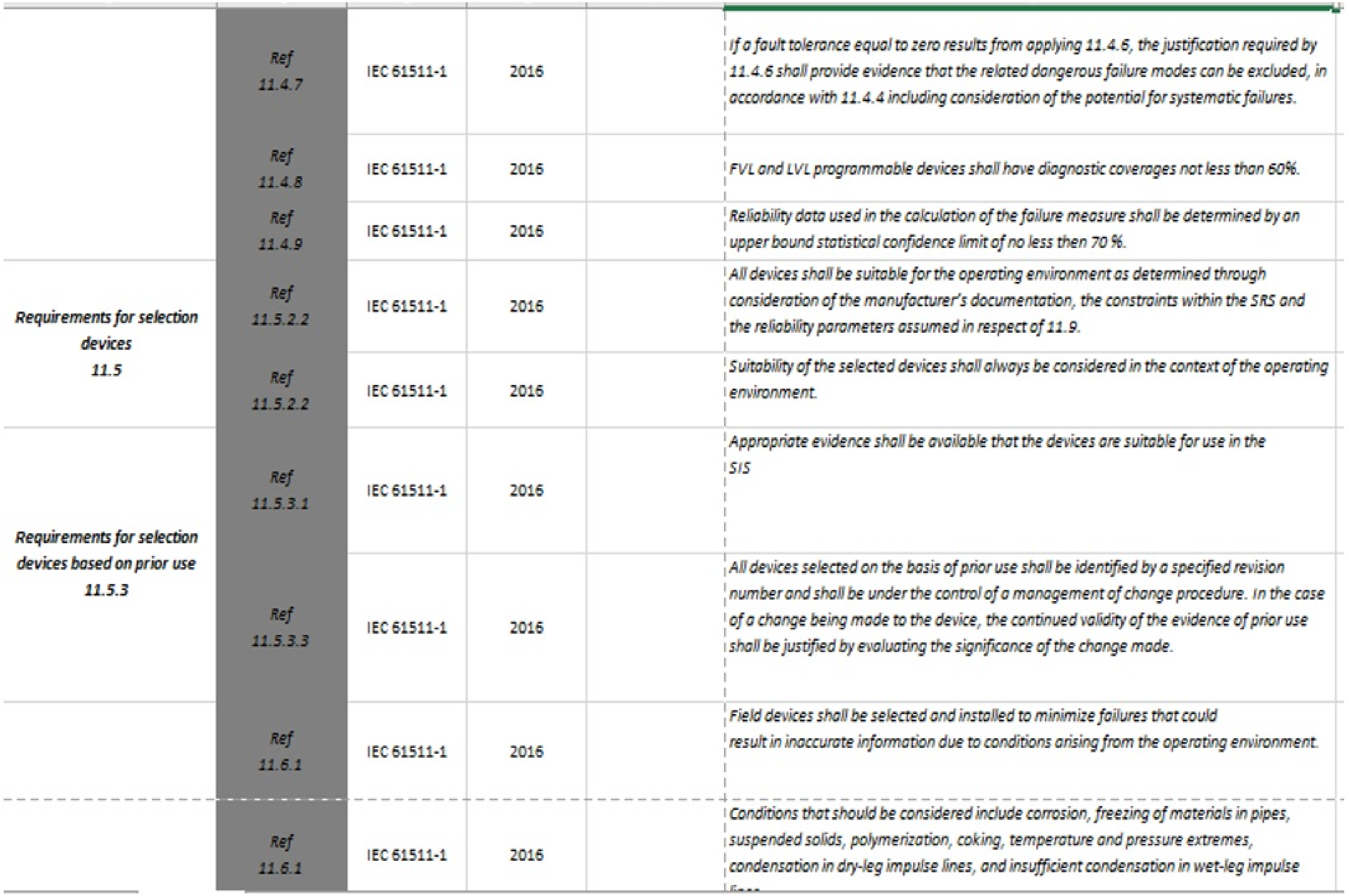
	Ref *11.2.11*	IEC 61511-1	2016		*For any SIS device that on loss of utility (e.g., electrical power, air, hydraulics or pneumatic supply) does not fail to the safe state, loss of utility and SIS circuit integrity shall be detected and alarmed (e.g., end-of-line monitoring, supply pressure measurement, hydraulic or pneumatic pressure monitoring) and action taken according to 11.3.*
	Ref *11.2.12*	IEC 61511-1	2016		*The design of the SIS shall be such that it provides the necessary resilience against the identified security risks .*
	Ref *11.2.13*	IEC 61511-1	2016		***A safety manual covering operation, maintenance, fault detection and constraints associated with the SIS shall be available covering the intended configurations of the devices and the intended operating environment .***
	Ref *11.2.14*	IEC 61511-1	2016		*All communications used to implement a SIF shall be established using techniques appropriate for safety applications to meet the required SIL.*
Requirements for system behaviour on detection of a fault	*Ref* *11.3.1*	IEC 61511-1	2016		*When a dangerous fault in a SIS has been detected (by diagnostic tests,proof tests or by any other means) then compensating measures shall be taken to mainatin safe operation.*
	Ref *11.3.1*	IEC 61511-1	2016		*If safe operation cannot be maintained, a specified action to achieve or maintain a safe state of the process shall be taken.*



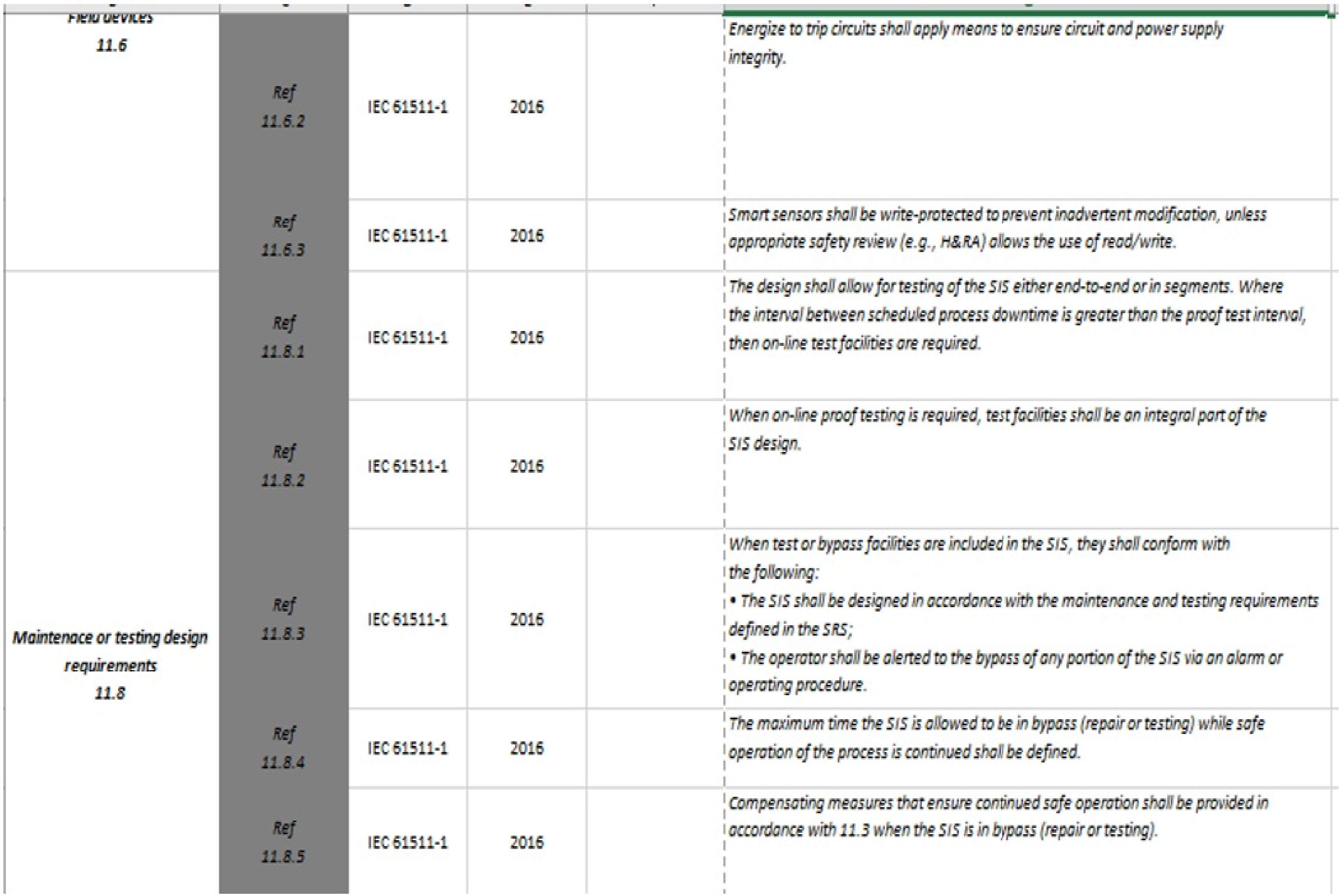
Requirements for system behaviour on detection of a fault	Ref 11.3.1	IEC 61511-1	2016		When a dangerous fault in a SIS has been detected (by diagnostic tests,proof tests or by any other means) then compensating measures shall be taken to mainatin safe operation.
	Ref 11.3.1	IEC 61511-1	2016		If safe operation cannot be maintained, a specified action to achieve or maintain a safe state of the process shall be taken.
	Ref 11.3.1	IEC 61511-1	2016		Where the compensating measures depend on an operator taking specific action in response to an alarm (e.g., opening or closing a valve) then the alarm shall be considered part of the SIS.
	Ref 11.3.2	IEC 61511-1	2016		Where any dangerous fault in an SIS is brought to the attention of an operator by an alarm then the alarm shall be subject to appropriate proof testing and management of change.
Hardware fault tolerance	Ref 11.4.1	IEC 61511-1	2016		The SIS shall have a minimum HFT with respect to each SIF it implements.
	Ref 11.4.2	IEC 61511-1	2016		When the SIS can be split into independent SIS subsystems (e.g. sensors, logic solvers and final elements), then the HFT can be assigned at the SIS subsystem level.
	Ref 11.4.4	IEC 61511-1	2016		When determining the achieved HFT, certain faults may be excluded, provided that the likelihood of them occuring is very low in relation to the safety integrity requirements.Any such fault exclusions shall be justified and documented.



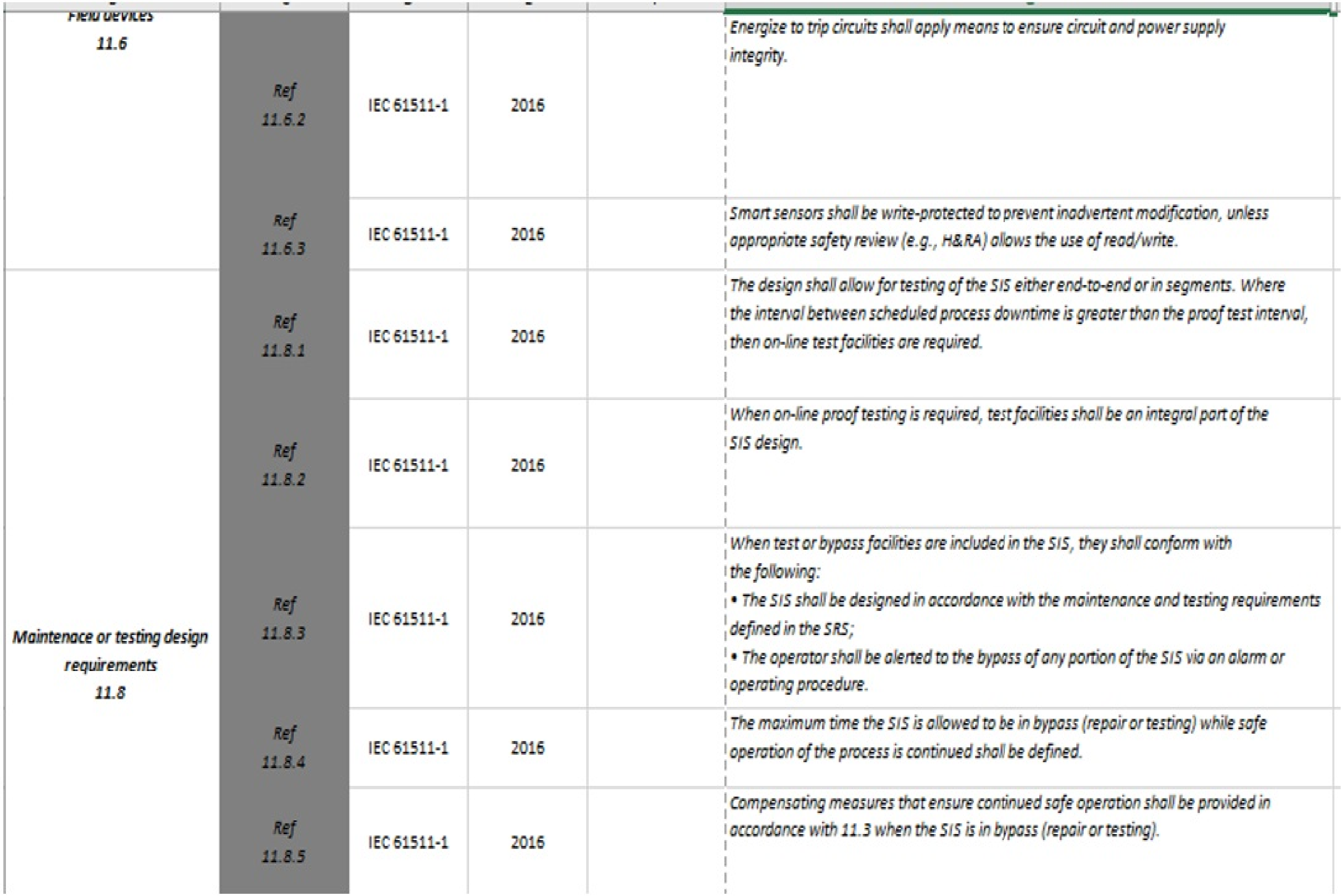
Ref *11.4.5*	IEC 61511-1	2016		*The minimum HFT for a SIS (or its SIS subsystems) implementing a SIF of a specified SIL shall be in accordance with Table 6 and if appropriate 11.4.6 and 11.4.7.*
Ref *11.4.6*	IEC 61511-1	2016		*For a SIS or SIS subsystem that does not use FVL or LVL programmable devices and if the minimum HFT as specified in Table 6, would result in additional failures and lead to decreased overall process safety, then the HFT may be reduced. This shall be justified and documented. The justification shall provide evidence that the proposed architecture is suitable for its intended purpose and meets the safety integrity requirements.*



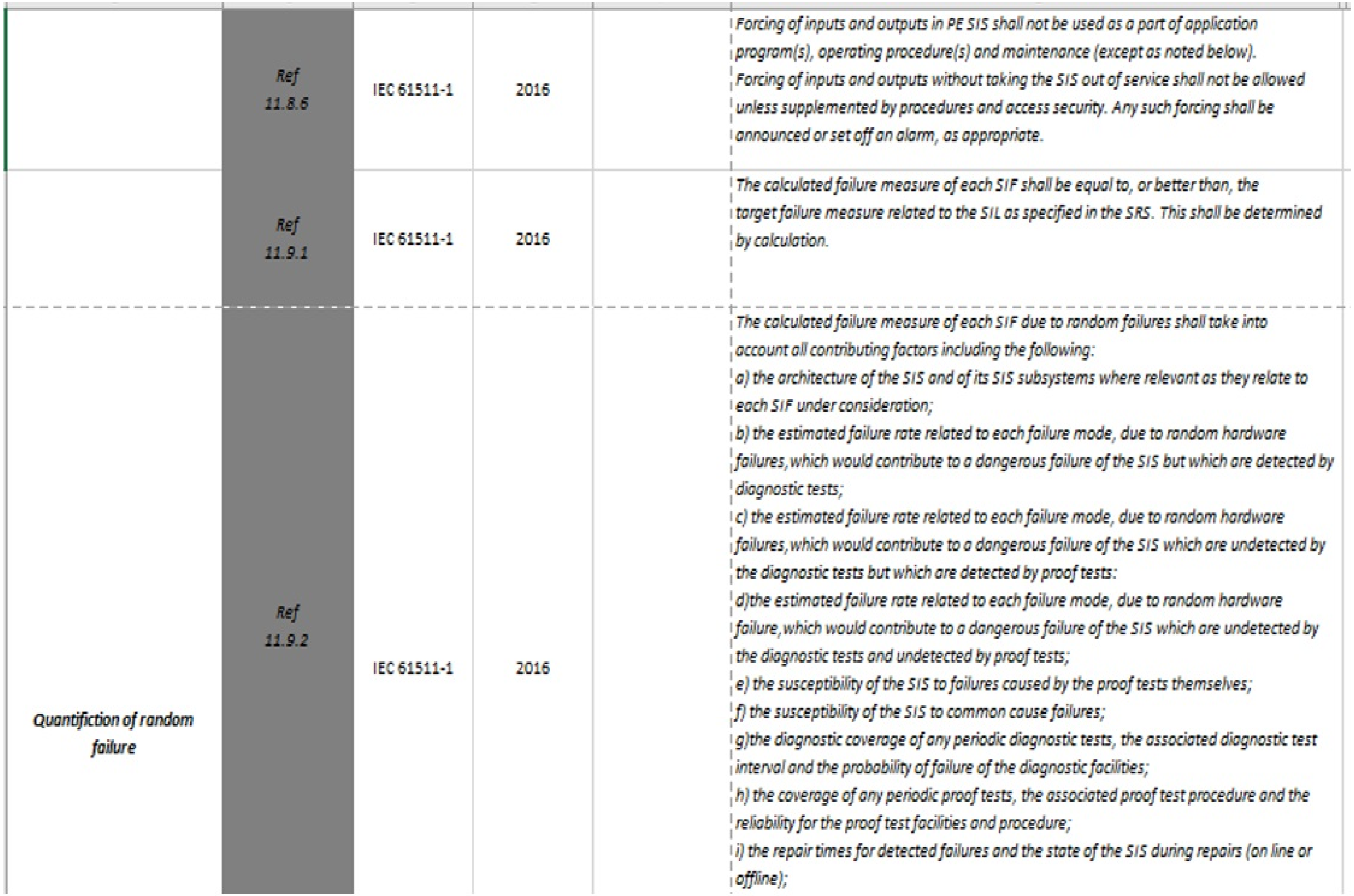
	Ref 11.4.7	IEC 61511-1	2016		If a fault tolerance equal to zero results from applying 11.4.6, the justification required by 11.4.6 shall provide evidence that the related dangerous failure modes can be excluded, in accordance with 11.4.4 including consideration of the potential for systematic failures.
	Ref 11.4.8	IEC 61511-1	2016		FVL and LVL programmable devices shall have diagnostic coverages not less than 60%.
	Ref 11.4.9	IEC 61511-1	2016		Reliability data used in the calculation of the failure measure shall be determined by an upper bound statistical confidence limit of no less then 70 %.
Requirements for selection devices 11.5	Ref 11.5.2.2	IEC 61511-1	2016		All devices shall be suitable for the operating environment as determined through consideration of the manufacturer's documentation, the constraints within the SRS and the reliability parameters assumed in respect of 11.9.
	Ref 11.5.2.2	IEC 61511-1	2016		Suitability of the selected devices shall always be considered in the context of the operating environment.
Requirements for selection devices based on prior use 11.5.3	Ref 11.5.3.1	IEC 61511-1	2016		Appropriate evidence shall be available that the devices are suitable for use in the SIS
	Ref 11.5.3.3	IEC 61511-1	2016		All devices selected on the basis of prior use shall be identified by a specified revision number and shall be under the control of a management of change procedure. In the case of a change being made to the device, the continued validity of the evidence of prior use shall be justified by evaluating the significance of the change made.
	Ref 11.6.1	IEC 61511-1	2016		Field devices shall be selected and installed to minimize failures that could result in inaccurate information due to conditions arising from the operating environment.
	Ref 11.6.1	IEC 61511-1	2016		Conditions that should be considered include corrosion, freezing of materials in pipes, suspended solids, polymerization, coking, temperature and pressure extremes, condensation in dry-leg impulse lines, and insufficient condensation in wet-leg impulse



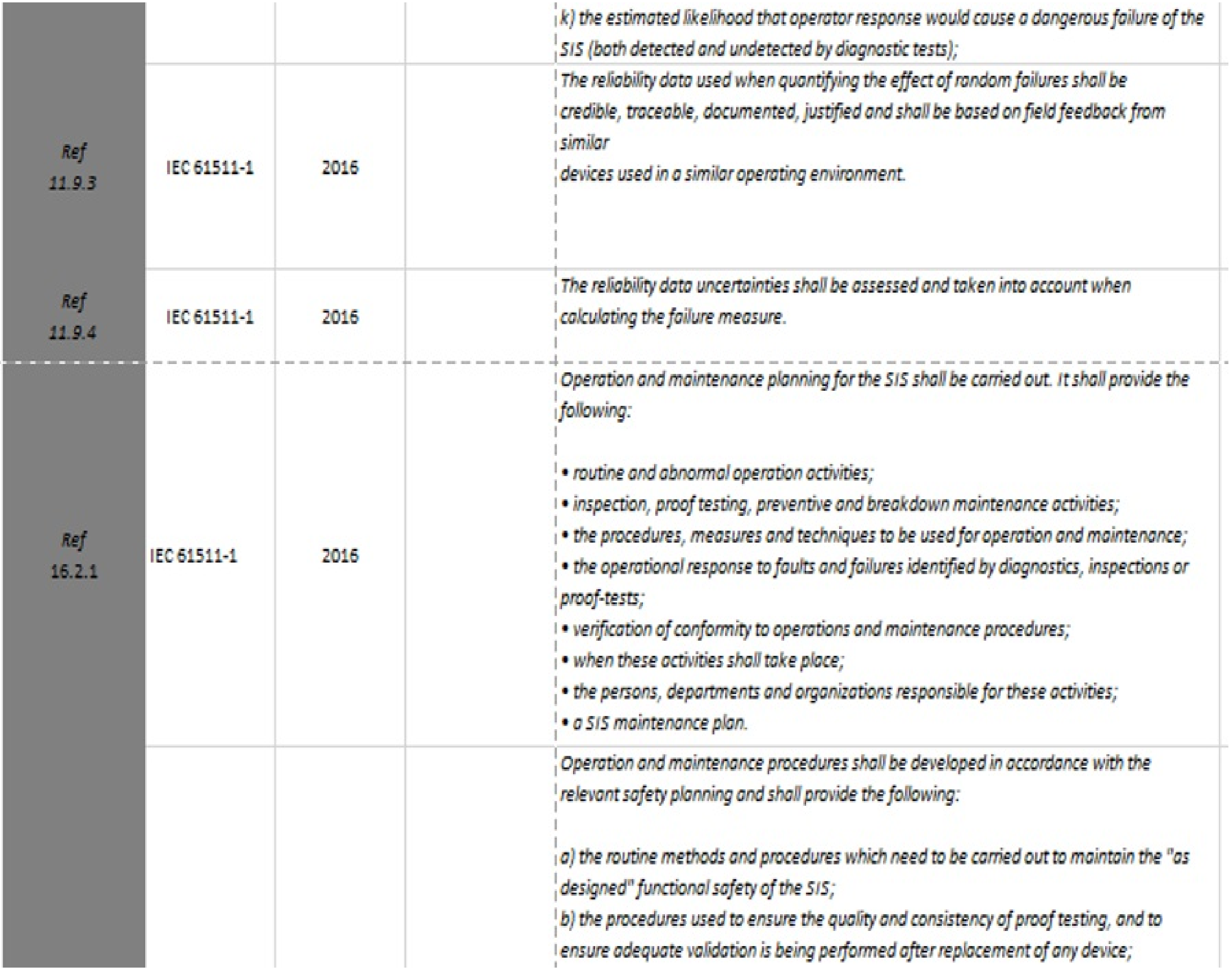
Field devices 11.6	Ref 11.6.2	IEC 61511-1	2016		Energize to trip circuits shall apply means to ensure circuit and power supply integrity.
	Ref 11.6.3	IEC 61511-1	2016		Smart sensors shall be write-protected to prevent inadvertent modification, unless appropriate safety review (e.g., H&RA) allows the use of read/write.
Maintenace or testing design requirements 11.8	Ref 11.8.1	IEC 61511-1	2016		The design shall allow for testing of the SIS either end-to-end or in segments. Where the interval between scheduled process downtime is greater than the proof test interval, then on-line test facilities are required.
	Ref 11.8.2	IEC 61511-1	2016		When on-line proof testing is required, test facilities shall be an integral part of the SIS design.
	Ref 11.8.3	IEC 61511-1	2016		When test or bypass facilities are included in the SIS, they shall conform with the following: • The SIS shall be designed in accordance with the maintenance and testing requirements defined in the SRS; • The operator shall be alerted to the bypass of any portion of the SIS via an alarm or operating procedure.
	Ref 11.8.4	IEC 61511-1	2016		The maximum time the SIS is allowed to be in bypass (repair or testing) while safe operation of the process is continued shall be defined.
	Ref 11.8.5	IEC 61511-1	2016		Compensating measures that ensure continued safe operation shall be provided in accordance with 11.3 when the SIS is in bypass (repair or testing).



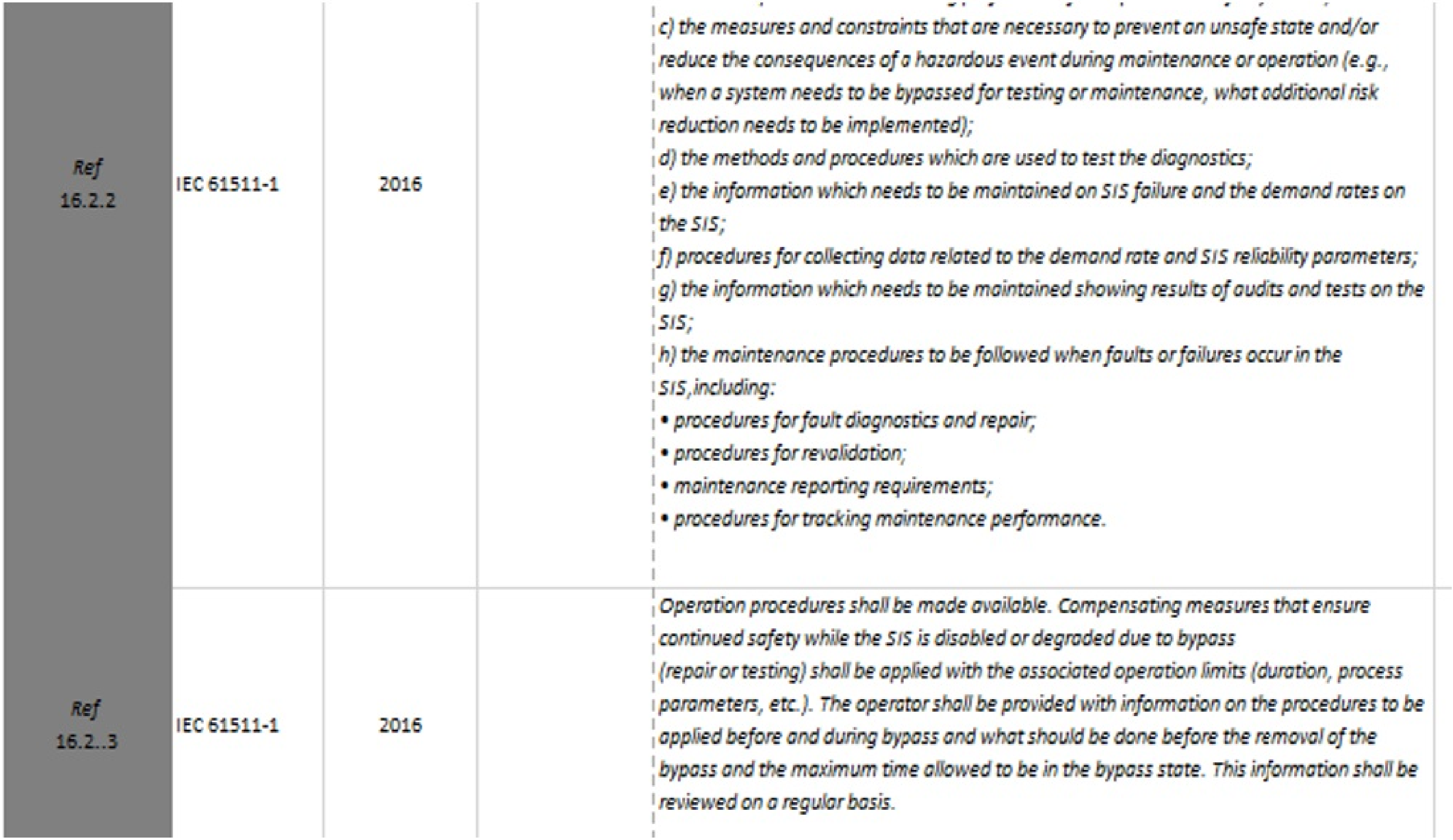
Field devices 11.6	Ref 11.6.2	IEC 61511-1	2016		Energize to trip circuits shall apply means to ensure circuit and power supply integrity.
	Ref 11.6.3	IEC 61511-1	2016		Smart sensors shall be write-protected to prevent inadvertent modification, unless appropriate safety review (e.g., H&RA) allows the use of read/write.
Maintenace or testing design requirements 11.8	Ref 11.8.1	IEC 61511-1	2016		The design shall allow for testing of the SIS either end-to-end or in segments. Where the interval between scheduled process downtime is greater than the proof test interval, then on-line test facilities are required.
	Ref 11.8.2	IEC 61511-1	2016		When on-line proof testing is required, test facilities shall be an integral part of the SIS design.
	Ref 11.8.3	IEC 61511-1	2016		When test or bypass facilities are included in the SIS, they shall conform with the following: • The SIS shall be designed in accordance with the maintenance and testing requirements defined in the SRS; • The operator shall be alerted to the bypass of any portion of the SIS via an alarm or operating procedure.
	Ref 11.8.4	IEC 61511-1	2016		The maximum time the SIS is allowed to be in bypass (repair or testing) while safe operation of the process is continued shall be defined.
	Ref 11.8.5	IEC 61511-1	2016		Compensating measures that ensure continued safe operation shall be provided in accordance with 11.3 when the SIS is in bypass (repair or testing).



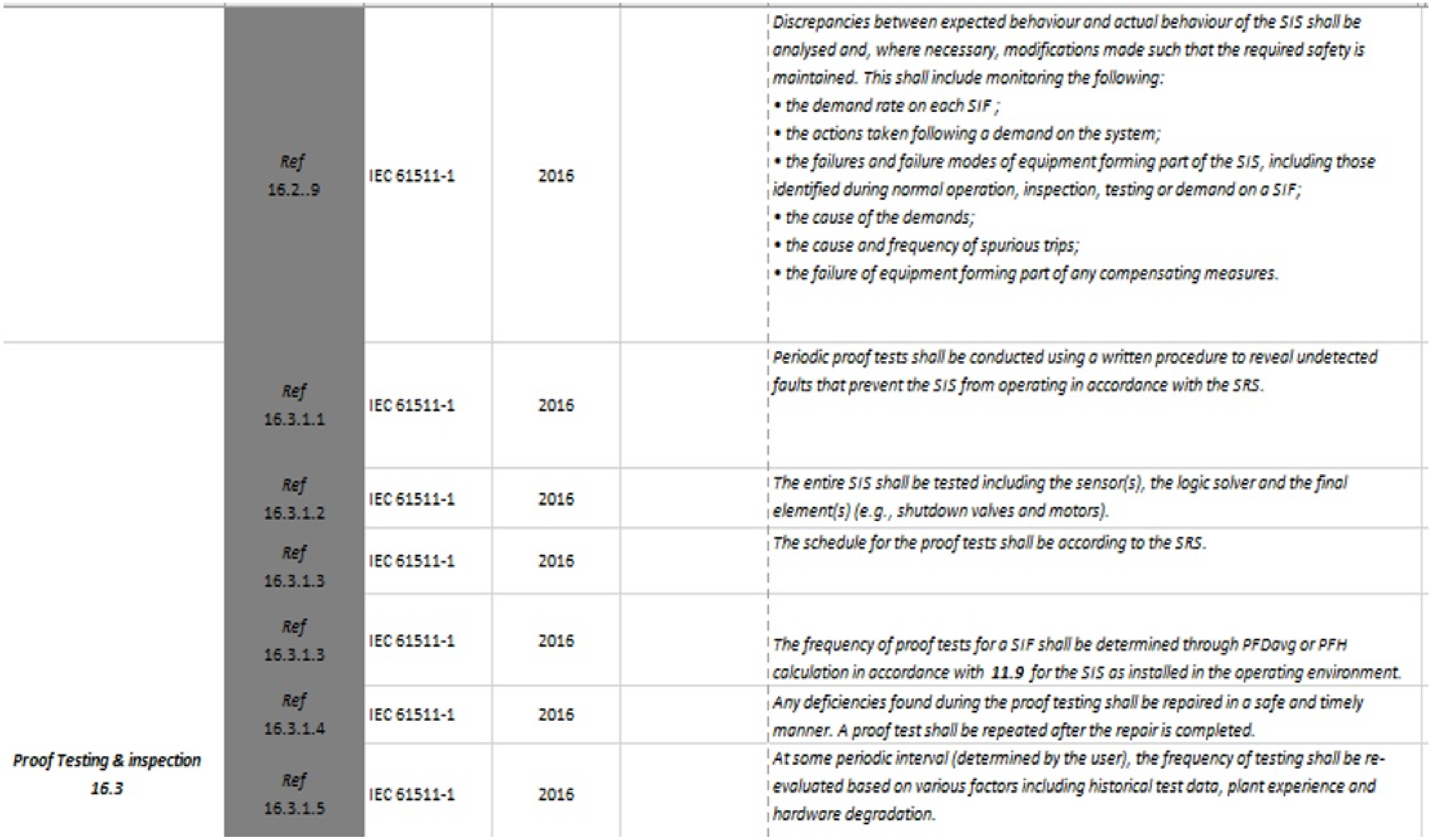
	Ref *11.8.6*	IEC 61511-1	2016		*Forcing of inputs and outputs in PE SIS shall not be used as a part of application program(s), operating procedure(s) and maintenance (except as noted below).* *Forcing of inputs and outputs without taking the SIS out of service shall not be allowed unless supplemented by procedures and access security. Any such forcing shall be announced or set off an alarm, as appropriate.*
	Ref *11.9.1*	IEC 61511-1	2016		*The calculated failure measure of each SIF shall be equal to, or better than, the target failure measure related to the SIL as specified in the SRS. This shall be determined by calculation.*
Quantifiction of random failure	*Ref* *11.9.2*	IEC 61511-1	2016		*The calculated failure measure of each SIF due to random failures shall take into account all contributing factors including the following:* *a) the architecture of the SIS and of its SIS subsystems where relevant as they relate to each SIF under consideration;* *b) the estimated failure rate related to each failure mode, due to random hardware failures,which would contribute to a dangerous failure of the SIS but which are detected by diagnostic tests;* *c) the estimated failure rate related to each failure mode, due to random hardware failures,which would contribute to a dangerous failure of the SIS which are undetected by the diagnostic tests but which are detected by proof tests:* *d)the estimated failure rate related to each failure mode, due to random hardware failure,which would contribute to a dangerous failure of the SIS which are undetected by the diagnostic tests and undetected by proof tests;* *e) the susceptibility of the SIS to failures caused by the proof tests themselves;* *f) the susceptibility of the SIS to common cause failures;* *g)the diagnostic coverage of any periodic diagnostic tests, the associated diagnostic test interval and the probability of failure of the diagnostic facilities;* *h) the coverage of any periodic proof tests, the associated proof test procedure and the reliability for the proof test facilities and procedure;* *i) the repair times for detected failures and the state of the SIS during repairs (on line or offline);*



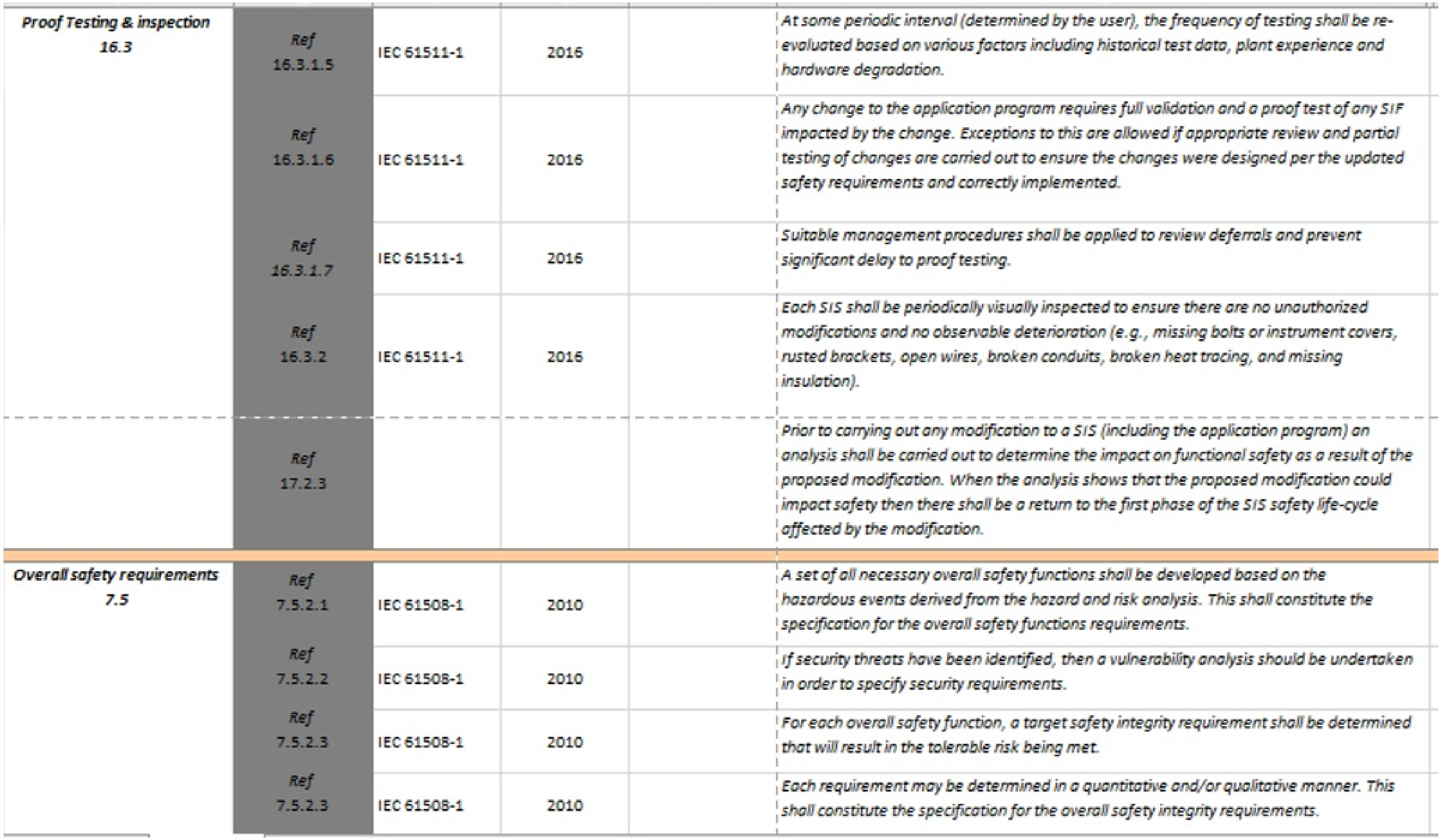
				k) the estimated likelihood that operator response would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);
Ref 11.9.3	IEC 61511-1	2016		The reliability data used when quantifying the effect of random failures shall be credible, traceable, documented, justified and shall be based on field feedback from similar devices used in a similar operating environment.
Ref 11.9.4	IEC 61511-1	2016		The reliability data uncertainties shall be assessed and taken into account when calculating the failure measure.
Ref 16.2.1	IEC 61511-1	2016		Operation and maintenance planning for the SIS shall be carried out. It shall provide the following: • routine and abnormal operation activities; • inspection, proof testing, preventive and breakdown maintenance activities; • the procedures, measures and techniques to be used for operation and maintenance; • the operational response to faults and failures identified by diagnostics, inspections or proof-tests; • verification of conformity to operations and maintenance procedures; • when these activities shall take place; • the persons, departments and organizations responsible for these activities; • a SIS maintenance plan.
				Operation and maintenance procedures shall be developed in accordance with the relevant safety planning and shall provide the following: a) the routine methods and procedures which need to be carried out to maintain the "as designed" functional safety of the SIS; b) the procedures used to ensure the quality and consistency of proof testing, and to ensure adequate validation is being performed after replacement of any device;



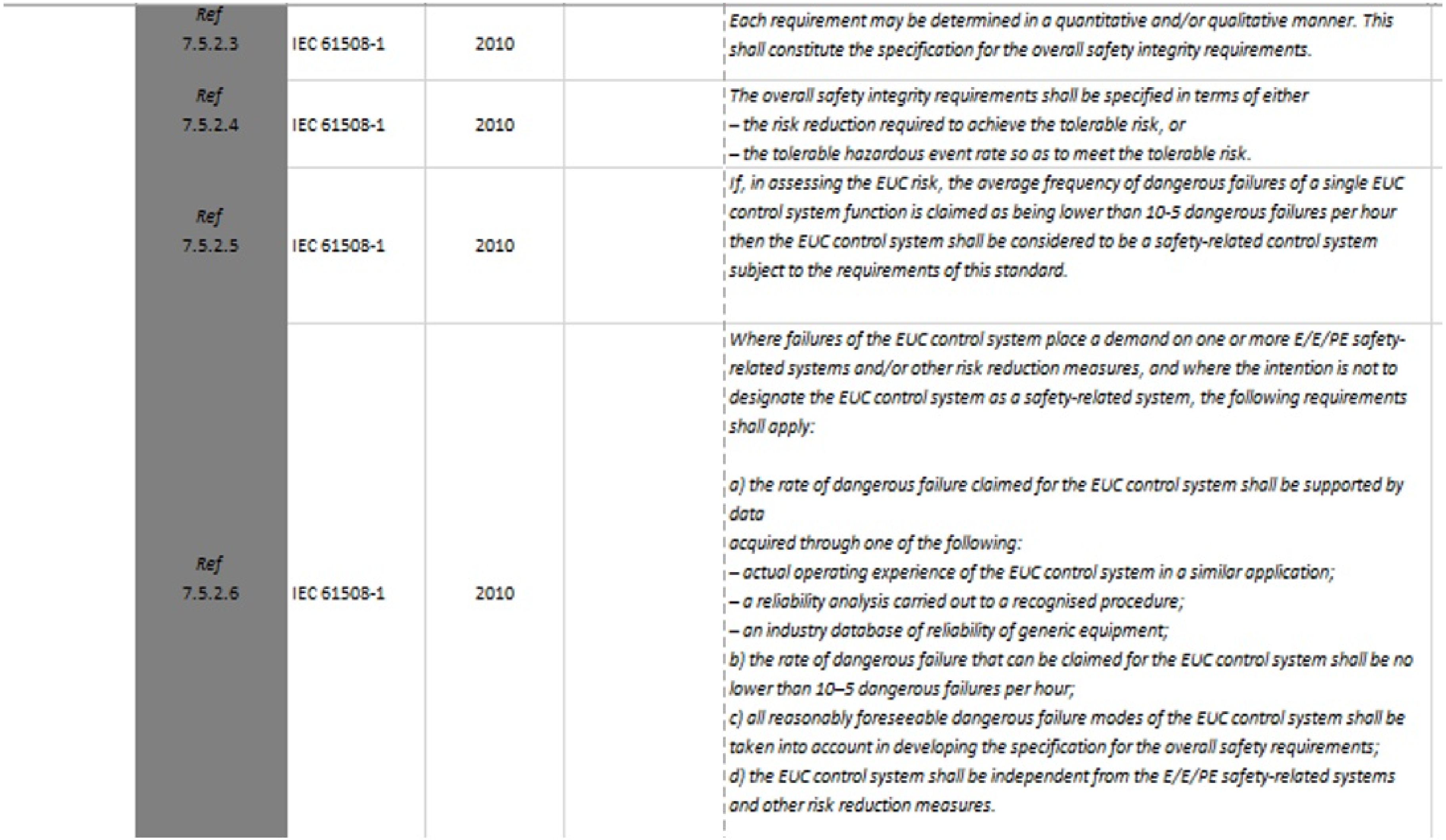
Ref 16.2.2	IEC 61511-1	2016		*c) the measures and constraints that are necessary to prevent an unsafe state and/or reduce the consequences of a hazardous event during maintenance or operation (e.g., when a system needs to be bypassed for testing or maintenance, what additional risk reduction needs to be implemented);* *d) the methods and procedures which are used to test the diagnostics;* *e) the information which needs to be maintained on SIS failure and the demand rates on the SIS;* *f) procedures for collecting data related to the demand rate and SIS reliability parameters;* *g) the information which needs to be maintained showing results of audits and tests on the SIS;* *h) the maintenance procedures to be followed when faults or failures occur in the SIS,including:* *• procedures for fault diagnostics and repair;* *• procedures for revalidation;* *• maintenance reporting requirements;* *• procedures for tracking maintenance performance.*
Ref 16.2..3	IEC 61511-1	2016		*Operation procedures shall be made available. Compensating measures that ensure continued safety while the SIS is disabled or degraded due to bypass (repair or testing) shall be applied with the associated operation limits (duration, process parameters, etc.). The operator shall be provided with information on the procedures to be applied before and during bypass and what should be done before the removal of the bypass and the maximum time allowed to be in the bypass state. This information shall be reviewed on a regular basis.*



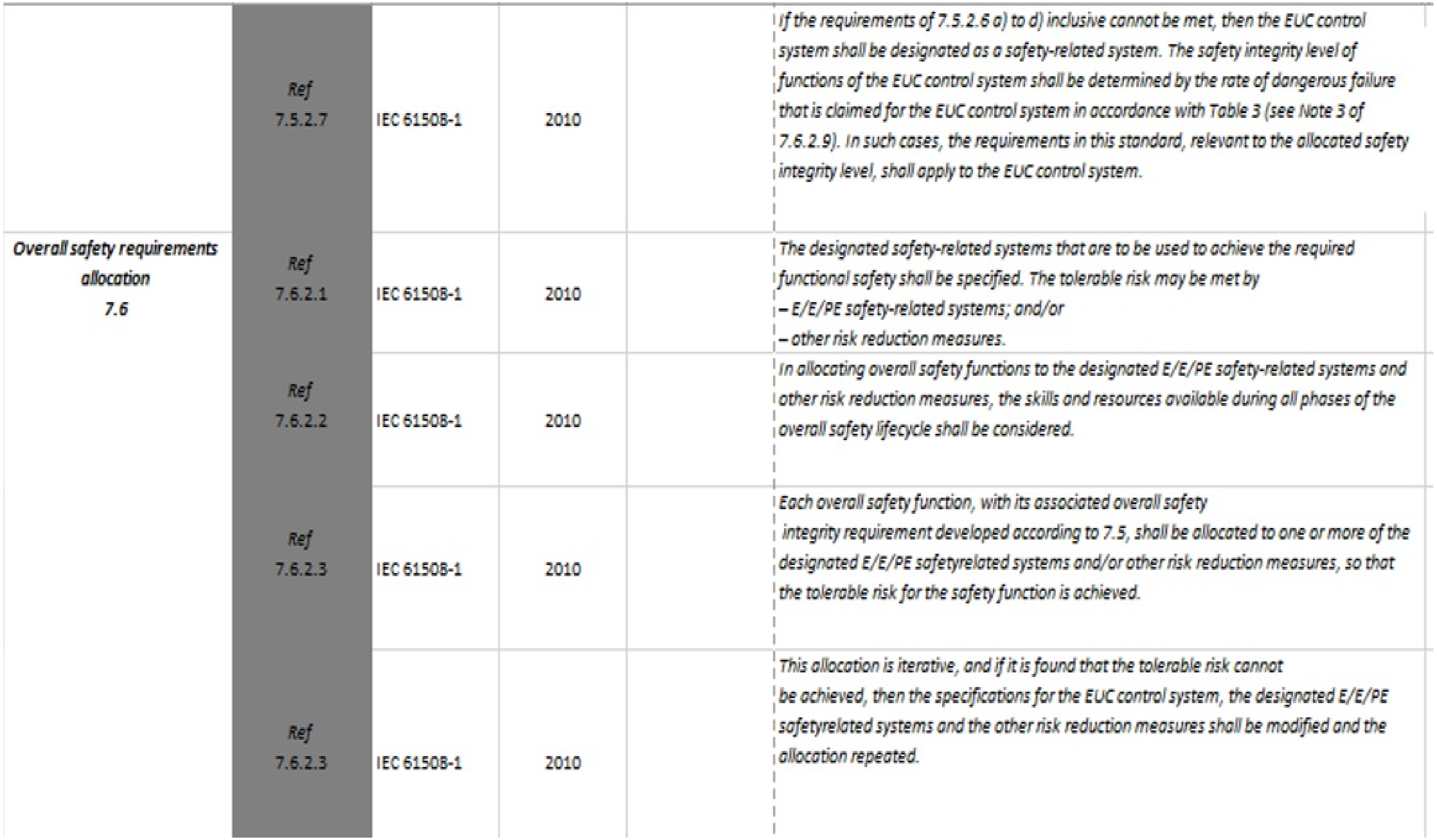
	Ref 16.2..9	IEC 61511-1	2016		*Discrepancies between expected behaviour and actual behaviour of the SIS shall be analysed and, where necessary, modifications made such that the required safety is maintained. This shall include monitoring the following:* *• the demand rate on each SIF ;* *• the actions taken following a demand on the system;* *• the failures and failure modes of equipment forming part of the SIS, including those identified during normal operation, inspection, testing or demand on a SIF;* *• the cause of the demands;* *• the cause and frequency of spurious trips;* *• the failure of equipment forming part of any compensating measures.*
Proof Testing & inspection* *16.3	*Ref* 16.3.1.1	IEC 61511-1	2016		*Periodic proof tests shall be conducted using a written procedure to reveal undetected faults that prevent the SIS from operating in accordance with the SRS.*
	Ref 16.3.1.2	IEC 61511-1	2016		*The entire SIS shall be tested including the sensor(s), the logic solver and the final element(s) (e.g., shutdown valves and motors).*
	Ref 16.3.1.3	IEC 61511-1	2016		*The schedule for the proof tests shall be according to the SRS.*
	Ref 16.3.1.3	IEC 61511-1	2016		*The frequency of proof tests for a SIF shall be determined through PFDavg or PFH calculation in accordance with* ***11.9*** *for the SIS as installed in the operating environment.*
	Ref 16.3.1.4	IEC 61511-1	2016		*Any deficiencies found during the proof testing shall be repaired in a safe and timely manner. A proof test shall be repeated after the repair is completed.*
	Ref 16.3.1.5	IEC 61511-1	2016		*At some periodic interval (determined by the user), the frequency of testing shall be re-evaluated based on various factors including historical test data, plant experience and hardware degradation.*



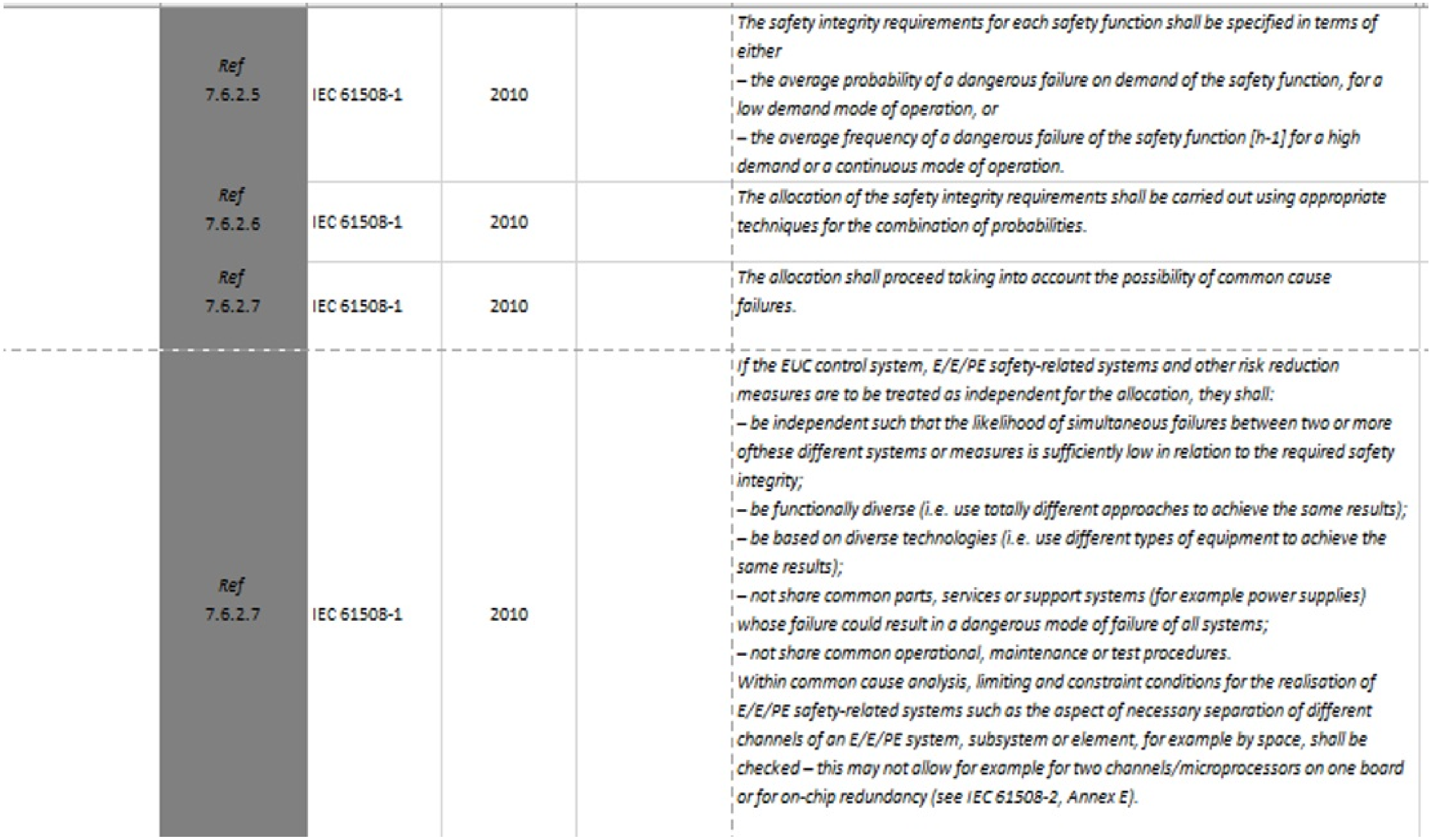
Proof Testing & inspection 16.3	*Ref* 16.3.1.5	IEC 61511-1	2016		*At some periodic interval (determined by the user), the frequency of testing shall be re-evaluated based on various factors including historical test data, plant experience and hardware degradation.*
	Ref 16.3.1.6	IEC 61511-1	2016		*Any change to the application program requires full validation and a proof test of any SIF impacted by the change. Exceptions to this are allowed if appropriate review and partial testing of changes are carried out to ensure the changes were designed per the updated safety requirements and correctly implemented.*
	Ref 16.3.1.7	IEC 61511-1	2016		*Suitable management procedures shall be applied to review deferrals and prevent significant delay to proof testing.*
	Ref 16.3.2	IEC 61511-1	2016		*Each SIS shall be periodically visually inspected to ensure there are no unauthorized modifications and no observable deterioration (e.g., missing bolts or instrument covers, rusted brackets, open wires, broken conduits, broken heat tracing, and missing insulation).*
	Ref 17.2.3				*Prior to carrying out any modification to a SIS (including the application program) an analysis shall be carried out to determine the impact on functional safety as a result of the proposed modification. When the analysis shows that the proposed modification could impact safety then there shall be a return to the first phase of the SIS safety life-cycle affected by the modification.*
Overall safety requirements 7.5	*Ref* 7.5.2.1	IEC 61508-1	2010		*A set of all necessary overall safety functions shall be developed based on the hazardous events derived from the hazard and risk analysis. This shall constitute the specification for the overall safety functions requirements.*
	Ref 7.5.2.2	IEC 61508-1	2010		*If security threats have been identified, then a vulnerability analysis should be undertaken in order to specify security requirements.*
	Ref 7.5.2.3	IEC 61508-1	2010		*For each overall safety function, a target safety integrity requirement shall be determined that will result in the tolerable risk being met.*
	Ref 7.5.2.3	IEC 61508-1	2010		*Each requirement may be determined in a quantitative and/or qualitative manner. This shall constitute the specification for the overall safety integrity requirements.*



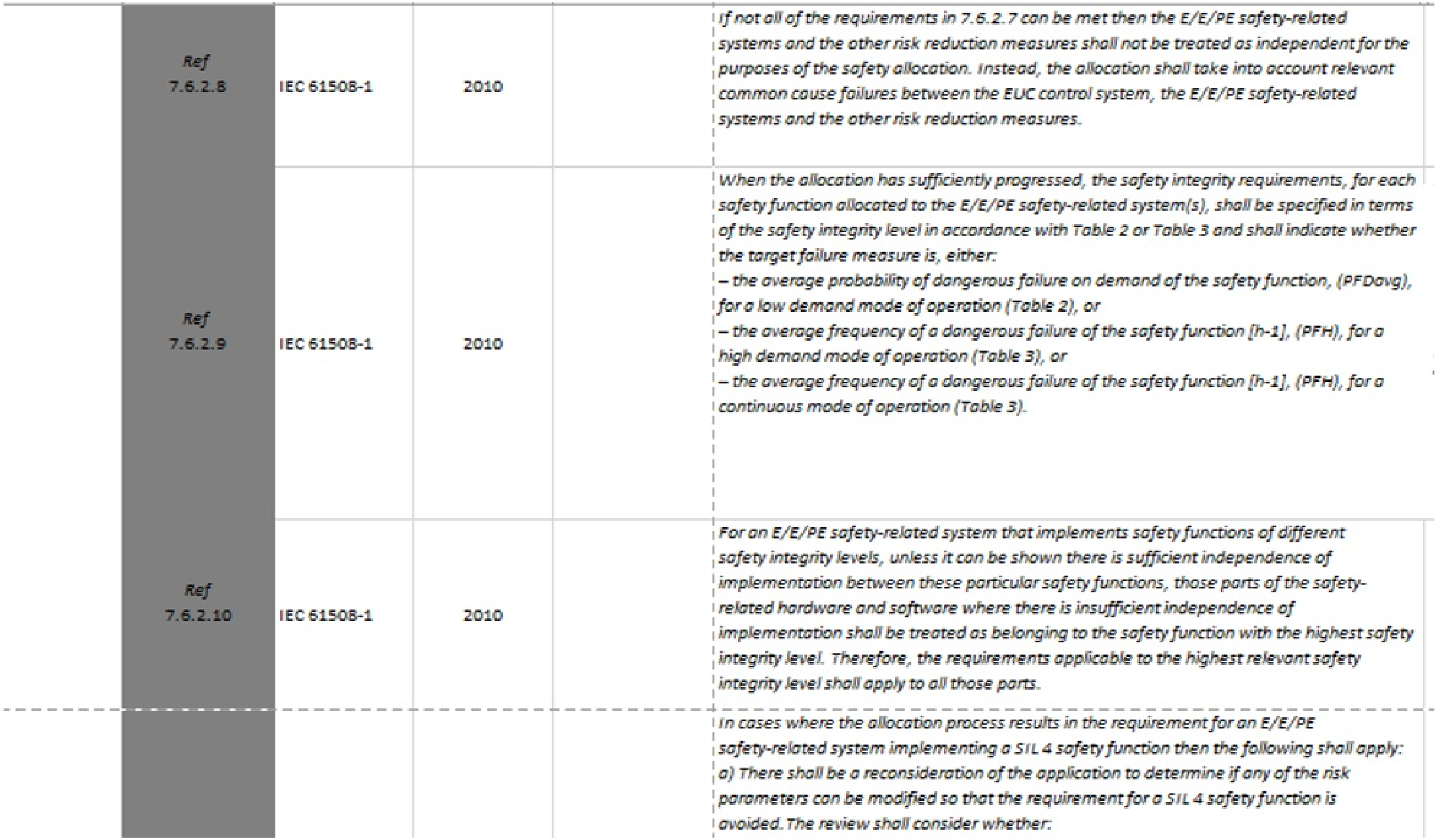
	Ref 7.5.2.3	IEC 61508-1	2010		*Each requirement may be determined in a quantitative and/or qualitative manner. This shall constitute the specification for the overall safety integrity requirements.*
	Ref 7.5.2.4	IEC 61508-1	2010		*The overall safety integrity requirements shall be specified in terms of either* *– the risk reduction required to achieve the tolerable risk, or* *– the tolerable hazardous event rate so as to meet the tolerable risk.*
	Ref 7.5.2.5	IEC 61508-1	2010		*If, in assessing the EUC risk, the average frequency of dangerous failures of a single EUC control system function is claimed as being lower than 10-5 dangerous failures per hour then the EUC control system shall be considered to be a safety-related control system subject to the requirements of this standard.*
	Ref 7.5.2.6	IEC 61508-1	2010		*Where failures of the EUC control system place a demand on one or more E/E/PE safety-related systems and/or other risk reduction measures, and where the intention is not to designate the EUC control system as a safety-related system, the following requirements shall apply:* *a) the rate of dangerous failure claimed for the EUC control system shall be supported by data* *acquired through one of the following:* *– actual operating experience of the EUC control system in a similar application;* *– a reliability analysis carried out to a recognised procedure;* *– an industry database of reliability of generic equipment;* *b) the rate of dangerous failure that can be claimed for the EUC control system shall be no lower than 10–5 dangerous failures per hour;* *c) all reasonably foreseeable dangerous failure modes of the EUC control system shall be taken into account in developing the specification for the overall safety requirements;* *d) the EUC control system shall be independent from the E/E/PE safety-related systems and other risk reduction measures.*



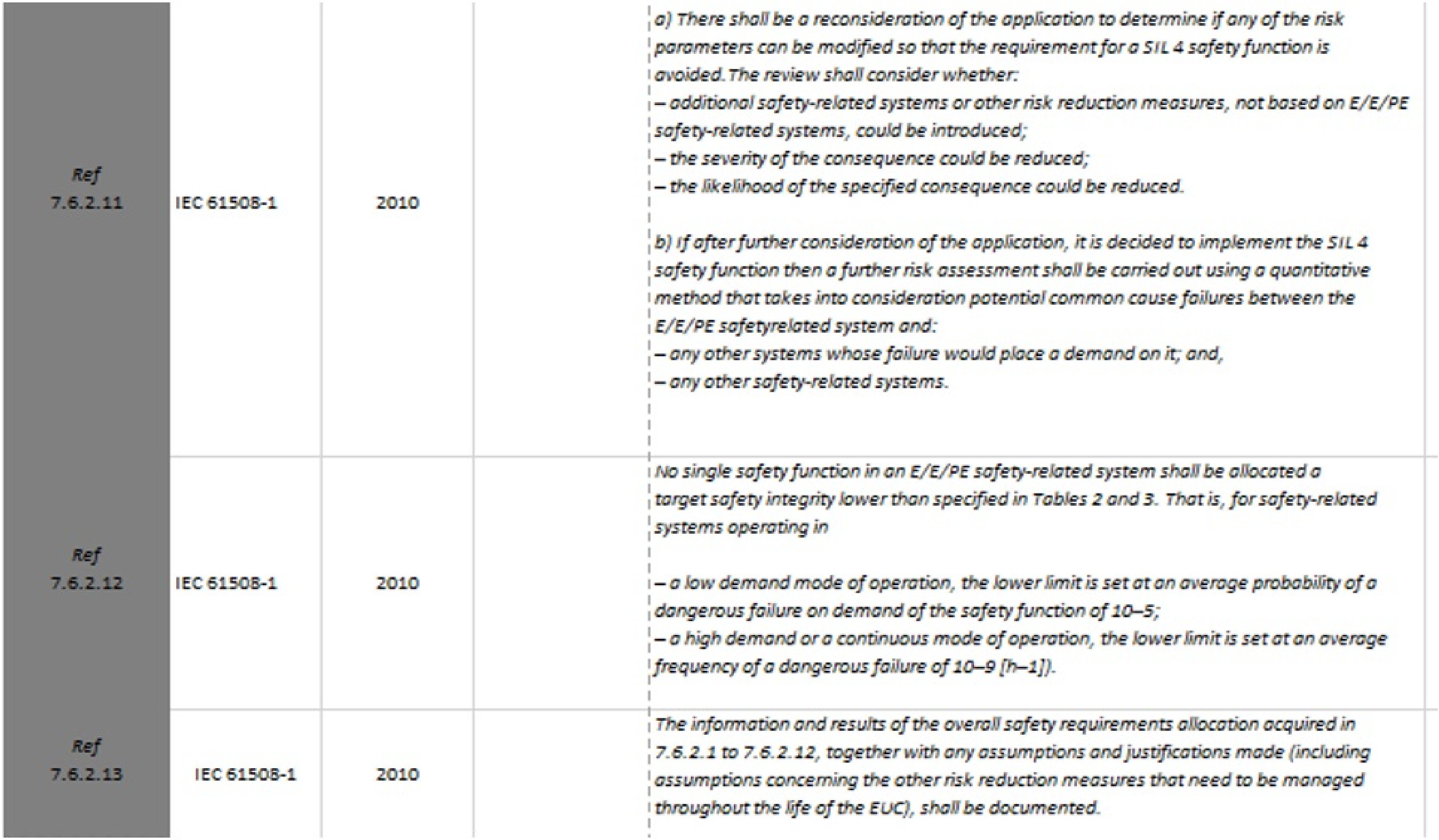
	Ref 7.5.2.7	IEC 61508-1	2010		*If the requirements of 7.5.2.6 a) to d) inclusive cannot be met, then the EUC control system shall be designated as a safety-related system. The safety integrity level of functions of the EUC control system shall be determined by the rate of dangerous failure that is claimed for the EUC control system in accordance with Table 3 (see Note 3 of 7.6.2.9). In such cases, the requirements in this standard, relevant to the allocated safety integrity level, shall apply to the EUC control system.*
Overall safety requirements allocation ***7.6***	*Ref* 7.6.2.1	IEC 61508-1	2010		*The designated safety-related systems that are to be used to achieve the required functional safety shall be specified. The tolerable risk may be met by* *– E/E/PE safety-related systems; and/or* *– other risk reduction measures.*
	Ref 7.6.2.2	IEC 61508-1	2010		*In allocating overall safety functions to the designated E/E/PE safety-related systems and other risk reduction measures, the skills and resources available during all phases of the overall safety lifecycle shall be considered.*
	Ref 7.6.2.3	IEC 61508-1	2010		*Each overall safety function, with its associated overall safety integrity requirement developed according to 7.5, shall be allocated to one or more of the designated E/E/PE safetyrelated systems and/or other risk reduction measures, so that the tolerable risk for the safety function is achieved.*
	Ref 7.6.2.3	IEC 61508-1	2010		*This allocation is iterative, and if it is found that the tolerable risk cannot be achieved, then the specifications for the EUC control system, the designated E/E/PE safetyrelated systems and the other risk reduction measures shall be modified and the allocation repeated.*



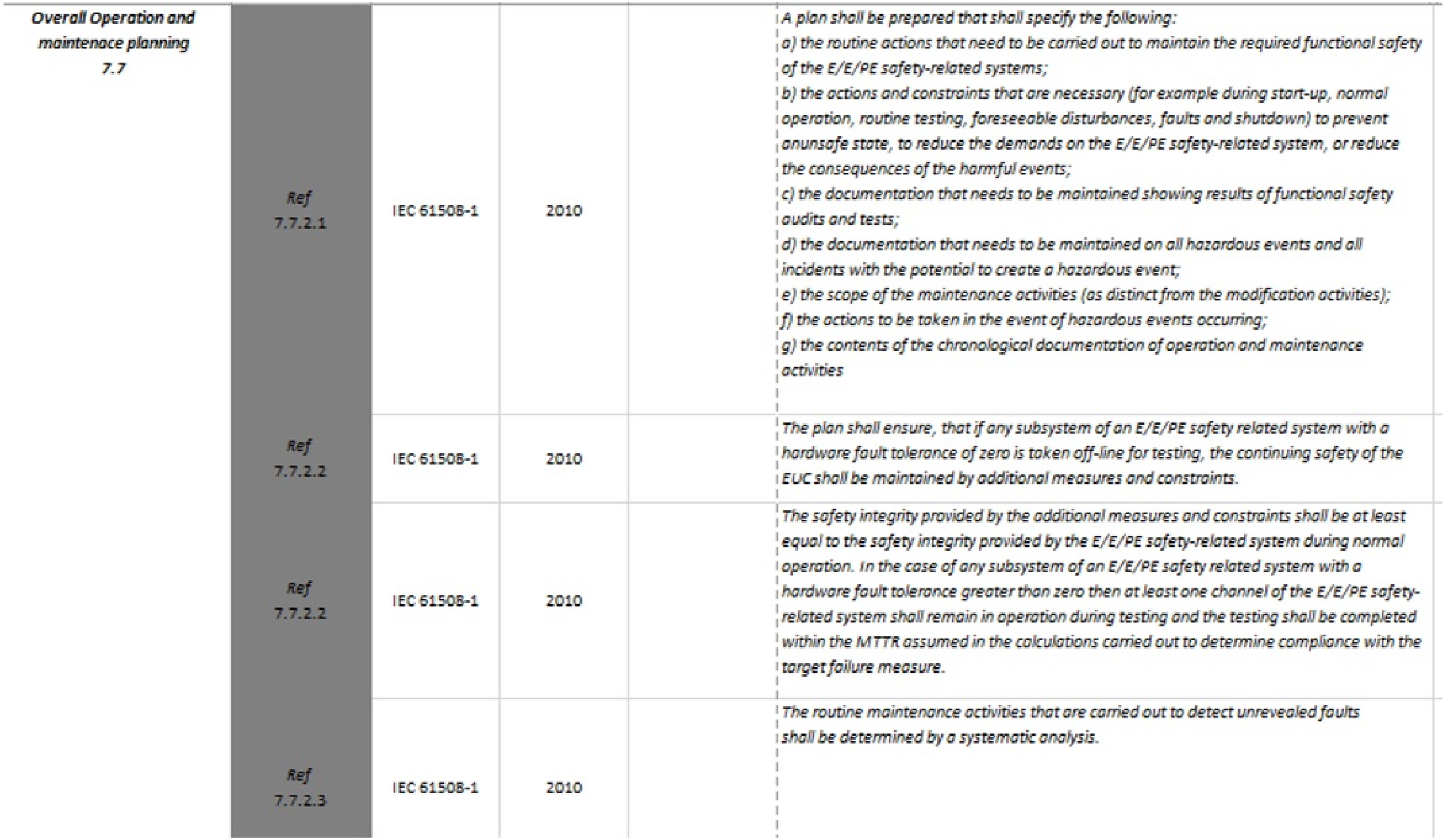
	Ref 7.6.2.5	IEC 61508-1	2010		The safety integrity requirements for each safety function shall be specified in terms of either – the average probability of a dangerous failure on demand of the safety function, for a low demand mode of operation, or – the average frequency of a dangerous failure of the safety function [h-1] for a high demand or a continuous mode of operation.
	Ref 7.6.2.6	IEC 61508-1	2010		The allocation of the safety integrity requirements shall be carried out using appropriate techniques for the combination of probabilities.
	Ref 7.6.2.7	IEC 61508-1	2010		The allocation shall proceed taking into account the possibility of common cause failures.
	Ref 7.6.2.7	IEC 61508-1	2010		If the EUC control system, E/E/PE safety-related systems and other risk reduction measures are to be treated as independent for the allocation, they shall: – be independent such that the likelihood of simultaneous failures between two or more ofthese different systems or measures is sufficiently low in relation to the required safety integrity; – be functionally diverse (i.e. use totally different approaches to achieve the same results); – be based on diverse technologies (i.e. use different types of equipment to achieve the same results); – not share common parts, services or support systems (for example power supplies) whose failure could result in a dangerous mode of failure of all systems; – not share common operational, maintenance or test procedures. Within common cause analysis, limiting and constraint conditions for the realisation of E/E/PE safety-related systems such as the aspect of necessary separation of different channels of an E/E/PE system, subsystem or element, for example by space, shall be checked – this may not allow for example for two channels/microprocessors on one board or for on-chip redundancy (see IEC 61508-2, Annex E).



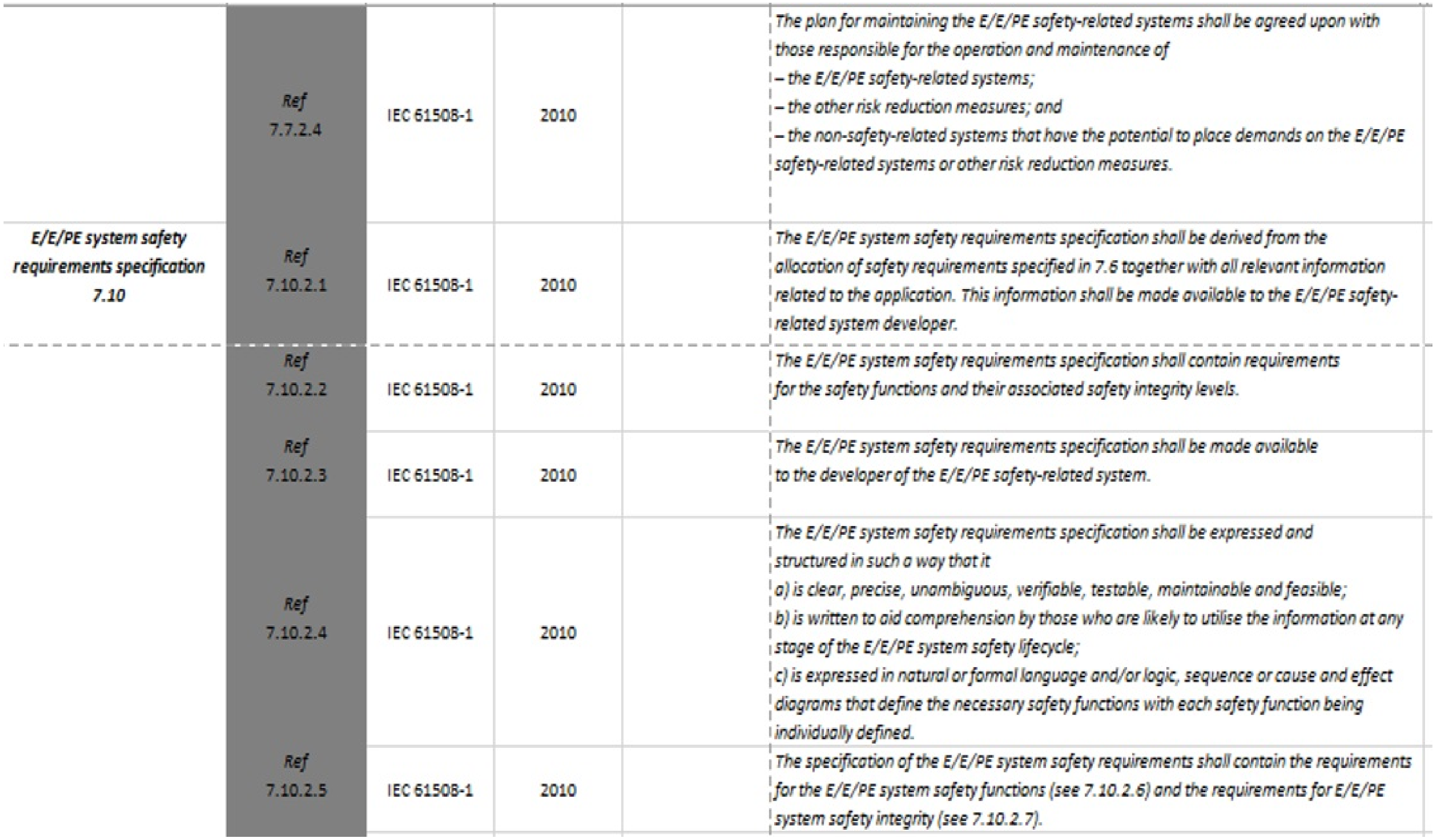
	Ref 7.6.2.8	IEC 61508-1	2010		*If not all of the requirements in 7.6.2.7 can be met then the E/E/PE safety-related systems and the other risk reduction measures shall not be treated as independent for the purposes of the safety allocation. Instead, the allocation shall take into account relevant common cause failures between the EUC control system, the E/E/PE safety-related systems and the other risk reduction measures.*
	Ref 7.6.2.9	IEC 61508-1	2010		*When the allocation has sufficiently progressed, the safety integrity requirements, for each safety function allocated to the E/E/PE safety-related system(s), shall be specified in terms of the safety integrity level in accordance with Table 2 or Table 3 and shall indicate whether the target failure measure is, either:* *– the average probability of dangerous failure on demand of the safety function, (PFDavg), for a low demand mode of operation (Table 2), or* *– the average frequency of a dangerous failure of the safety function [h-1], (PFH), for a high demand mode of operation (Table 3), or* *– the average frequency of a dangerous failure of the safety function [h-1], (PFH), for a continuous mode of operation (Table 3).*
	Ref 7.6.2.10	IEC 61508-1	2010		*For an E/E/PE safety-related system that implements safety functions of different safety integrity levels, unless it can be shown there is sufficient independence of implementation between these particular safety functions, those parts of the safety-related hardware and software where there is insufficient independence of implementation shall be treated as belonging to the safety function with the highest safety integrity level. Therefore, the requirements applicable to the highest relevant safety integrity level shall apply to all those parts.*
					In cases where the allocation process results in the requirement for an E/E/PE safety-related system implementing a SIL 4 safety function then the following shall apply: *a) There shall be a reconsideration of the application to determine if any of the risk parameters can be modified so that the requirement for a SIL 4 safety function is avoided. The review shall consider whether:*



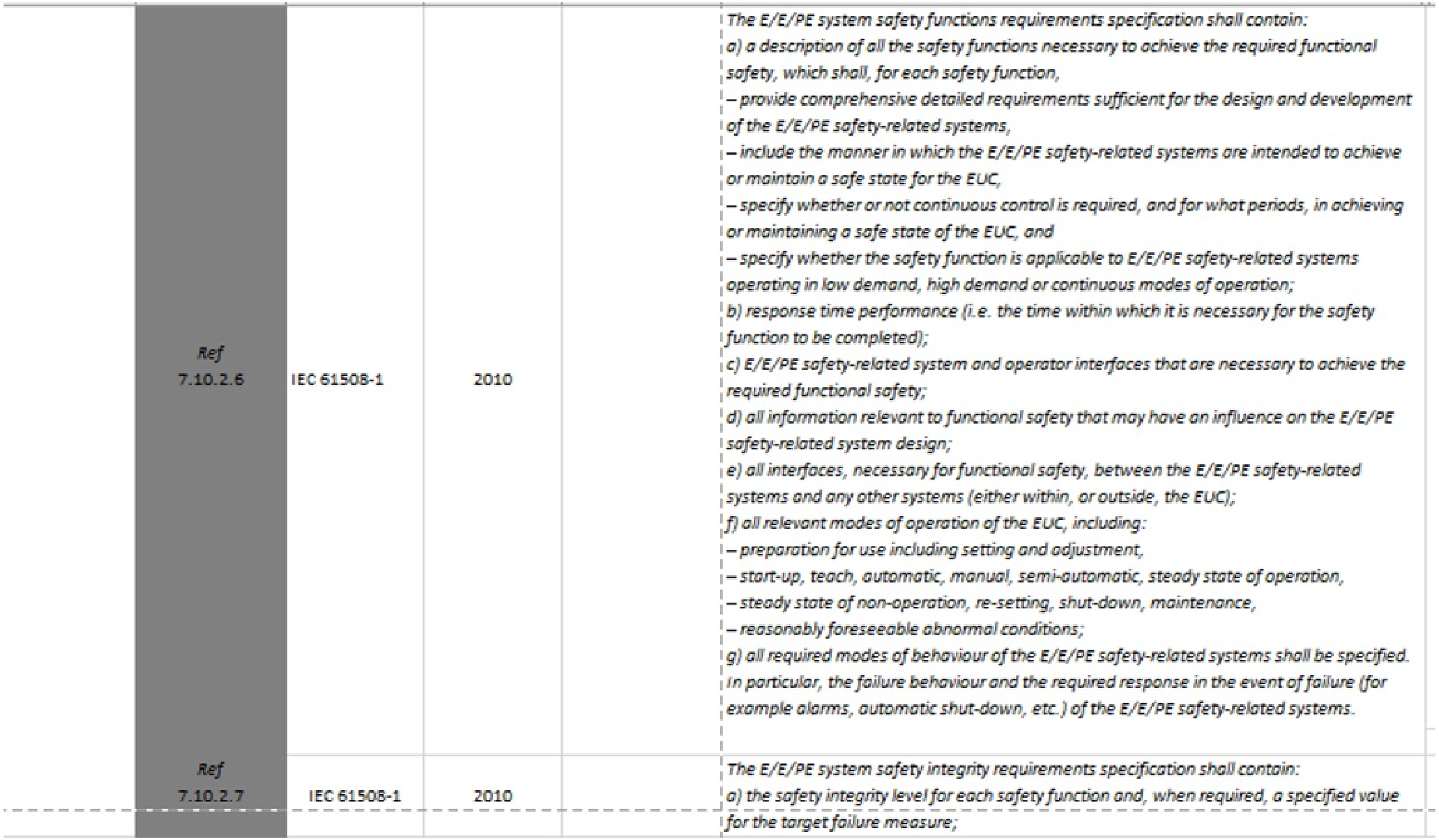
Ref 7.6.2.11	IEC 61508-1	2010		*a) There shall be a reconsideration of the application to determine if any of the risk parameters can be modified so that the requirement for a SIL 4 safety function is avoided. The review shall consider whether:* *– additional safety-related systems or other risk reduction measures, not based on E/E/PE safety-related systems, could be introduced;* *– the severity of the consequence could be reduced;* *– the likelihood of the specified consequence could be reduced.* *b) If after further consideration of the application, it is decided to implement the SIL 4 safety function then a further risk assessment shall be carried out using a quantitative method that takes into consideration potential common cause failures between the E/E/PE safetyrelated system and:* *– any other systems whose failure would place a demand on it; and,* *– any other safety-related systems.*
Ref 7.6.2.12	IEC 61508-1	2010		*No single safety function in an E/E/PE safety-related system shall be allocated a target safety integrity lower than specified in Tables 2 and 3. That is, for safety-related systems operating in* *– a low demand mode of operation, the lower limit is set at an average probability of a dangerous failure on demand of the safety function of 10–5;* *– a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of 10–9 [h–1]).*
Ref 7.6.2.13	IEC 61508-1	2010		*The information and results of the overall safety requirements allocation acquired in 7.6.2.1 to 7.6.2.12, together with any assumptions and justifications made (including assumptions concerning the other risk reduction measures that need to be managed throughout the life of the EUC), shall be documented.*



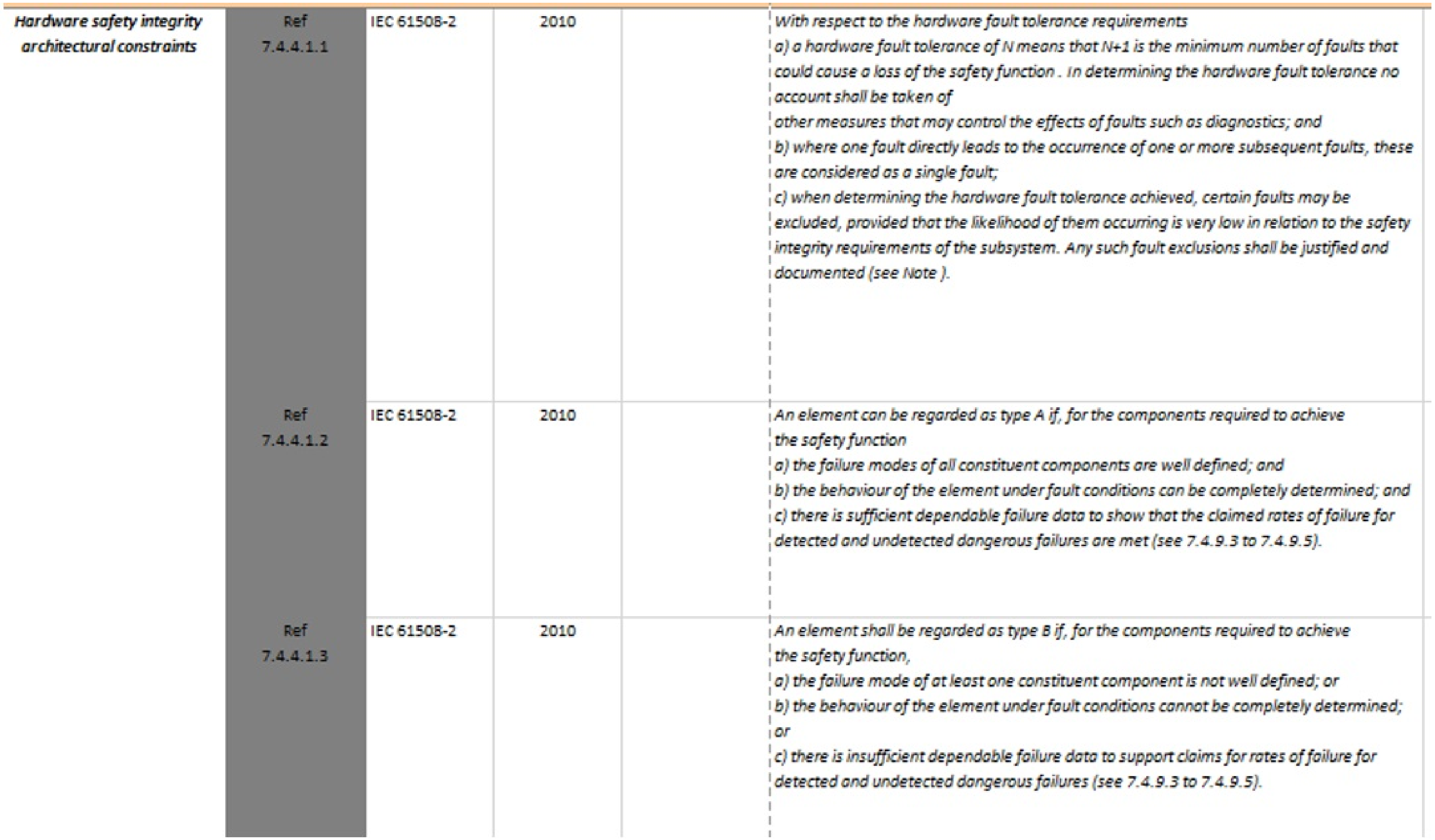
Overall Operation and maintenace planning 7.7	*Ref* 7.7.2.1	IEC 61508-1	2010		*A plan shall be prepared that shall specify the following:* *a) the routine actions that need to be carried out to maintain the required functional safety of the E/E/PE safety-related systems;* *b) the actions and constraints that are necessary (for example during start-up, normal operation, routine testing, foreseeable disturbances, faults and shutdown) to prevent anunsafe state, to reduce the demands on the E/E/PE safety-related system, or reduce the consequences of the harmful events;* *c) the documentation that needs to be maintained showing results of functional safety audits and tests;* *d) the documentation that needs to be maintained on all hazardous events and all incidents with the potential to create a hazardous event;* *e) the scope of the maintenance activities (as distinct from the modification activities);* *f) the actions to be taken in the event of hazardous events occurring;* *g) the contents of the chronological documentation of operation and maintenance activities*
	Ref 7.7.2.2	IEC 61508-1	2010		*The plan shall ensure, that if any subsystem of an E/E/PE safety related system with a hardware fault tolerance of zero is taken off-line for testing, the continuing safety of the EUC shall be maintained by additional measures and constraints.*
	Ref 7.7.2.2	IEC 61508-1	2010		*The safety integrity provided by the additional measures and constraints shall be at least equal to the safety integrity provided by the E/E/PE safety-related system during normal operation. In the case of any subsystem of an E/E/PE safety related system with a hardware fault tolerance greater than zero then at least one channel of the E/E/PE safety-related system shall remain in operation during testing and the testing shall be completed within the MTTR assumed in the calculations carried out to determine compliance with the target failure measure.*
	Ref 7.7.2.3	IEC 61508-1	2010		*The routine maintenance activities that are carried out to detect unrevealed faults shall be determined by a systematic analysis.*



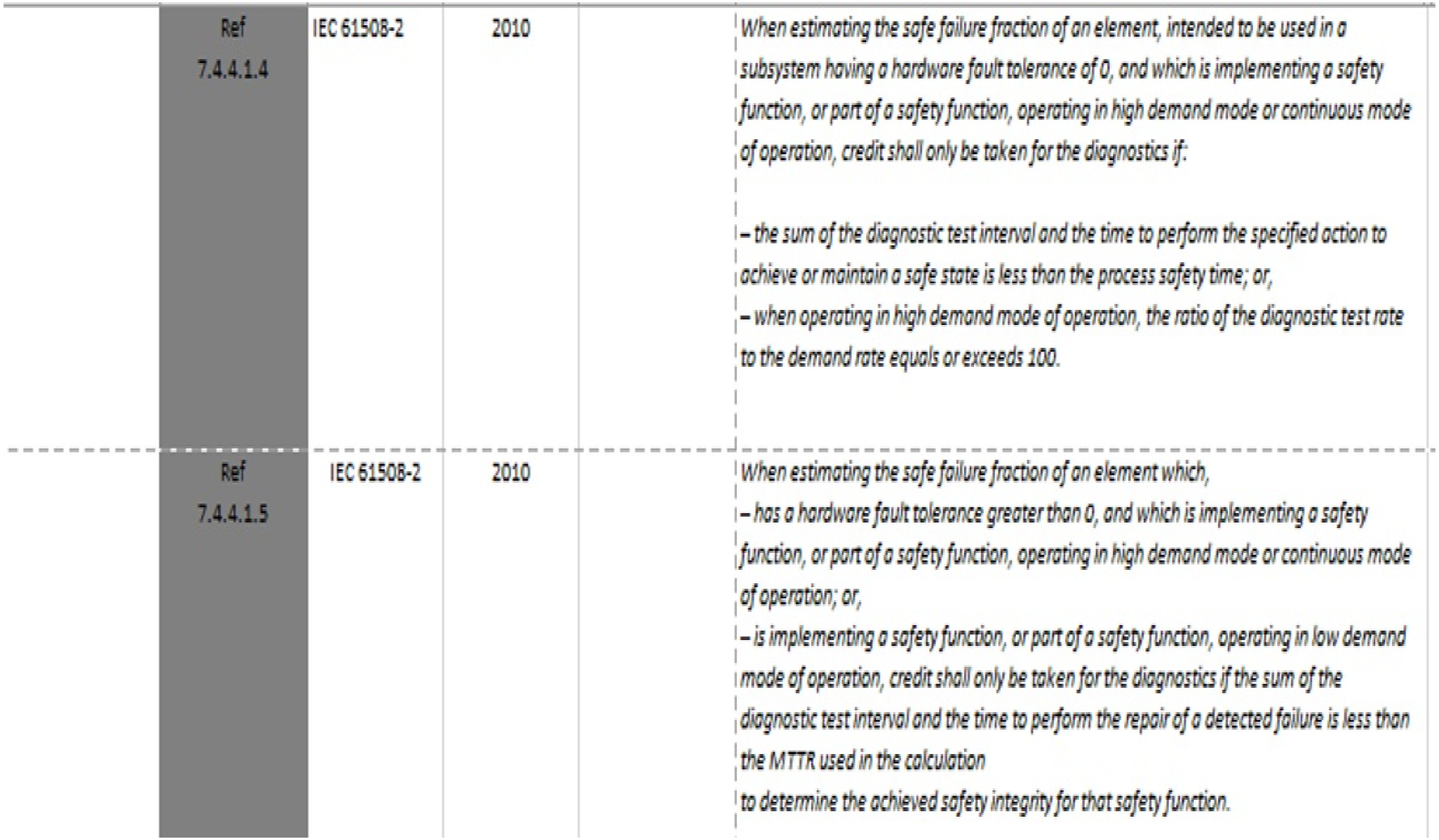
	Ref 7.7.2.4	IEC 61508-1	2010		*The plan for maintaining the E/E/PE safety-related systems shall be agreed upon with those responsible for the operation and maintenance of* *– the E/E/PE safety-related systems;* *– the other risk reduction measures; and* *– the non-safety-related systems that have the potential to place demands on the E/E/PE safety-related systems or other risk reduction measures.*
E/E/PE system safety requirements specification 7.10	*Ref* 7.10.2.1	IEC 61508-1	2010		*The E/E/PE system safety requirements specification shall be derived from the allocation of safety requirements specified in 7.6 together with all relevant information related to the application. This information shall be made available to the E/E/PE safety-related system developer.*
	Ref 7.10.2.2	IEC 61508-1	2010		*The E/E/PE system safety requirements specification shall contain requirements for the safety functions and their associated safety integrity levels.*
	Ref 7.10.2.3	IEC 61508-1	2010		*The E/E/PE system safety requirements specification shall be made available to the developer of the E/E/PE safety-related system.*
	Ref 7.10.2.4	IEC 61508-1	2010		*The E/E/PE system safety requirements specification shall be expressed and structured in such a way that it* *a) is clear, precise, unambiguous, verifiable, testable, maintainable and feasible;* *b) is written to aid comprehension by those who are likely to utilise the information at any stage of the E/E/PE system safety lifecycle;* *c) is expressed in natural or formal language and/or logic, sequence or cause and effect diagrams that define the necessary safety functions with each safety function being individually defined.*
	Ref 7.10.2.5	IEC 61508-1	2010		*The specification of the E/E/PE system safety requirements shall contain the requirements for the E/E/PE system safety functions (see 7.10.2.6) and the requirements for E/E/PE system safety integrity (see 7.10.2.7).*



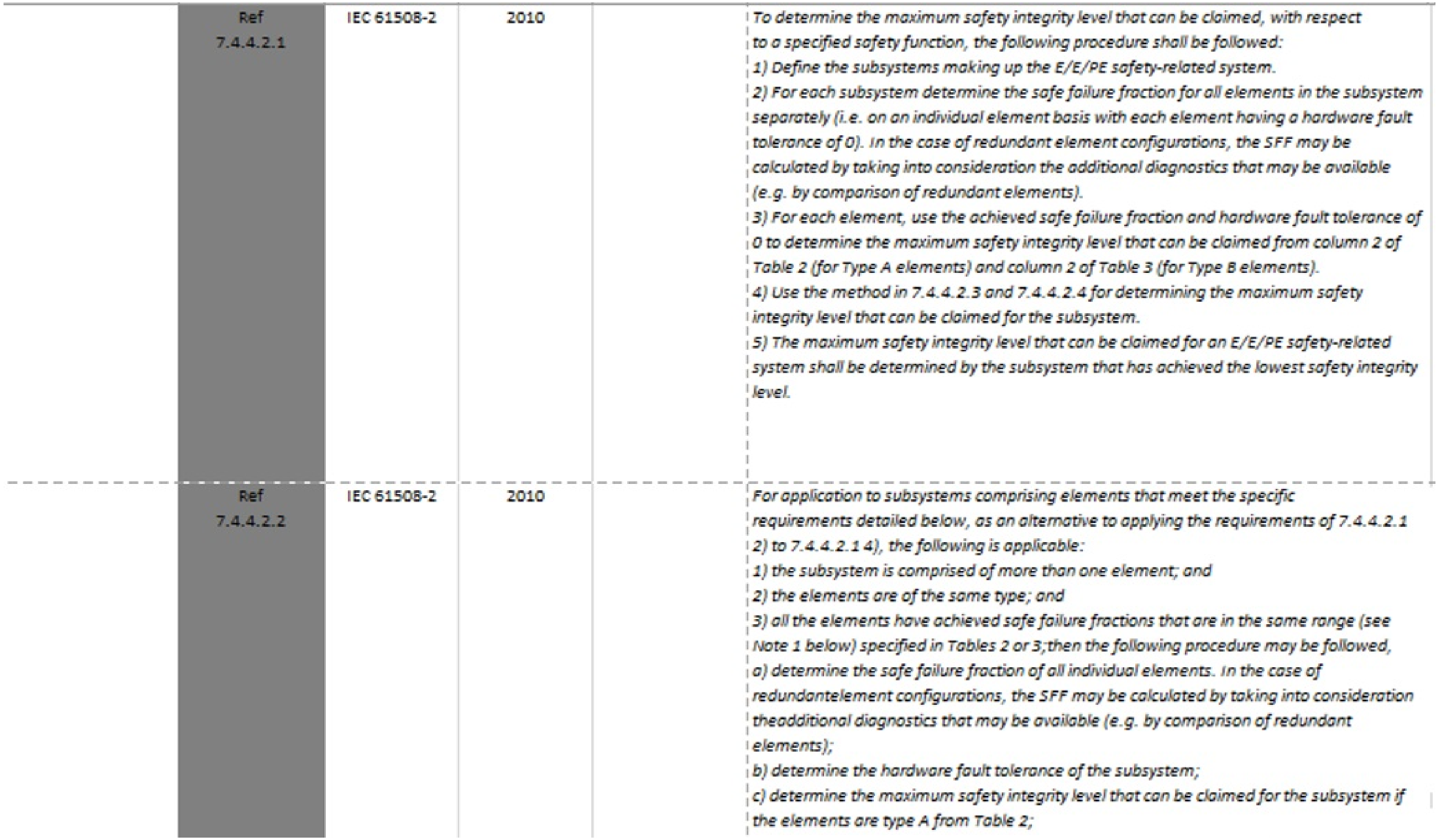
	Ref 7.10.2.6	IEC 61508-1	2010		*The E/E/PE system safety functions requirements specification shall contain:* *a) a description of all the safety functions necessary to achieve the required functional safety, which shall, for each safety function,* *– provide comprehensive detailed requirements sufficient for the design and development of the E/E/PE safety-related systems,* *– include the manner in which the E/E/PE safety-related systems are intended to achieve or maintain a safe state for the EUC,* *– specify whether or not continuous control is required, and for what periods, in achieving or maintaining a safe state of the EUC, and* *– specify whether the safety function is applicable to E/E/PE safety-related systems operating in low demand, high demand or continuous modes of operation;* *b) response time performance (i.e. the time within which it is necessary for the safety function to be completed);* *c) E/E/PE safety-related system and operator interfaces that are necessary to achieve the required functional safety;* *d) all information relevant to functional safety that may have an influence on the E/E/PE safety-related system design;* *e) all interfaces, necessary for functional safety, between the E/E/PE safety-related systems and any other systems (either within, or outside, the EUC);* *f) all relevant modes of operation of the EUC, including:* *– preparation for use including setting and adjustment,* *– start-up, teach, automatic, manual, semi-automatic, steady state of operation,* *– steady state of non-operation, re-setting, shut-down, maintenance,* *– reasonably foreseeable abnormal conditions;* *g) all required modes of behaviour of the E/E/PE safety-related systems shall be specified. In particular, the failure behaviour and the required response in the event of failure (for example alarms, automatic shut-down, etc.) of the E/E/PE safety-related systems.*
	Ref 7.10.2.7	IEC 61508-1	2010		*The E/E/PE system safety integrity requirements specification shall contain:* *a) the safety integrity level for each safety function and, when required, a specified value for the target failure measure;*



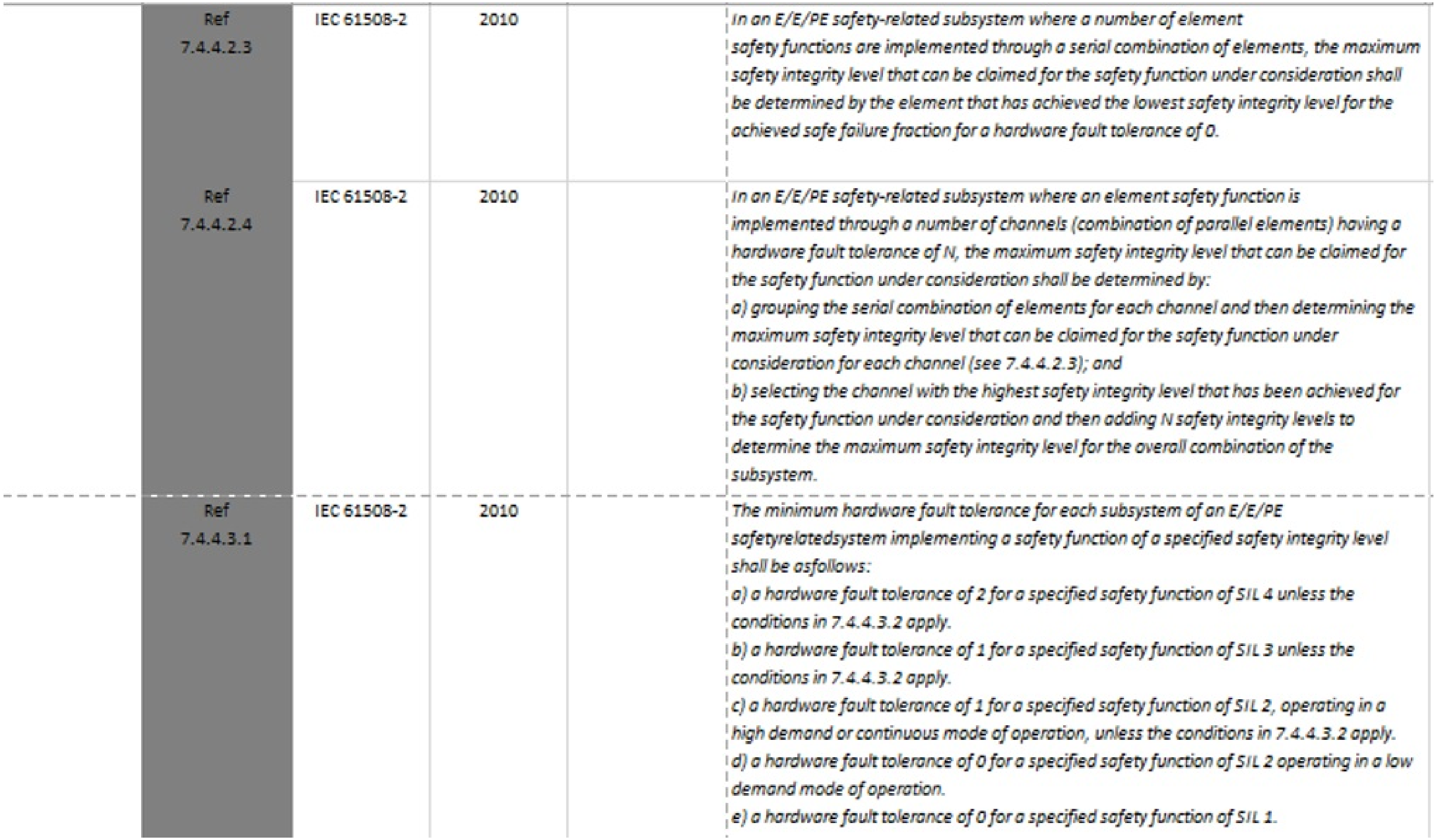
Hardware safety integrity architectural constraints	Ref 7.4.4.1.1	IEC 61508-2	2010		*With respect to the hardware fault tolerance requirements* *a) a hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function . In determining the hardware fault tolerance no account shall be taken of* *other measures that may control the effects of faults such as diagnostics; and* *b) where one fault directly leads to the occurrence of one or more subsequent faults, these are considered as a single fault;* *c) when determining the hardware fault tolerance achieved, certain faults may be excluded, provided that the likelihood of them occurring is very low in relation to the safety integrity requirements of the subsystem. Any such fault exclusions shall be justified and documented (see Note).*
	Ref 7.4.4.1.2	IEC 61508-2	2010		*An element can be regarded as type A if, for the components required to achieve the safety function* *a) the failure modes of all constituent components are well defined; and* *b) the behaviour of the element under fault conditions can be completely determined; and* *c) there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met (see 7.4.9.3 to 7.4.9.5).*
	Ref 7.4.4.1.3	IEC 61508-2	2010		*An element shall be regarded as type B if, for the components required to achieve the safety function,* *a) the failure mode of at least one constituent component is not well defined; or* *b) the behaviour of the element under fault conditions cannot be completely determined; or* *c) there is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures (see 7.4.9.3 to 7.4.9.5).*



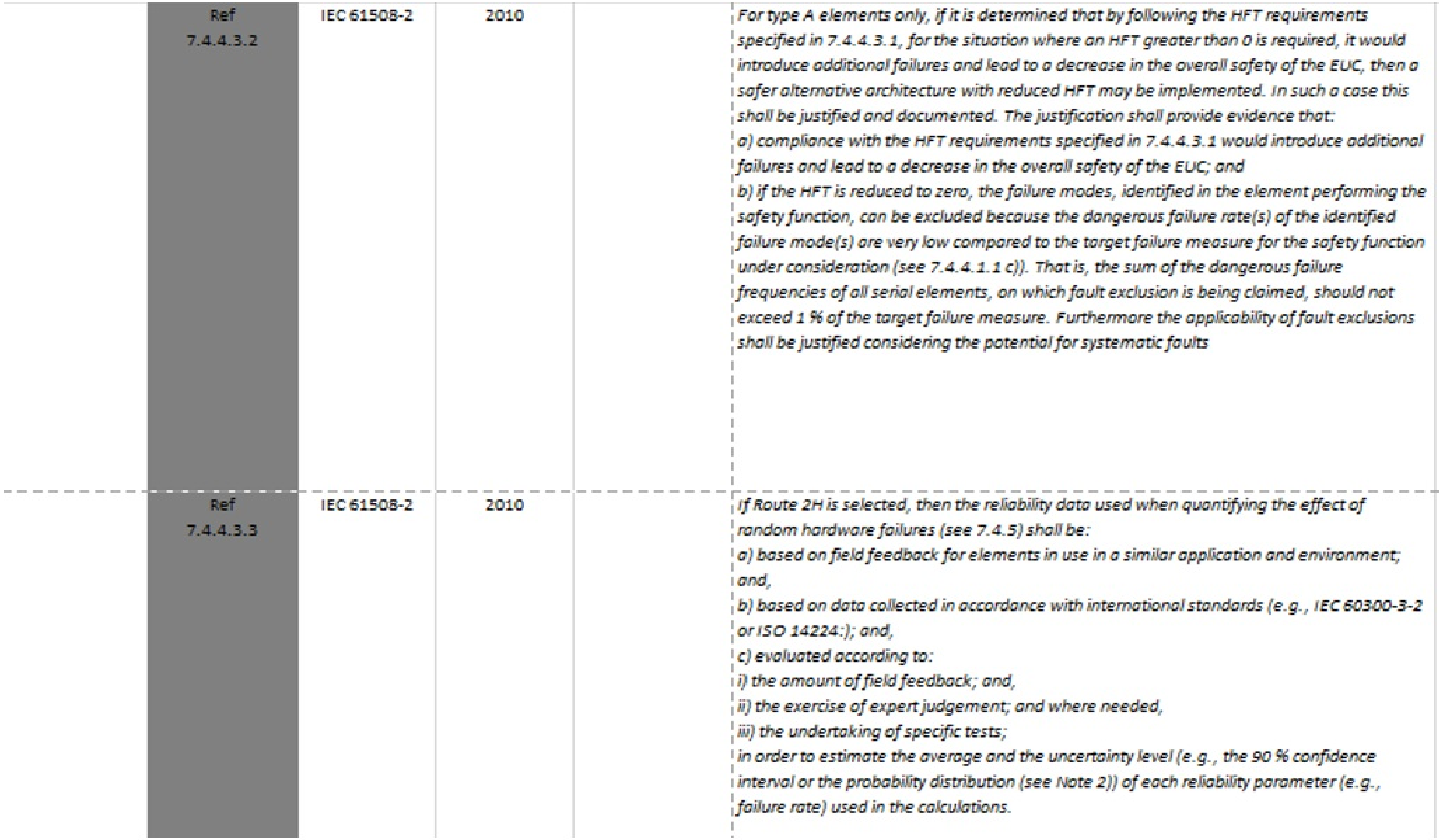
	Ref 7.4.4.1.4	IEC 61508-2	2010		When estimating the safe failure fraction of an element, intended to be used in a subsystem having a hardware fault tolerance of 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation, credit shall only be taken for the diagnostics if: – the sum of the diagnostic test interval and the time to perform the specified action to achieve or maintain a safe state is less than the process safety time; or, – when operating in high demand mode of operation, the ratio of the diagnostic test rate to the demand rate equals or exceeds 100.
	Ref 7.4.4.1.5	IEC 61508-2	2010		When estimating the safe failure fraction of an element which, – has a hardware fault tolerance greater than 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation; or, – is implementing a safety function, or part of a safety function, operating in low demand mode of operation, credit shall only be taken for the diagnostics if the sum of the diagnostic test interval and the time to perform the repair of a detected failure is less than the MTTR used in the calculation to determine the achieved safety integrity for that safety function.



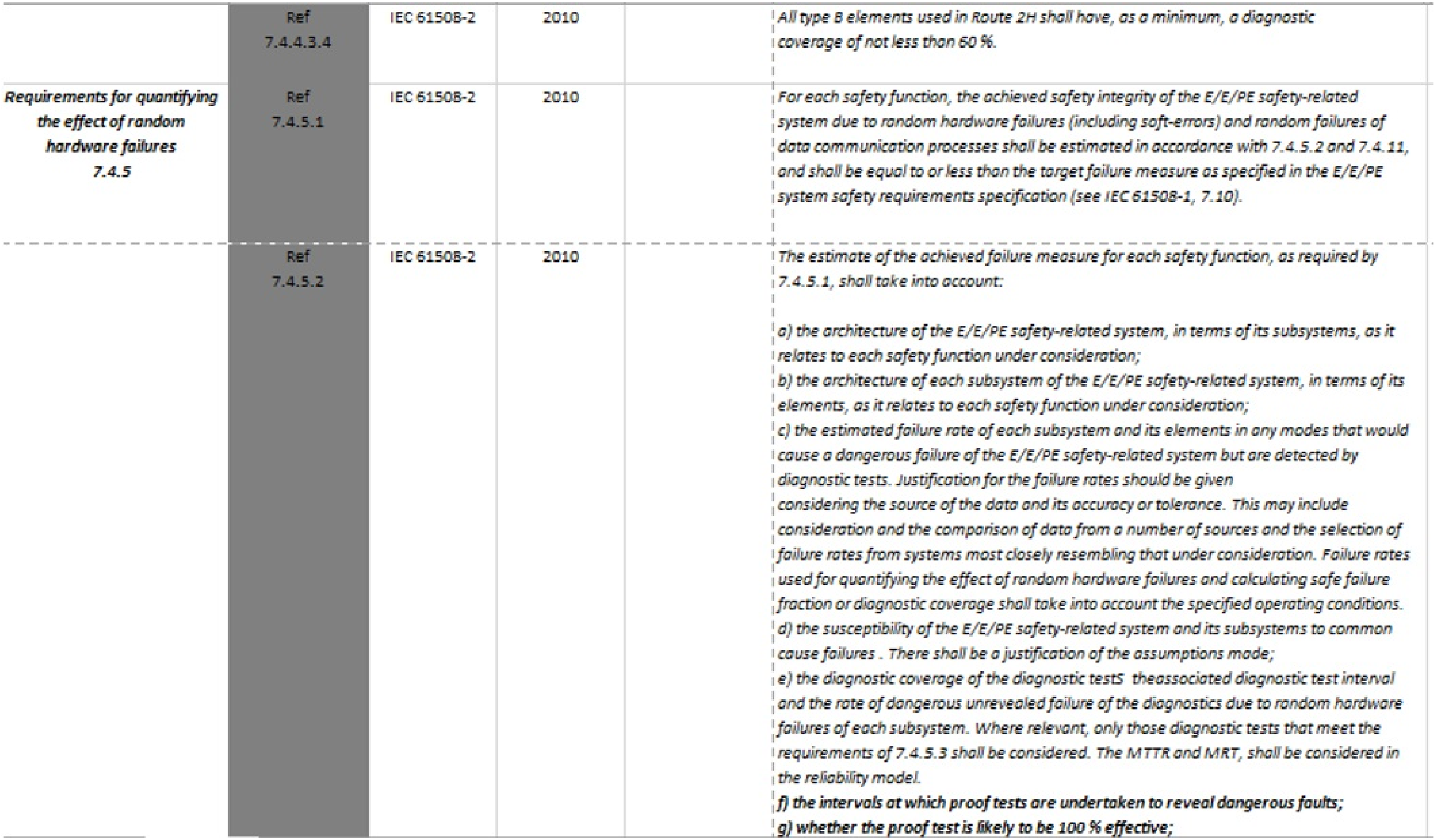
	Ref 7.4.4.2.1	IEC 61508-2	2010		To determine the maximum safety integrity level that can be claimed, with respect to a specified safety function, the following procedure shall be followed: 1) Define the subsystems making up the E/E/PE safety-related system. 2) For each subsystem determine the safe failure fraction for all elements in the subsystem separately (i.e. on an individual element basis with each element having a hardware fault tolerance of 0). In the case of redundant element configurations, the SFF may be calculated by taking into consideration the additional diagnostics that may be available (e.g. by comparison of redundant elements). 3) For each element, use the achieved safe failure fraction and hardware fault tolerance of 0 to determine the maximum safety integrity level that can be claimed from column 2 of Table 2 (for Type A elements) and column 2 of Table 3 (for Type B elements). 4) Use the method in 7.4.4.2.3 and 7.4.4.2.4 for determining the maximum safety integrity level that can be claimed for the subsystem. 5) The maximum safety integrity level that can be claimed for an E/E/PE safety-related system shall be determined by the subsystem that has achieved the lowest safety integrity level.
	Ref 7.4.4.2.2	IEC 61508-2	2010		For application to subsystems comprising elements that meet the specific requirements detailed below, as an alternative to applying the requirements of 7.4.4.2.1 2) to 7.4.4.2.1 4), the following is applicable: 1) the subsystem is comprised of more than one element; and 2) the elements are of the same type; and 3) all the elements have achieved safe failure fractions that are in the same range (see Note 1 below) specified in Tables 2 or 3;then the following procedure may be followed, a) determine the safe failure fraction of all individual elements. In the case of redundantelement configurations, the SFF may be calculated by taking into consideration theadditional diagnostics that may be available (e.g. by comparison of redundant elements); b) determine the hardware fault tolerance of the subsystem; c) determine the maximum safety integrity level that can be claimed for the subsystem if the elements are type A from Table 2;



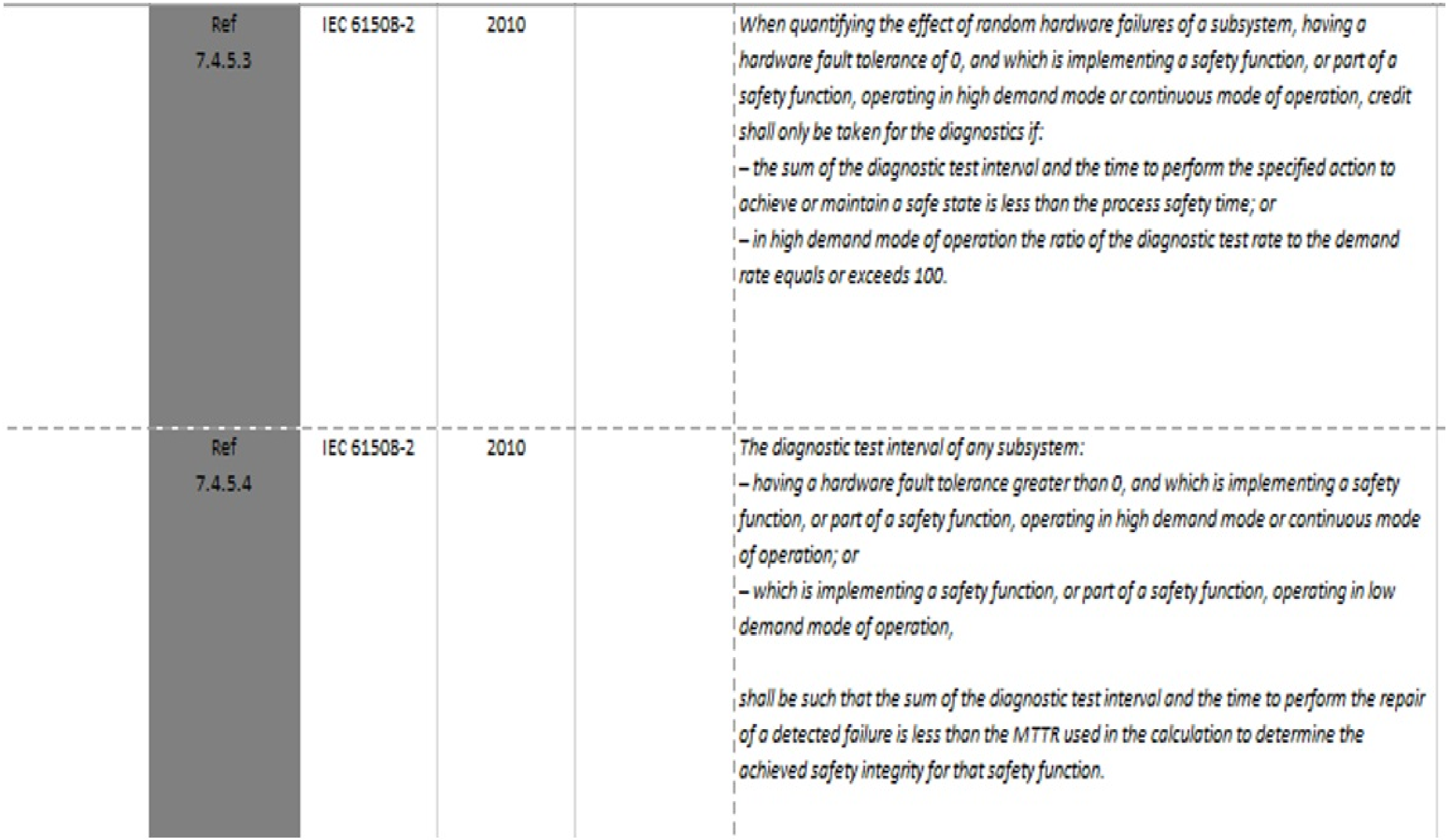
	Ref 7.4.4.2.3	IEC 61508-2	2010		In an E/E/PE safety-related subsystem where a number of element safety functions are implemented through a serial combination of elements, the maximum safety integrity level that can be claimed for the safety function under consideration shall be determined by the element that has achieved the lowest safety integrity level for the achieved safe failure fraction for a hardware fault tolerance of 0.
	Ref 7.4.4.2.4	IEC 61508-2	2010		In an E/E/PE safety-related subsystem where an element safety function is implemented through a number of channels (combination of parallel elements) having a hardware fault tolerance of N, the maximum safety integrity level that can be claimed for the safety function under consideration shall be determined by: a) grouping the serial combination of elements for each channel and then determining the maximum safety integrity level that can be claimed for the safety function under consideration for each channel (see 7.4.4.2.3); and b) selecting the channel with the highest safety integrity level that has been achieved for the safety function under consideration and then adding N safety integrity levels to determine the maximum safety integrity level for the overall combination of the subsystem.
	Ref 7.4.4.3.1	IEC 61508-2	2010		The minimum hardware fault tolerance for each subsystem of an E/E/PE safetyrelatedsystem implementing a safety function of a specified safety integrity level shall be asfollows: a) a hardware fault tolerance of 2 for a specified safety function of SIL 4 unless the conditions in 7.4.4.3.2 apply. b) a hardware fault tolerance of 1 for a specified safety function of SIL 3 unless the conditions in 7.4.4.3.2 apply. c) a hardware fault tolerance of 1 for a specified safety function of SIL 2, operating in a high demand or continuous mode of operation, unless the conditions in 7.4.4.3.2 apply. d) a hardware fault tolerance of 0 for a specified safety function of SIL 2 operating in a low demand mode of operation. e) a hardware fault tolerance of 0 for a specified safety function of SIL 1.



	Ref 7.4.4.3.2	IEC 61508-2	2010		For type A elements only, if it is determined that by following the HFT requirements specified in 7.4.4.3.1, for the situation where an HFT greater than 0 is required, it would introduce additional failures and lead to a decrease in the overall safety of the EUC, then a safer alternative architecture with reduced HFT may be implemented. In such a case this shall be justified and documented. The justification shall provide evidence that: a) compliance with the HFT requirements specified in 7.4.4.3.1 would introduce additional failures and lead to a decrease in the overall safety of the EUC; and b) if the HFT is reduced to zero, the failure modes, identified in the element performing the safety function, can be excluded because the dangerous failure rate(s) of the identified failure mode(s) are very low compared to the target failure measure for the safety function under consideration (see 7.4.4.1.1 c)). That is, the sum of the dangerous failure frequencies of all serial elements, on which fault exclusion is being claimed, should not exceed 1 % of the target failure measure. Furthermore the applicability of fault exclusions shall be justified considering the potential for systematic faults
	Ref 7.4.4.3.3	IEC 61508-2	2010		If Route 2H is selected, then the reliability data used when quantifying the effect of random hardware failures (see 7.4.5) shall be: a) based on field feedback for elements in use in a similar application and environment; and, b) based on data collected in accordance with international standards (e.g., IEC 60300-3-2 or ISO 14224:); and, c) evaluated according to: i) the amount of field feedback; and, ii) the exercise of expert judgement; and where needed, iii) the undertaking of specific tests; in order to estimate the average and the uncertainty level (e.g., the 90 % confidence interval or the probability distribution (see Note 2)) of each reliability parameter (e.g., failure rate) used in the calculations.

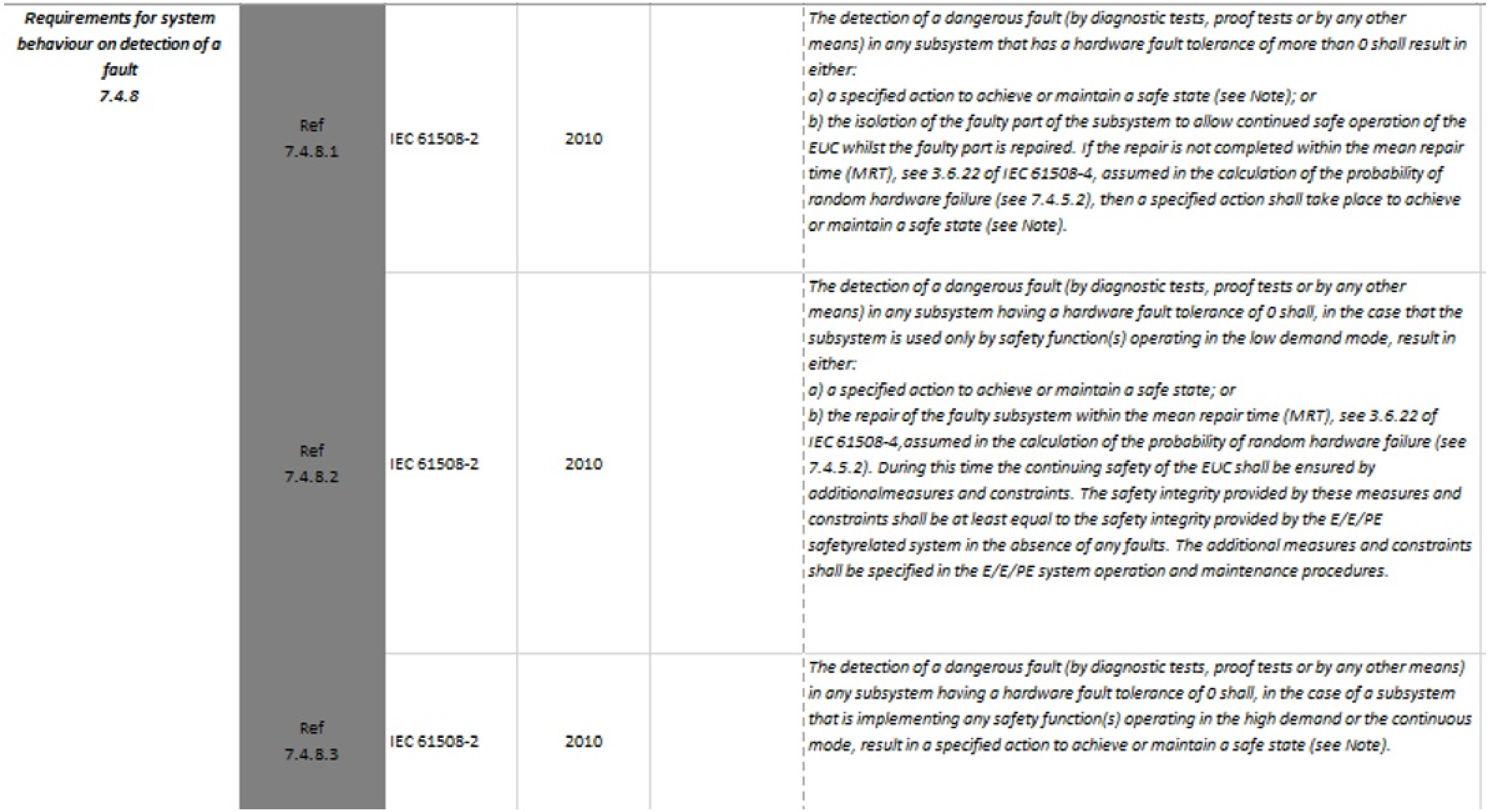


	Ref 7.4.4.3.4	IEC 61508-2	2010		*All type B elements used in Route 2H shall have, as a minimum, a diagnostic coverage of not less than 60 %.*
Requirements for quantifying the effect of random hardware failures 7.4.5	Ref 7.4.5.1	IEC 61508-2	2010		*For each safety function, the achieved safety integrity of the E/E/PE safety-related system due to random hardware failures (including soft-errors) and random failures of data communication processes shall be estimated in accordance with 7.4.5.2 and 7.4.11, and shall be equal to or less than the target failure measure as specified in the E/E/PE system safety requirements specification (see IEC 61508-1, 7.10).*
	Ref 7.4.5.2	IEC 61508-2	2010		*The estimate of the achieved failure measure for each safety function, as required by 7.4.5.1, shall take into account:* *a) the architecture of the E/E/PE safety-related system, in terms of its subsystems, as it relates to each safety function under consideration;* *b) the architecture of each subsystem of the E/E/PE safety-related system, in terms of its elements, as it relates to each safety function under consideration;* *c) the estimated failure rate of each subsystem and its elements in any modes that would cause a dangerous failure of the E/E/PE safety-related system but are detected by diagnostic tests. Justification for the failure rates should be given considering the source of the data and its accuracy or tolerance. This may include consideration and the comparison of data from a number of sources and the selection of failure rates from systems most closely resembling that under consideration. Failure rates used for quantifying the effect of random hardware failures and calculating safe failure fraction or diagnostic coverage shall take into account the specified operating conditions.* *d) the susceptibility of the E/E/PE safety-related system and its subsystems to common cause failures . There shall be a justification of the assumptions made;* *e) the diagnostic coverage of the diagnostic testS theassociated diagnostic test interval and the rate of dangerous unrevealed failure of the diagnostics due to random hardware failures of each subsystem. Where relevant, only those diagnostic tests that meet the requirements of 7.4.5.3 shall be considered. The MTTR and MRT, shall be considered in the reliability model.* ***f) the intervals at which proof tests are undertaken to reveal dangerous faults;*** ***g) whether the proof test is likely to be 100 % effective;***

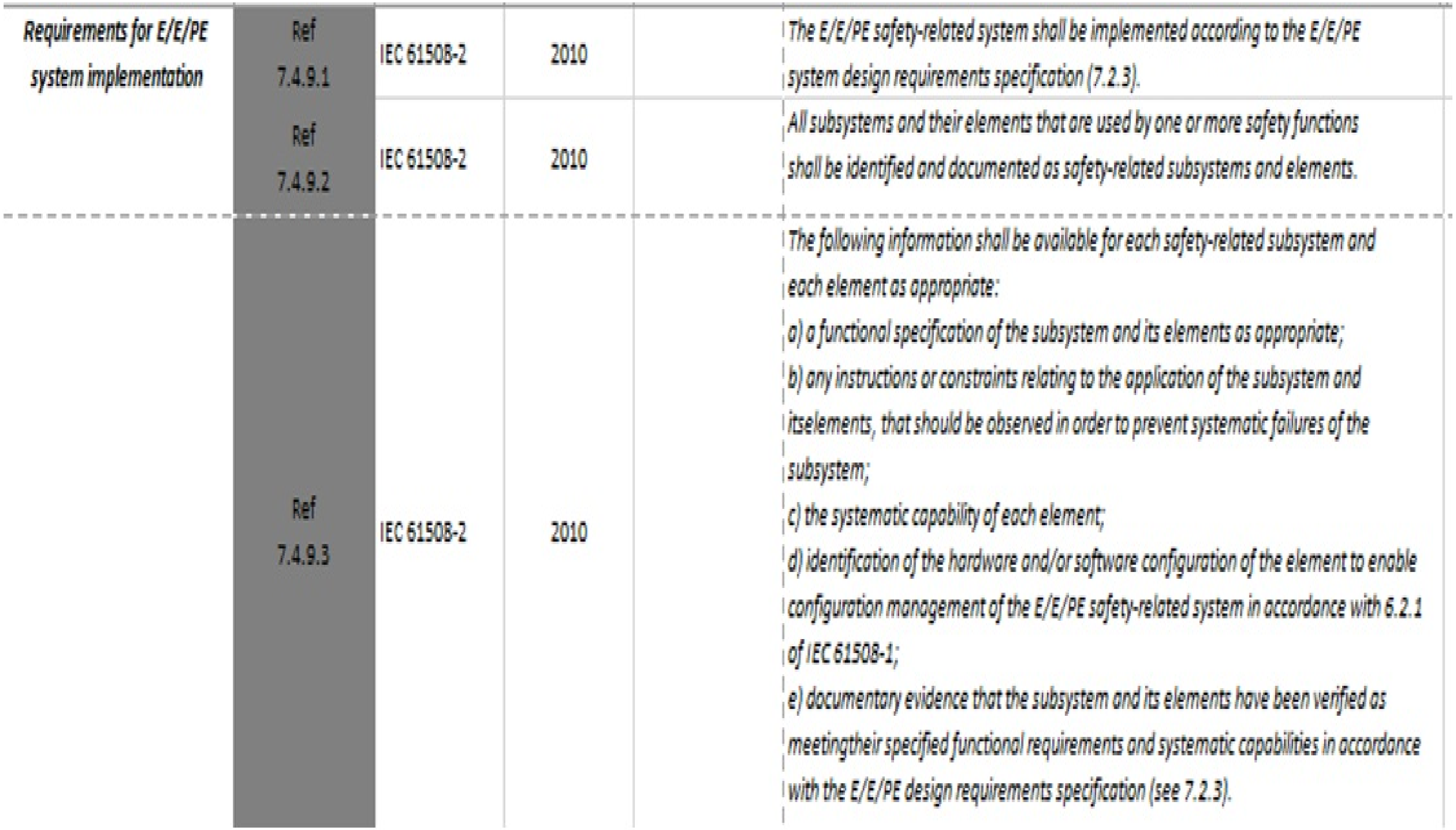


	Ref 7.4.5.3	IEC 61508-2	2010		When quantifying the effect of random hardware failures of a subsystem, having a hardware fault tolerance of 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation, credit shall only be taken for the diagnostics if: – the sum of the diagnostic test interval and the time to perform the specified action to achieve or maintain a safe state is less than the process safety time; or – in high demand mode of operation the ratio of the diagnostic test rate to the demand rate equals or exceeds 100.
	Ref 7.4.5.4	IEC 61508-2	2010		The diagnostic test interval of any subsystem: – having a hardware fault tolerance greater than 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation; or – which is implementing a safety function, or part of a safety function, operating in low demand mode of operation, shall be such that the sum of the diagnostic test interval and the time to perform the repair of a detected failure is less than the MTTR used in the calculation to determine the achieved safety integrity for that safety function.

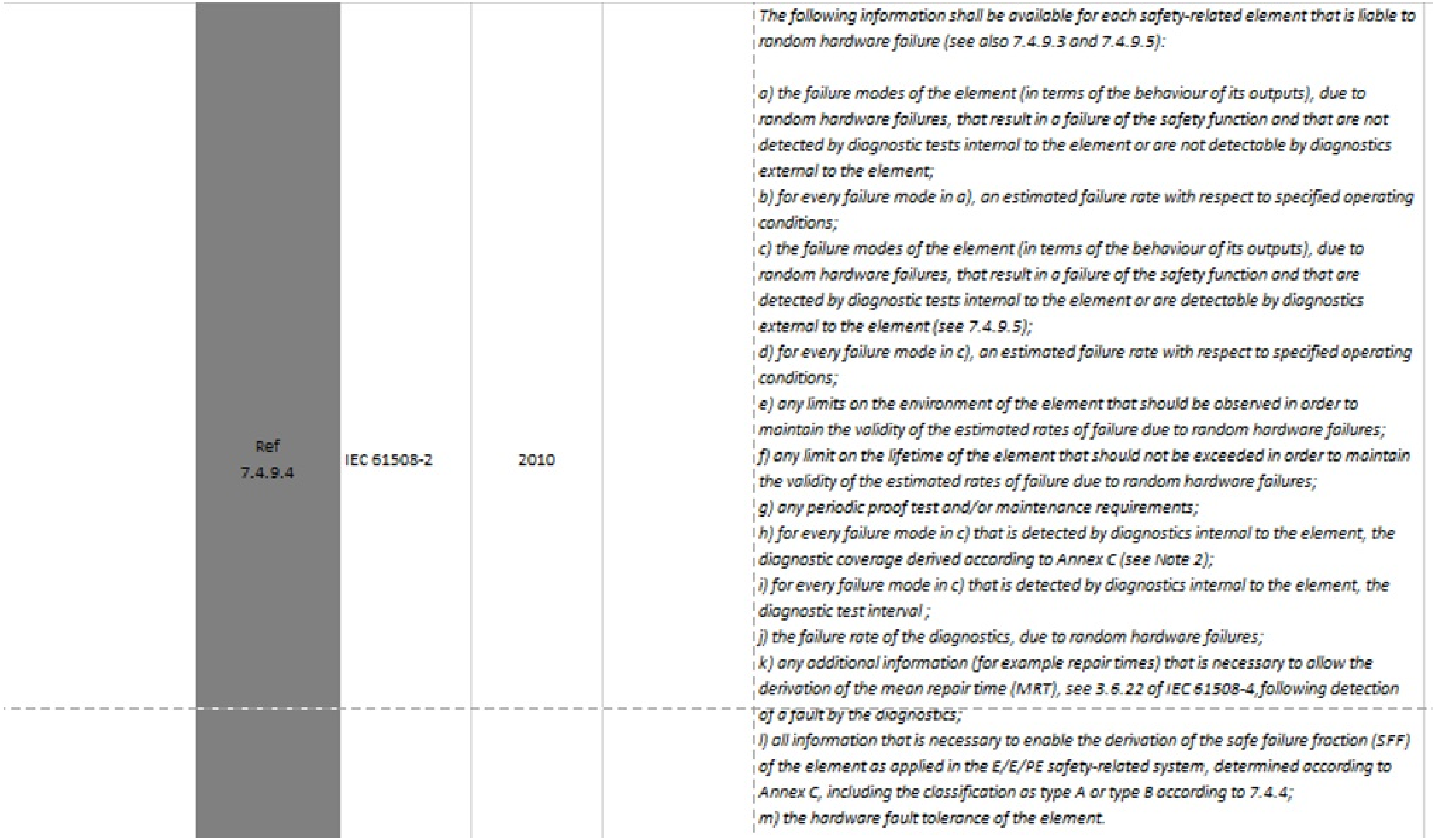
	Ref 7.4.5.5	IEC 61508-2	2010		*If, for a particular design, the safety integrity requirement for the relevant safety function is not achieved then:* *a) determine the elements, subsystems and/or parameters contributing most to the function's calculated failure rate;* *b) evaluate the effect of possible improvement measures on the identified critical elements, subsystems or parameters (for example, more reliable components, additional defences against common mode failures, increased diagnostic coverage, increased redundancy, reduced proof test interval, staggering tests, etc);* *c) select and implement the applicable improvements;* *d) repeat the necessary steps to establish the new probability of a random hardware failure*
Requirements for the control of systematic faults 7.4.7	Ref 7.4.7.1	IEC 61508-2	2010		*For controlling systematic faults, the E/E/PE system design shall possess design features that make the E/E/PE safety-related systems tolerant against:* *a) any residual design faults in the hardware, unless the possibility of hardware design faults can be excluded;* *b) environmental stresses, including electromagnetic disturbances;* *c) mistakes made by the operator of the EUC;* *d) any residual design faults in the software;* *e) errors and other effects arising from any data communication process (see 7.4.11).*
	Ref 7.4.7.2	IEC 61508-2	2010		*Maintainability and testability shall be considered during the design and development activities in order to facilitate implementation of these properties in the final E/E/PE safetyrelated systems.*



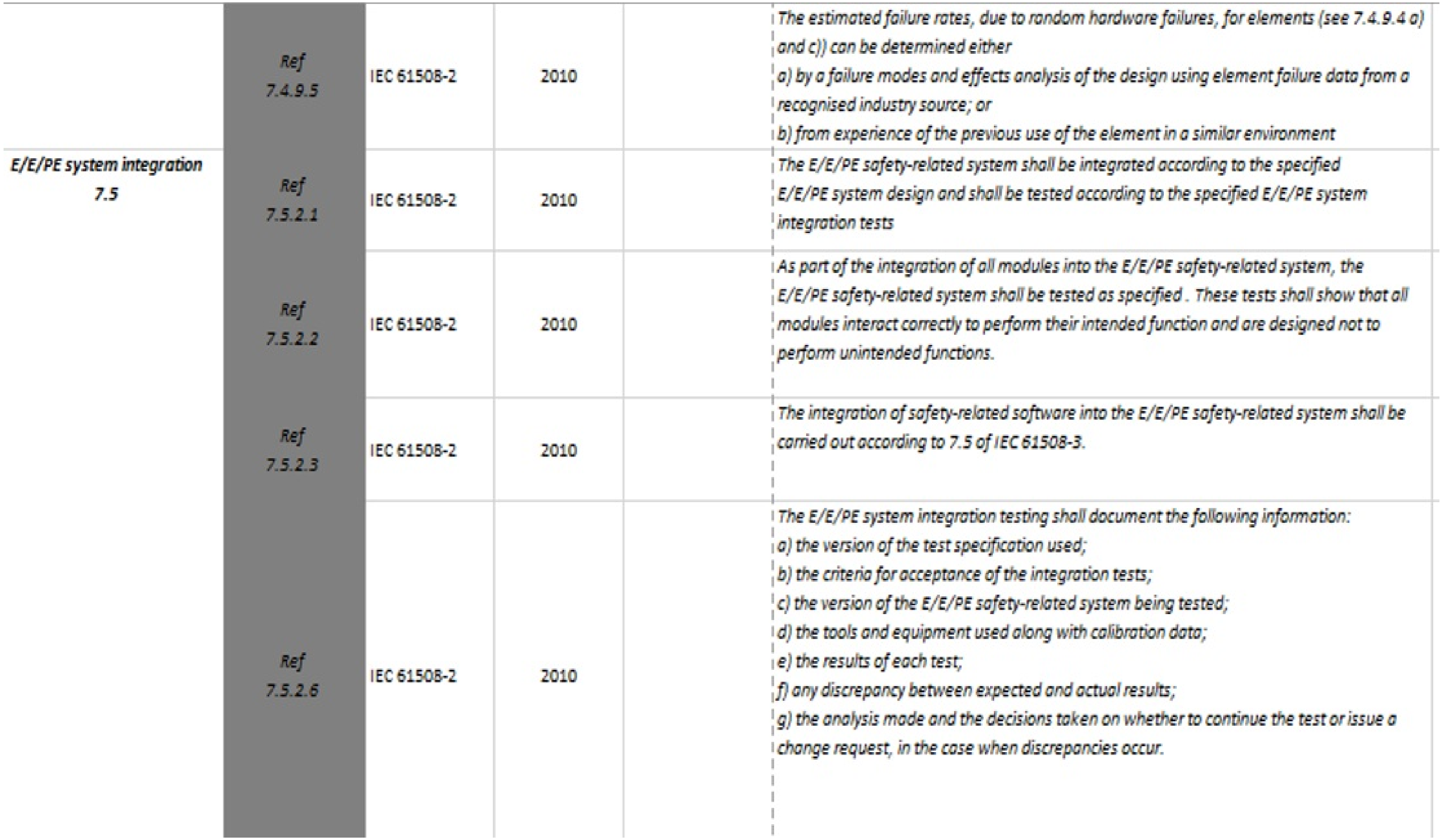
Requirements for system behaviour on detection of a fault ***7.4.8***	Ref 7.4.8.1	IEC 61508-2	2010		*The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem that has a hardware fault tolerance of more than 0 shall result in either:* *a) a specified action to achieve or maintain a safe state (see Note); or* *b) the isolation of the faulty part of the subsystem to allow continued safe operation of the EUC whilst the faulty part is repaired. If the repair is not completed within the mean repair time (MRT), see 3.6.22 of IEC 61508-4, assumed in the calculation of the probability of random hardware failure (see 7.4.5.2), then a specified action shall take place to achieve or maintain a safe state (see Note).*
	Ref 7.4.8.2	IEC 61508-2	2010		*The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem having a hardware fault tolerance of 0 shall, in the case that the subsystem is used only by safety function(s) operating in the low demand mode, result in either:* *a) a specified action to achieve or maintain a safe state; or* *b) the repair of the faulty subsystem within the mean repair time (MRT), see 3.6.22 of IEC 61508-4,assumed in the calculation of the probability of random hardware failure (see 7.4.5.2). During this time the continuing safety of the EUC shall be ensured by additionalmeasures and constraints. The safety integrity provided by these measures and constraints shall be at least equal to the safety integrity provided by the E/E/PE safetyrelated system in the absence of any faults. The additional measures and constraints shall be specified in the E/E/PE system operation and maintenance procedures.*
	Ref 7.4.8.3	IEC 61508-2	2010		*The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem having a hardware fault tolerance of 0 shall, in the case of a subsystem that is implementing any safety function(s) operating in the high demand or the continuous mode, result in a specified action to achieve or maintain a safe state (see Note).*



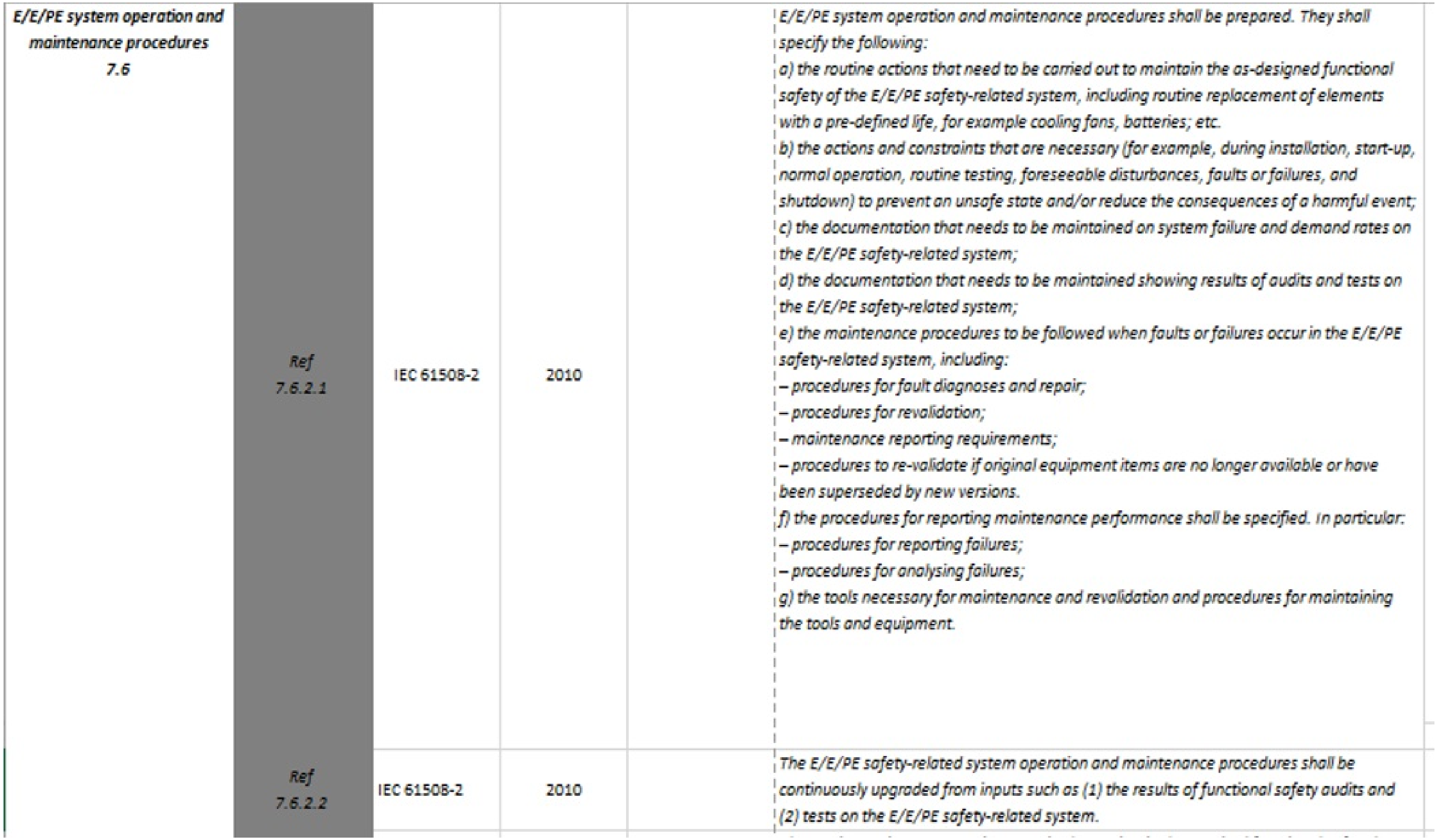
Requirements for E/E/PE system implementation	Ref 7.4.9.1	IEC 61508-2	2010		*The E/E/PE safety-related system shall be implemented according to the E/E/PE system design requirements specification (7.2.3).*
	Ref 7.4.9.2	IEC 61508-2	2010		*All subsystems and their elements that are used by one or more safety functions shall be identified and documented as safety-related subsystems and elements.*
	Ref 7.4.9.3	IEC 61508-2	2010		*The following information shall be available for each safety-related subsystem and each element as appropriate:* *a) a functional specification of the subsystem and its elements as appropriate;* *b) any instructions or constraints relating to the application of the subsystem and itselements, that should be observed in order to prevent systematic failures of the subsystem;* *c) the systematic capability of each element;* *d) identification of the hardware and/or software configuration of the element to enable configuration management of the E/E/PE safety-related system in accordance with 6.2.1 of IEC 61508-1;* *e) documentary evidence that the subsystem and its elements have been verified as meetingtheir specified functional requirements and systematic capabilities in accordance with the E/E/PE design requirements specification (see 7.2.3).*



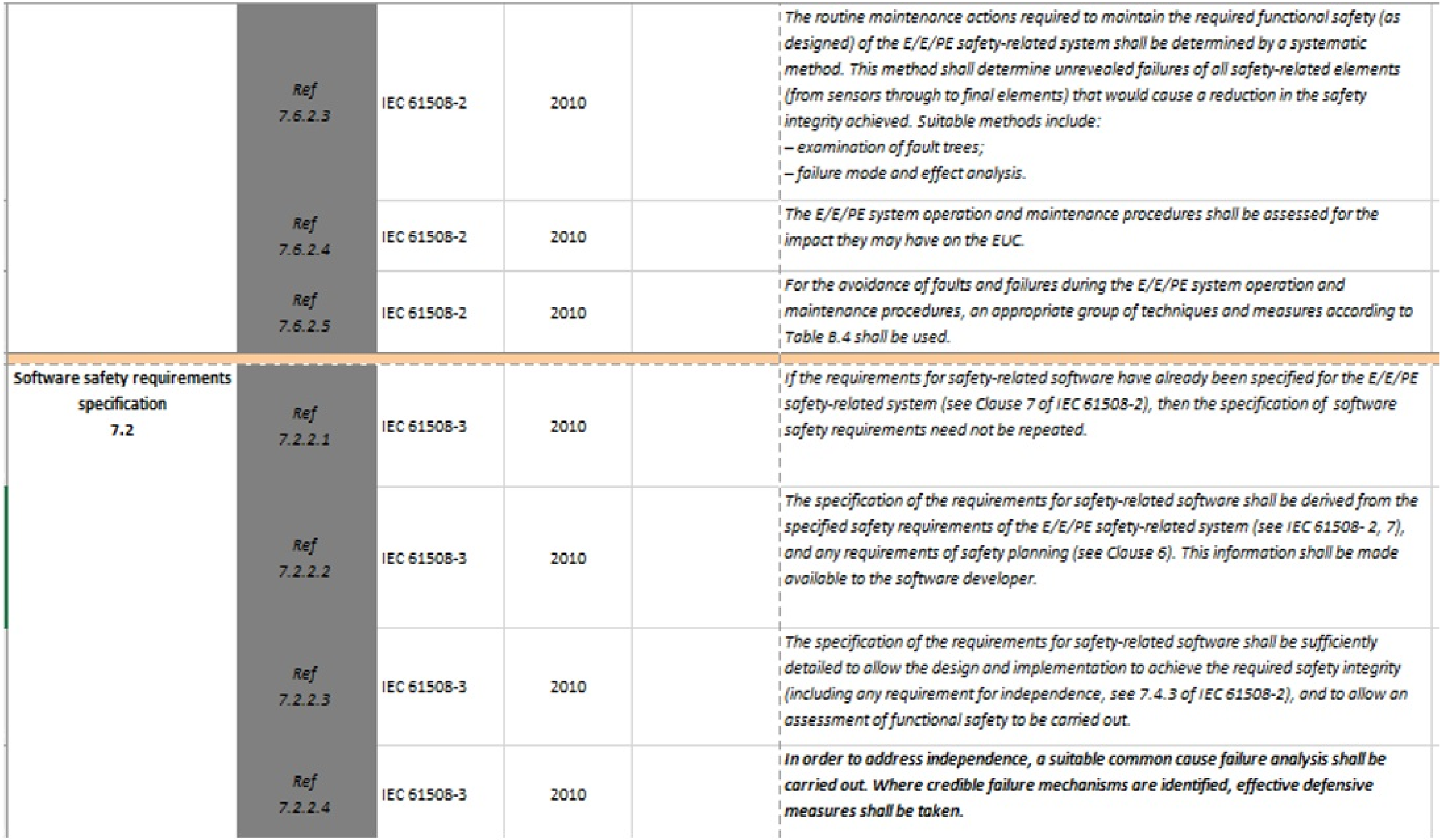
	Ref 7.4.9.4	IEC 61508-2	2010		*The following information shall be available for each safety-related element that is liable to random hardware failure (see also 7.4.9.3 and 7.4.9.5):* *a) the failure modes of the element (in terms of the behaviour of its outputs), due to random hardware failures, that result in a failure of the safety function and that are not detected by diagnostic tests internal to the element or are not detectable by diagnostics external to the element;* *b) for every failure mode in a), an estimated failure rate with respect to specified operating conditions;* *c) the failure modes of the element (in terms of the behaviour of its outputs), due to random hardware failures, that result in a failure of the safety function and that are detected by diagnostic tests internal to the element or are detectable by diagnostics external to the element (see 7.4.9.5);* *d) for every failure mode in c), an estimated failure rate with respect to specified operating conditions;* *e) any limits on the environment of the element that should be observed in order to maintain the validity of the estimated rates of failure due to random hardware failures;* *f) any limit on the lifetime of the element that should not be exceeded in order to maintain the validity of the estimated rates of failure due to random hardware failures;* *g) any periodic proof test and/or maintenance requirements;* *h) for every failure mode in c) that is detected by diagnostics internal to the element, the diagnostic coverage derived according to Annex C (see Note 2);* *i) for every failure mode in c) that is detected by diagnostics internal to the element, the diagnostic test interval ;* *j) the failure rate of the diagnostics, due to random hardware failures;* *k) any additional information (for example repair times) that is necessary to allow the derivation of the mean repair time (MRT), see 3.6.22 of IEC 61508-4,following detection of a fault by the diagnostics;* *l) all information that is necessary to enable the derivation of the safe failure fraction (SFF) of the element as applied in the E/E/PE safety-related system, determined according to Annex C, including the classification as type A or type B according to 7.4.4;* *m) the hardware fault tolerance of the element.*



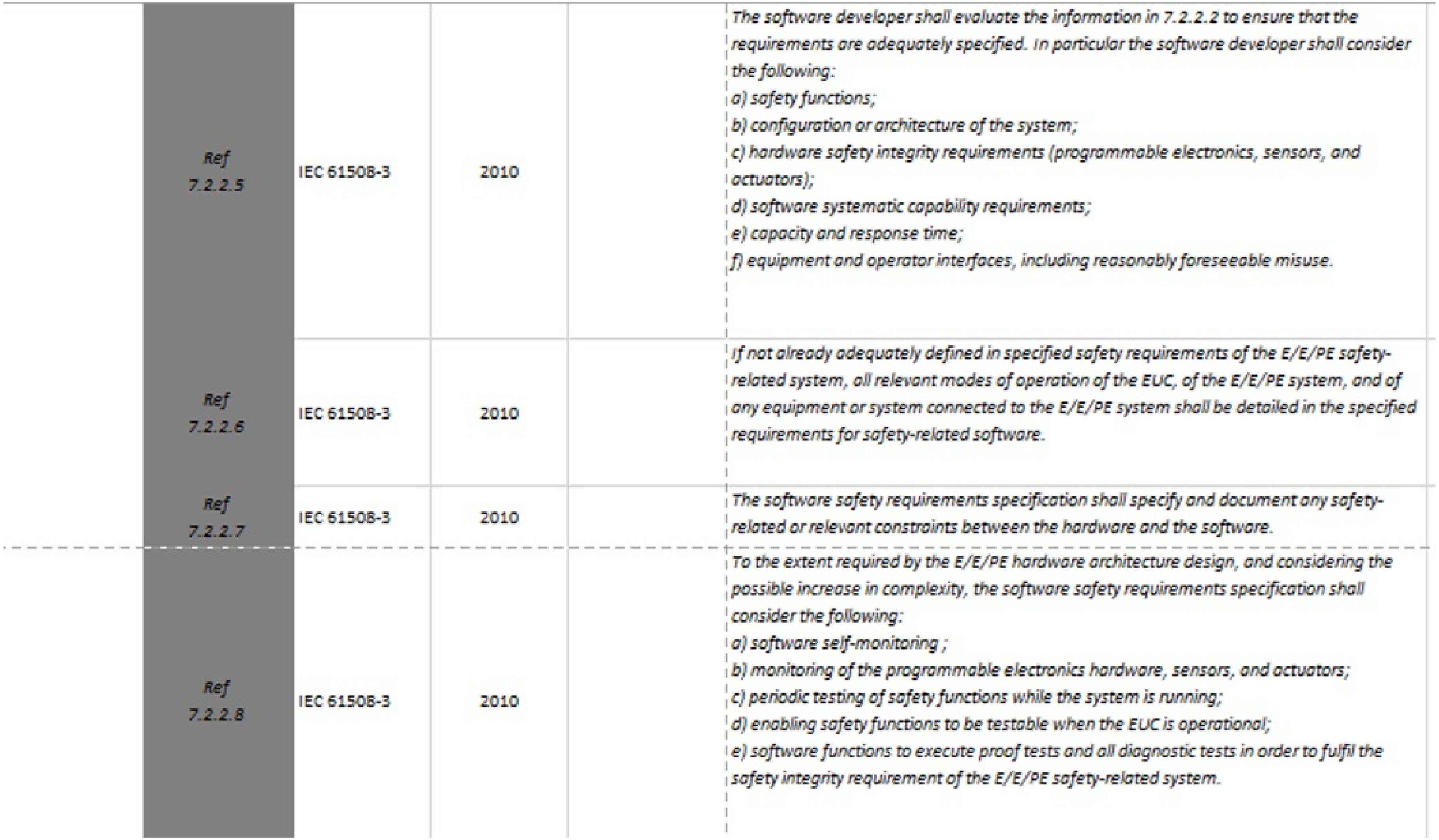
	Ref 7.4.9.5	IEC 61508-2	2010		The estimated failure rates, due to random hardware failures, for elements (see 7.4.9.4 a) and c)) can be determined either a) by a failure modes and effects analysis of the design using element failure data from a recognised industry source; or b) from experience of the previous use of the element in a similar environment
E/E/PE system integration **7.5**	Ref 7.5.2.1	IEC 61508-2	2010		The E/E/PE safety-related system shall be integrated according to the specified E/E/PE system design and shall be tested according to the specified E/E/PE system integration tests
	Ref 7.5.2.2	IEC 61508-2	2010		As part of the integration of all modules into the E/E/PE safety-related system, the E/E/PE safety-related system shall be tested as specified . These tests shall show that all modules interact correctly to perform their intended function and are designed not to perform unintended functions.
	Ref 7.5.2.3	IEC 61508-2	2010		The integration of safety-related software into the E/E/PE safety-related system shall be carried out according to 7.5 of IEC 61508-3.
	Ref 7.5.2.6	IEC 61508-2	2010		The E/E/PE system integration testing shall document the following information: a) the version of the test specification used; b) the criteria for acceptance of the integration tests; c) the version of the E/E/PE safety-related system being tested; d) the tools and equipment used along with calibration data; e) the results of each test; f) any discrepancy between expected and actual results; g) the analysis made and the decisions taken on whether to continue the test or issue a change request, in the case when discrepancies occur.



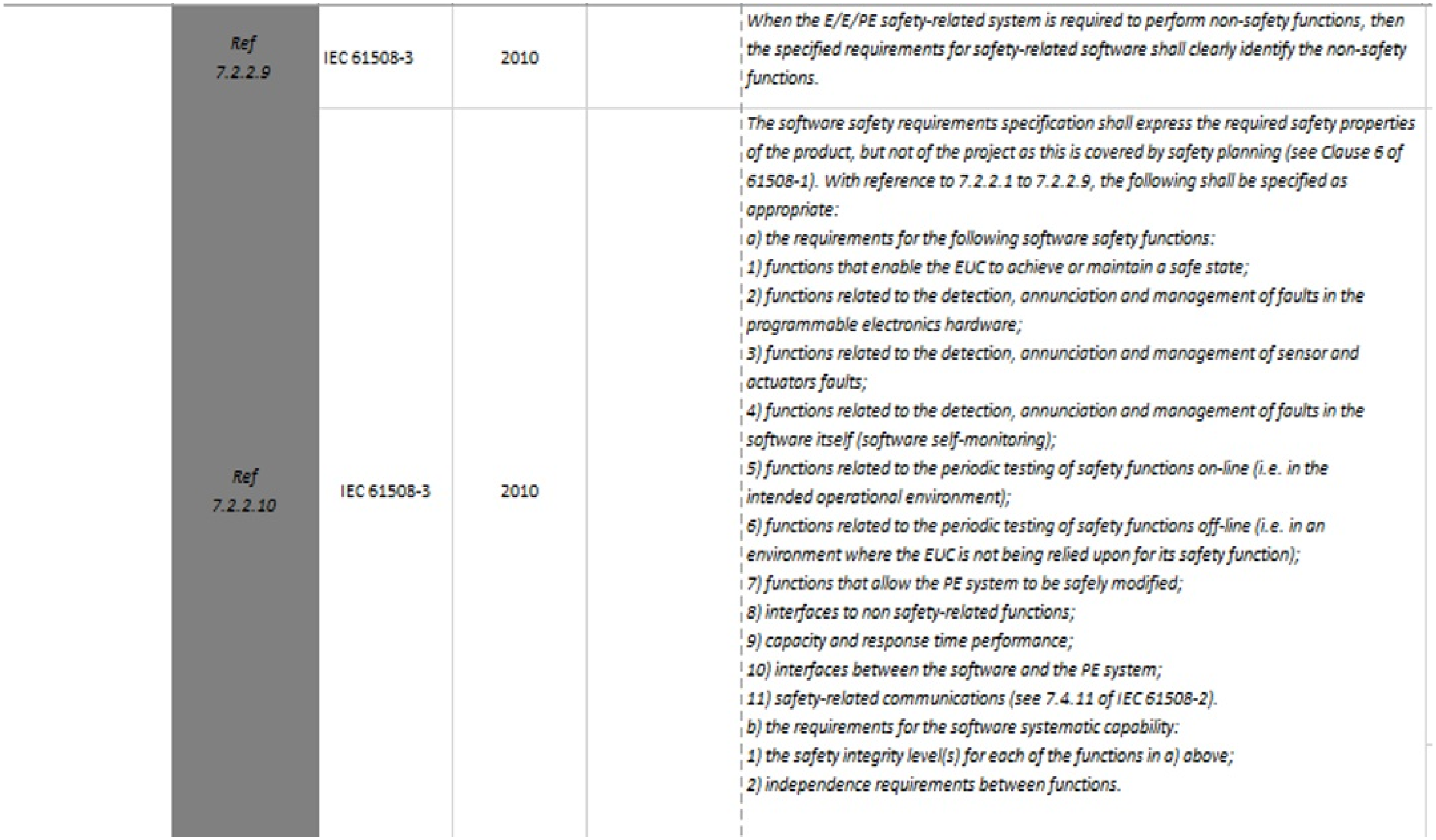
E/E/PE system operation and maintenance procedures 7.6	*Ref 7.6.2.1*	IEC 61508-2	2010		*E/E/PE system operation and maintenance procedures shall be prepared. They shall specify the following:* *a) the routine actions that need to be carried out to maintain the as-designed functional safety of the E/E/PE safety-related system, including routine replacement of elements with a pre-defined life, for example cooling fans, batteries; etc.* *b) the actions and constraints that are necessary (for example, during installation, start-up, normal operation, routine testing, foreseeable disturbances, faults or failures, and shutdown) to prevent an unsafe state and/or reduce the consequences of a harmful event;* *c) the documentation that needs to be maintained on system failure and demand rates on the E/E/PE safety-related system;* *d) the documentation that needs to be maintained showing results of audits and tests on the E/E/PE safety-related system;* *e) the maintenance procedures to be followed when faults or failures occur in the E/E/PE safety-related system, including:* *– procedures for fault diagnoses and repair;* *– procedures for revalidation;* *– maintenance reporting requirements;* *– procedures to re-validate if original equipment items are no longer available or have been superseded by new versions.* *f) the procedures for reporting maintenance performance shall be specified. In particular:* *– procedures for reporting failures;* *– procedures for analysing failures;* *g) the tools necessary for maintenance and revalidation and procedures for maintaining the tools and equipment.*
	Ref 7.6.2.2	IEC 61508-2	2010		*The E/E/PE safety-related system operation and maintenance procedures shall be continuously upgraded from inputs such as (1) the results of functional safety audits and (2) tests on the E/E/PE safety-related system.*



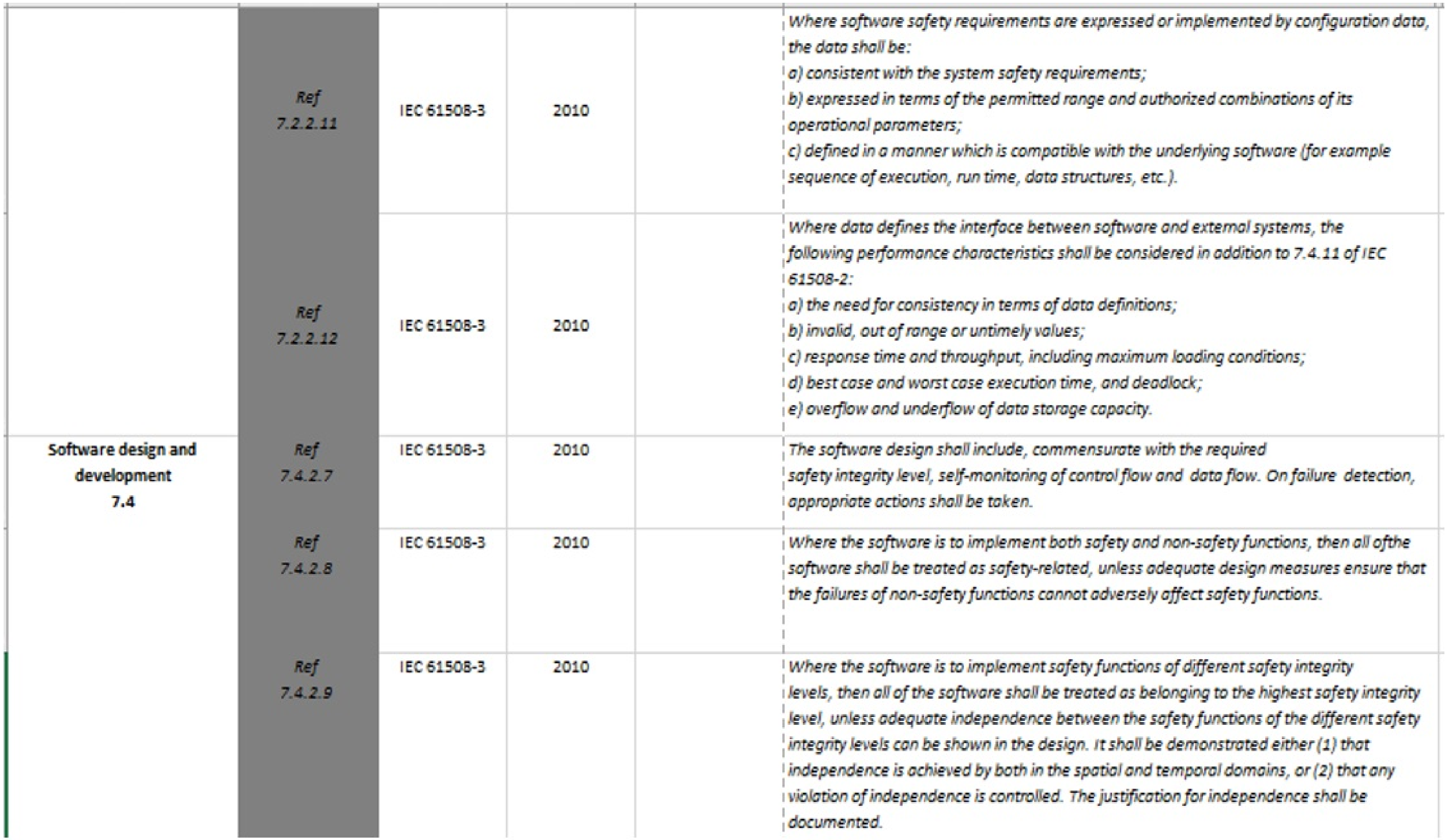
	Ref *7.6.2.3*	IEC 61508-2	2010		*The routine maintenance actions required to maintain the required functional safety (as designed) of the E/E/PE safety-related system shall be determined by a systematic method. This method shall determine unrevealed failures of all safety-related elements (from sensors through to final elements) that would cause a reduction in the safety integrity achieved. Suitable methods include:* *– examination of fault trees;* *– failure mode and effect analysis.*
	Ref *7.6.2.4*	IEC 61508-2	2010		*The E/E/PE system operation and maintenance procedures shall be assessed for the impact they may have on the EUC.*
	Ref *7.6.2.5*	IEC 61508-2	2010		*For the avoidance of faults and failures during the E/E/PE system operation and maintenance procedures, an appropriate group of techniques and measures according to Table B.4 shall be used.*
Software safety requirements specification **7.2**	*Ref* *7.2.2.1*	IEC 61508-3	2010		*If the requirements for safety-related software have already been specified for the E/E/PE safety-related system (see Clause 7 of IEC 61508-2), then the specification of software safety requirements need not be repeated.*
	Ref *7.2.2.2*	IEC 61508-3	2010		*The specification of the requirements for safety-related software shall be derived from the specified safety requirements of the E/E/PE safety-related system (see IEC 61508- 2, 7), and any requirements of safety planning (see Clause 6). This information shall be made available to the software developer.*
	Ref *7.2.2.3*	IEC 61508-3	2010		*The specification of the requirements for safety-related software shall be sufficiently detailed to allow the design and implementation to achieve the required safety integrity (including any requirement for independence, see 7.4.3 of IEC 61508-2), and to allow an assessment of functional safety to be carried out.*
	Ref *7.2.2.4*	IEC 61508-3	2010		***In order to address independence, a suitable common cause failure analysis shall be carried out. Where credible failure mechanisms are identified, effective defensive measures shall be taken.***



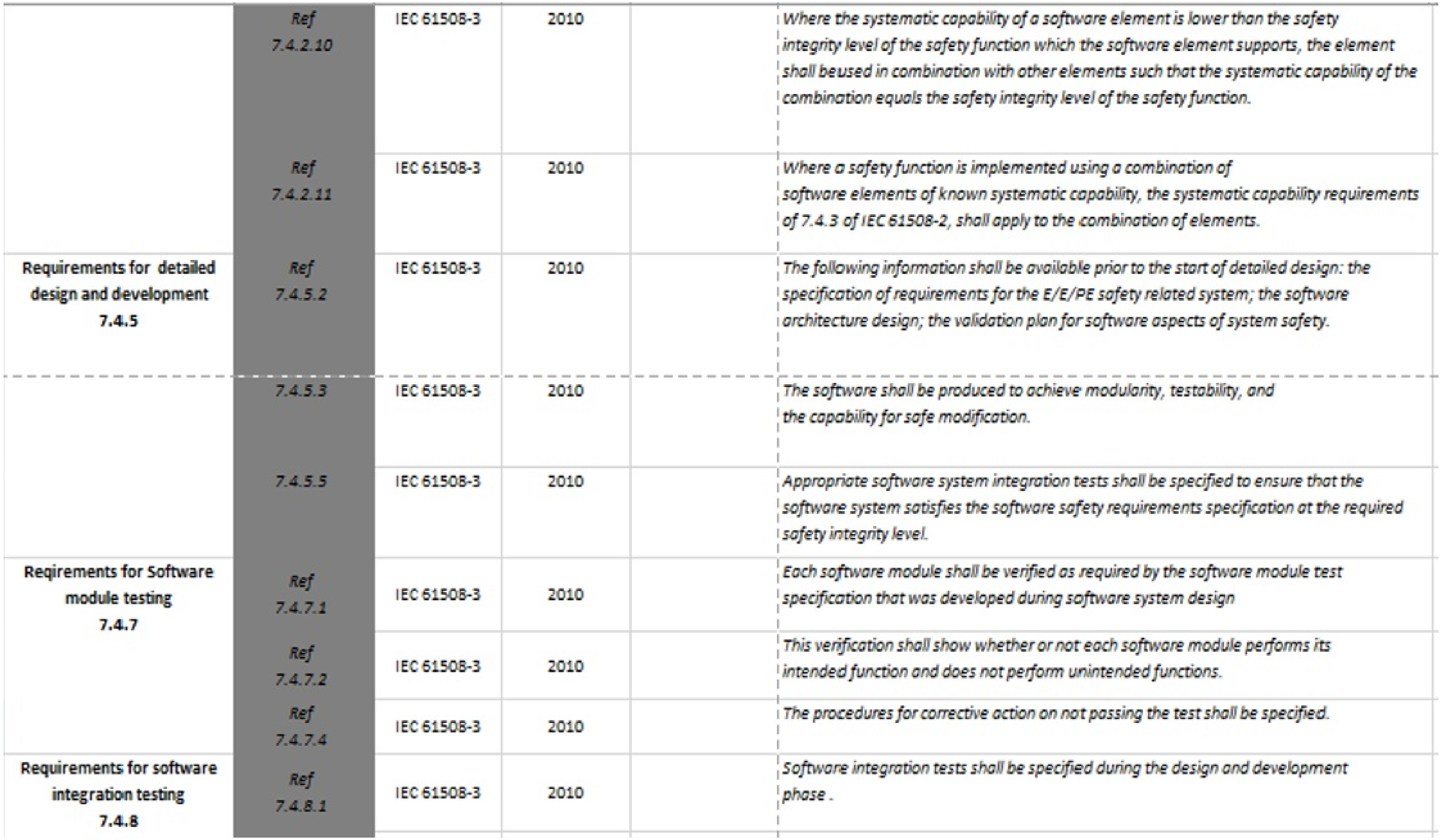
	Ref *7.2.2.5*	IEC 61508-3	2010		*The software developer shall evaluate the information in 7.2.2.2 to ensure that the requirements are adequately specified. In particular the software developer shall consider the following:* *a) safety functions;* *b) configuration or architecture of the system;* *c) hardware safety integrity requirements (programmable electronics, sensors, and actuators);* *d) software systematic capability requirements;* *e) capacity and response time;* *f) equipment and operator interfaces, including reasonably foreseeable misuse.*
	Ref *7.2.2.6*	IEC 61508-3	2010		*If not already adequately defined in specified safety requirements of the E/E/PE safety-related system, all relevant modes of operation of the EUC, of the E/E/PE system, and of any equipment or system connected to the E/E/PE system shall be detailed in the specified requirements for safety-related software.*
	Ref *7.2.2.7*	IEC 61508-3	2010		*The software safety requirements specification shall specify and document any safety-related or relevant constraints between the hardware and the software.*
	Ref *7.2.2.8*	IEC 61508-3	2010		*To the extent required by the E/E/PE hardware architecture design, and considering the possible increase in complexity, the software safety requirements specification shall consider the following:* *a) software self-monitoring ;* *b) monitoring of the programmable electronics hardware, sensors, and actuators;* *c) periodic testing of safety functions while the system is running;* *d) enabling safety functions to be testable when the EUC is operational;* *e) software functions to execute proof tests and all diagnostic tests in order to fulfil the safety integrity requirement of the E/E/PE safety-related system.*



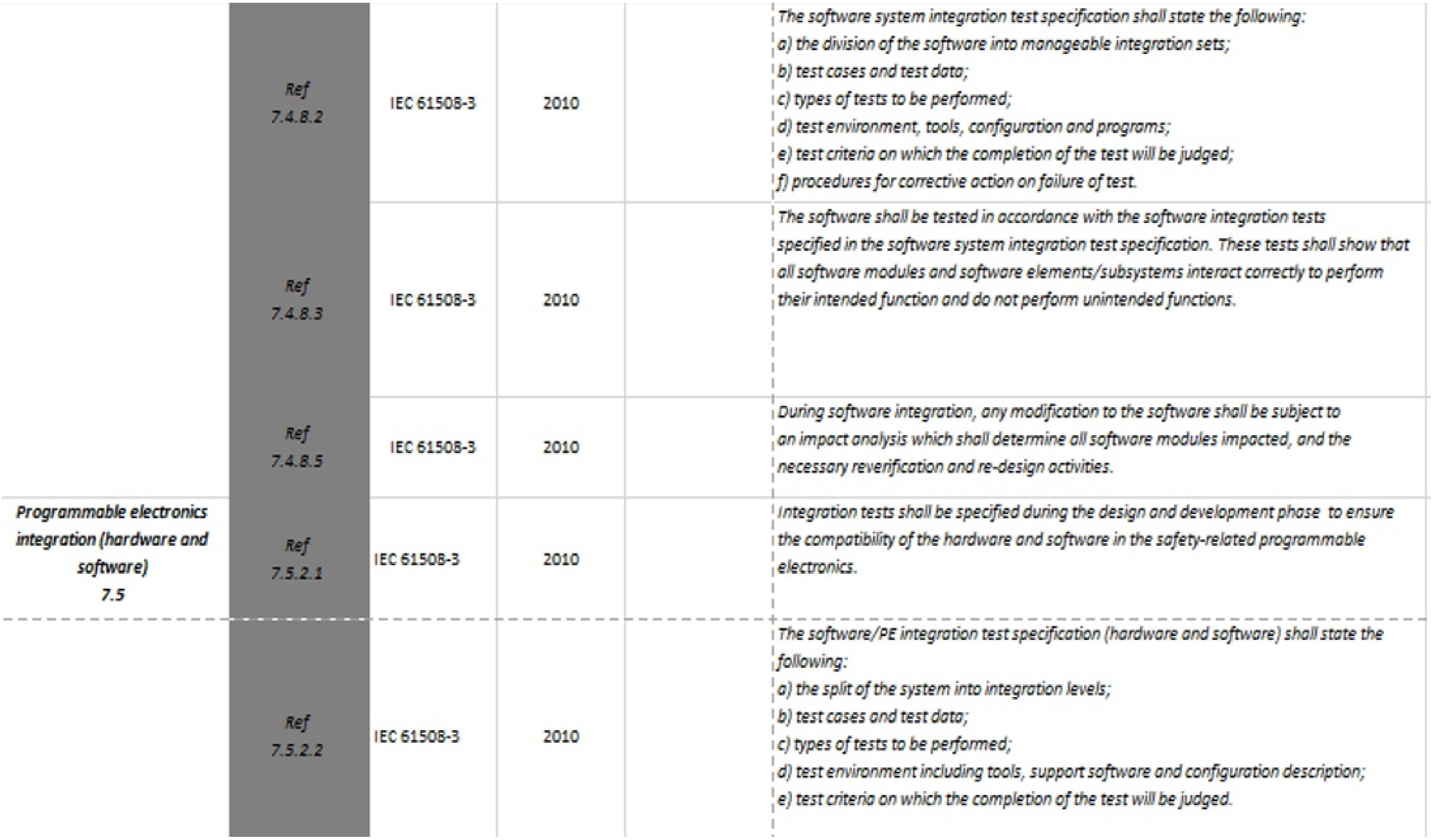
Ref *7.2.2.9*	IEC 61508-3	2010		*When the E/E/PE safety-related system is required to perform non-safety functions, then the specified requirements for safety-related software shall clearly identify the non-safety functions.*
Ref *7.2.2.10*	IEC 61508-3	2010		*The software safety requirements specification shall express the required safety properties of the product, but not of the project as this is covered by safety planning (see Clause 6 of 61508-1). With reference to 7.2.2.1 to 7.2.2.9, the following shall be specified as appropriate:* *a) the requirements for the following software safety functions:* *1) functions that enable the EUC to achieve or maintain a safe state;* *2) functions related to the detection, annunciation and management of faults in the programmable electronics hardware;* *3) functions related to the detection, annunciation and management of sensor and actuators faults;* *4) functions related to the detection, annunciation and management of faults in the software itself (software self-monitoring);* *5) functions related to the periodic testing of safety functions on-line (i.e. in the intended operational environment);* *6) functions related to the periodic testing of safety functions off-line (i.e. in an environment where the EUC is not being relied upon for its safety function);* *7) functions that allow the PE system to be safely modified;* *8) interfaces to non safety-related functions;* *9) capacity and response time performance;* *10) interfaces between the software and the PE system;* *11) safety-related communications (see 7.4.11 of IEC 61508-2).* *b) the requirements for the software systematic capability:* *1) the safety integrity level(s) for each of the functions in a) above;* *2) independence requirements between functions.*



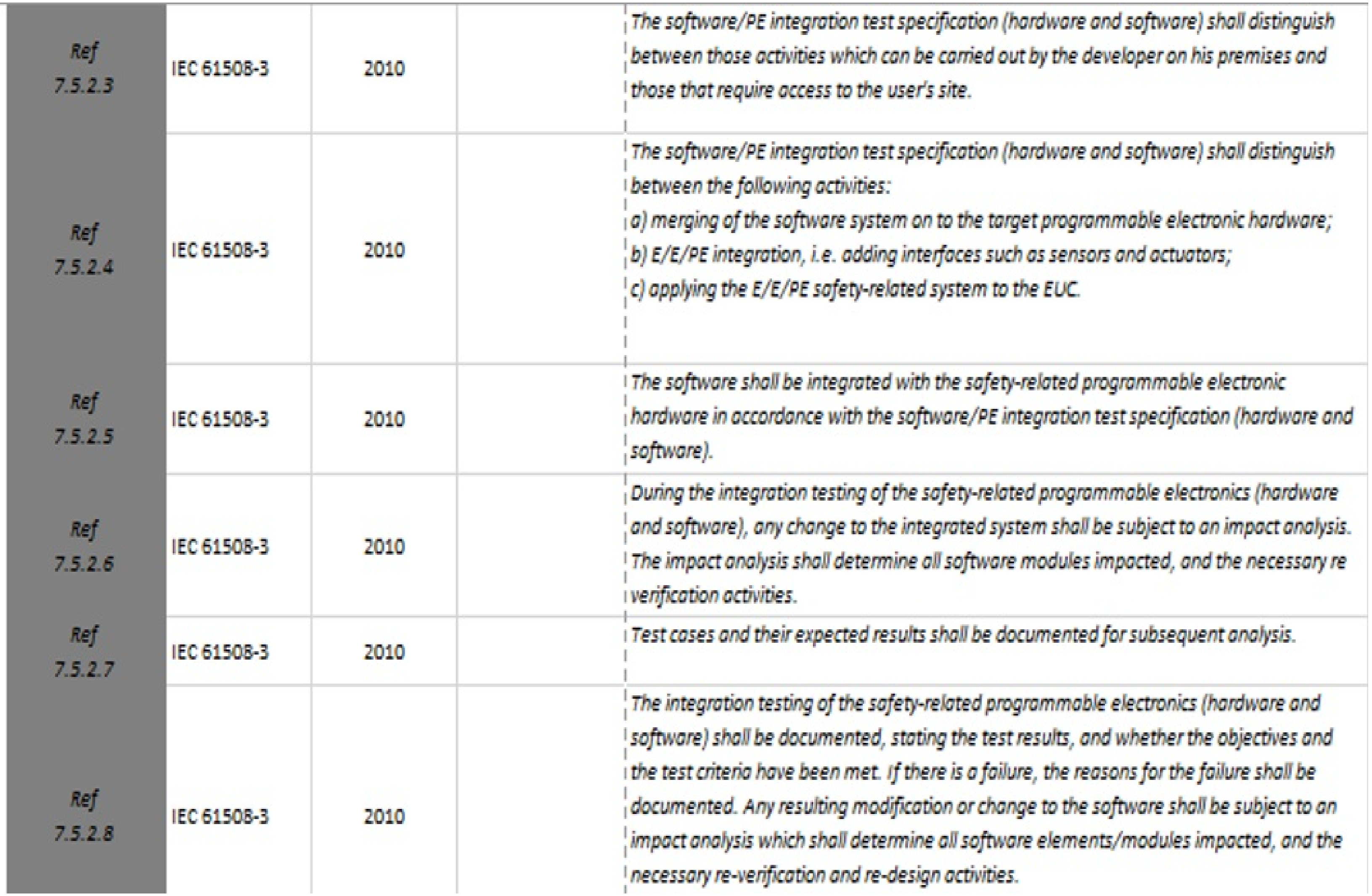
	Ref *7.2.2.11*	IEC 61508-3	2010		*Where software safety requirements are expressed or implemented by configuration data, the data shall be:* *a) consistent with the system safety requirements;* *b) expressed in terms of the permitted range and authorized combinations of its operational parameters;* *c) defined in a manner which is compatible with the underlying software (for example sequence of execution, run time, data structures, etc.).*
	Ref *7.2.2.12*	IEC 61508-3	2010		*Where data defines the interface between software and external systems, the following performance characteristics shall be considered in addition to 7.4.11 of IEC 61508-2:* *a) the need for consistency in terms of data definitions;* *b) invalid, out of range or untimely values;* *c) response time and throughput, including maximum loading conditions;* *d) best case and worst case execution time, and deadlock;* *e) overflow and underflow of data storage capacity.*
Software design and development **7.4**	*Ref* *7.4.2.7*	IEC 61508-3	2010		*The software design shall include, commensurate with the required safety integrity level, self-monitoring of control flow and data flow. On failure detection, appropriate actions shall be taken.*
	Ref *7.4.2.8*	IEC 61508-3	2010		*Where the software is to implement both safety and non-safety functions, then all ofthe software shall be treated as safety-related, unless adequate design measures ensure that the failures of non-safety functions cannot adversely affect safety functions.*
	Ref *7.4.2.9*	IEC 61508-3	2010		*Where the software is to implement safety functions of different safety integrity levels, then all of the software shall be treated as belonging to the highest safety integrity level, unless adequate independence between the safety functions of the different safety integrity levels can be shown in the design. It shall be demonstrated either (1) that independence is achieved by both in the spatial and temporal domains, or (2) that any violation of independence is controlled. The justification for independence shall be documented.*



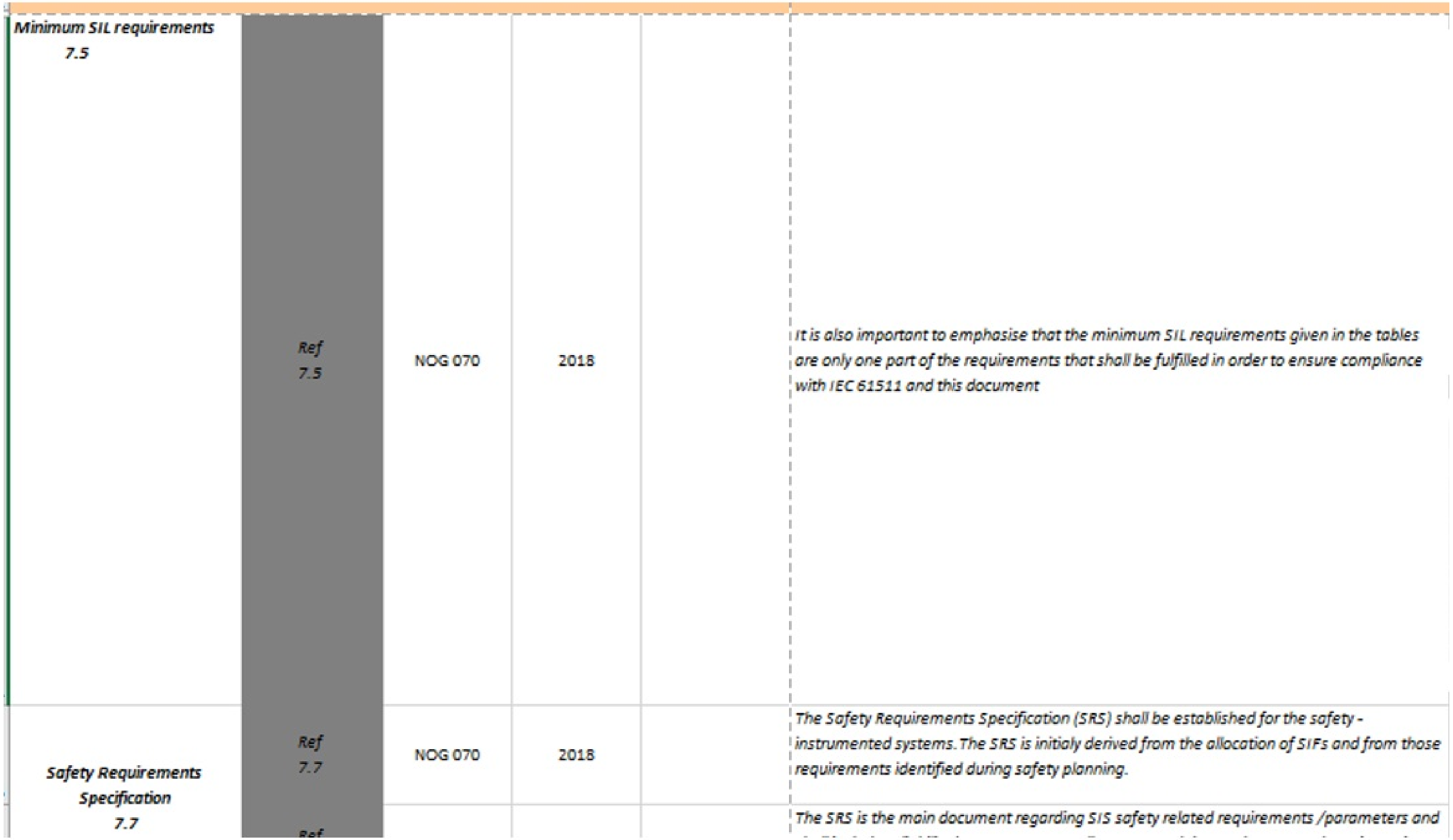
	Ref *7.4.2.10*	IEC 61508-3	2010		*Where the systematic capability of a software element is lower than the safety integrity level of the safety function which the software element supports, the element shall beused in combination with other elements such that the systematic capability of the combination equals the safety integrity level of the safety function.*
	Ref *7.4.2.11*	IEC 61508-3	2010		*Where a safety function is implemented using a combination of software elements of known systematic capability, the systematic capability requirements of 7.4.3 of IEC 61508-2, shall apply to the combination of elements.*
Requirements for detailed design and development 7.4.5	*Ref* *7.4.5.2*	IEC 61508-3	2010		*The following information shall be available prior to the start of detailed design: the specification of requirements for the E/E/PE safety related system; the software architecture design; the validation plan for software aspects of system safety.*
	7.4.5.3	IEC 61508-3	2010		*The software shall be produced to achieve modularity, testability, and the capability for safe modification.*
	7.4.5.5	IEC 61508-3	2010		*Appropriate software system integration tests shall be specified to ensure that the software system satisfies the software safety requirements specification at the required safety integrity level.*
Reqirements for Software module testing 7.4.7	*Ref* *7.4.7.1*	IEC 61508-3	2010		*Each software module shall be verified as required by the software module test specification that was developed during software system design*
	Ref *7.4.7.2*	IEC 61508-3	2010		*This verification shall show whether or not each software module performs its intended function and does not perform unintended functions.*
	Ref *7.4.7.4*	IEC 61508-3	2010		*The procedures for corrective action on not passing the test shall be specified.*
Requirements for software integration testing 7.4.8	*Ref* *7.4.8.1*	IEC 61508-3	2010		*Software integration tests shall be specified during the design and development phase .*



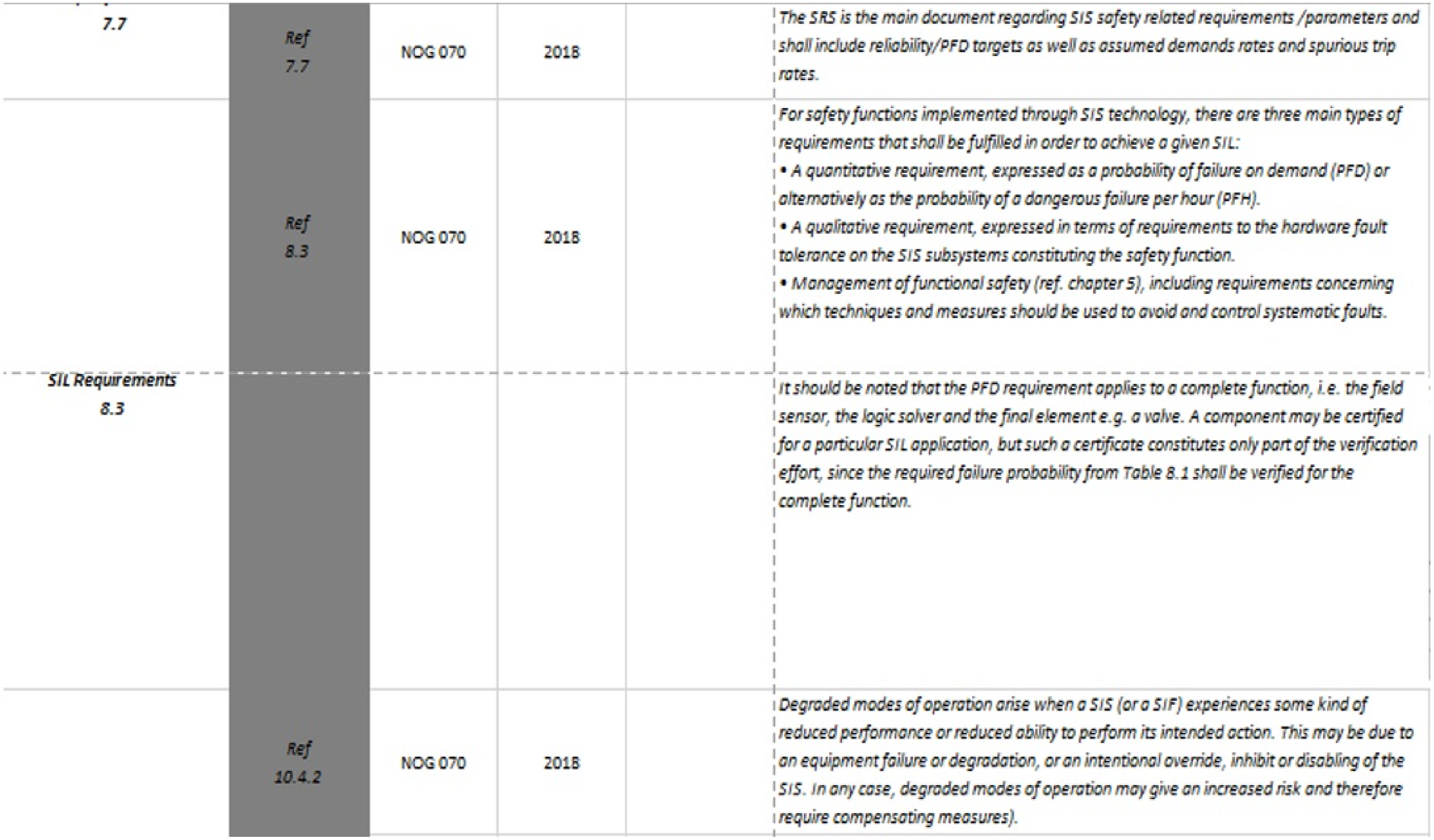
	Ref *7.4.8.2*	IEC 61508-3	2010		*The software system integration test specification shall state the following:* *a) the division of the software into manageable integration sets;* *b) test cases and test data;* *c) types of tests to be performed;* *d) test environment, tools, configuration and programs;* *e) test criteria on which the completion of the test will be judged;* *f) procedures for corrective action on failure of test.*
	Ref *7.4.8.3*	IEC 61508-3	2010		*The software shall be tested in accordance with the software integration tests specified in the software system integration test specification. These tests shall show that all software modules and software elements/subsystems interact correctly to perform their intended function and do not perform unintended functions.*
	Ref *7.4.8.5*	IEC 61508-3	2010		*During software integration, any modification to the software shall be subject to an impact analysis which shall determine all software modules impacted, and the necessary reverification and re-design activities.*
Programmable electronics integration (hardware and software) ***7.5***	*Ref* *7.5.2.1*	IEC 61508-3	2010		*Integration tests shall be specified during the design and development phase to ensure the compatibility of the hardware and software in the safety-related programmable electronics.*
	Ref *7.5.2.2*	IEC 61508-3	2010		*The software/PE integration test specification (hardware and software) shall state the following:* *a) the split of the system into integration levels;* *b) test cases and test data;* *c) types of tests to be performed;* *d) test environment including tools, support software and configuration description;* *e) test criteria on which the completion of the test will be judged.*



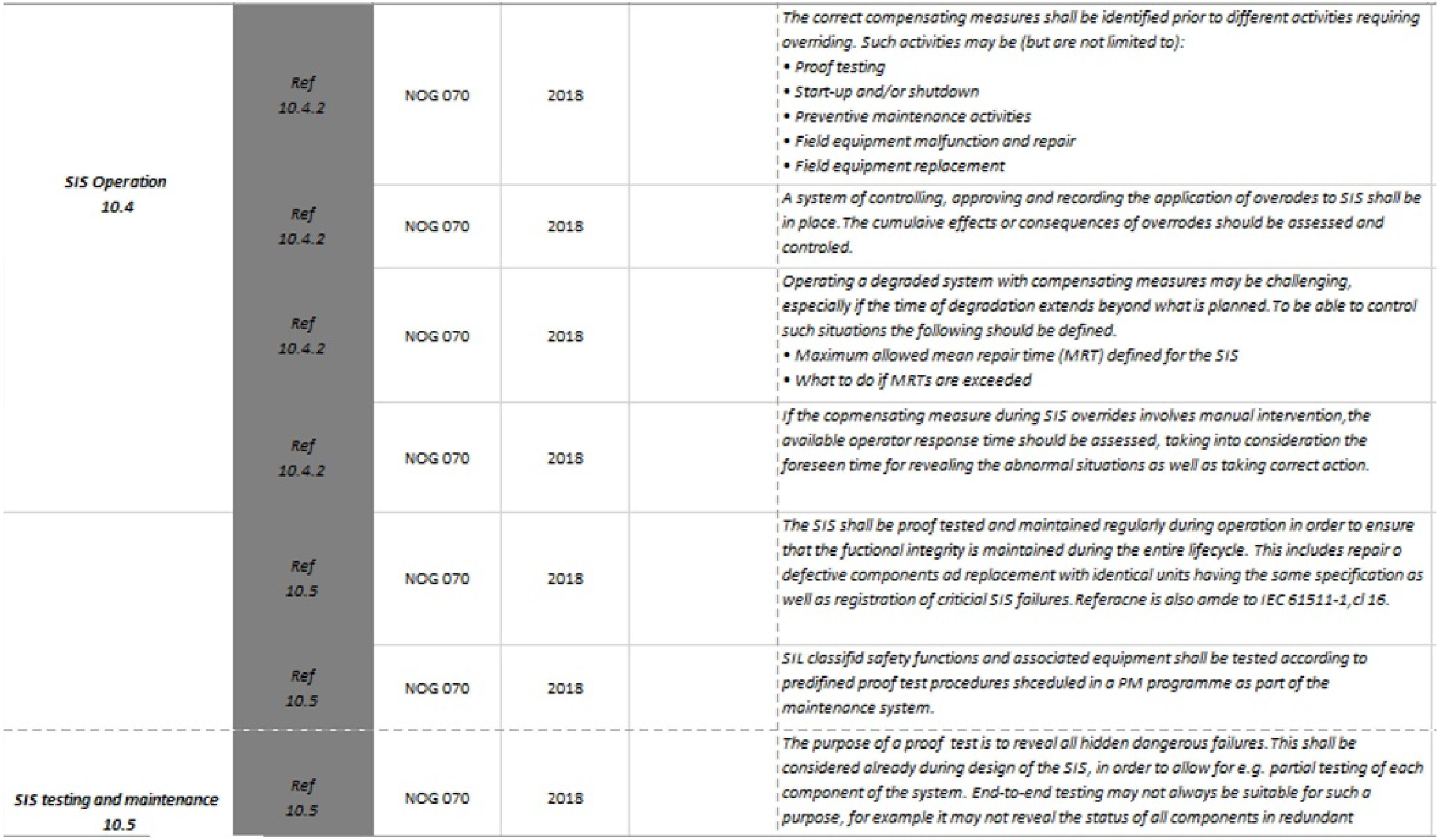
Ref 7.5.2.3	IEC 61508-3	2010		*The software/PE integration test specification (hardware and software) shall distinguish between those activities which can be carried out by the developer on his premises and those that require access to the user's site.*
Ref 7.5.2.4	IEC 61508-3	2010		*The software/PE integration test specification (hardware and software) shall distinguish between the following activities:* *a) merging of the software system on to the target programmable electronic hardware;* *b) E/E/PE integration, i.e. adding interfaces such as sensors and actuators;* *c) applying the E/E/PE safety-related system to the EUC.*
Ref 7.5.2.5	IEC 61508-3	2010		*The software shall be integrated with the safety-related programmable electronic hardware in accordance with the software/PE integration test specification (hardware and software).*
Ref 7.5.2.6	IEC 61508-3	2010		*During the integration testing of the safety-related programmable electronics (hardware and software), any change to the integrated system shall be subject to an impact analysis. The impact analysis shall determine all software modules impacted, and the necessary re verification activities.*
Ref 7.5.2.7	IEC 61508-3	2010		*Test cases and their expected results shall be documented for subsequent analysis.*
Ref 7.5.2.8	IEC 61508-3	2010		*The integration testing of the safety-related programmable electronics (hardware and software) shall be documented, stating the test results, and whether the objectives and the test criteria have been met. If there is a failure, the reasons for the failure shall be documented. Any resulting modification or change to the software shall be subject to an impact analysis which shall determine all software elements/modules impacted, and the necessary re-verification and re-design activities.*



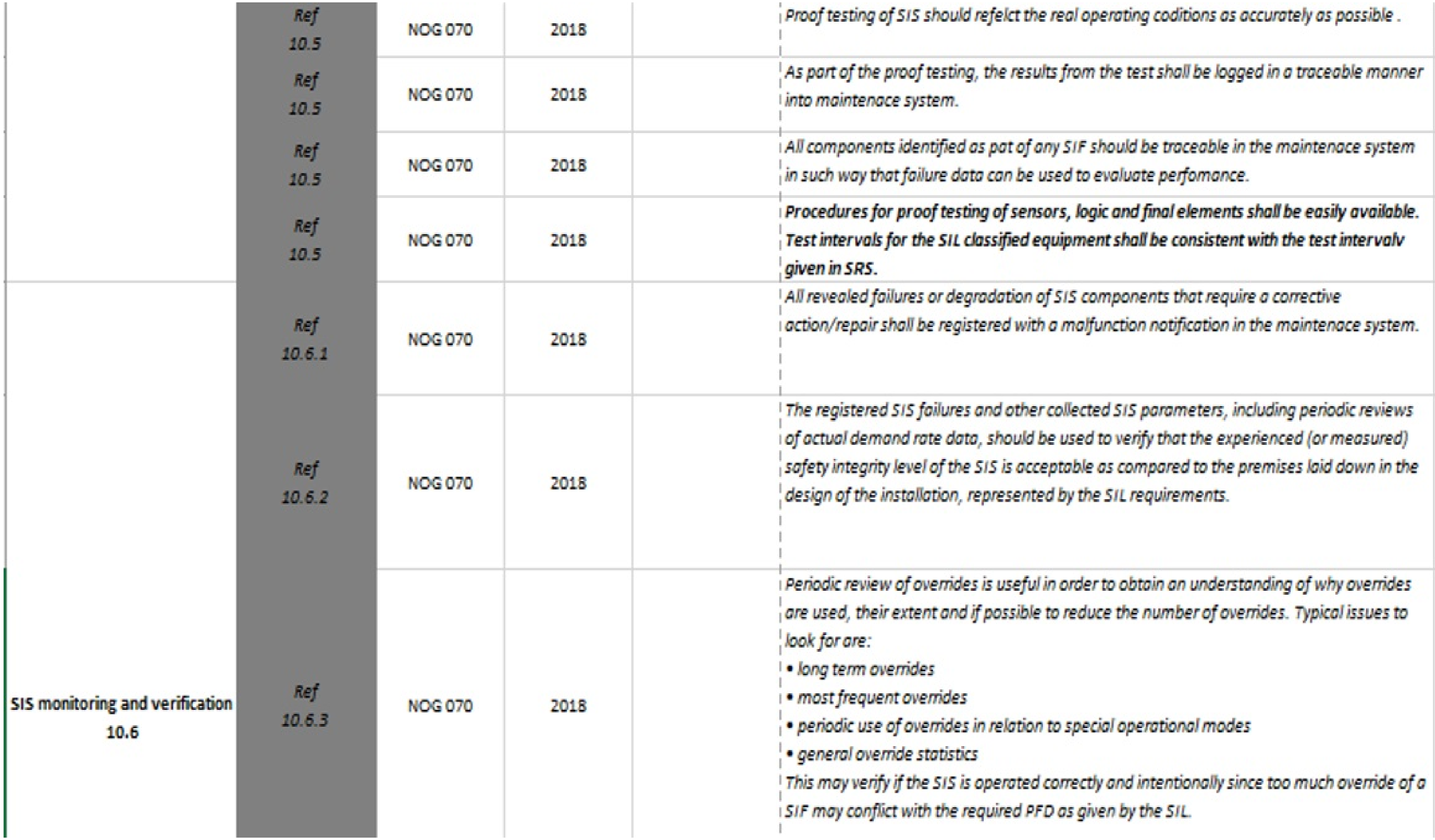
Minimum SIL requirements 7.5	Ref 7.5	NOG 070	2018		It is also important to emphasise that the minimum SIL requirements given in the tables are only one part of the requirements that shall be fulfilled in order to ensure compliance with IEC 61511 and this document
Safety Requirements Specification 7.7	Ref 7.7	NOG 070	2018		The Safety Requirements Specification (SRS) shall be established for the safety - instrumented systems. The SRS is initialy derived from the allocation of SIFs and from those requirements identified during safety planning.
	Ref				The SRS is the main document regarding SIS safety related requirements /parameters and



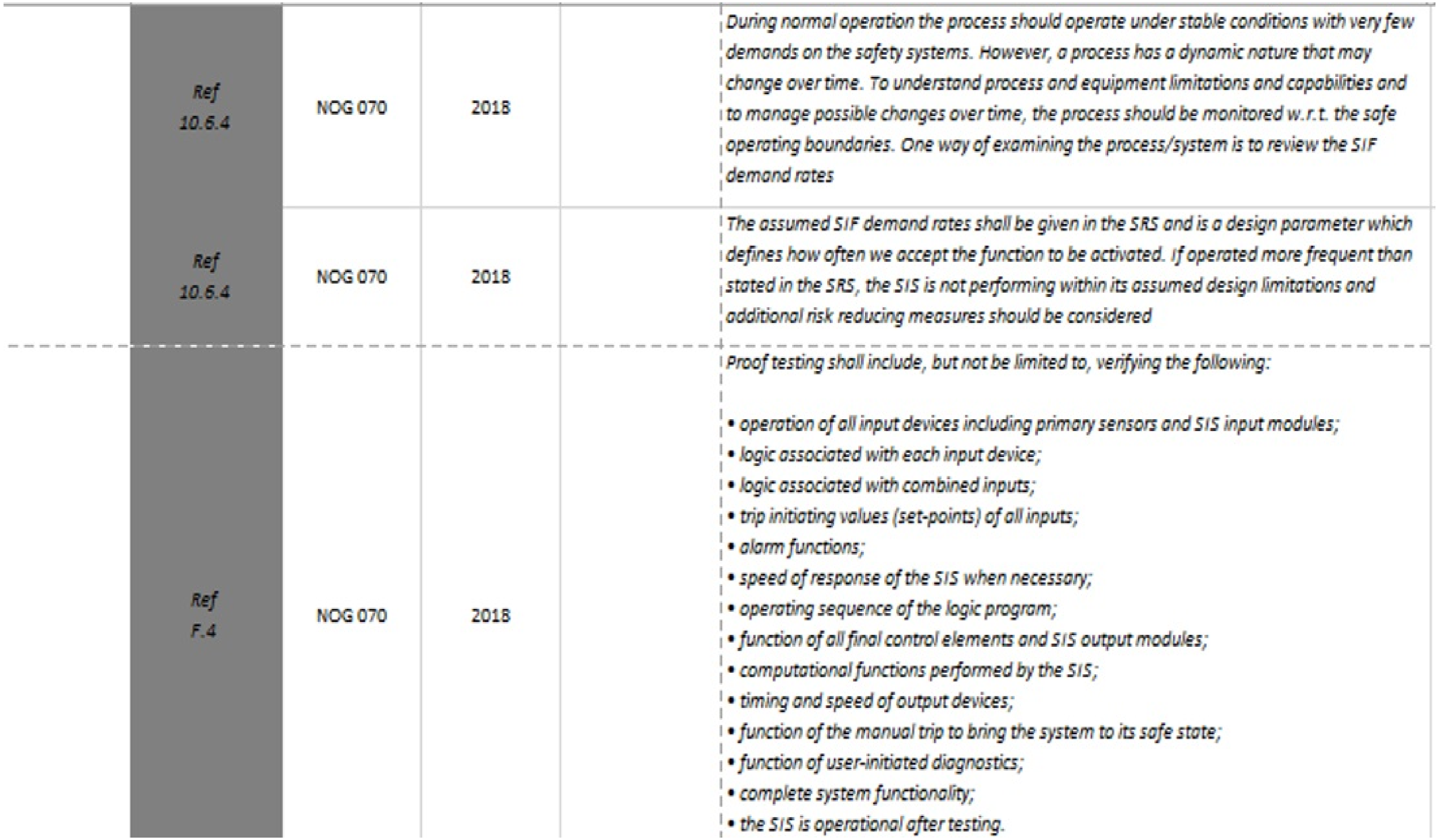
7.7	*Ref* *7.7*	NOG 070	2018		*The SRS is the main document regarding SIS safety related requirements /parameters and shall include reliability/PFD targets as well as assumed demands rates and spurious trip rates.*
	Ref *8.3*	NOG 070	2018		*For safety functions implemented through SIS technology, there are three main types of requirements that shall be fulfilled in order to achieve a given SIL:* *• A quantitative requirement, expressed as a probability of failure on demand (PFD) or alternatively as the probability of a dangerous failure per hour (PFH).* *• A qualitative requirement, expressed in terms of requirements to the hardware fault tolerance on the SIS subsystems constituting the safety function.* *• Management of functional safety (ref. chapter 5), including requirements concerning which techniques and measures should be used to avoid and control systematic faults.*
SIL Requirements *8.3*					*It should be noted that the PFD requirement applies to a complete function, i.e. the field sensor, the logic solver and the final element e.g. a valve. A component may be certified for a particular SIL application, but such a certificate constitutes only part of the verification effort, since the required failure probability from Table 8.1 shall be verified for the complete function.*
	Ref *10.4.2*	NOG 070	2018		*Degraded modes of operation arise when a SIS (or a SIF) experiences some kind of reduced performance or reduced ability to perform its intended action. This may be due to an equipment failure or degradation, or an intentional override, inhibit or disabling of the SIS. In any case, degraded modes of operation may give an increased risk and therefore require compensating measures).*



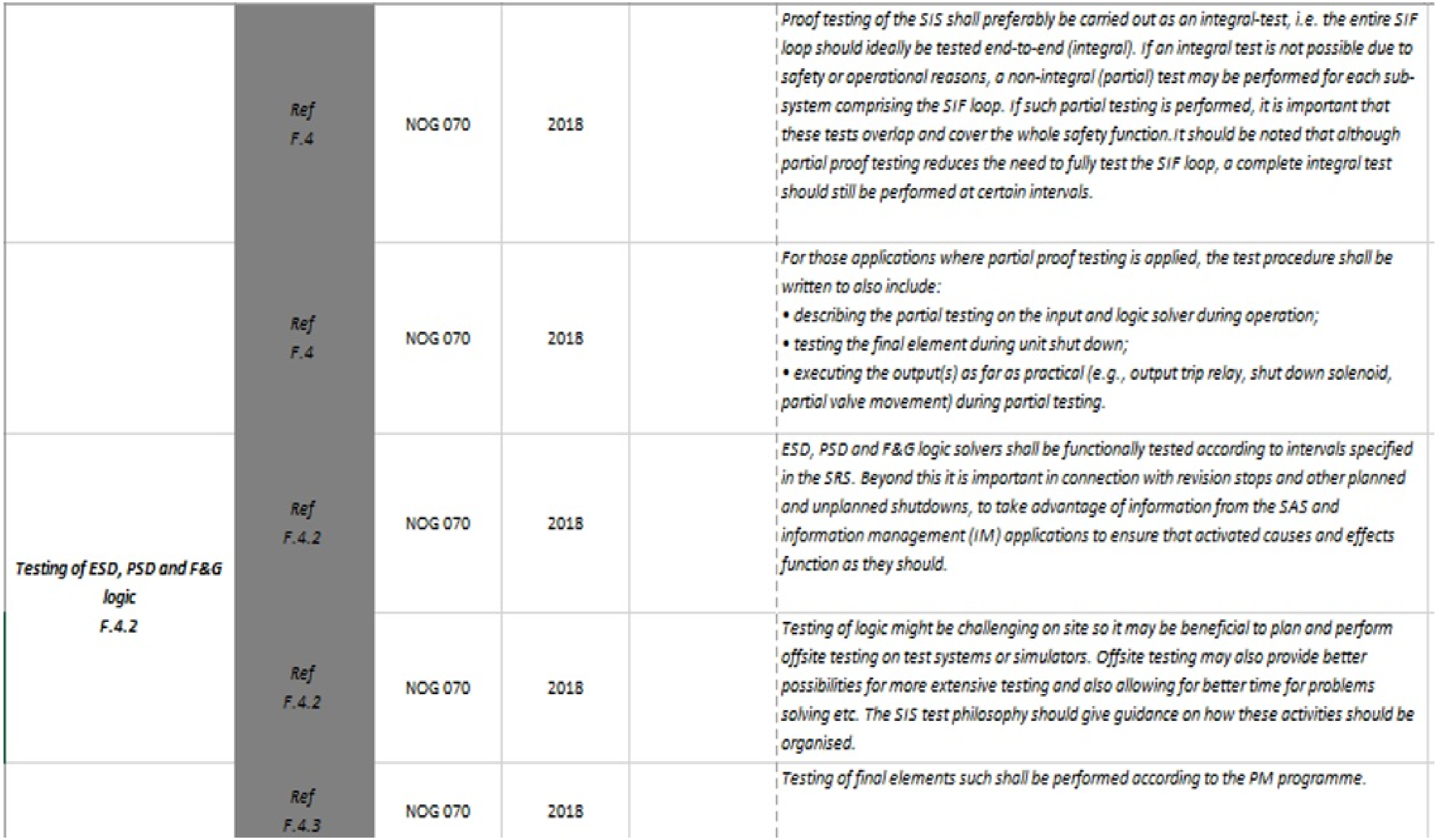
SIS Operation *10.4*	*Ref* *10.4.2*	NOG 070	2018		*The correct compensating measures shall be identified prior to different activities requiring overriding. Such activities may be (but are not limited to):* *• Proof testing* *• Start-up and/or shutdown* *• Preventive maintenance activities* *• Field equipment malfunction and repair* *• Field equipment replacement*
	Ref *10.4.2*	NOG 070	2018		*A system of controlling, approving and recording the application of overodes to SIS shall be in place. The cumulaive effects or consequences of overrodes should be assessed and controled.*
	Ref *10.4.2*	NOG 070	2018		*Operating a degraded system with compensating measures may be challenging, especially if the time of degradation extends beyond what is planned. To be able to control such situations the following should be defined.* *• Maximum allowed mean repair time (MRT) defined for the SIS* *• What to do if MRTs are exceeded*
	Ref *10.4.2*	NOG 070	2018		*If the copmensating measure during SIS overrides involves manual intervention, the available operator response time should be assessed, taking into consideration the foreseen time for revealing the abnormal situations as well as taking correct action.*
	Ref *10.5*	NOG 070	2018		*The SIS shall be proof tested and maintained regularly during operation in order to ensure that the fuctional integrity is maintained during the entire lifecycle. This includes repair o defective components ad replacement with identical units having the same specification as well as registration of criticial SIS failures. Referacne is also amde to IEC 61511-1, cl 16.*
	Ref *10.5*	NOG 070	2018		*SIL classifid safety functions and associated equipment shall be tested according to predifined proof test procedures shceduled in a PM programme as part of the maintenance system.*
SIS testing and maintenance *10.5*	*Ref* *10.5*	NOG 070	2018		*The purpose of a proof test is to reveal all hidden dangerous failures. This shall be considered already during design of the SIS, in order to allow for e.g. partial testing of each component of the system. End-to-end testing may not always be suitable for such a purpose, for example it may not reveal the status of all components in redundant*



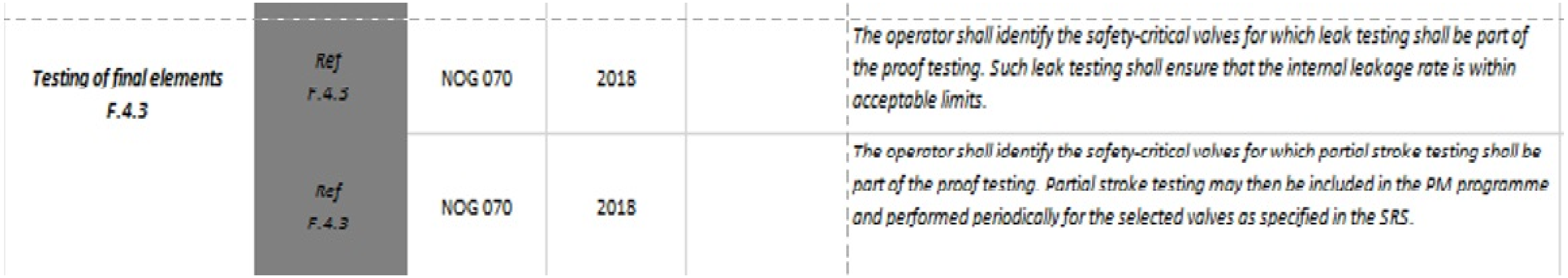
	Ref *10.5*	NOG 070	2018		*Proof testing of SIS should refelct the real operating coditions as accurately as possible .*
	Ref *10.5*	NOG 070	2018		*As part of the proof testing, the results from the test shall be logged in a traceable manner into maintenace system.*
	Ref *10.5*	NOG 070	2018		*All components identified as pat of any SIF should be traceable in the maintenace system in such way that failure data can be used to evaluate perfomance.*
	Ref *10.5*	NOG 070	2018		***Procedures for proof testing of sensors, logic and final elements shall be easily available. Test intervals for the SIL classified equipment shall be consistent with the test intervalv given in SRS.***
SIS monitoring and verification **10.6**	*Ref* *10.6.1*	NOG 070	2018		*All revealed failures or degradation of SIS components that require a corrective action/repair shall be registered with a malfunction notification in the maintenace system.*
	Ref *10.6.2*	NOG 070	2018		*The registered SIS failures and other collected SIS parameters, including periodic reviews of actual demand rate data, should be used to verify that the experienced (or measured) safety integrity level of the SIS is acceptable as compared to the premises laid down in the design of the installation, represented by the SIL requirements.*
	Ref *10.6.3*	NOG 070	2018		*Periodic review of overrides is useful in order to obtain an understanding of why overrides are used, their extent and if possible to reduce the number of overrides. Typical issues to look for are:* *• long term overrides* *• most frequent overrides* *• periodic use of overrides in relation to special operational modes* *• general override statistics* *This may verify if the SIS is operated correctly and intentionally since too much override of a SIF may conflict with the required PFD as given by the SIL.*



	Ref *10.6.4*	NOG 070	2018		*During normal operation the process should operate under stable conditions with very few demands on the safety systems. However, a process has a dynamic nature that may change over time. To understand process and equipment limitations and capabilities and to manage possible changes over time, the process should be monitored w.r.t. the safe operating boundaries. One way of examining the process/system is to review the SIF demand rates*
	Ref *10.6.4*	NOG 070	2018		*The assumed SIF demand rates shall be given in the SRS and is a design parameter which defines how often we accept the function to be activated. If operated more frequent than stated in the SRS, the SIS is not performing within its assumed design limitations and additional risk reducing measures should be considered*
	Ref *F.4*	NOG 070	2018		*Proof testing shall include, but not be limited to, verifying the following:* • *operation of all input devices including primary sensors and SIS input modules;* • *logic associated with each input device;* • *logic associated with combined inputs;* • *trip initiating values (set-points) of all inputs;* • *alarm functions;* • *speed of response of the SIS when necessary;* • *operating sequence of the logic program;* • *function of all final control elements and SIS output modules;* • *computational functions performed by the SIS;* • *timing and speed of output devices;* • *function of the manual trip to bring the system to its safe state;* • *function of user-initiated diagnostics;* • *complete system functionality;* • *the SIS is operational after testing.*



	Ref *F.4*	NOG 070	2018		*Proof testing of the SIS shall preferably be carried out as an integral-test, i.e. the entire SIF loop should ideally be tested end-to-end (integral). If an integral test is not possible due to safety or operational reasons, a non-integral (partial) test may be performed for each sub-system comprising the SIF loop. If such partial testing is performed, it is important that these tests overlap and cover the whole safety function.It should be noted that although partial proof testing reduces the need to fully test the SIF loop, a complete integral test should still be performed at certain intervals.*
	Ref *F.4*	NOG 070	2018		*For those applications where partial proof testing is applied, the test procedure shall be written to also include:* *• describing the partial testing on the input and logic solver during operation;* *• testing the final element during unit shut down;* *• executing the output(s) as far as practical (e.g., output trip relay, shut down solenoid, partial valve movement) during partial testing.*
Testing of ESD, PSD and F&G logic ***F.4.2***	*Ref* *F.4.2*	NOG 070	2018		*ESD, PSD and F&G logic solvers shall be functionally tested according to intervals specified in the SRS. Beyond this it is important in connection with revision stops and other planned and unplanned shutdowns, to take advantage of information from the SAS and information management (IM) applications to ensure that activated causes and effects function as they should.*
	Ref *F.4.2*	NOG 070	2018		*Testing of logic might be challenging on site so it may be beneficial to plan and perform offsite testing on test systems or simulators. Offsite testing may also provide better possibilities for more extensive testing and also allowing for better time for problems solving etc. The SIS test philosophy should give guidance on how these activities should be organised.*
	Ref *F.4.3*	NOG 070	2018		*Testing of final elements such shall be performed according to the PM programme.*



Testing of final elements F.4.3	*Ref F.4.3*	NOG 070	2018		*The operator shall identify the safety-critical valves for which leak testing shall be part of the proof testing. Such leak testing shall ensure that the internal leakage rate is within acceptable limits.*
	Ref F.4.3	NOG 070	2018		*The operator shall identify the safety-critical valves for which partial stroke testing shall be part of the proof testing. Partial stroke testing may then be included in the PM programme and performed periodically for the selected valves as specified in the SRS.*