New IEC 61511:2016: What is new?

1. INTRODUCTION

The new standard Ed.2 published in 2016, ignited much eagerness in the functional safety community. Interested parties were curious to learn how IEC 61511:2016 addressed the lack of clarity and alignment in processes and practices from Ed.1 and whether the new requirements and criteria minimise the conflicts between Ed. 1 and IEC 61508. Changes from Ed. 1 combined with the new measures and practices introduced in IEC 61511:2016 are still being broken down and analysed by the functional safety community.

Though there are no fundamental changes, the new standard presents specific additional requirements and clarifies some of the initial requirements; it provides more detail, modifies specific criteria and in general enhances the understanding and the applicability of the related methods and procedures. In general, the inconsistencies between IEC 61508 and 61511 Ed. 1 have been minimised. IEC 61511:2016 is mostly aligned with the requirements of the new IEC 61508:2010.

See below a summary of the modifications made in IEC 61511:2016. Some of the requirements remain unclear in a first reading and require detailed review and repeated reading for appropriate interpretations and to be able to apply them in real practice.

2. DISCUSSION ON NEW VERSION - GENERAL OBSERVATIONS

Many of the new requirements put forth in the new version, even seemingly small changes, will significantly affect functional safety practices.

The changes are of three classes:-

(a) New requirements or requirements with significant changes:

For example, there are some new requirements not included in the previous version and requirements/methods that are significantly different from the earlier version, e.g., 'architectural constraints criteria,' which is severely altered in the new version.

Important additional requirements and changes identified from the previous standard:-

- New Architectural or HFT requirements for SIF subsystems for SIL compliance.
- Added measures in consideration of failure data for analysis (prior use).
- A requirement for cyber security risk assessment for SIS.
- Additional requirements on application program SRS and safety lifecycle requirements.
- Additional emphasis on verification and testing requirements.
- An additional requirement in the O&M phase.

SCE SAFE CONTROLS ENGINEERING CONSULTANTS

(b) Major clarifications/explanations added to existing requirements which provide significant clarity to the related clauses:

Clarification and explanations of specific clauses in Ed. 1 were necessary to understand the requirements. These issues regularly reappeared in risk assessment reviews and posed difficulty in explaining the requirement's exact intent to the less informed functional safety implementer. Additional references and guidelines were required to explain such clauses. Many of those requirements, such as the allowable credit for BPCS risk reduction, common cause failure considerations, proven in use considerations, process safety time and similar have been better explained in the new standard.

New standard addresses certain grey areas in the earlier standard:-

1. Management procedures for personnel competence.
2. Functional Safety Management requirements for product suppliers.
3. Consideration for independence between systems and protection layers in the same system: for example, BPCS.
4. Common cause failure considerations.
5. Definition and requirements for process safety time.
6. Understanding of low and high demand mode systems in IEC 61508
7. Application of standard for F&G (mitigation) systems.

(c) Changes which are improvements or minor modifications

These changes and modifications enhance the clarity of various requirements; this includes the additional, improved definition of terms, clarification on requirements of procedures and similar.

The changes are described in the sections below. Only the first two categories of changes are identified in these sections, in the order of IEC 61511 clauses.

3. SOFTWARE SAFETY LIFECYCLE REQUIREMENTS

There is a certain amount of restructuring of 'software safety requirements. The software safety lifecycle requirements mentioned in Clause 12.0 in the Ed.1. of the standard is now included in Clause 6.0 of IEC 61511 Ed.2., along with the hardware safety lifecycle requirements. However, there are no significant changes in the contents and requirements.

4. MANAGEMENT OF FUNCTIONAL SAFETY

4.1 Personal competency assessment and documentation

The new standard requires a particular level of management competence for individuals involved in the SIS life cycle. The requirements include:

- Documentation and competence for individuals selected for each safety lifecycle activity and the chosen activities
- Periodic performance assessments and documentation for the competence of individuals against the activities/ roles they perform

4.2 Requirements for suppliers functional safety management system

The earlier standard mentioned that the product suppliers should ensure a quality management system for their products to be used in safety instrumented functions. The new standard identifies a clear requirement for a functional safety management system for equipment suppliers having a functional safety claim for their products meeting IEC 61508 Part-1, Clause 6. The requirement identifies demonstrated compliance for all such devices that have functional safety claims.

4.3 FSA (Functional Safety Audit) requirements emphasized

FSA requirements are now specified for all stages, and the earlier recommendation for at least one FSA has been removed. More importantly, the new requirement states that FSA's should be periodically performed during the operations and maintenance phase. The proposed interval for carrying out periodic FSA's is not specified. However, the requirement for regular FSA's is clear to ensure SIS maintenance and operations are carried out as per the assumptions made during the design stage.

Additional requirements for FSA and audits:-

- Include impact analysis while carrying out FSA's for SIS modifications.
- MOC procedures are required for all changes that may impact SIS requirements, e.g., BPCS, design changes, operational changes in particular areas, etc.

5. VERIFICATION

Requirements for verification are further enhanced in the new standard, including an additional emphasis on the following:-

- Inclusion of testing as part of the verification and the requisites for testing of hardware and application programs.
- Verification of integration of non-safety functions and safety functions for non-interference.
- Re-verification for modifications.
- Documentation requirements.

6. PROCESS HAZARD AND RISK ASSESSMENT

6.1 Requirements for cyber security assessments for SIS and related equipment

There is a new requirement to carry out a 'security risk assessment' to identify the security vulnerabilities of the SIS and connected equipment, including:-

- Identify the threats and vulnerabilities that could result in security events.
- Identify consequences of probable security events and their likelihood.
- Identify the measures taken to reduce or remove the threats.
- Recommendations for additional risk reduction.

However, the new version of standard does not provide details for the implementation of this requirement. A reference is made to ISA TR.00.00.09.

7. ALLOCATION OF SAFETY FUNCTIONS TO PROTECTION LAYERS

7.1 Implementation of the SIL-4 safety function

There are no significant changes in the section. Several review techniques and redesign methods are recommended in the new standard for implementation of SIL-4 integrity levels. IEC 61511 Ed.2. is more stringent in terms of SIL-4 implementation and provides recommendations to avoid SIL-4 safety malfunctions.

Methods suggest detailed evaluation for:-

- Process modification.
- Additional protection layers.
- Reduction in consequence severity by a change of design.
- Reduction in likelihood of initiating cause.

If the risk reduction of >10,000 is still required, stringent measures for implementation are suggested using multiple protection layers (SIS < BPCS) with independence between the layers demonstrated. Such a design should further include:-

- Detailed analysis of common cause failures between protection layers and between SIS and initiating events to ensure common cause failures are minimal.
- Detailed quantitative risk analysis of the scenarios to be carried out to ensure safety can be achieved.

7.2 Independence between systems and protection layers (Clause 9.3.4)

The questions discussed at length during LOPA assessments are how many independent protection layers can be taken in a specific given design, how many layers of protection are allowed within BPCS? And, how many credits for safety functions within the same SIS?

The earlier standard did not address this question. CCPS LOPA guidelines, however, specified two methods to allow credit for independent protection layers. Only a single protection layer can be credited within a system, and two independent protection layers within the same systems - provided sufficient independence can be established between the two protective functions. Examples are separate sensors, separate final elements and similar even though the logic solver is shared. In the second case, the logic solver shall be a redundant system.

New IEC 61511 standard allow a second protection layer for consideration in the same system. Though this provides sufficient grounds for applying a maximum of two protection layers in BPCS, the allocation is to be carefully made with consideration of common cause failures between the layers. Common cause failures can be caused by shared process tapping for sensors, shared components in the I/O wiring, shared components in the logic solver etc. Consideration shall include hot standby PLCs which may not be allowed multiple credits as they possibly have shared components.

8. SIS SAFETY REQUIREMENTS (SRS)

The new standard includes more clarity for SRS by referring to additional implementation details such as proof test planning and procedures, bypass procedures etc. The additional points included in SRS are:-

- Definition of safe state.
- Requirements for proof test implementation with details of test intervals, duration, test planning and procedures.
- SIS process measurements, range, accuracy, etc.
- Bypass implementation requirements to be specified in SRS, including written procedures for bypass and administerial controls.

SRS requirements in the new standard are detailed. Additional requirements specified in SRS application program designs and testing are:

- Real-time performance parameters like network bandwidth, CPU capacity, acceptable performance in the presence of faults and a trip signals check within a specified period.
- Program sequencing and time delays.
- Requirement for communication interfaces, limiting their use, data validity.
- Identify and process dangerous states generated within the application program.
- Definition of process variable validation criteria for each SIF.

9. SIS DESIGN AND ENGINEERING

9.1 Hardware Fault Tolerance (HFT) requirements

The HFT requirement is no longer associated with 'safe failure fraction (SFF)' as per the latest IEC 61511. The term 'SFF' has been removed from the definitions and has not used in this standard's new architectural requirements.

One of the significant changes in the standard is the HFT requirement.

HFT requirements for the earlier standard was different for PE logic solvers and non-programmable field devices. For logic solvers, HFT was decided based on safe failure fraction. The new version combines the requirements for PE and non-PE devices and eliminates the SFF calculation. The HFT requirement is no longer associated with 'safe failure fraction' as per the latest IEC 61511.

Minimum HFT is proposed as per Table 6 of IEC 61511: Ed.2. as below. HFT can be increased, if PFD criteria for the specific SIL level requires redundancy, or to reduce proof test intervals.

IEC 61511 Ed.2: 2016: HFT Selection Tables

Table 6 – Minimum HFT requirements according to SIL

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode or continuous mode)	1
4 (any mode)	2

The requirements in Table 6 of IEC 61511 Ed.2 should apply to subsystems with diagnostic coverage >60%. Also, the standard allows for devices that do not use FVL or LVL languages, e.g., simple devices (equivalent to Type A) HFT can be relaxed one level if it can be justified that redundancy would result in additional failures and lead to decreased overall process safety.

HFT requirements in the new standard are more relaxed than the earlier version. These are now aligned with IEC 61508: 2010 and for subsystems complying with the Route 2H analysis method. It is indicated that the route developed in IEC 61511 is derived from route 2H of IEC 61508-2.

A requirement for the SIL-3 subsystem in low demand mode are not indicated in the table. It is assumed that SIL-3 HFT requirements for high demand/continuous mode is applicable for 'low demand' SIFs too.

Summarising, the HFT requirement has been simplified in the new version, having no requirement for SFF calculation. However, the method is not as simple as it is presented. The basis for IEC 61511

analysis is 'proven in use' criteria and the credibility, justifiability, and compatibility of the failure data set used in PFDavg analysis have been given much more emphasis in the new standard. This requires compliance with route 2H data sampling and analysis and shall further meet the specific requirements highlighted in IEC 61511 Section 11.9.3, which recommends several of measures for ensuring the credibility of data used by manufacturers for hardware failure prediction:

- Requirements for credibility and justification of field feedback data used, data population, the suitability of the environment for which the data will be used.
- Reliable data confidence limits to be applied for field data.

Hence compliance with IEC 61511, though it appears simple, may not be an easy process.

9.2 Bypass requirements

Additional requirements for caution while SIS is bypassed should include:-

- Enforcing time limits for bypass.
- Limiting the number of bypasses at a given time.
- Compensating measures to be provided while SIS is in bypass for the continued safe operation of the process.

9.3 Added measures in consideration of failure data for analysis

The new standard provides detailed requirements for reliable data considerations for random hardware failure analysis (PFDavg), unlike the previous version which specified a short set of requirements for the selection of failure data for proven in use instruments. Much importance is given to failure data used from similar environments as that of the applicable industry and the specific limit requirements for the field data to be used for analysis.

The primary requirements are:-

- Reliable data should be based on field feedback for similar devices used in similar operating environments.
- Reliable data uncertainties should be evaluated for calculation of failure measures.

10. APPLICATION PROGRAM ADDITIONAL REQUIREMENTS

Application Program (AP) requirements have been presented in a restructured manner in the new standard. The contents of "Section 12: Requirements for application software, including selection criteria for utility software" in the earlier version has been redistributed in different sections in the new standard, viz: Section 6.3: Application program SIS safety life-cycle requirements, Section 10.3.

Application program safety requirements (SRS) and Section 12: SIS Application Program Development. However, the contents and requirements remain similar to that in the earlier standard mostly. SIS 'application software' has been renamed as 'Application Program' in the new version.

The AP safety life cycle in the new IEC 61511 Ed.2 is more elaborate and specific for AP in comparison to the earlier version of IEC, Fig 10. The safety lifecycle in Ed.2, (Fig 8) appears to be different from that of Ed.1 (Fig 10); however, there are no significant changes in the requirements and activities specified in the safety lifecycle.

Detailed changes in the application program will require separate evaluation.

11. FACTORY ACCEPTANCE TESTING (FAT)

Requirements during FAT remain the same except for minor updates:-

- Recommends integrated testing of field elements with logic solver during FAT for subsea application etc. where high confidence before installation is desirable.
- FAT testing shall include SIS response during power failure and restart when power is restored.
- FAT plans & procedures shall include a clear diagram of test set-up and highlight hazards posed by the testing.

12. SIS Safety Validation

Includes additional requirements for AP safety validation in accordance with:-

- AP safety requirements specified in the new standards.
- BPCS fault conditions for applicable interfaces between SIS and BPCS.

13. NEW REQUIREMENTS IN THE O&M PHASE

The standards propose additional measures for ensuring functional safety is maintained in the O&M phase. Below, see several techniques and activities recommended for this phase which were not identified earlier:

- Inclusion of SIS maintenance plan.
- Recording of operational responses and actions each time SIS faults and failures are identified by diagnostics, inspection or proof testing.
- Procedures for collection of failure data.

- Operational responses towards faults and additional restrictions and requirements while the SIS is taken on bypass.
- Requirement for bypass procedures and hazard analysis for bypass.
- Compensating measures during bypass.
- Ensure availability of spare parts to minimize bypass duration.
- Ensure awareness of the O&M personnel on the basis and assumptions on hazard and risk analysis to ensure assumptions made are valid.
- Monitoring of demand rate on each SIF.

FSA requirements:-

- Management of change procedures which should incorporate additional re-verification, FSA and review of hazard analysis parameters.
- Additional FSA requirements after modifications and periodic FSA's during the operational phase.

Proof testing requirements:-

- Identify failure causes that may lead to common cause failures and avoid them.
- Repetition of a proof test after any repair.
- Management procedures to review deferrals and delay to proof testing.

14. DOCUMENTATION REQUIREMENTS

Safety manual added in the required documents

15. APPLICATION OF STANDARD FOR F&G (MITIGATION) SYSTEMS

The earlier version identified safety instrumented preventive systems and safety instrumented mitigation systems under SIS. Even though no specific methods or directives were included in the standard on how to implement mitigative/preventive systems, the standard includes the requirements for both systems. The new standard has removed the reference to preventive/ mitigative safety systems. The broad requirements to achieve functional safety for F&G systems shall be as per IEC 61511; however, ISA TR84.007 will be used for the method of assessment for F&G risk reduction systems. For preventive SIFs, IEC 61511/61508 provides risk assessment methods and guidance.

16. NEW DEFINITIONS AND OTHER MODIFICATIONS

New IEC 61511:2016: What is new?

The changes and new definitions identified are significant additions and have a strong influence on the understanding and process of functional safety practices. Only the most important new definitions and terms are identified here.

16.1 Common cause failure considerations

Quantification of common cause failures is a challenging activity. The earlier version included common cause failures as a 'failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure'. The new version provides a detailed explanation of such failures differentiating such failures into two types:

- Common cause failures. They are concurrent failures of different devices resulting from a single event, where these failures are not consequences of each other.
- Common mode failures which are concurrent failures of different devices characterized by the same failure mode (e.g., identical faults).

The characteristics of common cause failures and common mode failures are:-

Common Cause Failures	Common Mode Failures	Remarks
Concurrent failures: Failure of two or more channels due to a common error/failure.	Concurrent failures: Failure of two or more channels in the same way due to any failure.	All failures resulting from a common cause or resulting in a common mode may not exactly occur at the same time, thus giving a possibility to detect before SIF fails.
Resulting from a single event: They may be due to external events (e.g., overvoltage, fire, corrosion), systematic fault (e.g., design, assembly or installation errors, bugs), human error (e.g., misuse), etc.	May result from single or different events/causes.	Common cause failures can lead to common mode failures. Multiple causes can also trigger common mode failures.
Reduces the effectiveness of redundancy and fault tolerance.	Reduces the effectiveness of redundancy and fault tolerance.	

16.2 Understanding low and high demand mode systems

Differences in definitions of modes of operation and applicability of target failure measures in each mode existed in the earlier revisions of IEC 61508 and 61511 standards. IEC61508 standard in its first revision specified low and high demand modes. In contrast, the earlier version of IEC 61511 deviated from these, and specified demand modes (for low demand functions) and continuous mode (including high demand) functions. IEC 61508 Ed 2010 came out with three distinct definitions: low demand, high demand and continuous modes of operation. Mode definitions in the new IEC 61511 are also similar to that of IEC 61508 Ed 2010.

New IEC 61511:2016: What is new?

The table below includes the definitions in the latest revision of IEC 61508 and 61511, which are almost identical.

	IEC 61508 Ed.2010	IEC 61511 Ed.2
Mode definitions: Low demand	Safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.	SIF is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is no greater than one per year.
High demand	Safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year.	SIF is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is greater than one per year.
Continuous	Safety function retains the EUC in a safe state as part of normal operations.	SIF retains the process in a safe state as part of normal operations.

16.3 Fault exclusion statement and definition added

Fault exclusion is elimination from further consideration of faults due to improbable failure modes. Specific faults can be excluded from the calculation of failure measures when it can be justified that their related dangerous failure rates are very low.

16.4 Introduction of systematic capability for systematic integrity level

Systematic capability is a measure (expressed on a scale of SC 1 to SC 4) of the confidence that the device's systematic safety integrity meets the requirements of the specified SIL for specified safety function when the device is applied per the instructions in the device safety manual. The new standard does not provide more details; however, Section 11.9.3 identifies the requirement for a systematic capability to be met for all functional safety devices for consideration as proven in use devices. Further IEC 61508 Part-2 & 3 are referenced in the standard for implementation requirements for systematic capability.

16.5 Bypass action

Action or facility to prevent all or part of the SIS function from being executed. Further examples of bypass application are provided. Detailed requirements for methods, procedures and caution when an SIS or part of the SIS functionality is bypassed are provided in various sections in the standard.

17. CONCLUSION

The IEC 61511 Ed.2 published in 2016 addressed and included various improvements on the performance requirements for functional safety for process industry in comparison with the earlier version. The sections above identifies most of the important changes which may help functional safety practitioners who are continuously associated with process safety implementation. However as the functional safety standards being performance based in their content and approach, a close watch and detailed and continuous discussions are required on these standards (IEC 61508/ IEC 61511) and the requirements set forth within them.