RECOMMENDED GUIDELINES

FOR

THE APPLICATION OF
IEC 61508 AND IEC 61511
IN THE PETROLEUM
ACTIVITIES ON THE NORWEGIAN
CONTINENTAL SHELF

THE NORWEGIAN
OIL INDUSTRY ASSOCIATION
Table of content

FOREWORD.............................................................................................................................................................................. 5

1 INTRODUCTION........................................................................................................................................................................ 6

2 PURPOSE AND SCOPE.................................................................................................................................................................. 12

3 REFERENCES ............................................................................................................................................................................. 14

4 ABBREVIATIONS AND DEFINITIONS ................................................................................................................................... 15
  4.1 ABBREVIATIONS............................................................................................................................................................. 15
  4.2 DEFINITIONS..................................................................................................................................................................... 16

5 MANAGEMENT OF FUNCTIONAL SAFETY.................................................................................................................................. 18
  5.1 OBJECTIVE....................................................................................................................................................................... 18
  5.2 REQUIREMENTS............................................................................................................................................................. 18
    5.2.1 Competence ......................................................................................................................................................... 18
    5.2.2 Responsible Person .............................................................................................................................................. 18
    5.2.3 Planning ............................................................................................................................................................... 19
    5.2.4 Implementing and monitoring............................................................................................................................... 19
    5.2.5 Assessment, auditing and revisions....................................................................................................................... 19
  5.3 RELATIONSHIP TO ISO 13702 ...................................................................................................................................... 19

6 VERIFICATION, VALIDATION AND FUNCTIONAL SAFETY ASSESSMENT ............................................................................. 21
  6.1 INTRODUCTION............................................................................................................................................................. 21
  6.2 VERIFICATION ............................................................................................................................................................. 21
  6.3 VALIDATION ................................................................................................................................................................. 22
  6.4 FUNCTIONAL SAFETY ASSESSMENT .............................................................................................................................. 22

7 DEVELOPMENT AND ALLOCATION OF SIL REQUIREMENTS .............................................................................................. 23
  7.1 OBJECTIVE ...................................................................................................................................................................... 23
  7.2 APPROACH ....................................................................................................................................................................... 23
  7.3 DEFINITION OF EUC .................................................................................................................................................... 25
    7.3.1 Definition of EUC for local safety functions ........................................................................................................ 25
    7.3.2 Definition of EUC for global safety functions .................................................................................................... 25
  7.4 HAZARD AND RISK ANALYSIS .................................................................................................................................... 25
    7.4.1 Scope of hazard and risk analysis .......................................................................................................................... 25
    7.4.2 Hazard identification (HAZID) ............................................................................................................................. 26
    7.4.3 Required output from the HAZID .......................................................................................................................... 27
  7.5 DEFINITION OF SAFETY FUNCTIONS .......................................................................................................................... 27
    7.5.1 Scope ....................................................................................................................................................................... 27
    7.5.2 Requirements ......................................................................................................................................................... 27
  7.6 MINIMUM SIL REQUIREMENTS ...................................................................................................................................... 28
    7.6.1 Scope ....................................................................................................................................................................... 28
    7.6.2 Rationale for the minimum SIL requirement table .............................................................................................. 28
    7.6.3 Minimum SIL requirements table ............................................................................................................................ 28
  7.7 METHODOLOGY FOR HANDLING OF DEVIATIONS FROM THE MINIMUM SIL TABLE ..................................................... 31
    7.7.1 Identification of deviations ........................................................................................................................................ 31
    7.7.2 Required input for handling of deviations .............................................................................................................. 31
    7.7.3 Determination of SIL for safety function deviations ............................................................................................. 32
  7.8 ALLOCATION OF SAFETY FUNCTIONS .......................................................................................................................... 32
    7.8.1 Objectives ............................................................................................................................................................... 32
    7.8.2 Requirements ......................................................................................................................................................... 32
## SIS Design and Engineering

### 8.1 Objectives

- Specification of Safety Instrumented Systems
- Specification for non-instrumented Safety Systems
- Specification for Safety Instrumented Systems
- Specification for non-instrumented Safety Systems

### 8.2 Organisation and Resources

- Planning
- Input Requirements
- Implementation of Safety Functions
  - 8.5.1 SIS requirements
  - 8.5.2 Subsystem interface
  - 8.5.3 Field Sensor
  - 8.5.4 Logic Solver
  - 8.5.5 Final element
  - 8.5.6 Utilities
  - 8.5.7 Integration

### 8.3 Planning

- Testing, inspection, and maintenance
- Frequency of functional testing
- Functional testing procedures
- On-line functional testing
- Documentation of functional testing

### 8.4 Input Requirements

- Personnel and Competence
- Equipment and Resources
- Change procedures
- Acceptance test (FAT)
- Factory Acceptance Test (FAT)
- Documentation from Design Phase

### 8.5 Implementation of Safety Functions

- Specification for Safety Instrumented Systems
- Specification for non-instrumented Safety Systems

## SIS Installation, Commissioning and Validation

### 9.1 Objectives

- Safety requirements
- Subsystem interface
- Field Sensor
- Logic Solver
- Final element
- Utilities
- Integration

### 9.2 Personnel and Competence

- Installation and mechanical completion
- Mechanical completion
- SIS safety validation planning
- SIS safety validation

### 9.3 Requirements

- Installation and mechanical completion planning
- Installation
- SIS safety validation planning
- SIS safety validation

### 9.4 Documentation

- On-line functional testing
- Functional testing procedures
- Functional testing procedures
- Documentation of functional testing
- Revision and continuous improvement of procedures

## SIS Operation and Maintenance

### 10.1 Objective

- Testing, inspection, and maintenance
- Functional testing
- Frequency of functional testing
- Functional testing procedures
- On-line functional testing
- Documentation of functional testing
- Revision and continuous improvement of procedures

### 10.2 Requirements

- Competence and training of operators
- Overrides
- Handling of non-conformities and demands

### 10.3 Operations and Maintenance Procedures

- Change procedures
- Acceptance test (FAT)
- Factory Acceptance Test (FAT)
- Documentation from Design Phase

## SIS Modification

### 11.1 Objective of Management of Change (MOC)

- MOC Procedure
- MOC Documentation

## SIS Decommissioning

### 12.1 Objectives

- Requirements
APPENDIX A  BACKGROUND FOR MINIMUM SIL REQUIREMENTS
APPENDIX B  EXAMPLES ON HOW TO DEFINE EUC
APPENDIX C  EXAMPLES ON HOW TO HANDLE DEVIATIONS
APPENDIX D  ESTIMATION OF PROBABILITY OF FAILURE ON DEMAND
APPENDIX E  LIFECYCLE PHASES FOR A TYPICAL OFFSHORE PROJECT
APPENDIX F  COLLECTION AND ANALYSIS OF RELIABILITY DATA
Foreword

This guideline has been developed as a joint industry project between operators and the various suppliers of services and equipment with the financial support of OLF.

This guideline can be found on http://www.itk.ntnu.no/sil. There also a mail-list for discussion of the guideline is found, together with some additional information.

The text in the main body of the guideline is to be considered as normative, whereas NOTES, clarifying examples and the Appendices are for information only.

This is the first official version of the guideline. Based on experience with the guideline and feedback from the users, an update of the guideline is planned towards the end of 2001 / beginning of 2002.

Attention is drawn to the fact that this document uses some terms, such as “shall”, which is rather “unconventional” in a guideline text (unless when referring directly to the standards). However, the reason for the selected wording is that the future status and type of the document is still somewhat unclear, although an expressed goal has been eventually to convert it into a standard.
1 Introduction

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 been difficult to handle as part of a development project, as it requires extensive additional analysis, and since requirements to safety functions can normally not be obtained directly from the Quantitative Risk Analysis (QRA) as it is performed today.

The Norwegian Petroleum Directorate (NPD) has in their forthcoming regulations recommended the use of IEC 61508 for defining the performance level for safety functions. A need for developing guidelines on how to use this standard has therefore evolved.

Whereas IEC 61508 is a generic standard common to several industries, the process industry is currently developing their own sector specific standard for application of SIS. This standard, IEC 61511, is available in draft version and has been extensively referred to in the present guideline. However, as indicated in Figure 1.1 below, the manufacturers and suppliers also have to relate to IEC 61508. Hence, references to both standards are given throughout this guideline.

Figure 1.1 Relationship between IEC 61511 & IEC 61508 (Figure 2a from IEC 61511-1)

In Figure 1.2, the references to the two different standards are further detailed and grouped on hardware and software development.

---

1 The standard IEC 61511; “Functional safety: Safety Instrumented Systems for the process industry sector”, is currently available in CDV version, dated 26-05-2000
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 given in Figure 1.3. References to relevant chapters in this guideline are included in the figure.

For the purpose of completeness, the lifecycle from IEC 61508 is also given in Figure 1.4.
Figure 1.3 Lifecycle from IEC 61511 (ref. Figure 8 from IEC 61511-1), with reference to relevant chapters in this guideline

Legend:

Typical direction of information flow

No detailed requirements given in IEC 61511

Requirements given in IEC 61511

NOTE:
1. Stage 1 through 5 inclusive defined in IEC 61511-1, subclause 5.2.6.1.3
Figure 1.4  Lifecycle from IEC 61508 (ref. Figure 2 from IEC 61508-1)

The requirement clauses of IEC 61511 relevant for each lifecycle phase are given in Table 1.1, together with the input/output specification for each phase.
Table 1.1 – SIS safety lifecycle overview (ref. Table 2 from IEC 61511-1)

<table>
<thead>
<tr>
<th>Safety lifecycle phase or activity</th>
<th>Title</th>
<th>Objectives</th>
<th>Requirements (Subclause in IEC 61511-1)</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Risk Analysis and Protection Layer Design</td>
<td>To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event, the requirements for risk reduction and the safety instrumented functions required to achieve the necessary risk reduction</td>
<td>8 Process design, layout, manning arrangements</td>
<td>A description of the required safety instrumented function(s) and associated safety integrity requirements</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Allocation of safety functions to protection layers</td>
<td>Allocation of safety functions to protection layers and for each safety instrumented function; determine the associated safety integrity level</td>
<td>9 A description of the required safety instrumented function(s) and associated safety integrity requirements</td>
<td>Description of allocation of safety requirements (see sub-clause 9).</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>SIS safety requirements specification</td>
<td>To specify the requirements for each SIS, in terms of the required safety instrumented functions and their associated safety integrity, in order to achieve the required functional safety.</td>
<td>10 Description of allocation of safety requirements (see sub-clause 9).</td>
<td>SIS safety requirements; Software safety requirements.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>SIS design &amp; engineering</td>
<td>To design the SIS to meet the requirements for safety instrumented functions and safety integrity.</td>
<td>11 &amp; 12.4 SIS safety requirements. Software safety requirements.</td>
<td>Design of the SIS in conformance with the SIS safety requirements; Planning for the SIS integration test.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>SIS installation commissioning &amp; validation</td>
<td>To integrate and test the SIS. To validate that the SIS meets, in all respects the requirements for safety in terms of the required safety instrumented functions and the required safety integrity.</td>
<td>12.3, 14.1, 14.2, 14.3 SIS design; SIS integration test plan. SIS safety requirements. Plan for the safety validation of the SIS.</td>
<td>Fully functioning SIS in conformance with the SIS design results of SIS integration tests. Safety validation of the SIS. SIS validation planning.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>SIS operation and maintenance</td>
<td>To ensure that the functional safety of the SIS is maintained during operation and</td>
<td>15 SIS requirements; SIS design. SIS operation and maintenance.</td>
<td>SIS operation and maintenance.</td>
<td></td>
</tr>
<tr>
<td>Safety lifecycle phase or activity</td>
<td>Title</td>
<td>Objectives</td>
<td>Requirements (Subclause in IEC 61511-1)</td>
<td>Inputs</td>
<td>Outputs</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------</td>
<td>------------</td>
<td>----------------------------------------</td>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>7 SIS modification</td>
<td></td>
<td>To make corrections, enhancements or adaptations to the SIS, ensuring that the required safety integrity level is achieved and maintained.</td>
<td>15.4 Revised SIS safety requirements.</td>
<td></td>
<td>Results of SIS modification.</td>
</tr>
<tr>
<td>8 De-commissioning</td>
<td></td>
<td>To ensure proper review, sector organisation, and ensure SIF remain appropriate.</td>
<td>16 As-built safety requirements and process information</td>
<td></td>
<td>SIS placed out-of-service.</td>
</tr>
<tr>
<td>9 SIS verification</td>
<td></td>
<td>To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase.</td>
<td>7, 12.7 Plan for the verification of the SIS for each phase.</td>
<td></td>
<td>Results of the verification of the SIS for each phase.</td>
</tr>
<tr>
<td>10 SIS functional safety assessment</td>
<td></td>
<td>To investigate and arrive at a judgement on the functional safety achieved by the SIS.</td>
<td>5 Planning for SIS functional safety assessment. SIS safety requirement.</td>
<td></td>
<td>Results of SIS functional safety assessment.</td>
</tr>
</tbody>
</table>
2 Purpose and scope

In most situations, safety is achieved by a combination of safety-related systems depending on different technologies (e.g. electrical, electronic, programmable electronic, mechanical, hydraulic, pneumatic, etc.). Hence, an overall safety strategy must take into consideration all the safety-related systems in order to ensure that the risk is reduced to an acceptable level. This is illustrated in Figure 2.1 below.

![Framework for risk reduction](image)

**Figure 2.1 Framework for risk reduction (ref. Figure A.1 in IEC 61508-5)**

Within this overall framework, IEC 61508 and IEC 61511 are concerned with the Safety Instrumented Systems (SIS). The purpose of this guideline is to simplify the application of these standards for use in the petroleum activities on the Norwegian Continental Shelf, in order to meet the NPD requirements.

Whereas IEC 61508 and IEC 61511 describe a fully risk based approach for determining Safety Integrity Levels (SIL), this guideline provides a table with minimum SIL requirements which shall be adhered to whenever possible. The requirements are based on experience, with a design practice that has resulted in a safety level considered adequate. Further rationale behind this approach is described in chapter 7 of this guideline.

The minimum SIL table provides requirements to common safety functions. Deviations from these requirements may, however, be identified, and in such case a methodology according to IEC 61508 should be applied. Handling of deviations is further described in section 7.7.

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 predictability of behaviour during fault conditions (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, and modification of SIS. Management of functional safety is also discussed.
Process safety functions are defined in ISO 10418 (API RP 14C), whereas global functions like ESD and F&G are defined by the NPD regulations. The systems to implement the various safety functions are described in relevant NPD regulations and in NORSOK standards.

The NPD regulations are not retroactive with respect to older installations designed and constructed in accordance with earlier standards. Hence, there is no statutory requirement to follow this guideline for such installations. However, in connection with significant modifications influencing the instrumented safety systems, the need for upgrading the existing safety requirement specification should be carefully considered. Alternatively, a new specification should be generated in accordance with IEC 61508.

In general, this guideline applies to all instrumented safety functions as defined by NPD and NORSOK. The present version, however, focuses on processing facilities on offshore installations, although the principles outlined in the guideline have general applicability also to drilling facilities, marine systems and onshore terminals. Table 2.1 provides a list of the functions covered explicitly in this guideline.

**Table 2.1 Safety functions covered explicitly in this guideline**

<table>
<thead>
<tr>
<th>Process protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process segregation / sectionalisation</td>
</tr>
<tr>
<td>Depressurisation (blow down)</td>
</tr>
<tr>
<td>Isolation of wells (with all three production barriers available)</td>
</tr>
<tr>
<td>Isolation of risers</td>
</tr>
<tr>
<td>Fire detection</td>
</tr>
<tr>
<td>Gas detection</td>
</tr>
<tr>
<td>Electrical isolation</td>
</tr>
<tr>
<td>Deluge (incl. fire pumps)</td>
</tr>
</tbody>
</table>

In a future version of the guideline it will be considered to include drilling systems as well as marine systems.

Requirements and guidance are given only concerning personnel safety. Environmental and asset protection is not focused, although several of the requirements, such as e.g. isolation towards well and pipeline, will be equally important for these aspects.
3 References

Of the references found below some are referred to in this document, and some are listed just for information. Where references are given in the body of the document to a standard or a specific paragraph of a standard, this is regarded as normative references, unless explicitly noted.

NORSOK standards, which are normative references, are found on http://www.nts.no/norsok/

Table 3.1 Table of references

<table>
<thead>
<tr>
<th>Document id.</th>
<th>Document title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 61511-1, version CDV 26/5/2000</td>
<td>Functional safety: Safety Instrumented Systems for the process industry sector -</td>
</tr>
<tr>
<td></td>
<td>Part 1: Framework, definitions, system, hardware and software requirements</td>
</tr>
<tr>
<td>IEC 61508, Edition 1.0</td>
<td>Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems -</td>
</tr>
<tr>
<td>Part 1, December 1998</td>
<td>Part 1: General requirements</td>
</tr>
<tr>
<td>Part 2, May 2000</td>
<td>Part 2: Requirements for E/E/PE Safety Related Systems</td>
</tr>
<tr>
<td>Part 3, December 1998</td>
<td>Part 3: Software requirements</td>
</tr>
<tr>
<td>Part 4, December 1998</td>
<td>Part 4: Definitions and abbreviations</td>
</tr>
<tr>
<td>Part 5, December 1998</td>
<td>Part 5: Examples of methods for determination of SIL</td>
</tr>
<tr>
<td>Part 6, April 2000</td>
<td>Part 6: Guidelines on the application of IEC 61508-2 and 61508-3</td>
</tr>
<tr>
<td>Part 7, March 2000</td>
<td>Part 7: Overview of techniques and measures</td>
</tr>
<tr>
<td>ISO/WD 10418, 07/05/1999, Rev. 4</td>
<td>Petroleum and natural gas industries - Offshore production installations – Analysis, design, installation and testing of basic surface safety systems for offshore installations – Requirements and guidelines</td>
</tr>
<tr>
<td>ISO 13702, 1999</td>
<td>Petroleum and gas industries - Control and mitigation of fires on offshore production installations – Requirements and guidelines</td>
</tr>
<tr>
<td>ANSI/ISA-S84.01 – 1996, approved 15/03/1997</td>
<td>Application of Safety Instrumented Systems for the Process Industries</td>
</tr>
<tr>
<td>Published by the OREDATA participants, 1997</td>
<td>Offshore Reliability Data Handbook - third Edition</td>
</tr>
<tr>
<td>UKOOA, November 1999, Issues No 2</td>
<td>Guidelines for Instrumented-Based Protective Systems</td>
</tr>
<tr>
<td>CCPS / AIChE, 1993</td>
<td>Guidelines for Safe Automation of Chemical Processes</td>
</tr>
<tr>
<td>CCPS / AIChE, 1994</td>
<td>Guidelines for Preventing Human Error in Process Safety</td>
</tr>
<tr>
<td>STF75 A93060, 15/03/1994</td>
<td>Human Dependability Methods for Control and Safety Systems</td>
</tr>
<tr>
<td>API RP 14C, March 1998, 6th Ed.</td>
<td>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)</td>
</tr>
</tbody>
</table>
4 Abbreviations and definitions

4.1 Abbreviations

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

AEMA - Action Error Mode Analysis
CPU - Central Processing Unit
DHSV - Downhole Safety Valve
EERS - Evacuation, Escape and Rescue Strategy
ESD - Emergency Shut down
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
HIPPS - High Integrity Pressure Protection System
HSE - Health, Safety and Environment
I/O - Input/Output
MOC - Management of Change
MooN - M out of N
NDE - Normally De-energised
NE - Normally Energised
NPD - Norwegian Petroleum Directorate
PFD - Probability of Failure on Demand
PSD - Process Shut down
PSV - Process Safety Valve
QA - Quality Assurance
QRA - Quantitative Risk analysis
SAT - Safety Analysis Table
SFF - Safe Failure Fraction
SIL - Safety Integrity Level
SIS - Safety Instrumented System
SRS - Safety Requirement Specification
TIF - Test Independent Failure
UPS - Uninterrupted Power Supply

For other abbreviations see also IEC 61511-1

NOTE: The term “VOTING” in this guideline 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 guideline.

Deviation

In this guideline 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 blowdown.

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/FDIS 9000)

NOTE: As opposed to “deviations”, non-conformities are a result of mistakes, i.e. they are revealed after the relevant activities are executed.

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/FDIS 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/FDIS 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. Figure 1.3 shows the relationship between management of functional safety and the phases of the safety lifecycle.

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 is 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 NPD 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 include:
• Ensuring that operations and maintenance procedures as defined in chapter 10 are available and used as intended. In particular, that appropriate records are maintained with respect to test results, maintenance activities, system failures, and demand rate on the system;
• Ensuring that the competency of operators, maintenance technicians and engineers who work with or on the system is adequate;
• Control of access to the system including the use of keys and passwords;
• Ensuring that the 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 Implementing and monitoring
Procedures shall be developed and implemented to ensure the expedition, follow up and resolution of recommendations relating to the SIS that arise from:
• Hazard analysis and risk assessment;
• Assessment activities;
• Verification activities;
• Validation activities.

5.2.5 Assessment, auditing and revisions
In accordance with the NPD 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 should include the necessary technical and operational expertise for the particular installation.

5.3 Relationship to ISO 13702

The forthcoming NPD regulations introduce the use of ISO 13702 (“Control and mitigation of fires and explosions on offshore installations”), and a corresponding requirement for developing a Fire and Explosion Strategy (FES) and an Evacuation, Escape and Rescue Strategy (EERS) for documentation of safety. Consequently, it is important that the Safety Requirement Specification (ref. section 7.9) is compatible with the FES and the EERS documents and with other relevant documentation resulting from the use of ISO 13702 and the NPD regulations.

Figure 5.1 indicates the relationship between ISO 13702 / NPD regulations and IEC 61508/61511 with respect to some of the documentation produced.
Figure 5.1 Relationship between documentation
6 Verification, Validation and Functional Safety Assessment

6.1 Introduction

ISO/NPD 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 6.2 – 6.4.

![Figure 6.1 Interpretation of the relationship between verification, validation and functional safety assessment according to ISO and IEC, respectively](image)

6.2 Verification

In this guideline 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.

When the installation is in operation, the SIS safety functions shall undergo SIL-verifications at predefined intervals to ensure that the integrity level is maintained and the system is operating according to the specification.
The results of the verification process shall be properly documented and available upon request.

### 6.3 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 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 section 9.3 of this guideline.

### 6.4 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. “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. The factors influencing this decision are likely to include:

- the size of the project;
- the degree of complexity,
- the safety integrity levels;
- the duration of the project;
- the consequences in the event of failure,
- the degree of standardisation of design features.
7 Development and allocation of SIL requirements

7.1 Objective

The overall objective of this chapter is to describe a methodology for determining and allocating 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;
- how to develop the specification for the overall safety requirements and perform SIL allocation between the various safety functions.

7.2 Approach

This guideline 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 and allocating SIL requirements as described in this chapter. This covers the lifecycle phases as represented by box 1-3 in Figure 1.3, or box 1–5 in Figure 1.4.
ACTIVITY

EUC definition

Hazard and risk analysis

Definition of safety functions

Apply table with recommended SIL requirements

Have safety functions for which SIL table is not applicable been identified?

YES

For each identified deviation: Apply risk based methodology for SIL determination

NO

Perform SIL allocation

Develop safety functions requirements specification

Provide input to SIS design and engineering

Ref. to IEC and/or relevant section of this guideline

IEC 61508-1: 7.2, 7.3
IEC 61511-1: NA
This Guideline: 7.3

IEC 61508-1: 7.4
IEC 61511-1: 8
This Guideline: 7.4

IEC 61508-1: 7.5
IEC 61511-1: 10
This Guideline: 7.5

IEC 61508: NA
IEC 61511: NA
This Guideline: 7.6

IEC 61508-1: 7.6
IEC 61511-1: 9
This Guideline: 7.7

IEC 61508-1: 7.5
IEC 61511-1: 10
This Guideline: 7.9

Figure 7.1 Flowchart – SIL development and allocation in this guideline
7.3 Definition of EUC

The purpose of this activity is to achieve a thorough understanding of the equipment under control (EUC), i.e., the equipment to be protected by the SIS, the other technology safety systems and the external risk reducing measures. This includes a concise definition of the boundaries for the EUC and the EUC control system.

IEC 61508 does not give any particular requirements as to how the EUC should be defined. Hence, it is entirely within the hands of 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.

On an offshore installation, the EUC will usually be defined as the equipment to be protected by the SIS or as a defined area on the installation. This will, however, depend on the type of safety function considered, and the further discussion of EUC definition is therefore split between local and global safety functions (for definitions see section 4.2).

7.3.1 Definition of EUC for local safety functions

Local safety functions are usually executed by the PSD system and PSVs, which safeguard the process against undesirable events.

The EUC should, according to ISO 10418 methodology, be defined as a process unit including piping and valves. In order to utilise the actions of the PSD system, the EUC boundaries should be defined in terms of the (PSD) sectionalising valves, or according to the pressure class breaks.

The EUC control system is according to IEC 61508 separate and distinct from the EUC (ref. IEC 61508-4, sub-clause 3.2.3).

An example on how to define EUC for local safety functions is given in Appendix B.1.

7.3.2 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 EUC for global safety functions should be defined as one or several fire areas on an offshore installation. The boundary for the EUC will typically consist of emergency shutdown valves and/or physical walls. A fire area can consist of several ESD segments, which again can consist of one or more blowdown segments. For some critical functions, the whole installation could be considered as the EUC.

Examples on how to define EUC for global safety functions are given in Appendix B.2.

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;

It should be noted that whereas IEC 61508 refers to EUC (Equipment Under Control), IEC 61511 refers to “Process”.
• 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, this guideline provides a table with minimum SIL requirements for determination of integrity levels for “standard” safety functions. 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.

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 in 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.

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”.

Relevant techniques for hazard identification will be:

• review of relevant codes and standards;
• use of checklists (ref. Annex C and D of ISO/DIS 17776);
• ISO 10418 analysis (SAT analysis)
• HAZOP
• FMEA/FMECA
• different task analysis techniques combined with Action Error Mode Analysis (AEMA), for identification of human errors (see e.g. STF75 A9306; “Human Dependability Methods for Control and Safety Systems”)

For an EUC defined in terms of local safety functions (ref. section 7.3.1), HAZOP combined with SAT analysis have proved suitable techniques for identifying potential process related hazards on offshore installations.

For an EUC defined in terms of global safety functions (ref. section 7.3.2), the hazard identification performed as part of the QRA provides a good starting point for analysis. It should, however, be kept in mind that QRA normally focuses on “post-leakage” events, and further that certain hazards might be excluded due to low historical frequencies or limited consequence potential.
As mentioned above, the HAZID will be an important tool in order to reveal hazards that require safety functions and/or integrity levels other than those given in the minimum SIL table (ref. Table 7.1). Applying the techniques listed above does not, however, give any guarantee as to whether all such “deviations” are identified. Furthermore, the listed techniques are more suitable for pinpointing particular problem areas than for coming up with alternative requirements. The issue of identifying deviations from the minimum SIL table is further discussed in section 7.7.

7.4.3 Required output from the HAZID

The HAZID must be properly documented in terms of:

- personnel participating and their background;
- method(s) applied;
- description of hazards revealed and factors contributing to them;
- operational modes / type of operations covered;
- documentation for why hazards have been excluded or not taken into consideration;
- assumptions made, including the influences from human factors;
- any follow-up actions from the HAZID.

For hazards requiring safety functions and/or integrity levels other than those described in Table 7.1, additional output from the risk analysis will be required as described in section 7.7.

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 with the minimum SIL table.

The allocation of the safety functions to different protection layers, i.e. to SIS, other safety-related systems and external risk reducing measures, is further described in section 7.8.

7.5.2 Requirements

For process safety design following an ISO 10418 analysis, the safety functions will be defined through the safety analysis tables documenting the analysis (example for overpressure of equipment: PSHH/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 given from the NPD regulations (ref. “Innretningsforskriften”) 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. NS-EN 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 is included. For functions requiring energy to operate, it is essential that the energy source is included as part of the safety function. E.g. if a valve is depending upon hydraulic supply to perform its intended function (two-ways, non fail-safe), then the safety function must include the hydraulic supply system.
7.6 **Minimum SIL requirements**

7.6.1 **Scope**

The objective of this section is to

- Discuss why a table of minimum SIL requirements has been provided;
- Present the table of minimum SIL requirements including definitions of the safety functions included in the table;

7.6.2 **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 will in particular apply for local 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 local safety 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 will 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 come up with a list of minimum safety integrity levels for the most common safety functions. The SIL requirements given in this list 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 calculations for more or less “standard solutions” and will ensure a minimum level of safety. Another advantage of using pre-determined SILs 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.

7.6.3 **Minimum SIL requirements table**

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 hanging in the balance between two SIL classes, generally the stricter SIL requirement has been chosen. This is also in line with the NPD requirement for continues improvement.

For several safety functions it has been difficult to establish generic definitions. Due to process specific conditions, size of fire area, 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 an entire 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. As discussed above, 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 not the only requirements that must be fulfilled in order to ensure compliance with IEC 61508/61511 and this guideline. As discussed in other parts of this guideline, management of functional safety, architectural constraints on hardware safety integrity and control and avoidance of systematic faults are other important aspects to be considered.
For more detailed definitions of the safety functions and background information on the minimum SIL requirements, reference is made to Appendix A.

Table 7.1  Minimum SIL requirements - local safety functions

<table>
<thead>
<tr>
<th>Safety function</th>
<th>SIL</th>
<th>Functional boundaries for given SIL requirement / comments</th>
<th>Ref. APP. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process segregation (through PSD)</td>
<td>1</td>
<td>The SIL requirement applies to the whole PSD function as defined in Appendix A.3.1.</td>
<td>A.3.1</td>
</tr>
<tr>
<td>(closure of several valves)</td>
<td></td>
<td>The function starts where the signal is generated and ends and includes all valves necessary to effectuate the actual segregation of the process equipment or section.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: The sensor element has not been included due to problems with giving a generic definition. However, including the initiator should generally not jeopardise the SIL 1 requirement (except PALL, see below).</td>
<td></td>
</tr>
<tr>
<td>PSD functions:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAHH</td>
<td>2</td>
<td>The SIL requirement applies to closure of the critical valve through the PSD system as defined in Appendix A.3.2.</td>
<td>A.3.2</td>
</tr>
<tr>
<td>LAHH</td>
<td></td>
<td>The function starts with (and includes) the process sensor and terminates with closing of the critical valve.</td>
<td></td>
</tr>
<tr>
<td>LALL</td>
<td></td>
<td>Note: The given requirement for PAHH and LAHH assumes that there is one common inlet line to the considered process equipment. In case of several inlet lines and hence several valves to close, a separate evaluation of required SIL should be performed.</td>
<td></td>
</tr>
<tr>
<td>(closure of one critical valve)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSD function: LAHH on flare KO drum</td>
<td>2</td>
<td>The SIL requirement applies to the whole PSD function as defined in Appendix A.3.3.</td>
<td>A.3.3</td>
</tr>
<tr>
<td>(detection and transfer of shutdown signal)</td>
<td></td>
<td>The function starts with (and includes) the process sensor and terminates at the unit(s) intended to perform the action (see Note 2 below).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note 1: When implemented in both the PSD and ESD system, this combined function can obtain SIL 3.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note 2: The final element(s) have not been included since a generic definition of this function has been impossible to give.</td>
<td></td>
</tr>
<tr>
<td>PSD function: TAHH/TALL</td>
<td>2</td>
<td>The SIL requirement applies to closure of the critical valve through the PSD system as defined in Appendix A.3.4.</td>
<td>A.3.4</td>
</tr>
<tr>
<td>(closure of one critical valve)</td>
<td></td>
<td>The function starts with (and includes) the temperature sensor and terminates with closing of the critical valve.</td>
<td></td>
</tr>
<tr>
<td>PSD function: PALL</td>
<td>NA</td>
<td>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 escalation is minimised.</td>
<td>A.3.5</td>
</tr>
<tr>
<td>(primary protection against leakage)</td>
<td></td>
<td>Note: 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).</td>
<td></td>
</tr>
</tbody>
</table>
Table 7.1 cont.  Minimum SIL requirements - global safety functions

<table>
<thead>
<tr>
<th>Safety function</th>
<th>SIL</th>
<th>Functional boundaries for given SIL requirement / comments</th>
<th>Ref. APP. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESD sectionalisation</td>
<td>2</td>
<td>The SIL requirement applies to the sub-function needed for closure of one ESD valve, i.e: - ESD-node - ESD valve including solenoide(s) and actuator</td>
<td>A.4</td>
</tr>
<tr>
<td>(closure of one ESD valve)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Depressurisation (blow down)</td>
<td>2</td>
<td>The SIL requirement applies to the sub-function needed for opening of one blowdown valve, i.e: - ESD-node - Blowdown valve including solenoide(s) and actuator</td>
<td>A.5</td>
</tr>
<tr>
<td>(opening of one blowdown valve)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Isolation of well;</td>
<td>3</td>
<td>The SIL requirement applies to the sub-function needed for isolation of one well, i.e: - ESD-node (wellhead control panel) - Wing valve (WV) and master valve (MV) including solenoide(s) and actuators - Downhole safety valve (DHSV) including solenoide(s) and actuator</td>
<td>A.6</td>
</tr>
<tr>
<td>(shut in of one well)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Isolation of riser;</td>
<td>2</td>
<td>The SIL requirement applies to the sub-function needed for isolation of one riser/flowline, i.e: - ESD-node - ESD valve including solenoide(s) and actuator</td>
<td>A.7</td>
</tr>
<tr>
<td>(shut in of one riser)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fire detection;</td>
<td>2</td>
<td>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&amp;G node</td>
<td>A.8</td>
</tr>
<tr>
<td>(alarm signal generated, processed and action signals transmitted)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gas detection;</td>
<td>2</td>
<td>The SIL requirement applies to the sub-function needed for gas detection, given exposure of one detector, i.e.: - Gas detector - F&amp;G node</td>
<td>A.9</td>
</tr>
<tr>
<td>(alarm signal generated, processed and action signals transmitted)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electrical isolation;</td>
<td>2</td>
<td>The SIL requirement applies to the sub-function needed for electrical isolation given signal from F&amp;G/ESD node, i.e.: - F&amp;G node - Circuit breakers</td>
<td>A.10</td>
</tr>
<tr>
<td>(signal giving action processed in F&amp;G logic and electrical ignition sources removed)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deluge;</td>
<td>2</td>
<td>The SIL requirement applies to the sub-function needed for opening of one deluge valve, given confirmed fire or gas, i.e: - F&amp;G node - Fire water pumps - One deluge valve</td>
<td>A.11</td>
</tr>
<tr>
<td>(fire water demand signal processed in Fire &amp; Gas logic, start of fire pump, and opening of deluge-valve)</td>
<td></td>
<td>The function is considered successful when a certain amount of water (l/min) flows through the deluge valve.</td>
<td></td>
</tr>
</tbody>
</table>

Risk reduction requiring a SIL 4 function should not be implemented. Rather, this should prompt a redistribution of required risk reduction across other measures.
7.7 Methodology for handling of deviations from the minimum SIL table

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 on an offshore production installation. However, deviations from this table will occur and must be identified and treated according to a risk based methodology.

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 the minimum SIL table. Such deviations may result from hazards requiring instrumented safety functions other than what is defined as conventional design according to ISO 10418, other relevant standards or what is described in the NPD regulations. 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\(^3\) 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 will according to ISO terms 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.

With respect to “integrity deviations”, the QRA will, as discussed in section 7.6.3, to some extent verify whether the chosen integrity levels is 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:

\(^3\) 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 description of the EUC and its control system (from section 7.3);
• a description of the hazardous event(s) causing the required 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 criteria must be defined in order to determine the required risk reduction. Such a risk acceptance criteria would normally be defined by the operator himself. In addition, NPD has in their forthcoming regulations (ref. “Innretningsforskriften”, §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 at present has a limited number of examples). The examples include:

• A quantitative method for establishing SIL requirements for HIPPS system (ref. Appendix C, example 1);
• Quantitative risk assessment for establishing requirements for isolation against wells/pipelines (ref. Appendix C, example 2).

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 Allocation of safety functions

7.8.1 Objectives

The objective of this section is to describe how to:
• allocate the safety functions to protection layers;
• allocate a safety integrity level to each safety instrumented function.

The specified safety functions can be implemented using one or several of the following systems:
• SIS (ESD, PSD, F&G, HIPPS, etc.);
• other technology safety-related systems (e.g. a PSV);
• external risk reduction facilities (e.g. fire walls, bunds, physical distance/layout, manual intervention/procedures, etc.).

7.8.2 Requirements

The input required to perform allocation of the safety functions is:

• Output from the hazard and risk analysis identifying all relevant hazards, and associated acceptance criteria for the risk, i.e. a maximum tolerable risk for the EUC;
• Identification of the safety functions to be implemented for protection against each identified hazard;
• Output from the minimum SIL requirement table.

When applying the minimum SIL table, a safety integrity level has already been allocated to the functions included in the table. Hence, the overall allocation will in such case constitute:
- For process safety related hazards, such as protection against high pressure in a separator, the allocation will, unless deviations have been identified, follow directly from the API analysis and the minimum SIL table. Whether the other level of protection, such as the PSV, shall be specified in terms of a SIL requirement, will depend upon specific project or company requirements, the need from other analyses like e.g. the QRA, etc.;
- For fire and explosion hazards, the situation will normally be that in addition to SIS (ESD, F&G, etc.), other technology related safety systems or external risk reducing measures (like fire walls, bunds, procedures, etc.), are required to bring the risk down to an acceptable level. Whereas the safety functions implemented through SIS normally are given an integrity level based on the minimum SIL table, quantification of the other protection levels, will again depend upon specific requirements resulting from other project activities;
- If a deviation, such as e.g. the need for HIPPS, has been identified, then integrity levels must be allocated to all identified functions protecting against the specific hazard. E.g. in case of overpressure protection of a given EUC, an acceptable risk from overpressure must be specified (and hence the required risk reduction), available safety functions must be identified and integrity levels must be allocated. This is exemplified in Figure 7.2 below.

![Figure 7.2 Example of allocation of safety function to protection layers for overpressure protection, in the presence of a deviation (HIPPS)](image)

For further discussion, reference is made to IEC 61508 part 1, sub-clause 7.6 and to IEC 61511, part 1 sub-clause 9. In particular, the following aspects should be considered when performing the actual allocation:

- The EUC control system as a layer of protection; i.e. if a risk reduction factor greater than 10 is claimed for the control system, then it shall be designed and operated according to IEC 61508/61511 (i.e. treated as a safety system);
- Common cause failures between the different protection layers

### 7.9 Safety Requirements Specification

The Safety Requirement Specification (SRS) is the main output from the SIL determination and allocation activities (i.e. from box 3 in Figure 1.3 or box 5 in Figure 1.4). The SRS is divided between instrumented safety systems, and non-instrumented safety systems in order to address the correct requirements.

In IEC 61511 and IEC 61508, requirements are only given for instrumented safety systems, but the necessary risk reduction will also require that safety functions depending on “other technology”/“external risk reduction” are capable of providing a given protection level.
7.9.1 Specification for Safety Instrumented Systems

**Hardware Specification**
IEC 61511, part 1, chapter 10.3 defines 21 items to be included in the Specification.

**Software Specification**
Ref. IEC 61511, part 1, chapter 12

**Relationship to ISO 13702**
ISO 13702 requires that performance standards for measures protecting against fires and explosion hazards are established. The term “performance standard” is, in the context of ISO 13702, regarded as a “statement”, which in qualitative and/or quantitative terms, specifies:

- The role of the system, or system component;
- What the system or component is required to do under stated circumstances (functional specification);
- With what integrity (reliability and availability) it is required to perform in those circumstances (integrity specification); and
- Any requirements for survivability after a major incident (survivability specification).

As seen from the above, the Safety Requirement Specification will represent such a performance standard, and a possible (simplified) format of this specification is shown in Table 7.2 below.

<table>
<thead>
<tr>
<th>Role of overall function</th>
<th>Safety function</th>
<th>Functional requirement</th>
<th>Integrity requirement</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent overpressure in EUC</td>
<td>PAHH</td>
<td>PSD valve shall close during the first 20 seconds after detected overpressure (above 91 barg)</td>
<td>SIL 2</td>
<td>Assumed testing each 6’th month of PSD valves</td>
</tr>
<tr>
<td>PSV</td>
<td>PSV shall open at 98 barg ± 3%</td>
<td>SIL 1</td>
<td>Assumed annual testing of PSV initially, possibly increasing to two years.</td>
<td></td>
</tr>
</tbody>
</table>

7.9.2 Specification for non-instrumented Safety Systems
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 not be contained in the safety requirement specifications as described in the IEC standards. However, it is important that these systems are included in the overall safety plan for the installation.

As an example, Figure 7.2 illustrates that overpressure protection may depend on a combination of SIS and non-SIS functions. It can be claimed that non-SIS function is technologically simpler and more robust than SIS functions, but nevertheless certain requirements will be have to be fulfilled also for these functions. This is exemplified in Table 7.2 above. E.g. credit for operator intervention should not be claimed unless written procedures are in place and actively used, and PSVs should be tested according to the assumed test intervals.

7.10 Documentation
The Following documents should be prepared during lifecycle phases 1-3 of IEC 61511 (ref. Figure 1.3) corresponding to lifecycle phases 1-5 of IEC 61508 (ref. Figure 1.4).

- Hazard and risk analysis report
- Overall safety requirements report
8 SIS Design and Engineering

8.1 Objectives

This section of the guideline covers the SIS realisation phase, i.e. box 4 in Figure 1.3 or box 9 in figure 1.4. Realisation of safety related systems other than SIS, is not covered by IEC 61508 or IEC 61511, and is therefore not included in this guideline.

The objective of the realisation phase is to create SIS conforming to the Safety Requirements Specification (ref. section 7.9). An overview of the different activities in the realisation phase is described in IEC 61508-2, Table 1.

Of special relevance to this phase is part 2 and 3 of IEC 61508 and clauses 11, 12 and 13 from IEC 61511-1.

8.2 Organisation and resources

Typically, the realisation phase involves a number of vendors. Hence, the work will 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 in this guideline.

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 to be developed fulfils 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 outsourced to 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;
• When the activities will take place;
• The procedures to be used for verification;
• The ones responsible 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 requirements

The input to the realisation phase from the previous life cycle phases (ref. chapter 7) shall contain:

a) An accurate specification for each safety function in terms of functionality and safety integrity;
b) A specified Safety Integrity Level (SIL) for each safety function such as ESD, Fire & Gas, HIPPS etc. (ref. IEC 61508-1, clause 7.6);
c) A description of relevant process scenarios;

d) Required minimum test intervals;

e) Environmental conditions;

f) Organisation or individuals responsible chart (ref. IEC 61508-1, clause 6.2.1).

### 8.5 Implementation of safety functions

#### 8.5.1 SIL requirements

For safety functions implemented through SIS technology, there are three main types of requirements that 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 represents a continuous mode system.

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

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Demand Mode of Operation (average probability of failure to perform its design function on demand - PFD)</th>
<th>Continuous / High Demand Mode of Operation (probability of a dangerous failure per hour)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>( \geq 10^{-5} ) to &lt; ( 10^{-4} )</td>
<td>( \geq 10^{-9} ) to &lt; ( 10^{-8} )</td>
</tr>
<tr>
<td>3</td>
<td>( \geq 10^{-4} ) to &lt; ( 10^{-3} )</td>
<td>( \geq 10^{-8} ) to &lt; ( 10^{-7} )</td>
</tr>
<tr>
<td>2</td>
<td>( \geq 10^{-3} ) to &lt; ( 10^{-2} )</td>
<td>( \geq 10^{-7} ) to &lt; ( 10^{-6} )</td>
</tr>
<tr>
<td>1</td>
<td>( \geq 10^{-2} ) to &lt; ( 10^{-1} )</td>
<td>( \geq 10^{-6} ) to &lt; ( 10^{-5} )</td>
</tr>
</tbody>
</table>

IEC 61508 requires that a quantitative analysis being 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. Fieldbus).

There is no explicit requirement to perform quantification of human reliability. If, however, active operator intervention is required to fulfil a safety function (e.g. response to an alarm), the likelihood of correct action being taken should be considered.

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. It is therefore incorrect to refer to any individual item or equipment having a safety integrity level. 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.
During design, it may be chosen to establish a SIL budget, where a certain percentage of the target failure probability is distributed to the sensors, the logic solver and the final element. This split is a matter of convenience, and should not be considered an absolute requirement.

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

- the hardware fault tolerance of the subsystem;
- 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;
- 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, subclause 7.4. The architectural requirements for different SILs 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)

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Hardware fault tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>&lt; 60 %</td>
<td>SIL1</td>
</tr>
<tr>
<td>60 % - 90 %</td>
<td>SIL2</td>
</tr>
<tr>
<td>90 % - 99 %</td>
<td>SIL3</td>
</tr>
<tr>
<td>&gt; 99 %</td>
<td>SIL3</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Hardware fault tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>&lt; 60 %</td>
<td>not allowed</td>
</tr>
<tr>
<td>60 % - 90 %</td>
<td>SIL1</td>
</tr>
<tr>
<td>90 % - 99 %</td>
<td>SIL2</td>
</tr>
<tr>
<td>&gt; 99 %</td>
<td>SIL3</td>
</tr>
</tbody>
</table>

NOTES:
1. This guideline considers 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. 1oo1D).
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 the sole mathematical reliability calculations (ref. IEC 61508-2, subclause 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 6150-2 for hardware and IEC 61508-3 for software.
In the PDS – projects (Norw.: “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 – 1998 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.

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 quantify 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 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, this guideline defines the interfaces towards the logic solver to be on the termination where the field equipment is connected. External equipment like signal adapters, interface relays, Ex barriers etc. belongs to the logic solver subsystem.

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

8.5.3 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. Such documentation can either be based on third party certification, or as proven in use with the appropriate failure data etc. documented.

Redundancy/architecture

The requirements for design of the system architecture are given by IEC 61511, clause 11. The redundancy requirements apply for the use of standard equipment but by using special components these requirements can be reduced (ref. above point regarding type). It should be noted that redundancy is frequently a result of regularity considerations, rather than safety.

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. Comparison with control system devices for surveillance and comparison is recommended.

Line monitoring when energised to trip

When there is a requirement for an energised to trip shutdown logic, due to special applications, 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 process to process 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).

Alarms/notification of bypasses
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 higher SIL systems it should be considered to remove the capability of overriding the system if this is considered feasible.

8.5.4 Logic Solver

Safety Firmware
The safety firmware constitutes the basic logic solver equipment 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.

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

Hardware application
The nature of logic solvers is normally such that 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 hardware, 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;
• When working with certified equipment, the difference between certified components and components certified for non-interference should be noted:
  - Certified components: for use in safety critical functions;
  - Components certified for non-interference: may be used but not in safety critical functions.
• 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;
• For non-certified equipment the maximum time in degraded mode should be calculated;
• For certified equipment the maximum time in degraded mode 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 guideline 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;
• 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.

8.5.5 Final element

Type
Final elements can be valves (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.

For valves, the type should be selected based on the specific process conditions and required function. This may result in the use of axial flow, ball, butterfly or gate/globe valves depending on service. However, the choice should be clearly documented with verified failure data, verifiable design, materials etc., and proven in use in comparable service.
Materials
Materials should be carefully chosen to withstand the process medium and process conditions in question. For valves, the materials must also be able to withstand the mechanical stress from the quick operation service required.

Tolerances
For a valve, it is very important that the tolerances in production are kept at the very minimum, in order for the valve to be able to withstand the closing or opening forces in operation.

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).

Diagnostic coverage
Diagnostic coverage should be introduced for safety valves in order to meet stringent reliability criteria, and for the purpose of increasing the test intervals. A partial stroke testing of a valve with diagnostic equipment can provide information about the state of the valve, its seals, packing, stem friction and torque reserve. When performed with short test intervals, such a test may for example increase the required interval for a full stroke test to coincide with the annual shutdown. A partial stroke test without any sort of diagnostic equipment will not have a similar effect on the test intervals.

Control Panel design
The valve control panel should include a low-pressure pilot on the air supply to counteract seeping. Great care should also be taken to ensure that the discharge lines from the valve actuator cannot be isolated which would cause the valve to be stuck. 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.

Bypass valves
Bypass valves should be mechanically interlocked in order to avoid that the shutdown valves are inadvertently bypassed. Mechanical interlocks should also be included on isolation valves in the process lines where there are parallel streams, with one in standby for operational requirements.

8.5.6 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 happen 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 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 (such requirement can result from regularity considerations). The design inside the control panel should ensure that redundancy is carried forward through the racks/cards where these are redundant.

8.5.7 Integration
A system can only reach a required integrity level if the whole loop from process to process including the field sensors, the logic solvers and the final elements are considered. Hence, 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 must also be ensured that the final installed and documented system meets the 3rd party
certification requirements, whether that 3rd party operates on the client's behalf or as part of the SIS delivery (ref. IEC 61508-1, sub-clause 8.2.14, Table 5).

It is the responsibility of the system integrator to ensure that all such requirements are fulfilled, in addition to the actual purchase of approved or certified components.

8.6 Factory Acceptance Test (FAT)

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

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 when the test is considered complete;
- procedures for corrective action 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;
- what is actually being tested;
- 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 shall 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 reason shall be documented and analysed and corrective actions shall be implemented.

8.7 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 8.2 below (the figure origins from one specific system supplier and will therefore not be complete with respect to all different documentation from the design phase).
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;
9 SIS INSTALLATION, COMMISSIONING AND VALIDATION

9.1 Objectives

The objectives of the requirements in this chapter are to:
- install the SIS according to the 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 Safety Requirement Specification.

9.2 Personnel and competence

Persons, departments, organisations or other units which are responsible for carrying out and reviewing the SIS installation, commissioning 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 in this guideline.

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;
- when these activities shall take place;
- the persons, 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.

The SIS shall be mechanically completed according to the plan(s) before the final system validation. Mechanical completion activities shall include, but not be limited to, confirmation of the following:
- grounding has been properly connected;
- energy sources have been properly connected and are operational;
- transportation stops and packing materials have been removed;
- no physical damage is present;
- all instruments have been properly calibrated;
- all field devices are operational;
- logic solver and input/outputs are operational;
- interfaces to other systems and peripherals are operational.
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, 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 mechanical completion 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/fail 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 in this guideline shall mean all necessary activities 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.

SIS safety validation must not be confused with functional safety assessment which shall ensure the quality of the Safety Requirement Specification.
The validation of the safety instrumented system and its associated safety instrumented functions shall be carried out in accordance with the safety instrumented system validation planning. 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 of 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.

The software validation shall confirm that all of the specified software safety requirements are correctly performed. Further 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. The information of the validation activities shall be available.

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;
- all forces shall be removed and if applicable all force enables shall be removed.

### 9.4 Documentation

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 made and the decisions taken on whether to continue the test or issue a change request, in the case when discrepancies occur.
When discrepancies occur between expected and actual results, the analyses made and the decisions taken shall be available as part of the results of the software safety validation. Here it shall be stated whether it was decided to (1) continue the validation, or (2) 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 ensure that the Safety Instrumented Systems (SIS) is operated and maintained to ensure that it functions in accordance with the Safety Requirement Specification throughout the SIS operational life.

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 having exactly the same specification. In addition, functional proof testing and handling of non-conformities and demands are included. Any form of modifications or changes in design made to the SIS, including set-point changes, are not included. These are covered in chapter 11, modifications.

10.2 Requirements
Operation and maintenance planning for the SIS shall be carried out during the design stage prior to putting the SIS into operation. This activity shall include but not be limited to consideration of the following factors:

- Routine and abnormal operational activities;
- Functional proof testing;
- Preventative and breakdown maintenance activities;
- The application and control of overrides to SIS;
- The procedures, measures and techniques to be used for operation and maintenance;
- Verification of adherence to operation and maintenance procedures;
- When the activities shall take place;
- Equipment and tools needed for carrying out the activities;
- The persons, 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 (ref. Appendix F).

10.3 Operations and Maintenance Procedures
Operation and maintenance procedures shall be developed to take account of the above factors to ensure that the SIS performs throughout the life of the installation in accordance with the Safety Requirements Specifications. These procedures shall include but not be limited to the following:

- The routine actions which need to be carried out to maintain the required functional safety of the SIS;
- Limits of safe operation (i.e. trip points) and the safety implications of exceeding them;
- How the SIS takes the process to a safe state;
- 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 response to SIS alarms and trips;
- 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 on the SIS;
- The maintenance procedures to be followed when faults or failures occur in the SIS;
- Procedures for tracking maintenance performance;
- Procedures for tracking of activation and failures of the SIS;
- Procedures for ensuring that test equipment used during normal maintenance activities are properly calibrated and maintained;
- Documentation of the above.
10.4 Operation
This section addresses considerations necessary when operating the SIS.

10.4.1 Competence and Training of Operators
All activities concerning operation of the SIS shall be performed by personnel who have been formally assessed as being competent to do so.

Operators shall be periodically trained on the function and operation of the SIS in their area of responsibility. This training shall address the following:

- understanding of how the SIS functions (trip points and the resulting action that is taken by the SIS);
- understanding of 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;
- the operation of any manual shutdown switches and when these manual shutdown 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).

10.4.2 Overrides
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. It should be considered to differentiate between SIL classes in order to reflect the greater safety impact of overriding a SIL 3 system than say a SIL1 system. This could imply imposing different requirements to implementation of compensating measures and to define different upper limits for allowed override time, depending on the integrity level of the SIS under consideration.

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 careful consideration 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 as part of a sequential start-up, can improve safety as it removes the possibility for operator error in forgetting to reset an override.

10.4.3 Handling 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 made such that the required SIL is maintained.

The following shall as a minimum be monitored and recorded:

- actions taken following a demand on the system;
- failures of equipment forming part of the SIS to act on demand;
- failure of equipment forming part of the SIS during routine testing;
- 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 normal demands on the SIS.

---

3 Ideally, the allowed override times should be based upon the safety availability requirements relevant for different integrity levels, ref. Table 8.1 (this applies when production is maintained during override of the SIS).
As discussed in section 7.7, no specific demand rates form the basis for the minimum SIL requirements given in chapter 7. However, if any safety functions experience frequent failures or demands, the typical demand rates given in appendix A should be used as a basis for comparison, unless other more project specific assumptions exist. For a more detailed discussion of how to collect and analyse reliability data, reference is made to Appendix F.

10.5 Maintenance

A maintenance program shall be established, which includes written procedures for maintaining, testing, and repairing the SIS to maintain the required integrity level. This program shall be designed to reveal faults that are not automatically detected by the SIS. Consideration needs to be given to non-availability during routine testing and the effect of mean time to repair on the overall availability of the system.

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.

Replacement of a component in a SIS with another with different characteristics should be treated as a modification.

10.5.1 Testing, inspection, and maintenance

Vendor manuals that describe the SIS maintenance and testing requirements (e.g., battery maintenance, fuse replacement, etc.) may be included in the maintenance procedures.

If a SIS function needs to be bypassed while the process is in a hazardous state, administrative controls and written procedures shall be provided to maintain the safety of the process. Particular attention should be put on resetting any inhibits or overrides that may be necessary during testing, inspection and maintenance of the SIS.

10.5.2 Functional testing

Not all system faults are self-revealing. Covert faults that may inhibit SIS action on demand can only be detected by testing the entire system.

Periodical functional tests shall be conducted using a documented procedure to detect covert faults that prevent the SIS from operating according to the Safety Requirement Specifications. The entire SIS shall be tested including the sensor(s), the logic solver, and the final element(s) (e.g., shutdown valves, motors).

It is recommended to record and analyse activation of SIS functions to include the activation as part of the functional testing. If proper operation and documentation thereof exist for a period, the manual proof test for that period may be omitted. Observe that the spurious activation of an ESV due to a PSD, does not test the entire function of the same valve during an ESD action.

10.5.3 Frequency of functional testing

The SIS shall be tested at specific intervals based on the frequency specified in the Safety Requirement Specifications. Note that different portions of the SIS may require different periodic test intervals.

At some periodic interval (determined by the user), the frequency(s) 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 is handled as a modification.

Any change to the application logic requires full functional testing, and shall be treated as a modification. Exceptions to this are allowed if appropriate review and partial testing of changes are done to ensure that the SIL has not been compromised.
10.5.4 Functional testing procedures

A documented functional test procedure, describing each step to be performed, shall be provided for each SIS. The functional testing procedures 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 diagnostics;
- Complete system functionality;
- The SIS is operational after testing.

10.5.5 On-line functional testing

Procedures shall be written to allow on-line functional testing (if required). For those applications where activating the final trip element may not be practical, the procedure shall be written to include:

- testing the final element during unit shut down; and
- executing the output(s) as far as practical (e.g., output trip relay, shut down solenoid, partial valve movement) during on-line testing.

It should be noted that although partial valve movement reduces the need to fully test the valve, the entire loop still has to be fully tested at certain intervals.

10.5.6 Documentation of functional testing

A description of all tests performed shall be documented. The user shall maintain records to certify that tests and inspections have been performed.

Documentation, which may be recorded in an electronic maintenance database, shall include the following information as a minimum:

- 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 (“as-found” and “as-left” condition);
- Details of any faults found and the corrective action taken.

It is important for technicians carrying out these duties, to understand the importance of recording accurate data related to SIS testing.

10.6 Revision and continuous improvement of 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. The assurance that planned testing is carried out on time and as specified, and that any backlogs are investigated and corrective action 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.
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:
- 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, document, review the change, and approve 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 fix 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; and
- software (embedded, utility, application).

The MOC procedure shall ensure that the following considerations are addressed prior to any change:
- the technical basis for the proposed change;
- impact of change on safety and health;
- 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 of the change and trained prior to implementation of the change or start-up of the process, as appropriate.

All changes to the SIS shall initiate a return to the appropriate phase (first phase affected by the modification) of the Safety Life Cycle. All subsequent Safety Life Cycle 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.

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 are as a minimum made in accordance 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 take place:

- Major replacements or upgrades of the SIS;
- Where major units or modules are replaced or installed;
- Major changes in the process characteristics of the fluids or gasses handled by the installation may create a need for increased safety integrity from the existing SIS;
- Where new rules with retro-active effect show that the existing SIS fails to meet the requirements;
- Where new knowledge gained from, for example, incidents or major studies shows that the existing SIS can no longer deliver 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 safety instrumented system 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.