The long awaited IEC 61511 edition 2 and what it means for the process industry

Andrew. W. Derbyshire IEng MIET, DNV GL, Principal Safety Engineer

As the concept of risk management has gathered momentum in the oil and gas industry over the past decade, so has the adoption of the internationally recognised standard for functional safety in the process industry; IEC 61511. IEC 61511 is a process industry derivative of IEC 61508, a risk based standard, which utilises the concept of an Electrical/Electronic/Programmable Electronic based control system in order to implement autonomous means of risk reduction, against a pre-defined unwanted hazardous deviation in a process.

IEC 61508, the foundation for IEC 61511, was first introduced in 2000 and was subsequently updated in 2010. Nevertheless 12 years on from the release of IEC 61511 edition 1 in 2003 we find ourselves still using the same edition, that is until now. The second edition of IEC 61511 is in the final stages of publication and like with the second edition of IEC 61508 there are some significant changes afoot. So what are the changes and how will these effect the way in which the industry implement the requirements. These plus many other thought provoking changes and questions shall be discussed in this paper.

IEC 61511 Edition 2, Safety Instrumented System, Safety Requirement Specification, Functional Safety Assessment.

Bibliography

Andrew W Derbyshire started his career in the Royal Air Force before joining BAE Systems after a 9 year tour of duty where he worked as a Systems Safety Engineer in the Airworthiness division on the Eurofighter project. During his time at BAE systems Andrew was involved in several projects as an airworthiness systems safety engineer his last of which was overseeing the development of a safety case for the Nimrod MR2 and R1 post the Haddon Cave enquiry into the loss of XV230 over Afghanistan. Andrew moved into the oil and gas industry over 5 years ago where he became a Senior Functional Safety consultant and certification engineer for SIRA Certification a CSA International company and has since moved to DNV GL where he is now a Principal Safety Engineer. Andrew is a member of the management committee at the IEC 61508 Association and a convener of a Working Group for the association. He is also a member of the Board of Directors at CASS (Conformity Assessment of Safety related Systems) which is a non for profit holder of the CASS assessment scheme aimed at promoting the Functional Safety set of standards. Furthermore Andrew is a member of the Professional Review Interviewers (PRI) panel at the IET interviewing prospective Incorporated and Chartered Engineers for the Engineering Council. Andrew has recently been the Independent Functional Safety Assessor for the QC LNG Project in Queensland, Australia and also works as a Functional safety expert for LNG terminals in Europe.

Objective

The objectives of this paper are to inform the reader of the changes to IEC 61511 with the advent of edition 2 and what these changes represent to the industry.

Introduction

IEC 61511, is a process industry derivative of the internationally recognised standard for functional safety, IEC 61508. Since the advent of IEC 61508 other industries, including the process industry, have elected to develop an industry specific derivative of the more general IEC 61508 for their own means in order to reduce the burden and complexity of complying with a very general standard such as IEC 61508. IEC 61508 first edition was published in 2000 but it wasn't until 3 years later that the International ElectroTechnical Commission (IEC) published an industry specific variant of IEC 61508 for the process industry, namely IEC 61511.

The following diagram (See Figure 1) represents the typical *family tree* of Functional Safety.

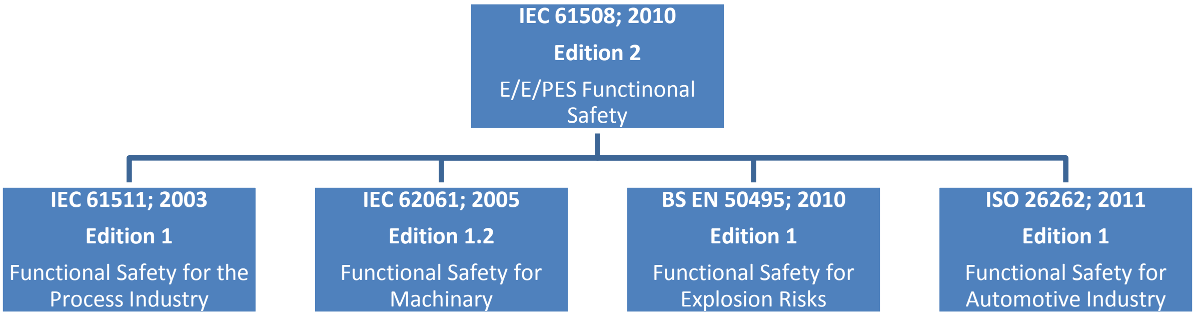
IEC 61508; 2010
Edition 2
E/E/PES Functinonal Safety
IEC 61511; 2003
Edition 1
Functional Safety for the Process Industry
IEC 62061; 2005
Edition 1.2
Functional Safety for Machinary
BS EN 50495; 2010
Edition 1
Functional Safety for Explosion Risks
ISO 26262; 2011
Edition 1
Functional Safety for Automotive Industry

Figure 1

The individual industry based standards for functional safety all follow a cradle to grave approach to the implementation of an autonomous means of risk reduction against defined hazardous deviations, as typically shown for IEC 61511 in Figure 3, below.

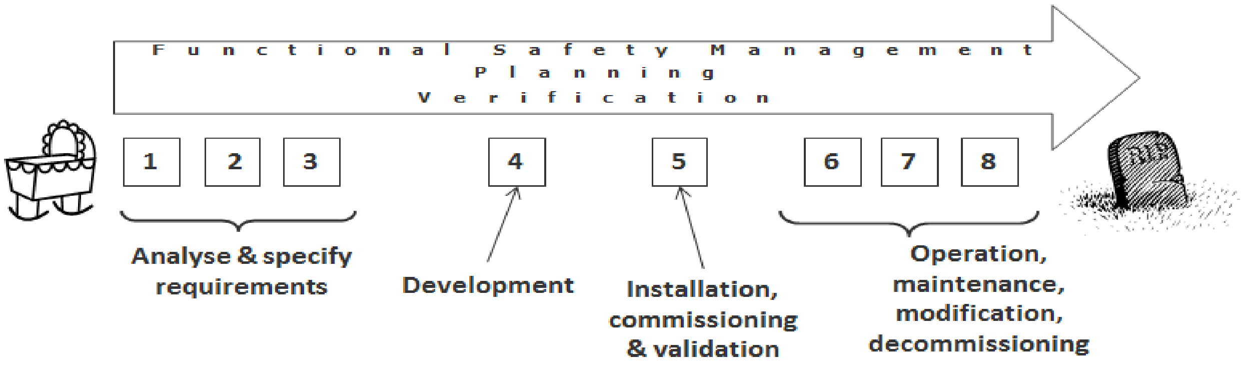
Functional Safety Management
Planning
Verification
1
2
3
4
5
6
7
8
RIP
Analyse & specify requirements
Development
Installation, commissioning & validation
Operation, maintenance, modification, decommissioning

Figure 2

Anyone currently working with IEC 61511 will understand that this lifecycle approach has a reach across several technical disciplines including Process Engineering, Software Engineering and Controls & Instrumentation whilst also considering Instrumentation and Control Technicians responsible for the ongoing maintenance and testing of the systems which is all then governed by managerial processes which are akin to the fundamentals of ISO 9001 for Quality Management Systems (QMS).

This reach across several disciplines is better represented by labelling the lifecycle, shown below in Figure 3 (as represented in Figure 8 of IEC 61511 edition 1), against the typical disciplines involved.

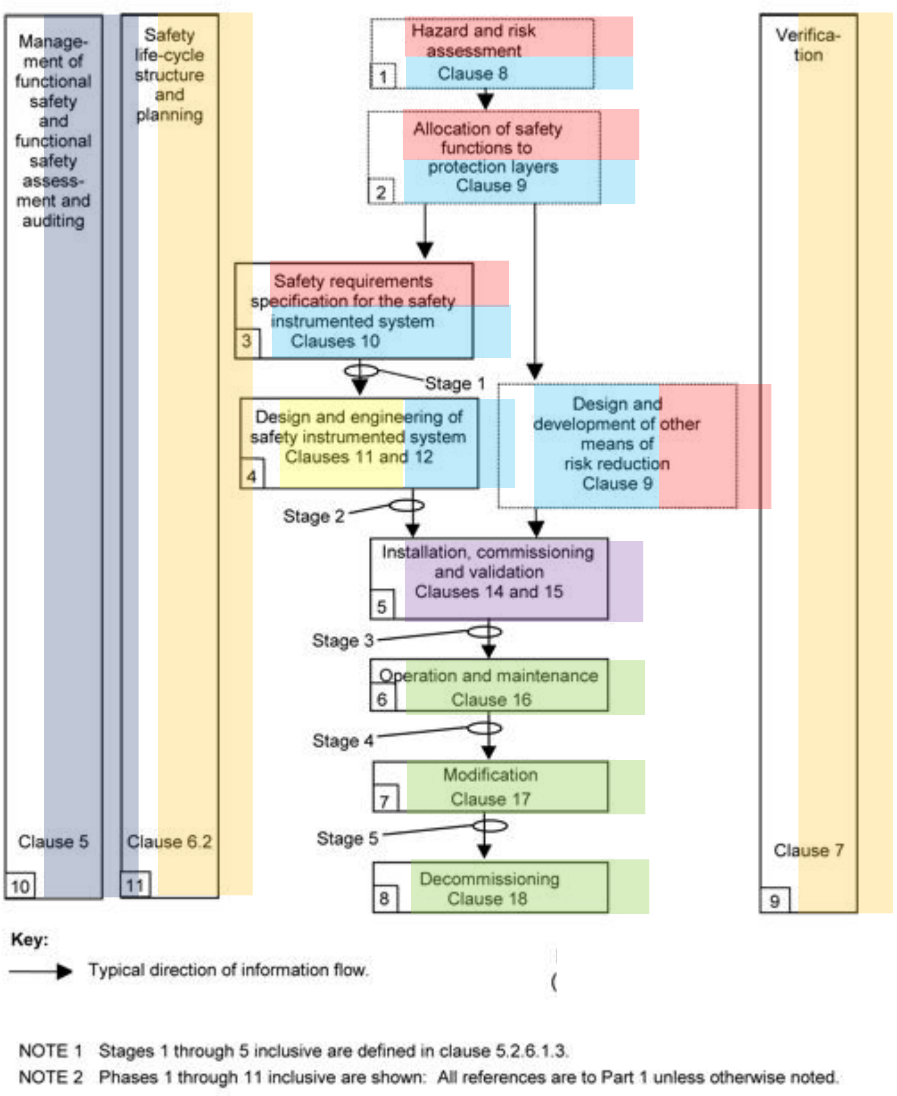
Management of functional safety and functional safety assessment and auditing
Clause 5
10
Safety life-cycle structure and planning
Clause 6.2
11
Hazard and risk assessment
Clause 8
1
Allocation of safety functions to protection layers
Clause 9
2
Safety requirements specification for the safety instrumented system
Clauses 10
3
Stage 1
Design and engineering of safety instrumented system
Clauses 11 and 12
4
Design and development of other means of risk reduction
Clause 9
Stage 2
Installation, commissioning and validation
Clauses 14 and 15
5
Stage 3
Operation and maintenance
Clause 16
6
Stage 4
Modification
Clause 17
7
Stage 5
Decommissioning
Clause 18
8
Verification
Clause 7
9
Key:
Typical direction of information flow.
NOTE 1 Stages 1 through 5 inclusive are defined in clause 5.2.6.1.3.
NOTE 2 Phases 1 through 11 inclusive are shown: All references are to Part 1 unless otherwise noted.

Figure 3

Key:

🟥 Process Engineering

🟦 Controls and Instrumentation Engineering

🟨 Software Engineering

🟩 Controls and Instrumentation Technicians / Operational Management

🟪 Commissioning

🟧 Project Management

⬛ Management of Process and Procedure (Namely Functional Safety Management; FSM)

Since the individual disciplines concentrate most of their efforts on the lifecycle phase(s) they are responsible for this paper on the changes to IEC 61511 for edition 2 will be structured in such a way as to break the changes down into the disciplines involved and what significance it has for them.

Process / Controls & Instrumentation During Detailed Design

The process by which hazards are identified and risk assessed has not altered nor has the safety requirements however there have been some subtle changes to the standard in the earlier phases as described below:

Cyber Security (Clause 8.2.4)

In the main clause 8 has no fundamental changes to the way in which hazards should be identified and risks assessed however one significant inclusion is the introduction of Cyber Security.

As functional safety related control systems have become ever more complex with programmable logic and the use of networks to monitor and control such systems. So has the need to identify and manage threats to the ongoing safe operation of the safety system from cyber attacks. The 2010 edition of IEC 61508 (Edition 2) identified the need, through use of internationally recognised standards for Cyber Security, namely IEC 62443. To include cyber security in the requirements for the identification and management of threats from Cyber Security on the control system.

In response IEC 61511 Edition 2 has included cyber security within the standard which now emphasis the threat to ongoing operations that a cyber attack can pose and the importance of early identification. Whilst IEC 61508 was the first functional safety standard to define the requirements for Cyber Security, IEC 61511 has gone one step further by defining three, rather than just one, possible guidance document, namely:

ISA TR84.00.09

ISO/IEC 27001:2013

IEC 62443-2-1:2010

It should be noted that the Cyber Security standard, IEC 62443, also follows a lifecycle approach to identifying threats, engineering solutions and managing the ongoing threat to security however on this basis it is not clear why IEC 61511, like IEC 61508, has only sought to identify threats to Security without then notifying the reader of the additional requirements as part of the latter phases. It is worth then mentioning that whilst the identification of threats to security are essential it is of equal importance that the engineering of any solutions and the ongoing management of security are also adhered to as defined in IEC 62443.

The inclusion of this additional requirement to clause 8 means that as part of the initial hazard and risk assessment it is now mandatory for a security risk assessment to be carried out on the proposed SIS, however bear in mind that Clause 8.2.4 Note 4 states this risk assessment can be carried out on individual SIFs rather than the complete SIS and therefore an element of engineering judgement should be exercised when deciding on the breadth of the analysis.

Safety Integrity Level 4 (Clauses 9.2.5 – 9.2.7)

The first edition of IEC 61511 defined the requirements associated with the use of SIL 4 and the limitations of going beyond this integrity level. It went on further to describe the avoidance of such high integrity level requirements where reasonable practicable, however this is as far as the standard went. Edition 2 of IEC 61511 has now elaborated on this by providing guidance on the techniques that can be used in order to avoid the use of high integrity level safety systems.

The inclusion of these additional clauses in the standard now allows a more informed judgement to be made when considering the methods necessary to reduce the requirements on a safety system to below SIL 4.

BPCS as a protection layer (Clause 9.3.4)

The use of a Basic Process Control System (BPCS) as a means of risk reduction against an unwanted hazardous deviation is nothing new and is common practice, however the first edition of IEC 61511 stated that a risk reduction claim for a BPCS should be <10 (less than 1 in 10 years; <1.00E-01). A subtle change in the latest edition is to state that a risk reduction claim for a BPCS should be ≤10 (less than or equal to 1 in 10 years; ≤1.00E-01). Whilst it has been common practice to use a claim of 1.00E-01 risk reduction for a BPCS the standard has now aligned with this practice albeit it subtly.

The major difference with edition 2 when considering a BPCS is that where the BPCS is not to conform to the requirements of IEC 61511, e.g. in the case where no greater than 10 is to be claimed for the BPCS. Then the following shall be considered:

> ***9.3.4*** *If it is not intended that the BPCS conform to the IEC 61511 series, then:*
>
> *• No more than one BPCS protection layer shall be claimed for the same sequence of event leading to the hazardous event when the BPCS is the initiating source for the demand on the protection layer; or*

• No more than two BPCS protection layers shall be claimed for the same sequence of event leading to the hazardous event when the BPCS is not the initiating source of the demand.

The inclusion of this additional clauses in the standard should be considered when drafting a Terms of Reference for a Risk study involving Risk Graph or LoPA or when performing such a workshop. It would also be expected that these additional requirements shall form part of the evidence that will be sought during an Functional Safety Assessment by the assessment team.

Safety Requirement Specification (Clause 10.2)

The first edition to IEC 61511 suggested that an SRS should be structured in a clear, precise, verifiable, maintainable and feasible manner. A welcome addition to the latest version of IEC 61511 is making these requirements now mandatory.

It is the opinion of the author that all too often an SRS is drafted in the same manner as a report with a lot of irrelevant information contained within. The author has always maintained that the SRS should be considered a technical dossier that is clear, to the point, and user friendly to maintenance crews.

Take the example where a Controls and Instrumentation Technician is out in the field attempting to perform a proof test on a SIF with the SRS in hand. In order to get to the information they require in the SRS they have to navigate 25 pages of project history and references before they finally reach the technical information relevant to the SIF being tested. In this example they are far less likely to continue on with using the SRS as reference during the proof test which has the potential for a systematic failure of the processes that govern the ongoing success of the safety system as a means of risk reduction. This situation is clearly undesirable and every effort should be made to negate this situation from occurring.

Whilst the author accepts that using subjective terminology in the standard such as precise, and maintainable is difficult to verify. The author equally feels that by making these requirements mandatory, it focuses the minds of those during detailed design to the ongoing requirements facing maintenance teams during later lifecycle phases.

Safety Requirements all in one place (Clause 10.3)

Another welcome addition to IEC 61511 is to have all of the requirements within the same clause of the standard. Traditionally the first edition of IEC 61511 had the requirements for the software detailed in clause 12, rather than clause 10 however in a welcome move the requirements are now all within clause 10.

The inclusion of all requirements for the SIS in the same clause now means it is less likely that application software specific requirements are missed as a result of only considering clause 10.

Additional scope to the Safety Requirements (Clause 10.3.2 & 10.3.5)

As you would expect with 12 years of knowledge using the current version of the standard the latest edition has included additional requirements within clause 10, these being:

SIS Requirements (Clause 10.3.2)

A list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification (e.g., field tag list);

Requirements relating to proof test implementation;

Application software requirements (Clause 10.3.5)

Real time performance parameter such as, CPU capacity, network bandwidth, acceptable real time performance in the presence of faults, and all trip signals are received within a

Specified time period;

program sequencing and time delays if applicable;

the requirements for communication interfaces, including measures to limit their use and

the validity of data and commands both received and transmitted;

process dangerous states (for example closure of two isolation gas valves at the same

time that could lead to pressure fluctuations thus leading to a dangerous state) generated by the application program shall be identified and avoided;

definitions of process variable validation criteria for each SIF.

Safety Manual (Clause 11.2.13)

Annex D of IEC 61508:2010 Part 2 defines the mandatory need for a Safety manual for compliant items. The recent edition 2 update to IEC 61511 has also included a mandatory requirement to have a Safety manual for the SIS.

Furthermore the latest edition has now removed the original requirements under 11.5.4 & 11.5.5 for a safety manual to be produced based on specific SIL level requirements. It is more than likely that the inclusion of 11.2.13, as mention above, is the justification for removing these clauses in the standard.

The inclusion of this requirement in the standard should be considered when drafting a design file or similar technical file for the SIS that shall be handing over to operations. Furthermore as part of the look forward it is expected that during a mandatory stage 3 Functional Safety Assessment the assessment team will look for evidence that such a file exists.

HFT now aligned with Route 2H in IEC 61508 Part 2 (Clause 11.4.5)

In part 2 of IEC 61508 there are 2 different routes to comply with the Hardware safety integrity requirements:

> **Route 1_H** – based on hardware fault tolerance and safe failure fraction concepts
>
> **Route 2_H** – based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specific safety integrity levels.

Edition 1 of IEC 61511 used the concept of minimum hardware fault tolerance however this requirement was misaligned with IEC 61508 which resulted in a claim against either IEC 61508 or IEC 61511 being made during detailed design depending on whether or not a SIF could achieve the requirements of IEC 61511, a practice not advocated by the author. The latest edition 2 of IEC 61511 has now aligned the requirements of IEC 61508:2010 Part 2 Route 2_H with those of IEC 61511 which makes perfect sense given that IEC 61511 is predominantly used by end users who will have access to proven in use data for the SIS.

Dedicated independent wiring for each SIF (Clause 11.6.3)

The latest edition of IEC 61511 has done away with the requirement for each individual field device to have its own dedicated wiring to the system input/output module on the logic controller.

Whilst in some cases the removal of such a requirement would make one think that common cause failure becomes more of an issue in the main the wiring between the field devices (e.g. Sensor, I.S. Barrier or Final Element) has never been considered as a failure mechanism within the hardware safety integrity calculation and therefore the removal of this requirement overall will have a negligible effect.

Prior Use of Equipment (Clause 11.5.3.3)

The second edition has started to place greater emphasis on the collecting of data in order to derive a failure rate for equipment based on prior use however in order to make this data auditable the standard has included an additional clause which states:

> ***11.5.3.3*** *All devices selected on the basis of prior use shall be identified by a specified*
>
> *revision number and shall be under the control of a management of change procedure. In the*
>
> *case of a change being made to the device, the continued validity of the evidence of prior use shall be justified by evaluating the significance of the change made.*

The inclusion of this additional clause in the standard now closes the gap on the argument for prior use and allows operators to readily identify those devices that rely on the data being collected in order to maintain the validity of the prior use argument.

The use of Reliability Data (Clause 11.9.3/11.9.4)

The second edition of the standard has also placed more stringent requirements on the selection and validity of reliability datebooks used to calculate the hardware safety integrity for all individual SIFs. The use of reliability handbooks is common practice in the industry and in the main the practice is well understood however the author has seen evidence of past claims that have been made as to the reliability of particular devices with no evidence or justification of the data source, which is a practice not advocated. Furthermore the standard has now included a clause related to the confidence in the data which aligns IEC 61511 with IEC 61508.

The inclusion of these additional clauses in standard helps to support the reliability claims for devices whilst also ensuring an auditable trail of evidence to source is provided.

Software Engineering

Application Program (Clause 12.2.3)

The only significant change that impacts on the development of Software is a welcome change in that IEC 61511 edition 2 has removed the original statement in 12.2.3 and replaced it with:

> ***12.2.3*** *The IEC 61511 series addresses programming in Limited Variability Languages (LVL) and the use of devices using Fixed Program Languages (FPL). The IEC 61511 series does not address Full Variability Language (FVL) and the IEC 61511 series does not address SIL 4 application programming. Where function blocks are written in FVL then these shall be developed and modified under IEC 61508-3:2010.*

Other than the above there is little in the way of changes to the requirements defined in clause 12 for the application software, apart from the safety requirements being moved to clause 10, see *safety requirements all in one place*.

Commissioning

With regards to the requirements associated with the factory acceptance and onsite validation testing, as defined in clauses 13 & 14, there has been little in the way of changes and there are no new clauses that will fundamentally change the way in which the standard expects these activities to be conducted.

FAT of SIS not just Logic and S/w integration (Clause 13.1)

The standard has subtly changed the objective of the Factory Acceptance Testing to test the devices in the SIS as opposed to the Logic and Application Software.

The change to the wording associated with the Factory Acceptance Testing is not expected to impact on the activities that are conducted during factory testing and it is already common place to see integration testing of Software and Hardware as part of FAT in order to reduce the likelihood of test creep during commissioning (Site Acceptance Testing; SAT).

Evidence of the discrepancy analysis during SAT (Clause 15.2.7)

One welcome addition to clause 15.2.7 of the standard is the expectation that any analysis on discrepancies as part of commissioning shall be documented and available.

The inclusion of this requirement to the existing clause in the standard is welcomed by the author as previous experiences has shown that where a commissioning test has yielded a different result than expected. The analysis and subsequent decisions that are made are not documented and therefore cannot be verified.

C&I Technicians / Operational Managers

This area of the standard is where we see most of the changes. The emphasis has shifted towards the collection and extrapolation of in use field data in order to derive more accurate claims of integrity for the SIS with more expectation on recording and verifying key requirements.

Stage 4 FSA (Clause 5.2.6.1.10)

One inclusion in the second edition that will have a major impact at the operational level is the mandatory requirement to perform periodic stage 4 Functional Safety Assessments during operations. Until now the standard has only made a Functional Safety Assessment mandatory before the introduction of hydrocarbons however this additional mandatory requirement means a stage 3 FSA is no longer the only mandatory FSA to consider.

The inclusion of this mandatory clause means during operations the requirement to define the period and scope of the FSA should be considered and evidence to show it is being fulfilled should be demonstrated.

It is worth noting that the regulator in the UK looks for evidence of a stage 3 FSA during pre-start up reviews and it is likely that with the advent of an additional requirement during operations the regulator will also look to seek evidence on an ongoing basis. How this will look is unclear however one possibility will be to include the evidence as part of the offshore safety case and onshore COMAH report periodically.

Bypass of a SIS (Clause 11.8.4)

The standard has included some additional requirements associated with the use of by-passes, namely:

> ***11.8.4*** *The maximum time the SIS is allowed to be in bypass (repair or testing) while safe operation of the process is continued shall be defined.*
>
> ***11.8.5*** *Compensating measures that ensure continued safe operation shall be provided in accordance with 11.3 when the SIS is in bypass (repair or testing).*

The inclusion of these requirements means the use of by-passes needs to be better defined and a greater emphasis on the management of risk whilst operating with a SIF in by-pass mode is also required.

Quality and Consistency of Proof Testing (Clause 16.2.2; b)

One addition associated with the proof tests is the requirement to monitor the quality and consistency of these procedures.

The inclusion of this clause is considered by the author to link to the ongoing requirement associated with the audit of procedures related to the lifecycle as defined in 5.2.6.2.

Data collection on demands and reliability (Clause 16.2.2; f)

The emphasis has certainly shifted in the later phases to the collection and management of data for devices in order to demonstrate the demand rates and reliability of the SIS. This would seem to make sense given the original perceived analysis for the system performed in detailed design may no longer be relevant or justified so having to collect such data would seem appropriate and this additional clause seems to suggest just that.

Spare parts (Clause 16.2.12)

The Use of the by-passes is clearly on the agenda for the standard committee and the MTTR value in the SIL calculation is somewhat misunderstood and claims of an 8 hour MTTR can often be overly optimistic which can result in a by-pass being on for a considerable length of time. Therefore the standard has now included a clause to state that infantry stock should be identified and readily available to prevent unnecessary long periods operating with by-pass overrides on.

Review of Hazard and Risk analysis (Clause 16.2.13)

Whilst the author can see the relevance of including this clause in the operation and maintenance section it is also worth considering that this clause is associated with the earlier lifecycle phases of hazard and risk analysis. Nonetheless the standard has now made it mandatory for hazard and risk studies to be reviewed to ensure the assumptions are valid. The question still remains on how often and at what point should this be done.

Proof Test after repair (Clause 16.3.1.4)

The standard has now made it clear that a proof test is mandatory after repair. A practice often adopted but never formally documented up until now.

App S/W changes require Full Validation (Clause 16.3.1.6)

Another addition is the expectation that following a change to the application programme the system shall be subjected to a full validation and a proof test. In the past the standard has only described the need to perform a proof test after a change to the software.

Deferral of Proof Testing (Clause 16.3.1.7)

Like with the issue concerning by-passes the standard seems to be leaning towards greater control over the risk reduction being provided by the SIS. This additional clause in the standard now requires operators to have sufficient managerial procedures associated with the use of and review of proof test deferrals. The deferral of a proof test is somewhat unavoidable given resource and environmental issues that may prevent such tests occurring when required however it is important to demonstrate that the SIS is still able to provide the necessary risk reduction whilst potentially increasing the level of unavailability, in order to demonstrate ALARP. The introduction of this additional clause in the standard now making that process mandatory is considered a welcome move by the author.

Project Management

The requirements for planning of lifecycle activities and the activities associated with those phases has not changed however there are subtle additions to clause 6, namely:

A change to an earlier lifecycle phase now requires review and potentially revalidation of evidence. See Clause 6.2.4

Planning for the development of application software is also now a mandatory requirement. See Clause 6.3.1

If testing is to be performed as part of the verification then the standard has now included a handy list of requirements that should be referenced before conducting such tests. See Clause 7.2.2

The plan now needs to consider an Impact analysis as part of any modification and evidence of such impact analysis is being suggested as part of an FSA on a modification. See Clause 5.2.6.1.9 & 7.2.5

Quality Management System

As part of the update to the standard the committees have taken the unusual step of agreeing to remove the clause in the standard which states:

> ***5.2.1.2*** *A safety management system shall be in place so as to ensure that where safety instrumented systems are used, they have the ability to place and/or maintain the process in a safe state.*

However later on in same chapter under clause 5.2.6.2.1 the committee have now agreed to state:

> ***5.2.6.2.1*** *The purpose of the audit is to review information documents and records to determine whether the functional safety management system (FSMS) is in place, up to date, and being followed. Where gaps are identified, recommendations for improvements are made.*

It remains unclear what thought process was being followed when the decision was made to remove clause 5.2.1.2 considering this appears to be a valid objective for clause5. With regards to the management of functional safety there are a few more subtle changes, namely:

Audit of lifecycle Procedures (Clause 5.2.6.2.2)

The standard has taken the bold step of making it mandatory that all procedures identified as being necessary for the lifecycle activities are subject to a safety audit.

Independence of auditor (Clause 5.2.6.2.3)

Furthermore the standard has also made it mandatory that a Functional Safety audit be performed by an independent person, and that procedures associated with the frequency, degree and recording of such audits be defined.

Competence (Clause 5.2.2.3)

Following the release of IEC 61508 there was a lot of emphasis placed on the management of competency given that the standard had opted to make it a mandatory requirement that there be a competency management system. The committees associated with IEC 61511 have chosen to follow suit and IEC 61511 now also describes the mandatory requirement to have a procedure for the management of competence. IEC 61511 also goes one step further to describe the mandatory requirement to carry out periodic assessment on those competencies.

FSM for Supplier (Clause 5.2.5.2)

Edition 1 of the standard only defined the need for a supplier to have a Quality Management System however in a change of policy the standard has now differentiated between the requirements to have a QMS or FSM, as stated below;

> ***5.2.5.2*** *Any supplier, providing products or services to an organization that has overall responsibility for one or more phases of the SIS safety life-cycle, shall deliver products or services as specified by that organization and shall have a quality management system. Procedures shall be in place to demonstrate the adequacy of the quality management system.*
>
> *If a supplier makes any functional safety claims for a product or service, which are used by the organization to demonstrate compliance with the requirements of this part of IEC 61511, the supplier shall have a functional safety management system. Procedures shall be in place to demonstrate the adequacy of the functional safety management system.*

> *The functional safety management system shall meet the requirements of the basic safety standard IEC 61508-1:2010, Clause 6, or the functional safety management requirements of the standard derived from IEC 61508 to which functional safety claims are made.*

Legacy Systems (Clause 5.2.5.4)

To better define the requirements for legacy systems the standard now includes an additional statement, namely:

> ***5.2.5.4*** *For existing SIS designed and constructed in accordance with code, standards, or practices prior to the issue of this standard the user shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.*

Conclusion

To conclude, the second edition of IEC 61511 has a number of significant changes that impact on the management of Functional Safety with one major inclusion being the mandatory requirement to carry out periodic stage 4 Functional Safety Assessments. The standard has also seemed to place a greater emphasis, during maintenance and operation, on the continued safe operation of the SIS whilst also placing greater control over the use of by-passes and deferral procedures in order to maintain the level of risk reduction being achieved by the SIS.

The standard is now better aligned with IEC 61508 in key areas such as Hardware safety integrity, confidence levels in reliability figures and cyber security.

The earlier hazard and risk analysis phases, clauses 8 & 9, have seen little in the way of changes, so has the Factory and onsite testing (FAT & SAT) as part of clauses 13 & 14.

There is a greater emphasis on the need to plan for and provide evidence on any modification to the application programme with a significant change now requiring full validation post a modification.

Having read the revised standard in great detail with time to then reflect on the changes the author is of the opinion that the significant changes being brought into the second edition are welcomed and it is envisaged that the adoption of these additional requirements will support the industry to better manage and control the safety systems during their operational life which in theory should result in a safer more secure environment for us all to work in.