CHAPTER 8

Second Tier Documents—Process, Oil and Gas Industries

8.1 IEC International Standard 61511: Functional Safety—Safety Instrumented Systems for the Process Industry Sector (Second Edition was published in 2016)

IEC 61511 is intended as the process industry sector implementation of IEC 61508.

It gives application specific guidance on the use of standard products for the use in "safety instrumented" systems using the proven-in-use justification. The guidance allows the use of field devices to be selected based on proven in use for application up to SIL 3 and for standard off-the-shelf PLCs for applications up to SIL 2.

The first edition was issued at the beginning of 2003. Edition 2 was published during 2016 and this chapter has been updated to include the main changes from edition 1. Unfortunately part 1 which was published in February 2016 contained many editorial mistakes. Some of these editorial mistakes may lead the reader to misinterpret the technical requirements. Example of these are:

- Table 6 in paragraph 11.4.5 has "high demand" missing in the 4th row and "low demand" in the fifth row.
- Table 5 in paragraph 9.2.4 title should say "high demand" not "demand."
- Paragraph 9.2.5/9.2.6/9.2.7 has "$>10^{-8}$" which should be "$<10^{-8}$."
- Paragraph 15.2.4 the penultimate bullet point, at the end should have 'only after a reset'

The standard was corrected during 2017 but still issued as edition 2, thus users with copies purchased in 2016 or early 2017 should check and if necessary correct the above points.

The standard is in three parts:

- Part 1: The normative standard
- Part 2: Informative guidance on Part 1
- Part 3: Informative guidance on hazard and risk analysis

Part 1 of the standard covers the life cycle including:

- Management of Functional Safety
- Hazard and Risk Analysis

The Safety Critical Systems Handbook. https://doi.org/10.1016/B978-0-12-820258-6.00008-5

- Safety Instrumented Systems (SIS) Design
- *through to*
- SIS decommissioning

It is intended for the activities of SIS System Level Designers, Integrators, and Users in the process industry.

Component level product suppliers, such as field devices and logic solvers, are referred back to IEC 61508 as is everyone in the case of SIL 4.

Part 2 gives general guidance to the use of Part 1 on a paragraph-by-paragraph basis.

Part 3 gives more detailed guidance on targeting the Safety Integrity Levels and has a number of Appendixes covering both quantitative and qualitative methods.

Since the standard is only aiming at the integration level of the SIS, rather than the individual elements, the requirements for design and development of the SIS (covered by Parts 2 and 3 of IEC 61508) have been significantly simplified. Hardware design has been replaced by a top-level set of straightforward requirements, such as, "*unless otherwise justified the system shall include a manual shutdown mechanism which bypasses the logic solver.*" The software requirements are restricted to the applications software using either limited variability languages or fixed programs. Thus, the software requirement tables that are given in Part 3 of IEC 61508 have been expressed in textual terms using the requirements for SIL 3 but, in general, confined to the "HR" (i.e., highly recommended) items and using engineering judgment on the suitability at the applications level. For applications software using full variability languages the user is referred to IEC 61508.

The techniques and measures detailed within IEC 61511, and hence this chapter, are suitable for the development and modification of the E/E/PE system architecture and software using Limited Variability Languages up to SIL 3 rated safety functions. Unless specifically identified the same techniques and measures will be used for SILs 1, 2, and 3.

Where a project involves the development and modification of a system architecture and application software for SIL 4 or the use of full variability languages for applications software (or the development of a subsystem product), then IEC 61508 should be used.

An existing system designed and installed to some previous standard, prior to IEC 61511, shall be acceptable if it can be demonstrated that it is adequately safe.

IEC 61511 now calls for Cyber security to be addressed during both assessment and design. This is covered further in Chapter 17.

Figure 8.1 shows the relationship between 61511 and 61508.

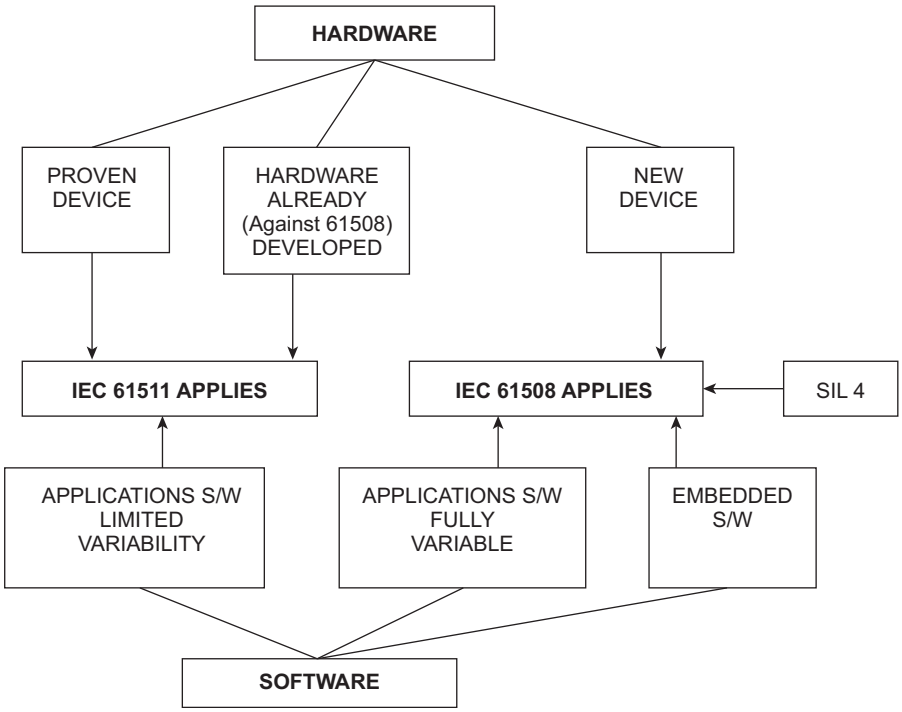

Figure 8.1: IEC 61511 versus IEC 61508.

8.1.1 Organizing and Managing the Life Cycle

The requirements for the management of functional safety and life-cycle activities are basically the same as given in IEC 61508 and are therefore covered by the preceding chapters. The life cycle is required to be included in the project Quality and Safety Plan.

Each phase of the life cycle needs to be verified for:

- Adequacy of the outputs from the phase against the requirements stated for that particular phase
- Adequacy of the review, inspection, and/or testing coverage of the outputs
- Compatibility between the outputs generated at different life cycle phases
- Correctness of any data generated
- Performance of the installed safety-related system in terms of both systematic and hardware failures compared to those assumed in the design phase
- Actual demand rate on the safety system compared with the original assessment

If, at any stage of the life cycle, a change is required which affects an earlier life-cycle phase, then that earlier phase (and the following phases) needs to be re-examined and, if changes are required, repeated and re-verified.

Procedures need to be in place to manage, and document, the competence (both in the technical knowledge of the technologies and in functional safety) of all those involved in the SIS life cycle.

The assessment team should include at least one senior, competent person not involved in the project design. All assessments will be identified in the safety plan and, typically, should be undertaken:

- After the hazard and risk assessment
- After the design of the safety-related system
- After the installation and development of the operation/maintenance procedures
- After gaining operational/maintenance experience
- After any changes to plant or safety system

The requirement to perform a hazard and risk analysis is basically the same as for IEC 61508, but with an additional requirement to consider any security vulnerability of the SIS and with additional guidance being given in Parts 2 and 3.

Part 1 of 61511 describes the typical layers of risk reduction (namely control and monitoring, prevention, mitigation, plant emergency response, and community emergency response). All of these should be considered as means of reducing risk and their contributing factors need to be considered in deriving the safety requirement for any safety instrumented system, which form part of the PREVENTION layer.

It is possible to claim up to one risk reduction layer within the BPCS (Basic Process Control System) for the same hazard event when the BPCS is also the initiating event. Two risk reduction layers may be claimed within the BPCS if it is not part of the initiating cause. A risk reduction of no more than 10:1 can be claimed for each layer. Also the protection layer, and the initiating cause or the two protection layers, should not share the same field devices or I/O modules or processor module.

If the total risk reduction of both the BPCS plus the SIS is equivalent to 10,000:1 (i.e., SIL 4) or higher, then a review should be carried out with the aim of reducing the need to claim a total risk reduction for electrical-based systems to less than SIL 4. If, after the review, there is still a need to have electrical-based systems with risk reduction of 10,000:1 or higher, then detailed assessments shall be undertaken to identify common cause failures between initiating causes, protection layers, and maintenance activities.

Part 3 gives examples of numerical approaches, a number of risk graphs and of LOPA (as covered in Section 2.1.2).

8.1.2 Requirements Involving the Specification

The system Functional Design Specification (FDS) will address the PES system architecture and application software requirements. The following need to be included:

- Definition of safety functions, including SIL targets
- Requirements to minimize common cause failures

- Modes of operation, with the assumed demand rate on the system
- A description of process measurements (with their trip points) and output actions
- Subsystem and component selection referencing evidence of suitability for use at the specified SIL
- Hardware fault tolerance
- Capacity and response time performance sufficient to maintain plant safety
- Environmental performance
- Power supply requirements and protection (e.g., under/over voltage) monitoring
- Operator interfaces and their operability including:
  - Indication of automatic action
  - Indication of overrides/bypasses
  - Indication of alarm and fault status
- Procedures for non-steady state of both the plant and Safety System, i.e., start up, resets etc.
- Action taken on bad process variables (e.g., sensor value out of range, detected open circuit, detected short circuit)
- Software self-monitoring, if not part of the system-level software
- Proof tests and diagnostic test requirements for the logic unit and field devices
- Repair times and the action required on detection of a fault to maintain the plant in a safe state
- Identification of any subcomponents that need to survive an accident event (e.g., an output valve that needs to survive a fire)
- Design to take into account human capability for both the operator and maintenance staff
- Manual means (independently of the logic unit) of operating the final element should be specified unless otherwise justified by the safety requirements
- Safety functions will be described using semiformal methods such as Cause and Effect Charts, Logic Diagrams, or Sequence Charts.

8.1.3 Requirements for Design and Development

(a) Selection of components and subsystems

Components and subsystems for use in safety instrumented systems should either be in accordance with IEC 61508 or meet the requirements for selection based on prior use given in IEC 61511 as summarized below.

The standard gives guidance on the use of field devices and non-PE logic solvers for up to SIL 3 safety functions using prior-use justification and for PE logic solvers, such as standard PLC, guidance on the use for up to SIL 2 safety functions using prior-use justification.

For non-PE Logic Solvers and field devices (non-software programmable items, up to SIL 3) the requirements are based on:

- Manufacturers Quality and Configuration Management
- Adequate identification and specification

- Demonstration of adequate performance in similar operation
- Volume of experience

For field devices (FPL software, up to SIL 3) the requirements are based on:

- As above
- Consider I/P and O/P characteristics: mode of use, Function and configuration.
- For SIL 3, formal assessment is required

Logic Solvers (up to SIL 2) the requirements are based on:

- As for field devices
- Experience must consider SIL, complexity, and functionality
- Understand unsafe failure modes
- Use of configuration that address failure modes
- Software has a history in safety-related applications
- Protection against unauthorized/unintended modification
- Formal assessment for SIL 2 applications

(b) Architecture (i.e., safe failure fraction)

IEC 61511 provides a minimum configuration table which is based on the IEC 61508 route 2_H. At any time the table in IEC 61508 covering route 1_H can nevertheless be used (See Section 3.3.2).

The 61511 version is shown below, in which:

Simplex infers no redundancy and is referred to as **Hardware Fault Tolerance 0**

(m + 1) infers 1 out of 2, 2 out of 3, etc. and is referred to as **Hardware Fault Tolerance 1**

(m + 2) infers 1 out of 3, 2 out of 4 etc. and is referred to as **Hardware Fault Tolerance 2**

SIL	Low-demand HFT	High-demand or continuous HFT
1	0	0
2	0	1
3	1	1
4	2	2

The diagnostic coverage of any FVL (full variability language) or LVL (limited variability language) programmable device shall not be less than 60%, and an upper-bound confidence of 70% shall be used for reliability data used in the calculation of the failure measure.
For non LVL and FPL elements: HFT can be reduced by 1, if an HFT > 0 is specified and it is shown this would lead to a decrease in the overall safety

(c) Predict the random hardware failures

Random hardware failures will be predicted as already covered in Chapters 5 and 6. The random hardware failure calculation should consider the proof test coverage and the effect of random hardware failures in any automatic test circuits.

(d) Software (referred to as "program")

(i) Requirements

- The application software architecture needs to be consistent with the hardware architecture and to satisfy the safety-integrity requirements
- The application software design shall:
  - Be traceable to the requirements
  - Be testable
  - Include data integrity and reasonableness checks as appropriate
- Communication link end-to-end checks (rolling number checks)
- Range checking on analog sensor inputs (under and overrange)
- Bounds checking on data parameters (i.e., have minimum size and complexity)

(ii) Software library modules

Previously developed application software library modules should be used where applicable.

(iii) Software design specification

A Software Design Specification will be provided detailing:

- Software architecture
- The specification for all software modules and a description of connections and interactions
- The order of logical processing
- Any non-safety-related function that is not designed in accordance with this procedure and evidence that it cannot affect correct operation of the safety-related function
- Once the system output is in a safe state then it must remain so until reset including during power recycle
- On initial power up of system outputs must remain in a safe state until reset, unless specified differently in the software requirement specification (SRS)

A competent person, as detailed in the Quality and Safety Plan, will approve the software design specification.

(iv) Code

The application code will:

- Conform to an application specific Coding Standard
- Conform to the Safety Manual for the Logic Solver where appropriate
- Be subject to code inspection

(v) Programming support tools

The standard programming support tools provided by the logic solver manufacturer will be utilized together with the appropriate Safety Manual.

8.1.4 Integration and Test (Part of the Verification Process)

The following minimum verification activities need to be applied:

- Design review on completion of each life-cycle phase
- Individual software module test
- Integrated software module test

Factory Acceptance testing will be carried out to ensure that the logic solver and associated software together satisfy the requirements defined in the safety requirements specifications. This will include:

- Functional test of all safety functions in accordance with the Safety Requirements
- Inputs selected to exercise all specified functional cases
- Input error handling
- Module and system-level fault insertion
- System response times including "flood alarm" conditions

8.1.5 Validation (Meaning Overall Acceptance Test and Close Out of Actions)

System validation will be provided by a Factory or site Acceptance Test and a Close-out Audit at the completion of the project.

The complete system shall be validated by inspection and testing that the installed system meets all the requirements, that adequate testing and records have been completed for each stage of the life cycle, and that any deviations have been adequately addressed and closed out. As part of this system validation the application software validation, if applicable, needs to be closed out.

8.1.6 Modifications

Modifications will be carried out using the same techniques and procedures as used in the development of the original code. Change proposals will be positively identified, by the

Project Safety Authority, as Safety-Related or Non-Safety-Related. All Safety-Related change proposals will involve a design review, including an impact analysis, before approval.

8.1.7 Installation and Commissioning

An installation and commissioning plan will be produced which prepares the system for final system validation. As a minimum the plan should include checking for completeness (earthing, energy sources, instrument calibration, field devices operation, logic solver operation, and all operational interfaces). Records of all the testing results shall be kept and any deviations evaluated by a competent person.

8.1.8 Operations and Maintenance

The object of this phase of the life cycle is to ensure that the required SIL of each safety function is maintained and to ensure that the hazard demand rate on the safety system and the availability of the safety system are consistent with the original design assumptions. If there are any significant increases in hazard demand rate or decreases in the safety system availability between the design assumptions and those found in the operation of the plant which would compromise the plant safety targets, then changes to the safety system will have to be made in order to maintain the plant safety.

The operation and maintenance planning need to address:

- Routine and abnormal operation activities
- Proof testing and repair maintenance activities
- Procedures, measures, and techniques to be used
- Recording of adherence to the procedures
- Recording of all demands on the safety systems along with its performance to these demands
- Recording of all failures of the safety system
- Competency of all personnel
- Training of all personnel

8.1.9 Conformance Demonstration Template

In order to justify that the SIL requirements have been correctly selected and satisfied, it is necessary to provide a documented assessment. The following Conformance Demonstration Template (for both hardware and software) is suggested as a possible format.

Under "EVIDENCE" enter a reference to the project document (e.g., spec, test report, review, calculation) which satisfies that requirement. Under "REQUIREMENTS" take the text in conjunction with the fuller text in this chapter and/or the text in the IEC 61511 Standard.

TABLES FOR ASSESSING OVERALL COMPLIANCE FOR A SYSTEM

MANAGEMENT OF FUNCTIONAL SAFETY (IEC 61511 CLAUSE 5)

Requirements for management of functional safety

Requirements for all SIL rated SIFs	Evidence
Clear accountabilities across the various departments and organizations, including sub-suppliers for each life cycle phase.	
Method for assessment, documenting and management of personnel competency with regards to carrying safety life cycle activities.	
Existence of a quality and safety (Q&S) plan, including document hierarchy, roles and competency, validation plan etc.	
Description of overall novelty, complexity.	
Clear documentation hierarchy (Q&S plan, functional specification, design documents, review strategy, integration and test plans etc.).	
Adequately cross-referenced documents, which identify the functional safety requirements.	
Adequate project management as per company's FSM procedure and SIS configuration management.	
The project plan should include adequate plans to validate the overall requirements. It should state the state tools and techniques to be used.	
Suppliers, product and services, claiming functional safety claims have FSM system in place.	
Functional safety audit to address all documents etc to verify that requirements are being met.	

SAFETY LIFE CYCLE REQUIREMENTS (IEC 61511 CLAUSE 6)

Requirements for safety life cycle requirements

Requirements for all SIL rated SIFs	Evidence
Suitable safety life cycle specified and planned.	
Required activities, inputs and outputs of each life cycle phase specified.	

VERIFICATION (IEC 61511 CLAUSE 7)

Requirements for safety life cycle verification

Requirements for all SIL rated SIFs	Evidence
Verification activities carried out according to the verification and validation plan. Typical verification activities include e.g. design reviews, audits of procedure implementation and integration testing	
Verification planned, carried out for the appropriate safety life cycle activities	
Results of verification activities sufficiently documented	

PROCESS HAZARD AND RISK ASSESSMENT (IEC 61511 CLAUSE 8)

Requirements for Process Hazard and Risk Assessment

Requirements for all SIL rated SIFs	Evidence
A description of each identified hazardous event and the factors that contribute to it (including human errors).	
A description of the consequences and likelihood of the event.	
Consideration of conditions such as normal operation, start-up, shutdown, maintenance, process upset, emergency shutdown.	
The determination of requirements for additional risk reduction necessary to achieve the required safety.	
A description of, or references to information on, the measures taken to reduce or remove hazards and risk.	
A detailed description of the assumptions made during the analysis of the risks including probable demand rates and equipment failure rates, and of any credit taken for operational constraints or human intervention.	
Allocation of the safety functions to layers of protection taking account of potential reduction in effective protection due to common cause failure between the safety layers and between the safety layers and the Basic Process Control System (BPCS).	
Identification of those safety function(s) applied as safety instrumented function(s).	
Has the security vulnerability of the SIS been considered	

ALLOCATION OF SAFETY FUNCTIONS TO PROTECTION LAYERS (IEC 61511 CLAUSE 9)

Requirements for allocation of safety functions to protection layers

Requirements for all SIL rated SIFs	Evidence
Process hazard and the corresponding safety function.	
SIL target.	
Mode of operation (low or high).	
Claims for BPCS as a protection layer where it can also be an initiator OR (when not an initiator) claims of up to two layers of protection.	
Preventing common cause, common mode, and dependent failures.	
Where there is a total risk reduction of >10,000:1 by BPCS and one or multiple SISs then have alternative measures been evaluated.	

SIS SAFETY REQUIREMENTS SPECIFICATION, SRS, (IEC 61511 CLAUSE 10)

Requirements for SIS safety requirement specification

Requirements for all SIL rated SIFs	Evidence
Description of all the safety instrumented functions necessary to achieve the required functional safety.	
Definition of the safe state of the process for each identified safety instrumented function and any combined concurrent safe states that could cause a hazard.	
The assumed sources of demand and demand rate on the safety instrumented function.	
Requirement for proof test intervals.	
Response time requirements for the SIS to bring the process to a safe state.	
Description of SIS process measurements and their trip points.	
Description of SIS process output actions and the criteria for successful operation, e.g., requirements for tight shut-off valves.	
Requirements for resetting the SIS after a shutdown.	
Failure modes and desired response of the SIS (e.g., alarms, automatic shut-down).	
Procedures for starting up and restarting the SIS.	
Interfaces between the SIS and any other system.	
Requirements for overrides/inhibits/bypasses including how they will be cleared.	
The mean time to repair which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints.	

(*Continued*)

Requirements for all SIL rated SIFs	Evidence
The extremes of all environmental conditions.	
Electromagnetic compatibility (EMC) addressed. EMC directive/EN 61000.	
Application program safety requirements derived from the SRS and logic solver suitable for application.	
Application program safety requirements specify all necessary requirements associated with proof test and self-test for all SIF components including field devices.	

SIS DESIGN AND ENGINEERING (IEC 61511 CLAUSE 11)

Requirements for functional specification

Requirements for all SIL rated SIFs	Evidence
Clear text. Describes safety-related functions (SIFs) and separation of Equipment under control (EUC)/SIS, responses, performance requirements, well defined interfaces, modes of operation	
SIL for each SIF, high/low demand	
Hardware fault tolerance addressed	
Default states on fault detection	
Equipment intended environmental requirements both for normal operation and ad-normal operation	
Sector-specific guidance addressed as required	
Equipment in hazard areas adequately addressed	
Communication to other systems and human—machine interface (HMI)	
Power-up, reset, and bypasses considered	
Inspection/review of the specification	
Operability, maintainability, and testability	
SIF Independence from BPCS	
Hardware fault tolerance using route 1_H (IEC 61508) or 2_H (IEC 61511)	
Random hardware failures are to be predicted and compared with the SIL or other quantified target	
Random hardware failures assessment. Include reliability model, common cause failure (CCF) model, justification of choice of failure rate data, coverage of all the hazardous failure modes	
Selection of devices either with IEC 61508 compliance or prior use (IEC 61511)	
Acquired subsystems; SIL requirements reflected onto suppliers and compliance demonstrated	

APPLICATION SOFTWARE SAFETY LIFE CYCLE REQUIREMENTS (IEC 61511 CLAUSE 12)

Requirements for application software summary

Activity	Requirements for all SIL rated SIFs	Evidence
General requirement	Existence of software (S/W) development plan including: Procurement, development, integration, verification, validation and modification activities Rev number, configuration management, deliverables Responsible persons Evidence of reviews	
	Clear documentation hierarchy (Q&S Plan, functional specification, design documents, review strategy, integration and test plans, etc.)	
	Adequate configuration management as per company's FSM procedure	
	There is a software safety requirements specification including: Reviewed, approved, derived from the functional specification All modes of operation considered, support for functional safety (FS) and non-FS functions clearly defined External interfaces specified Clear text and some graphics, use of checklist or structured method, complete, precise, unambiguous and traceable Describes safety-related functions and their separation, performance requirements, well-defined interfaces, all modes of operation	
Validation planning	Validation plan explaining technical and procedural steps including: When and who responsible, pass/fail, test environment, techniques (e.g. manual, auto, static, dynamic, statistical, computational)	
	Plan reviewed	
Design and development	Structured S/W design, recognized methods	
	Use of standards and guidelines	
	Visible and adequate design documentation	
	Modular design with minimum complexity whose decomposition supports testing	
	Readable, testable code (each module reviewed)	
	Small manageable modules (and modules conform to the coding standards)	
	Internal data is not erroneously duplicated and appropriate out of range action	
	Structured methods	
	Trusted and verified modules	
	Identification of timing constraints, memory allocation, global variables	
	Identification of all interfaces (e.g., HMI to BPCS)	
	Identification of internal and external self testing	

(*Continued*)

Activity	Requirements for all SIL rated SIFs	Evidence
Language and support tools	Language fully defined, seen to be error free, unambiguous features, facilitates detection of programming errors, describes unsafe programming features	
	Coding standard/manual (fit for purpose and reviewed)	
	Confidence in tools	
Integration and test	Overall test strategy in Q&S plan showing steps to integration and including test environment, tools and provision for remedial action	
	Test specs, reports/results and discrepancy records and remedial action evidence	
	Test logs in chronological order with version referencing	
	Module code review and test (documented)	
	Integration tests with specified test cases, data and pass/fail criteria	
	Pre-defined test cases with boundary values	
	Response times and memory constraints	
	Functional and black box testing	
Verification	The results of each phase shall be checked to confirm the adequacy of the output against the requirements	

FACTORY ACCEPTANCE TESTING (FAT) (IEC 61511 CLAUSE 13)

Requirements for FAT

Requirements for all SIL rated SIFs	Evidence
FAT carried out according to verification and validation planning	
FAT requirements stated (e.g., test procedure, environment, tools, pass/fail criteria, location of test etc.)	
Procedure for corrective actions	
Competence of test personnel	
Testing has taken place on defined version of the logic solver	
Testing was sufficient and detailed to ensure system is tested against requirement specification	
Result of FAT recorded	
Impact analysis of any modifications as a result of FAT	

SIS INSTALLATION AND COMMISSIONING (IEC 61511 CLAUSE 14)

Requirements for installation and commissioning

Requirements for all SIL rated SIFs	Evidence
Installation and commissioning according to the installation and commissioning plan	
Installed as per specifications and drawings	
Equipment is calibrated, configured, and setup ready for safety validation	
Commissioning activities recorded	
Impact analysis of any installation and commissioning activities that deviates from the design requirements	

SIS SAFETY VALIDATION (IEC 61511 CLAUSE 15)

Requirements for SIS safety validation

Requirements for all SIL rated SIFs	Evidence
Validation activities carried out according to the verification and validation plan	
SIS is validated against the safety requirement specification	
SIS software is validated against the software requirement specification	
Impact analysis of any modifications as a result of validation	
Functional safety assessment carried out by personnel sufficiently independent of the project	

SIS OPERATION AND MAINTENANCE (IEC 61511 CLAUSE 16)

Requirements for SIS operation and maintenance

Requirements for all SIL rated SIFs		**Evidence**
Training of operation personnel on the operation and function of the SIS		
Development of operational and maintenance procedures and plan	Proof testing and inspection (see below)	
	Management of overrides	
	Activities on diagnosed failures	
	Activities on repair or replacement of faulty components	
Proof test and inspection procedure includes	Testing identifies failure modes unrevealed by operation in the entire SIS (sensor, logic solver and final element(s))	
	An unambiguous written procedure documenting the procedure, pass fail criteria, recording of test results, date and name of personnel carrying out the testing, equipment identifier reference e.g. tag number	
	Visual inspection	
	Method for recording and reporting failure tests	
Compensation measures are available to maintain safety whilst SIS is disabled, degraded or bypassed		
Recording of equipment failures and demands placed on the safety function		
Functional safety audits to ensure compliance with operational requirements		
Functional safety audits once operational experience has been gained, to ensure actual system behavior and performance is analyzed and compare with expected behavior		

SIS MODIFICATION (IEC 61511 CLAUSE 17)

Requirements for SIS modification

Requirements for all SIL rated SIFs	**Evidence**
Authorisation of required change	
Safety planning for modification and re-verification available	
Identification of impact of required change e.g., impact analysis	
Appropriate testing carried out according to the impact analysis	
Management of change fully documented	

8.1.10 Prior Use

The purpose of the "proven-in-use" clause in IEC 61508 is to allow existing products that have appropriate field experience to use the field experience as an alternative means of meeting the systematic requirements. The purpose of "Prior Use" IEC 61511 is also to allow existing products that have appropriate field experience to use the field experience as an alternative means of meeting either or both the random hardware failure rate/PFD and/or the systematic requirements.

In all cases it is still required to review the product manufacturer's design and production quality system to ensure that there are adequate procedures in place to maintain the quality of the product even with minor changes being implemented.

The following Conformance Demonstration Template is suggested as a possible format.

Under "EVIDENCE" enter a reference to the project document (e.g., spec, test report, review, calculation) which satisfies that requirement. Under "REQUIREMENT" take the text in conjunction with the fuller text in this chapter and/or the text in the IEC 61511 Standard.

TABLES FOR ASSESSING, FROM PRIOR USE, A STANDARD PLC (LVL PROGRAMMABLE DEVICE) UP TO SIL2

(Section 11.5.2–11.5.5)

Field experience

Requirement	Evidence
Demonstration that it is able to perform the required functions and that the previous use has shown there is a low enough probability that it will fail in a way which could lead to a hazardous event when used as part of the safety instrumented system, due to either random hardware failures or systematic faults in hardware or software in systems in similar operating profiles and physical environments, factors to consider: Volume of the operating experience; The complexity and functionality of the component or sub-system; The embedded software has a good history of use in application with safety type functions.	

Manufacturer's QA & procedures

Requirement	Evidence
Consideration of the manufacturer's quality management and configuration systems. The specific revision number shall be identified and shall be under management of change control. Appropriate standards have been used for hardware as well as the embedded and utility software.	

System features

Requirement	Evidence
Adequate identification and specification of the components or sub-systems.	
Unused features of the components and sub-systems shall be identified in the evidence of suitability, and it shall be established that they are unlikely to jeopardize the required safety instrumented functions.	
Understanding of unsafe failure modes.	
Protection against unauthorized or unintended modifications.	
Measures are implemented to detect faults during program execution and initiate appropriate reaction; these measures shall comprise all of the following: Program sequence monitoring; Protection of code against modifications or failure detection by on line monitoring; Failure assertion or diverse programming; Range check of variables or plausibility check of values; Modular approach.	
It has been tested in typical configurations, with test cases representative of the intended operational profiles;	
Trusted verified software modules and components have been used;	
The system has undergone dynamic analysis and testing;	
The system does not use artificial intelligence nor dynamic reconfiguration.	

Safety manual

Requirement	Evidence
Safety manual including constraints for operation, maintenance and fault detection shall be available covering the typical configurations of the device and the intended application profiles; Use of techniques for safety configuration that address the identified failure modes.	

For SIL 3, formal assessment report/safety manual

Requirement	Evidence
Formal assessment on both the field experience, system features and manufactures QA and procedures.	

TABLES FOR ASSESSING, FROM PRIOR USE, A FIELD DEVICE UP TO SIL3

(Sections 11.5.2–11.5.4).

Field experience

Requirement	Evidence
Demonstration that it is able to perform the required functions and that the previous use has shown there is a low enough probability that it will fail in a way which could lead to a hazardous event when used as part of the safety instrumented system, due to either random hardware failures or systematic faults in hardware or software in systems in similar operating profiles and physical environments, factors to consider; Volume of the operating experience; The complexity and functionality of the component or sub-system; Any embedded software has a good history of use in application with safety type functions.	

Manufacturer's QA and procedures

Requirement	Evidence
Consideration of the manufacturer's quality management and configuration systems. The specific revision number shall be identified and shall be under management of change control. Appropriate standards have been used for hardware as well as the embedded and utility software.	

System features

Requirement	Evidence
Adequate identification and specification of the components or sub-systems with revision numbers.	
It has been used or tested in typical configurations, with test cases representative of the intended operational profiles.	

Formal assessment report/Safety Manuals

Requirement	Evidence
For SIL 3 a formal assessment on both the field experience and manufactures QA and procedures.	
Safety manual including constraints for operation, maintenance and fault detection shall be available covering the typical configurations of the device and the intended application profiles.	

8.2 Institution of Gas Engineers and Managers IGEM/SR/15: Programmable Equipment in Safety-Related Applications—5th Edition 2010

This is the Gas Industry 2nd tier guidance to IEC 61508. It is suitable for oil and gas and process applications.

SR/15 describes both quantitative and risk matrix approaches to establishing target SILs but a **very strong** preference for the quantitative approach is stressed. It addresses the setting of maximum tolerable risk targets (fatality rates). The tolerable risk targets were shown in Chapter 2 of this book.

Cost per life saved and ALARP are also addressed.

In order to avoid some of the repetition present in 61508, the life-cycle activities are summarized into three chapters such as provide:

- Those common to Hardware and Software
- Those specific to Hardware
- Those specific to Software

Detailed lists of headings are offered for such essential documents as the Safety Plan, the Safety Specification, the Safety Manual and the Functional Safety assessment.

Some specific design guidance is given for pressure and flow control, gas holder control, burner control, fire and gas detection and process shutdown systems.

There is a worked example of an assessment of a gas detection system.

SR/15 also includes a checklist schedule to aid conformity in the rigor of carrying out assessments based on Appendix 2 of this book. The term "Required" is used to replace the more cumbersome "Highly Recommended" of IEC 61508. The document has 107 pages.

8.3 Guide to the Application of IEC 61511 to Safety Instrumented Systems in the UK Process Industries

This replaces the former UKOOA document: **Guidelines for Process Control and Safety Systems** on Offshore Installations. It was prepared by representatives of EIC, EEMUA, Oil and Gas UK (formerly UKOOA) and HSE and addresses the responsibility and deliverables of organizations involved in the specification, supply, and maintenance of Safety Instrumented Systems.

This guide is applicable to process industries such as onshore and offshore oil and gas, nonnuclear power generation, chemicals and petrochemicals. Other process industries may choose to use the guidelines at their own discretion. It outlines general information for all users plus guidance on organizational responsibilities for end users, designers, suppliers (of

systems and products), integrators, installers and maintainers. It does not provide checklists or detail on how to design, operate and maintain such systems.

Clause 3 provides an overview of IEC 61511-1, Clause 4 provides an overview of the legal aspects, Clause 5 focuses on issues that affect all users, and Clause 6 addresses activities of specific users covering the whole life cycle of the SIS. Technical detail and examples are given in the annexes.

8.4 ANSI/ISA-84.00.01 (2004)—Functional Safety, Instrumented Systems for the Process Sector

The original, Instrumentation Systems and Automation Society S84.01, 1996: Application of Safety Instrumented Systems for the Process Industries was from 1996 and pre-dated IEC 61511. ISA have now adopted IEC 61511 and have revised ISA84 using the contents of IEC61511.

An exception is the "grandfather" clause stating that ISA 84 does not need to be applied to plant which predated 2004.

The authors assume that ISA will adopt the 2nd Edition of IEC61511 in a similar way.

8.5 Recommended Guidelines for the Application of IEC 61508 and IEC 61511 in the Petroleum Activities on the Norwegian Continental Shelf OLF-070—Rev 2, 2004

Published by the Norwegian Oil Industry Association, this document provides typical safety loops along with the recommended configuration and anticipated SIL. It should be noted that these recommended SILs are typically ONE LEVEL higher than would be expected from the conventional QRA approach described in Chapter 2 of this book.

This is the result of a Norwegian law which states that any new standard, associated with safety, must IMPROVE on what is currently being achieved. Therefore the authors of OLF-070 assessed the current practices in the Norwegian sector and calculated the expected PFDs for each safety loop and determined which SIL band they fitted.

Whereas IEC 61508 and 61511 present a risk based approach to setting integrity targets OLF-070 differs in that it sets out a number of common instrumented safety functions with typical SIL levels assigned. One is then guided towards the design to the examples in the guidance and allocating the given SIL targets.

The aim of this approach is to minimize the amount of time and resource spent on SIL targeting, whilst maintaining a minimum standard for common instrumented functions. This would provide greater standardization across the industry.

This approach needs to be treated with care, however, as there are a number of assumptions incorporated in the "common" functions. All functions are assumed to be LOW DEMAND, and the requirements for a second layer of protection are assumed (e.g. Pressure Relief). All the assumptions in these "common" functions need to be verified against the actual design to ensure that nothing is missed.

Only where the safety function cannot be matched to one of the "common" functions in the guidance then a risk based approach following 61508 is then recommended.

It should also be noted that the guidelines give failure rate figures for systematic, as well as random hardware failures.

In general the guidance in respect of safety management, installation, commissioning, operation and maintenance is much the same as in IEC 61508.

In conclusion, although the OLF-070 guidelines much the same principles as IEC 61508/61511 the main difference is the initial determination of integrity levels. Whereas the IEC standard defines a risk based approach, the OLF-070 guideline attempts match the safety instrumented functions to "common" typical loops and assign a minimum integrity level. The disadvantage of this approach is that the demand rate, severity, and personnel exposure to the hazard are not

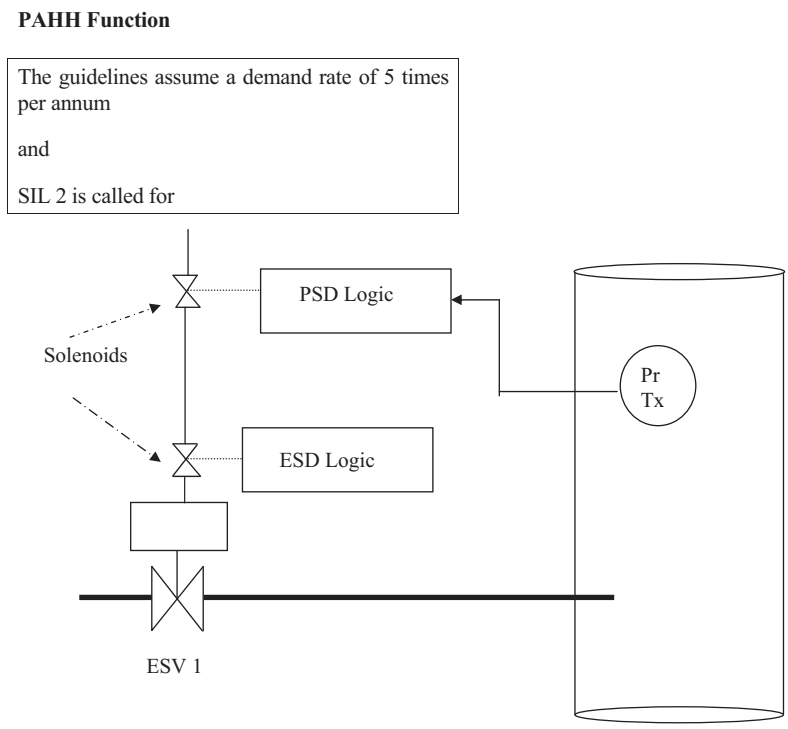

Figure 8.2: OLF-070—process shutdown functions: PAHH, LAHH, LALL.

taken into consideration in the assessment. The second main difference is the method of dealing with systematic failures. IEC-61508/61511 provides a number of procedural methods for dealing with systematic failures, with the level of rigor increasing with the SIL level applied. OLF-070 assigns a failure rate to the systematic failures which is added to the PFD to assess the overall Safety Integrity (PFD).

A typical example of a recommended loop design is shown in Figure 8.2.

8.6 Energy Institute: Guidance on Safety Integrity Level (SIL) Determination, Expected to be Published 2016

This document provides guidance on safety integrity level (SIL) determination in the context of IEC 61511 for the process industries, such as the energy industry and chemical manufacturing industry. Practically, it builds on IEC 61511 by in-filling the requirements of the standard with user experience and worked examples.

The publication recognizes that there should be a balanced approach to risk management starting with adoption of inherently safer design principles, with elimination of hazards as the first priority. SIL targeting is usually determined by adopting a risk-based approach either quantitatively, qualitatively or a mixture of both. Guidance on safety integrity level (SIL) determination considers the required performance of the safety instrumented function (SIFs) to be implemented by protection systems to prevent specific hazardous events or to mitigate the consequence of those hazardous events. Whilst the main focus of the publication is safety and environmental risk, the guidance can also be applied to other risk drivers (e.g. as a basis for asset protection).

The scope of the publication is relevant to SIFs operating in any of the following modes of operation: low demand, high demand or continuous. It illustrates a number of methods available for ensuring that an appropriate SIL is selected for each SIF.