APPLICATION OF IEC 61508 AND IEC 61511 IN THE NORWEGIAN PETROLEUM INDUSTRY

THE NORWEGIAN
OIL INDUSTRY ASSOCIATION

Table of content

Foreword

This document was originally developed as a joint industry project between operators and the various suppliers of services and equipment with the financial support of OLF. The original work was performed during the autumn of 2000 and the first revision of the document was issued February 2001.

Through the application of the IEC standards and this guideline on various projects, a need was identified for updating the document. This work was initiated early spring 2003 and the present document is the first official update of the original guideline.

The overall purpose of the document is to issue a guideline on the application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry, and thereby simplify the use of the standards.

Additional information can be found at www.itk.ntnu.no/sil.

1 Introduction

1.1 Scope and purpose of document

The purpose of this document is to adapt and simplify the application of the IEC 61508 and IEC 61511 standards for use in the Norwegian petroleum industry.

According to the PSA management regulations (§1 and §2), performance requirements shall be established for all safety barriers on an installation. For instrumented safety systems, special reference is made to IEC 61508 and this document as the recommended standard for specification, design and operation of such safety systems.

Whereas IEC 61508 describes a fully risk based approach for determining SIL (Safety Integrity Level) requirements, this document provides minimum SIL requirements for the most common instrumented safety functions on a petroleum production installation (ref. chapter 7). Deviations from these requirements may however be identified (ref. section 7.7), and in such case the overall methodology and documentation should be in accordance with IEC 61508.

As a basis for the given SIL requirements, typical loop diagrams for a number of safety functions have been provided, together with industrially verified component reliability data (ref. appendix A). It should be noted that the given reliability data, and in particular the rate of dangerous failures (λ_{DU}), are based on a number of assumption concerning diagnostic coverage, fail-safe design, etc. Hence, if the provided data are used for SIL verification, it must be ensured that the actual purchased components are satisfying all these assumptions.

Some key areas related to SIS design are:

- Relationship between Safety Integrity Level (SIL) and failure probability (ref. Table 8.1);
- Restrictions on design based on the Safe Failure Fraction, Hardware Fault Tolerance and the complexity of the component (ref. Table 8.2 and 8.3);
- Avoidance and control of systematic failures.

These aspects are discussed in more detail in chapter 8. Furthermore, the document provides guidance on additional design issues, on operation and maintenance, on modification of SIS and on management of functional safety.

In general, this document applies to all instrumented safety functions as defined by PSA and NORSOK. In the guideline to the PSA Facilities Regulations, a list of relevant safety functions is given. Some of these functions are covered explicitly in this document whereas some are not. Furthermore, some safety functions not explicitly defined by the PSA are also covered in this document. Table 1.1 summarises the functions covered / not covered in this document.

Table 1.1 Safety functions covered / not covered in this document

Safety functions defined in PSA Guidelines, The Facilities Regulations	Safety functions covered in this document	Ref. APP. A	Notes
Sectioning of the process	X	A.4	
Fire detection	X	A.8	Manual initiation of F&G / ESD functions from field and from CCR is covered in A.15
Gas detection	X	A.9	See above comment.
Isolation of sources of ignition	X	A.10	See above comment.
Maintaining overpressure in unclassified areas	-		Not covered by this document.
Starting and stopping fire pumps, both manually and	X	A.11	Part of deluge function

Safety functions defined in PSA Guidelines, The Facilities Regulations	Safety functions covered in this document	Ref. APP. A	Notes
automatically			
Active fire fighting	X	A.11	Deluge
Process safety	X	A.3.1 - A.3.5	
Well safety	X	A.6	Isolation of wells included in this document
Isolation of riser*	X	A.7 and A.13	*Isolation of riser is not explicitly listed by PSA
Subsea ESD isolation*	X (new)	A.13	*Subsea ESD isolation is not explicitly listed by PSA (covered under "Well safety")
Topside and subsea HIPPS protection*	-	-	*Covered as a deviation in appendix C. Ref. also section 7.7.
Depressurisation	X	A.5	
General alarm and evacuation alarm	(X)		Initiating signals from F&G system are covered in this document by A.8 / A.9 Alarm generation and distribution by the PA or dedicated alarm system is not covered.
Emergency power	-		Presently not covered by this document.
Emergency lighting	-		Presently not covered by this document. Particular requirements – Luminaries for emergency lighting covered by IEC 60598-2-22
Ballasting for floating facilities*	X (new)	A.12	*Both initiation of rig re-establishment and emergency stop of ballast system covered
Maintenance of correct pressure, humidity, temperature and gas composition in diving facilities	-		Presently not covered by this document.
Prevention of blowouts and prevention of well leaks during drilling operations*	X(new)	A.14	*Prevention of blowouts is not explicitly listed by PSA but can be seen as part of "well safety"
Prevention of blowouts and prevention of well leaks during well intervention operations*	-	A.14	*As discussed in appendix A.14 no background has been found for stating a SIL requirement for this function.

Process safety functions, like PSD, shall be designed in accordance with ISO 10418 (former API RP 14C). SIL requirements to these functions are however not specified in ISO 10418, but are given in this document. Implementation of global safety functions like ESD and F&G are described by the PSA regulations and in relevant NORSOK standards, whereas SIL requirements are given in this document.

1.2 Risk reduction, SIS and safety barriers

In most situations safety is achieved by using a combination of various safety-related systems, including SIS (e.g. ESD and F&G), safety systems based on other technology (e.g. PSV, firewalls, drain system) and additional risk reduction facilities (e.g. procedures and separation/distance.). Hence, an overall safety strategy must take into consideration all the safety-related systems and measures in order to reduce the risk to an acceptable level. This is illustrated in Figure 1.1 below.

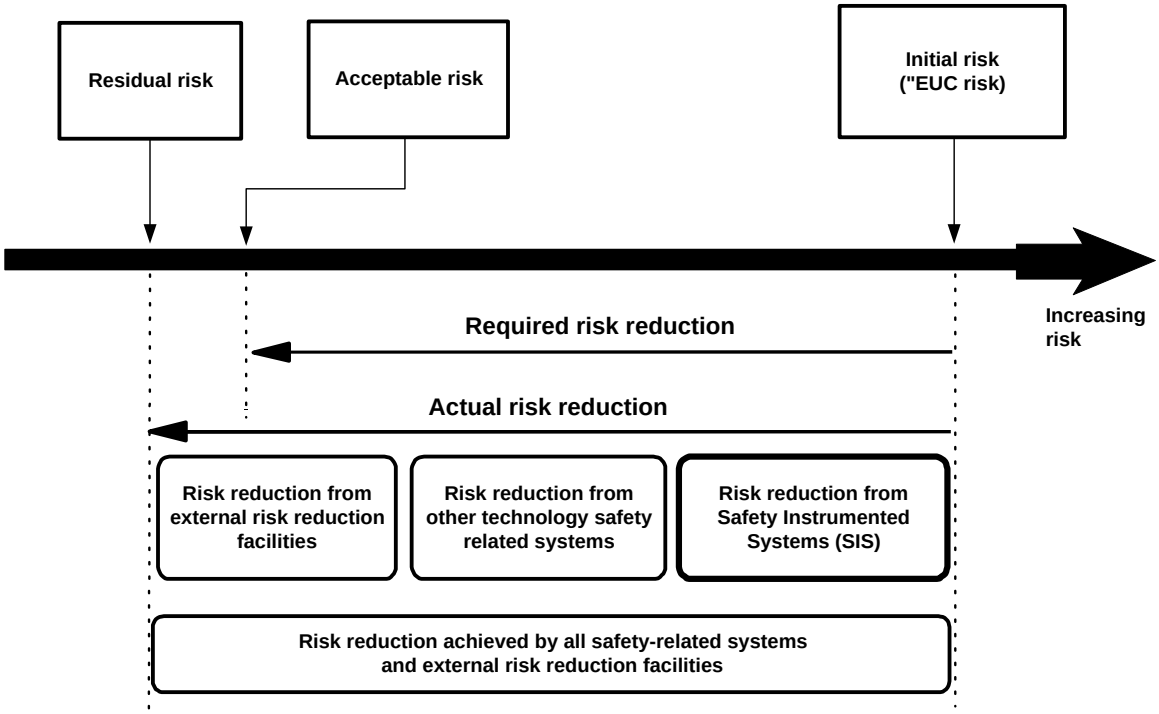

Figure 1.1 Framework for risk reduction (based on figure A.1 in IEC 61508-5)

The frequently used term "safety barrier" can also be related to the above framework. A safety barrier is often interpreted as a function which must be fulfilled in order to reduce the risk, and such a function can be implemented in terms of different systems and elements, both technical and operational. E.g. the safety function "avoid ignition" may be implemented in terms of "ignition source isolation" and "control of hot work permits".

Hence, safety barriers are used to reduce risk and safety barriers can comprise a number of *barrier systems and elements* including instrumented safety systems (SIS) as well as other risk reducing systems and measures. In the management regulations, § 2 (PSA, 2002) safety barriers are specifically described. PSA indicates that general principles and strategies given in IEC 61508 can be applied to all safety systems, although the standard and this document focus on instrumented safety systems. Such general principles and strategies include:

- principles for risk reduction (ref chapter 7)
- the overall lifecycle approach given in IEC 61508 (ref. chapter 2, figure 2.3)
- the nomination of a designated responsible person or job position (ref. chapter 5)
- the performance and follow-up of verification and validation activities (ref. chapter 6)
- follow-up during operation (ref. chapter 10)

It should be noted that this document only gives requirements to instrumented safety functions. These requirements are generally not given on an “overall safety barrier level”, but rather on a level corresponding to barrier elements. Hence, the connection between risk and hazard evaluation and the requirements to barriers is not explicitly covered in this document. This connection should therefore be covered elsewhere, and in this regard the overall facility QRA is an important tool. For a further discussion of the connection between the QRA, the EUC related risks and the use of IEC 61508/61511 for implementation of SIS, please refer to appendix C.

2 The IEC 61508 and IEC 61511 standards

The international standard IEC 61508 has been widely accepted as the basis for specification, design and operation of Safety Instrumented Systems (SIS). The standard sets out a risk-based approach for deciding the Safety Integrity Level (SIL) for systems performing safety functions. This approach has proved difficult to handle as part of a development project, as it requires extensive analysis work, and since requirements to safety functions can normally not be obtained directly from the Quantitative Risk Analysis (QRA) as it is performed today. This document is therefore provided in order to simplify the application of IEC 61508.

Whereas IEC 61508 is a generic standard common to several industries, the process industry has developed their own sector specific standard for application of SIS. This standard; IEC 61511, is also extensively referred in the present document. In Figure 2.1, some guidance on when to apply IEC 61508 and IEC 61511 respectively is given.

IEC 61508 and 61511 are widely accepted industry standards for the implementation of SIS, and application of the standards is recommended in the PSA regulations. Other relevant regulations and standards may not issue similar references to the IEC standards and/or may recommend a different approach to the implementation of SIS.

For further description concerning the use of IEC 61508 and 61511 within different regulations applicable for the offshore industry, reference is made to http://www.ptil.no

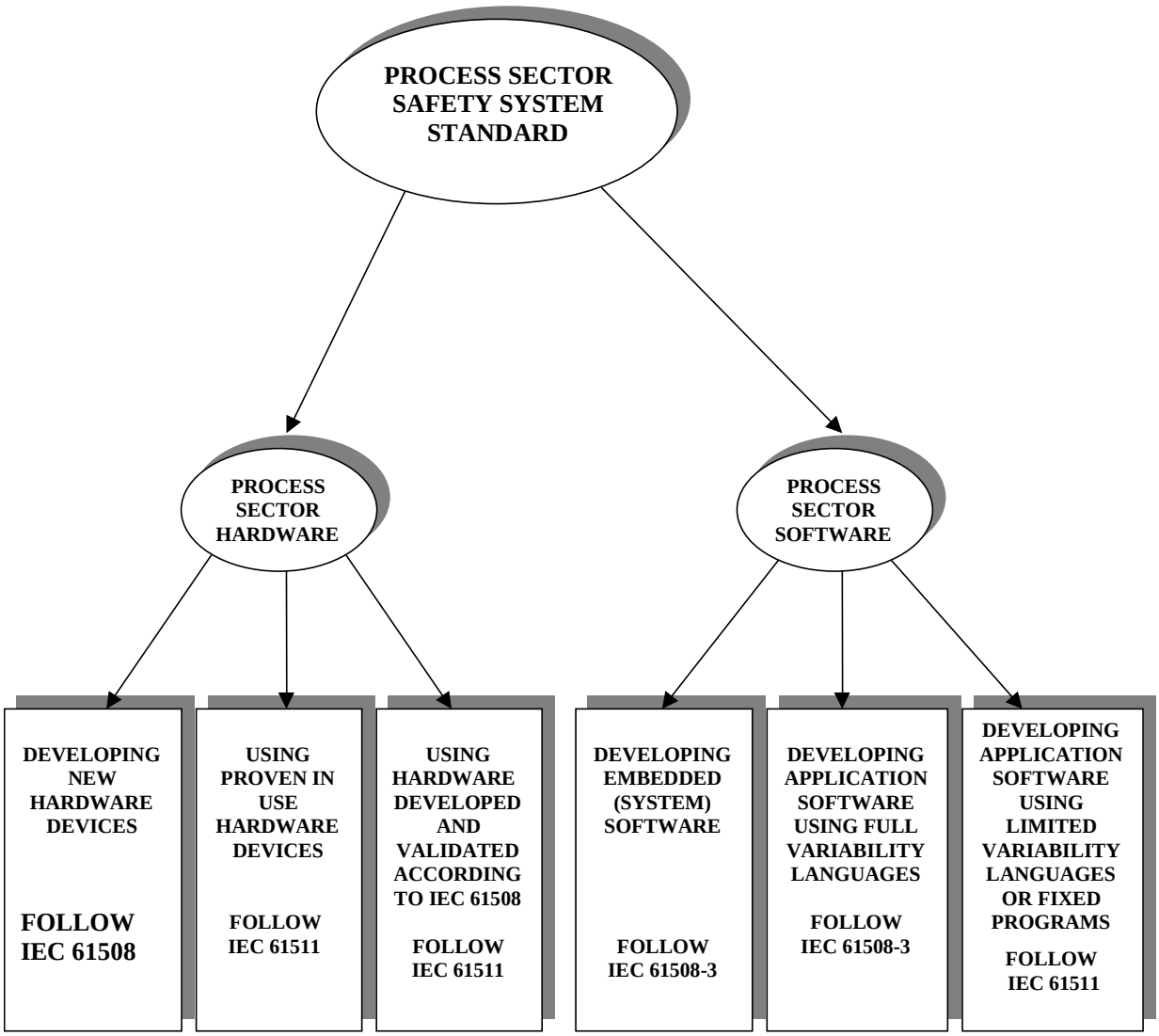

Figure 2.1 Guidance on when to apply IEC 61511 or IEC 61508 (Figure 3 from IEC 61511-1)

Both IEC 61508 and IEC 61511 use the "safety lifecycle" as a framework in order to structure requirements relating to specification, design, integration, operation, maintenance, modification and decommissioning of a Safety Instrumented System (SIS). Each phase has a set of defined inputs and outputs, and towards the end of each phase, a check (or verification) shall be performed to confirm that the required outputs are as planned. The safety lifecycle from IEC 61511 is shown in Figure 2.2 below. For a summary of requirements related to each lifecycle phase, reference is made to Table 2 in IEC 61511-1.

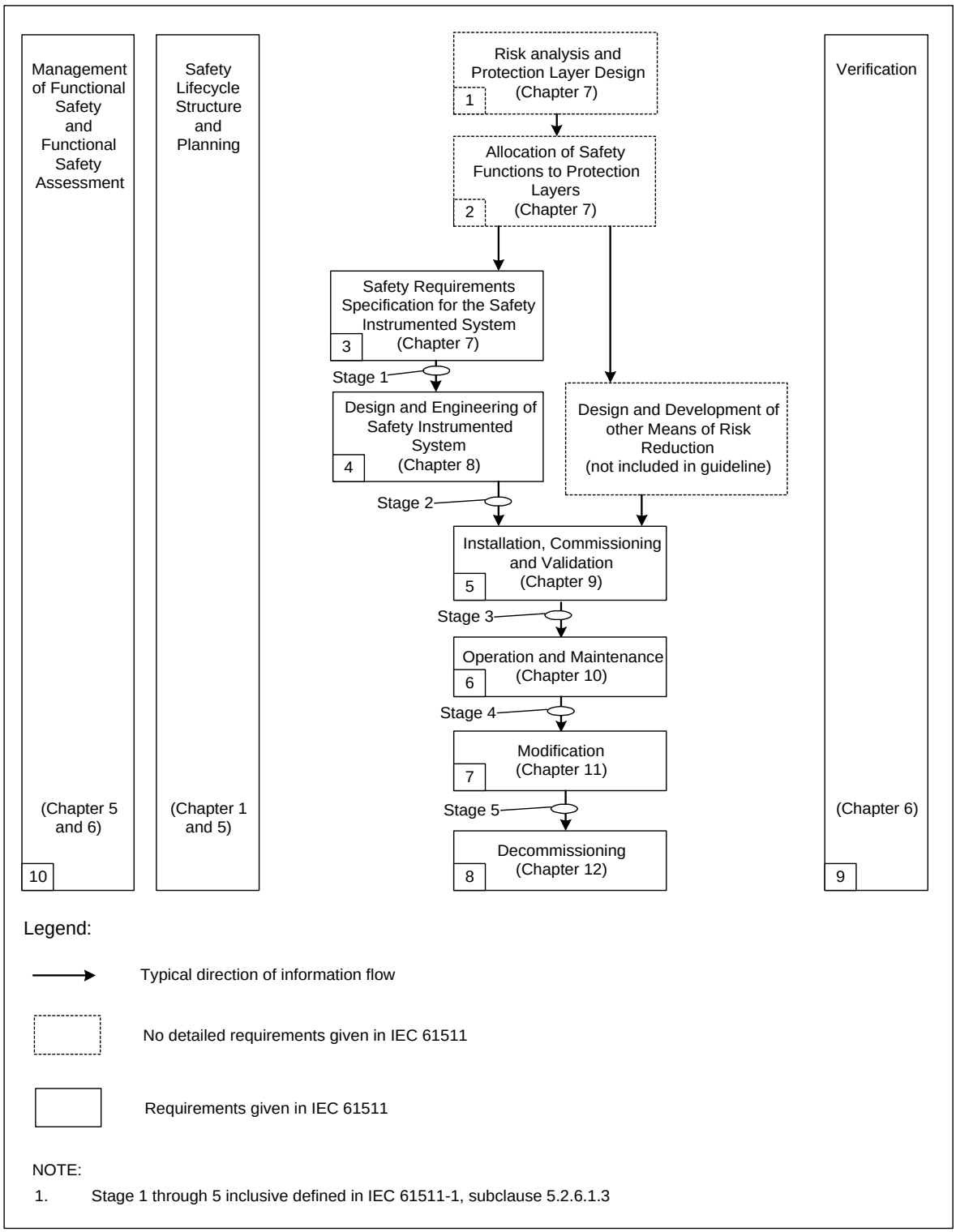

Figure 2.2 Lifecycle from IEC 61511 (ref. Figure 8 from IEC 61511-1), with reference to relevant chapters in this document (in brackets).

For the purpose of completeness, the lifecycle figure from IEC 61508 is also included, ref. Figure 2.3 below. For further specification of requirements to each lifecycle phase, reference is made to Table 1 in IEC 61508-1.

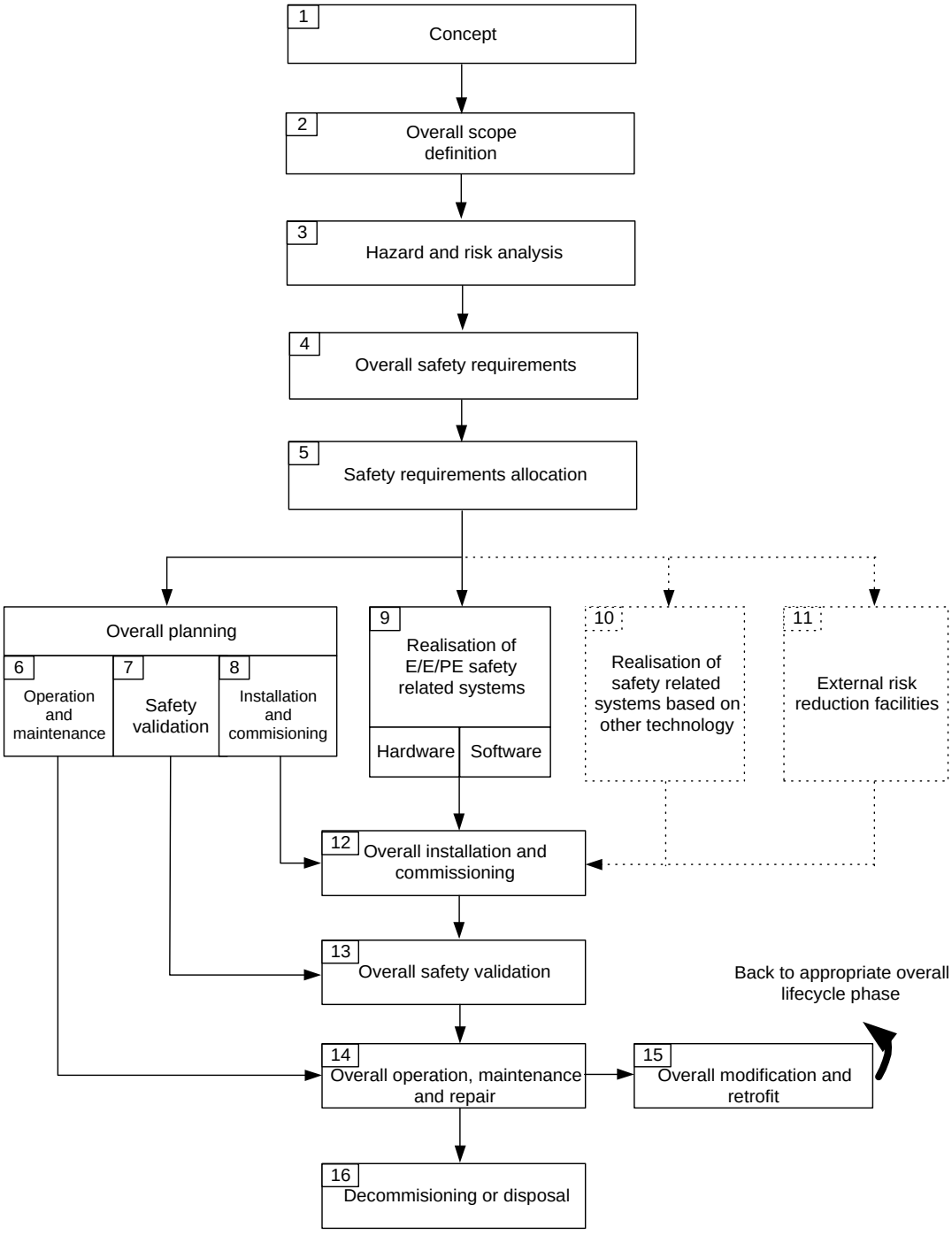

Figure 2.3 Lifecycle from IEC 61508 (ref. Figure 2 from IEC 61508-1)

3 References

Of the references found below some are referred to in this document, and some are listed just for information.

Table 3.1 Table of references

Document id.	Document title
IEC 61511 Part 1, 2003-01 Part 2, 2003-07 Part 3, 2003-03	Functional safety: Safety Instrumented Systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements Part 2: Guidelines in the application of IEC 61511-1 Part 3: Guidance for the determination of the required safety integrity levels.
IEC 61508 Part 1, 1998-12 Part 2, 2000-05 Part 3, 1998-12 Part 4, 1998-12 Part 5, 1998-12 Part 6, 2000-04 Part 7, 2000-03	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems Part 3: Software requirements Part 4: Definitions and abbreviations Part 5: Examples of methods for determination of safety integrity levels Part 6: Guidelines on the application of IEC 61508-2 and 61508-3 Part 7: Overview of techniques and measures
PSA Regulations	Petroleum Safety Authority Norway; joint regulations - The Management regulations (January 2002) - The information duty regulations (January 2002) - The facilities Regulations (January 2002) - The Activities Regulations (January 2002) http://www.ptil.no
NORSOK	http://www.standard.no
ISO 10418, 2003	Petroleum and natural gas industries -- Offshore production installations -- Basic surface process safety systems
API RP 14C, March 2001, 7th Ed.	Recommended practice for Analysis, Design, Installation and Testing of Basic Surface Safety Systems for Offshore Production Platforms (Note that the 4th Edition was issued as ISO 10418)
ISO 13702, 1999	Petroleum and gas industries - Control and mitigation of fires on offshore production installations – Requirements and guidelines
ISO 17776, 2000	Petroleum and natural gas industries -- Offshore production installations -- Guidelines on tools and techniques for hazard identification and risk assessment
ISO 9000	http://www.standard.no, http://www.iso.org
ANSI/ISA-S84.00.01-3 – 2004	Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Part 1-3
PDS Method, 2003	Reliability Prediction Method for Safety Instrumented Systems SINTEF Report STF38 A02420, http://www.sydvest.com
PDS Data, 2004	Reliability Data for Safety Instrumented Systems, SINTEF Report STF38 A04423, http://www.sydvest.com
Published by the OREDA participants, 2002	Offshore Reliability Data Handbook 2002 - fourth Edition
UKOOA, November 1999, Issues No 2	Guidelines for Instrumented-Based Protective Systems
CCPS / AIChE, 1993	Guidelines for Safe Automation of Chemical Processes
CCPS / AIChE, 1994	Guidelines for Preventing Human Error in Process Safety
STF75 A93060, 15/03/1994	Human Dependability Methods for Control and Safety Systems

4 Abbreviations and definitions

4.1 Abbreviations

Below, a list of abbreviations used in this document is given.

BDV	-	Blow down Valve
BOP	-	Blow out Preventor
CCF	-	Common Cause Failure
CCR		Central Control Room
CIV	-	Chemical Injection Valve
CPU	-	Central Processing Unit
DC	-	Diagnostic Coverage
DCV	-	Directional Control Valve
DHSV	-	Downhole Safety Valve
EERS	-	Evacuation, Escape and Rescue Strategy
EPU	-	Electric Power Unit
ESD	-	Emergency Shutdown
ESV	-	Emergency Shutdown Valve
EUC	-	Equipment under Control
FAT	-	Factory Acceptance Test
FES	-	Fire and Explosion Strategy
F&G	-	Fire and Gas
FMEA	-	Failure Mode Effect Analysis
FMECA	-	Failure Mode Effect and Criticality Analysis
HAZID	-	Hazard Identification
HAZOP	-	Hazard and Operability study
HFTL	-	Hardware Fault Tolerance
HIPPS	-	High Integrity Pressure Protection System
HPU	-	Hydraulic Power Unit
HSE	-	Health, Safety and Environment
I/O	-	Input/Output
LT	-	Level Transmitter
MOC	-	Management of Change
MooN	-	M out of N
NDE	-	Normally De-energised
NE	-	Normally Energised
OREDA	-	Offshore Reliability Data
PCS	-	Process Control System
PFD	-	Probability of Failure on Demand
PLC	-	Programmable Logic Controller
PSA	-	Petroleum Safety Authority Norway (former NPD- Norwegian Petroleum Directorate)
PSD	-	Process Shutdown
PSF	-	Probability of Systematic Failure (previously denoted TIF)
PSV	-	Process Safety Valve
PT	-	Pressure Transmitter
PMV	-	Production Master Valves
PWV	-	Production Wing Valve
QA	-	Quality Assurance
QRA	-	Quantitative Risk analysis
RBD	-	Reliability Block Diagram
RNNS	-	Risikonivå på Norsk Sokkel (eng: Risk Level on the Norwegian Continental Shelf)
SAR	-	Safety Analysis Report
SAT	-	Safety Analysis Table
SFF	-	Safe Failure Fraction
SIF	-	Safety Instrumented Function
SIL	-	Safety Integrity Level
SIS	-	Safety Instrumented System
SRS	-	Safety Requirement Specification

SSIV	-	Subsea Isolation Valve
TT	-	Temperature Transmitter
UPS	-	Uninterrupted Power Supply
XV	-	Process Shutdown Valve

For other abbreviations see also IEC 61511-1

NOTE: The term "VOTING" in this document always refers to safety availability, and not to production availability. This means that in a MooN voting, the result will be a safe state when at least M of the N subsystems fulfils their predefined actions. This is independent of NE/NDE design

4.2 Definitions

The definitions given below are meant to be additional to those found in IEC 61508-4 and 61511-1. If repeated, the definitions below are included for the purpose of clarification, using terminology familiar to the offshore industry.

Commissioning	The functional verification of equipment and facilities that are grouped together in systems NOTE: The term Commissioning used in the IEC 61508 and IEC 61511 standards is equal to the term Mechanical Completion as used within this document.
Dangerous failure	Failure which has the potential to put the safety-related system in a hazardous or fail-to-function state NOTE: A fraction of these failures, i.e. the "dangerous detected failures", will be revealed by automatic diagnostic tests. The residual dangerous failures, not detected by self test, are denoted "dangerous undetected failures"
Deviation	In this document the term deviation is applied to denote a departure from the requirements specified in the minimum SIL table, either with respect to function or with respect to integrity level NOTE: As opposed to "non-conformities", deviations are a result of a planned activity, i.e. the need for deviations are identified prior to the execution of the relevant activities
Fire area	A fire area is assumed to withstand the dimensioning fire load. The determination of dimensioning fire load is based on the amount of hydrocarbon that is found in the process segment confined by the fire area
Functional Safety Assessment	Functional Safety Assessment is an investigation, based on evidence, to judge the functional safety achieved by one or more protection layers (ref. IEC 61511-1). NOTE: See chapter 6 for further discussion and relationship between verification, validation and functional safety assessment
Global safety function	Global safety functions, or "fire and explosion hazard safety functions", are functions which typically provide protection for one or several fire cells. Examples will be emergency shutdown, isolation of ignition sources and emergency blow down
Local safety function	Local safety functions, or "process equipment safety functions", are functions confined to protection of a specific process equipment unit. A typical example will be protection against high level in a separator through the PSD system
Mechanical Completion	The checking and testing of equipment and construction to confirm that the installation is in accordance with drawings and specifications and ready for commissioning in a safe manner and in compliance with project requirements.
Non-conformity	Non-fulfilment of a requirement (ref. ISO 9000) NOTE: As opposed to "deviations", non-conformities are a result of mistakes, i.e. they

	are revealed after the relevant activities are executed
Safe failure	Failure which does not have the potential to put the safety-related system in a hazardous or fail-to-function state NOTE: A fraction of these failures, i.e. the “safe detected failures”, will be revealed by automatic diagnostic tests. The residual safe failures, not detected by self test, are denoted “safe undetected failures”
Systematic failure	Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors (ref. IEC 61508-4)
Validation	Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled NOTE 1: The term "validated" is used to designate the corresponding status NOTE 2: The use conditions for validation can be real or simulated (ref. ISO 9000) NOTE 3: See chapter 6 for further discussion
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled NOTE 1: The term "verified" is used to designate the corresponding status NOTE 2: Confirmation can comprise activities such as - performing alternative calculations, - comparing a new design specification with a similar proven design specification, - undertaking tests and demonstrations, and - reviewing documents prior to issue. (ref. ISO 9000) NOTE 3: See chapter 6 for further discussion

5 Management of functional safety

5.1 Objective

The objective of this chapter is to identify the management activities that are necessary to ensure that functional safety requirements are met.

Health, Safety and Environment (HSE) management within the scope of IEC 61508 and IEC 61511 constitutes all activities necessary to ensure that the SIL requirements are identified, designed and maintained during the entire lifecycle of the systems. These activities are referred to as *management of functional safety*.

It should be noted that the term "HSE management" in general has a broader scope than the IEC 61508 and IEC 61511 interpretation. Safety related aspects of an installation like conceptual design, structural and stability aspects, total system design and operation, drilling, environment aspects, working environment, construction safety, interface between operator and contractors etc., all need to be included in the overall management system.

5.2 Requirements

5.2.1 Competence

All activities that affect the safety life cycle of the SIS shall be managed and performed by personnel who are competent to do so in accordance with the relevant requirements in the PSA regulations and in IEC 61508 and IEC 61511. As a minimum, the following items should be addressed when considering the competence issue:

- engineering knowledge, training and experience appropriate to the:
  - process application;
  - technology used (e.g., electrical, electronic or programmable electronic);
  - sensors and final elements.
- safety engineering knowledge (e.g., process safety analysis);
- knowledge of the legal and safety regulatory requirements;
- adequate management and leadership skills appropriate to their role in safety lifecycle activities;
- understanding of the potential consequences of undesirable events;
- the safety integrity level of the safety instrumented functions;
- the novelty and complexity of the application and the technology.

Furthermore, both operators and contractors working with such systems must have formal employee appraisal and training programs to ensure the above.

5.2.2 Responsible Person

All personnel and organisational units responsible for carrying out and reviewing each of the safety lifecycle phases shall be identified and be informed of the responsibilities assigned to them.

It is important that clear lines of responsibility are established for each phase of the safety lifecycle. This should be under the control of a designated responsible person or job position with the necessary authority assigned to it. All persons with significant involvement with SIS should understand and know the nature and extent of their responsibilities.

The person or job position with overall responsibility for the SIS must ensure that the system performance is in accordance with the SIS Safety Requirements Specification. This includes:

- Ensure that operations and maintenance procedures (ref. chapter 10) are available and used as intended. In particular, ensure that appropriate records are maintained with respect to test results, maintenance activities, system failures and failure types, and demand rate on the system;
- Ensure that the competency of operators, maintenance technicians and engineers who work with or on the safety system is adequate;

- Ensure that access control to the safety system including the use of keys and passwords is in place;
- Ensure that management of change procedures as defined in chapter 11 are available and applied.

5.2.3 Planning

A clear and concise plan shall be developed to define the required activities, persons, department, organisation or other units responsible to carry out these activities. This plan shall be a “live” document, i.e. updated and maintained throughout the entire safety lifecycle.

All verification, validation and assessment activities, as further described in chapter 6, must be included in the plan.

5.2.4 Follow up

Procedures shall be developed and implemented to ensure the expedition, follow-up and resolution of recommendations relating to the SIS that arises from:

- Hazard analysis and risk assessment;
- Other assessment activities;
- Verification activities;
- Validation activities;
- Functional Safety Assessment (FSA).

5.2.5 Assessment, auditing and revisions

In accordance with the PSA regulations, a programme shall be in place for regular audits, reviews and revisions of the processes throughout the safety lifecycle. The assessment team appointed for this purpose shall include the necessary technical and operational expertise for the particular installation.

6 Verification, Validation and Functional Safety Assessment

6.1 Introduction

Verification, validation and safety assessment activities shall be performed at defined milestones. The minimum requirements for such milestones are as shown in Figure E.1 attachment E.

6.2 Interpretation of terms

ISO/PSA and IEC 61508/61511 interpret the terms Verification, Validation and Functional Safety Assessment in somewhat different ways. Figure 6.1 is an attempt to clarify the relationship between the terms, which are further explained in chapters 6.3 – 6.5.

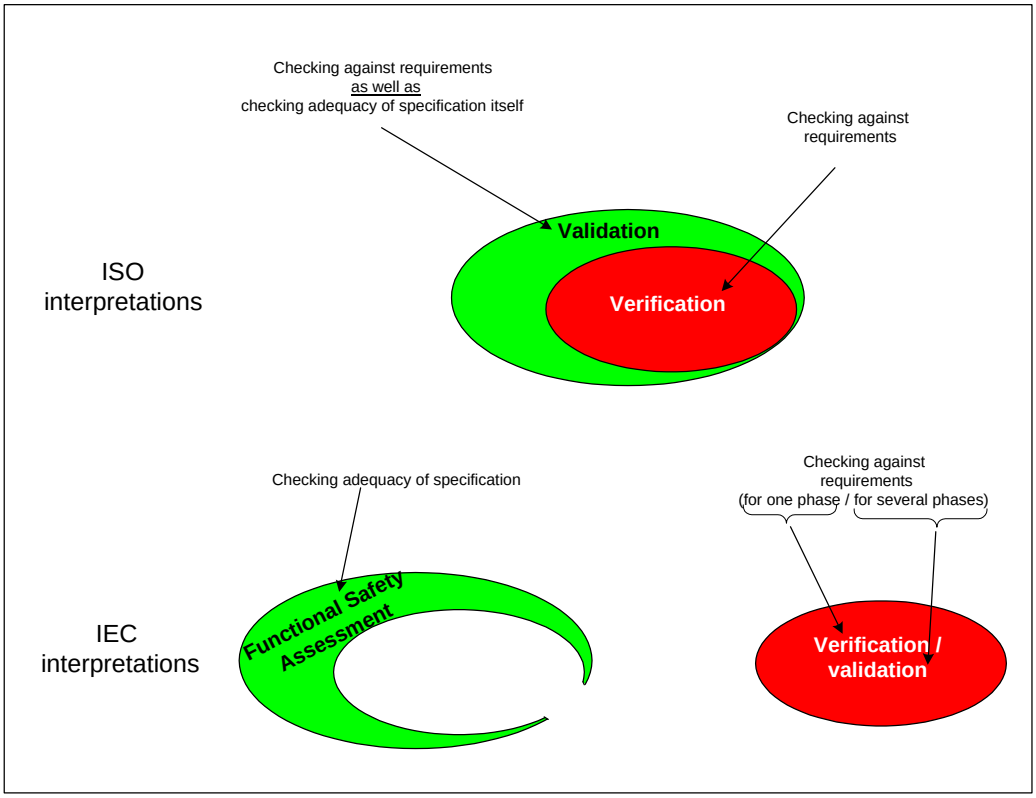

Figure 6.1 Interpretation of the relationship between verification, validation and functional safety assessment according to ISO and IEC, respectively

6.3 Verification

In this document verification implies performing independent checks for each phase of the safety lifecycle and, for specified inputs, to demonstrate that the deliverables meet the requirements and objectives for the phase.

The checks could, for example, include independent document reviews and/or independent calculations or tests. The verification plan should define:

- The items to be verified;
- The procedures to be used for verification;
- When the verification activities should take place;

- The parties responsible for the verification activities, including the required level of independence;
- The basis for the verification, i.e. the information/specification(s) to verify against;
- How to handle deviations and non-conformities.

The results of the verification process shall be properly documented and available upon request.

6.4 Validation

The ISO definition of validation (ref. section 4.2) implies checking whether the design is fit for the intended use or application. This includes checking if the user requirements are adequate, as well as ensuring that the design is capable of fulfilling the user requirements.

It should be noted that in the context of IEC 61508 and IEC 61511, validation very much resembles verification, the main difference being that when performing a validation, the extent of the checking covers several lifecycle phases. IEC 61508 and IEC 61511 describe two such validation activities: First, a SIS safety validation shall be performed at the end of the design phase. This activity includes checking the design against the Safety Requirements Specification, and is defined as a ***validation.*** This is because the design phase is broken down in several stages, the last stage constituting the SIS validation (ref. figure 2 in IEC 61508-2). Secondly, an overall safety validation is prescribed after installation and mechanical completion, in order to demonstrate that the SIS meets the Safety Requirements Specification in all respects.

Hence, when using the ISO definitions from section 4.2, it is seen that the IEC 61508/61511 validations are actually verifications. The activity of ensuring the quality of e.g. the Safety Requirements Specification (i.e. whether it is adequate) is in IEC 61508/61511 not defined as a validation, but rather as a functional safety assessment.

NOTE: The activity of demonstrating that the SIS meets the Safety Requirements Specification after installation and mechanical completion, is also sometimes referred to as a *Site Acceptance Test (SAT)* or *final commissioning*. Overall safety validation is further described in sections 9.3.4 – 9.3.6 of this document.

6.5 Functional Safety Assessment

Functional safety assessment in the context of IEC 61508 and IEC 61511 implies performing independent reviews and audits at predefined stages of the safety lifecycle (often referred to as “independent 3’rd part verifications”). “Independent” implies that personnel not involved in the design should perform the Functional Safety Assessment. Tables 4 and 5 in IEC 61508-1 specify the minimum level of independence of such personnel. It is important to involve highly competent personnel with diverse competence in the assessment, in order to reveal possible weaknesses, systematic failures and omissions. Functional Safety Assessment may be performed by means of, for example, Design Reviews, Peer Reviews and/or Technical Safety Audits.

IEC 61511 recommends such assessments to be made at the following stages:

i. After the hazard and risk assessment has been carried out, the required protection layers have been identified and the safety requirement specification has been developed;
ii. After the safety instrumented system has been designed;
iii. After the installation, pre-commissioning and final validation of the safety instrumented system has been completed and operation and maintenance procedures have been developed;
iv. After gaining experience in operation and maintenance;
v. After modification and prior to decommissioning of a safety instrumented system.

Especially the first (i.) and also the third (iii.) assessment listed above are of particular importance when it comes to making the safety functions fit for use.

The number, size and scope of functional safety assessment activities depend on the specific circumstances. Factors influencing this decision will include the size, complexity and duration of the project, the safety integrity levels, the consequences in the event of failure and the degree of standardisation of design features.

7 Development of SIL requirements

7.1 Objective

The overall objective of this chapter is to describe a methodology for determining SIL requirements for instrumented safety functions. This includes:

- to propose definitions of Equipment Under Control (EUC) for local and global safety functions;
- to describe the required extent of hazard and risk analysis;
- to describe minimum SIL requirements and how to identify deviations from these requirements;
- to propose suitable methods for handling deviations from the minimum SIL table.

Since this document provides minimum SIL requirements for the most common instrumented safety functions, allocation of SIL requirements between function (as specified by IEC 61508) is not described as a separate activity in this chapter.

7.2 Approach

This document *does not* describe a fully risk based approach for determining SIL requirements according to IEC 61508. Rather, a table of minimum SIL requirements is given and shall be adhered to whenever relevant. The rationale behind these predefined integrity levels is to ensure a minimum safety level, to enhance standardisation across the industry, and also to avoid time-consuming calculations and documentation for more or less standard safety functions. A more detailed discussion of this is given in section 7.6.

Needs for deviating from these requirements will, however, arise, e.g. due to technological advances as well as special conceptual or operational aspects. Whenever identified, these "deviations" need to be treated according to IEC 61508/61511 methodology, i.e. the safety integrity level should be based upon a qualitative or quantitative risk based method (ref. section 7.7).

Figure 7.1 below illustrates the process for developing SIL requirements as described in this chapter. This covers the lifecycle phases as represented by box 1-3 in Figure 2.2, or box 1–5 in Figure 2.3.

7.3 Definition of EUC

The purpose of this activity is to achieve a thorough understanding of the equipment under control (EUC).
IEC 61508 does not provide any specific rules as to how the EUC and its boundaries shall be defined. However, based on IEC definitions, the EUC could be a piece of equipment, machinery, part of an offshore installation, or even the entire installation. The EUC shall be considered as the source of hazards and hence shall be protected either by Safety Instrumented Systems (SIS), other technology safety systems, external risk reducing measures, or a combination of these systems.

In this document a distinction is made between two main types of EUC; Those protected by local safety functions (such as PSD) and those protected by global functions (such as ESD). Examples on how to define EUC for these two cases are given in Appendix B.1 and B.2 respectively.

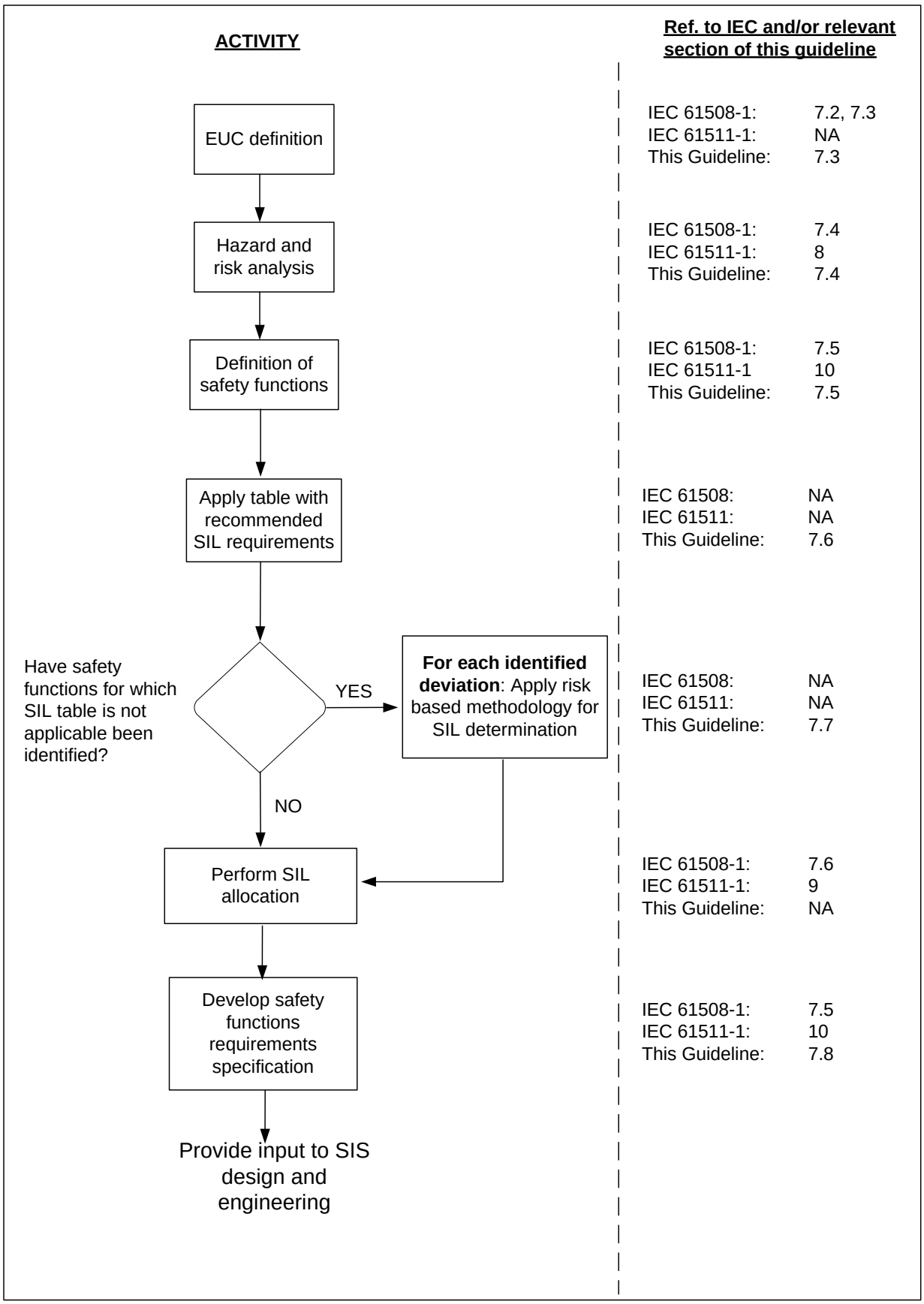

Figure 7.1 Flowchart – development of SIL requirements

7.4 Hazard and risk analysis

7.4.1 Scope of hazard and risk analysis

The hazard and risk analysis shall, according to IEC 61508, determine the following issues:

- the hazards and the hazardous events of the EUC and associated control equipment;
- the event sequence leading to the hazards;
- the EUC risks associated with the identified hazards;
- the requirements for risk reduction.

The hazard and risk analysis shall consider all reasonable foreseeable circumstances including possible fault conditions, misuse and extreme environmental conditions. The hazard and risk analysis shall also consider possible human errors, and abnormal or infrequent modes of operation of the EUC.

As discussed in section 7.2, a table with minimum SIL requirements for determination of integrity levels for "standard" safety functions is provided. This approach, as compared to a fully risk based IEC 61508 analysis, will limit the required scope and extent of the risk analysis, and will direct focus towards the hazard identification, and in particular the identification of deviations from the minimum SIL table. Furthermore, an important activity will be, whenever possible, to verify by QRA that the minimum SIL requirements are sufficient to fulfil the overall risk acceptance criteria.

7.4.2 Hazard identification (HAZID)

Hazard identification (HAZID) must be performed for the defined EUC and its associated control system. The objective of the HAZID will be to identify the inherent hazard potential of the EUC, without safety related functions present. The HAZID must be sufficiently detailed so as to enable identification of potential deviations from the minimum SIL table.

The HAZID shall be carried out with due consideration to issues such as:

- properties of the fluids being handled;
- operating and maintenance procedures;
- the different operations and operational modes affecting the EUC, such as start-up, shutdown, maintenance, pigging, well interventions, etc.;
- hazards arising from human intervention with the EUC, i.e. the effect of human/operational errors;
- the novelty and complexity of the installation under consideration;
- the subsequent need for special protection functions due to the hazards identified;
- whether a failure of the PCS can cause separate hazards and/or a demand on the SIS.

In order to reduce the chance of omitting any hazards during the examination of the EUC, the hazard identification should be performed by a multidiscipline team covering the relevant engineering disciplines as well as operational and maintenance experience.

The type of technique(s) applied for identification of hazards will depend on factors such as the lifecycle stage at which the identification is undertaken (information available) and the type and complexity of the installation. Generally, the more novel and complex an installation, the more "structured" approach will be required. For a more detailed discussion of this topic, see e.g. ISO 17776; "Guidelines on tools and techniques for identification and assessment of hazardous events".

7.5 Definition of safety functions

7.5.1 Scope

The overall objective of this activity is to define the safety instrumented functions that should either conform with the minimum SIL table (ref. section 7.6) or which represent deviations from this table (ref. section 7.7). This includes:

- Describe the safety functions required to protect against the risks identified;
- Define safety functions to be implemented in SIS (i.e. safety instrumented functions);
- Define safety instrumented functions that do not conform to the minimum SIL table.

7.5.2 Requirements

For process safety design following an ISO 10418 analysis, the local safety functions will be defined through the safety analysis tables documenting the analysis (example for overpressure of equipment: PAHH/PSD + PSV). Deviation from conventional ISO 10418 design such as the use of HIPPS, or other deviations from the minimum SIL table, shall be identified and documented in the SAT tables.

Requirements for global safety functions are to a large degree specified in the PSA regulations (ref. the "facility regulations") and NORSOK. Additional requirements relevant to the global safety functions may follow from the Quantitative Risk analysis (QRA) or from preparing the Fire and Explosion Strategy (FES, ref. ISO 13702).

Based on the ISO 10418 analysis, HAZOP studies, the QRA, the FES and/or other analyses, safety function deviations may have been identified. Definition and handling of such deviations are further described in section 7.7.

For all other safety instrumented functions, the minimum SIL requirements as given in Table 7.1 below shall apply.

It is essential that the safety instrumented functions are defined such that all equipment / utilities required to fulfil the specified action are included. For functions requiring energy to operate, it is essential that the energy source is included as part of the safety function. For example, this will imply (but not be limited to):

- for a valve depending upon local hydraulic supply to perform its intended function (i.e., double acting hydraulic valves), the safety function shall include also the local hydraulic supply system
- the UPS must be included in safety functions requiring this supply source, e.g. the UPS may be required for opening the deluge valve
- for systems not being fail safe it is necessary to consider which energy sources are available and required during different scenarios (main power, emergency power, UPS)

7.6 Minimum SIL requirements

Table 7.1 below presents the minimum SIL requirements. When stating minimum SIL requirements like the ones below, one main objective has been to ensure a performance level equal to or better than today's standard. Hence, in cases where the generic reliability data has indicated a requirement just between two SIL classes, generally the stricter SIL requirement has been chosen. This is also in line with the PSA requirement for continuous improvement.

For several safety functions it has been difficult to establish generic definitions. Due to installation specific conditions, design and operational philosophies etc., the number of final elements to be activated upon a specified cause will for example differ from case to case. Consequently, several of the requirements are given on a sub-function level rather than for a complete safety function.

It is important to emphasise that the tabulated SIL requirements are minimum values, and therefore need to be verified with respect to the overall risk level. The minimum SIL requirements should be used as input to QRA, which will then represent a verification of the stated requirements, especially for the global safety functions. If the QRA reveals that the overall risk level is too high, e.g. due to a particularly large number of high pressure wells or risers, then this could trigger a stricter requirement to one or more of the safety functions in Table 7.1 (ref. example in Appendix C.2). Similarly, other types of analyses performed in the design phase may introduce more stringent requirements than specified in the minimum SIL table (ref. discussion in section 7.7).

It is also important to emphasise that the minimum SIL requirements given in Table 7.1 are only one part of the requirements that must be fulfilled in order to ensure compliance with IEC 61508/61511 and this document. As discussed in other sections of this document, management of functional safety, architectural constraints on hardware safety integrity, behaviour upon detection of a fault and control and avoidance of systematic faults are other important aspects to be considered.

The following additional assumptions constitute the basis for the requirements given in Table 7.1:

- The SIL requirements given in the table basically apply for risk to personnel. When using the table to consider environmental risk and risk to assets / production, special care should be taken as to the applicability of the requirements. For some cases, e.g. particularly vulnerable environmental areas, special considerations might result in a need for stricter requirements, whereas in other cases the requirements might be relaxed;

- The requirements to PSD functions implicitly assume a second level of protection (e.g. a PSV) as specified in ISO 10418. It should be noted that HIPPS in this document is considered as a deviation from conventional design (ref. examples in Appendix C);
- Basically the given SIL requirements apply for all systems involving the specified functions and where failure of these may constitute a risk with respect to personnel, the environment or to economical assets. If, for some reason, it is decided to apply lower requirements for special types of systems (e.g. selected utility systems, low pressure vessels, low flammability liquids, etc.), it must be demonstrated that this achieves an acceptable risk level (e.g. by the use of risk graph, QRA, or other type of analyses);
- Failure data used for verifying the quantitative PFD requirements must be qualified as described in Section 8.5.2
- For functions like activation of firewater and start of ballasting, the SIL requirements only include start up of pumps. The additional importance of having a running function for a specified time period should also be considered, e.g. in the SRS.

For detailed definitions of the safety functions and background information concerning assumed failure rates, test intervals and demand rates (all typical values), reference is made to Appendix A.

Table 7.1 Minimum SIL requirements - local safety functions

Safety function	SIL	Functional boundaries for given SIL requirement / comments	Ref. APP. A
Process segregation (through PSD) (closure of several valves)	1	The SIL requirement applies to the whole PSD function as defined in Appendix A.3.1. The function starts where the signal initiating shutdown is generated and includes all valves necessary to effectuate the actual segregation of the process equipment or section. Note: The sensor element has not been included in the function. However, doing this should generally not jeopardise the SIL 1 requirement.	A.3.1
PSD functions : *PAHH* *LAHH* *LALL* (closure of critical valve(s))	2	The SIL requirement applies to closure of critical valve(s) through the PSD system as defined in Appendix A.3.2. The function starts with (and includes) the process sensor and terminates with closing of critical valve(s) within the time required to avoid process conditions above design limits. Note: The given requirement for PAHH and LAHH is for closing the hydrocarbon inlet to the considered process equipment independent of number of valves/lines.	A.3.2
PSD/ESD function: LAHH on flare KO drum (detection and transfer of shutdown signal through both PSD and ESD)	3	The SIL requirement applies to the combined PSD and ESD function as defined in appendix A.3.3. The function starts with (and includes) the process sensors and terminates at the unit(s) intended to perform the action (see Note below). Note: The final element(s) have not been included since a generic definition of this function has been impossible to give.	A.3.3
PSD function: TAHH/TALL (closure of final element)	2	The SIL requirement applies to closure of the critical valve through the PSD system as defined in Appendix A.3.4. The function starts with (and includes) the temperature sensor and terminates with closing of the critical valve. Note 1: the final element could be different from a valve, e.g. a pump which must be stopped.	A.3.4
PSD function: PALL (primary protection	NA	No particular SIL requirement is given for leak detection through the PSD system. This applies only if a gas detection system is capable of detecting gas occurrences such that the likelihood of	A.3.5

Safety function	SIL	Functional boundaries for given SIL requirement / comments	Ref. APP. A
against leakage)		escalation is minimised. Note 1: No particular requirement to SIL is given due to the assumed low reliability of detecting low pressure. When disregarding the initiator, this function is capable of fulfilling a SIL 1 requirement (as for "*process segregation through PSD"* above). Note 2: For under pressure protection the SIL requirements should be individually addressed	

Table 7.1 cont. Minimum SIL requirements - global safety functions

Safety function	SIL	Functional boundaries for given SIL requirement / comments	Ref. APP. A
ESD sectioning (closure of one ESD valve)	2	The SIL requirement applies to the sub-function needed for closure of one ESD valve, i.e.: - ESD-node - ESD valve including solenoid(s) and actuator	A.4
Depressurisation (blow down); (opening of one blow down valve)	2	The SIL requirement applies to the sub-function needed for opening of one blow down valve, i.e.: - ESD-node - Blow down valve including solenoid(s) and actuator Note: The given requirement assumes a "standard" blow down system. If another design solution, such as e.g. sequential blow down, is implemented, this must be treated as a deviation if the SIL 2 requirement is not fulfilled.	A.5
Isolation of topside well; (shut in of one well by the ESD including PSD function)	3	The SIL requirement applies to the sub-function needed for isolation of one topside well, i.e.: - ESD-node (wellhead control panel) - PSD-node - Wing valve (WV) and master valve (MV) including solenoid(s) and actuators - Down hole safety valve (DHSV) including solenoid(s) and actuator The function starts at the unit where the demand is initiated (unit not included), and ends with the valves shutting in the well.	A.6
Isolation of riser; (shut in of one riser)	2	The SIL requirement applies to the sub-function needed for isolation of one riser/flow line, i.e.: - ESD-node - ESD valve including solenoid(s) and actuator The function starts at the unit where the demand is initiated (unit not included), and ends with the valve closing towards the riser.	A.7
Fire detection; (alarm signal generated, processed and action signals transmitted)	2	The SIL-requirement applies to the sub-function needed for fire detection, given exposure of one detector, i.e.: - Fire detector (heat, flame or smoke) - F&G node	A.8
Gas detection; (alarm signal generated, processed and action	2	The SIL-requirement applies to the sub-function needed for gas detection, given exposure of one detector, i.e.: - Gas detector - F&G node	A.9

Safety function	SIL	Functional boundaries for given SIL requirement / comments	Ref. APP. A
signals transmitted)			
Electrical isolation; (signal giving action processed in F&G logic and electrical ignition sources removed)	2	The SIL-requirement applies to the sub-function needed for electrical isolation given signal from F&G/ESD node, i.e.: - F&G node - Circuit breakers (6 off)	A.10
Release of firewater / Deluge; (fire water demand signal processed in Fire & Gas logic, start of fire pump, and opening of deluge-valve)	2	The SIL requirement applies to the sub-function needed for opening of one deluge valve, given confirmed fire or gas, i.e.: - the fire water demand signal processed in the fire pump logic - start of fire pumps - Opening of one deluge-valve (given confirmed fire) The function is considered successful when a certain amount of water (l/min) flows through the deluge valve.	A.11
Manual initiation of F&G / ESD functions from field/CCR	2	The SIL requirement applies to manual function initiated from field; - Safety Node - Push button	A.15
Start of ballast system for Initiation of rig re-establishment (opening of three ballast control valves and starting of one of two ballast pumps)	1	The SIL requirement applies to the sub-function needed for opening of three valves and starting of one pump, i.e.: - Ballast control node - Three ballast control valves including solenoids - Motor starter for one pump (in a 2x100% configuration)	A.12
Emergency stop of ballast system (Pushbutton initiated relay logic stopping one pump by removing the electrical power to the motor and closing one valve by removing the electrical power in the logic output signal loop controlling the valve)	2	The SIL requirement applies to the sub-function needed for pushbutton initiated emergency stopping of one pump and one valve, i.e.: - Emergency pushbutton - Shutdown relay logic for one pump and one valve - Contactor for pump motor - Valve, including solenoid and pilot	A.12

Table 7.1 cont. Minimum SIL requirements - subsea safety functions

Safety function	SIL	Functional boundaries for given SIL requirement / comments	Ref. APP. A
Subsea ESD Isolate one subsea well	3	Shut in of one subsea well. The SIL requirement applies to a conventional system with flow line, riser and riser ESD valve rated for reservoir shut in conditions. Isolation of one well by activating or closing: - ESD node - Topside Hydraulic (HPU) and/or Electrical Power Unit (EPU) - Wing Valve (WV) and Chemical Injection Valve (CIV) including actuators and solenoid(s) - Master Valve (MV) - Downhole Safety Valve (DHSV)) including actuators and solenoid(s) Note) If injection pressure through utility line may exceed design capacity of manifold or flow line, protection against such scenarios must be evaluated specifically.	A.13

Note: If a PSD system is specified for a conventional system for safety reason, the PSD functions shall be minimum SIL 1.

Table 7.1 cont. Minimum SIL requirements – drilling related safety functions

Safety function	SIL	Functional boundaries for given SIL requirement / comments	Ref. APP. A
Drilling BOP function Closing of relevant BOP valve(s) in order to prevent blowout and/or well leak	2	Annular/pipe ram function [1)]	A.14.2
	2	Blind shear ram function [1)]	A.14.2

1) The total safety functions include activation from the drillers console or the tool pushers console and the remotely operated valves needed to close the BOP sufficiently to prevent blowout and/or well leak.

7.7 Handling of deviations from the minimum SIL requirements

7.7.1 Identification of deviations

As discussed in section 7.6, the objective of the minimum SIL table is to cover the most common safety functions. However, deviations from this table will occur and must be identified and treated according to IEC 61508 methodologies.

In the context of the minimum SIL requirements given in Table 7.1, the following types of deviations are relevant to consider:

- *A Functional deviation*: i.e. a safety function not covered by Table 7.1. Such deviations may result from hazards requiring instrumented safety functions other than those defined as conventional design according to ISO 10418, other relevant standards or those described in the PSA regulations and in this document. This would typically be HIPPS as a replacement for PSV capacity, instrumented protection instead of full flow PSV capacity, safety interlock systems, pipeline protection systems, unproven technology, etc.

- *An integrity deviation*, i.e. an instrumented safety function as described in the minimum SIL table has been identified, but particular conditions imply a different integrity level requirement. Such a requirement could arise from:
  - a special consideration related to the *frequency* of the associated hazard, e.g.

- a high demand rate[1] on a particular safety function is foreseen or experienced. Identification of a high demand rate may be done in the design phase, e.g. during HAZOP, but would normally result from operational experience (in which case it according to ISO terms, will actually represent a non-conformity, ref. section 4.2). A very high demand rate on a safety function would often represent an operational problem with respect to production availability and as such initiate alternative solutions and/or re-design.
- a high *accumulated* demand rate is foreseen for a particular safety function, e.g. due to a very large number of risers, in which case a higher SIL requirement for the function "isolation of riser" could result.

- a special consideration related to the *consequences* of the associated hazard, e.g. due to concept specific aspects concerning layout, process conditions (pressures, temperatures, fluid characteristics), manning, etc.

Identification of "functional deviations" as defined above may result from HAZOP, flare studies, design reviews or other design activities. Such deviations shall be treated according to IEC 61508 methodology.

With respect to "integrity deviations", the QRA will, as discussed in section 7.6, to some extent verify whether the chosen integrity levels are compatible with the overall acceptable risk level. Consequently, the QRA will represent one means of identifying integrity deviations. Furthermore, such deviations may also be identified through HAZOP analyses, from dedicated reliability analyses, from fire and explosion consequence modelling, etc.

As discussed in section 7.4, the application of analysis techniques like HAZOP and QRA, does not give any guarantee as to whether all potential deviation cases are actually identified. However, in order to minimise the likelihood of disregarding any deviation cases, the important point will be to ensure a consistent approach towards hazard identification and assessment. It has been suggested that if ISO 13702 is properly fulfilled, the methodology described herein facilitates a consistent approach towards such identification. Furthermore, the NORSOK standard Z-013 ("Risk and Emergency Preparedness Analysis") as well as ISO 17776 both represent useful references with respect to hazard identification and assessment.

7.7.2 Required input for handling of deviations

In order to determine the integrity level for a given safety function deviation, the following input is required:

- a description of the EUC and its control system (from section 7.3);
- a description of the condition(s) causing the deviation (from section 7.4);
- a description of the frequency (demand rate) and the consequences of the event(s) (from separate risk analysis);
- a description of additional safety functions available (if any).

Furthermore, a risk acceptance criterion must be defined in order to determine the required risk reduction. Such a risk acceptance criterion would normally be defined by the operator himself. In addition, PSA have in their regulations (ref. the Facilities Regulations, §6 and §9) indicated an acceptable annual frequency for loss of main safety functions such as escape routes, structural integrity and evacuation means.

7.7.3 Determination of SIL for safety function deviations

Both IEC 61508 (part 5) and IEC 61511 (part 3) contain several risk based methods for establishing safety integrity levels. A problem, however, being that the number of methods available is considerable whereas the description of which method to use for which case is limited. Furthermore, and as discussed in section 7.6, experience has proved that the use of e.g. risk graphs may result in non-consistent determination of SIL and also has a limited application for global safety functions.

In appendix C some examples are therefore given on how to handle functional and integrity deviations from the tabulated minimum SIL requirements (please note that the appendix has a limited number of examples). The examples include:

[1] No specific demand rates form the basis for the minimum SIL requirements in Table 7.1. However, in Appendix A some "typical" demand rates for an "average" operation are given and can be used as a basis unless more project specific information is available. If, for some reason, the demand rate is foreseen to be significantly higher (i.e. a factor 5 or more) than these typical demand rates, then the overall risk is likely to be higher than average and this should trigger a re-evaluation of the integrity requirement.

- A quantitative method for establishing SIL requirements for topside and subsea HIPPS systems (ref. Appendix C.2, example 1 and 2 respectively);
- Quantitative risk assessment for establishing requirements for isolation against wells/pipelines (ref. Appendix C.3, example 3).

Regardless of which method is chosen for determination of SIL, the crucial point will be that the process for arriving at the specific integrity requirement is properly documented.

7.8 Safety Requirements Specification

The Safety Requirement Specification (SRS) shall be established for the safety instrumented systems. The SRS is initially derived from the allocation of safety instrumented functions and from those requirements identified during safety planning. The SRS shall provide a basis for design, and the document shall be further developed and maintained through all lifecycle phases of the SIS.

As the IEC 61508 and IEC 61511 do not focus on safety functions related to systems based on “other technologies” or “external risk reduction”, these safety systems will only be briefly mentioned in the SRS. However, it is important that these systems are included in the overall safety plan for the installation.

Main content of the SRS will be quantitative safety integrity requirements as well as functional requirements (such as capacities and response times). For further discussion of SRS content, reference is made to IEC 61511-1, chapter 10.3 and to appendix E which includes a proposed structure and list of content for the SRS.

8 SIS Design and Engineering

8.1 Objectives

This section covers the SIS realisation phase, i.e. box 4 in Figure 2.2 or box 9 in figure 2.3. The objective of the realisation phase is to create SIS conforming to the Safety Requirements Specification (ref. section 7.8). Of special relevance to the realisation phase are part 2 and 3 of IEC 61508 and clauses 11, 12 and 13 from IEC 61511-1. An overview of the different activities in the realisation phase is described in IEC 61508-2, Table 1 and IEC 61508-3, Table 1.

Realisation of safety related systems other than SIS, is not covered by IEC 61508 or IEC 61511, and is therefore not included in this document.

8.2 Organisation and resources

Typically, the realisation phase involves a number of vendors. Hence, the work will normally be split between engineering contractors, system suppliers, control system vendors, field equipment vendors, etc., with the subsequent possibility of ambiguous responsibilities. It is therefore important that an organisation or a responsible person is identified for each phase of the SIS safety lifecycle (ref. figure 2 and 3 of IEC 61508-3). Furthermore, continuity of key personnel must be ensured. As a minimum, such persons must be available all through the phase they are responsible for.

For further requirements, reference is made to section 5.2.

8.3 Planning

IEC 61508 requires that plans are made for each phase of the SIS safety lifecycle and the software safety lifecycle, and also that each phase shall be verified.

In order to ensure that the SIS meets, in all respects, the Safety Requirement Specification, a SIS validation shall be performed after integration (ref. Figure 8.1 below and Figure 2 in IEC 61508-2). However, since validation is planned only at this stage, it would most probably result in several non-conformities, unless the results from each of the intermittent phases (ref. Figure 8.1) have been checked. It is therefore important that a verification activity runs in parallel throughout the entire design phase, e.g. during the detailing of specifications, as these specifications will contain elements that cannot be verified by the higher-level documents. In particular, the verification team members should participate in safety related design review activities like HAZOP.

A plan shall be made to organise the SIS validation and verification activities necessary to demonstrate that the SIS will fulfil all safety requirements. For each phase the result shall be verified. See figure 8.1 below (V-model).

SIS development is part of the overall control and safety system development. Due to the complexity of this package, the detailed planning is not contained in the master plan for the project development. Rather, it is contained as a sub-plan of the master plan. The plan for commissioning is handled in the same way. Planning of operations and maintenance is usually outside the master plan, and is handled by a separate organisation.

The validation/ verification activities, HAZOP, technical reviews or tests can either be listed directly in the SIS-plan, or they may be included in other documents, e.g. in the QA plan.

By nature, testing is usually the best verification/validation method for safety instrumented systems. A test shall be performed according to predefined procedures, the scope of which will be to describe the various test steps and the method applied in order to ensure reproducible test results.

Hence, the “safety validation plan” according to IEC 61508, will be covered by two separate types of documents:

- SIS progress plan or QA plan, with validation / verification activities;
- Test procedure.

The plan shall define:
- The SIS validation and the verification activities;
- At which time the activities will take place;
- The procedures to be used for verification;
- The responsible part for these activities; a separate person, or a separate organisation, and the required level of independence;
- References from the validation activity to relevant test procedures.

The test procedure shall contain:
- Description of test set-up;
- Environmental requirements;
- Test strategy;
- Who shall perform the tests, and the required presence of assessors;
- Test steps necessary to verify all safety requirements listed;
- Test steps necessary to verify correct operation during various modes of operation and/or abnormal conditions;
- Defined fail / pass criteria for the various tests.

The status and progress of the tests shall be available for inspection and all test results shall be properly documented.

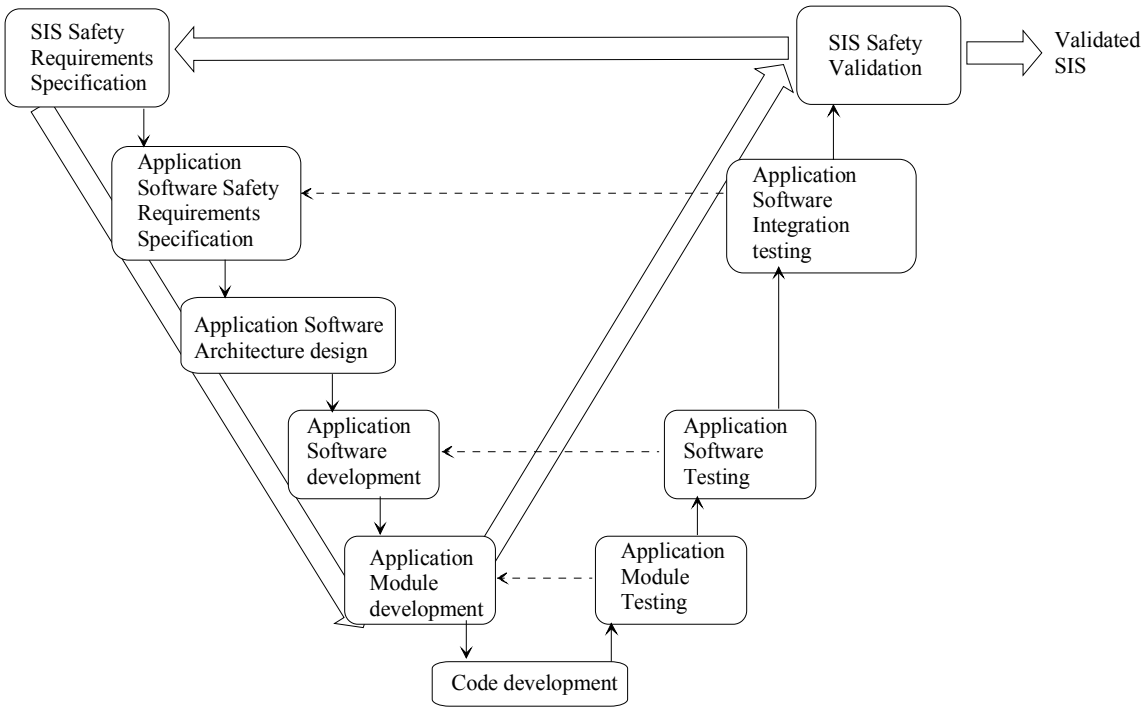

Figure 8.1 V-model for Verification and Validation (from 61511-1, figure 12)

8.4 Input

The SRS documents will provide the design basis for required Safety Instrumented Systems. Vendors and subcontractors shall verify that assumptions specified in the SRS are in complete agreement with their products' specification. Operational, functional and environmental limitations related to different subsystems/components which do not satisfies the SRS requirements shall be identified and brought to the attention of the main contractor and customers.

8.5 Requirements

8.5.1 SIL requirements

For safety functions implemented through SIS technology, there are three main types of requirements that all have to 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, according to Table 8.1 below;
- A qualitative requirement, expressed in terms of architectural constraints on the subsystems constituting the safety function, ref. Table 8.2 or 8.3 below;
- Requirements concerning which techniques and measures should be used to avoid and control systematic faults.

Below, these three types of requirements are briefly discussed.

Quantitative requirements
IEC 61508 applies both to systems operating 'on demand' as well as to systems operating continuously in order to maintain a safe state. An example of a demand mode system would be the ESD system, whereas the process control system for an unstable process like an exothermic reactor will represent a continuous mode system.

In Table 8.1 the relationship between the SIL and the required failure probability is shown.

Table 8.1 Safety integrity levels for safety functions operating on demand or in a continuous demand mode from IEC 61508-1, Table 2 and 3)

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)
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 $< 10^{-5}$

IEC 61508 requires that a quantitative analysis is performed in order to verify that the required failure probability can be achieved for the safety function. Such analysis shall include random hardware failures, common cause failures, and if relevant, failures of any data communication systems used to support the safety function (e.g. Field bus).

It should be noted that the SIL requirement applies to a complete function, i.e. the field sensor, the logic solver and the final element. A separate component can 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 must be verified for the complete function.

Architectural requirements
Architectural constraints on hardware safety integrity are given in terms of three parameters

- the hardware fault tolerance of the subsystem (HFT);
- the safe failure fraction (SFF), i.e. the fraction of failures which can be considered "safe" because they are detected by diagnostic tests or do not cause loss of the safety function, ref. appendix D;
- whether the subsystem is of "A-type" or "B-type". For type A subsystems all possible failure modes can be determined for all constituent components, whereas for type B subsystems the behaviour under fault conditions cannot be completely determined for at least one component (e.g. a logic solver).

For further details, reference is made to IEC 61508-2, sub clause 7.4. The architectural requirements for different safety integrity levels are given in Table 8.2 and 8.3 below.

Table 8.2 Hardware safety integrity: architectural constraints on type A safety-related subsystems (IEC 61508-2, Table 2)

Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - 90 %	SIL2	SIL3	SIL4
90 % - 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

Table 8.3 Hardware safety integrity: architectural constraints on type B safety-related subsystems (IEC 61508-2, Table 3)

Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60 %	not allowed	SIL1	SIL2
60 % - 90 %	SIL1	SIL2	SIL3
90 % - 99 %	SIL2	SIL3	SIL4
> 99 %	SIL3	SIL4	SIL4

NOTES:
1. This document considers programmable logic solvers to be of type B components according to the standard;
2. Systems that are verified and documented to have a certain diagnostic coverage factor and that have the ability to enter degraded mode of operation in a controlled way will have an extra D in their architecture designation code (e.g., 1oo2D).
3. It should be noted that the 'hardware safety integrity' provides the maximum integrity level that is permitted to be claimed even though, in some cases, a higher safety integrity level could derive from solely mathematical reliability calculations (ref. IEC 61508-2, sub clause 7.4.3.1.1).

Avoidance and control of systematic faults

Systematic faults are faults in hardware and software introduced during specification, design, operation or maintenance/testing, which may result in a failure of the safety function under certain conditions (e.g. for particular input signal states). In IEC 61508/61511 such failures are, unlike random hardware failures, not quantified. The approach of IEC 61508 is to recommend that certain measures and techniques are adopted to avoid and control such failures. These measures and techniques shall be adopted during the design phase and are graded according to the SIL requirements. For details on these methods, reference is made to IEC 61508-2 for hardware and IEC 61508-3 for software.

In the PDS – projects (Norwegian: "pålitelighet av datamaskinbaserte sikkerhetssystemer"), it was well documented that systematic failures constitute a major contributor towards unavailability of safety functions, e.g.

- insufficient functional test procedure;
- human error during functional test (e.g. leave in by-pass);
- failure due to software error.

Even if systematic failures are difficult to quantify, the PDS data handbook ("Reliability Data for Control and Safety Systems – 2003 Edition") provides generic values, and also a method for obtaining plant specific values for gas detectors. Thus, leaving out systematic failures from the analysis would seem as a "step backwards" as compared to what was obtained in the PDS projects. Furthermore, since the PFD figures for the safety functions will be used as input to the QRA, it is important that these figures are as realistic as possible. I.e. in the QRA systematic failures must be added in order to give a realistic figure of the SIS performance (ref. Appendix A and Appendix D).

In conclusion, it is recommended to consider using the PDS method in favour of the calculation method described in IEC 61508, since the PDS method quantifies both safety unavailability caused by systematic failures and random hardware failure. For a more detailed discussion of this topic, reference is made to Appendix D.

8.5.2 Requirements to Failure Data

Relevant failure data for the components in the safety function shall be used when the probability of failure on demand (PFD) is calculated. The failure data shall be properly documented, and the assumptions for the data shall be given. Reference is also made to section 8.6 regarding selection of components based on prior use.

Both the failure rate for Dangerous Undetectable failures (λ_{DU}) and the total failure rate (λ_{TOT}) or SFF shall be given. Note that λ_{TOT} shall only include critical failures, i.e. failures that affect the safety function. If relevant, also parameters used for assessing common mode/common cause failures (e.g. β-factors) shall be included and documented as part of the failure data.

Failure data may be obtained in three different ways, or a combination of these:

- Experience data from same or similar applications:
  - The data must be based on components that are used under similar environmental and operating conditions, and the design of the components must be identical.
  - For this type of failure data source the number of performed tests of the relevant safety function shall be given together with how many of these functional tests that resulted in failure. Further, the time interval between these functional tests shall be given. If the data is collected from several sources, it is preferred that this information is given per data source.
  - The PFD and λ_{DU} estimates shall be conservative (IEC 61508 requires that any failure rate data used shall have a statistical confidence level of at least 70%).
  - It is not sufficient to know the operating time of the component/s, the basis for the failure data estimation should be as given above.
  - If the experience data is based on tests in the laboratory, the tests must reflect the relevant operating conditions and demands of the actual safety function. E.g. stroke tests of valves according to API do not reflect this.
  - Some further information relevant for this topic is given in Appendix F.

- Third party certificate or similar:
  All requirements and assumptions relevant for the certificate must be documented. Thus, in addition to the certificate itself, the documentation must also include the background information (assessment report or similar).

- Assessment of the component/system based on failure data from generic sources:
  The assessment must be properly documented through a Failure Mode and Effects Analysis (FMEA) or equivalent. Note that the assessed component/system must have the same type of use, the same safe state and the same design with respect to safe state (i.e. NE-normally energized vs. NDE-normally de-energized). Further, if the assessment is based on MIL-HDBK predictions or similar, all necessary parameters (e.g. environment and quality) must be relevant for the current application, and shall be stated as part of the documentation.

8.5.3 Subsystem interface

The subsystems of a safety function implemented through SIS, need a proper definition with respect to the interface between the initiator subsystem and the logic solver as well as between the logic solver and the final element. Such definitions are needed due to the requirements and methods for design and calculation of the individual safety functions.

The definitions given in IEC 61508 might, however, result in different interpretations. In order to simplify and to provide a general understanding, the interfaces towards the logic solver are defined to be on the termination devices that belong as an integrated part of the programmable controller equipment.

The physical interface might differ depending on the type of equipment, the important point being that it is always defined.

8.5.4 Field Sensor

Type
When selecting an input device (field sensor) for a SIS with a given SIL requirement, this should be performed in accordance with the requirements laid down in IEC 61511-1, clause 11. Here, it is defined that any component can be used, certified or not, as long as it fulfils the requirements for documented reliability (ref. section 8.5.2 and 8.6).

Separate field sensors for shutdown
Field sensors used in a SIS function shall be separate and independent from other field devices and dedicated to SIS duty only.

Line monitoring of normally de-energised input signal
For special applications requiring energise to trip shutdown actions, all field devices and the power supply must be equipped with monitoring facilities. The requirement for a shutdown must be considered for each case separately.

Mounting considerations
Attention must be given to the mounting of field sensors in order to avoid accidental isolation, common mode failures due to freezing/clogging, etc. Similarly, consideration must be given to the location of sensors with respect to any shut-off valves, in order to monitor the correct pressures as well as being able to reset the system safely.

Integral testing facilities, full or partial testing
SIL classified systems are frequently subject to strict testing requirements. Hence, it is important to include facilities for both full and partial testing. The testing can be performed for a separate element or part of the loop, but will normally have to be performed for the complete loop from sensor to final element within some predefined interval. It must be possible to reset the system after testing, which has an impact on location of the sensors (see above point).

Comparison between sensors

Most relevant here will be to compare readings from sensors in the safety systems with readings from sensors in the process control system (PCS). This measure is in IEC 61508 -7, A.12 referred to as "reference sensor". In table A.14 in IEC 61508-2 it is specified that the maximum allowable credit that can be given for a "reference sensor" is "high" (i.e. 99% diagnostic coverage), and it is stated that it "Depends on diagnostic coverage of failure detection."

Further, Appendix C in IEC 61508-2 specifies how analyses shall be performed for each sub-system to calculate its diagnostic coverage (DC). This involves e.g. performing a FMECA to determine the effect of each failure mode for all (group of) components.

The following comments apply when transmitter DC is increased by giving credit to comparison with PCS:

- It is particularly important to investigate sources of common cause failures (CCF) between PCS transmitter and safety system transmitters. Both random hardware failures and systematic failures may cause PCS to be "unavailable for a true comparison". In particular, the beta factor for transmitters, e.g. β=0.02 (for random hardware failures) and the probability of systematic failures (for PCS transmitter alone), say PSF $\approx 5 \cdot 10^{-4}$, will impose restrictions in the choice of DC. Furthermore, the failure rate of the PCS itself will limit the reliability of the comparison function;
- Unless detailed analyses are performed, it is therefore suggested that the maximum credit given for such comparison should be DC = 90%;
- As described in Appendix C of IEC 61508-2, detailed analyses of failure modes are required in order to increase the coverage. This analysis should focus on CCFs, e.g. common testing/maintenance, common component vendor/type, common impulse line, etc. If such a detailed analysis is performed, the coverage can be increased beyond 90%. It is, however, suggested that that the maximum credit given for comparison should be DC = 97% (thus allowing for common cause failures to be somewhat higher than 2% in the actual application).
- In order to take credit for comparison between safety system transmitters and transmitters in the PCS, it is as a minimum required that a discrepancy automatically generates an alarm. The comparison algorithm shall be implemented in the logic solver of the control system and not in the safety system. The discrepancy alarm threshold shall be set commensurate with a documented acceptable deviation of the primary variable

8.5.5 Logic Solver

Logic Solver Equipment
The logic solver equipment constitutes the basic components from which the safety applications are built:

- framework, racks, cabinets;
- processor/memory boards;
- communication boards;
- I/O boards;
- termination units;
- power supplies;
- system software;
- application software libraries;
- application programming tools;
- communication protocols;
- human/system interfaces.

Logic solver compliance with IEC 61508 shall be documented. A Safety Users Manual shall be made and shall provide instructions on how to use the actual equipment in order to build safety applications that comply with IEC61508.

Hardware application
Normally, control signals from initiator and final element are interfaced to a central processing unit, either via discrete I/O channels or via communication links.

When designing the logic solver architecture, the following should be taken into account:

- A safety user design manual should exist which describes how non-certified equipment shall be used in safety critical applications. For certified equipment this is normally available as part of the certification;
- Appropriate designated architecture must be selected for the central processing unit. As a minimum, the selected architecture shall meet the highest SIL level of the relevant safety functions;
- If possible, the architecture of the I/O and interface modules should be selected individually for each safety function;
- For non-certified equipment PFD calculations shall be performed to show that the contribution from the logic solver is within acceptable limits;
- For certified equipment the maximum contribution to the PFD figure is normally part of the certification report and is therefore available as pre-calculated and verified parameters;

Software application
For development of application software, this document suggests a V-model (ref. Figure 8.1), comprising:

- application software specification;
- cause & effect overview plan;
- individual safety function specification;
- written description;
- associated tag list;
- logic specification;
- timing requirements;
- safety response time;
- logic delay times;
- safety thresholds and limits;
- bypass requirements;
- alarm, log and event treatment specification;
- application software verification plan;
- application software design specification;
- structure;
- modularization;
- application software module test specification;
- application software integration test specification.

Furthermore:

- A safety user-programming manual should exist which describes how non-certified equipment shall be used in safety critical applications. For certified equipment this is normally available as part of the certification;
- Programming languages based on configuration and parameterisation of standardised functions should be used. Use of languages of type-structured text etc. should be avoided;
- Attention should be paid to the activity of loading/dumping/reloading of application software. This is normally achieved by a serial communication protocol. For non-certified systems special attention should be paid to this protocol regarding safe communication. For certified systems these activities are verified and documented as part of the certification.

8.5.6 Final element

Type
Final elements can be valves (also quick shut-off or quick opening valves), circuit breakers, fire doors or dampers, etc. Each individual application should be considered on its own merits and the most suitable type of final element should be chosen for that specific application.

Architecture
As for field sensing elements, the architecture is both dependant upon the SIL requirements, but also on the type and quality of the components used, as well as regularity requirements imposed (ref. IEC61511-1, clause 11).

Control panel design
For very critical safety functions it should be considered to keep the valve control panel lockable in order to avoid inadvertent or unauthorised operation of the solenoid valves.

Partial stroke testing (PST)
For valves, partial operation with feedback on movement can be applied to reduce manual testing activities. PST shall normally be treated as a functional test which covers only a fraction of the possible failures, and not as self test with diagnostic coverage. The fraction detected shall be properly documented through an FMECA or similar.

8.5.7 Utilities

Type of utility
By utilities is understood the power and driving forces required for a system to operate correctly. This can be electrical power / UPS, hydraulic power, air supply, batteries, seawater batteries, etc. These supplies will affect the system with respect to availability, and possibly safety. In case of fail safe design, then a loss of power will cause the system to go to a safe position. However, if this happens on a regular basis, then the risk of operator forced inputs or outputs to avoid frequent trips will increase, and the safety function may not be fulfilled. If the safety function is not fail safe, redundancy, diagnostics and alarm to control room is required. All parts of a SIS, including the utility systems, must be tested periodically.

Supply lines/tubes/pipes
Lines must be sized in order to ensure sufficient capacity to open and close the valves. The tubing must be protected from mechanical damage where required (falling loads).

Redundancy of supplies
If the safety function implemented through SIS has redundancy in one or more components, it should be considered whether redundant power supply is also required for safety reasons. The design inside the control panel should ensure that redundancy is carried forward through the racks/cards where these are redundant.

Cabling
In fail-safe design, cabling and other passive components in the loop will normally not contribute. For NDE loops and active components, all relevant failures shall be assessed by a FMECA or similar.

8.5.8 Integration

All the various components must be installed in the correct manner, the architecture must be correct and the documentation must be complete and in accordance with the requirements.

It is the responsibility of the system integrator to ensure that all requirements are fulfilled.

8.6 Selection of components

Appropriate evidence shall be available to document that the components and sub-systems are suitable for use in the safety instrumented system. The level of details of the evidence should be in accordance with the complexity of the considered component or sub-system and with the probability of failure claimed to achieve the required safety integrity level of the safety instrumented function(s).

The evidence of suitability shall include the following:

- consideration of the manufacturer's quality management and configuration management systems;
- adequate identification and specification of the components or sub-systems;
- demonstration of the performance of the components or sub-systems in similar operating profiles and physical environments;
- the volume of the operating experience.

If a component can be documented as one of the following,

- "proven in use" in compliance with requirements in IEC 61508-2 clause 7.4.7.6 - 7.4.7.12,
- "prior use" can be claimed as described in IEC61511-1, clause 11.5,
- the component is "low complexity" in accordance with definition in IEC61508-4, clause 3.4.4 and dependable field experience exists (ref. IEC61508-1, clause 4.2),

the formal requirements to component documentation can be reduced. This is further described in figure E.2 in Appendix E.

8.7 HMI – Human Machine Interface

The HMI can include several elements in a single or combined/redundant arrangement, i.e. VDU operator stations, electronic operator panels or operator panels made with pushbuttons, switches and lamp - / LED elements.

Means for human machine interfaces of any SIS may be realised within dedicated safety facilities or within a common HMI arrangement. In either case, any failure of the HMI shall not adversely affect the ability of the SIS to perform its safety functions.

For some cases (as those described below), the SIL requirements relevant to SIF shall be assessed and will become applicable for the SIF related facilities of the HMI:

- When the final function of the instrumented safety loop is to alarm the operator and operator response is required as a part of total safety function: An adequate alarm function, ensuring operator warning, shall be provided in compliance with the SIL requirements of the SIF.
- When operator action is the initiating element in the safety function: An adequate alarm, ensuring operator warning, and action function shall be provided in compliance with the SIL requirements of the SIF.
- When the operator by manual intervention can prevent the action of the safety function, i.e. Blocking: The monitoring function (i.e. blocking present), the display function (i.e. notify the operator) and the remove function (i.e. remove all blockings) must be provided with a PFD contribution that does not compromise the total SIL of the SIF.

All bypasses, overrides and inhibits of a SIL classified system must be alarmed/notified to the operators in the control room. This can be done via the control system, and does not have to be hardwired, as the safety functions themselves should work independently of all other systems. All SIL system override facilities should be carefully considered with respect to:

- the need for restricted access, e.g. password protection
- facilities for automatic recording of any overrides/bypasses
- definition of an upper limit for allowed override time depending on the SIL class

- whether to include override timers to limit the test time available and to ensure that no overrides are forgotten

For SIL 3 functions it should be considered to remove the capability of overriding the function if this is considered feasible.

Reference is also made to Appendix G. For details regarding alarms to be presented in various scenarios, please refer to PSA guideline YA-711 “Principles for alarm system design” and NORSOK Standard I-002 “Safety and Automation System (SAS)”.

8.8 Independence between safety systems

To fulfil the requirements of the PSA and IEC 61508/61511 concerning independences between safety systems (i.e. a failure in one systems shall not adversely affect the intended safety function of another system), no communication or interaction shall occur from the PCS system to any safety system, from the PSD system to ESD, or from the PSD system to F&G. Special measures shall be implemented to avoid adverse effects between SIS and non SIS systems and applications, and between SIS nodes. If special measures are implemented, a limited degree of interconnection can be allowed. Such special measures together with examples of unacceptable and conditionally acceptable solutions are given in Appendix G.

8.9 Factory Acceptance Test (FAT)

The term Factory Acceptance Test (FAT) is not explicitly used in IEC 61508, but is described in IEC 61511-1, informative clause 13.

Objective
The objective of a FAT is to test the logic solver and associated software together to ensure that it satisfies the requirements defined in the Safety Requirement Specification. By testing the logic solver and associated software prior to installation, errors can be readily identified and corrected (IEC 61511-1, sub-clause 13.1.1).

The software validation shall confirm that all of the specified software safety requirements are correctly performed. Further, it shall be verified that the software does not jeopardise the safety requirements under SIS fault conditions and in degraded modes of operation or by executing software functionality not defined in the specification.

Recommendations
The need for a FAT should be specified during the design phase of a project. The planning of FAT should specify the following:

- types of test to be performed;
- test cases, test description and test data;
- dependence on other systems/interfaces;
- test environment and tools;
- logic solver configuration;
- criteria for acceptance of test;
- procedures for corrective actions in case of failure of the test;
- test personnel competencies;
- location of test.

For each FAT, the following should be addressed

- the version of the test plan being used;
- specification of the test object;
- a chronological record of the test activities;
- the tools, equipment and interfaces used.

FAT Documentation.

The FAT documentation is a part of the overall safety system documentation and should according to IEC 61511-1 contain (1) the test cases, (2) the test results, and (3) whether the objectives and the test criteria have been met. If there is a failure during the test, the cause should be documented, analysed and corrective actions proposed.

8.10 Documentation from design phase

The documentation developed should reflect the different phases of the system lifecycle. The documentation and its structure could resemble that shown in Figure 8.3 below (the figure originates from one specific system supplier and will therefore not be complete with respect to all different documentation from the design phase).

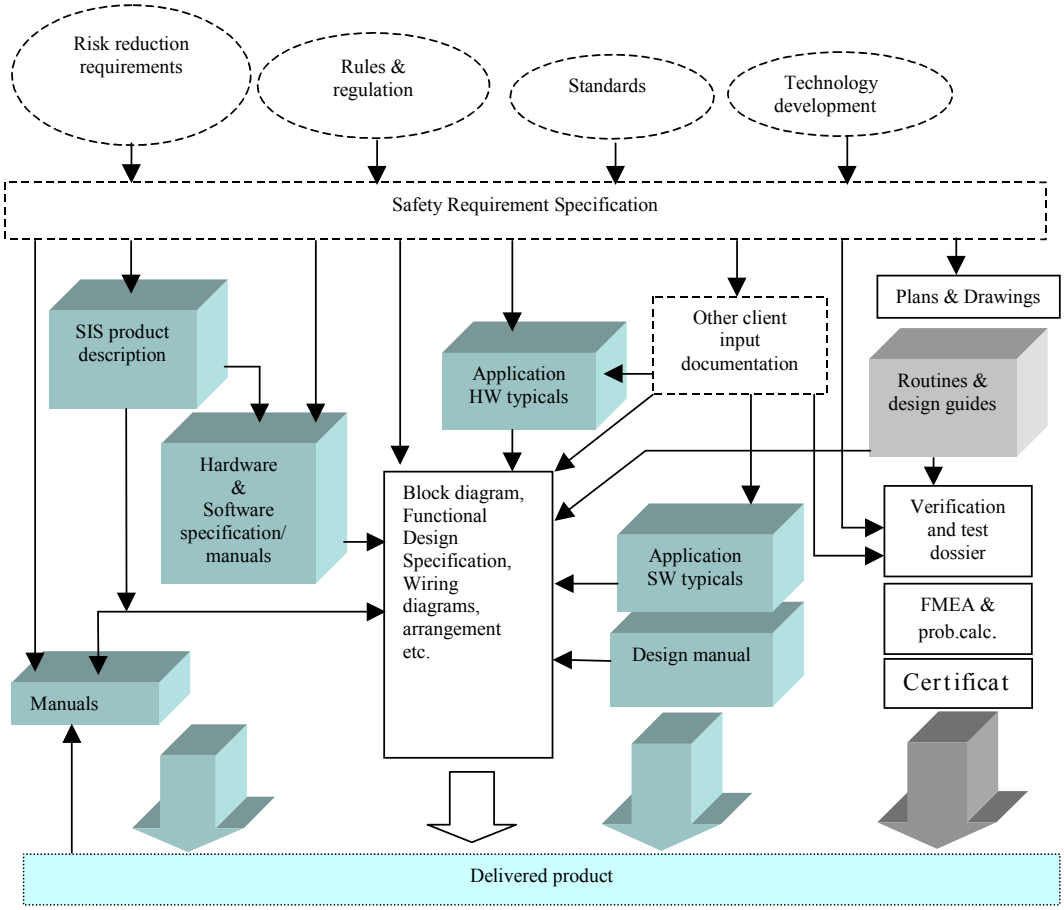

Figure 8.3 Example of possible document structure

The "Verification and test dossier" contains all documentation describing tests to be performed on system components, including a document describing verification for the complete system throughout the SIS-lifecycle.

A Safety Analysis Report should be part of the phase documentation and should include:

- System description;
- System Topology and Block diagram;
- Operational description of the system;
- Failure rate of the components;
- Recommended time interval between functional testing;
- Mean Time to Repair (MTTR);
- Diagnostic coverage;
- Voting;
- Common cause failures;
- Behaviour of system on detection of a fault
- Avoidance and control of systematic failures

- if relevant; PFD calculations

For further discussion of the Safety Analysis Report content and structure, reference is made to Appendix E.

9 SIS INSTALLATION, MECHANICAL COMPLETION AND VALIDATION

9.1 Objectives

The objectives related to the requirements in this chapter are to:

- install the SIS according to specifications and drawings;
- perform mechanical completion of the SIS so that it is ready for final system validation;
- validate, through inspection and testing, that the installed and mechanical complete SIS and its associated safety instrumented functions, do achieve the requirements as stated in the SRS.

9.2 Personnel and competence

Personnel, departments, organisations or other units which are responsible for carrying out and reviewing the SIS installation, mechanical completion and validation phase, shall be identified and be informed of the responsibilities assigned to them (including where relevant, licensing authorities or safety regulatory bodies).

For further requirements, reference is made to section 5.2.

9.3 Requirements

9.3.1 Installation and mechanical completion planning

Installation and mechanical completion planning shall define all activities required for installation and mechanical completion. This includes:

- the installation and mechanical completion activities;
- the procedures, measures and techniques to be used for installation and mechanical completion;
- the time at which these activities shall take place;
- the personnel, departments and organisations responsible for these activities.

Installation and mechanical completion planning shall verify the procedures for handling non-conformities where the actual installation does not conform to the design information established.

9.3.2 Installation

All safety instrumented system components shall be properly installed per the design and installation plan(s).

9.3.3 Mechanical completion

Mechanical completion encompasses all activities ensuring that all fabrication and installation work has been performed according to the requirements of the project specifications, the design drawings and as defined through other contract documents, and that the relevant subsystems/systems or installations are ready for commissioning.

Appropriate records of the mechanical completion of the SIS shall be produced, stating the test results and whether the objectives and criteria identified during the design phase have been met. If there is a failure, the reasons for the failure shall be recorded.

If it has been revealed that the actual installation does not conform to the design information, this non-conformity shall be evaluated by a competent person (ref. section 5.2.2), and the likely impact on safety determined. If it is found that the non-conformity has no impact on safety, then the design information shall be updated to as built status. Otherwise, the installation shall be modified to meet the design requirements.

9.3.4 SIS safety validation planning

Validation planning of the SIS should define all activities required for validation. The following items shall be included:

- the validation activities, including validation of the SIS with respect to the safety requirements specification and implementation and resolution of resulting recommendations;
- validation of all relevant modes of operation of the process and its associated equipment including:

  - preparation for use including setting and adjustment;
  - start-up, teach, automatic, manual, semi-automatic and steady state of operation;
  - re-setting, shut down and maintenance;
  - reasonably foreseeable abnormal conditions.
- the procedures, measures and techniques to be used for validation;
- reference to information against which the validation shall be carried out (e.g., cause and effect chart, system control diagrams).
- when the activities shall take place;
- the persons, departments and organisations responsible for the activities and levels of independence for validation activities;

Additional validation planning for the safety application software shall include the following:

a) Identification of the safety-related software which needs to be validated for each mode of process operation before commissioning commences;

b) Information on the technical strategy for the validation including;
  - manual and automated techniques;
  - static and dynamic techniques;
  - analytical and statistical techniques.

c) In accordance with (b), the measures (techniques) and procedures that shall be used for confirming that each safety instrumented function conforms with (1) the specified requirements for the software safety instrumented functions, and (2) the specified requirements for software safety integrity;

d) The required environment in which the validation activities are to take place (for example for tests this would include calibrated tools and equipment);

e) The pass/fall criteria for accomplishing software validation including;
  - the required process and operator input signals with their sequences and their values;
  - the anticipated output signals with their sequences and their values;
  - other acceptance criteria, for example memory usage, timing and value tolerances.

f) The policies and procedures for evaluating the results of the validation, particularly failures.

9.3.5 SIS safety validation

SIS safety validation is here defined as all activities necessary to validate that the installed and mechanical completed SIS and its associated instrumented functions, meets the requirements as stated in the Safety Requirement Specification.

Where measurement accuracy is required as part of the validation, then instruments used for this function must be calibrated against a specification traceable to a national standard or to the manufacturer's specification.

Validation activities shall as a minimum confirm that:

- the safety instrumented system performs under normal and abnormal operating modes (e.g., start-up, shutdown, etc.) as identified in the Safety Requirement Specification;
- adverse interaction with the basic process control system and other connected systems do not affect the proper operation of the safety instrumented system;
- the safety instrumented system properly communicates (where required) with the basic process control system or any other system or network;
- sensors, logic solver, and final elements perform in accordance with the safety requirement specification, including all redundant channels;
- safety instrumented system documentation reflects the installed system;
- the safety instrumented function performs as specified on bad (e.g., out of range) process variables;
- the proper shutdown sequence is activated;
- the safety instrumented system provides the proper annunciation and proper operation display;
- computations that are included in the safety instrumented system are correct;
- the safety instrumented system reset functions perform as defined in the safety requirement specification;

- bypass functions operate correctly;
- manual shutdown systems operate correctly;
- the proof test intervals are documented in the maintenance procedures;
- diagnostic alarm functions perform as required;
- the safety instrumented system performs as required on loss of power or a failure of a power supply and confirm that when power is restored, the safety instrumented system returns to the desired state.

Prior to using the SIS for its intended purpose and after the validation activity is complete, the following activities shall be carried out:

- all bypass functions (e.g., programmable electronic logic solver and sensor forces, disabled alarms) shall be returned to their normal position;
- all process isolation valves shall be set according to the process start-up requirements and procedures;
- all test materials (e.g., fluids) shall be removed;
- a final shutdown test shall be performed

9.3.6 Documentation from SIS safety validation

Appropriate information of the results of the SIS validation shall be produced which provides:

- the version of the SIS validation plan being used;
- the safety instrumented function under test (or analysis), along with the specific reference to the requirements identified during SIS validation planning;
- tools and equipment used, along with calibration data;
- the results of each test;
- the version of the test specification used;
- the criteria for acceptance of the integration tests;
- the version of the SIS being tested;
- any discrepancy between expected and actual results;
- the analyses performed and the decisions taken on whether to continue the test or issue a change request, in the case when discrepancies occur;
- In case of discrepancies between expected and actual results, the analyses performed and the decisions taken shall be available as part of the results of the hardware and software safety validation. Here, it shall be stated whether it was decided to (1) to continue the validation, or (2) to issue a change request and return to an earlier part of the development lifecycle.

10 SIS Operation and Maintenance

10.1 Objective

The objective of this chapter is to describe how the SIS shall be operated and maintained to ensure that it functions in accordance with the Safety Requirement Specification throughout the SIS operational lifetime.

Included in the term operation are all daily routines, including PCS operations and SIS operations required in the SRS, necessary to maintain the specified integrity level.

Maintenance in this context is concerned with ensuring that the SIS does not deteriorate below the specified integrity level. It includes repairs of defective components and replacements with identical units. In addition, functional proof testing and reporting of non-conformities and demands are included. Any modification or design changes made to the SIS, including all software changes, are covered in chapter 11; SIS modifications.

10.2 Operation and maintenance planning

SIS operation and maintenance planning shall be done during the design stage prior to SIS operation. This activity shall include, but not be limited to consideration of the following factors:

- routine and abnormal operational activities;
- preventative and breakdown maintenance activities;
- functional proof testing;
- the application and control of overrides to SIS;
- identification of procedures, routines, measures and techniques to be used during operation and maintenance;
- compensating measures to maintain SIS risk reduction when detecting dangerous failures or overrides, inhibits or disabling of the SIF or part of the SIF;
- verification of adherence to operation and maintenance procedures;
- at which time the activities shall take place;
- the personnel, departments and organisations who will be responsible for these activities;
- the training and competency requirements for staff carrying out the activities relating to operation and maintenance of SIS;
- consideration for differentiation of operations and maintenance practices to reflect the various SIL levels;
- specification of which reliability data that should be collected and analysed during the operational phase.

An overview of the above factors / parameters and their possible implications on different operation and maintenance activities is given in Appendix F.1.

10.3 Operations and Maintenance Procedures

Operation and maintenance routines and procedures shall be available to the extent necessary to ensure that the SIS performs in accordance with the Safety Requirement Specification throughout the lifetime of the installation. These shall be supplemented by descriptions to the extent necessary. Aspects to be address shall include, but not be limited to the following:

- the activities to be carried out in order to maintain the required functional safety of the SIS;
- how the SIS takes the process to a safe state;
- limits of safe operation (i.e. trip points) and the safety implications of exceeding them;
- timing requirements for SIS functions including output devices;
- the correct use of operational or maintenance bypasses, ‘permissives’, system resets, etc. to prevent an unsafe state and/or reduce the consequences of a hazardous event (e.g. when a system needs to be bypassed for testing or maintenance, which compensating measures must be implemented);
- the correct operator response to SIS alarms and trips;
- measures to handle faults or failures occurring in the SIS;

- tracking maintenance performance;
- tracking of activation and failures of the SIS;
- the information which needs to be maintained on system failure and demand rates on the SIS;
- the information which needs to be maintained showing results of audits and tests of the SIS;
- routines for ensuring that test equipment used during normal maintenance activities are properly calibrated and maintained;
- documentation of the above.

10.4 Competence and Training

All activities concerning operation of the SIS shall be performed by competent personnel. Operators shall have the proper competence and training on the function and operation of the SIS. Such competence shall include an understanding of the following issues:

- the general principles of safety integrity levels;
- how the SIS functions (trip points and the resulting action that is taken by the SIS);
- the hazards which the SIS is protecting against;
- the operation and consequences of operation of all bypass switches and under what circumstances these bypasses are to be used and recorded;
- use of compensating measures;
- the operation of any manual shutdown switches and under which conditions these switches are to be activated;
- behaviour upon activation of any diagnostic alarms (e.g., what action shall be taken when any SIS alarm is activated indicating there is a problem with the SIS itself).

Maintenance personnel shall be trained to sustain full functional performance of the SIS (hardware and software) to its targeted integrity. This includes also periods of reduced functionality due to maintenance and testing.

10.5 Maintenance

A maintenance program shall be available, which includes descriptions for maintaining and testing the SIS to maintain the required integrity level. The maintenance routines should also describe compensatory measures required (if any) for the testing to reveal faults that are not automatically detected by the SIS.

SIS maintenance shall include, but not be limited to, the following:

- regularly scheduled functional testing of the SIS;
- regular inspection of field equipment to ensure that there is no observable deterioration, for example: corrosion or mechanical damage, damaged cabling or terminations, ineffective heat tracing, blockage of fire and gas detectors, etc.;
- regularly scheduled preventative maintenance, as required (e.g., replacement of ventilation filters, lubrication, battery replacement, calibration, etc.);
- repair of detected faults, with appropriate testing after repair.

Vendor manuals that describe the different maintenance and testing requirements for sub-systems (e.g., battery maintenance, fuse replacement, etc.) shall be input to the maintenance procedures.

Replacing a SIS component with a new component having different characteristics (including system software upgrades) should be treated as a modification in accordance with chapter 11.

10.5.1 Functional testing

Not all system faults are self-revealing. Hidden failures that may prevent SIS action on demand can only be detected by periodical functional tests. Such tests shall be conducted using documented instructions and descriptions to detect hidden failures that prevent the SIS from operating according to the Safety Requirement Specifications.

Functional testing (Proof test) of the SIS shall reflect the real operating conditions as accurately as possible. Effective SIS proof testing shall confirm the correct operation of the entire SIS loop including sensing element(s), logic solver and the actuating devices.

Functional 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.

Proof testing of the SIS shall preferably be carried out as an integral-test, i.e. the entire SIS loop should be tested together (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 SIS loop. Some sub-systems may be tested under normal operation by providing inhibit of the input signal or override of an output action. Testing of other sub-systems such as e.g. valves often causes process shutdown and may therefore be performed during planned shutdown periods. It should be noted that although partial functional testing reduces the need to fully test the SIS loop, a complete integral test should still be performed at certain intervals.

For those applications where partial functional testing is applied, the 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.

Actual shutdowns during operation may be given credit as fully functional tests under the following conditions:

- the shutdown must document equivalent information as registered during the corresponding described functional test
- the shutdown must cover all equipment covered by the corresponding described functional test, if not, the equipment not covered must be tested separately
- the shutdown must occur within the last half of the current test interval.

If these conditions are fulfilled, the next planned functional test may be skipped. The PFD will, resultantly, be somewhat increased as a result of the extended test interval. However, as shown in Appendix F, the average increase will be limited. Obviously, actual shutdowns can also be used intentionally to decrease the PFD if the next planned test is not omitted.

Observe that the activation of an emergency shutdown valve due to a PSD does not test the entire function as if the valve was activated by ESD.

10.5.2 Maintenance reporting

The user shall maintain records to document that all tests and inspections have been performed.

Documentation, which may be recorded in an electronic maintenance database, shall enable retrieval of the following information:

- date of inspection;

- name of the person who performed the test or inspection;
- serial number or other unique identifier of equipment (loop number, tag number, equipment number, user approved number, etc.);
- results of inspection/test;
- details of any faults found and the corrective action taken, e.g. failure code.

Based on the collected information, it shall be possible to calculate required reliability parameters such as λ_{TOT} and $\lambda_{DU,}$ etc., ref. Appendix F.

10.6 Compensating measures upon overrides and failures

In general it is not allowed to operate with impaired barriers. Necessary actions to correct or compensate the impaired barrier(s) shall be taken (ref. PSA Management Regulations, §2).

10.6.1 Compensating measures procedures

Operation and maintenance planning for the SIS shall address possible compensating measures to maintain SIS risk reduction during the following operating scenarios:

- dangerous detected failures;
- overriding of the SIF or parts of the SIF for functional proof testing or maintenance activities.

Operation and maintenance routines shall take account of the above factors to ensure that the risk level throughout the lifetime of the installation is in accordance with the Safety Requirements Specifications. Aspects to be addressed are (but not limited to):

- the events/operations causing the demand requiring compensating measures;
- the correct use of compensating measures to prevent an unsafe state and/or reduce the consequences of a specified hazardous;
- in which manner the compensating measure brings the process to a safe state;
- the consequence of failure in initiating compensating measure;
- timing requirements for the function.

10.6.2 Dangerous Detected Failure

All failures that are defined as dangerous detected failures in any part of the SIS require manual actions or compensating measures to maintain an acceptable risk level. It is therefore necessary to identify the correct operator response to any diagnostic alarms such as:

- Feedback fault alarms
- Line-monitoring alarms
- Out of range alarms
- Redundancy deviation alarms

10.6.3 Override/Inhibit/Disable

All overriding, inhibiting or disabling of any part of the SIS will impair the ability of the safety function to perform its intended action, and will therefore require manual actions or compensating measures in order to maintain the risk level. It is necessary to identify the correct compensating measure during different activities requiring overriding. Such activities may be (but are not limited to):

- Functional proof testing
- Preventive maintenance activities
- Field equipment malfunction
- Field equipment replacement

A system of controlling, approving, and recording the application of overrides to SIS shall be in place. The cumulative effects of overrides shall be assessed and controlled.

If manual intervention represents the compensating measure during SIS overrides, the available operator response time must be assessed, taking into consideration the foreseen time for revealing the abnormal situation as well as taking correct action.

Consideration should be given to the use of timed overrides. This implies that an override will be automatically re-set after a predetermined interval. Clearly, this requires clear warning of the operator and an option to prolong the override before re-setting, since automatically resetting an override on a system still being worked upon, could represent a risk in itself. However, the use of timed automatic overrides can improve safety as it rules out the possibility of the operator forgetting to reset an override when the compensating measure is removed.

10.7 Reporting of non-conformities and demands

In order to ensure that the SIS is performing in accordance with the design intent and hence the required integrity level, it is necessary to record non-conformities between expected behaviour and actual behaviour of the SIS. These shall be recorded and analysed and where necessary, modifications shall be performed in accordance with Chapter 11 to achieve the required integrity.

The following shall as a minimum be monitored and recorded:

- actions taken following a demand on the system when non-conformities are recorded;
- failures of equipment forming part of the SIS to act on demand;
- failures of equipment with no demand on the system
- failure of equipment forming part of the SIS during routine testing;
- failures of equipment forming part of the compensating measure to act on demand;
- cause of the demands;
- that the frequency of the demands is in accordance with the assumptions made in the original SIL assessment.

Preference should be given to systems that provide automatic recording and reporting of non-conformities during demands on the SIS. See App F3 and F5.

10.8 Continuous improvement of Operation and Maintenance procedures

It is important that the person responsible for the SIS is able to easily extract functional test documentation and installation trip and shutdown reports. The carrying out of audits and statistical analysis on these data are essential to ensure that the SIS is performing and being maintained as intended, and to ensure that the installation is being operated at an acceptable risk level. The assurance that planned testing is carried out on time and as specified, and that any backlogs are investigated and corrective actions taken, is vital for ensuring the performance of the SIS.

Operation and maintenance procedures should be regularly reviewed in the light of discrepancies found during functional safety audits or as a result of non-conformances reports.

At some periodic interval (determined by the user), the frequency of testing for the SIS or portions of the SIS shall be re-evaluated based on historical data, installation experience, hardware degradation, software reliability, etc. Change of interval shall be handled as a modification. For further details reference is made to Appendix F.5.

Any change to the application logic including adjustment of thresholds, timers, filters etc. shall be treated as a modification in accordance with chapter 11.

11 SIS Modification

Modifications are defined as any changes to the SIS other than those defined in chapter 10; SIS operation and maintenance.

11.1 Objective of Management Of Change (MOC)

The objectives of the requirements of this sub-clause are:

- to ensure that modifications to any safety instrumented system are properly planned; reviewed and approved prior to making the change;
- to ensure that the required safety integrity of the SIS is maintained due to any changes made to the SIS.

11.2 MOC procedure

A written procedure shall be in place to initiate, review, approve and execute changes to the SIS other than "replacement in kind". The MOC procedure could be required as a result of modifications in the following areas:

- component(s) with different characteristics;
- new proof test interval or procedures;
- changed set-point due to changes in operating conditions;
- changes in operating procedures;
- a new or amended safety legislation;
- modified process conditions;
- changes to the Safety Requirement Specifications;
- a correction of software or firmware errors;
- correction of systematic failures;
- as a result of a failure rate higher than desired;
- due to increased demand rate on the SIS;
- software (embedded utility, application).

The MOC procedure shall include an impact analysis to ensure that the following considerations are addressed prior to any change:

- the technical basis for the proposed change;
- the general impact of change on safety and health;
- the impact of change on other EUCs;
- modifications of operating procedures;
- necessary time period for the change;
- authorisation requirements for the proposed change;
- availability of memory space;
- effect on response time;
- on-line versus off-line change, and the risks involved.

The review of the change shall ensure that:

- the required safety integrity has been maintained; and
- personnel from appropriate disciplines have been included in the review process.

Personnel affected by the change shall be informed and trained prior to implementation of the change or start-up of the process, as appropriate.

In principle, all changes to the SIS shall initiate a return to the appropriate phase (first phase affected by the modification) of the safety lifecycle. All subsequent safety lifecycle phases shall then be carried out, including appropriate verification that the change has been carried out correctly and documented. Implementation of all changes (including application software) shall adhere to the previously established SIS design procedures.

Deviations from the above are allowed for limited software changes in existing SIS, provided the impact analysis identifies appropriate review activities and partial testing required to ensure that the SIL has not been compromised. This shall also apply to system software upgrades through the safety lifecycle.

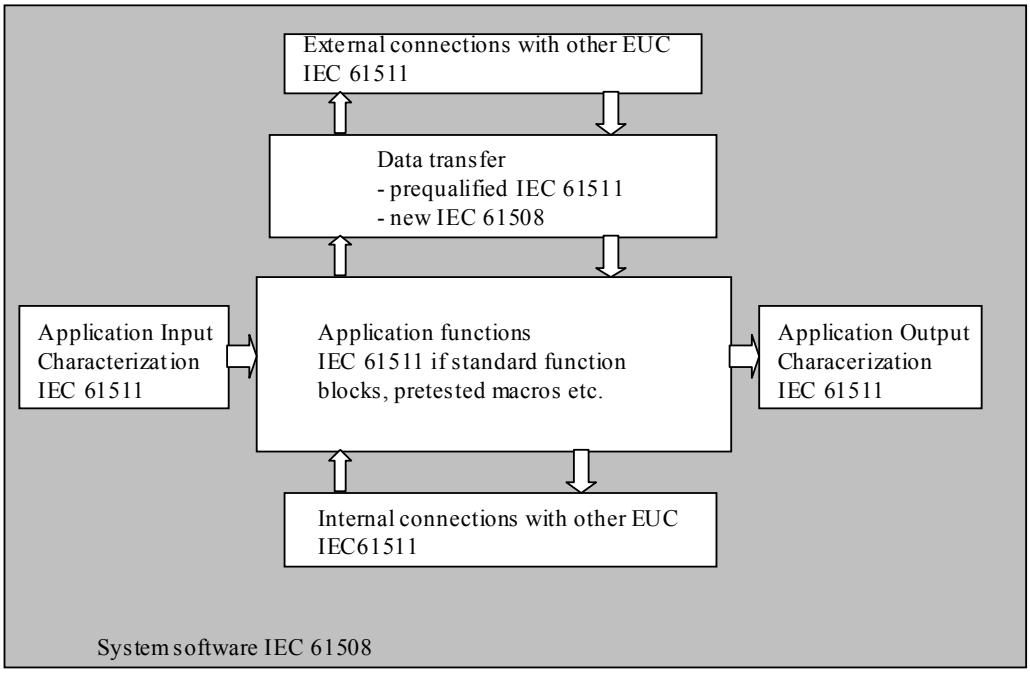

Figure 11.1 Software relationships

The impact analysis for exceptional software modifications shall, as a minimum, document analysis of the items described in the following table and define the appropriate method of achieving the recommended level of verification/validation (R = review, PT = partial testing):

Impact analysis shall document the effect on:	Upgraded system Software	New EUC	Modified EUC (Field equipment)	Modified function (App. programmes C&E, pre-tested macros etc.)	Characterizations (Application Thresholds, spans, timers, filters etc.)
Existing equipment under control (process)	R		PT	PT	PT
Existing related equipment under control (process)	R	PT	R	R	R
Existing related equipment under control (functional) e.g. software interfaces logic to logic, controller to controller etc.	PT	PT	PT	PT	R
Existing SIS (physical) e.g. hardware capacity, power requirements etc.	R	R	R		
Existing SIS (functional) e.g. memory usage, transmission capacities etc.	R	R		R	
Existing SIS (characteristics) e.g. cycle times, response times etc.	R	R	R	R	
HMI	PT	PT	PT	PT	R

For existing SIS designed and constructed in accordance with codes, standards or practices prior to the issue of IEC 61508, the owner / operator shall determine that changes to the SIS as a minimum comply with the original design basis. However, careful consideration shall be given for the need to upgrade the existing Safety Requirement Specifications or generate one in accordance with IEC61508, when for example the following changes are introduced:

- major replacements or upgrades of the SIS;
- where major units or modules are replaced or installed;
- major changes in the characteristics of the process medium handled by the installation;
- where new rules with retroactive effect result in the existing SIS failing to meet the requirements;
- where new knowledge gained from, for example, incidents or major studies indicate that the existing SIS can no longer deliver an appropriate performance or an acceptable level of integrity.

11.3 MOC documentation

All changes to operating procedures, process safety information, and SIS documentation (including software) shall be noted prior to start-up, and updated accordingly.

The documentation shall be appropriately protected against unauthorised modification, destruction, or loss.

All SIS documents shall be revised, amended, reviewed, approved, and be under the control of an appropriate document control procedure.

12 SIS Decommissioning

12.1 Objectives

The objectives of the requirements of this chapter are:

- to ensure that prior to decommissioning any SIS from active service, a proper review is conducted and required authorisation is obtained; and
- to ensure that the safety instrumented functions remain appropriate during decommissioning activities.

12.2 Requirements

Management of change procedures as described in section 11.2 shall be implemented for all decommissioning activities.

The impact of SIS decommissioning on adjacent operating units and facilities or other field services shall be evaluated prior to decommissioning.

APPENDIX A

BACKGROUND FOR MINIMUM SIL REQUIREMENTS

CONTENT

A.1 Introduction

This appendix documents the background for the minimum SIL requirements as presented in Table 7.1, section 7.6, of this guideline. The formulas used in the calculations are discussed in Appendix D.

A.1.1 Rationale for the minimum SIL requirement table

Ideally, Quantitative Risk Assessment (QRA) should have been used when establishing the integrity requirements to safety functions. However, the level of detail of the QRA as it is performed today makes it more appropriate for evaluating conceptual options and for verification purposes, than for stating absolute criteria. As a result, SIL requirements to safety functions can normally not be obtained directly from the QRA. This applies particularly e.g. for PSD safety functions.

IEC 61508/61511 suggests a number of qualitative and semi-qualitative methods for determining SIL requirements (e.g. risk graph, hazardous event severity matrix, etc.). These methods are primarily screening tools and have proved difficult to actually apply for some of the safety functions. Whereas the use of risk graphs for example can work when determining integrity levels for PSD functions, the use of this method for global safety functions, such as ESD and F&G, seems to cause considerable problems.

In all, using these methods may introduce considerable amounts of additional analysis work and a possibility of selecting sub-optimal safety integrity levels, when taking into consideration the numerous safety functions present on an average offshore installation. Consequently, it has been decided to establish minimum safety integrity level requirements for the most common safety functions. The given SIL requirements are based on experience, with a design practice that has resulted in a safety level considered adequate. This will reduce the need for time-consuming SIL analysis work for more or less "standard solutions" and will ensure a minimum level of safety. Another advantage of using pre-determined SIL is that these figures can be used as input to QRA during early design stages and thereby set up a link between the risk analysis and the integrity levels for important safety functions.

A.1.2 Considerations and assumptions

When stating minimum SIL requirements like the ones given in this guideline, one main objective should be to ensure a performance level equal to or better than today's standard. In this regard, there are certain considerations to be made in order to avoid that the stated criteria actually result in a relaxation of the safety level. Some of these considerations are discussed below:

- When using "conservative" failure rates and/or long test intervals for calculating the failure probability of a given function, the resulting PFD $\approx = \lambda_{DU} \cdot \tau / 2$, becomes "high". Accordingly, a "low" SIL value will be claimed for the function, resulting in a "non-conservative" requirement in the minimum SIL table;
- Consequently, it is important that the input data fed into the calculations in this appendix are realistic both with respect to the failure rates being representative for new equipment as well as the test intervals.
- For several important safety functions, the failure probability "on demand" seem to become in the order of $1 \cdot 10^{-2}$ (e.g. $1.1 \cdot 10^{-2}$) when calculating the PFD using "standard" reliability data and test intervals. If this results in a SIL 1 requirement, there are two aspects to be kept in mind: (1) In such case the PFD can vary between 0.1 – 0.01 and (2) As discussed above the historical data from e.g. from OREDA and PDS might be conservative for new equipment. Therefore, as a general rule in this appendix, a SIL N requirement has been claimed when the calculated PFD is in the lower end of the interval of SIL N-1. E.g. when the estimated PDF = $1.1 \cdot 10^{-2}$, a SIL 2 requirement is given. This is also in line with the PSA requirement for continuous improvements.

The failure data, which are presented below and as used in the "generic quantifications", are considered to be typical values, often used in previous calculations of this type. **However, it is stressed that these values should *not* be used uncritically in future calculations. Actually some of the input data may now be outdated, and more important, in actual calculations it is crucial that application specific data are applied whenever available and documented. Please refer to Section 8.5.2 in this guideline regarding qualification of failure data used for PFD calculations.**

Another important aspect concerns the failure rate λ_{DU}, which is the rate of critical failures undetectable by automatic self-test. The λ_{DU} values applied in the example calculations assumes a certain diagnostic coverage, which is given from the applied data source (mainly PDS - see below). It is therefore important that during the process of SIL

verification, the assumed diagnostic coverage factors are properly documented. This requirement will, in addition, follow from the documentation of hardware safety integrity, ref. Table 2 and 3 in IEC 61508-2, where requirements to (amongst other) diagnostic coverage (DC) and safe failure fraction (SFF) are given depending on the claimed SIL.

For the simplified loop diagrams shown in this appendix, some details are omitted, e.g. barriers, relays, cables and signal adapters. In the final calculations, to prove compliance, all components and modules that may influence PFD of the function have to be included. In addition to the quantitative PFD requirements, all other requirements have to be fulfilled to prove compliance.

A.2 Data dossier

This section contains a collection of the reliability data used in the calculations and the assumed test intervals.

A.2.1 Reliability Data

Table A.1 summarises the failure rates used in this appendix. λ_{DU} is here the rate of failures causing the component to fail upon demand, undetected by automatic self-test.

With respect to the applied failure rates, these are to a large degree based upon the updated PDS reliability data, ref. /A.1/, as developed in the PDS-BIP project “Brukervennlig analyseverktøy for instrumenterte sikkerhetssystemer”. The specified SFF values are also based on this report. These data are documented in the PDS 2004 data handbook.

PSF (Probability of Systematic Failure) is the probability that a component which has just been functionally tested will fail on demand (earlier denoted TIF = Test Independent Failure). The PSF values are based on the PDS report “Reliability Data for Safety Instrumented Systems, 2003 Edition”.

As discussed in the previous section the given reliability data and in particular the rate of dangerous failures (λ_{DU}), are based on a number of assumption concerning safe state, diagnostic coverage, fail-safe design, loop monitoring, NE/NDE design etc. Hence, if the provided data are used for SIL verification, it must be ensured that the actual purchased components are satisfying all these assumptions.

It should also be noted that the reliability data provided in table A.1 is mainly based on operational experience (OREDA, RNNS, etc.) and as such reflect some kind of average field performance of the components. When comparing these data to reliability figures found in supplier certificates and reports a major gap will often be found. Supplier certificates and reports normally exclude failures caused by inappropriate maintenance and usage mistakes, design related systematic failures and also wear out. Care should therefore be taken when data from such certificates and reports are used for reliability prediction and verification purposes.

Table A.1 Applied failure rates (topside equipment)

Component	λ_{DU} ($\cdot 10^{-6}$)	SFF (%)	PSF	Data source / comments
Pressure transmitter	0.3	77	$3 \cdot 10^{-4}$ 1) $5 \cdot 10^{-4}$ 2)	Updated PDS-BIP data, ref. /A.1/. 1) For smart transmitter 2) For standard transmitter
Level transmitter	0.6	80		
Temperature transmitter	0.3	83		
Smoke detector	0.8	78	- *	Updated PDS-BIP data, ref. /A.1/. * No PSF values are given for the detectors since the definitions of F&G functions in table 7.1 assume exposed detector, whereas the PSFs given in PDS include the likelihood of the detector not being exposed.
Heat detector	0.5	79		
Flame detectors, conventional	1.6	80		
Gas detector, catalytic	1.8	64		
IR Gas detector, Conventional point detector	0.7	83		
IR Gas detector, Line	0.7	87		
ESD pushbutton	0.2	82	$1 \cdot 10^{-5}$	Reliability Data for Safety Instrumented Systems, 2003 Edition (PDS)
Standard industrial PLC – single system	5	83	$5 \cdot 10^{-4}$	Updated PDS-BIP data, ref. /A.1/.
Programmable safety system – single system	1	95	$5 \cdot 10^{-5}$	Updated PDS-BIP data, ref. /A.1/.
Hardwired safety system – single system	0.1	95	$0.5 \cdot 10^{-5}$	Updated PDS-BIP data, ref. /A.1/.
ESV/XV incl. actuator (ex. pilot)	2.0	62	$1 \cdot 10^{-6}$ 1) $1 \cdot 10^{-5}$ 2)	Updated PDS-BIP data, ref. /A.1/. 1) For complete functional testing 2) For incomplete functional testing
Blowdown valve incl. actuator (ex. pilot)	2.0	62		
Topside X-mas tree valves Wing and Master Valve	0.8	62		
Solenoid / pilot valve	0.9	72	-	Updated PDS-BIP data, ref. /A.1/.
Circuit Breaker, < 660 V	0.15	-	-	T-Boken: "Reliability data of components in Nordic nuclear power plants", rev. 5
Circuit Breaker, 6 KV - 10 KV	0.2	-	-	
Fire damper	7.3	-	-	Updated PDS-BIP data, ref. /A.1/.
Fire water pump (centrifugal) (including power transmission, pump unit, control &monitoring, lubrication system and misc.)	Fail to start on demand : $9.4 \cdot 10^{-4}$		-	OREDA 2002, 1.3.1.18 The failure rate includes only the critical failure mode "fail to start" ("fail while running" not included). The population includes 108 pumps, 1060 demands and 5 FTS failures.
Fire water diesel engine	Fail to start on demand: $1.9 \cdot 10^{-3}$		-	OREDA 2002, 1.4.1.5 The failure rate includes only the critical failure mode "fail to start on demand" ("breakdown" not included). The population includes 8 diesel engines, 1060 demands and 2 FTS failures.
Electric generator (motor driven, 1000-3000 kVA)	Fail to start on demand: $1.4 \cdot 10^{-3}$		-	OREDA 2002, 2.1.1.1.2 The failure rate includes only the critical failure mode "fail to start on demand" ("spurious stop" not included). The population includes 12 generators, 1470 demands and 2 FTS failures.
Electric motor (pump driver)	Fail to start on demand: $1.4 \cdot 10^{-3}$		-	OREDA 2002, 2.2.2 The failure rate includes only the critical failure mode "fail to start on demand". The population includes 135 motors, 5020 demands and 16 FTS failures.
Deluge valve including actuator, solenoid and pilot valve	4.7	-	-	Updated PDS-BIP data, ref. /A.1/.

Table A.1 (cont.) Applied failure rates (subsea equipment)

Component	λ_{DU} ($\cdot 10^{-6}$)	SFF (%)	Data source / comments
HPU hydraulic fail safe valve	0.9	72	Ref. Table A.1 for topside equipment. Data for topside pilot valves has been assumed since the HPU is located topside.
Hydraulic Control Valves (located in subsea Control Module)	0.1	60	OREDA Handbook 2002, page 811, solenoid control valves (1429 off, 10 critical failures). Assuming a coverage of 0% for subsea valves and approximately 60% / 40% distribution between safe and dangerous failures.
Directional Control Valve (DCV)	0.1	60	OREDA Handbook 2002, page 811, solenoid control valves Data for solenoid control valves – same assumptions as above. The OREDA figures do not give any background for splitting between different operational modes of the DCV. Hence, a general λ_{DU} failure rate is given for the DCV.
PMV, PWV	0.1	60	OREDA Handbook 2002, page 833, X-mas tree valve process isolation (550 off, 4 critical failures). Again assuming a coverage of 0% for subsea valves and approximately 60% / 40% distribution between safe and dangerous failures.
CIV	0.4	60	OREDA Handbook 2002, page 833, Valve utility isolation (181 off, 3 critical failures) Again assuming a coverage of 0% for subsea valves and approximately 60% / 40% distribution between safe and dangerous failures.
DHSV	2.5	60	Updated PDS-BIP data, ref. /A.1/.
Subsea Isolation Valves (SSIV)	0.1	60	OREDA 2002 Handbook, page 823, Valve subsea isolation (146 off, 0 critical failures) Assuming one (1) critical failure, zero coverage and a 60% / 40% distribution between safe and dangerous failures.
Pressure Transmitter (PT)	0.4	78	OREDA Handbook 2002, page 811, Pressure sensor (294 off, 14 critical failures). Assuming the same coverage and the same distribution between safe and dangerous failures as for topside pressure transmitters.
Temperature Transmitter (TT)	0.1	67	OREDA Handbook 2002, page 811, Temperature sensor (179 off, 2 critical failures) Assuming the same coverage and the same distribution between safe and dangerous failures as for topside temperature transmitters. This gives a value of 0.05 for λ_{DU} which is rounded up to 0.1.
Combined PT/TT	0.2*	78	OREDA 2002 Handbook, page 811, combined PT/TT sensor (30 off, 1 critical failure) Assuming the same coverage and distribution between safe and dangerous failures as for topside pressure transmitters. * This estimate is based on only 30 components; hence the confidence in this figure is very low (the standard deviation is approx. 0.5).

Component	λ_{DU} ($\cdot 10^{-6}$)	SFF (%)	Data source / comments
Umbilical Signal Lines* (power / signal line)	0.24	90	OREDA 2002 handbook, page 811, Static umbilical, power/signal line (63 off, 8 critical failures) *λ_{DU} has been based on critical failures of power/signal lines in static umbilical. Assuming 50% safe failures and a coverage of 80%, since the majority of failures should be detectable immediately.
SEM – Subsea Electronic Module	1.9	85	OREDA 2002 Handbook, page 811, subsea electronic module (107 off, 117 critical failures) Assuming the same distribution between safe and dangerous failures as for topside safety systems (ref. /A.1/).

Please note that PSF values are not given for subsea equipment. It is here referred to values for topside equipment, since no separate evaluations have been made with respect to systematic failures for subsea components.

Table A.2 Assumed test intervals (topside equipment)

Component	Test interval (months)	Test interval (hours)	Comments / assumptions
Transmitters	12	8760	
Fire and gas detectors	6	4380	
Logic incl. I/O card (single PLC)	12	8760	6 months interval for ESD might be optimistic; OK for PDS and F&G
Topside valves (ESV/XV/blowdown)	12	4380	Taking into consideration that such valves occasionally trip. In addition to the full stroke functional testing (e.g. once every year) partial stroke testing can be performed which will reveal most failures
Solenoid /pilot valve	12	4380	
Circuit Breakers	24	17520	
Fire dampers	3	2190	
Fire water pumps	-	-	NFPA requires weekly starts of fire water pumps
Deluge valve	6	4380	

Table A.2 (cont.) Assumed test intervals (subsea equipment)

Component	Test interval (months)	Test interval (hours)	Comments / assumptions
HPU hydraulic fail safe valve (located topside)	6	4380	
Directional Control Valve (DCV)	6	4380	
PMV, PWV	6	4380	
DHSV	6	4380	When installed these valves might be tested as often as each month, increasing to every third month and then to twice a year.
Umbilical Signal Lines	6	4380	
SEM	6	4380	
PT/TT	6	4380	
Relay	6	4380	

Table A.3 below summarises the above input data with respect to resulting PFD (probability of failure on demand), i.e.:

$$PFD = \lambda_{DU} \cdot \tau / 2.$$

When Table A.1 presents several values (as for the PSF-probability), one value within the interval is chosen in Table A.3. Finally, also some "typical" β-factors are included in Table A.3. This is partly based on the PDS Reliability Data (2003 Edition). The PDS values for some components are combined values for random hardware and systematic failures. However, Table A.3 provides separate β's for these two failure categories. An analysis performed for Norsk Hydro (Tune) is another source for the β-factors for random hardware failures presented in Table A.3. This Hydro analysis applied the IEC 61508 approach for calculating some β-factors. According to these data sources the suggested β-values are perhaps somewhat optimistic. All values for random hardware failures are within the range that follows from the IEC approach; i.e. 0.5%<β<5% for logic, and 1%<β<10% for sensors and actuators.

It is stressed that Table A.3 in no way presents "The recommended values". They are simply "typical values" used in the "example calculations".

Table A.3 Summary of component reliability values used in example calculations.

Component	Test interv. τ, (months)	Fail. rate, λ_{DU} per 10^6 hrs	PFD	PSF-prob.	β-factor[5]
Pressure transmitter	12	0.3	$1.3 \cdot 10^{-3}$	$3 \cdot 10^{-4}$ - $5 \cdot 10^{-4}$ [1]	2% (5% for PSF)
Level transmitter	12	0.6	$2.6 \cdot 10^{-3}$		
Temperature transmitter	12	0.3	$1.3 \cdot 10^{-3}$		
Smoke detector	6	0.8	$1.8 \cdot 10^{-3}$	$5 \cdot 10^{-4}$ [2]	5% (20% for PSF)
Heat detector	6	0.5	$1.1 \cdot 10^{-3}$		
Flame detectors, conventional	6	1.6	$3.5 \cdot 10^{-3}$		
Gas detector, catalytic	6	1.8	$3.9 \cdot 10^{-3}$		
IR Gas detector, Conv. point detector	6	0.7	$1.5 \cdot 10^{-3}$		
IR Gas detector, Line	6	0.7			
Standard industrial PLC – single system	12	5	$2.19 \cdot 10^{-2}$	$5 \cdot 10^{-4}$	1% (50% for PSF)
Programmable safety system – single system	12	1	$4.4 \cdot 10^{-3}$	$5 \cdot 10^{-5}$	
Hardwired safety system – single system	12	0.1	$0.4 \cdot 10^{-3}$	$0.5 \cdot 10^{-5}$	
Manual pushbutton (ESD / F&G)	12	0.2	$8.8 \cdot 10^{-4}$	$1.1 \cdot 10^{-5}$	-
ESV/XV incl. actuator (ex. pilot)	12	2.0	$8.8 \cdot 10^{-3}$	$5 \cdot 10^{-6}$	2% (5% for PSF)
Blowdown valve incl. actuator (ex. pilot)	12	2.0	$8.8 \cdot 10^{-3}$		
Topside X-mas tree valves - Wing valve (WV) - Master Valve (MV)	12	0.8	$3.5 \cdot 10^{-3}$		
Down Hole Safety Valve – DHSV	6	2.5	$5.5 \cdot 10^{-3}$	$5 \cdot 10^{-6}$ [3]	-
Solenoid / pilot valve	12	0.9	$3.9 \cdot 10^{-3}$	- [4]	2%-10%[6]
Circuit Breaker, < 660 V	24	0.15	$1.3 \cdot 10^{-3}$	-	-
Circuit Breaker, 6 KV - 10 KV	24	0.20	$1.8 \cdot 10^{-3}$	-	-
Fire damper	3	7.3	$8.0 \cdot 10^{-3}$	-	-
Fire water pump, (fail to start)	-	-	$9.4 \cdot 10^{-4}$	-	5%
Fire water diesel engine (fail to start)	-	-	$1.9 \cdot 10^{-3}$	-	5%
Electric generator (fail to start)	-	-	$1.4 \cdot 10^{-3}$	-	5%
Electric motor (fail to start)	-	-	$1.4 \cdot 10^{-3}$	-	5%
Deluge valve incl. actuator, solenoid and pilot valve, (fail to open)	6	4.7	$1.0 \cdot 10^{-2}$	-	-
Manual push button	12	0.2	$0.88 \cdot 10^{-3}$	$1.1 \cdot 10^{-4}$	-
Output card	6	0.08 [7]	$0.18 \cdot 10^{-3}$	-	-

Component	Test interv. τ, (months)	Fail. rate, λ_{DU} per 10^6 hrs	PFD	PSF-prob.	β-factor[5)]
Hydraulic Control Valves (located in subsea Control Module)	6	0.1	$2.2 \cdot 10^{-4}$	- [8)]	- [9)]
Directional Control Valve (DCV)	6	0.1	$2.2 \cdot 10^{-4}$	- [8)]	- [9)]
PMV, PWV	6	0.1	$2.2 \cdot 10^{-4}$	- [8)]	- [9)]
CIV	6	0.4	$8.8 \cdot 10^{-4}$	- [8)]	- [9)]
DHSV	6	2.5	$5.5 \cdot 10^{-3}$	- [8)]	- [9)]
Subsea Isolation Valves (SSIV)	6	0.1	$2.2 \cdot 10^{-4}$	- [8)]	- [9)]
Pressure Transmitter (PT)	6	0.4	$8.8 \cdot 10^{-4}$	- [8)]	- [9)]
Temperature Transmitter (TT)	6	0.1	$2.2 \cdot 10^{-4}$	- [8)]	- [9)]
Combined PT/TT	6	0.2	$4.4 \cdot 10^{-4}$	- [8)]	- [9)]

[1)] For smart / conventional respectively
[2)] Suggested PSF-probability, given exposed detector
[3)] It is suggested to use same PSF -probability as for XV/ESV
[4)] PSF -probability for pilot is included in figure for main valve/actuator.
[5)] Value applies to dangerous undetectable random hardware failures (duplicated system). Values in parenthesis apply for systematic failures (PSF). The estimated β-factors are generally based on Reliability Data for Safety Instrumented Systems, 2003 Edition (PDS)
[6)] β=10% for pilot valves on the same valve, otherwise β=2%
[7)] Assuming that 5% of the total undetected dangerous failure rate for logic (incl. I/O) originates from the output card
[8)] Please note that PSF values are not given for subsea equipment. It is here referred to values for topside equipment, since no separate evaluations have been made with respect to systematic failures for subsea components.
[9)] Please refer to section A.13 where separate considerations have been made

A.2.2 Demand rates

It should be noted that this revision of the document does not include average demand rates. This has been deleted due to several reasons:

- The demand rates are highly installation specific and it is therefore difficult to give generic values;
- Since this document gives standard SIL requirements, the demand rates are not applied when determining the SIL requirements (see chapter 7 in main document);

In order to enable follow-up during operation, it will however, be required to estimate the demand rates as part of the SRS work.

A.2.2 Additional comments

Some additional comments should be made concerning the following example calculations:

- For the purpose of this document all safety functions have been treated as low demand functions. It should be pointed out that separate considerations must be made for each specific case in order to verify that this assumption is relevant:
- In the example calculations involving redundant components the contribution from independent failures, i.e. both components failing independently, has generally been neglected. In some cases this assumption may not be 100% correct (e.g. if the β factor is very small). Hence, in actual calculations / verifications this contribution must be considered;
- In the following calculations, only the quantitative SIL requirements have been considered. Architectural requirements related to Hardware Fault Tolerance (HFT), Safe Failure Fraction (SFF) and type of components have not been considered (ref. section 8.5.1 in main document). Hence, for a given technical solution, it must be verified that these hardware requirements are also fulfilled.

A.3 PSD functions

A.3.1 Process segregation through PSD

Definition of functional boundaries
An example of the function "*segregation of process section*" is given in figure A.1 below. The EUC will here be the separator to be segregated from the rest of the process.

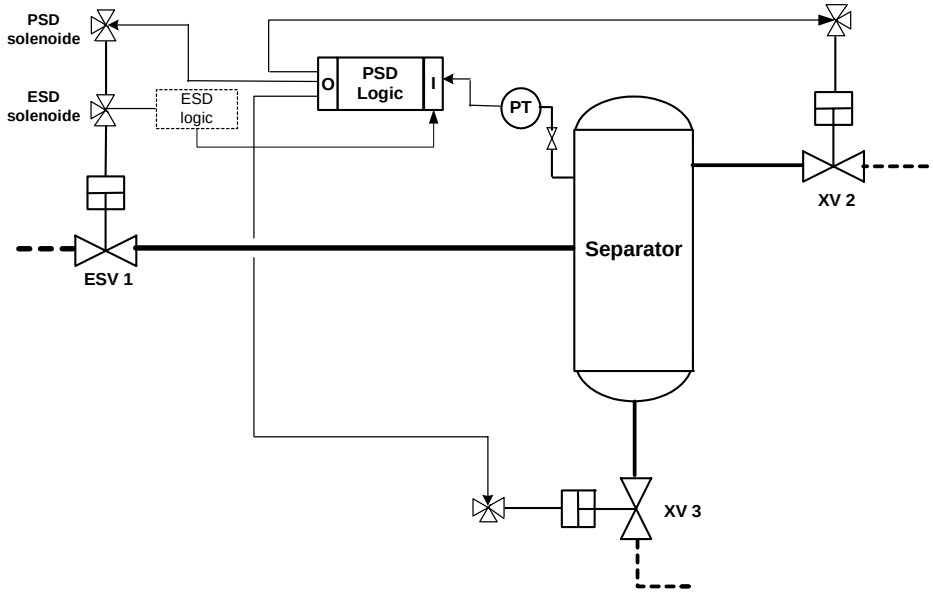

Figure A.1 Possible definition of the function "segregation of process section through PSD"

The function "*segregation of process section*" is here defined by the PSD system receiving and processing some signal (e.g. a PALL or a shutdown signal from the ESD system), which activates a closure of ESV 1, XV 2 and XV 3 in order to isolate the vessel.

The function starts where the signal is generated (not including transmitter or ESD system) and ends and includes closing of all the necessary valves. The transmitter is not included as this function is most probably activated on an ESD demand. Requirement to the PT is covered by the function PAHH in A.3.2.

Basic assumptions
It should be noted that the specific valves needed for segregation depends on the situation, as some of the valves used in the segregation will be "nice to have" – while others will be essential. The hazard analysis will pinpoint the essential valves/actions and only these valves should be included in the PSD function. This is further discussed in section A.3.2 – A.3.5 below where specific process deviations are considered.

Safe state of the process will for this case be closure of the inlet and outlet valves to the separator. It is assumed that this safety function will be normally energised (NE), i.e. upon loss of power or signal, the separator will be automatically isolated and the process will go to a safe state. Hence, the power source will not be included in the quantification of this safety function.

Quantification of safety function
The Reliability Block Diagram (RBD) for this function is given below. Just one Solenoid box is drawn although there shall be three in series. This is indicated by "x3" above this box. The PFD quantification is presented in Table A.5. The last column also provides the PSF for the function.

For the PSD logic, the figure for "Programmable safety system – single system" from Table A.3 has been applied.

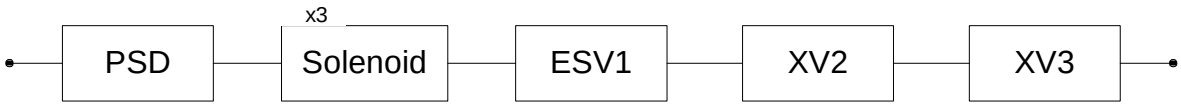

Figure A.2 RBD for Process segregation through PSD.

Table A.5 PFD for Process segregation through PSD

Component	No. of components	PFD per component	Total PFD	Total PSF
PSD logic (incl. I/O)	1	$2.19 \cdot 10^{-2}$	$4.4 \cdot 10^{-3}$	$5 \cdot 10^{-5}$
ESV/XV	3	$8.8 \cdot 10^{-3}$	$2.64 \cdot 10^{-2}$	$0.5 \cdot 10^{-5}$
Solenoid / pilot	3	$3.9 \cdot 10^{-3}$	$1.17 \cdot 10^{-2}$	-
Total Function	**-**	**-**	**0.043**	**$5.5 \cdot 10^{-5}$**

As seen the PFD is estimated to be ≈ 0.04, and a SIL 1 requirement therefore seems achievable based on a pure quantitative consideration.

A.3.2 PSD functions: PAHH, LAHH, LALL, (primary protections)

Definition of functional boundaries

Figure A.3 illustrates the boundaries for the PSD functions PAHH, LAHH and LALL. Again the EUC will be the separator.

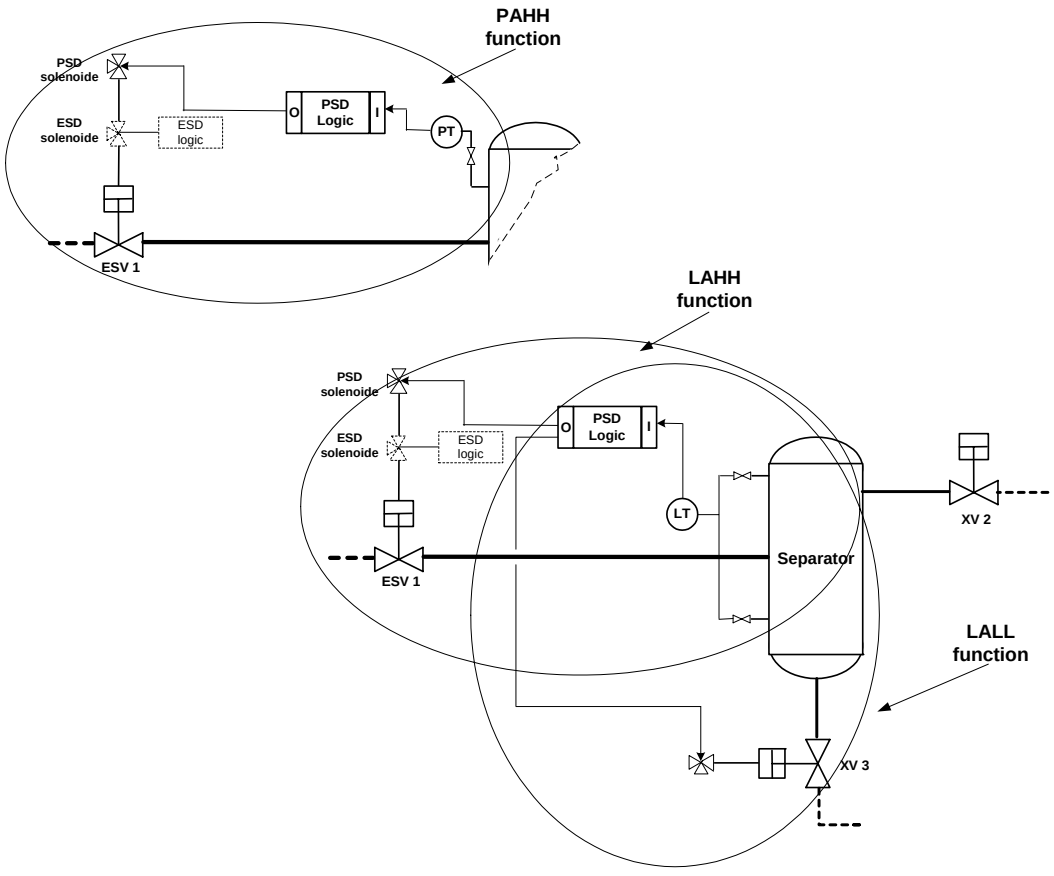

Figure A.3 Example of definition for the functions: PAHH, LAHH and LALL

Basic assumptions
It is here assumed that:

- A PAHH will only close the inlet valve(s), not the outlet valves;
- A LAHH will close the same valves as a PAHH;
- A LALL will only close the valve on the liquid outlet.

The function starts inside the process where the high pressure or level is detected, and ends within the process with closing of the valve.

It should be noted that when the SIL requirement is derived, it is assumed that there is one common inlet valve to the separator. However, the PSD functions PAHH and LAHH might depend upon closure of several valves if there is more than one line into the separator and no common inlet valve. In such case the same SIL requirement applies. If the SIL requirement is not fulfilled, whether it is because of several inlet lines or for other reasons, this must be treated as a deviation.

Safe state for the process will be closure of the specified valves. It is here assumed that these safety functions will be normally energised (NE), i.e. upon loss of power or signal, the shutdown actions will be initiated automatically and the process will go to a safe state. Hence, the power source will not be included in the quantification of these safety functions.

Quantification of safety functions
The Reliability Block Diagram for this function is given below. The PFD quantification is presented in Table A.6. The presentation is common for all three functions: PAHH, LAHH and LALL (closure of one valve).

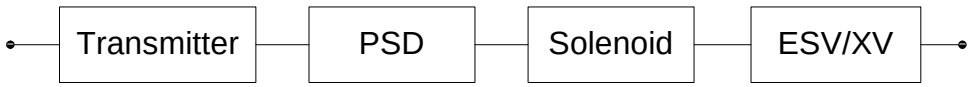

Figure A.4 RBD for PAHH, PALL and LALL.

Table A.6 PFD for process shutdown of one valve (PAHH, PALL and LALL)

Component	No. of components	Total PFD	Total PSF
Transmitter (PT)	1	$1.3 \cdot 10^{-3}$	$3 \cdot 10^{-4}$
PSD logic (incl. I/O)	1	$4.4 \cdot 10^{-3}$	$5 \cdot 10^{-5}$
ESV / XV	1	$8.8 \cdot 10^{-3}$	$0.5 \cdot 10^{-5}$
Solenoid / pilot	1	$3.9 \cdot 10^{-3}$	-
Total Function	**-**	**0.018**	**$3.6 \cdot 10^{-4}$**

As seen from the above table, these PSD functions only fulfil a quantitative SIL 1 requirement. By considering the input data underlying the above table the following can be concluded:

- by more frequent testing and/or by collecting information from actual shutdowns, a SIL 2 requirement seems obtainable;
- by using equipment with “better” (qualified) reliability data that the figures summarised in Table A.3, a SIL 2 requirement may also be obtainable;
- Also increased used of partial stroke testing may improve the PFD figures for the valves.

Consequently, a SIL 2 requirement is achievable.

A.3.3 PSD function: LAHH in flare KO drum

Definition of functional boundaries

A LAHH in the flare KO drum shall close the feed to the vessel and will therefore generally require a closure of the inlet lines to the installation and/or to the inlet separator. Since it will normally be difficult to detect from where the overfeeding originates, a LAHH in the flare KO drum will often initiate a global shutdown of the process through the PSD system and possibly also through the ESD system in order to increase the reliability of the function.

Consequently, a generic definition of the function *LAHH in flare KO drum* with respect to what is actually shut down is difficult to give, and rather the function is defined in terms of the detection device and the processing of the signal, i.e. as illustrated in Figure A.5 below.

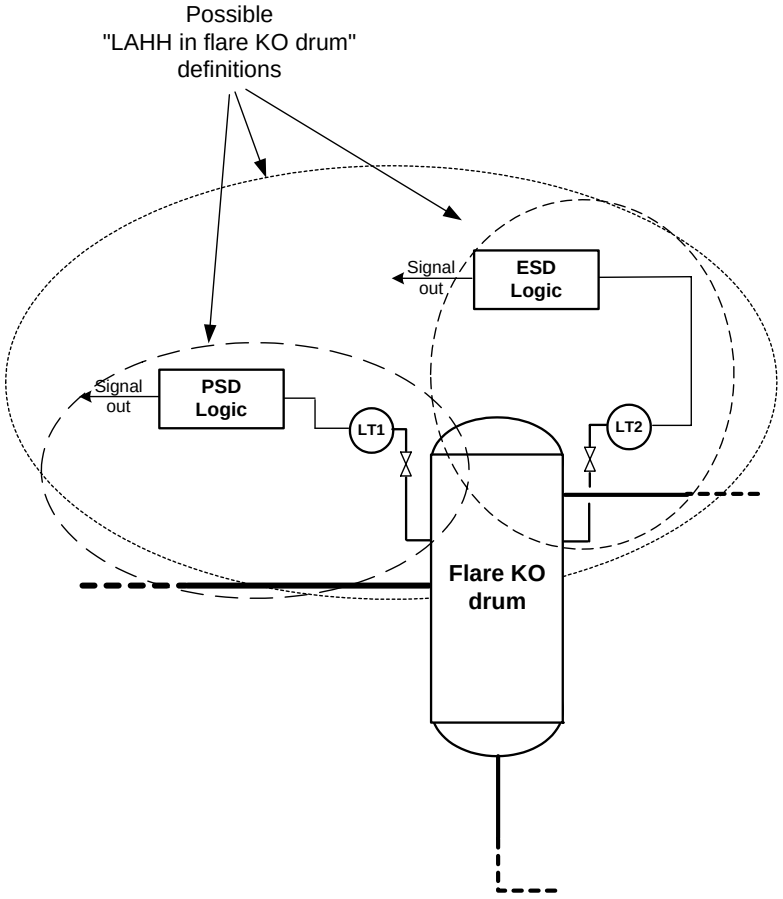

Figure A.5 Possible definitions of the function: LAHH in flare KO drum

Basic assumptions

As indicated on the figure, shutdown as a result of LAHH in the flare KO drum can be executed through the PSD system, the ESD system or through both. A possibility, not shown on the figure, could be that one common transmitter is applied to send a signal to both the PSD and the ESD system. *Here we will assume that shutdown is performed both through the ESD and the PSD system, with separate transmitters to the two systems.*

Hence, the function starts inside the process where the high level is expected, and ends at the unit(s) intended to perform the action (these units are not included).

Safe state for the process will here be a confirmed shutdown signal from the PSD and/or the ESD logic. It is here assumed that this function will be normally energised (NE), i.e. upon loss of power or signal, the feed to the KO drum will be automatically isolated and the process will go to a safe state. Hence, the power source will not be included in the quantification of this safety function.

Quantification of safety functions

The technical solutions considered here is "shutdown executed through both PSD and ESD; using separate LTs". A simplified RBD for this function is given in figure A.6 below.

The PFD values for the relevant single and duplicated components are presented in Table A.7 whereas the resulting PFD value for the safety function is presented in Table A.8.

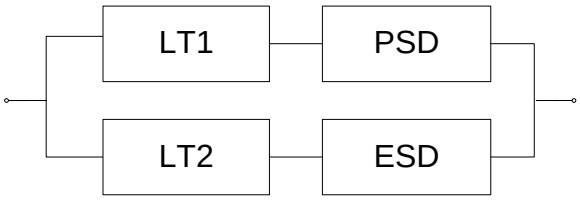

Figure A.6 RBDs for LAHH in flare KO drum

Table A.7 PFD input for LAHH in flare KO drum

Component	PFD, single component	PFD, duplicated comp.	PSF, single component	PSF, duplicated comp.
LT	$2.6 \cdot 10^{-3}$	$5.2 \cdot 10^{-5}$	$3 \cdot 10^{-4}$	$1.5 \cdot 10^{-5}$
PSD/ESD logic (incl. I/O)	$4.4 \cdot 10^{-3}$	$4.4 \cdot 10^{-5}$	$5 \cdot 10^{-5}$	$2.5 \cdot 10^{-5}$

Table A.8 PFD results for LAHH in flare KO drum

Solution	PFD for function	PSF-probability for function
Shutdown through PSD and ESD; separate LTs	$9.6 \cdot 10^{-5}$	$4 \cdot 10^{-5}$

As seen from the table, a SIL 3 requirement seems achievable given that the function is implemented through both the PSD and ESD system with separate level transmitters.

A.3.4 PSD function: TAHH/TALL

Definition of functional boundaries

A TAHH/TALL will close the inlet valve(s) and the definition of the function will therefore resemble the definition of PAHH above (ref. Figure A.3), the only difference being that the pressure transmitter is substituted with a temperature transmitter.

Basic assumptions

Safe state for the process will be to close inlet valve(s) and if relevant, to shutdown any heating or cooling devices. It is here assumed that the TAHH/TALL function will be normally energised (NE), i.e. upon loss of power or signal, the separator will be automatically isolated and the process will go to a safe state. Hence, the power source will not be included in the quantification of this safety function.

Quantification of safety functions

The RBD and quantification is exactly as in Section A.3.2. Thus, the estimated total PFD for the TAHH/TALL function is PFD ≈ 0.018. However, also for this function a SIL 2 requirement seems achievable if corresponding measures as discussed in section A.3.2 is implemented.

A.3.5 PSD function: PALL (primary protection against leakage)

Definition of functional boundaries
The PALL function is frequently applied as primary protection against leakage (in addition to gas detection) and will normally initiate a closure of both the inlet and outlet valves. Consequently, this particular PSD function is similar to the function "*segregation of process section* " as described in section A.3.1 above. Since the reliability of the low pressure detection itself is highly uncertain for all leaks except very large ones, the definition of PALL should be as for *segregation of process section,* i.e. excluding the sensor device.

Hence, the function starts inside the process where the low pressure is expected, and ends within the process with the valve.

Quantification of safety function
No special requirements apply according to this guideline. This requires that adequate automatic gas detection is provided to cover the leakage. It should, however, be noted that excluding the sensor device, the function fulfils a SIL 1 requirement.

A.4 Segregation through ESD with one ESD valve

Definition of functional boundaries
Isolation of an ESD segment occurs on demand from the ESD system, i.e. on detection of HC leaks or a fire on the installation. The number of ESD valves to close in such a situation will vary from case to case. Hence, a general definition of the ESD segregation function is difficult to give. It has therefore been decided to define an ESD sub-function in terms of:

- the ESD node
- one Emergency Shutdown Valve (ESV) including solenoid and actuator

This definition is illustrated in Figure A.7 below:

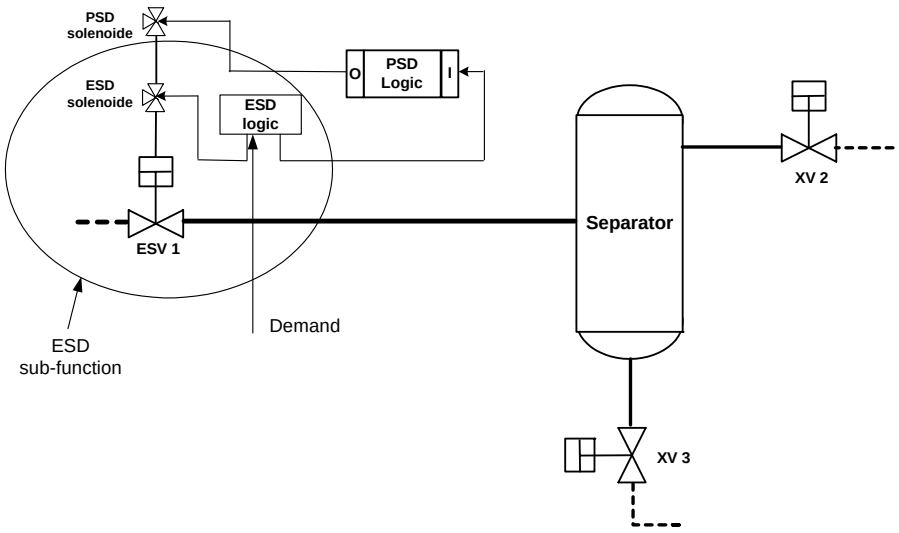

Figure A.7 Definition of the ESD sub-function

Basic assumptions
As seen from Figure A.7, the ESD sub-function is defined as closure of one valve through the ESD system. In order to increase the reliability of the sub-function, it will also be possible to include activation of the ESV through the PSD-system by a separate PSD solenoid.

The function starts at the unit giving the demand (unit not included), and ends within the process with the valve.

The safe state of the process is defined by closure of the ESD valve(s). It is here assumed that this safety function will be normally energised (NE), i.e. upon loss of power or signal, the ESD valve will close. Hence, the power source will not be included in the quantification of this safety function.

Quantification of safety functions
The Reliability Block Diagram for this function is given below. The PFD quantification is presented in Table A.9.

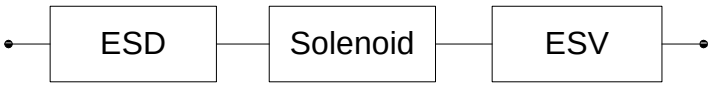

Figure A.8 RBD for ESD sub-function (Segregation through ESD with one ESD valve).

Table A.9 PFD for Segregation through ESD

Component	No. of components	Total PFD	Total PSF
ESD logic (incl. I/O)	1	$4.4 \cdot 10^{-3}$	$5 \cdot 10^{-5}$
ESV	1	$8.8 \cdot 10^{-3}$	$0.5 \cdot 10^{-5}$
Solenoid / pilot	1	$3.9 \cdot 10^{-3}$	-
Total Function	**-**	**0.017**	**$5.5 \cdot 10^{-5}$**

As seen from the above table, the defined ESD function only fulfils a quantitative SIL 1 requirement. By considering the input data underlying the above table the following can be concluded:

- by more frequent testing and/or by collecting information from actual shutdowns, a SIL 2 requirement seems obtainable;
- by using equipment with "better" (qualified) reliability data that the figures summarised in Table A.3, a SIL 2 requirement may also be obtainable;
- For the ESD logic a failure rate (λ_{DU}) of $1 \cdot 10^{-6}$ per hour has been applied, i.e. corresponding to the failure rate for a single system. Typically, an ESD system will have redundant CPUs and I/Os, and based on the type of redundancy applied, a lower failure rate for the overall ESD logic may be argued;
- Also increased used of partial stroke testing may improve the PFD figures for the valves.

Consequently, it is concluded that a SIL 2 is obtainable.

A quantitative risk analysis should be conducted to verify that the minimum SIL-requirement gives an overall acceptable risk when all the ESD valves are taken into consideration. The following should then be considered:

- number of ESD-valves needed to isolate each fire area;
- scenarios where the system is demanded (e.g. leak and fire scenarios);
- process conditions (pressure, temperature) and duration of leaks and fires;
- criticality of valve (e.g. consequence of ESD valve not closing);
- common cause failures;
- etc.

A.5 Blowdown

Definition of functional boundaries
The sub-function blow down includes:

- the ESD node
- one blow down valve (BDV) incl. solenoid and actuator

Figure A.9 illustrates the sub-function “blow down”.

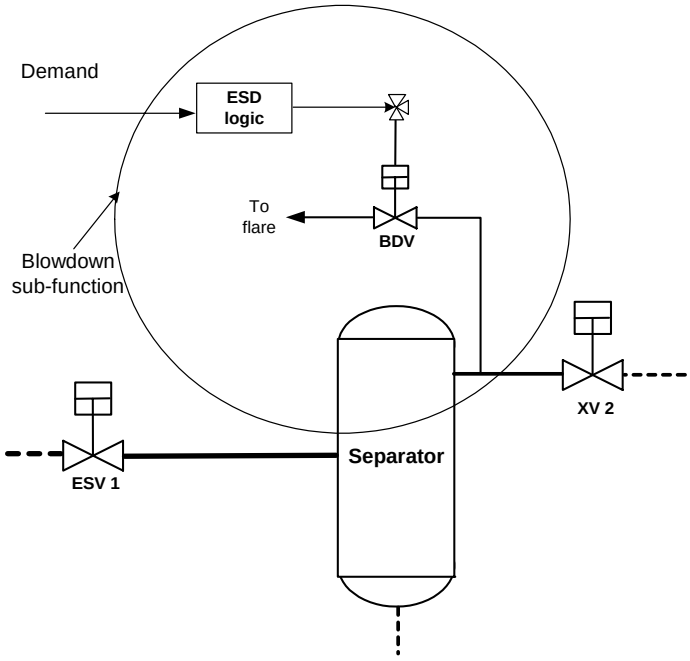

Figure A.9 Definition of the sub-function “blow down”

Basic assumptions

The function starts at the unit giving the demand (unit not included) and ends with the inventory having free access through the BDV. Note that the probability of successful manual blow down activation is not included in the definition of this function.

The safe state of the process is defined by opening of the blow down valve. It is here assumed that this safety function will be normally energised (NE), i.e. upon loss of power or signal, the BDV will open. Hence, the power source will not be included in the quantification of this safety function.

It should be noted that on installations were the blow down function is normally de-energised (NDE), e.g. due to sequential blow down and/or insufficient flare capacity, the power source must be included in the calculations. Furthermore, it is important that the reliability data applied for equipment in such de-energised functions do reflect the relevant failure modes (which may differ from failure modes of equipment applied in normally energised functions, ref. e.g. the logic solver).

Quantification of safety function

The Reliability Block Diagram for this function is given below. The PFD quantification is presented in Table A.10.

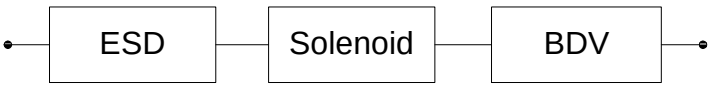

Figure A.10 RBD for sub-function blow down

Table A.10 PFD for Blow down

Component	No. of components	Total PFD	Total PSF
ESD logic + I/O	1	$4.4 \cdot 10^{-3}$	$5 \cdot 10^{-5}$
BDV	1	$8.8 \cdot 10^{-3}$	$0.5 \cdot 10^{-5}$
Solenoid / pilot	1	$3.9 \cdot 10^{-3}$	-
Total Function	**-**	**0.017**	**$5.5 \cdot 10^{-5}$**

Based on the same arguments as for the above ESD function (ref. section A.4), a SIL 2 requirement seems obtainable.

A quantitative risk analysis should be conducted to verify that the minimum SIL-requirement gives an overall acceptable risk. The following should be considered:

- number of blow down-segments in each fire area;
- scenarios where the system is demanded (fire scenarios);
- process conditions (pressure, temperature) and duration of fires;
- common-cause failures.

It should be noted that, if design solutions such as e.g. sequential blow down is implemented, the SIL 2 requirement will still apply. Otherwise, this must be treated as a deviation.

A.6 Isolation of topside well

Definition of functional boundaries
The sub-system *isolation of topside well* is defined as the system needed to isolate one topside well. For a standard production well, the sub-system consists of the following:

- ESD node
- PSD node
- Wing valve (WV)
- Master Valve (MV)
- Down hole safety valve (DHSV)
- Solenoid valves

Figure A.11 illustrates the function "isolation of topside well".

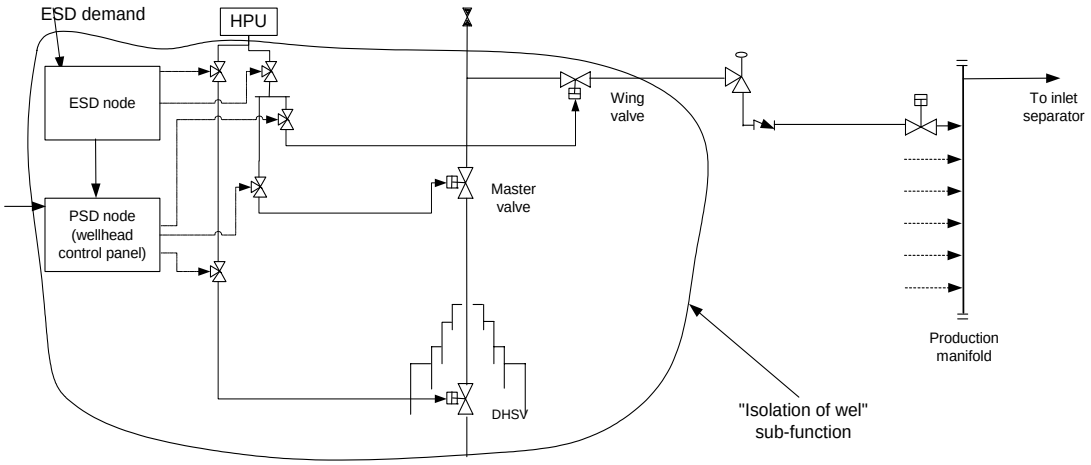

Figure A.11 Definition of the sub-function "isolation of topside well"

Basic assumptions

The isolation function concerns only the ESD functions related to the isolation, not the overpressure protection realised through the PSD system. The well or inlet to the platform will also be isolated due to PSD demands, but these are not included in this function. Depending on for example the event and C&E, this may cause a demand on the same valves or other valves.

The function starts at the unit where the demand is initiated (unit not included), and ends with the valves shutting in the well.

Depending on the scenario having triggered the demand for isolation, one of the three valves will be sufficient to isolate the well. However, in the event of a fire in the wellhead area, the well is usually also isolated by the DHSV.

The safe state of the process will be defined by closure of the ESD valve(s) and isolation of well. All valves (WV, MV & DHSV) are assumed hydraulically fail-safe and one of the valves electrically fail-safe. Hence, the power sources will not be included in the quantification of this safety function.

Quantification of safety functions

The function "isolation of one well", can be represented by a Reliability Block Diagram as shown in Figure A.12 below. The illustrated solution is to have separate solenoids for the MV, the WV and the DHSV (activated by PSD), and one solenoid (activated directly by ESD) to remove hydraulic power to all three valves. Note that this RBD is slightly simplified.

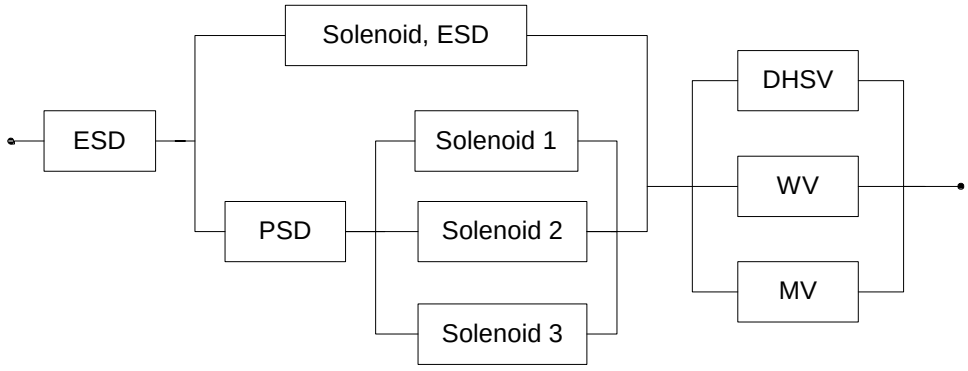

Figure A.12 RBD for "failure to isolate one well"

The calculations are presented in Table A.11, and the result in Table A.12. The quantifications assume common cause failure between the master and the wing valve, but not between MV/WV and DHSV. The essential contribution is from the ESD-system. In addition, the quantification here gives a small contribution from common cause failures of the solenoids, (as the IEC model gives the same result for common cause failure, irrespective of whether there is a 1oo2, 1oo3 or 1oo4 configuration).

Table A.11 PFD input for isolation of one well

Component	PFD, single component	PFD, duplicated comp.	PSF, single component	PSF, duplicated comp.
ESD/PSD logic +I/O	$4.4 \cdot 10^{-3}$	-	$5 \cdot 10^{-5}$	-
Solenoid	$3.9 \cdot 10^{-3}$	$7.8 \cdot 10^{-5}$ [1)]	-	-
MV /WV	$3.5 \cdot 10^{-3}$	$7 \cdot 10^{-5}$	$5 \cdot 10^{-6}$	$0.3 \cdot 10^{-6}$
DHSV	$5.5 \cdot 10^{-3}$	-	$5 \cdot 10^{-6}$	-

[1)] Note that for the three parallel solenoid valves, the *standard IEC* β-factor model has been used, i.e. using a β value of 2% irrespective of there being a 1oo3 or a 1oo2 voting (cf. Appendix D). A more refined modelling would give a better value for 1oo3 of a factor 3. However, this only marginally influences the overall function PFD.

Table A.12 PFD results for isolation of one well

Solution	PFD for function	PSF-probability for function
1. Separate solenoids for MV, WV and DHSV. Additional "ESD solenoid" to remove hydraulic power to valves,	$4.4 \cdot 10^{-3}$	$5 \cdot 10^{-5}$

As seen from table A.12 the PFD is estimated to be 0.0044, and based on a pure quantitative consideration SIL 2 requirement is achievable for the isolation of a single well. By introducing a redundant ESD-logic (1oo2 voting), the example calculation would give a considerably lower PFD, and a SIL 3 is therefore clearly achievable.

Since isolation of the well is considered a crucial safety function, and since three valves are available for isolation, a SIL 3 requirement has been stated. As observed, this can be achieved by introducing redundancy with respect to safety in the ESD logic.
A quantitative risk analysis should be conducted to verify that the minimum SIL-requirement gives an acceptable risk when the total number of wells is taken into consideration. The following should be considered:

- Number of wells
- Production / injection wells with or without gas-lift
- Wells in connection with special operations, such as wire line, coiled tubing, work over, testing, cleanup, etc.

A simplified example of how a verification of the stated SIL 3 requirement can be performed using QRA, is given in Appendix C.2.

A.7 Isolation of riser

Definition of functional boundaries
Isolation of the riser occurs on demand from the ESD system, i.e. on detection of HC leaks or fire on the installation. The sub-function *isolation of riser* is defined as the function needed to isolate one riser:

- the ESD node
- one Riser Emergency Shutdown Valve (ESV) including solenoid and actuator

The sub-function starts at the unit where the demand is initiated (unit not included), and ends with the valve closing towards the riser. The sub-function is illustrated in Figure A.13 below.

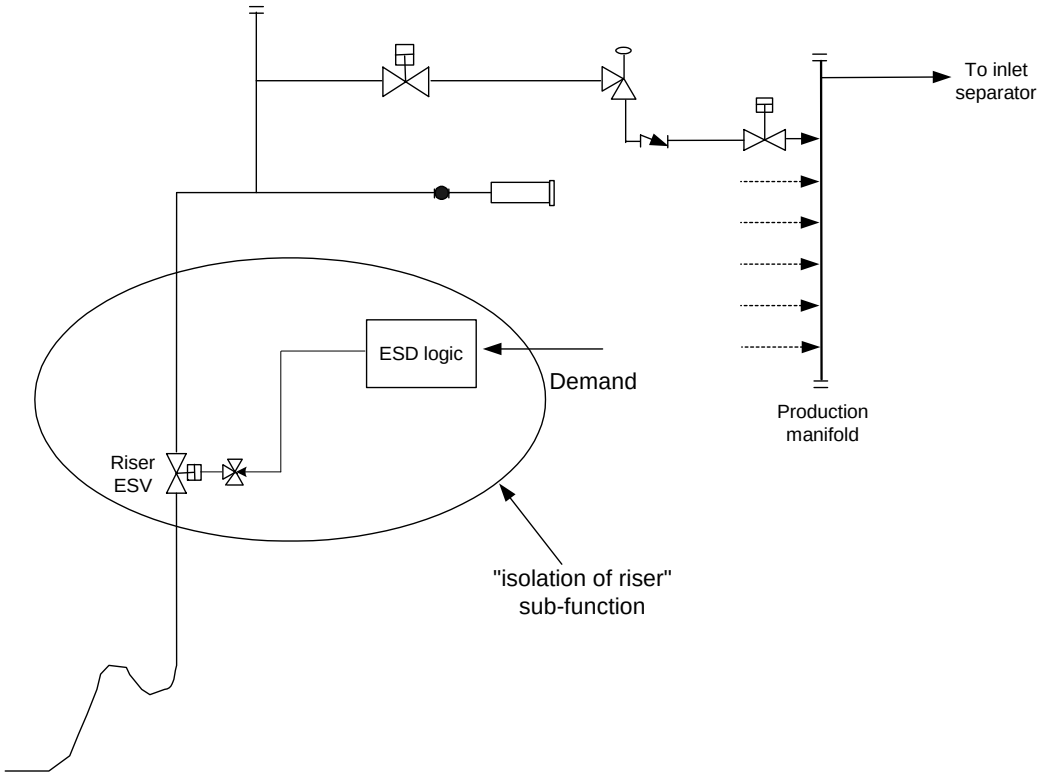

Figure A.13 Definition of the sub-function "isolation of riser"

Basic assumptions
The safe state of the process will be defined by closure of the riser ESD valve and isolation of the riser. It is here assumed that this safety function will be normally energised (NE), i.e. upon loss of power or signal, the ESD valve will close. Hence, the power source will not be included in the quantification of this safety function.

Quantification of safety functions
The RBD and calculations will be exactly as for "Segregation through ESD", see Section A.4. Thus the calculated PFD = 0.017. By considering the same measures as described in section A.4, a SIL 2 requirement should, consequently, be achievable. It may also be relevant to consider the use of two valves in order to achieve the SIL 2 requirement.
A quantitative risk analysis should be conducted to verify that the minimum SIL-requirement gives an acceptable risk. The following should be considered:

- number of risers
- fluid (gas, oil or condensate)
- process conditions (pressure, temperature)
- size/length of riser/flow line

A.8 Fire detection

Definition of functional boundaries
The Fire & Gas detection system consists mainly of detectors and Fire&Gas logic solvers. Fire detection is generally based on three principles, i.e. smoke detection, heat detection and flame detection:

- For smoke detection the sub-function starts when the smoke has entered the detection chamber, and ends with the signal given from the F&G system.
- For heat detection the sub-function starts when the radiation has entered the detection chamber, and ends with the signal given from the F&G system.
- For flame detection the sub-function starts when the flames are present at the detection device, and ends with the signal given from the F&G system.

Note that the fire detection sub-function is defined in terms of one single detector.

Basic assumptions
Safe state for the process will here be a signal from the F&G node. It is assumed that this safety function will be normally energised (NE), i.e. upon loss of power or signal to the detector or the F&G system, the described F&G actions will be activated.

It should be noted that if a large proportion of the fire detection systems in operation today apply dedicated fire–centrals. If a fire-central or some other equipment is used to interface between the detector and the F&G, this has to be included in the calculations. This has not been done in the example calculations below.

It should be noted that considerations related to number of and layout of detectors must be covered by separate studies (e.g. simulation studies and QRA).

Quantification of safety functions
The RBD is presented in Figure A.14. The PFDs for the three cases, *smoke detection, heat detection* and *flame detection* are presented in Table A.13. This indicates that a SIL 2 requirement is achievable for all three sub-functions.

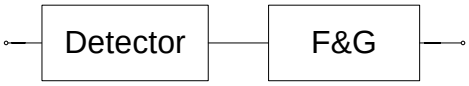

Figure A.14 RBD for fire detection sub-function

Table A.13 PFD and PSF results for fire detection

Function	PFD for F&G logic [1)]	PFD for one detector	PFD for function	PSF for function
1. Smoke detection	0.0044	0.0018	0.006	$6 \cdot 10^{-4}$
2. Heat detection	0.0044	0.0011	0.006	
3. Flame detection	0.0044	0.0035	0.008	

[1)] Note that the PFD figure for the F&G logic is based on a single system

Hence, a SIL 2 requirement is obtainable.

A.9 Gas detection

Definition of functional boundaries
Gas detection is in general based on two different principles; point detection and line detection:

- For point detectors the function starts when the gas has entered the detection chamber, and ends with the signal given from the F&G system.
- For line detectors the function starts when the gas has entered the beam, and ends with the signal given from the F&G system.

The F&G detection system will have different actions based on configuration of the logic. There are different actions depending on where the gas is detected, and typically for new platforms (signal is given at 20% of LEL);

- 1ooN detectors will give an alarm in CCR.
- 1ooN detectors in non-hazardous areas will give electrical isolation of this area.
- 2ooN in any area will give electrical isolation and stop production.

Here, the gas detection sub-function is defines in terms of one single detector.

Basic assumptions
Safe state for the process will here be a signal from the F&G node. It is assumed that this safety function will be normally energised (NE), i.e. upon loss of power or signal to the detector or the F&G system, the described F&G actions will be activated.

It should be noted that considerations related to number of and layout of detectors must be covered by separate studies (e.g. simulation studies and QRA).

Quantification of safety function
The RBD for a single gas detector is identical to that for fire detection (Figure A.14). The quantification for gas detection is given in Table A.14.

Table A.14 PFD and PSF results for gas detection sub-function (i.e. single detector)

Function	PFD for F&G logic [1)]	PFD for one detector	PFD for function	PSF for function
1. Catalytic detector	0.0044	0.0039	0.008	$6 \cdot 10^{-4}$
2. IR gas detector, point detector	0.0044	0.0015	0.006	
3. IR gas detector, line detector	0.0044	0.0015	0.006	

[1)] Note that the PFD figure for the F&G logic is based on a single system

From the table it is seen that a SIL 2 requirement is achievable. It should be noted that in Appendix D.7, some example calculations have been performed for different types of gas detection voting configurations.

A.10 Electrical isolation

Electrical isolation of ignition sources is typically initiated upon HC gas detection, confirmed fire detection, high level in KO drum and manual ESD activation.

Definition of functional boundaries
The SIL-requirement applies for the subsystem needed for electrical isolation given signal from F&G node, i.e.:

- F&G node
- Circuit breakers / relay

The function starts at the unit initiating the demand (unit not included), and ends when the equipment is isolated.

Note): Electrical isolation may also include the ESD system, e.g. if isolation of ignition sources is performed via ESD. If so also
the ESD node must be included in the SIL calculations.

Basic assumptions
Electric isolation is initiated from the F&G detection system. There are different actions depending on where the gas is detected. On new platforms, 1ooN detection in non-hazardous area gives electrical isolation of this area, while 2ooN in any area isolates this area or shut down main power.

The safe state for the process will be to isolate electric ignition sources. Hence, upon loss of power or signal, the ignition sources will be automatically isolated and this function is therefore assumed to be NE.

It should be noted that isolation of certified explosion proof equipment is not regarded as part of the basic requirements for this safety function. Isolation of Ex. equipment is seen as an additional safety measure but is not an absolute requirement (ref. NORSOK S-001N).

Quantification of safety function
The RBD is presented in Figure A.15, for the case of 6 circuit breakers. The PFD values are presented in Table A.15, using data for 6kV-10kV circuit breakers.

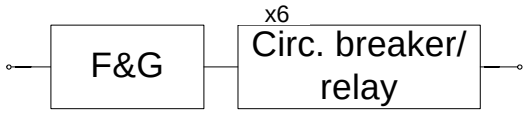

Figure A.15 RBD for Electrical Isolation

Table A.15 PFD results for Electrical isolation. Example with 6 circuit breakers

Component	No. of components	PFD per component	Total PFD	Total PSF
F&G logic + I/O [1)]	1	$4.4 \cdot 10^{-3}$	$4.4 \cdot 10^{-3}$	$5 \cdot 10^{-5}$
Circ. Breaker (6kV–10kV)	6	$1.8 \cdot 10^{-3}$	$10.8 \cdot 10^{-3}$	
Total Function [2)]	**-**	**-**	**0.0152**	**$5 \cdot 10^{-5}$**

[1)] Note that the PFD figure for the F&G logic is based on a single system.

[2)] Often activation of electrical isolation will be implemented via the ESD system. In such case failure of the ESD logic should also be included in the failure estimate.

As seen from the above table it will not be straightforward to achieve a SIL 2 requirement for this function. Using the data from Table A.3 would allow only 3 circuit breakers included in the function in order to obtain the quantitative SIL 2 target. Of course, test interval < 24 months would help. Also it should be noted that the F&G logic has been assumed to be a single system. To conclude, the SIL 2 requirement can be achieved if only a few circuit breakers need to open or if other measures are implemented (e.g. more frequent testing).

A.11 Firewater supply

Definition of functional boundaries
The system boundaries includes

- the fire water demand signal processed in the fire pump logic
- start of fire pumps
- opening of one deluge-valve (given confirmed fire).

It is here assumed that the firewater pump system consists of 2x100 % capacity pumps.

The nozzles, water intake, strainers, ring main etc. are not included but are assumed covered by inspection and maintenance program.

The function starts at the unit initiating the demand (unit not included), and ends when there is flowing water through the deluge valve.

Basic assumptions
Safe state for the process will be that fire water is released. This safety function will however be normally de-energised, due to the inconvenience related to a spurious release of firewater. It is therefore important that the UPS power supply for opening of the deluge valve is included in the calculations. Here, the following is however assumed:

- the power supply from the UPS to the deluge valve will be continuously monitored (e.g. by routing the 24V supply into the F&G logic through a separate input card);
- upon loss of signal, an alarm will be given in the CCR;
- compensating measures (or a shutdown) will be initiated immediately in case of an alarm.

Hence, a failure of the UPS power supply will have a very high degree of coverage (i.e. in IEC terms most of the UPS power supply failures become dangerous detected failures). Therefore, for the purpose of the below example calculations, the same PFD figure has been used for the F&G logic as for normally energised functions.

During actual calculations / verifications, it is important that these aspects are considered specifically for the installation under consideration. Furthermore, it should be verified that the reliability data applied for equipment in such de-energised functions do reflect the relevant failure modes (e.g. for the logic solver).

Quantification of safety function

The RBD is presented in Figure A.16. The resulting PFD calculations are given in Table A.16. Note that included in the "F-W pump" boxes are the fire water diesel engine, the generator, the electric motor and the pump itself.

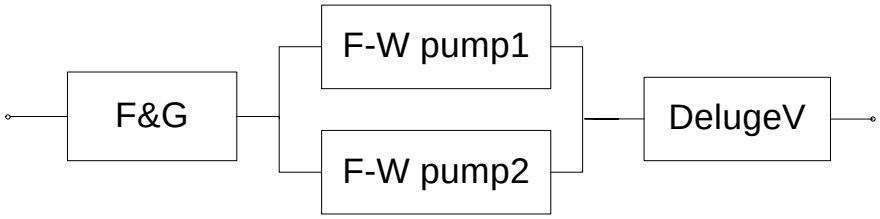

Figure A.16 Reliability block diagram for deluge function

Table A.16 PFD results for deluge

Component	Voting	PFD per component	System PFD	System PSF
F&G logic + I/O	1oo1	$4.4 \cdot 10^{-3}$	$4.4 \cdot 10^{-3}$	$5 \cdot 10^{-5}$
Fire water pump	1oo2	$9.4 \cdot 10^{-4}$	$5 \cdot 10^{-5}$	-
Fire water diesel engine	1oo2	$1.9 \cdot 10^{-3}$	$1 \cdot 10^{-4}$	-
Electric generator	1oo2	$1.4 \cdot 10^{-3}$	$7 \cdot 10^{-5}$	-
Electric motor	1oo2	$1.4 \cdot 10^{-3}$	$7 \cdot 10^{-5}$	-
Deluge valve	1oo1	$1 \cdot 10^{-2}$	$1 \cdot 10^{-2}$	-
Total Function	**-**	**-**	**0.015**	**$5 \cdot 10^{-5}$**

The above quantifications indicate that only a quantitative SIL 1 level is obtained. As seen from the above table a SIL 2 function can be achieved by:

- better (verified) reliability data for the deluge valve and/or more frequent testing of the valve
- for the F&G logic a failure rate (λ_{DU}) of $1 \cdot 10^{-6}$ per hour has been applied, i.e. corresponding to the failure rate for a single system. Typically, the F&G system will have redundant CPUs and I/Os, and based on the type of redundancy applied, a lower failure rate for the overall F&G logic may be argued;

It is therefore concluded that the SIL 2 requirement is achievable and this requirement is therefore given.

A.12 Ballasting Safety Functions

A.12.1 Sub-function: Start of ballast system for initiation of rig re-establishment

Definition of functional boundaries

The purpose of rig re-establishment is to restore acceptable inclination and draft after an accidental event.
The sub-function starts when the operator has demanded emptying of one ballast water tank, and ends when emptying of that tank has been initiated. The following equipment is involved in the sub-function, ref. Figure A.17 below:

- Ballast control node
- Tank valve
- Ballast control pump (2x100%)
- Ringmain/manifold valve
- Discharge valve

The valves are fail close, motors are fail stop, and ballast control output signals are fail close/stop.

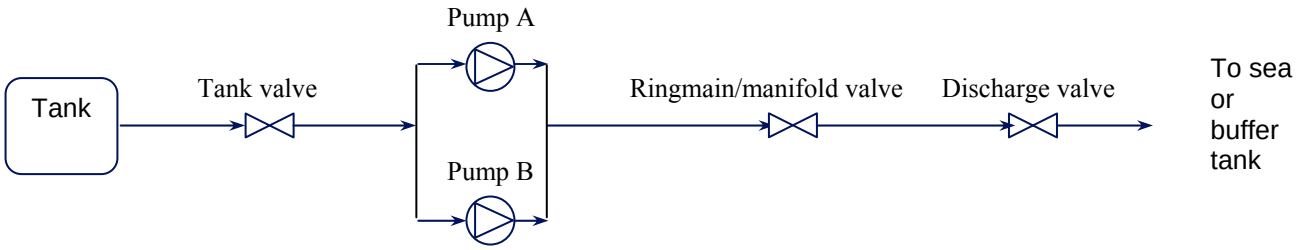

Figure A.17 Definition of the ballast control sub-function for initiation of rig re-establishment

Basic assumptions

Safe state for the installation will be to start the ballast pumps in order to restore acceptable inclination and draft after an accidental event. There might, however, be situations when start of the ballast pumps is not desirable and this safety function is therefore normally de-energised.

In order to start the ballast pumps, the UPS power (and main electric supply) will be required; hence the UPS power and the main electric supply should be included in the PFD calculations. As for the firewater function, the following is, however, assumed:

- the power supply from the UPS to the control system will be continuously monitored (e.g. by routing the 24V supply into the ballast control logic through a separate input card);
- the power supply to the ballast pumps will also be continuously monitored (e.g. by routing the electric power supply into the ballast control logic through a separate input card);
- upon loss of signal, an alarm will be given in the CCR;
- compensating measures (or a shutdown) will be initiated immediately in case of an alarm.

Hence, power supply failure will have a very high degree of coverage (i.e. in IEC terms most of the power supply failures become dangerous detected failures). Therefore, for the purpose of the below example calculations, the same PFD figure has been used for the logic as for normally energised functions.

During actual calculations / verifications, it is important that these aspects are considered specifically for the installation under consideration. Furthermore, it should be verified that the reliability data applied for equipment in such de-energised functions do reflect the relevant failure modes (e.g. for the logic solver).

Quantification of safety function

The RBD is presented in Figure A.18. The resulting PFD calculations are given in Table A.17.

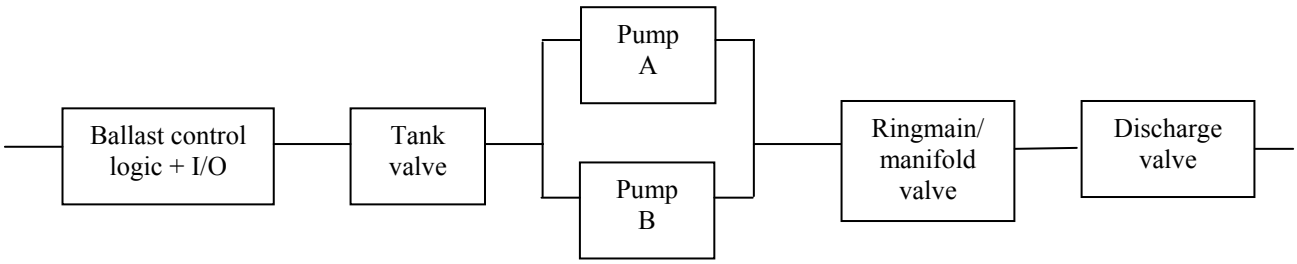

Figure A.18 RBD for ballast control sub-function for initiation of rig re-establishment

Table A.17 PFD results for initiation of rig re-establishment.

Component	Voting	PFD per component	System PFD	System PSF
Ballast control logic + I/O	1oo1	$4.4 \cdot 10^{-3}$	$4.4 \cdot 10^{-3}$	$5 \cdot 10^{-5}$
Tank valve + solenoid/pilot	1oo1	$1 \cdot 10^{-2}$ Note 1	$1 \cdot 10^{-2}$ Note 1	-
Pumps	1oo2	$9.4 \cdot 10^{-4}$ Note 2	$5 \cdot 10^{-5}$ Note 2	-
Ringmain/manifold valve + solenoid/pilot	1oo1	$1 \cdot 10^{-2}$ Note 1	$1 \cdot 10^{-2}$ Note 1	-
Discharge valve + solenoid/pilot	1oo1	$1 \cdot 10^{-2}$ Note 1	$1 \cdot 10^{-2}$ Note 1	-
Total function	-	-	**0.034**	**$5 \cdot 10^{-5}$**

General: note that states after completion of relevant actions are generally opposite of the fail safe states. Assumed test intervals are weekly for the pumps, 6 months for valves and 12 months for the ballast control logic.
Note 1: Assumed identical to deluge valve, for which failure is failure to open, and the control signal loop is normally de-energised
Note 2: Assumed same figure as for "fail to start" for fire water pumps in deluge function

As seen from the above table, the quantifications indicate that a SIL 1 requirement can be achieved. It should be noted that the ballast system is run more or less continuously on a floating installation. Hence, it may be argued, that the test interval for the logic and the valves will be more frequent than the intervals assumed above.

A.12.2 Sub-function: Emergency stop of ballast system

Definition of functional boundaries

The Norwegian Maritime Directorate specifies that there shall be an emergency stop mechanism of the ballast system in addition to and separate from the programmed ballast control functions. The purpose of such an emergency stop function is to ensure a safe installation by closing all relevant valves and stopping all relevant pumps, i.e. the ballast control valves/pumps, and for installations with cargo storage, cargo handling valves/pumps as well.

The sub-function starts when the operator has operated the emergency stop pushbutton, and ends when the pump motor has stopped and the valve has closed. The following equipment is included in the sub-function:

- Emergency pushbutton
- Safety relay
- Isolation relay
- MCC shutdown relay
- Contactor to the motor
- Valve assembly (solenoid/pilot/valve)

Basic Assumptions
Safe state for the installation will in this case be to stop the ballast pumps and close valves.

This sub-function will be independent of all utility systems since upon loss of power the function goes to a safe state (i.e. relays and contactors will open and the valves will close). The emergency pushbutton is manual, operate-to-open.

Quantification of safety function
The RBD is presented in Figure A.19. The resulting PFD calculations are given in Table A.18.

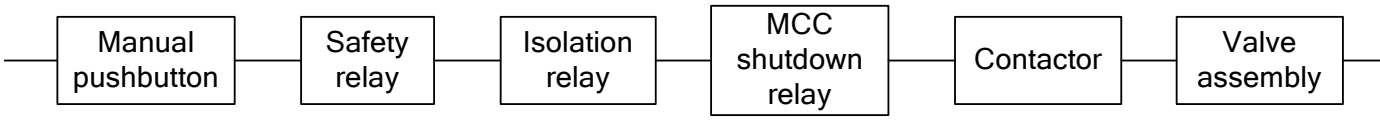

Figure A.19 RBD for the sub-function emergency stop of ballast system

Table A.18 PFD results for emergency stop of ballast system

Component	No. of components	Total PFD	System PSF
Emergency pushbutton	1	$4.4 \cdot 10^{-4}$ Note 1	$1 \cdot 10^{-5}$ Note 1
Safety relay	1	$1.75 \cdot 10^{-3}$ Note 2	-
Isolation relay	1	$1.75 \cdot 10^{-3}$ Note 2	-
MCC shutdown relay	1	$1.75 \cdot 10^{-3}$ Note 2	-
Contactor	1	$1.75 \cdot 10^{-3}$ Note 2	-
Valve	1	$8.8 \cdot 10^{-3}$ Note 3	$0.5 \cdot 10^{-5}$
Solenoid / pilot	1	$3.9 \cdot 10^{-3}$ Note 3	-
Total function	**-**	**0.020**	**$1.5 \cdot 10^{-5}$**

General: A two year test interval has been assumed throughout for relays and contactors, except for solenoid/pilot/valve where a 1 year test interval is assumed.
Note 1: Values taken from the PDS handbook (λ_{DU} for ESD pushbutton = $0.2 \cdot 10^{-6}$).
Note 2: A λ_{DU} for relays and contactors of $0.2 \cdot 10^{-6}$ has been applied throughout.
Note 3: Standard failure data for shutdown valves and solenoid are applied (ref. Table A.3).

As seen from the above quantifications, only a SIL 1 requirement is met with the given assumptions. However, by increasing the test frequency for relays and contactors (from 24 months) and for the valve assembly (from 12 months), and/or by introducing redundancy of the valves, a SIL 2 requirement seems achievable and is therefore stated.

A.13 Isolation of subsea well

Definition of functional boundaries
The isolation function concerns only the ESD functions related to the isolation, not the overpressure protection realised through the PSD system.

The sub-system *isolation of subsea well* is defined as the system needed to isolate one well. For a standard subsea well, the sub-system normally consists of the following:

- Topside/onshore located ESD node
- Topside/onshore located ESD hydraulic bleed down solenoid valve in HPU and/or
- Topside/onshore located EPU ESD electrical power isolation relay in EPU
- Production Wing Valve (PWV) and Chemical Injection Valve (CIV) including actuators and solenoid(s)
- Production Master Valve (PMV) including actuators and solenoid(s)
- Down hole safety valve (DHSV) including actuators and solenoid(s)

The function starts at the unit where the demand is initiated (unit not included), and ends with the valves shutting in the well. The sub-function “isolation of subsea well” is illustrated on figure A.20 below.

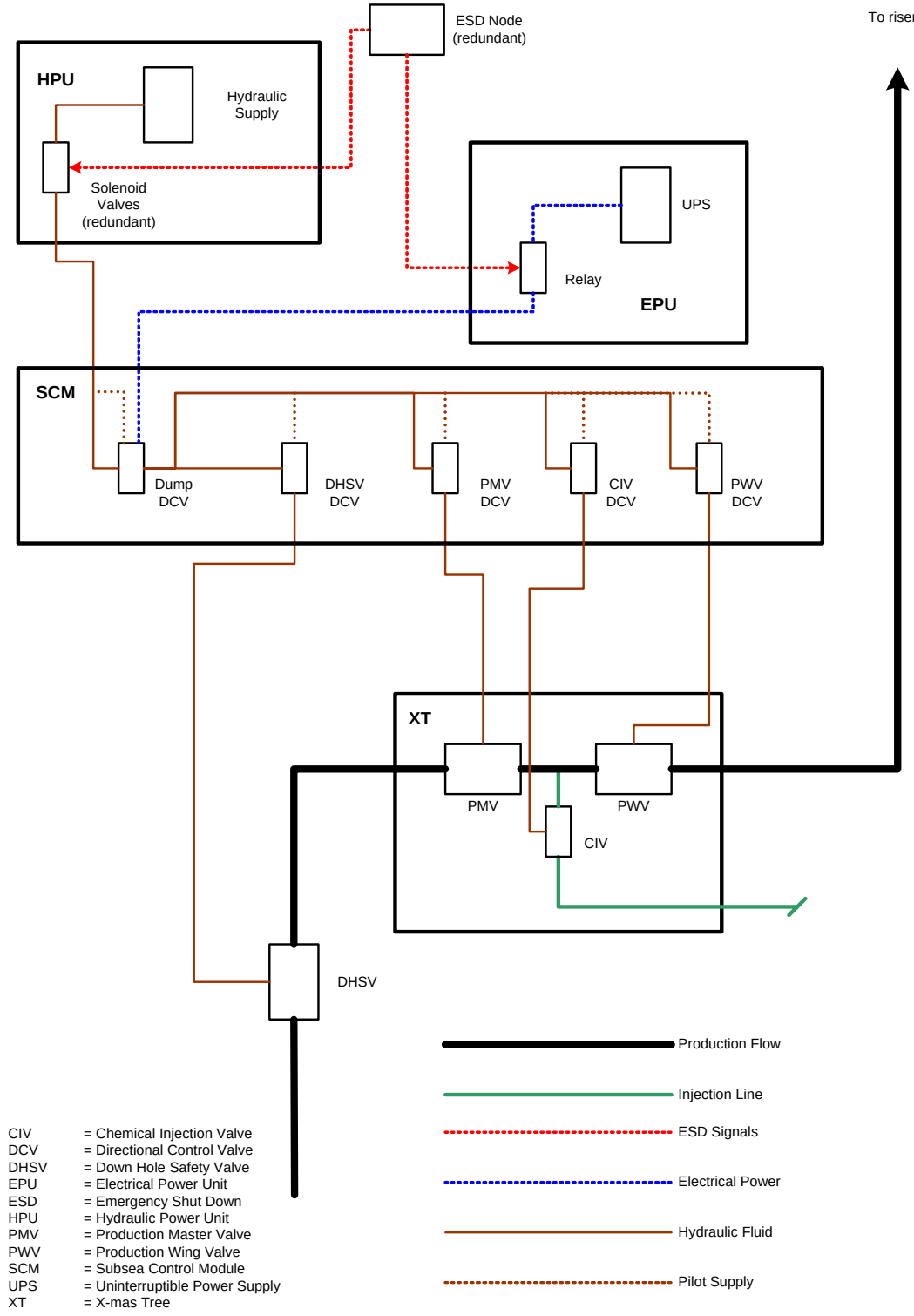

Figure A.20 Definition of the sub-function "isolation of subsea well"

Basic Assumptions

All valves for well isolation (PWV, CIV, PMV and DHSV) are assumed hydraulically fail-safe. The Directional Control Valves (DCV) are assumed hydraulically fail-safe vent and the optional "Dump" DCV electrically fail-safe vent.

Depending on the scenario having triggered the demand for isolation, one of the well isolation valves (PMV) will be sufficient to isolate the well. However, in the event of the highest levels of shut down, the well should be isolated by the DHSV. The well or inlet to the platform/plant will also be isolated due to PSD demands, but these are not

included in this function. Depending on for example the event and Cause&Effect (C&E), this may cause a demand on the same valves or other valves.

For design cases where the pipeline and/or risers are not rated for full shut in pressure, this should be treated as a deviation. See section 7.7 and appendix C.

Quantification of safety function

The function "ESD isolation of one subsea well", can be represented by a Reliability Block Diagrams as shown in Figure A.21 below. Note that there are 3 different modes of operation, only dangerous undetected failure modes are calculated and the RBD is slightly simplified.

The relevant operational modes are:

Table A.19 Operational modes relevant for subsea ESD isolation

Function	Components not part of function	Comment
APS isolation of well (both hydr. & el.)	None	Closing of all well isolation valves
ESD isolation of well (hydraulic)	EPU, Dump DCV, DHSV DCV, DHSV	Closing of X-mas tree isolation valves only
ESD isolation of well (electrical)	HPU, DHSV DCV, DHSV	Closing of X-mas tree isolation valves only

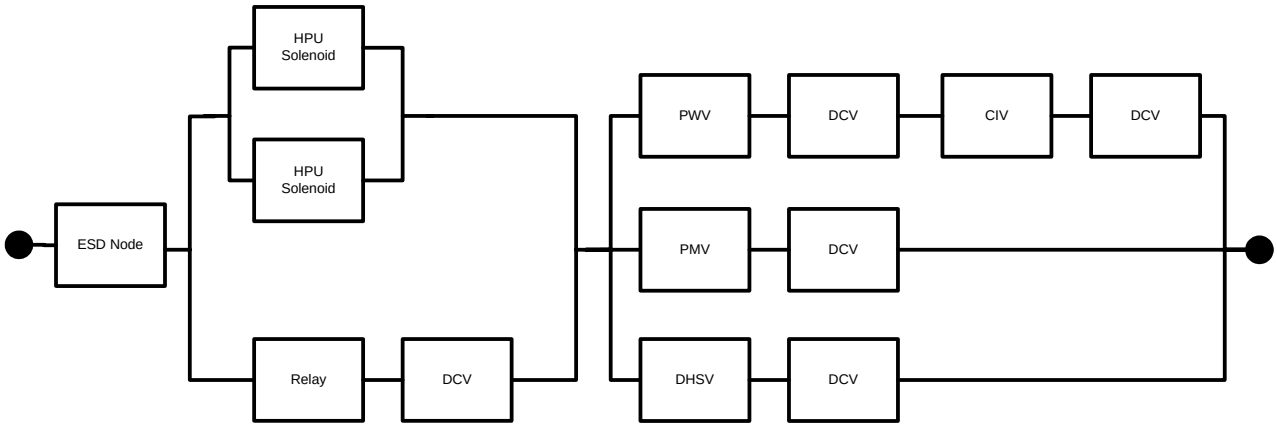

Figure A.21.1 RBD for Abandon Platform (APS) isolation of well, hydraulic bleed down in HPU and electric power disconnect in EPU

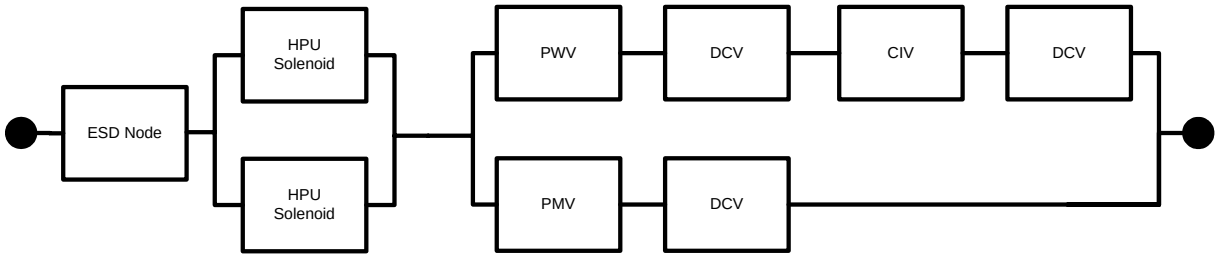

Figure A.21.2 RBD for ESD isolation of well, hydraulic bleed down in HPU

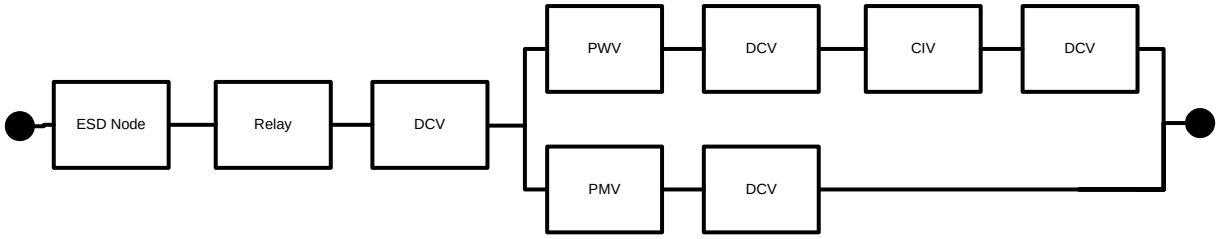

Figure A.21.3 RBD for ESD isolation of well, electric power disconnect in EPU

The assumed analysis input is given in Table A.20 below.

Table A.20 PFD input for safety function "ESD isolation of one subsea well"

Component	PFD (single comp.)	PFD (duplicated comp.)	PSF (single comp.)	PSF (duplicated comp.)
ESD logic	$4.38 \cdot 10^{-3}$	$2.2 \cdot 10^{-4}$	$5 \cdot 10^{-5}$	$2.5 \cdot 10^{-5}$
HPU Solenoid	$1.97 \cdot 10^{-3}$	$2.0 \cdot 10^{-4}$	-	-
DCV [1)]	$2.2 \cdot 10^{-4}$	$2.2 \cdot 10^{-5}$	-	-
PMV/PWV	$2.2 \cdot 10^{-4}$	$2.2 \cdot 10^{-5}$	$1 \cdot 10^{-5}$	$1 \cdot 10^{-6}$
DHSV	$5.48 \cdot 10^{-3}$	$5.5 \cdot 10^{-4}$	$1 \cdot 10^{-5}$	$1 \cdot 10^{-6}$
CIV	$8.8 \cdot 10^{-4}$	$8.8 \cdot 10^{-5}$	$1 \cdot 10^{-5}$	$1 \cdot 10^{-6}$
Relay	$1.18 \cdot 10^{-3}$	$1.2 \cdot 10^{-4}$	-	-

Note [1)]: The DCVs in figure A.20 will operate in different modes: (1) Dump mode, the valve is electrically held open and has fail safe dump hydraulic pressure, (2) Hydraulic bleed down mode, where the DCV fail safe shift to vent upon loss of hydraulic pressure and (3) Flow by mode, where the function and supply line ports are connected by small flow path. Due to lack of data no spilt has been made between these three modes in table A.3.

For all components a β-factor of 10% has been used, except for ESD logic where a β-factor of 5% has been used. A β-factor of 10% has also been applied to the PSF, except for the ESD logic where a β-factor of 50% has been applied for systematic failures in duplicated logic. The following common mode failures are included in the analysis model:

- failures affecting redundant ESD logic
- failures affecting both HPU solenoids
- failures affecting all DCVs in SCM
- failures affecting PMV and PMV

For all components a test interval of 4380 hours has been assumed, except for ESD logic (located topside), where a test interval of 8760 hours has been used.
The ESD node and HPU solenoids have been assumed to be redundant.
Based on the above assumptions, the PFD figure has been calculated for the safety function.

Table A.21 Estimated PFD for "ESD isolation of one subsea well"

Function	ESD Node	PFD	SIL
APS isolation of well (both hydr. & el.)	Redundant	$2.4 \cdot 10^{-4}$	**3**
ESD isolation of well (hydr.)	Redundant	$4.7 \cdot 10^{-4}$	**3**
ESD isolation of well (el.)	Redundant	$1.7 \cdot 10^{-3}$	**2**

When cutting hydraulic power topside to close subsea valves, it is necessary to take into account the time it takes to bleed off the hydraulic fluid. This may be case specific, and in some cases hydraulic bleed-off topside will not be good enough due to the long bleed-off time. Here electrical cut should be considered for the ESD isolation.

A.14 Drilling and well intervention

A.14.1 Drilling related safety functions

There are a number of safety functions related to the drilling and well intervention operations. These safety functions are allocated to and realised by instrumented safety systems, by mechanical systems, by procedures and by personnel. The following safety functions / systems have been discussed explicitly in this appendix:

- *Drilling Blowout Preventor (BOP) function*
- Well Intervention BOP function
- Kick detection function
- Mud circulation function
- Kill function
- Marine Drilling Riser – Anti Recoil function
- Marine Drilling Riser – Emergency Disconnect function
- Lifting, Rotation and Pipe Handling

Explicit SIL requirements have only been put upon the first function, i.e. the drilling BOP function. For the other safety functions no explicit minimum SIL requirements have been stated. The reason for this is further discussed in section A 14.3 and A.14.4.

A.14.2 Drilling BOP

The relevant safety functions are prevention of blowouts and prevention of well leaks.

Definition of functional boundaries
The sub-function includes:

- The panels necessary to activate the function
- The signal transmission and hydraulics necessary
- The individual valves and equipment of the BOP

See Figure A.22 and A.23 for an overall description of the systems involved.

The design of BOP control is based on a combination of electrical/electronic control as well as hydraulic control. There is a wide variety of system designs available on the market; ranging from those that are primarily hydraulically operated to those primarily electronically controlled. This guideline is limited to the electrical/electronic control systems and standard BOP functions.

The following functions are defined for the BOP:

1. Seal around drill pipe
2. Seal an open hole
3. Shear drill pipe and seal off well

Function 1 above is the most commonly used. The BOP has annular preventors and pipe ram preventors for the purpose. There can be limitations to when the pipe rams work properly, such as closing on drill collars, tool joints, perforation guns, etc.

For function 2, the blind shear ram will be the means to seal the well. If a leak should occur there will be a possibility to run pipe in the hole and close the annular around the pipe. The blind shear ram may then be opened and the pipe stripped further in so the pipe rams may also be used.

For function 3 above the drill pipe has to be sheared before the well can be sealed off. Historically this has been an event where the well has blown out through the drill string and stabbing the top drive and/or the Kelly valve on the drill floor has failed. It is not industry practice to test on a regular basis the function of the shear ram with pipe in the BOP. It is considered a destructive test. Factory acceptance testing is performed for the BOP to shear a pipe.

A typical BOP is shown in figure A.22

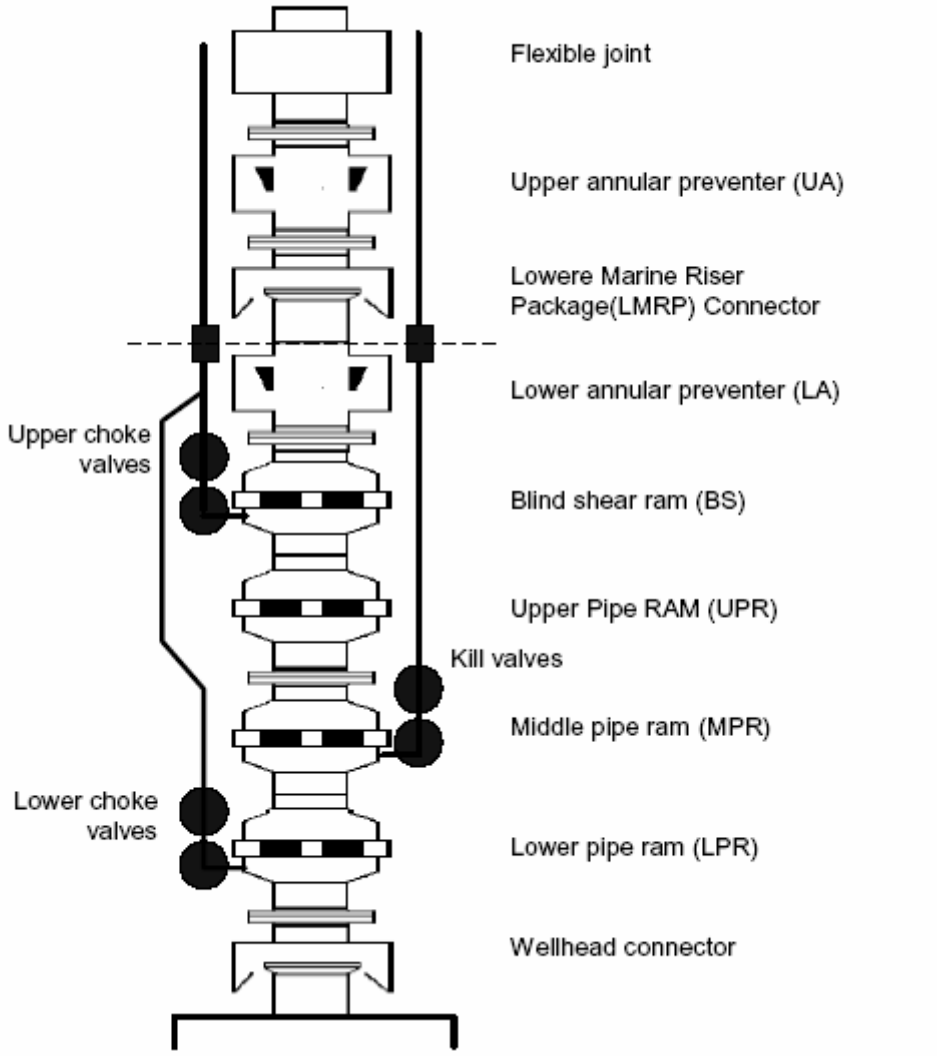

Figure A.22 A typical BOP (SINTEF)

The total safety function addressed in this guideline includes activation from the drillers console or the tool pushers console and the remote operated valves needed to close the BOP sufficiently so as not to lead to a blowout.

A simplified schematic of a typical BOP control system is shown in figure A.23 below.

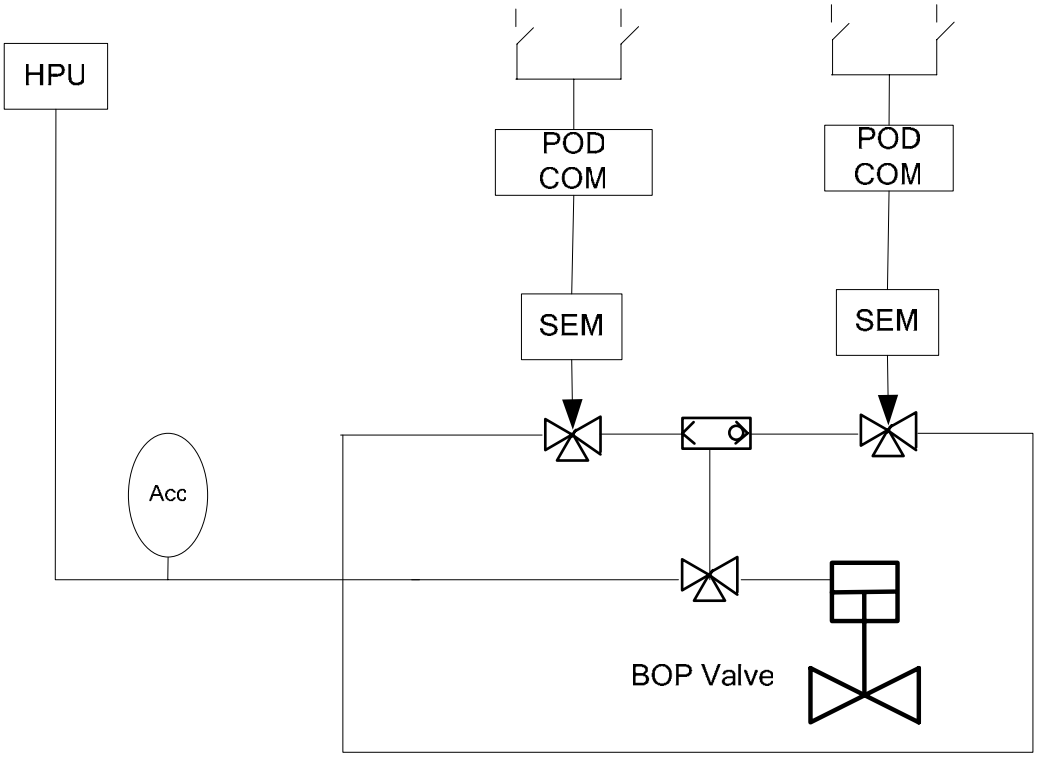

Figure A.23 Schematic of simplified BOP control system

The pushbuttons are normally located at Driller's and Tool Pusher's panels, and operate in a 1oo2 configuration for both channels of the redundant control system. As the solution is not electrically fail safe, the power to the system has to be monitored. The same applies to the HPU's since hydraulic power has to be present in the accumulator to operate the pilot and valves.

Basic assumptions
In this document the SIL function related to closing in the well has been restricted to closing of the valve(s) and do not include the actual shearing of the pipe. Functions 2 and 3 as discussed above can thus be combined; i.e. closing of the blind shear ram.

Hence, we differentiate between two main functionalities and set SIL levels for:

- the annular/pipe ram function (i.e. function 1);
- the blind shear ram function (i.e. functions 2 and 3 combined).

The function starts when the operator (e.g. driller, tool pusher) pushes the button to close the well and ends when the BOP closes and seals off the well.

The safe state of the process is a sealed well without blowouts or leakage.

Quantification of safety function
In this section some different statistics related to BOP reliability and blow-out frequencies are discussed in order to arrive at a reasonable SIL requirement for the above defined functions.

Scandpower report
On the basis of the Scandpower Report, Blowout and Well Release Frequencies 27.005.004/R2, combined with activity data and kick data from the PSA, the following probabilities of failure can be estimated.

PFD Exploration Drilling BOP

- Average BO frequency Exploration Drilling, estimate: 4.1×10^{-4} per well drilled
- Average Kick probability P_{kick}: 16%
- Coarse Approximation:
  - 1 Well Drilled x P_{kick} x $PFD_{BOP} < 4.1 \times 10^{-4}$
  - $PFD_{BOP} < 2 \times 10^{-3}$

PFD Development Drilling BOP

- Average BO frequency Development Drilling, estimate: 1.0×10^{-4} per well drilled
- Average Kick probability P_{kick}: 8%
- Coarse Approximation:
  - 1 Well Drilled x P_{kick} x $PFP_{BOP} < 1.0 \times 10^{-4}$
  - $PFP_{BOP} < 1 \times 10^{-3}$

The data discussed above indicates that the industry is operating with a "blowout prevention reliability" somewhere close to SIL 3 on average; *which includes electronic and manual systems*. The estimates include activation from the drillers console, the tool pushers console and the manual panel and valves needed to close the BOP sufficiently so as not to lead to a blowout. Closing of the drill string or circulating mud would be included in the above estimate, as would closing of the shear seal or closing of the pipe rams with IBOP or sub. Consequently, the "blowout prevention reliability" discussed above will include operational measures additional to the defined BOP functions, and the BOP function may therefore be somewhat less reliable than SIL 3.

RNNS (Risikonivået på Norsk Sokkel) data
Data from the RNNS project (2002 and first half of 2003) has been reviewed for the function "BOP isolation". Failure of this function is in RNNS reported per valve. From the RNNS data one has 459 tests of single valves in a BOP and of these 17 are reported as failures. This gives a PFD estimate of 17/(2*459) = 0.0185 for closing one of the valves in the BOP.

It should be noted that there are several uncertainties related to the RNNS BOP data:
- The data only include reports from some operators and some installations
- The RNNS data may include "start-up" tests, i.e. tests prior to the actual use of the BOP (when the time period since last application may exceed one week by far)

When the BOP is in actual use the valves will in reality be tested once a week, as a pressurization and functional test are both performed weekly, but shifted one week.

SINTEF studies
Studies of operational data by SINTEF[2] indicate that the PFD for closing of the BOP to prevent a kick is close to 0.001 and that the PFD for closing any of the valves is less than 0.005. (For the annular preventor, 4 failures are reported for 7449 days in service and test is performed every 14 day i.e. 7449/14=532 tests, 4/(2*532) =0.0038).

The above is directly applicable for the blind shear ram, showing that a SIL 2 may be achieved. As cutting e.g. the drill pipe at the joint is not possible, proper control of positions is important for the successful operation. It is also assumed above that the blind shear ram is properly sized to cut the pipe. Testing with a pipe is a destructive test; therefore all functional testing is performed with open hole.

For sealing of the annulus, several valves are available. For the well to be under control when only the annulus valves are used, also the drill pipe have to be closed topside, or mud balancing the reservoir pressure has to be applied.

Conclusion:

[2] SINTEF reports: STF38 A99426 Reliability of Subsea BOP Systems for Deepwater Application, Phase II DW and STF38 A01419 Deepwater Kicks and BOP Performance, Unrestricted version

Setting a SIL 3 level to either function would lead to a significant increase in the standard for drilling BOPs. The challenge lies mainly in the need for documentation of the system reliability. Setting a SIL 3 level would most certainly also result in the need for changing existing control system. It would also be necessary to include additional rams in standard BOP assemblies.

The required PDF/SIL for the BOP function for each specific well should be calculated and a tolerable risk level set as part of the process of applying for consent of exploration and development of the wells. As a minimum the SIL for isolation using the annulus function should be SIL 2 and the minimum SIL for closing the blind / shear ram should be SIL 2.

A.14.3 Well intervention BOP

The blowout frequencies for well intervention blowouts can be obtained from the Scandpower report BLOWOUT FREQUENCIES, 27.005.004/R225 April 2003

Wireline : 2.5×10^{-6} per operation
Coiled Tubing : 1.1×10^{-4} per operation
Snubbing : 1.3×10^{-4} per operation

The demand rate for the BOP, i.e. failure of the injector heads or failure of tubing/snubbing pipe, can not be extracted from these data. The equipment failure rates are not known. Furthermore, variation between subsea and platform well intervention BOP's is not known.

The frequency of coiled tubing and snubbing related blowouts, per operation, have been increasing in recent years.

For wireline operations, the master valve can be used as a barrier in addition to the wireline BOP. For such operations there is also one less leak path through the intervention tubing/pipe. This is reflected in the significantly lower blowout frequency for wireline operations.

A high injector head/tubing failure rate would indicate very reliable BOP based on the blowout statistics. On the other hand, a low failure rate would indicate a low reliability of the BOP. A reasonable estimate for the failure rate of the injector head/tubing will be somewhere between 0.1 and 0.01 per operation. This would indicate a BOP failure on demand rate in the order of 1×10^{-3} - 1×10^{-2}, i.e. a SIL 2. This is at best a coarse estimate.

It should be noted that for coiled tubing and snubbing operations, a SIL 3 system; i.e. X-mas tree and downhole safety valve, is overridden by a less reliable system. The demand on the system is also increased because packing systems are less reliable than welded pipe. This is of course for a short period of time and has been accepted up to date.

Conclusion:
Background for setting a minimum SIL requirement is not found to be available.

A.14.4 Other drilling related safety functions

As discussed in A.14.1, there will be a number of other safety functions related to the drilling operation. These are discussed separately below.

A.14.4.1 Kick detection

The broad definitions of kick detection systems that were evaluated are:

Historical

- Tripping - Level measure of trip tank gain / loss with alarm
- Drilling - Difference between flow in and flow return and gain / loss

New Technology

- Early kick detection. Sensors that detect pressure waves, monitor rig movement, stand pipe pressure gain / loss combined with mathematical models (multi-parameter comparison)
- Well stability analyser – losses, wash out, restrictions, etc.

The response to a kick alarm depends on the combined judgement of the situation by the mud logger, driller and tool pusher / drilling supervisor. Alternative responses include start of circulation, increase mud weight or closure of the BOP. Without the kick detection system, assessment of loss of well control and ultimate action for closing the BOP will be taken.

Kick detection is only one of the information elements required in the decision process for activating the BOP.

Kick detection is required for process control of the mud column. It does not automatically initiate an action.

Conclusion:
It is not recommended to set a minimum SIL requirement for kick detection

A.14.4.2 Mud circulation

The mud circulation system is one of the two main barriers for drilling and completing a well. The mud column and its control is an operations function, even though loss of control can lead to an emergency situation. It is comparable thus to the process control function of a process plant; only in instances of loss of process control (LAHH, LALL, PAHH, TALL, etc.) are minimum SIL requirements set for the safety function. Similar is the case for the mud column, e.g. in case of loss of well control, requirements for the safety function "closing the BOP", are set.

The reliability of the mud circulation system as a barrier is very dependent on geological factors of the well, mud mixing and the knowledge of the people involved. The impact of the instrumented systems is marginal.

Conclusion:
It is not recommended to set a minimum SIL requirement for the mud circulation system.

A.14.4.3 Well kill

The kill system has the following primary functions:

- Dynamic killing
- Re-establishment of mud barrier after BOP closed

Dynamic killing when drilling riserless may be the only safety function for preventing flow of hydrocarbons to sea. The ability to move the rig off location will be the main safety function for saving personnel.

The kill system is not an instrumented system but a safety related system based on other technology.

Conclusion:
It is not recommended to set a minimum SIL requirement for the kill system.

A.14.4.4 Marine drilling riser – anti recoil system

The anti-recoil system is a complex instrumented system and its function will be to:

- Prevent any damage in the moon pool area in the event of an emergency disconnect

The damage potential in case of failure is significant. Failure of the anti-recoil system and subsequent damage is, however, a rare event. The likelihood that there is a person in the area when this event happens is even lower since the moon pool area is normally unmanned.

Under the assumption that the moon pool is normally not manned, the safety function is related to economic loss. Based on this it is not recommended to set a minimum SIL requirement.

Conclusion:
It is not recommended to set a minimum SIL requirement for the anti-recoil system.

A.14.4.5 Marine Drilling Riser – Emergency Disconnect System

The safety function of the emergency disconnect system is:

- Close the BOP and disconnect from the well. The disconnect is required to prevent damage to the wellhead and BOP in the event that the drilling rig moves off location which can lead to damage to environment or loss of lives on the rig. The causes for demands on the emergency disconnect are:
  - drift off, or
  - drive off
- Allow the rig to move off location in the event of an uncontrolled blowout.

The demand rate for the first safety function is about once per year per rig based on an IMO DP Class 3 rig.

The marine drilling riser is a causal mechanism for blowout and is thus a subset of the BOP discussions. When drilling subsea wells, the reliability of the emergency disconnect function needs to be evaluated as part of the application for consent process and a tolerable risk level must be decided.

In the event if improper disconnect of the marine drilling riser, this can lead to a blowout, i.e. the water column cannot maintain well pressure. If the demand rate for emergency disconnect function is on the order of 10^{-1} - 10^{-2} per well, the disconnect and isolation should be at SIL 2 level to maintain a blowout frequency corresponding to a historical level.

Another event is that the marine drilling riser is improperly disconnected during a well control situation. Given a fractional time of well control per well in the order of 10^{-2}, then a SIL 1- SIL2 level on the emergency disconnect and isolation would be reasonable to assume.

Conclusion:
Required SIL level for emergency disconnect for each specific well should be calculated and a tolerable risk level set as part of the application for consent process for exploration and development wells. The emergency disconnect for the marine drilling riser should have a minimum SIL level of SIL 2. This is based on historical information more than a detailed assessment of existing emergency disconnect systems. It is not known whether this can be documented for existing systems.

A.14.4.6 Lifting, rotation and pipe handling

The evaluation is related to lifting, rotation and pipe handling systems such as:

- Crane safety systems
- Brakes emergency stop
- Emergency stop devices
- Crown saver
- Floor saver
- Slack wire
- Anti-Collision
- Overload protection
- Prevention of unintentional opening of lifting/holding equipment
- Emergency lowering
- Emergency stop for rotation
- Iron roughneck emergency stop
- Heave compensator when locked to bottom

The heave compensator for normal operation is not included.

There are good standards and regulations for lifting equipment:

- "EU Machine Directive". Note that mobile installations are not required to follow the EU Machine Directive. Flag State and Classification Mobile installations also not required to implement IEC 61508.
- Norway – "Forskrift om Maskiner"
- Machine Directive is supported by EN standards e.g. "Offshore cranes"

Generally, it can be said that problems related to lifting and pipe handling can not be explained by inadequate standards, but rather by the fact that existing standards are not followed or implemented adequately.

There is a need for a holistic approach and adequate implementation of "Forskrift om Maskiner" and existing standards. A pure "electronic" approach (based on IEC 61508) to complex machinery do not seem to be the right approach in order to obtain an overall high safety level.

Conclusion:
It is not recommended to set a minimum SIL requirement for the lifting, rotation and pipe handling.

A.15 Manual initiators

Definition of functional boundaries
Following are some of the important manual initiators implemented on an offshore platform. Figure A.23 shows a typical connection of such devices to ESD / F&G nodes.

The manual initiator function starts when the buttons have been pushed and ends when the output signal(s) has been generated.

1. ESD manual push buttons located on matrix within CCR
2. ESD manual push buttons located in hazardous areas
3. Manual Electrical Isolation (MEI) push buttons
4. Deluge/inert gas/water mist release manual push buttons

Basic assumptions
Safe state for the installation will be to give a confirmed signal to the logic solver. The inputs are normally energised and will upon loss of power go to a safe state.

It should be noted that the pushbuttons in the CAP panel will initiate actions independent of the ESD system.

Quantification of safety function

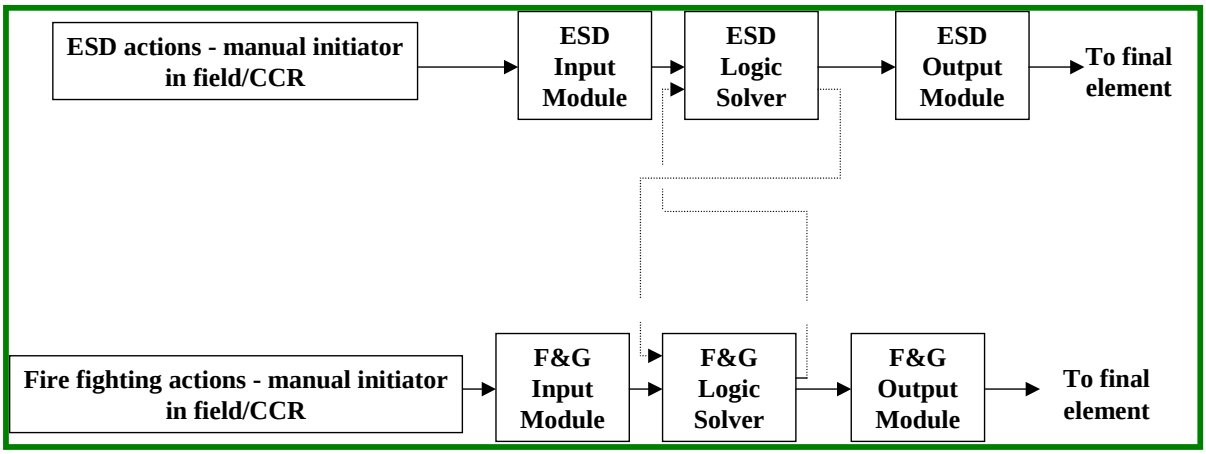

Figure A.23 Functional Block Diagram for ESD, F&G manual initiator

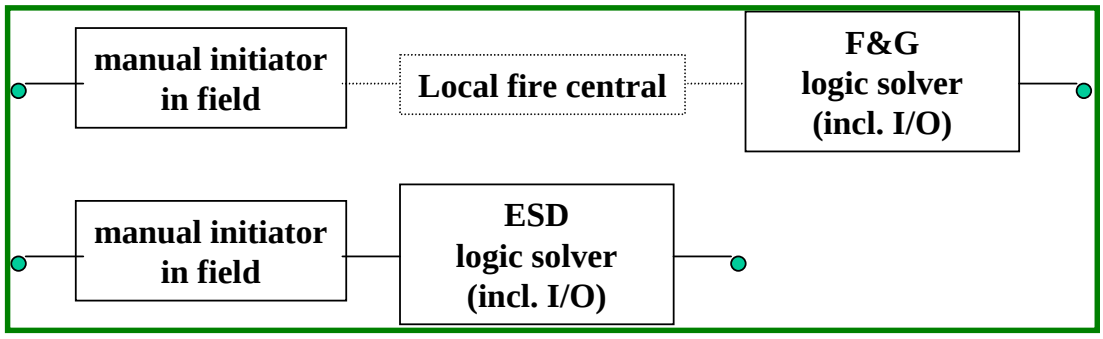

Figure A.24 RBD for ESD, F&G manual initiator

Table A.22 Estimated PFD for manual initiation of F&G function

Function	PFD for function	PSF for function
Manual initiation of ESD functions from field /CCR	0.005	$6 \cdot 10^{-5}$
Manual initiation of F&G functions from field / (CCR)	0.008 / (0.005)	

Based on this estimation a SIL 2 requirement can be claimed for manual initiation of F&G, ESD functions from the field and CCR.

A.16 References

/A.1/ Report from PDS-BIP activity 1 (in Norwegian). Also given in the PDS Data handbook, 2004.

APPENDIX B

EXAMPLES ON HOW TO DEFINE EUC

CONTENT

B.1 Introduction

IEC 61508 does not give any particular requirements as to how the EUC should be defined. Hence, it is up to those who wish to claim conformance to the standard to define the scope and boundary of the system to be considered. The important point will be that the EUC boundaries are clearly defined and in a manner such that all the relevant hazards to be considered in later lifecycle stages can be identified and described.

However, since definition of EUC is an important aspect of IEC 61508, section 7.3 of the guideline briefly discusses how EUC can be defined for local and global safety functions. In this appendix, an example of a possible EUC definition is given for each type of these safety functions.

B.2 Definition of EUC for local safety functions

HAZOP and SAT analyses are normally used to allocate local safety functions to identified hazards. Consequently, an appropriate EUC definition would be parallel to the definition of process components applied in ISO 10418 (i.e. API RP 14C), i.e. the definition should include the process unit and associated piping and valves.

Consider a process with a high-pressure separator for a two-phased separation of oil and gas. A simplified schematic of the separator is shown in figure B.1 together with an indication of possible EUC definition. Protection of the separator is designed according to ISO 10418, with a primary and secondary barrier against undesirable events. The local safety functions for the separator are implemented through the PSD system and the PSV.

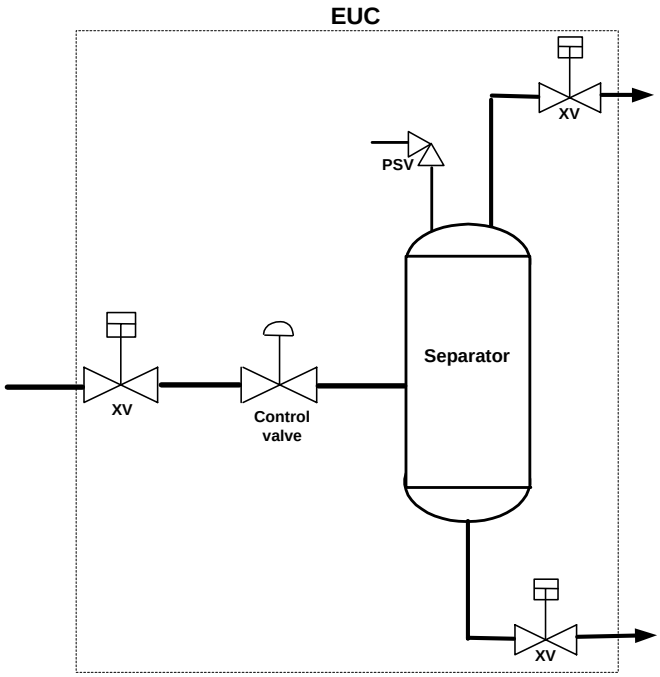

Figure B.1 Example of EUC definition for local safety functions

Hence, for this example the EUC boundaries are defined in terms of the PSD valves, which are used to isolate the separator during different PSD scenarios (ref. Appendix A.3).

B.3 Definition of EUC for global safety functions

Global safety functions on an offshore installation may include the following functions:

- Emergency shutdown function;
- Blowdown function;
- Electrical isolation function;
- Fire and Gas detection function; and
- Fire fighting function.

The purpose of these functions will be to prevent abnormal conditions, e.g. a hydrocarbon release, from developing into a major hazardous event, and further to control and mitigate the effects from such an event.

Typically, the installation will be divided into several fire areas. For process areas, emergency shutdown valves will usually be located within and at the boundaries of the fire area, e.g. next to a firewall, in order to prevent an escalation of the event from one area to another.

Hence, when considering fire and explosion events, a fire area seems an appropriate definition of the Equipment Under Control (EUC). This is illustrated in Figure B.2 below.

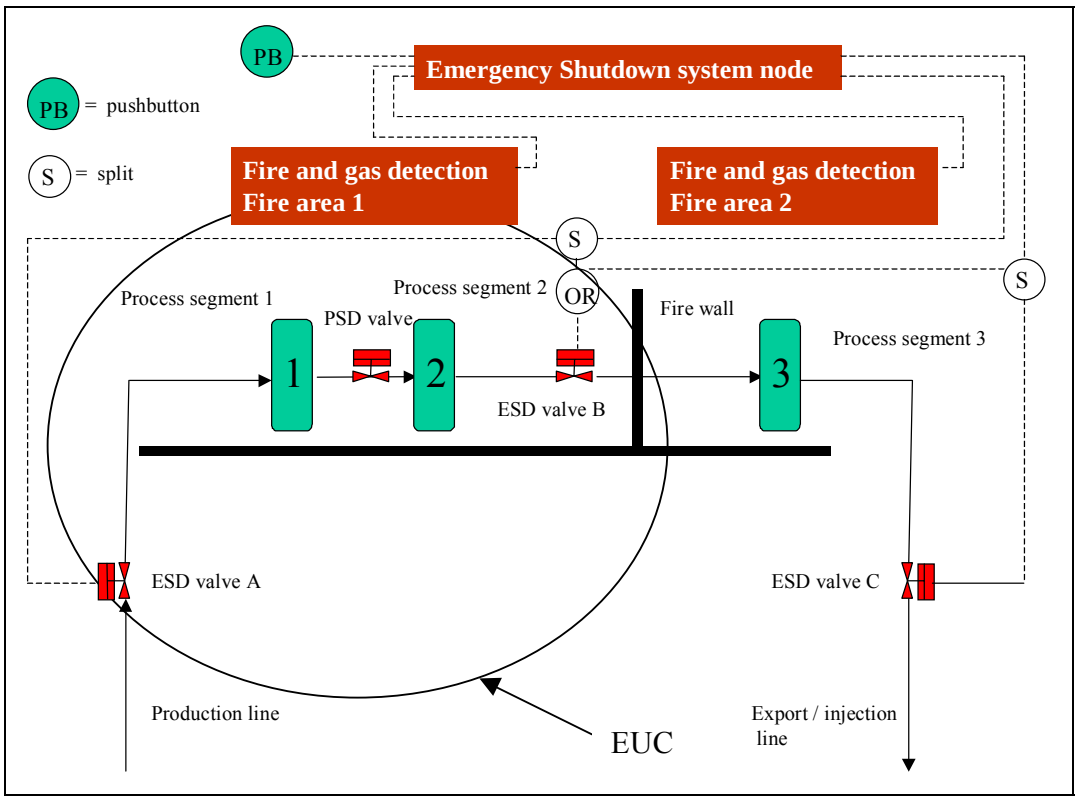

Figure B.2 Example of EUC definition for global safety functions

For this example, the EUC comprises process segments 1 and 2, whereas process segment 3 has been separated from segment 2 by a firewall and is therefore here considered as a separate EUC.

One important motivation for defining the EUC as a fire area will be the associated possibility of defining an acceptable EUC risk as required by IEC 61508/61511. With respect to acceptance criteria, the operators will have different types, which often will have the format of:

- an overall acceptance criteria for the installation (e.g. given in terms of an acceptable Fatal Accident Rate, FAR) and;
- different criteria related to the main safety functions, such as loss of escape routes, safe haven and evacuation means, as well as criteria related to loss of structural integrity and escalation of the event.

Whereas the overall FAR criterion will normally not be very suitable for defining acceptable EUC risk, the escalation criterion appears to be more applicable. This criterion would e.g. typically be defined in terms of the acceptable annual frequency for escalation of an event to another area. For the above example, the acceptable EUC risk could for example be defined as follows: *For a fire or explosion event originating in process segment 1 or 2, i.e. within the EUC, escalation to another area on the installation shall not occur with an accumulated frequency above* $1 \cdot 10^{-4}$ *per year.*

It should be noted that when using the minimum SIL table as given in section 7.6 of the guideline, EUC definition and the definition of an acceptable EUC risk will mainly apply to the handling of deviations.

When defining the EUC as indicated above, this may well include several process segments and several blowdown sections connected by process shutdown valves. Furthermore, with respect to electrical isolation, the extent of actual isolation will vary considerably depending on where gas is detected and will also interact closely between the different areas. For the above example (Figure B.2), gas detection in process segment 3 would e.g. typically initiate electrical isolation both in this area and in the EUC under consideration.

If found more appropriate it might be considered to define the EUC in terms of several fire areas. E.g. all the hazardous areas on the installation can be defined as one EUC, whereas the non-hazardous areas can be defined as another EUC. As indicated initially in this chapter, the important point will be to define EUC in a manner such that all relevant hazards can be identified.

APPENDIX C

HANDLING OF DEVIATIONS – USE OF QRA

CONTENT

C.1 Introduction

This appendix includes a brief description of a recommended methodology for handling of functional deviations from standard ISO 10418 (API RP 14C) designs. Example 1 includes a case where insufficient PSV capacity has been compensated by choosing a HIPPS solution. Example 2 includes a case with the use of subsea PSD and subsea HIPPS for protection of a flowline/riser not designed for full well shut-in pressure.

Further, the appendix includes a simplified example on how Quantitative Risk Analysis (QRA) can be applied in order to verify that the SIL requirement to "isolation of well" is sufficient to fulfil the stated acceptance criterion, ref. C.3.

Finally, the appendix discusses briefly the link between QRA and EUC risk, and presents a list of aspects which is not covered by an IEC 61508 analysis and therefore should be included in the QRA (ref. C.4).

C.2 Examples on handling of deviations (example 1 and 2)

C.2.1 Example 1 – SIL requirement to topside HIPPS function

Assume a separator as shown on figure C.1 below, without sufficient PSV capacity to protect against certain process situations. I.e. overpressure is here the defined hazard. Furthermore, a HIPPS solution is being considered in addition to the available PSD function.

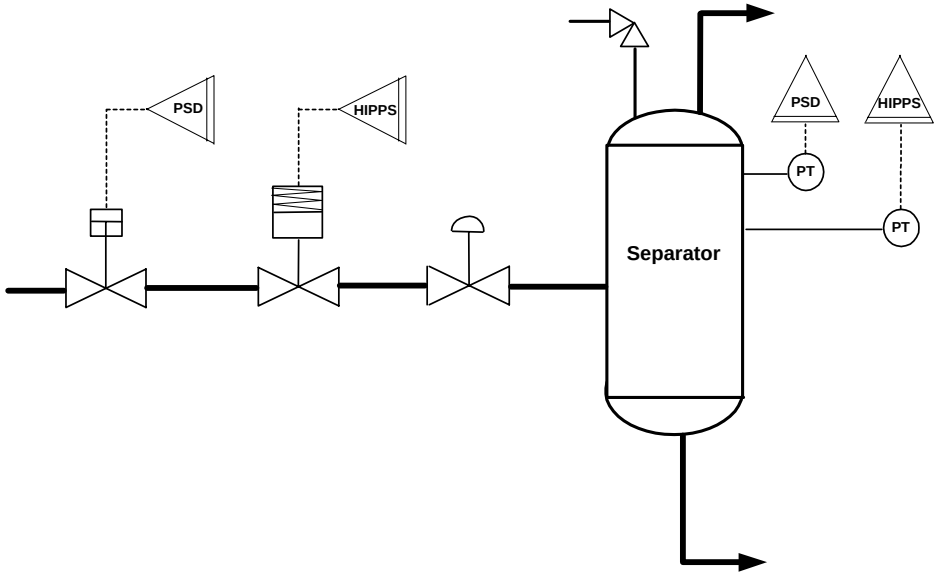

Figure C.1 Overpressure protection of separator

The following quantitative method could be applied for determining required SIL for this HIPPS function:

1. Define the EUC and its control system
2. Define exactly the overpressure scenario(s) to be considered and appropriate acceptance criteria. The latter might be expressed as an acceptable upper frequency for exceeding the test pressure of the separator, e.g. $1x10^{-5}$ per year
3. Consider which additional safety functions are available to protect the separator against the defined overpressure scenario(s). This could be the PSD function (if confirmed to be sufficiently quick), manually initiated ESD (depending on available operator response time), partial PSV (might provide some protection by reducing speed of pressure build-up), etc.
4. Estimate the frequency of events with a potential to cause a demand on the defined overpressure protection functions, including demands caused by failure of the control system. If the demand frequency is not affected by failures in the control system, the control system can be considered as a potential mean of reducing the demand rate.
5. Estimate the effect of the identified safety functions other than HIPPS, in terms of potential risk reduction

6. Estimate resulting (residual) requirement on HIPPS function in order to achieve stated acceptance criteria.

This method will in addition to providing SIL requirement on the HIPPS function also result in quantitative requirements for the other available safety functions.

C.2.2 Example 2 – SIL requirements to subsea PSD and HIPPS functions

In this example, a case with a flowline / riser *not designed for full well shut-in conditions* is described. In order to protect the flowline and riser against overpressure, subsea PSD and HIPPS are implemented.

Installations designed for shut-in conditions up to the riser ESV will normally not require subsea PSD and/or subsea HIPPS.

Overall system description

A subsea production system with HIPPS is described below (ref. Figure C.2 below).

The allocation of SIL for the subsea protection functions is based upon the following assumptions/criteria:

1) Frequency of exceeding process test condition in flowline shall not exceed 10^{-5} per year
2) Frequency of exceeding process design condition in flowline shall not exceed 10^{-3} per year

Performance requirements (closing time, etc.) must be established based upon risk analyses, process simulations, etc. for each case.

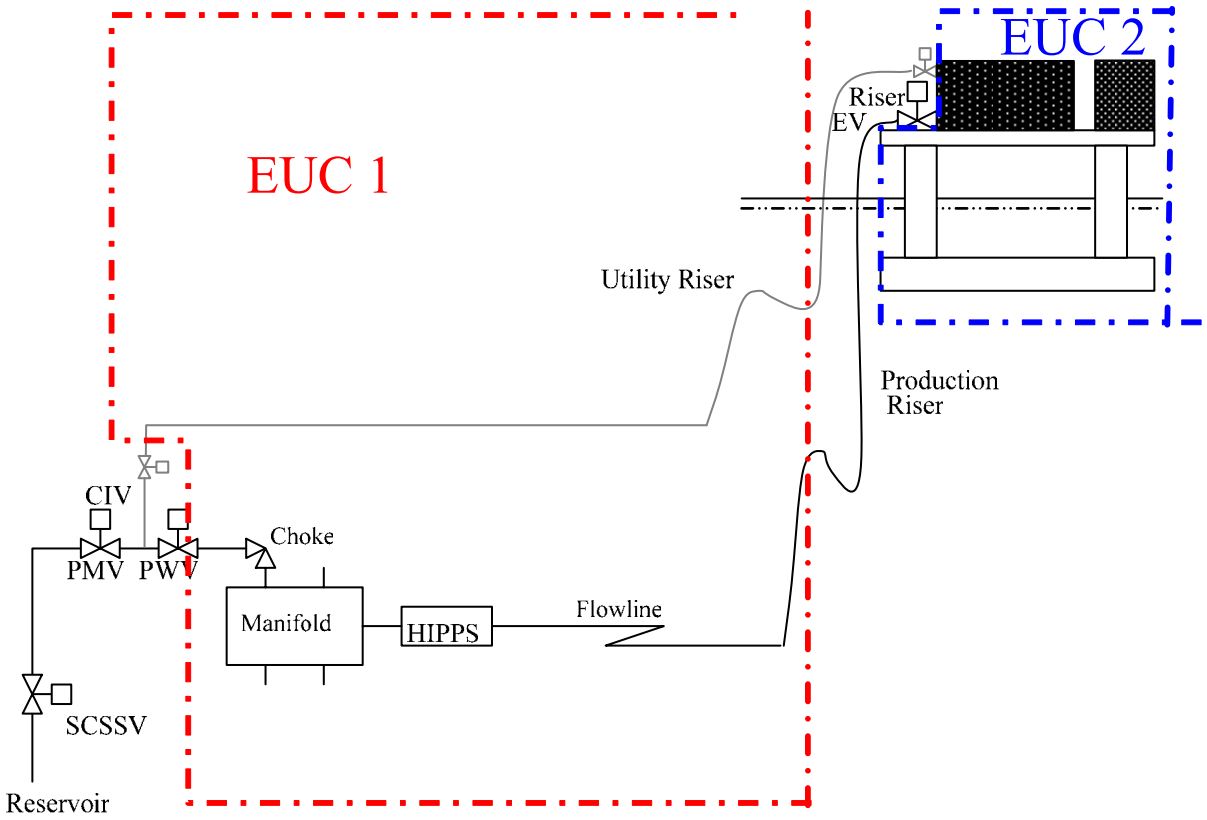

Figure C.2 Subsea production system with HIPPS

Subsea Process Protection - Definition of functional boundaries
The following Final Elements (FE) subsea may be available to complete the function:

PMV	-	Production Master Valve
PWV	-	Production Wing Valve
HIPPS	-	High Integrity Pressure Protection System
CIV	-	Chemical Injection Valve

The overall safety function to be fulfilled is defined as "Isolate subsea well from flowline by closing PMV or (PWV and CIV) or HIPPS". The objective of the safety function will be to protect the flowline and/or the riser from pressures in excess of the design parameters.

The function concerns process protection only, through PSD and/or HIPPS. The subsea equipment under control (EUC 1) is the flowline and the riser, the topside equipment under control (EUC 2) is not part of the function.

Figure C.5 and C.6 shows a (simplified) example of the PSD and HIPPS function respectively.

Quantification of safety function - PSD isolation of subsea well
The subsea PSD protection function can be represented by a Reliability Block Diagram as shown in Figure C.3 below. Note that the PSD node includes the topside modems and all the PSD logic. For assumed configuration of the PSD please refer to Figure C.5.

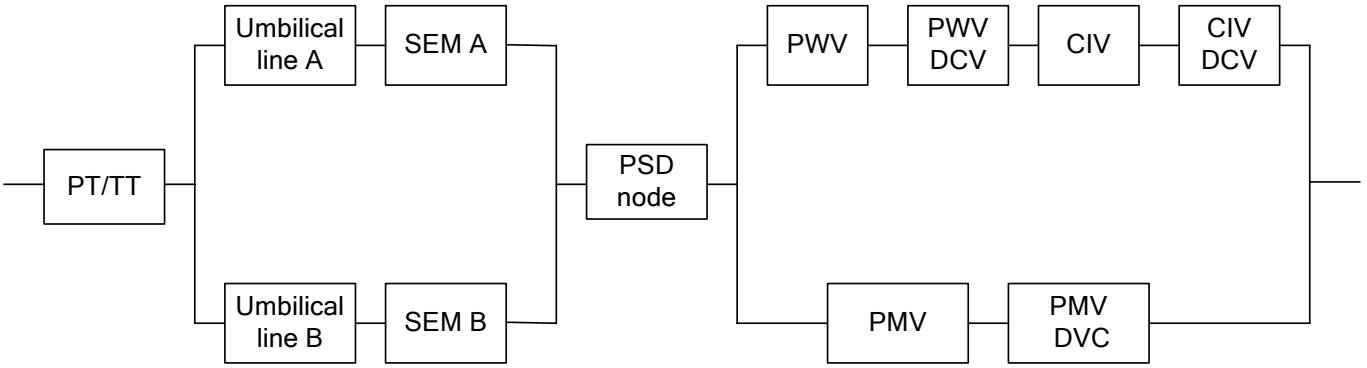

Figure C.3 RBD for PSD isolation of one subsea well

The assumed analysis input is given in Table C.1 below (based on Appendix A, Table A.3).

Table C.1 Analysis input for safety function "PSD isolation of one subsea well"

Component	PFD (single comp.)	PFD (duplicated comp.)	PSF (single comp.)	PSF (duplicated comp.)
PSD logic [1)]	$8.76 \cdot 10^{-3}$	-	$5 \cdot 10^{-5}$	$2.5 \cdot 10^{-5}$
DCV	$2.2 \cdot 10^{-4}$	$2.2 \cdot 10^{-5}$	-	-
PMV/PWV	$2.2 \cdot 10^{-4}$	$2.2 \cdot 10^{-5}$	$1 \cdot 10^{-5}$	$1 \cdot 10^{-6}$
CIV	$8.8 \cdot 10^{-4}$	$8.8 \cdot 10^{-5}$	$1 \cdot 10^{-5}$	$1 \cdot 10^{-6}$
SEM	$4.16 \cdot 10^{-3}$	$2.1 \cdot 10^{-4}$	$5 \cdot 10^{-5}$	$2.5 \cdot 10^{-5}$
Umbilical Signal Lines	$5.3 \cdot 10^{-4}$	$5.3 \cdot 10^{-5}$	-	-
PT	$8.8 \cdot 10^{-4}$	-	$5 \cdot 10^{-4}$	$5 \cdot 10^{-5}$

[1)] For the purpose of this example a failure rate λ_{DU} of $2 \cdot 10^{-6}$ per hour has been used for the single PSD node in order to reflect that this includes both the topside modems and the PSD logic

For all components a β-factor of 10% has been used, except for PSD and SEM logic, where a β-factor of 5% has been used. A β-factor of 10% has also been applied to the PSF, except for the PSD and SEM logic where a β-factor of

50% has been applied for systematic failures in duplicated logic. The following common mode failures are included in the analysis model:

- failures affecting both umbilical signal lines
- failures affecting both SEM's
- failures affecting all DCVs in Subsea Control Module (SCM)
- failures affecting both the PMV and the PWV

For all components a test interval of 4380 hours has been assumed, except for the PSD logic, where a test interval of 8760 hours has been used. The PSD-node has further been assumed to be single.

Based on the above assumptions, the PFD figure has been calculated for the safety function. It should be noted that the applied PSF values (and to some degree the β-factors) apply for topside equipment and therefore need to be further considered in an actual subsea application.

Table C.2 Estimated PFD for "PSD isolation of one subsea well"

Function	PFD	SIL
PSD isolation of well	$1.0 \cdot 10^{-2}$	1

As seen from the above table, the subsea PSD function, with the given assumptions, only fulfils a quantitative SIL 1 requirement. With other test intervals (and other/better reliability data), a quantitative SIL 2 requirement seems achievable. It should however be noted that architectural constraints (ref. table 8.3) and software in SEM may impose restrictions on the obtainable SIL.

Quantification of safety function – subsea HIPPS isolation

The subsea HIPPS protection function can be represented by a Reliability Block Diagram as shown in Figure C.4 below (simplified). For assumed configuration of the HIPPS please refer to Figure C.6.

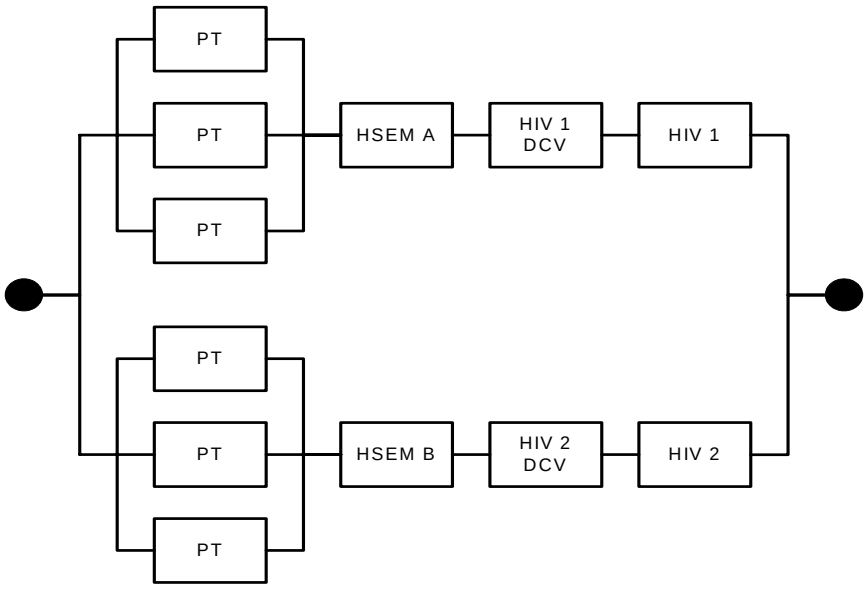

Figure C.4 RBD for subsea HIPPS isolation

The assumed analysis input is given in Table C.3 below.

Table C.3 Analysis input for safety function "HIPPS isolation"

Component	PFD (single comp.)	PFD (duplicated comp.)	PSF (single comp.)	PSF (duplicated comp.)
DCV	**$2.2 \cdot 10^{-4}$**	**$2.2 \cdot 10^{-5}$**	**-**	**-**
HIV (HIPPS Isolation Valve) [1)]	**$2.2 \cdot 10^{-4}$**	**$2.2 \cdot 10^{-5}$**	**$1 \cdot 10^{-5}$**	**$1 \cdot 10^{-6}$**
HSEM (HIPPS Subsea Electronic Module) [2)]	**$4.16 \cdot 10^{-3}$**	**$2.1 \cdot 10^{-4}$**	**$5 \cdot 10^{-5}$**	**$2.5 \cdot 10^{-5}$**
PT	**$8.8 \cdot 10^{-4}$**	**$8.8 \cdot 10^{-5}$**	**$5 \cdot 10^{-4}$**	**$5 \cdot 10^{-5}$**

[1)] PFD value for HIV is set to be equal to a X-mas tree valves (PMV / PWV) due to lack of documented field data.
[2)] PFD value for HSEM is set to be equal to SEM due to lack of documented field data. PFD for certified HIPPS logic will have significantly lower PFD (but may be a single system).

For all components a β-factor of 10% has been used, except for the HSEM logic, where a β-factor of 5% has been used. A β-factor of 10% has also been applied to the PSF, except for the HSEM logic where a β-factor of 50% has been applied for systematic failures in duplicated logic. The following common mode failures are included in the analysis model:

- failures affecting all PT transmitters
- failures affecting both HIV DCVs
- failures affecting both HSEMs
- failures affecting both HIVs

For all components, a test interval of 4380 hours has been assumed.

Based on these assumptions, the PFD figure has been calculated for the HIPPS safety function.

Table C.4 Estimated PFD for "HIPPS isolation"

Function	PFD	SIL
HIPPS isolation of well	**$4 \cdot 10^{-4}$**	**3**

As seen from the above, the HIPPS function fulfils a quantitative SIL 3 requirement.

It should be noted that the above quantification is only an example. Both the HIPPS configurations as well as the applied reliability data are likely to differ from the above. E.g. another possible configuration will be to install a single HIPPS logic (certified for SIL 3 application), redundant HIPPS valves and 2 x 1oo2 pressure transmitters.

Possible link towards overall acceptance criteria

As stated initially in this example, the annual frequency of exceeding process test condition in the flowline shall not exceed 10^{-5}. It is therefore interesting to find out how much risk reduction is obtained from the combined PSD and HIPPS function.

Furthermore, assume that the demand rate on the overpressure protection function is 15 per year. I.e. there will be 15 topside shutdowns per year requiring the subsea protection function to be activated.

For the purpose of this simplified example, it is assumed that the common cause failure (CCF) rate between the HIPPS and the PSD system is 1%, and a geometric mean (ref. appendix D.9) of the PFD values for the two functions have here been used (in a real calculation a more detailed consideration of the CCF failure rate must be done considering each component separately).

Based on these assumptions the annual frequency of overpressure, based on a case with only one well, can then be estimated by:

$$F_{overpressure} = 15 \cdot (P_{HIPPS\ failure} \times P_{PSD\ failure} + CCF_{HIPPS\&PSD}) = 15\ (1.0 \cdot 10^{-2} \cdot 4 \cdot 10^{-4} + 0.01 \cdot (1.0 \cdot 10^{-2} \cdot 4 \cdot 10^{-4})^{1/2})$$

$$= 3.6 \cdot 10^{-4} \text{ per year.}$$

As seen from the above calculation, the acceptance criterion of 10-5 per year is exceeded, and some additional measures must therefore be implemented in order to meet the criteria, e.g.

- installation of a PSV function on the flowline / riser;
- If a topside PSD (which is the most likely “blocked outlet” source) automatically initiates a subsea PSD, then the PSD function will not depend on the pressure transmitter for most of the demands and the overall failure probability will therefore decrease:
- If the operator reveals that the subsea pressure is increasing beyond the HIPPS set point he is likely to initiate a manual ESD;
- If communication with HSEMs is lost, manual shutdown is initiated using either electric or hydraulic fail safe properties.

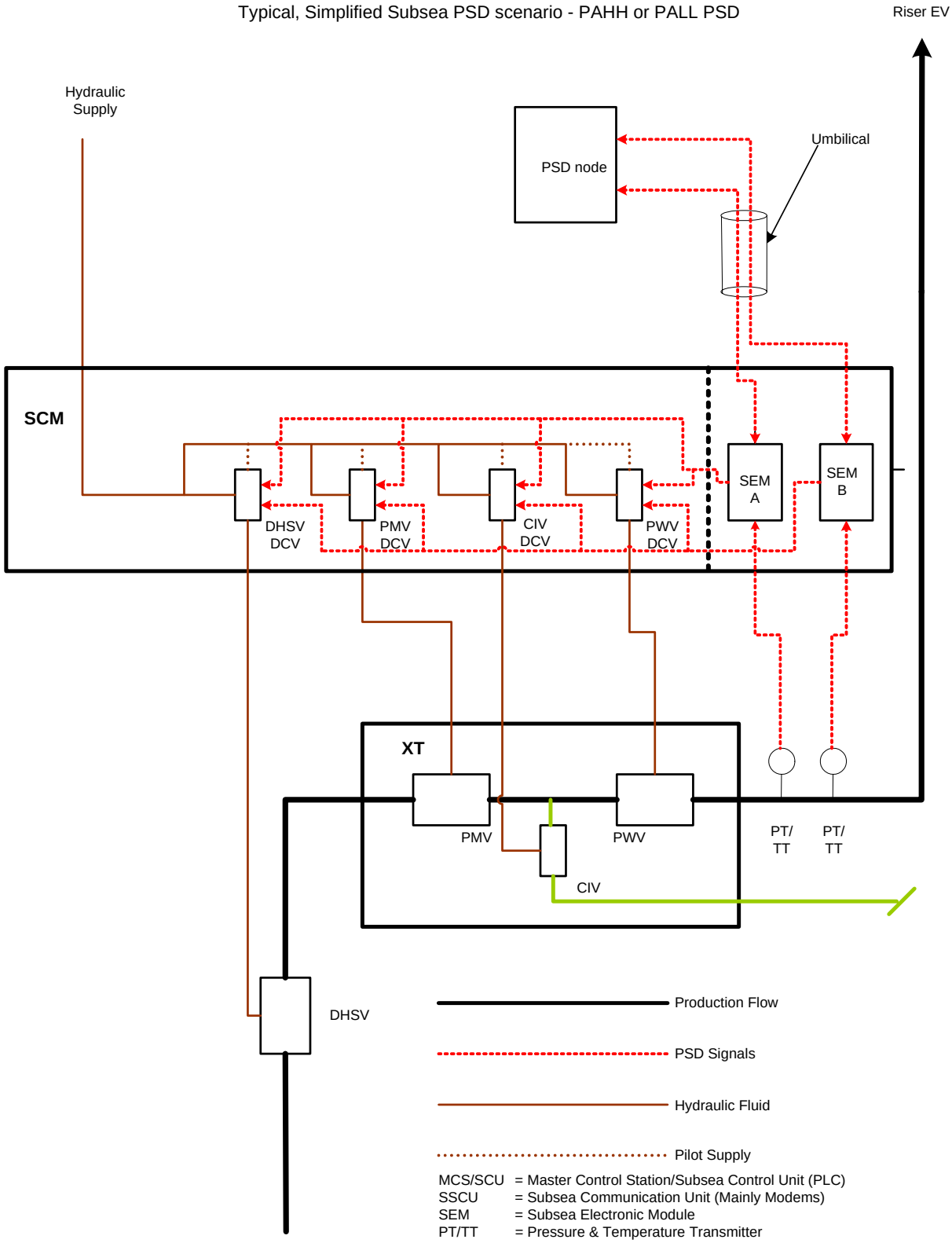

Figure C.5 Simplified subsea PSD schematic

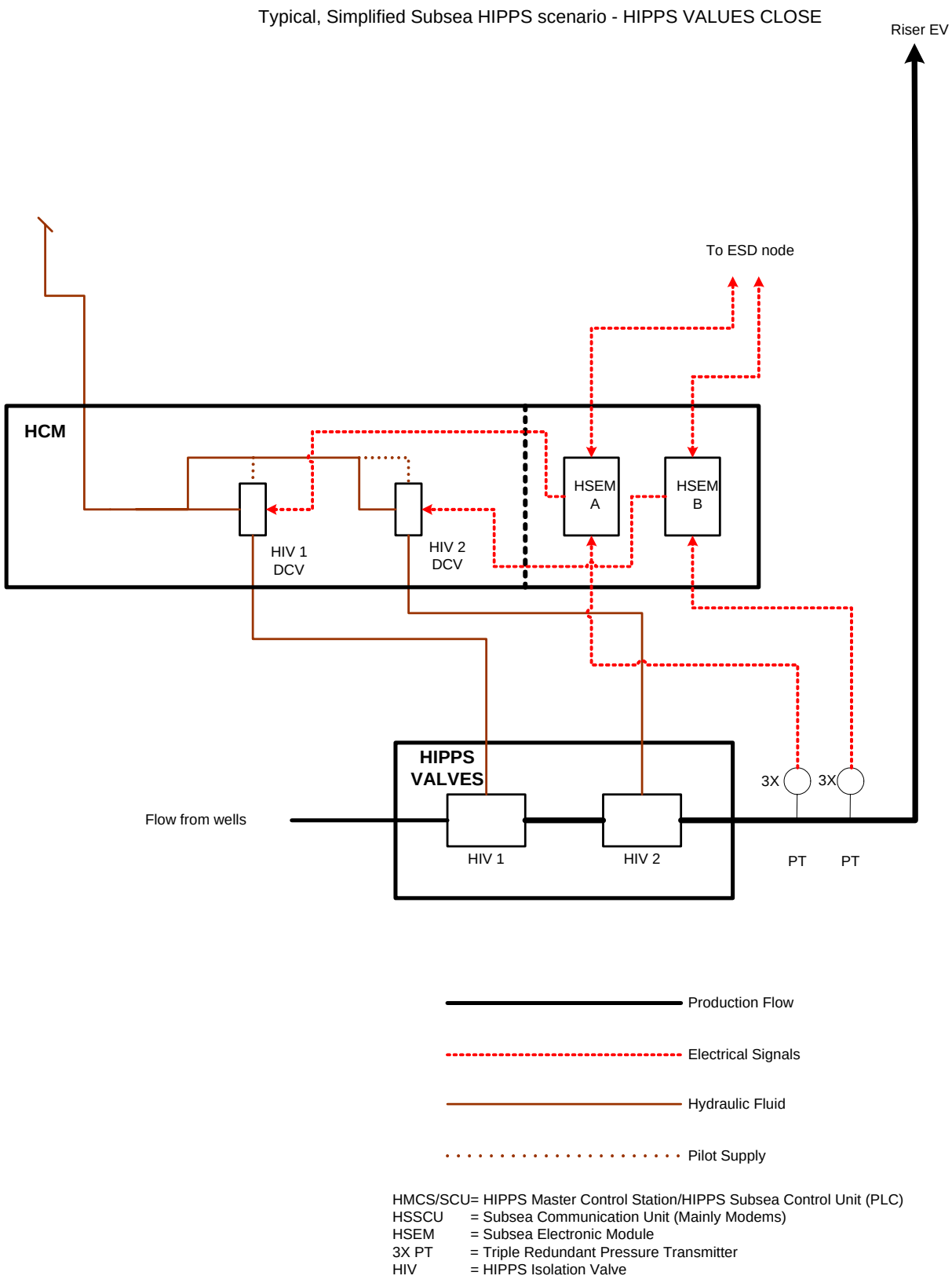

Figure C.6 Simplified subsea HIPPS schematic

C.3 Verification by QRA of a stated Safety Integrity Level (Example 3)

This section gives a (simplified) example on how QRA (Quantitative Risk Analysis) can be used to verify that a standard SIL requirement is acceptable with respect to the overall risk on an installation.

C.3.1 Risk acceptance criteria

Regulatory requirements
Paragraph 6 of the PSA "management regulations" stipulates that operators (or parties responsible for operation of an installation) in the petroleum industries shall define acceptance criteria for risk in the petroleum activities. In addition, paragraph 10 in "the facility regulations" stipulates that accidental (or environmental) loads should not cause impairment of a main safety function with a frequency exceeding $1 \cdot 10^{-4}$ per year. Main safety functions are defined in paragraph 6 of the same regulation to be;

- prevention of escalation of accidental events in order to prevent personnel outside the immediate vicinity of the area affected by the accident from being injured;
- maintaining the structural integrity of load bearing construction for the time required to evacuate the installation;
- protect rooms of importance for mitigating the accidental events for the time required to evacuate the installation;
- keep at least one escape route open from each area in which personnel can be located until evacuation to a safe haven and rescue of personnel have been carried out.

Personnel risk
Generally, risk acceptance criteria used by operators on the Norwegian continental shelf define an upper limit on the acceptable risk, using varying measures for risk to personnel, environment and assets. The overall risk acceptance criteria are normally not split pr. accidental event. This allows for some degree of flexibility, i.e. it is possible to tolerate a higher risk from process accidents, as long as this is compensated by reduction in the risk from other accident categories in order to ensure that the total risk level is acceptable. The ALARP principle is often used, implying that the risk should be reduced to a level "as low as reasonably practicable". ALARP is normally demonstrated using cost/benefit evaluations with risk reducing measures being implemented when e.g. the cost of averting a fatality are not prohibitively high.

Material damage risk / safety functions
The NORSOK standard Z-013 specifies that "*a frequency 1 x 10^{-4} per year for each type of accidental load has been used frequently as the limit of acceptability for the impairment of each main safety function. Sometimes one prefers an overall frequency summing up all accidental load types. For these purposes an overall frequency of 5 x 10-4 per year has been used as the impairment frequency limit*".

The 1 x 10^{-4} criteria may be derived from "the facility regulations", and can be used as a basis for SIL determination. It should be noted that several operators on the Norwegian continental shelf have chosen to use an overall 5 x 10^{-4} criteria, not setting a level for the maximum risk contribution from each accidental event. It should also be noted that the interpretation of how the risk acceptance criteria are to be applied may vary between the different operators.

Risk acceptance vs. SIL requirements
The SIL requirements given in this document may influence both the likelihood of an event (e.g. SIL requirements to PSD functions) and the consequence of an accidental event (e.g. SIL requirements to ESD and F&G functions). It therefore seems reasonable to expect a certain consistency between the SIL requirements and the overall risk acceptance criteria. Where this guideline specifies SIL requirements for sub functions, quantitative risk analyses should be applied to ensure that the overall risk is acceptable when compared to the established acceptance criteria. In general, setting "standard" safety integrity levels may be compared to setting a "standard" level of risk acceptance. Such "standard" criteria will not take into consideration installation specific elements, ref. discussion in section C.4.

In order to verify whether or not the standard Safety Integrity Levels will result in an acceptable overall risk level, a more detailed analysis is required. Example calculations are given below.

C.3.2 Isolation of topside production wells

General – application of acceptance criteria

The guideline specifies that the subsystem "isolation of one well" should meet a minimum safety integrity level of SIL 3. The following high-level example is intended to demonstrate whether or not this is adequate in order to meet an overall risk acceptance criterion. Reference is also made to Annex C of IEC 61511-3 for additional examples.

The acceptance criterion to be applied in the following example is that *any single accidental event should not contribute to the frequency of escalation (i.e. loss of fire area integrity) with a frequency exceeding 1 x 10^{-4} per year*.

Assumptions

The installation considered has a process layout as indicated in Figure C.7 below. This includes;

- five production wells with "standard" wellhead configuration;
- a wellhead area segregated from other areas with an H-120 firewall;
- a production manifold located in the wellhead area, separated from the oil and gas separation process by an ESD valve.

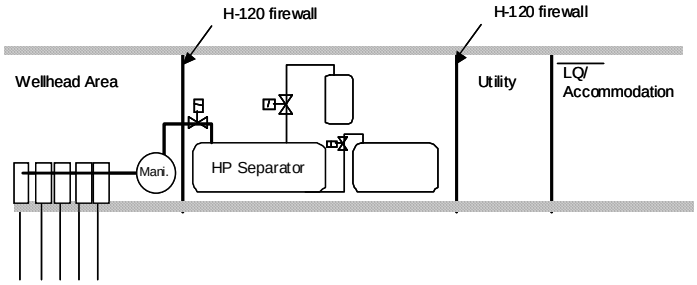

Figure C.7 Example Wellhead / Process layout

For the purpose of this example it is assumed that any fire originating in the production manifold will have duration of less than 120 minutes if isolation is successful. The fire will then not threaten the firewall separating the process and wellhead areas. However, failure to isolate the segment (failure to shut in wells) will result in the fire duration exceeding 120 minutes, with a high likelihood of failure of the firewall.

General

To limit inventory available to feed any leak, all wells must be shut in, and the ESD valve downstream the production manifold must close. Closing in wells can typically be achieved by closing at least one of the following valves;

- DHSV
- Upper master valve
- Production wing valve

Note that the DHSV is the only valve that can prevent flow to surface in the event of damage to the wellheads. A minimum SIL of 3 has been set for isolation of each well, in accordance with specifications given in this guideline. Section A.6 indicates that this is achievable with current technology. This SIL requirement is used to establish a probability of isolation failure for further use in the risk model.

Simplified event tree analysis

In order to evaluate the annual frequency of failure of the firewall due to fires from the production manifold, an event tree approach is used. For the purpose of this simplified example, it is assumed that depressurisation of the HP separator segment is successful. It can then be assumed that a failure to close the ESD valve upstream of the HP separator is not critical with respect to the firewall integrity (such a failure will result in an increased fire duration but not exceeding 120 minutes). The critical aspect will then be whether or not it is possible to shut in the wells.

An example event tree is given in Figure C.8.

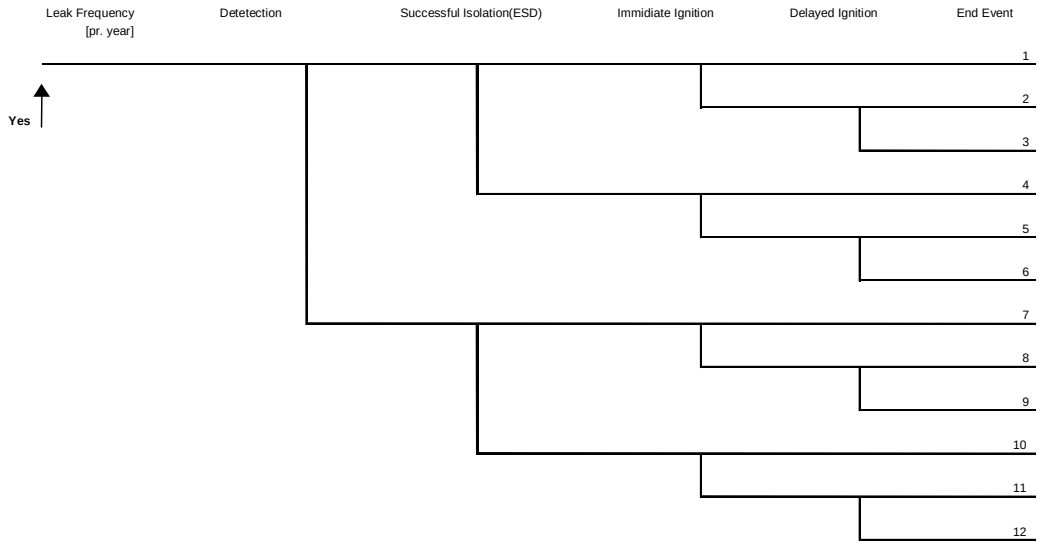

Figure C.8 Example event tree

The above event tree takes into account the following branch probabilities;

- Detection: Likelihood of successful gas detection
- Successful Isolation (ESD): Likelihood of successful isolation of the fire cell
- Likelihood of ignition: Likelihood of immediate or delayed ignition of the released hydrocarbon inventory

The above event tree is simplified, i.e. it does not take into account all factors normally considered in a full QRA event tree. As an example, the NORSOK Z-013 standard requires event tree analyses to take into account;

- leak cause, source and location
- leak rate, volume and duration
- leak medium (e.g. gas/oil)
- effectiveness of shutdown system on leak volume
- gas spreading/dispersion
- probability of ignition, time of ignition
- probability of explosion in the event of ignition, effect of explosion
- effectiveness of fire-fighting system
- effectiveness of blowdown system
- accident escalation
- escape possibilities and evacuation system
- distribution of personnel

In order to produce a quantitative example using the above event tree, the following input is used:

- A leak in the production manifold (or associated piping) is assumed to occur with a frequency of, say, $5 \cdot 10^{-3}$ pr. year[3].

- The likelihood of immediate ignition of the leak is assumed to be in the order of 10%, with a 2.5% and 5% likelihood of delayed ignition for scenarios with successful and unsuccessful ESD, respectively[4].

- The manifold area is assumed covered by a sufficient amount of gas detectors

- With “isolation of well” being a SIL 3 function, the probability of failure to isolate one or more well in a wellhead area with five producing wells can be approximated by (1-0.999) x 5 = 0.005.

[3] This example considers one release scenario only. It should be noted that available data indicate that the majority of leaks will be of a very limited size and can be considered not to have a significant escalation potential (naturally, this will depend on the layout of the installation).

[4] Here, a detailed QRA would take into account ignition sources in the wellhead area and possibly use a time-dependent ignition model to determine installation-specific ignition probabilities.

Using the above data and assumptions in the example event tree, the quantitative example will be as indicated in C.9 below.

Leak Frequency [pr. year]	Detection	Successful Isolation (ESD)	Immediate Ignition	Delayed Ignition	End Event	Frequency [pr. year]	P(Escalation)	F(Escalation) [pr. year]
5.00E-03	0.9	0.995	0.1		1	4.48E-04	0.00	0.00E+00
	4.50E-03	*4.48E-03*	*4.48E-04*					
			0.9	0.025	2	1.01E-04	0.25	2.52E-05
			4.03E-03	*1.01E-04*				
				0.975	3	3.93E-03	0.00	0.00E+00
				3.93E-03				
		0.005	0.1		4	2.25E-06	0.95	2.14E-06
		2.25E-05	*2.25E-06*					
			0.9	0.06	5	1.22E-06	0.95	1.15E-06
			2.03E-05	*1.22E-06*				
				0.94	6	1.90E-05	0.00	0.00E+00
				1.90E-05				
	0.1	0	0.1		7	0.00E+00	0.00	0.00E+00
	5.00E-04	*0.00E+00*	*0.00E+00*					
			0.9	0.05	8	0.00E+00	0.25	0.00E+00
			0.00E+00	*0.00E+00*				
				0.95	9	0.00E+00	0.00	0.00E+00
				0.00E+00				
		1	0.1		10	5.00E-05	0.95	4.75E-05
		5.00E-04	*5.00E-05*					
			0.9	0.05	11	2.25E-05	0.95	2.14E-05
			4.50E-04	*2.25E-05*				
				0.95	12	4.28E-04	0.00	0.00E+00
				4.28E-04				
						5.00E-03		9.74E-05

Figure C.9 Example event tree with assumed figures included[5]

The above example indicates that the acceptance criterion of $1 \cdot 10^{-4}$ per year with respect to escalation can be met, but with small margins, using a SIL 3 requirement for isolation of well. It should be noted that several other options for risk reduction exist, that could be considered had the above approach indicated that the risk was unacceptable, or if the margin to the acceptance criterion is considered too small, e.g.

- Reduction of number of leak sources in the manifold system (lower leak frequency);
- Reduction or improved maintenance of potential ignition sources (lower ignition probability);
- Improved gas detection;
- Improved fire protection on firewall (lower probability of escalation);
- Change of layout in wellhead area to reduce explosion overpressure (lower probability of escalation).

[5] I should be stressed that all numbers in the event tree (leak frequency and branch probabilities) are *installation specific*, and that the above numbers are to be considered examples only.

C.4 QRA and IEC 61508

The overall safety for the EUC and the overall facility shall be handled by means of a Health, Safety and Environment (HSE) plan. As a part of this, an overall QRA covering all risks for the facility should be developed and maintained throughout the life cycle of the facility.

The QRA shall account for the total risk at a given facility. The overall risk originates from all types of risks ranging from structural collapse to minor personnel injuries.

When stating SIL requirements as given in Table 7.1 in this document, and when performing verifications of these requirements according to IEC 61508, there will be a number of "risk elements" that may not be explicitly addressed. These elements therefore need to be addressed in other analyses such as the overall QRA, and some examples may include:

- The gas detectors are not exposed as assumed and the safety function is therefore not activated (wind direction, detector layout, size of release, etc.):
- The activation of the safety function is correct, but the safety function does not work as intended due to factors not explicitly covered in the IEC 61508 analysis (e.g. firewater does not hit/extinguish the fire);
- Additional risks originating from spurious activation (trip) of safety function are introduced (e.g. blowdown, etc.);
- Unintended side effects of the safety function add new hazards (shut-down in one system trips another critical continuous system e.g. crane operation and detected gas in area, equipment protection stops propulsion system, etc.);
- The combined effects of connected systems or installations outside the EUC and the EUC control system (e.g. diesel oil leak from one fire pump to another hot surface system)
- Risk effects from application of common equipment items (safety node) for several functions/loops. If a common safety node fails, several safety functions/loops may be simultaneously disabled (e.g. the ESD system initiates several safety function in different systems such as segmentation of process, blowdown, starting of firewater pumps, isolation of ignition sources, etc.);
- Influence on risk from operator intervention which may result in both an increase or a decrease of the risk (e.g. the operator fails to activate a manual ESD (increased risk) or an operator manually activates an automatic PSD action which has failed (decreased risk));
- Several of the safety functions described in Table 7.1 and in Appendix A are incomplete, i.e. in order to provide input to the QRA, some additional (installation specific) considerations need to be done. E.g. for the gas detection function (ref. section A.9) the actual detector voting and the likelihood of exposing the detectors need to be reflected, whereas for the "LAHH in flare knock out drum" function (ref. section A.3.3) the relevant final elements need to be specified.

It should be noted that some of the "additional risk elements" listed above will typically fall into the category of systematic failures. This underlines an important point; when performing calculations according to IEC 61508, the standard explicitly states that systematic failures shall not be quantified but shall be controlled and reduced by the use of qualitative checklists. However, when performing QRA, the goal should be to obtain a "correct" estimate of the risk, and in this respect it will be important to also include the PSF (Probability of Systematic Failure) contributions towards failure of the considered safety functions.

APPENDIX D

QUANTIFICATION OF PROBABILITY OF FAILURE ON DEMAND (PFD)

CONTENT

D.1 Relation between PFD and other measures for loss of safety

First, some definitions related to loss of safety, i.e. *safety unavailability,* as defined in the PDS method (cf. ref. /D.1/) are given. Both in IEC 61508 (ref. part 6, Annex B) and PDS, the main measure for loss of safety is denoted:

PFD = *Probability of Failure on Demand*.

This is used to quantify loss of safety due to random hardware failures. In PDS this measure is split into the following two contributions:

- PFD_{UK} represents the *unknown* (UK) part of the safety unavailability. It quantifies the loss of safety due to dangerous undetected failures, during the period when it is not known that the function is unavailable. The average duration of this period is $\tau/2$, where τ = test period.

- PFD_K represents the *known* (K) part of the safety unavailability. It quantifies the loss of safety due to dangerous failures, during the period when it is known that the function is unavailable. The average duration of this period is the mean repair time, MTTR i.e. time from failure is detected until safety function is restored or time until compensating measures are effectuated.

Thus, $PFD = PFD_{UK} + PFD_K$. The PDS method also introduces:

PSF = *Probability of Systematic Failure, (i.e. a non-physical, dangerous failure, cf IEC 61508).* This is the probability that the module/system will fail to carry out its intended function due to a systematic failure. Essentially, this is the probability that a component that has just been functionally tested will fail on demand. (Previously this was in PDS denoted the probability of test-independent-failures, TIF).

CSU = *Critical Safety Unavailability*. The probability that the module/safety system due to a *non-revealed* fault will fail to automatically carry out a successful safety action on the occurrence of a hazardous/accidental event. The CSU includes contributions both from *random hardware failures* and *systematic failures*, and so CSU = PFD + PSF[6].

NSU = *Non-critical safety unavailability*. This is the unavailability caused by functional tests, and equals the probability that it is known (actually planned) that the safety system is unavailable due to functional testing.

Observe that CSU = PFD + PSF, see Fig. D.1

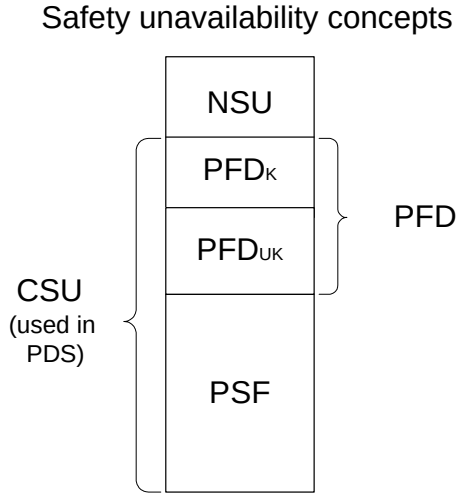

Figure D.1 Relation between loss of safety concepts

[6] The more correct formula is CSU = 1 – (1-PFD) · (1- PSF). However, as in other parts of the report, we assume that the probabilities are sufficiently small to let CSU=PFD+PSF, (that is, the product term PFD·PSF is negligible). The same approximation is used where PFD for different parts of e.g. a function is added. Normally this is a conservative approximation.

Now, the following topics should be investigated:

1. How are failures classified in IEC and PDS? What is the difference?
2. How is PFD = PFD_{UK} + PFD_K quantified in PDS and IEC, respectively?
3. How should NSU be quantified?
4. What are the arguments for quantifying the PSF also when IEC 61508 is applied?
5. In conclusion, what is the recommended approach for loss of safety quantification when adhering to IEC, but at the same time not losing the aspects of the PDS method which are important for a realistic evaluation of safety systems?

These topics are treated below. The PDS method and notation is followed, which is now compatible with the IEC 61508 notation. The following notation applies:

MTTR: Mean Time to Repair for a component
τ : Time interval between proof tests (denoted T_1 in IEC 61508)
λ : Component failure rate
β : Beta-factor for common cause failures

The rate of random hardware failures is in IEC and PDS split as follows:

Table D.1 IEC vs. PDS notation – random hardware failures

IEC notation	PDS notation	Description (rates of random hardware failures)
$\lambda_D = \lambda_{DU} + \lambda_{DD}$		Rate of dangerous (D) failures
λ_{DU}		Rate of dangerous undetected (DU) failures; i.e. rate of dangerous failures which lie outside the coverage of the diagnostic tests
λ_{DD}		Rate of dangerous detected (DD) failures; i.e. rate of dangerous failures which are detected by the diagnostic tests
$\lambda_S = \lambda_{SU} + \lambda_{SD}$		Rate of safe (S) failures (i.e. spurious trip or non-critical failures)
λ_{SU}	$\lambda_{STU} + \lambda_{NONC}$	Rate of safe undetected (SU) failures. In PDS this is interpreted as the sum of the rates of undetected spurious trip and non-critical failures.
λ_{SD}	λ_{STD}	Rate of safe detected (SD) failures. In PDS this is interpreted to be the same as the rate of detected spurious trip failures.
	λ_{STU}	Rate of undetected spurious trip failures
	$\lambda_{ST} = \lambda_{STU} + \lambda_{STD}$	Rate of failures due to spurious trip, (i.e. operation without demand)
	λ_{NONC}	Rate of non-critical failures, (neither dangerous nor spurious trip), i.e. safety function not directly affected

For dangerous (D) failures the definitions in PDS and IEC are identical. For safe (S) failures there is however an apparent difference; The IEC standard does not discuss critical versus non-critical failures. Hence, safe (S) failure as defined in IEC can be interpreted as including both spurious trip (ST) failures and non-critical failures. However, PDS also introduces the category:

Non-critical (NONC) failures = Failure where the main functions are not affected. Hence, such failures are neither dangerous nor spurious trip failures (e.g. sensor imperfection, which has no direct effect on control path).

Thus, the λ_{SU} rate used in IEC is in PDS split into $\lambda_{SU} = \lambda_{STU} + \lambda_{NONC}$. Hence, the PDS method considers three main failure modes, dangerous, spurious trip and non-critical. Further, the rate of critical failures, $\lambda_{crit} = \lambda_D + \lambda_{ST}$ is also split into rate of *undetectable* and *detectable*, i.e.

$$\lambda_{crit} = \lambda_{undet} + \lambda_{det}$$

The following table shows how PDS splits the rate of critical (random hardware) failures into various categories:

Table D.2 PDS split of critical (random hardware) failures

	Undetected	Detected	Sum
Dangerous	λ_{DU}	λ_{DD}	λ_{D}
Spurious Trip	λ_{STU}	λ_{STD}	λ_{ST}
Sum	λ_{undet}	λ_{det}	λ_{crit}

Note 1:
The formulas that are given below will follow as closely as possible the notation of the IEC. It will apply the β-factor model, but include the modification factors for voting as introduced in PDS. However, the formulas for PFD provided in Appendix B of IEC 61508-6 are rather complex and are not well documented. Thus, in Table D.4 below, new formulas are provided for PFD_{UK}. These formulas are taken from the PDS handbook /D.1/, and differ slightly from the formulas given in the IEC standard.

Note 2:
Table D.5 will provide approximate results for PFD_K. These simple formulas just express the probability of all N "channels" being unavailable due to repair of a dangerous failure. The decision to restrict to dangerous failures follows the IEC standard.

Note 3:
The IEC approach does not include unavailability due to functional testing, i.e. NSU. This seems inconsistent, as the unavailability due to repair *is* included. However, following IEC, we ignore this unavailability due to testing in the formulas below. Observe that this NSU could be given as Δ/τ, where Δ is the inhibition period (per test) for functional testing of the system.

Note 4:
The formulas below assume degraded operation by detection/repair of failures. So for instance, when a failure is detected on a duplicated system, the system is degraded to a 1oo1 system, and the failure is repaired on-line. Similarly, a 2oo3 system is assumed to be degraded to a 1oo2 system.

Note 5:
All formulas are actually approximations, valid when the test interval τ is not too long and the failure rate λ is small. For instance a main term, like $\lambda_{DU} \cdot \tau / 2$ is actually an approximation for $(1 - \exp(-\lambda_{DU} \cdot \tau)) / (\lambda_{DU} \cdot \tau)$.

D.2 Failure classification

The PDS method gives a well-defined and rather detailed failure classification, see Figure D.2 below (adapted from /D.1/).

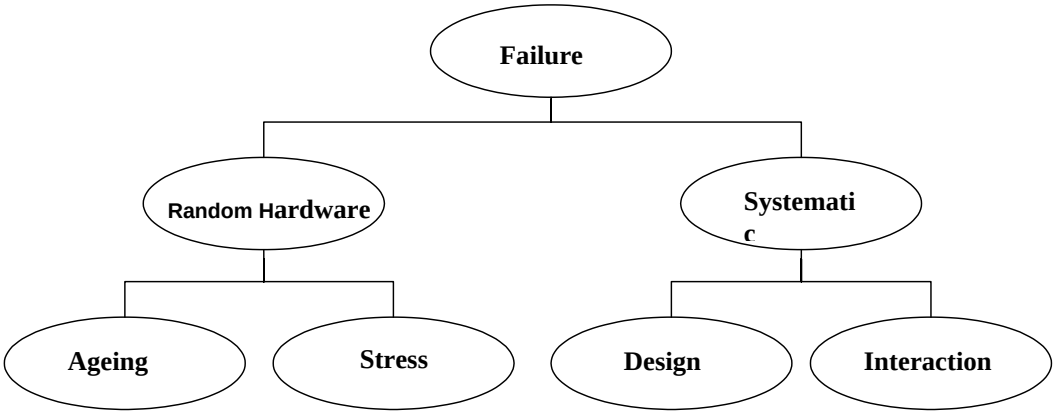

Figure D.2 Failure classification in PDS.

This classification details the categorisation of failures given in the IEC standard:

- Random hardware failures
- Systematic failures

The PDS interpretation is that "random hardware failures" is more or less identical to "physical failures", and that "systematic failures" is more or less identical to “non-physical failures”. The loss of safety caused by the first category (Random hardware failures) is quantified in IEC (by PFD), while loss of safety caused by systematic failures is not quantified here. Thus, the PFD will *not* include unavailability due to e.g.:

- Failure of detector to react due to "wrong" location of detector
- Failure of detector to discriminate between true and false alarm
- Failure due to software error
- Unavailability of system due to erroneous inhibition

In order to make the quantifications of loss of safety in PDS and IEC compatible, we here specify PSF to entirely relate to non-physical (systematic) failures and PFD entirely to relate to (physical) random hardware failures.

D.3 Common cause failure model

Regarding the handling of common cause failure (dependent failures), the use of the β-factor model has been rejected in PDS. In order to make a comparison between say 1oo2, 1oo3 and 2oo3 votings meaningful, there should be different β's for different voting configurations. This aspect is not included in the standard β-factor model as described in IEC 61508-2. Therefore, the PDS method, see /D.1/, has introduced the C_{MooN} factor. This means that the β-factor of a system with an M-out-of-N (MooN) voting (M<N) equals:

$$\beta_{MooN} = C_{MooN} \cdot \beta$$

Here the modification factor C_{MooN} reflects the configuration (voting), see Table D.3 below. Further, the beta-factor that applies for 1oo2 voting equals β. Thus, $C_{1oo2} = 1$.

Table D.3 Numerical values of modification factors for CCF of a MooN voting.

Voting	1oo2	1oo3	2oo3	1oo4	2oo4	3oo4
C_{MooN}	1.0	0.3	2.4	0.15	0.8	4.0

D.4 Calculation of PFD_{UK}

The contribution PFD_{UK} comes from dangerous undetected (DU) failures that occur with rate λ_{DU} (and are detected during manual tests with interval τ). For redundant systems we also have a contribution to PFD_{UK} where one unit is unavailable due to a repair (degraded operation). Following the IEC formulas we restrict to Dangerous failures (with rate λ_D). The suggested (detailed) formulas for PFD_{UK} are given in Table D.4, with the main term in bold. Note that the detailed formulas will depend on operational philosophy.

Table D.4 Formulas for PFD_{UK} (the approximate formula in bold)

Voting	Formula for PFD_{UK}	Comment
1oo1	$\boldsymbol{\lambda_{DU} \cdot \tau / 2}$	-
1oo2	$\boldsymbol{\beta \cdot \lambda_{DU} \cdot \tau / 2}$ + $[(1-\beta) \cdot \lambda_{DU} \cdot \tau]^2/3$ + $2 \cdot (1-\beta) \cdot \lambda_{det} \cdot MTTR \cdot \lambda_{DU} \cdot \tau/2$	The first term is caused by common cause DU failures. The 2nd term corresponds to two independent DU failures, and the 3rd term represents degraded operation, i.e. one unit has a detected failure (being repaired), and the other gets a DU failure.
2oo2	$\boldsymbol{(2-\beta) \cdot \lambda_{DU} \cdot \tau / 2}$ + $2 \cdot (1-\beta) \cdot \lambda_{det} \cdot MTTR \cdot \lambda_{DU} \cdot \tau/2$	The first term is caused by DU failures. The 2nd term represents degraded operation, i.e. one unit has a detected failure, and the other gets a DU failure.

2oo3	**$2.4 \cdot \beta \cdot \lambda_{DU} \cdot \tau$ /2** $+ [(1\text{-}1.7 \cdot \beta) \cdot \lambda_{DU} \cdot \tau]^2$ + $3 \cdot (1\text{-}1.7 \cdot \beta) \cdot \lambda_{det} \cdot MTTR \cdot \beta \cdot \lambda_D \cdot \tau/2$	The first term is caused by common cause DU failures. The 2nd term corresponds to two independent DU failures, and the 3rd term represents degraded operation, i.e. one unit has a detected failure, and then there is a common cause DU failure (of the degraded 1oo2 system).

D.5 Calculation of PFD_K

When maintenance activity is done while the plant is operating, the safety system is set in the off-line state. The time that the safety system is in off-line state due to repair is in IEC included as a part of *total PFD,* and this contribution can become significant if short time interval between proof tests (τ) is practised, or MTTR is long. Table D.5 presents formulas for the unavailability of safety system due to repair (giving the main term only).

Table D.5 Approximate formulas for PFD_K (main term only)

Voting	Formula for PFD_K	Comment
1oo1	$\lambda_D \cdot MTTR$	Component having dangerous failure is repaired
1oo2	$\beta \cdot \lambda_D \cdot MTTR$	Repair of both components due to a common cause failure.
2oo2	$(2\text{-}\beta) \cdot \lambda_D \cdot MTTR$	Repair of component(s) having dangerous failure
2oo3	$2.4 \cdot \beta \cdot \lambda_D \cdot MTTR$	Repair of two or three components due to a common cause failure.

D.6 Why should we also quantify systematic failures (PSF)?

In PDS it has been documented that unavailability of safety functions often are caused by "systematic failures", e.g.

- Failure of detector to react due to "wrong" location of detectors;
- Failure of detector to discriminate between true and false alarm;
- Insufficient functional test procedure;
- Human error during functional test:
  - detector left in by-pass;
  - wrong calibration of transmitter;
- Failure of shutdown valve to close since operator has left the isolation valve on the bleed off line in closed position;
- Failure to execute safety function due to software error.

These are typical elements constituting the PSF (Probability of Systematic Failure). In PDS it was strongly argued that it is not sensible to quantify only the contribution of hardware failures, and leaving out such a *major* contributor to loss of safety. It is true that it may be more difficult to quantify the PSF. However, the PDS project succeeded in providing typical generic values and for gas detectors an approach for obtaining "plant specific" PSF was also developed, see Appendix F of /D.1/. It is also possible to establish simpler approaches, e.g. along the lines of obtaining "plant-specific" β's as presented in IEC 61508-6, Annex D. It should also be noted that there are ongoing work in the PDS (BIP) project to provide guidelines on how to establish installation specific PSF values.

Regarding the quantification of PSF, it should be observed that:

1. The PSF is closely linked to the actual application / installation, and
2. objective data for PSF is often missing, so that quantification to a larger extent must be based on "subjective" data, i.e. expert judgements,

Hence, there are strong arguments for quantifying the PSF probability *separately*, and not just give the "total" CSU. Ref. also section C.4 in appendix C where the link towards QRA is discussed.

D.7 Recommended approach for quantification of loss of safety when IEC 61508 is used

Important elements of the safety unavailability were identified in Section D.1. Below the "short version" of the definitions are given:

- PFD_{UK} = Safety unavailability due to unknown (not *detected*) random hardware failures.
- PFD_K = Safety unavailability due to known random hardware failures, i.e. safety unavailability due to repair.
- PSF = Safety unavailability due to systematic failures.
- NSU= Safety unavailability due to functional testing.

Below, some recommendations regarding the approach for quantification of safety unavailability for safety systems are summarised:

1) Dependence on operating philosophy

The operating philosophy (degraded operation, on-line repair, etc) should be explicitly stated. The formulas presented above are based on the assumption that on-line repair is always carried out; also for a single (1oo1) safety system, and that degraded operation applies for duplicated and triplicated systems. Alternative formulas should be used when other assumptions apply (e.g. that degraded operation is not allowed, or on-line repair is not carried out when all channels have failed).

2) Data requirements

The quantifications require data on failure rates (split on dangerous/spurious trip/noncritical and undetected/detected), coverage, β-factor and test interval τ. As far as possible the data should be "plant specific", cf. the IEC approach for obtaining the β-factor.

3) Common cause failures

Regarding the handling of common cause failure (dependent failures), the use of the β-factor model has been rejected in PDS. The reason is that this model is not satisfactory with respect to comparing say 1oo2, 1oo3 and 2oo3 votings. If comparison between these voting logics shall be meaningful, there should be different β's for different voting configurations. This point is illustrated in Section D.8 below.

The IEC approach to find "plant-specific" β-factors is a good principle, and should be adopted.

4) Various contributions to loss of safety

As discussed above there are various contributions to safety unavailability. Which of these should be quantified?

As a *minimum* PFD_{UK} should *always* be quantified. However, the importance of systematic failures is well documented (cf. Section D.6 and section C.4 in Appendix C). The IEC approach of *not* quantifying this contribution to loss of safety, will represent a significant step backwards, as compared to the practise recommended in the PDS-method. However, providing separate values for PFD_{UK} and PSF and not only giving the sum CSU (as was previously done in PDS), seems a good idea.

So, in conclusion, it is *recommended* that all the four above elements of safety unavailability should be calculated as part of an overall evaluation of the safety system. Then also PFD (as defined in IEC) is directly found by adding two of these contributions. However, it is considered unfortunate that PFD mixes the unavailability due to “unknown” and “known” failures.

5) Quantification formulas

The formulas for quantification of PFD given in IEC are rather complex. "All" such formulas are actually approximations. However, it is suggested that the IEC formulas are not the most sensible approximations. The formulas presented above (Sections D.4 - D.5) are simpler and are recommended as a sounder basis for the quantifications. Whether only the main term corresponding to dependent failures (as used in PDS), or also the contributions from independent failures should be included must be decided for each application, based on the available data.

In the quantification of unavailability due to repair, not only the rate, λ_D, but also (part of) the rate of safe failures, λ_S could apply. This will require a modification of the formulas given above.

D.8 Example quantification

In this section, some quantifications of systems with MooN-voting are carried out, assuming that the β-factor for a MooN-voting is $\beta_{MooN} = \beta \cdot C_{MooN}$. Here β is the beta factor given in Table A.3, and C_{MooN} is a "configuration" factor, taking into account the applied voting logic of the system channels. Observe that $\beta \cdot C_{MooN} \cdot \lambda_{DU}$ is the (failure) rate of CCF giving a DU failure of the system, when this has a MooN voting; (that is the rate of CCF giving failure of at least M-N+1 of the N channels). Further observe that in this example, it is assumed that the MTTR is negligible and hence only the unknown failures are considered.

Table D.3 presents the numerical values of C_{MooN} suggested in PDS. The β-values given in Table A.3 apply for 1oo2, and thus $C_{1oo2} = 1$.

This approach will for instance give that PFD for a 1oo3 voting is significantly lower than for 1oo2, which again has a PFD significantly lower than for 2oo3. The standard β-factor model, as described in IEC 61508-2, will lack this feature, as then the dominant term in all three cases will be $PFD_{MooN} \approx \beta \cdot \lambda_{DU} \cdot \tau /2$ rather than

$$PFD_{MooN} \approx C_{MooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2; (M<N)$$

which is the formula used in the quantifications presented below. Note that this also can be written

$$PFD_{MooN} \approx C_{MooN} \cdot \beta \cdot PFD_{1oo1}; (M<N),$$

where PFD_{1oo1} is the single component PFD also given in Table A.3

For the NooN votings we below use $PFD_{NooN} \approx N \cdot \lambda_{DU} \cdot \tau /2 \approx N \cdot PFD_{1oo1}$ as a suitable approximation.

For Probability of Systematic Failures (PSF) we use

$$PSF_{MooN} \approx C_{MooN} \cdot \beta_{SF} \cdot PSF_{1oo1}; (M<N)$$

Here PSF_{1oo1} is the component PSF value given in Table A.3, and β_{SF} is the β-value for systematic failures (also found in Table A.3). For NooN the simple approximation $PSF_{NooN} \approx N \cdot PSF_{1oo1}$ is used here.

Table D.6 PFD and PSF for gas detectors, 1ooN voting logics (data from Table A.3)

Component	1oo1 [1]		1oo2		1oo3	
	PFD	PSF	PFD	PSF	PFD	PSF
Gas detector, catalytic	$3.9 \cdot 10^{-3}$	$5 \cdot 10^{-4}$	$2.0 \cdot 10^{-4}$	$1.0 \cdot 10^{-4}$	$0.6 \cdot 10^{-4}$	$0.3 \cdot 10^{-4}$
IR Gas detector [2]	$1.5 \cdot 10^{-3}$		$0.8 \cdot 10^{-4}$		$0.2 \cdot 10^{-4}$	

[1] As given in Table A.3
[2] Both conventional point detector and line detector

Table D.7 PFD and PSF for gas detectors, 2ooN voting logics (data from Table A.3)

Component	2oo2		2oo3		2oo4	
	PFD	PSF	PFD	PSF	PFD	PSF
Gas detector, catalytic	$7.8 \cdot 10^{-3}$	$1.0 \cdot 10^{-3}$	$4.7 \cdot 10^{-4}$	$2.4 \cdot 10^{-4}$	$1.6 \cdot 10^{-4}$	$0.8 \cdot 10^{-4}$
IR Gas detector [1]	$3.0 \cdot 10^{-3}$		$1.8 \cdot 10^{-4}$		$0.6 \cdot 10^{-4}$	

[1] Both conventional point detector and line detector

These results have been prepared as a basis for evaluating / choosing between various voting configurations for gas detectors. Note that the tables give the PFD and PSF for the *detectors* only, and so does not include e.g. the F&G logic solver.

D.9 Common cause failures between different types of components (diversity)

Sometimes the redundancy involves *non-identical* components. For instance two valves A and B, used in a 1oo2 configuration, are different (one being an ESV the other a CV). Then, a generalisation of the standard approach is required.

We should define some kind of average value for λ_{DU} for the two redundant components. If this average values are denoted $\lambda_{DU,Mean}$, and similarly β is the beta factor for the two non-identical (diverse) components, we would proceed as in the standard case, i.e. for 1oo2 we have the approximation $PFD_{1oo2} \approx \beta \cdot \lambda_{DU,Mean} \cdot \tau / 2$

The first question is how to define the average $\lambda_{DU,Mean}$ in a sensible way. In order to motivate the choice we first consider the following example: The two non-identical components A and B have DU rates, $\lambda_{DU,A}$ and $\lambda_{DU,B}$ that are very different, say

$\lambda_{DU,A} = 10^{-6}$ per hours, $\lambda_{DU,B} = 10^{-4}$ per hours,

Then, observe that the standard average, $\lambda_{DU,Ave} = (\lambda_{DU,A} + \lambda_{DU,B})/2 \approx 0.5 \cdot 10^{-4}$ may not give very sensible results. If the relevant beta is chosen as β=0.04, then the rate of CCF for the 1oo2 configuration equals $\beta \cdot \lambda_{DU,Ave} \approx 0.5 \cdot 10^{-4} \cdot 0.04 = 2 \cdot 10^{-6}$ per hours, which is higher than the DU rate of the A components, $\lambda_{DU,A} = 10^{-6}$ per hours. Thus, this approach results in the redundant 1oo2 system performing worse than having a single A component (in a 1oo1 configuration). Even if B has a much higher DU-rate than A, this is very unreasonable. Credit should be given for having the redundant component B.

Therefore another way to define the average λ_{DU} is suggested. We apply the so-called geometric mean:

$$\lambda_{DU,A,B} = \sqrt{\lambda_{DU,A} \cdot \lambda_{DU,B}}$$

In the above example this gives $\lambda_{DU,A,B} = \sqrt{10^{-6} \cdot 10^{-4}} = \sqrt{10^{-10}} = 10^{-5} / hrs$, (observe that the exponent of the Mean, i.e. -5, equals the average of the exponents of the A and B rate). In this case the rate of CCF for the 1oo2 configuration becomes $0.04 \cdot 10^{-5} = 4 \cdot 10^{-7}$ which is a much more sensible result.

This choice of using the geometric means of non-identical components i.e. $\lambda_{DU,A,B} = \sqrt{\lambda_{DU,A} \cdot \lambda_{DU,B}}$ is therefore suggested, as it is much more "robust" to the case of having very different DU rates. In extreme cases with *very* different DU rates of A and B, we could get the same problem also for this definition of $\lambda_{DU,A,B}$, but this is very unlikely to occur in practice.

For a triplicated system (with components A, B and C), the average DU rate is now similarly defined as

$$\lambda_{DU,A,B,C} = \sqrt[3]{\lambda_{DU,A} \cdot \lambda_{DU,B} \cdot \lambda_{DU,C}}$$

(of course two of these DU rates could very well be identical).

Finally, the β for non-identical (diverse) components can be assessed e.g. by the approach suggested in IEC 61508, part 6. Note that this usually will result in a β which is smaller than the β which is used for identical components.

D.10 Some useful formulas

The Safe Failure Fraction (SFF) can be calculated using several different formulas, but one possible formula is:

$SFF = 100(\lambda_{TOT} - \lambda_{DU}) / \lambda_{TOT}$

Given the total failure rate, the Mean Time To Failure (MTTF) can be calculated

$MTTF = 1 / \lambda_{TOT}$

D.11 References

/D.1/ Reliability Prediction Method for Safety Instrumented System. PDS Method Handbook, 2003 Edition. SINTEF report STF38 A02420.

/D.2/ Reliability Data for Safety Instrumented System. PDS Data Handbook, 2003 Edition. SINTEF report STF38 A02421.

APPENDIX E

LIFECYCLE PHASES, ACTIVITIES AND DOCUMENTATION

CONTENT

E.1 Lifecycle phases for a typical offshore project

INVESTMENT STUDIES

The Feasibility Phase
The Feasibility phase is the first phase after the decision is made to establish a field development project.

The Concept Phase
This phase starts when a decision is made to substantiate further field development and ends when a decision is made whether or not to prepare a plan for development and operation (PDO).

The Pre-Execution Phase (PDO-phase)
This phase starts when one field development concept is selected and the decision is made to prepare the PDO. It is completed when the PDO is sent to the authorities and the main engineering contractor is selected.

INVESTMENT PROJECT EXECUTION

Detail Engineering and Construction Phase
This part of Project Execution starts with the final decision to execute the project and by the award of the main contract(s), and ends when the facilities are mechanically complete (pre-commissioning).

The Final Commissioning and Start-up Phase
This part of Project Execution starts when systems or parts of systems are mechanically completed (pre-commissioning), and is concluded when all systems are handed over to operations and finally accepted by the customer.

OPERATION AND DE-COMMISSIONING

The Operational Phase
This phase starts when the installation is handed over and accepted by operations.

The De-commissioning Phase
This phase starts with the decision to shut down the field and remove the installation.

Lifecycle phases as described in IEC 61511 with reference to typical offshore project

Risk Analysis and Protection Layer Design

This activity will start in the concept phase and continues into detail engineering. Concludes with an "as built" risk analysis report. When major design changes occur, the report shall be updated.

An update of the risk analysis will normally be conducted at certain time intervals after the installation has come into operation (e.g. every five years).

Allocation of Safety Functions to Protection Layers

This activity starts in the pre-execution phase and concludes with a report (specification) in the detail engineering phase.

Safety Requirements Specification for the Safety Instrumented System

This activity starts in the pre-execution phase and concludes with a report (specification) in the detail engineering phase. The SRS document shall be subject to follow-up and updating in the operation and maintenance phase.

Design and Engineering of Safety Instrumented System

This activity starts in the pre-execution phase and concludes in the detail engineering phase.

Installation, Commissioning and Validation

This activity starts in the construction phase and concludes with the final commissioning.

Operation and Maintenance

This activity will be part of the operational phase of the installation.

Modification

This activity will be part of the operational phase.

Decommissioning

This activity is taking place in the decommissioning phase

In addition there will be activities related to verification, management and planning, ref. figure 2.2 in main document.

E.2 SRS structure and content

This section outlines possible structure and content of the Safety Requirement Specification (SRS).

IEC61511-1, ch.10.3, shall form the basis for the information in the SRS. The SRS shall be a separate and complete "living document" during all lifecycles and will be updated as described in Figure E.1.

Generally, the SRS shall contain the relevant key information for use in specifying and operating the instrumented safety functions. However, the information required may be contained in other project documents, referred to in the SRS. Duplication of information should be avoided. Where electronic documentation is used, these references shall as far as possible be of an interactive type (i.e. hyperlink). When using such references care should however be taken; the SRS shall be a living document also through the operational phases, while many project documents are not updated after
as-built status.

The SRS shall contain three main types of requirements:

- Functional requirements like capacities and response times
- Integrity requirements like PFD and SIL
- Operating prerequisites and constraints

It is important that the SRS states the required manual test frequencies and to ensure that these requirements are compatible with the planned manning level at the installation taking into consideration time available for performing the tests.

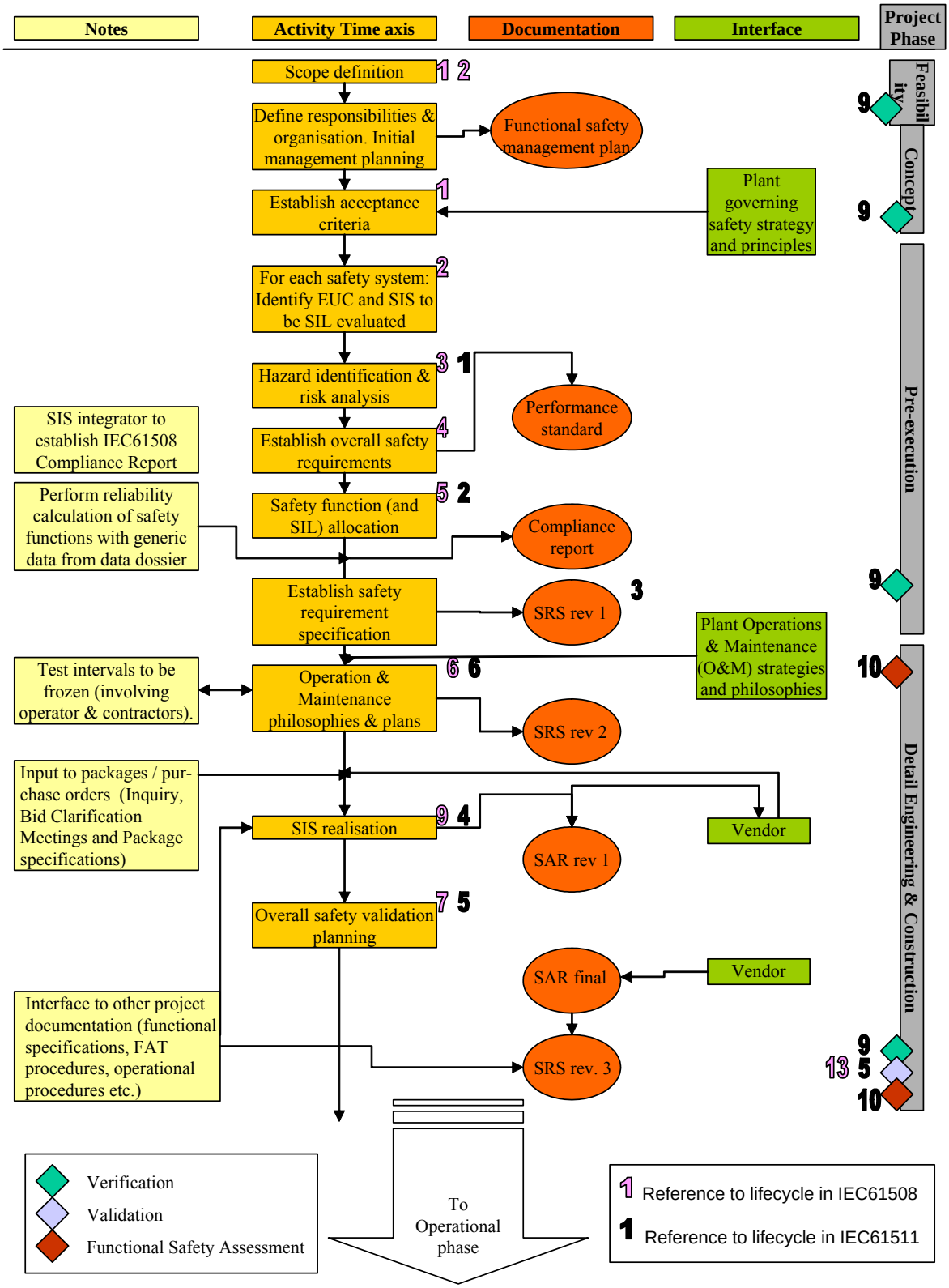

Figure E.1a SRS time axis, part 1.

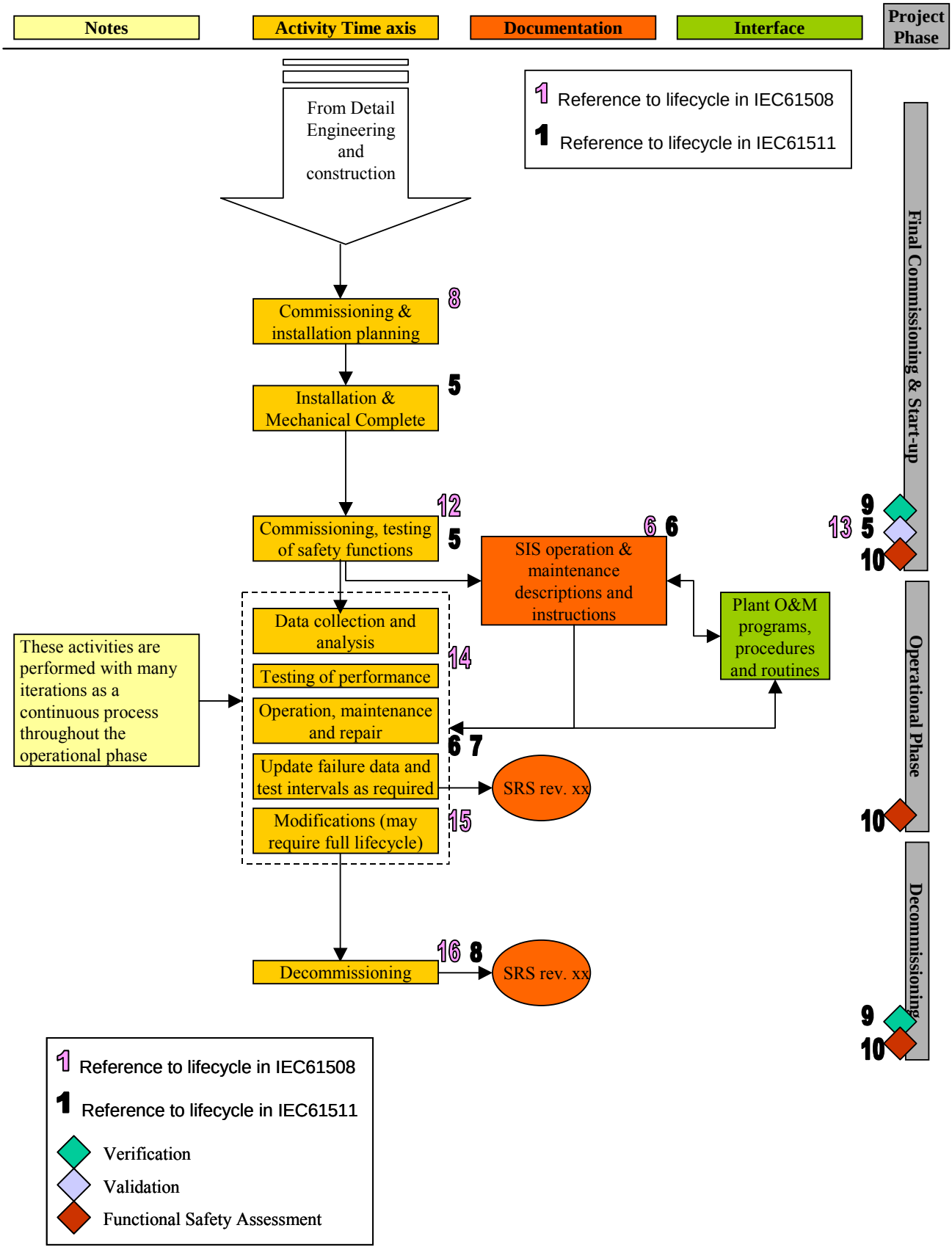

Figure E.1b SRS time axis, part 2.

Tables with suggested content for the SRS based on IEC61511-1, 10.3, have been made and are shown as examples below. It should be noted that all elements listed in IEC 61511 are not relevant for all types of SIS. Further, note that much of the required content of the SRS will not be available during early project phases. Therefore, the relevant SRS revision number (reflecting chronological order or events – ref. figure E.1; SRS "time axis") are based on the time/phase at which a requirement should be included.

The two example tables shown below are based on a document structure where one SRS is produced *per system*. It should be noted that other SRS structures will be possible, e.g. one common SRS for all the defined safety functions. An example of an SRS format with a common document for all the defined safety functions is available at: http://www.itk.ntnu.no/sil/ .

Example table E.1 shows a proposed SRS list of content for the PSD system. The PSD system will connect to most of the plant processes, which are documented in other design documents (e.g. ISO 10418, SAT tables).

PSD systems for other than hydrocarbon systems are not covered by ISO 10418. The design and supply of these systems will normally be specified in a Functional Specification for the unit or system.

Example table E.2 indicates an SRS list of content for the F&G and the ESD system. Requirements to these two global safety systems will be defined in safety specifications. These systems will also have safety interfaces to other systems (shut down of electrical systems, HVAC systems, etc). The instrumented safety function shall be described completely in the SRS for the F&G and ESD system, while equipment data for the interfaced systems shall be included in the relevant system Functional Specification.

As discussed above, some of the required content of the SRS cannot be given at early phases of the project execution, hence the relevant SRS revision number (reflecting chronological order or events – ref. SRS time axis) have been given when a requirement should be included. Some requirements must be established before the first SRS is produced, then the relevant project phase is referred.

The two example tables given below suggest where the different information shall be found. It should be noted that these are only suggestions as the project may select other documentation structures.

Table E.1 List of content for SRS for PSD system.

ID	Reference, IEC61511, Ch.10.3	PSD for hydrocarbon systems	PSD for other process systems	Lifecycle phase (ref. figure E.1)
1	Description of all the necessary instrumented functions to achieve the required functional safety	ISO 10418 SAT	Functional Specification	SRS rev. 1
2	Requirements to identify and take account of common cause failures	SRS	Functional Specification	SRS rev. 2
3	Definition of the safe state of the process for each identified safety instrumented function	SRS	SRS	SRS rev. 1
4	Definition of any individually safe process states which, when occurring concurrently, create a separate hazard	ISO 10418 SAT	Functional Specification	SRS rev. 3
5	Assumed sources of demand and demand rate of the safety instrumented function	SRS	SRS	Pre-execution
6	Requirement of proof test intervals	SRS	SRS	Pre-execution
7	Response time requirement for the SIS to bring the process to a safe state	SRS	SRS	SRS rev. 2
8	Safety integrity level for each safety instrumented function (SIF) and mode of operation (demand /continuous) for each SIF	SRS	SRS	Pre-execution
9	Description of SIS process measurements and their trip points	SRS	SRS	SRS rev. 3
10	Description of SIS process output actions and the criteria for successful operation.	ISO 10418 SAT	Functional Specification	SRS rev. 3
11	Functional relationship between process inputs and outputs, including logic, mathematical functions	PI&D/SCD and C&E	PI&D/SCD and C&E	SRS rev. 2
12	Requirements for manual shutdown	SRS	SRS	SRS rev. 2
13	Requirement related to energize or de-energize to trip	SRS	SRS	SRS rev. 2
14	Requirements for resetting the SIS after a shutdown	SRS	SRS	SRS rev. 2
15	Maximum allowable spurious trip rate	SRS	SRS	SRS rev. 2
16	Failure modes and desired response of the SIS	SRS	SRS	SRS rev. 3
17	Any specific requirements related to the procedure for starting up and restarting the SIS	SRS	SRS	SRS rev. 2
18	Interfaces between the SIS and any other system	SRS	SRS	SRS rev. 2
19	Description of the modes of operation of the plant and identification of the SIFs required to operate within each mode	Functional Specification	Functional Specification	SRS rev. 3
20	The application of software safety requirements	Ref 61511, section 12.2.2	Ref 61511, section 12.2.2	SRS rev. 2
21	Requirements for overrides/ inhibits/ bypasses including how they will be cleared	SRS	SRS	SRS rev. 2
22	Specification of any action necessary to achieve a safe state in the event of faults being detected by the SIS. Any such action shall be determined taking account of all relevant human factors	SRS	SRS	SRS rev. 2
23	Minimum worst-case repair time, which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints etc.	SRS	SRS	SRS rev. 3
24	Dangerous combinations of output states of the SIS must be addressed	SRS	SRS	SRS rev. 3
25	The extremes of all environmental conditions that are likely to be encountered by the SIS shall be identified. This may require consideration of the following; temperature, humidity, contaminants, grounding, electromagnetic interference, etc. (see IEC61511, cht. 10.3)	SRS	SRS	SRS rev. 2
26	Identification to normal and abnormal modes for both the plant as whole and individual plant operational procedures (for example, equipment maintenance, sensor calibration and/or repair)). Additional safety instrumented functions may be required to support these modes of operation.	Functional Specification	Functional Specification	Pre-execution
27	Definition of the requirement for any safety instrumented function necessary to survive a major accident event, for	Safety specification	Safety specification	SRS rev. 2

	example, time required for a valve to remain operational in the event of a fire.			

Table E.2 List of content for SRS for F&G and ESD systems.

ID	Reference, IEC61511, Ch.10.3	F&G system	ESD system	Lifecycle phase (ref. figure E.1)
1	Description of all the necessary instrumented functions to achieve the required functional safety	Safety specification	Safety specification	SRS rev. 1
2	Requirements to identify and take account of common cause failures	SRS	SRS	SRS rev. 2
3	Definition of the safe state of the process for each identified safety instrumented function	SRS	SRS	SRS rev. 1
4	Definition of any individually safe process states which, when occurring concurrently, create a separate hazard	SRS	SRS	SRS rev. 3
5	Assumed sources of demand and demand rate of the safety instrumented function	SRS	SRS	Pre-execution
6	Requirement of proof test intervals	SRS	SRS	Pre-execution
7	Response time requirement for the SIS to bring the process to a safe state	SRS	SRS	SRS rev. 2
8	Safety integrity level for each safety instrumented function (SIF) and mode of operation (demand /continuous) for each SIF	SRS	SRS	Pre-execution
9	Description of SIS process measurements and their trip points	SRS	SRS	SRS rev. 3
10	Description of SIS process output actions and the criteria for successful operation.	Functional Specification	Functional Specification	SRS rev. 3
11	Functional relationship between process inputs and outputs, including logic, mathematical functions	Fire Protect. Data Sheets	C&E	SRS rev. 2
12	Requirements for manual shutdown	SRS	SRS	SRS rev. 2
13	Requirement related to energize or de-energize to trip	SRS	SRS	SRS rev. 2
14	Requirements for resetting the SIS after a shutdown	SRS	SRS	SRS rev. 2
15	Maximum allowable spurious trip rate	SRS	SRS	SRS rev. 2
16	Failure modes and desired response of the SIS	SRS	SRS	SRS rev. 3
17	Any specific requirements related to the procedure for starting up and restarting the SIS	SRS	SRS	SRS rev. 2
18	Interfaces between the SIS and any other system	SRS	SRS	SRS rev. 2
19	Description of the modes of operation of the plant and identification of the SIFs required to operate within each mode	SRS	SRS	SRS rev. 3
20	The application of software safety requirements	Ref 61511, section 12.2.2	Ref 61511, section 12.2.2	SRS rev. 2
21	Requirements for overrides/ inhibits/ bypasses including how they will be cleared	SRS	SRS	SRS rev. 2
22	Specification of any action necessary to achieve a safe state in the event of faults being detected by the SIS. Any such action shall be determined taking account of all relevant human factors	SRS	SRS	SRS rev. 2
23	Minimum worst-case repair time, which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints etc.	SRS	SRS	SRS rev. 3
24	Dangerous combinations of output states of the SIS must be addressed	SRS	SRS	SRS rev. 3
25	The extremes of all environmental conditions that are likely to be encountered by the SIS shall be identified. This may require consideration of the following; temperature, humidity, contaminants, grounding, electromagnetic interference, etc. (see IEC61511, cht. 10.3)	SRS	SRS	SRS rev. 2
26	Identification to normal and abnormal modes for both the plant as whole and individual plant operational procedures (for example, equipment maintenance, sensor calibration and/or repair)). Additional safety instrumented functions may be required to support these modes of operation.	SRS	SRS	Pre-execution

27	Definition of the requirement for any safety instrumented function necessary to survive a major accident event, for example, time required for a valve to remain operational in the event of a fire.	Safety specification	Safety specification	SRS rev. 2

E.3 SAR structure and content

In this section an outline of the structure and content of the Safety Analysis Report (SAR) is given.

The SAR shall be produced by each equipment supplier as part of the Detailed Engineering and Construction phase, in order to document compliance with requirements given in the SRS. See Figure E.2 below for SAR production and vendor compliance with SRS.

Since an instrumented safety function will often comprise equipment from several vendors, the information contained in each of the SARs has to be integrated and compliance with the SRS requirements for the function must be demonstrated. This may be done as part of the SRS documentation.

Any updates to the equipment after the SARs have been approved in the engineering phase, shall be documented in the SRS in order to ensure compliance with the SRS requirements. Hence, the SAR need not necessarily be updated as part of the equipment change.

In the following, a possible structure for the table of content for a SAR is given. Please note that this is only an example. It is important that the SAR table of content reflects the requirements in the SRS.

SAR Table of content - example

I Abbreviations
II References
III Summary

1. Introduction
2. System Description
3. System Topology and Block Diagram
4. Operational description of the system (including modes of operation)
5. List of all assumptions
6. Failure rate of the components
7. Common Cause failures
8. Diagnostic Coverage & Safe Failure Fraction
9. Behaviour of system/components on detection of a fault
10. Factory testing
11. Operational testing (incl. test procedures and recommended functional test interval)
12. Architectural Constraints
13. Avoidance and Control of Systematic Failures
14. Software documentation
15. Results

Appendices
E.g. Certificates, test documentation, FMECA, Failure reports.

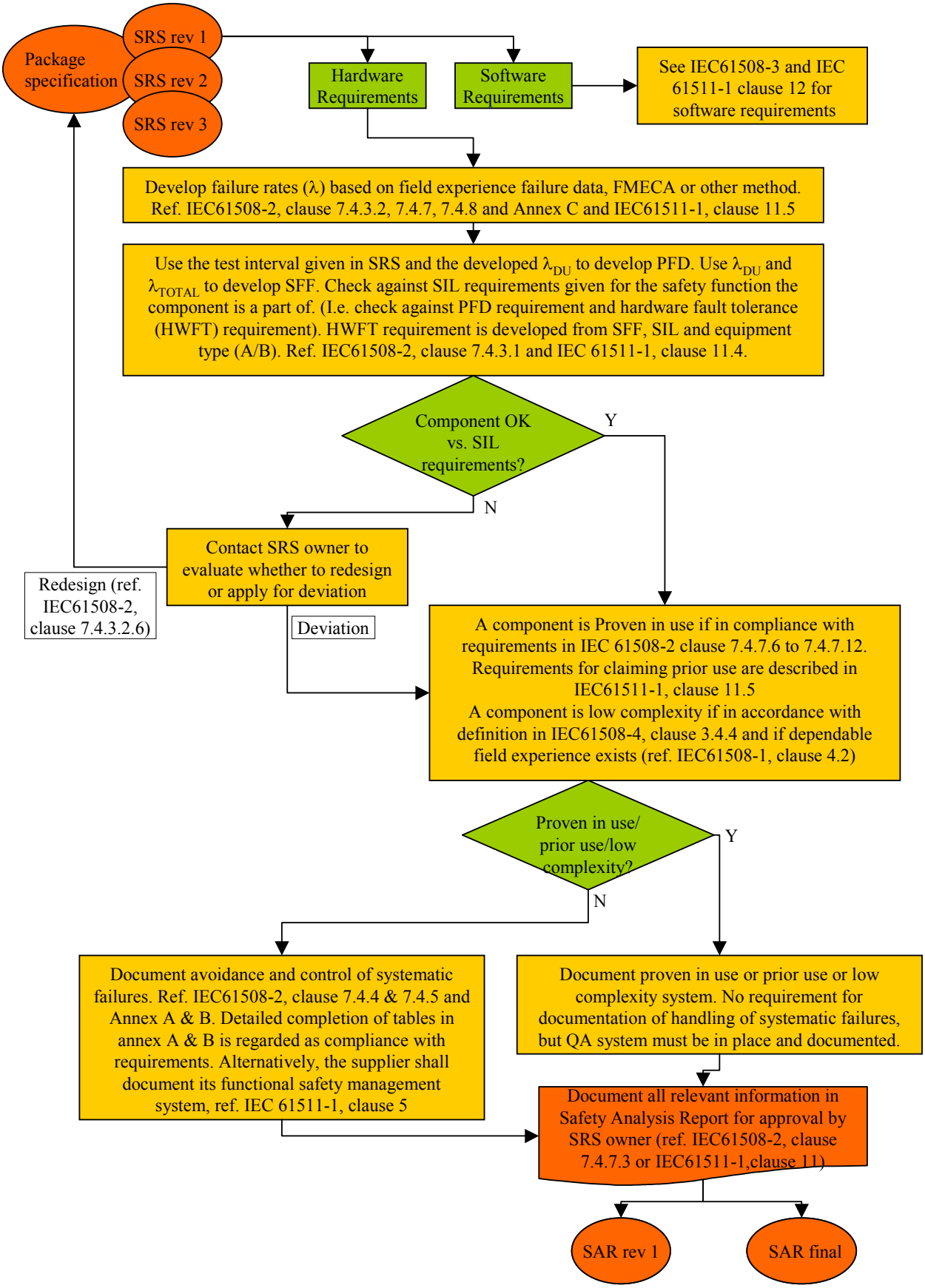

Figure E.2 SAR production and vendor compliance

APPENDIX F

SIL FOLLOW UP

CONTENT

F.1 Overview of operation and maintenance activities for SIL work

Table F1 below gives an overview of SIL related operation and maintenance activities.

Table F.1 Overview of SIL related operation and maintenance activities

OPERATION		MAINTENANCE/TEST		
	OPERATIONS	**Preventive Maintenance**	**Corrective Maintenance (to restore SIL function)**	**Functional proof / performance test according to SRS**
Normal Operations (including maintenance shutdowns)	Description and procedure of the various safety functions to ensure operations in accordance with the allocated safety performance requirements. The limits and premises for safe operation to be defined, including possible different modes of operations for process and equipment and effects on the safety functions in each of the operating modes.	The PM activities shall be reviewed and defined to ensure SIL compliance. The initial test frequency to be defined.	The main failure modes to be identified and reviewed. Description of safety function behaviour in the presence of errors shall be described. Premises for performing corrective maintenance during normal operations to be described, including instructions for carrying out repair.	The methods for testing, full scale and / or partial, during normal operations and periods of maintenance shutdown shall be described in detail. Pass and fail criteria shall be defined. The initial test frequency to be defined.
Abnormal Operations (emergency / start-up / shutdown)	Description and, if required, procedures for ensuring optimal use of the various safety functions in an abnormal situations including demand of safety functions (emergency situations). Emergency response / manual intervention to be included. The limits and premises for safe operation to be defined.	-	-	The methods for testing, full scale and / or partial, as part of planned shut down of the facilities shall be described in detail. The initial test frequency to be defined. Conditions and measures required to re-instate any safety functions in testing modes to nominal operating condition in case of occurrence of abnormal situations shall be described.
Blocking / override	Procedures and premises for allowing and setting blocking and overrides during specifically defined operating conditions such as start-up shall be described. These may, if adequate for the specific facilities, be covered by Company's general procedures. Establish required manual intervention or other compensating measures if required.	See Corrective Maintenance	Procedures and premises for allowing and setting blocking and overrides for performing maintenance and testing activities shall be described. These may, if adequate for the specific facilities, be covered by Company's general procedures. Establish required manual intervention or other compensating measures if required.	See Corrective Maintenance.

OPERATION		MAINTENANCE/TEST		
	OPERATIONS	**Preventive Maintenance**	**Corrective Maintenance (to restore SIL function)**	**Functional proof / performance test according to SRS**
Logging/ reporting	Procedures shall be in place to ensure that all relevant data for safety functions are retrieved and logged / documented, including unexpected call for the safety functions. Any deficiency disclosure of safety function operating condition or performance requirements shall be reported. Handling of deviations shall be described.	-	-	See Operation – logging / reporting. The procedure shall address the requirement to record the real demand as (partial) proof / performance test. The procedure shall address how this may replace / postpone the scheduled tests of the activated safety functions. Any deficiency disclosure of safety function operating condition or performance requirements shall be reported. Handling of deviations shall be described.
Verification	Routines and/or procedure for verification of adherence to operational procedures, premises and limitations related to the safety functions.	See Corrective Maintenance	Routines and/or procedure for verification that maintenance activities are properly executed and reported.	Routines and/or procedure for verification that proof / performance tests are properly executed and reported. Routines for regular verifications of the instrumented safety function, i.e. to confirm compliance with the Safety Requirements Specification.

F.2 Procedures for update of test intervals

In this section a *calculation procedure for obtaining performance and test interval throughout the entire life time of a safety function* is discussed. Two alternative approaches are proposed; one simplified approach (ref. section F.2.1) and a somewhat more advanced approach (ref. section F.2.2).
These methods are only given as examples and guidance, and both simpler and even more elaborate theories exist for follow-up.

F.2.1 Simplified PFD and failure rate estimate

Assume that equipment failure data has been collected as part of the periodic testing activities on an installation. For a specific type of equipment, e.g. ESV/XV valves, assume:

- n components have been tested with respect to their ability to close on demand,
- X failures have been observed either due to functional testing or as a consequence of demands

Then a simple estimate of the PFD can be obtained by taking:

$$PFD = X / 2n$$

Multiplying by the factor 2 simply reflects the fact that a functional test is performed at the end of the interval.
Assume further that the test interval τ is known. Then, an estimate of the dangerous failure rate λ_{DU} for undetected failures can be obtained by the approximate formula:

$$\lambda_{DU} = X / (n \cdot \tau)$$

i.e. the number of DU failures divided by the total estimated operational time of the sample[7].

For a situation where the test interval τ is changed, the above formulas make use of accumulated information difficult, therefore the more elaborate method is proposed below. In addition to the above calculations, some criterion for changing the test interval based on deviations from required PFD has to be given. The above parameters may then serve as input to the approach described below.

F.2.2 Example of approach for updating test intervals and failure rate estimates

This approach gives updated test intervals and failure rate estimates as field specific data becomes available. In addition to the updated values some guidance is given on actually changing the test interval.

General

A (sub) function is specified, for which it is decided to use an identical test interval of length,τ. Thus, a group of components (e.g. transmitters) is identified that also

- *is considered identical, (e.g. assuming the same environment, application, failure rate and beta-factor)*
- *has the same voting logic, denoted* MooN

It must also be decided how often the test interval is considered for updating. The steps 1- 3 are performed once *(providing some fundamental input to the updating), the remaining steps are carried out each time a possible update of the test interval is considered.*

A common time unit must be specified (hours, days, months, years). Below it is assumed that we use "hours" both for the test intervalτ and the failure rate λ_{DU}.

Step 1 Specify parameters of (sub) function

The initial values for the input parameters to the updating procedure are found directly from Appendix D!

Insert the following parameters for the (sub) function in question:

Best estimate, rate of DU failures,	$\lambda_{DU,BE}$	= _____
Conservative estimate, rate of DU failures,	$\lambda_{DU,CE}$	= _____
Beta factor,	β	= _____
Min. no. of components that have to function to ensure system function,	M	= _____
No. of redundant "channels" of sub function,	N	= _____

[7] If credit is taken for demands and operations during the test period, the actual PFD will be lower than that given by these formulas. However, the λ_{DU} -estimate will not change due to these demands. The operational time $n \cdot \tau$ is in fact constant, and it is not important for the λ_{DU} -estimate whether failures are detected by test or demand. If demands and operations are credited as tests, the average PFD over the test period will be smaller than without, and the formulas also for the more advanced method have to be changed.

Step 2 Establish the risk acceptance criterion, PFD^A

Specify the highest acceptable PFD for the given (sub)function, i.e.

$PFD < PFD^A =$ _____

Step 3 Specify initial value for "uncertainty parameters" (for the rate of DU failures)

Generally, the estimate of λ_{DU} will be written as $\lambda_{DU} = U_2/ U_1$. These U_1 *and* U_2 are denoted the *uncertainty parameters*, and initial values for these have to be specified, e.g.

$U_1 = \lambda_{DU,BE} / [\lambda_{DU,CE} - \lambda_{DU,BE}]^2 =$ _____

$U_2 = U_1 \times \lambda_{DU,BE} =$ _____

The following steps are performed each time an update of the test interval is considered (based on new operational data).

Step 4 Collect new field specific failure data, and update the failure rate estimate

Let X denote the accumulated number of component failures observed since last updating, and let t denote the total operational time for all components during this period, (this is typically the calendar time since last update multiplied with the number of components).

No. of DU failures (component level), $X =$ _____
Total operational time (all components), $t =$ _____

Next update U_1 *and* U_2 :

$U_1(\text{new}) = 0.9U_1(\text{old}) + t =$ _____

$U_2(\text{new}) = 0.9U_2(\text{old}) + X =$ _____

and using these new U_1 and U_2 we find the new updated rate of DU failures as:

$$\lambda_{DU} = \frac{U_2}{U_1} =$$ _____

Step 5 Failure cause analysis

An analysis should be performed to eliminate the root cause of the failures reported.

Step 6 Update test interval based on new data

The PFD can be calculated based on the length of the test interval, τ, the rate of DU failures, λ_{DU}, the beta factor β, and the voting *MooN*, (giving "voting factor" C_{MooN}). All parameters except τ are given/updated in the previous steps, and thus PFD can be calculated for various values of τ. A simple spreadsheet in MS EXCEL (PDS-PFD.XLS) can be downloaded from http://www.itk.ntnu.no/sil/ to do these calculations for various relevant values of τ (these are approximate formulas based on MTTR being small. Figure F.1 shows the screen which is found under the "FollowUp" tab).

The obtained PFD values are inserted in a Table, see below:

	τ = 720 *hrs* (= 1 *month*)		τ = 2190 *hrs* (= 3 *months*)	τ =4380 *hrs* (= 6 *months*)	τ = 8760 *hrs* (= 12 *months*)	
PFD=						

From this Table it is easily seen for which τ the acceptance criterion

$PFD^A \geq PFD$

is satisfied. The maximum τ satisfying the acceptance criterion and the corresponding PFD are now recorded:

$\tau_0 =$ _____

PFD = _____

This τ_0 is a candidate to be the new updated length of the test interval.

Step 7 Verify new test interval

If Step **6** results in an increase of the length of the test interval, τ_0, some verification is required before this increase is implemented, i.e. to obtain the final test interval, τ.

- The increase of the length of the test interval (in one updating) should never exceed 50%
- The increase of the length of the test interval (in one updating) should never be more than 0.5 year.
- In order to optimise the grouping of several maintenance intervals, one could accept up to 10% increase in the PFD, i.e. we could accept $1.1 \times PFD^A \geq$ PFD in Step **6**.

To violate these requirements it would be needed that a thorough analysis is conducted to assure e.g. that an extended interval will not increase the rate of DU failures due to the reduction in preventive maintenance (following the introduction of a longer test interval.)

Similarly, for a new installation with no plant specific data it is not recommended to start with a $\tau > 8760$ hours.

Step 8 Trend analysis

A Nelson Aalen plot should be constructed to help identifying any systematic change in the failure rate of the components being analysed. The following procedure is recommended for construction of the Nelson Aalen plot.

i) The x-axis represents the calendar time

ii) The dates for observed component failures are marked on the x-axis. This will typically be either the data for the functional tests, or the data for any real demand. Let X_t be the number of failures observed at time t(date of test or demand). Let N_t denote the number of units included in the analysis at time t.

iii) Plot ($\Sigma_t X_t / N_t$) against t. Here $\Sigma_t X_t / N_t$ is calculated by increasing the Y-value with X_t / N_t for each t-value.

If the plot shows a convex behaviour, this indicates an increasing failure rate. On the other hand, if the plot shows a concave behaviour, this indicates an improvement of the situation.

Numerical example

In the following we give an example where a 2oo3 detector configuration is analysed. Reliability data etc are found in the PDS data handbook. We note that a conservative estimate is not given in the PDS data handbook, but in the OREDA 2002 data handbook we find the standard deviation of the estimate, and hence we set the conservative estimate equal to the best estimate plus the standard deviation.

Step 1 Specify parameters of (sub)function

Best estimate, rate of DU failures, $\lambda_{DU,BE} = 0.7\times10^{-6}$

Conservative estimate, rate of DU failures, $\lambda_{DU,CE} = 1.3\times10^{-6}$

Beta factor, $\beta = 2\%$

Min. no. of components that have to function to ensure system function, $M = 2$

No. of redundant "channels" of subfunction, $N = 3$

Step 2 Establish the risk acceptance criterion, PFD^A

$PFD < PFD^A = 1.0\times10^{-4}$

Step 3 Specify initial value for "uncertainty parameters" (for the rate of DU failures)

$U_1 = \lambda_{DU,BE} / [\lambda_{DU,CE} - \lambda_{DU,BE}]^2 = 1944444$

$U_2 = U_1 \times \lambda_{DU,BE} = 1.36$

Step 4 Collect new field specific failure data, and update the failure rate estimate

No. of DU failures (component level), $X = 1$

Total operational time (all components), $t = 430\,000$

Next update U_1 *and* U_2 :

$U_1(\text{new}) = 0.9U_1(\text{old}) + t = 2\,180\,000$

$U_2(\text{new}) = 0.9U_2(\text{old}) + X = 2.23$

and using these new U_1 and U_2 we find the new updated rate of DU failures as:

$$\lambda_{DU} = \frac{U_2}{U_1} = 1\times10^{-6}$$

Step 5 Failure cause analysis

Not conducted in this calculation example

Step 6 Update test interval based on new data

	τ = 720 *hrs* (= 1 *month*)		τ = 2190 *hrs* (= 3 *months*)	τ =4380 *hrs* (= 6 *months*)	τ = 3650 *hrs* (= 5 *months*)	τ = 2880 *hrs* (= 4 *months*)
PFD=	2.3×10^{-5}		7.6×10^{-5}	1.7×10^{-4}	1.5×10^{-4}	1.0×10^{-4}

The maximum τ satisfying the acceptance criterion and the corresponding PFD are now recorded:

τ_0 = 2880 *hrs* (= 4 *months*)

PFD = 1.0×10^{-4}

This τ_0 is a candidate to be the new updated length of the test interval.

Below, we have shown how the result from step 4 and 6 could be repeated for several periods (P1, P2, …). The output from the PDS-PFD.xls program (Follow up tab, ref. http://www.itk.ntnu.no/sil/) is:

Parameter	Value
PFD^A	1,0E-04
$\lambda_{DU,BE}$	7,0E-07
$\lambda_{DU,CE}$	1,3E-06
M	2
N	3
β	2,00 %
RF	90 %
SD_{λ}	6,0E-07
U_1	1944444
$U2$	1,361111

=Fields to enter data into

=Result fields (Do not modify!)

Parameter	P0(Init)	P1	P2	P2	P3	P4	P5	P6	P7
X -this period		1	0	0	0	1	1	0	1
t - this period		430 000	525 600	525 600	525 600	525 600	525 600	525 600	525 600
N_{FT} this period									
ΣX	0	1	1	1	1	2	3	3	4
Σt	0	430000	955600	1481200	2006800	2532400	3058000	3583600	4109200
ΣN_{FT}	0	0	0	0	0	0	0	0	0
U_1	1944444	2180000	2487600	2764440	3013596	3237836	3439653	3621287	3784759
$U2$	1,36	2,23	2,00	1,80	1,62	2,46	3,21	2,89	3,60
λ_{DU} (Bayes)	1,3E-06	1,0E-06	8,0E-07	6,5E-07	5,4E-07	7,6E-07	9,3E-07	8,0E-07	9,5E-07
λ_{DU} (MLE)		2,3E-06	1,0E-06	6,8E-07	5,0E-07	7,9E-07	9,8E-07	8,4E-07	9,7E-07
τ (GoalSeek)	2 816	3 587	4 547	5 615	6 801	4 821	3 918	4 582	3 845
τ (hours)	2 817	3 587	4 551	5 618	6 801	4 821	3 918	4 582	3 845
τ (months)	3,9	4,9	6,2	7,7	9,3	6,6	5,4	6,3	5,3
PFD	1,0E-04	1,0E-04	1,0E-04	1,0E-04	1,0E-04	1,0E-04	1,0E-04	1,0E-04	1,0E-04

Figure F.1 – Output from the PDS-PFD.xls program

F.3 Actual shutdowns as test

To give a rough estimate of the increase in *PFD* if the next planned functional test is skipped, we shall introduce a specific situation:

- The last functional test was performed at time t.
- The length of the test interval is τ.
- A shutdown has occurred at time t_s, t_s is inside the interval $[t+ \tau/2, t+ \tau]$; that is, the shutdown was within the last half of the current test interval. The functional test at time $t+\tau$ is therefore skipped, and the next test is scheduled at time $t+ 2\tau$.

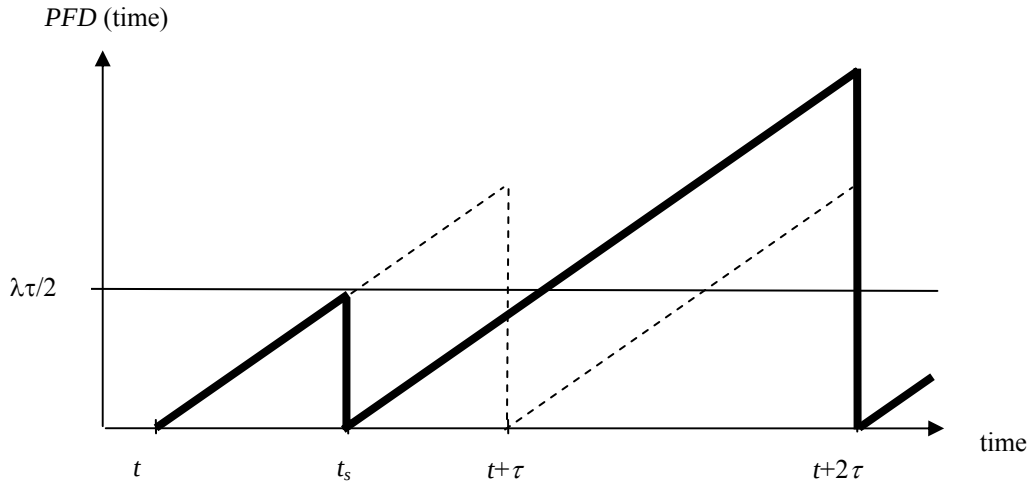

Figure F2: *PFD* as a function of time for the two cases "No shutdown" (dashed line) and "Shutdown followed by skipped test" (solid line).

We want to calculate the increase in *PFD* (averaged over the lifetime of the system) due to the skipped test. To do so, we make some simplifying assumptions:

- Skipping a functional test will increase the *PFD* only for the time period until the next functional test is performed (that is, in the period $[t+\tau, t+2\tau]$). When the average PFD is calculated (over the life-length of the installation), PFD over the limited period will contribute marginally. As a simplification we first calculate *PFD* over these two test intervals that are affected.
- If we have more than one shutdown within the period $[t, t+2\tau]$, this will contribute to reduce the (negative) effect of skipping a test. Thus, we make the simplifying assumption that there is *only one* shutdown inside the interval.

We can summarize these assumptions by saying that we have selected the most conservative demand rate. I.e., we consider the frequency of demands that gives the worst possible effect on the PFD when the next functional test is skipped.

Now, we can calculate the average *PFD* for the time interval $[t, t+2\tau]$, and find that the worst-case (that is, when the shutdown occurred exactly at the start of the interval with $t_s = \tau/2$) leads to $PFD = 5/4 \cdot \lambda_{DU}\ \tau/2$, that is, an increase in the PFD of 25%. The value when we average over t_s inside the interval $[t+\tau/2, t+\tau]$ gives an **average increase of 8.33% in PFD**. This is absolutely worst case. Note that if there for instance is only one demand within say 20 test intervals (rather than one demand in two intervals), the increase in the average PFD is only 0.8%.

Finally, one should notice that although these values show only a moderate increase in the average *PFD* when a test is skipped, there are some points in time when the *PFD* is higher than normal. If we only consider the last half of the second test interval (that is, $[t+1.5\tau, t+2\tau]$), then the average *PFD* in this interval is as high as $2.5 \cdot \lambda_{DU}\ \tau/2$. Whether this is acceptable or not must be decided for each case.

APPENDIX G

INDEPENDENCE BETWEEN SAFETY FUNCTIONS

CONTENT

G.1 Implementation of independence between systems

The PSA regulations[8], IEC 61508/61511[9] and ISO 10148[10] all include a requirement related to independence between systems. Such a requirement is mainly introduced as a defence against making several barriers vulnerable to one common event or cause, and to avoid negative effects from one function onto another. Dependencies where a failure most likely result in several functions going to a safe state (e.g. failure of common power), are not considered here.

The purpose of this section is to provide a guide for the interpretation and implementation of the independence requirement in practice. This is done by describing two types of solutions:

1. Solutions denoted as "*conditionally acceptable*"; i.e. the solution may be acceptable given that a number of *conditions* are fulfilled;
2. Solutions denoted as "*unacceptable*" that shall not be implemented.

The conditions for making solutions acceptable will include mechanisms that shall be implemented to avoid negative dependence between systems. Such mechanisms are usually realised as system software functions, and will as such be subject to the software quality requirements of IEC 61508.

The list of examples in this appendix is not exhaustive. Focus has been put upon solutions that are frequently discussed and which are relevant for implementation in the petroleum industry. Straightforward solutions, as e.g. a dedicated SIS which is physically separated from the PCS and does not exchange any data with it, are not considered.

Before going on to discuss conditionally acceptable and unacceptable solutions, the overall (preferred) basis for how systems should be interconnected is illustrated in Figure G.1 below.

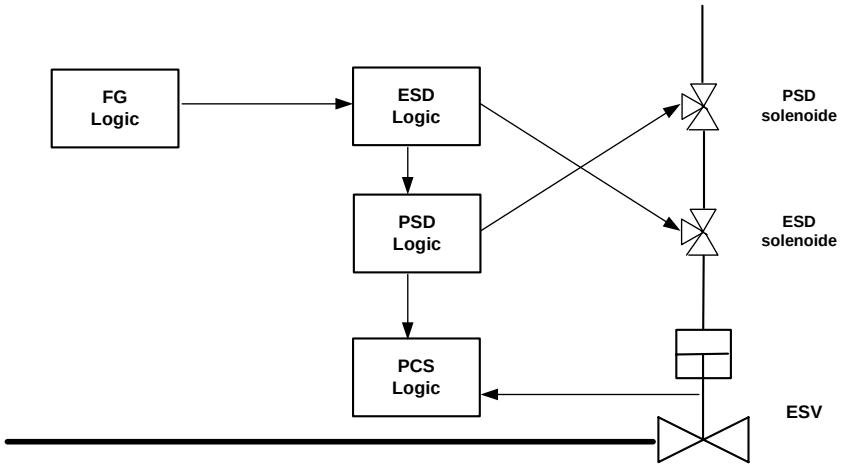

Figure G.1 Typical interconnection of systems

[8] PSA "Facility regulations", §§31, 32 and 33.

[9]
- IEC 61508-1, 7.5.2.4, d)
- IEC 61508-2, 7.4.2.3
- IEC 61508-4, 3.4.1, NOTE 3
- IEC 61511-1, 11.2.2
- IEC 61511-1, 11.2.4
- IEC 61511-1, 11.2.10
- IEC 61511-1, 11.7.1.5

[10] ISO 10418, 6.2.5, 6.2.9

In the figures in this Appendix, the arrowhead gives the direction of information flow. If unidirectional, no information or influence is allowed in the other direction.

G.2 Connection between systems

G.2.1 Conditionally acceptable solutions

G.2.1.1 Systems interconnected via a common main communications facility

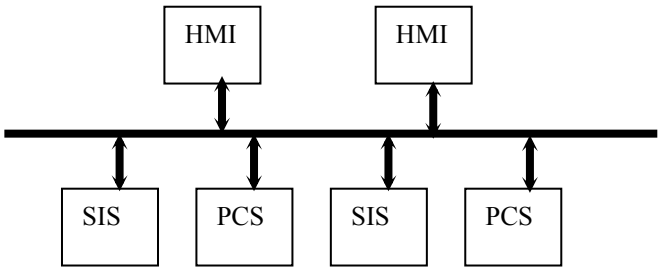

Figure G.2 Systems interconnection via a common communication facility

The VDU based HMIs have the physical capability of communicating with any SIS and any PCS.

This is a frequently used architecture, with e.g. a dual redundant Ethernet as the common main communications facility. For further requirements concerning communication, ref. IEC 61511-1, section 11.7.3.

Conditions:

- The safety instrumented function with the allocated safety integrity level, shall be realised within the SIS part of the system;
- All safety functions shall be designed and programmed to prevent them from failing as a consequence of any error/event/condition of data transport on the common main communications facility, including total loss of communication;
- The VDU based HMIs shall be equipped with a user authorisation system, restricting access to the safety functions;
- The VDU based HMIs shall be designed in a manner so that it is always evident to the operator whether he/she is currently accessing a safety or non-safety function;
- Dedicated safety system pictures shall be provided and shall be the only means of accessing the function of the SIF from the VDU based HMI (e.g. inhibitation, change of parameters, etc.);
- There shall be a dedicated Critical Action Panel (CAP), implemented independently from the common main communications facility and the instrumented systems[11]. The CAP shall encompass the action and display elements sufficient for safe operation in the absence of all VDU based HMI. See also NORSOK I-002, section 4.2.

Maintaining a sufficient degree of independence while using a common backbone bus for both SIS and PCS controllers can be achieved by providing evidence of the following features implemented in the SIS controllers:

- protection against network storms (or guaranteed trip to safe state)
- independency of network hang situations (or guaranteed trip to safe state)
- protection against faulty telegrams or wrong telegram addressing

[11] PSA “Facility regulation”, §32

G.3 Connections to external systems

The safety and process control systems will usually be interfaced to remote non-safety systems as well as to local external systems. If the SISs, PCSs and HMIs are interconnected via a common main communications facility (ref. previous section), then connecting remote and local external systems to the PCSs, will imply that these external systems are connected to the SISs, as well. For this reason, the solutions listed below do not distinguish between connecting external systems to the SISs or the PCSs.

An example of a remote system is an administrative database system. An example of a local external system is a local office PC network.

For the remainder of this section, the remote non-safety systems and the local external systems are collectively termed "external systems".

G.3.1 Conditionally acceptable solutions

Generally, the following means shall be implemented.

Conditions:

- mechanisms to prevent unauthorised access;
- mechanisms to control virus, worms, etc.;
- an approved strategy for securing the communication between safety and control system and external systems.

G.3.1.1 Connection to external systems via a Data Filtering Function

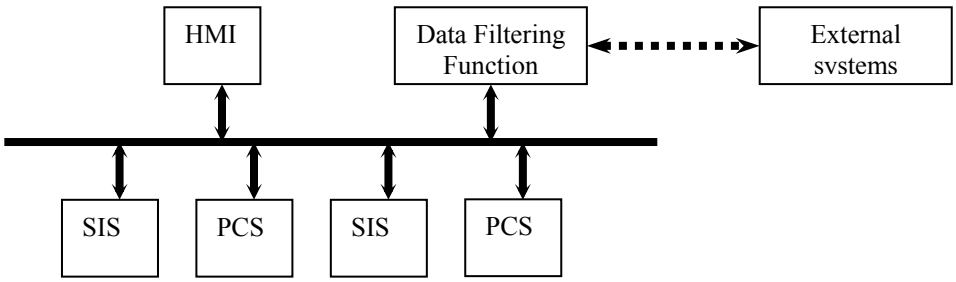

Figure G.3 Connection to external systems via a data filtering function

The Data Filtering Function may e.g. be an integrated Information Management System (IMS) or one or more PCS computers (nodes) and thus be part of the PCS.

Conditions:

- The Data Filtering Function shall be designed and programmed to stop all data from external systems from flowing directly onto the common main communications facility. The Data Filtering Function may however act on its own onto the common main communications facility as any PCS is allowed to do, e.g. executing transactions requested by external systems after evaluating the request.

G.3.2 Unacceptable solutions

G.3.2.1 Direct connection to external systems

The following solution shall not be implemented.

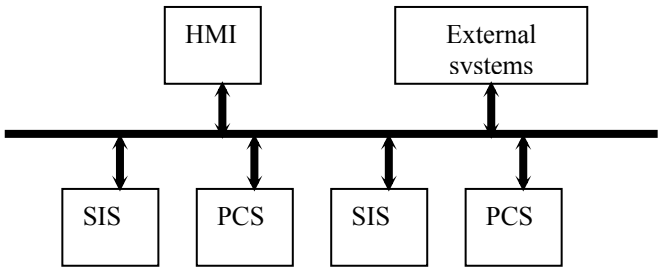

Figure G.4 Direct connection to external systems

G.4 Data flow between systems

The systems considered here is the following:

- Safety systems (SISs):
  - ESD (Emergency Shutdown System)
  - FGS (Fire and Gas System)
  - PSD (Process Shutdown System)
- Non-safety systems:
  - PCS (Process Control System)

Data flows considered are data flows between SISs and between a SIS and the PCS.

G.4.1 Conditionally acceptable solutions

G.4.1.1 Transmitting safety actions between SISs over a common communications facility

If safety demands are sent over the backbone network, the safety controller must be able to monitor the ability to transfer such demands and bring the SIF to a safe state:

- within the defined response-time for the SIF
- with a PFD-contribution not compromising the SIL of the complete safety function

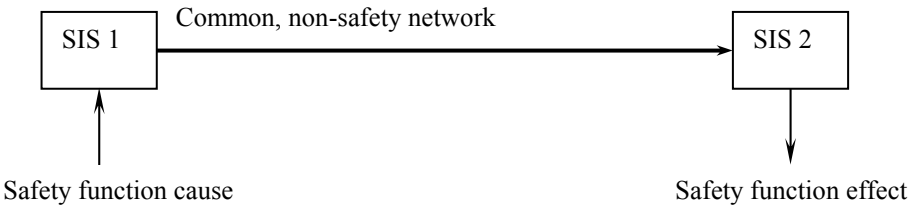

Figure G.5 Transmitting safety actions between SIS

The solution may be used for:

- ESD initiating PSD actions
- ESD initiating ignition source isolation by FGS
- FGS initiating ignition source isolation by ESD
- One PSD node initiating PSD actions by another PSD node

Reference is also made to “System interconnected via a common main communication facility” (ref. section G.2.1.1).

Conditions:

- Only end to end data address exchange shall be applied, i.e. no intermittent “intelligent” devices shall be used;
- The safety system communications protocol shall be implemented with fail-safe functionality.

The safety system protocol shall uncover:

- Random malfunctions (due to EMI impact on transmission channel);
- H/W faults;
- Systematic malfunction (transmission fault), H/W or S/W.

Hence, the protocol must cover the following types of faults:

• Data corruption	The telegram has upon arrival one or more faults compared to the sent telegram
• Time delay	The receiver is waiting too long for the telegram message to arrive
• Deleted telegram	Sent telegram is failing to arrive at intended recipient
• Repetition	The telegram is unintentionally received several times
• Inserted telegram	Telegram (interference) from other source is unintentionally received
• Re-sequenced telegram	Telegrams are received in wrong order
• FIFO failure	Addressing error
• Masquerade	Other type telegram is accepted as a safety telegram

G.4.1.2 Transmitting shutdown status (state) from PSD to PCS

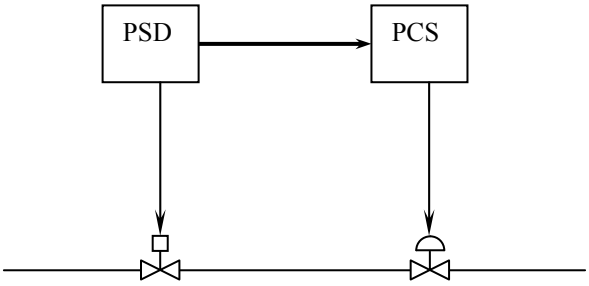

Figure G.6 Transmission of shutdown status from PSD to PCS

Such a solution may be used for:

- getting the PCS into a known state for easier start-up after shutdown
- control valve closure after PSD action
- initiation of machinery protection shutdown after PSD action

Conditions:

- Shall be designed and programmed so that no flow of data occur in the opposite direction, except for data as permitted by sections "Using PSD for performing control actions on request from PCS" (ref. section G.4.1.5) and "Using PSD to operate ESD valve automatically on request from PCS" (ref. section G.4.1.7).
- Reference is also made to “Systems interconnected via a common main communication facility” (ref. G.2.1.1), if such communication is applied.

G.4.1.3 Using PCS for operating ESD valves, with PCS solenoid and limit switches connected to PCS

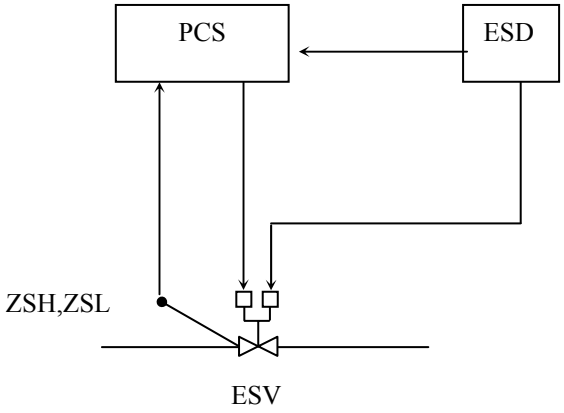

Figure G.7 Using PCS for operating ESD valves

This solution is typically used for operation of blow down valves during automatic gas purge/pressurisation sequences at process system start-up.

Conditions:

- The pneumatic/hydraulic/mechanical arrangement of the ESV shall be designed and built so that the ESD action is never prevented, i.e. to bring the ESV to the safe state.

G.4.1.4. Manual operation of PSD valves

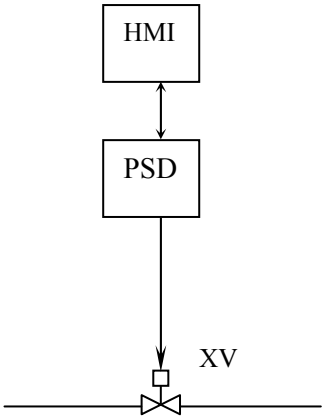

Figure G.8 Manual operation of PSD valves

Conditions:

- The PSD system shall be designed and programmed as to always prioritise bringing the valve to the safe state if process conditions dictate it, independent of whether the operator has requested opening or closure of the valve.
- Reference is also made to “Systems interconnected via a common main communication facility” (ref. G.2.1.1), if such communication is applied.

G.4.1.5 Using PSD for performing control actions on request from PCS

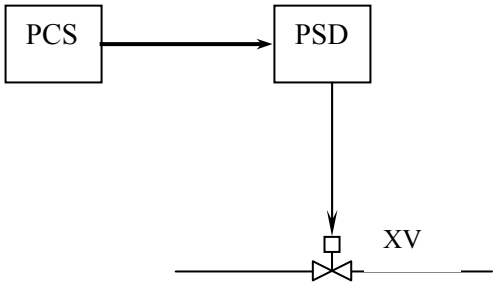

Figure G.9 Using PSD for performing control actions on request from PCS

This solution is typically used for automated PSD valve operations during process system start-up.

Conditions:

- The PSD functions operating the valve are totally independent of the PCS;
- The PSD system is designed and programmed as to always prioritise bringing the valve to the safe state if process conditions dictate it, independent of whether PCS has requested opening or closure of the valve;
- The proper allocation of functions has been made between PCS (e.g. machinery protection) and PSD (process safety); and, the need for the function has been critically evaluated; and, alternative solutions[12] have been explored;
- The architecture of the PSD system shall be such that any failure in the part handling PCS can not propagate to the part handling PSD and influence its PSD function;
- Shall not be used instead of implementing PSD functionality, i.e. shall not be used for a valve operation that would normally be a PSD action;
- Reference is also made to “Systems interconnected via a common main communication facility” (ref. G.2.1.1), if such communication is applied.

[12] E.g. Manual operation of the XV during start-up, or additional solenoid controlled from PCS

G.4.1.6 Manual operation of ESD valves via PSD, with PSD solenoid and limit switches connected to PSD

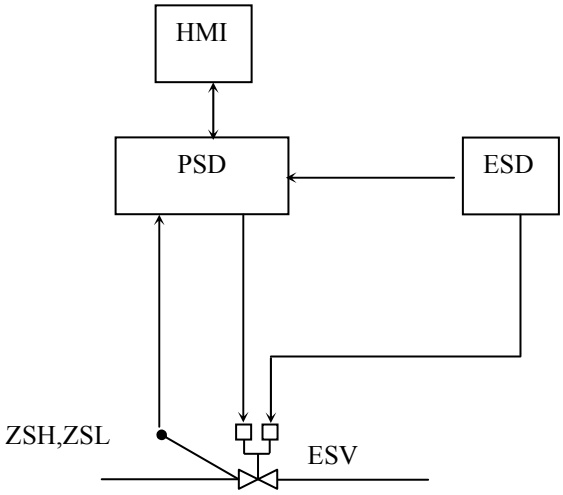

Figure G.10 Manual operation of ESV valves via PSD

Conditions:

- The PSD related arrangement of the ESV shall be designed and built such as to never prevent the ESD action, which is to bring the ESV to the safe state.
- The PSD system shall be designed and programmed as to always prioritise bringing the valve to the safe state if process conditions or an ESD command dictate it, independent of whether the operator has requested opening or closure of the valve.
- Shall not be used instead of implementing ESD or PSD functionality, i.e. shall not be used for a valve operation that would normally be an ESD or PSD action;
- Reference is also made to “Systems interconnected via a common main communication facility” (ref. G.2.1.1), if such communication is applied.

G.4.1.7 Using PSD to operate ESD valve automatically on request from PCS

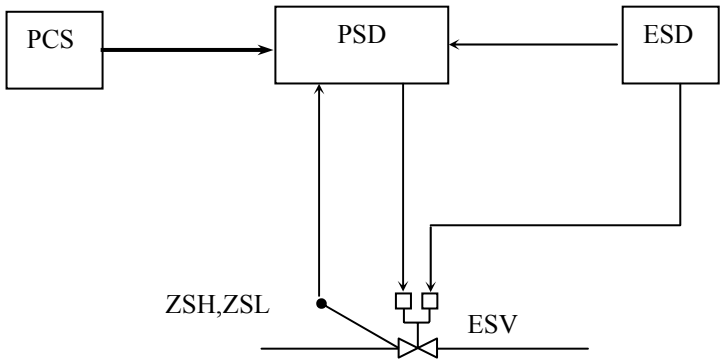

Figure G.11 Using PSD to operate ESD valve upon request from PCS

This solution is typically used for:

- operation of sectioning valves during automatic gas purge/pressurisation sequences at process system start-up;
- blowdown as part of machinery protection shutdown in PCS.

Conditions:

- All conditions in section G.4.1.5 and G.4.1.6 shall be fulfilled

G.4.1.8 Inhibit/override from common operator station

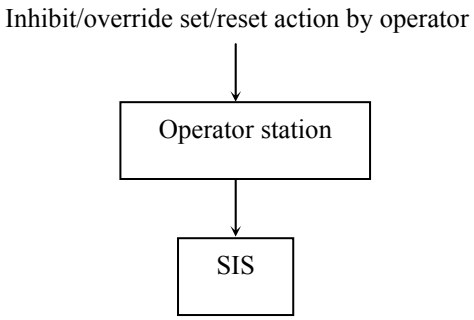

Figure G.12 Inhibit / override from common operator station

Conditions:

- Individual inhibits / overrides shall be logged and feedback status shall be available to the operator, i.e. via the VDU based HMI safety displays.
- The Critical Action Panel (CAP) shall have a global mechanism for easily resetting all currently active inhibits and overrides, covering all the SIS;
- Reference is also made to “Systems interconnected via a common main communication facility” (ref. G.2.1.1), if such communication is applied.

G.4.2 Unacceptable solutions

G.4.2.1 Suppressing PSD action from PCS

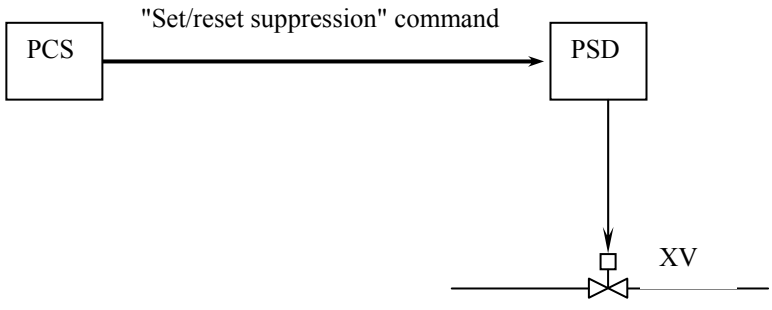

Figure G.13 Suppression of PDS action from PCS

In some cases this solution has been used in automated gas compression start-up sequences, in order to avoid PSD shutdown before reaching stable and normal process conditions.

This solution shall not be implemented, even though the duration of the suppression is limited by a timeout mechanism in PSD.

PSD shutdown upon leakage detection (PALL) on pump/compressor discharge line will in practice not function as a leakage detection and should thus preferably be removed or reclassified as a PCS signal, both cases handled as a deviation to ISO 10418. It may alternatively be permissible to set the action limit as low as to avoid shutdown when the pump/compressor is stopped (i.e. the action limit set below the settle-out pressure). See also Table 7.1 and Appendix A, section 3.5 for the use PALL as leakage detection.

G.4.2.2 Safety function being totally dependent on operator station

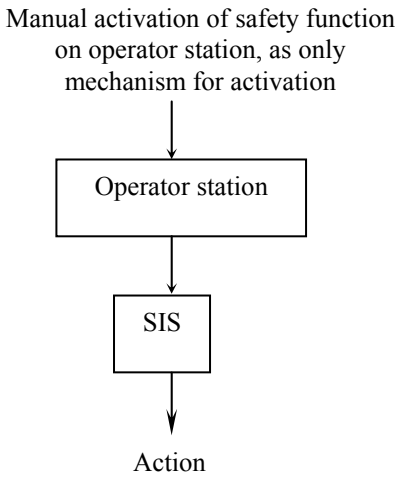

Figure G.14 Manual activation of safety function

This solution, i.e. manual activation via operator station only, shall not be implemented.

The necessary parallel activation mechanism may be implemented in the Critical Action Panel (CAP), see section "Systems interconnected via a common main communication facility" above (ref. G.2.1.1). There shall be a SIL requirement on such CAP functions, ref. Table 7.1 and Appendix A, section A.15.

G.4.2.3 Data transport from PSD to FGS

Solutions implying transport of data from PSD to FGS shall not be implemented.

G.4.2.4 Data transport from PSD to ESD

Solutions implying transport of data from PSD to ESD shall not be implemented.