Safety Instrumented System Functional Safety Assessment Experiences

By Jon Keswick, Principal Consultant - eFunctionalSafety, 20 Station Road, Cambridge, CB1 2JD

Given that the process industry now has more than fifteen years of experience with the functional safety life-cycle, it is not unreasonable to expect that there have been some improvements in the specification, design, testing, operation, maintenance and modification of Safety Integrity Level (SIL) rated safety systems.

There are, however, significant challenges in demonstrating conformance with functional safety standards for the design and testing of new safety systems, and even greater challenges for existing safety systems which require modification.

This paper will seek to describe some of the challenges that were witnessed at first-hand during functional safety assessments, audits, and in general during projects involving Safety Instrumented Systems (SIS) during the past ten to fifteen years.

It is hoped that by sharing experiences of real-world functional safety assessment and audit non-conformances, duty holders, engineering service companies and equipment suppliers will be able to learn how to avoid costly re-work and potentially dangerous weak-link designs.

Introducing Safety instrumented functions (SIF), systems (SIS) and safety integrity level (SIL)

When processes still have intolerable risks after the consideration and adoption of inherent risk reduction measures, it is commonplace to employ Independent Protection Layers (IPL) to reduce risk to tolerable or acceptable levels. There are multiple types of IPL which can be selected to prevent escalation of hazardous events into undesired consequences, or which provide consequence mitigation post-event.

One special type of IPL used primarily as a prevention layer is known as a safety instrumented function (SIF). A SIF comprises at least one element for directly sensing a dangerous process condition, a logic solver to decide on the action(s) to be taken, and a final element which will take direct action on the process to prevent an undesired event. As there are usually multiple SIF in a system, and systems require additional elements such as operator interface, the overall system collective is known as a safety instrumented system (SIS).

Functional safety design principles, when applied in the context of SIF such as trips and interlocks, should ensure that there is sufficient integrity to match the level of risk posed. Or, putting it another way, a high level of risk should result in the design of a high integrity SIF, whereas low levels of risk may be tolerable without any form of instrumented safety function.

The term Safety Integrity Level (SIL) is now familiar to all duty holders with hazards that are significant enough to require a SIF. When correctly applied, a SIL requirement from SIL 1 to SIL 4 can be assigned to an end-to-end SIF to provide a marker of the level of integrity required for a given hazard; SIL 1 being the lowest integrity and SIL 4 the highest.

In practice, most non-nuclear process industry safety instrumented functions must be designed to meet SIL 1 or SIL 2. There are very few applications where integrity of SIL 3 is required. Any application requiring SIL 4 typically indicates that there is some problem with setting tolerable risk or the risk analysis method, or that the process design needs re-visiting to consider inherent safety reduction measures.

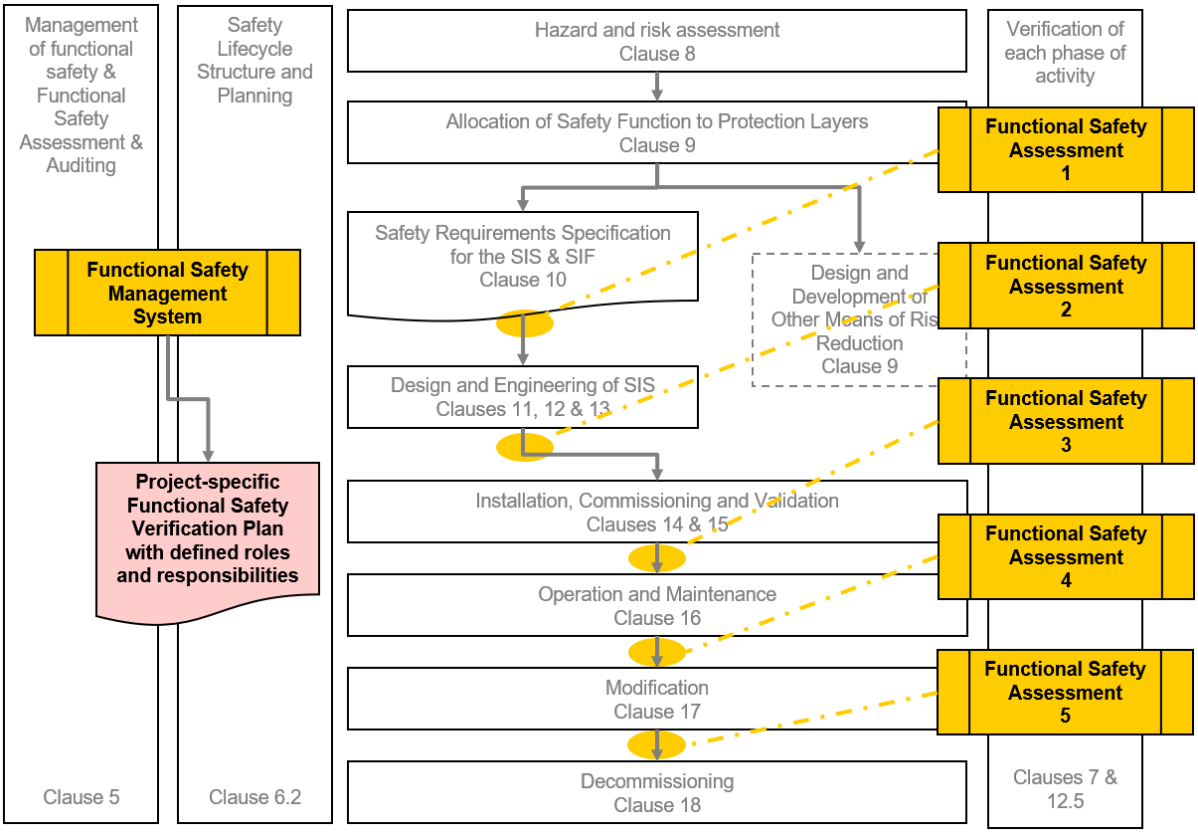
Background on functional safety standards and the safety life-cycle

At the turn of this century, the International Electrotechnical Commission published the very first version of functional safety standard IEC 61508 [IEC61508]. For the first time, IEC 61508 provided an internationally accepted standard for employing electrical, electronic, and especially programmable electronic systems in safety-related applications.

A few years after the first publication of IEC 61508, sector standard IEC 61511 [IEC61511] was issued; specifically designed for functional safety of Safety Instrumented Systems (SIS) in the process industry sector. The functional safety principles are broadly identical in both standards, but IEC 61511 distils the four normative parts of IEC 61508 into a single normative standard of around 80 pages, aimed specifically at the application of SIS in chemical, oil & gas, non-nuclear power generation, pharmaceuticals, pulp and paper and food & beverage plants.

An important model for organising project activities is a safety life-cycle for duty holders and other parties to follow. The SIS safety life-cycle is an outline flowchart of typical phases of the expected activities in the lifetime of an SIS, from initial hazard and risk assessment through to final decommissioning. Importantly, the outline life-cycle does not go into great detail or assign responsibilities to any particular party, so it should only be a starting point for any new-build or modification project involving SIS.

Figure 1: The SIS Safety Life-cycle showing FSA stages 1 to 5 (adapted from Figure 7 of IEC 61511-1:2016)



Demonstrating conformance to IEC 61511

Although IEC 61511 is a distilled version of the parent standard, it is still relatively complicated to implement in practice. It is largely non-prescriptive in how it can be applied, which provides great flexibility to the duty holder in the design of SIF and SIS, but this flexibility means extra complexity when it comes to the question of conformance.

IEC 61511 states the following in the opening clause after the introductory scope, references and definitions:

> *To conform to the IEC 61511-1:2016, it shall be shown that each of the requirements outlined in Clause 5 through Clause 19 has been satisfied to the defined criteria and therefore the clauses' objectives have been met.* IEC 61511-1:2016, clause 4.

So, in following the requirements of the fifteen clauses 5 through 19, and meeting the objectives of each one, it should be possible for a duty holder to demonstrate conformance.

This sounds relatively straightforward, but it is not.

Here are some of the reasons why IEC 61511 conformance is far more complex than it at first seems:

- The standard does not assign responsibilities to any organisation or individual discipline, so the primary challenge in any SIS project is the division of activities to responsible parties. Ultimately, the duty holder (hazard owner) must accept that they live with the hazard and must, therefore, take the lead role.
- Although there are hundreds of requirements, there are few specific techniques or methods prescribed in IEC 61511. This flexibility means that many different techniques can be used to achieve the same goal, so assessment of conformance requires knowledge of many techniques and a pragmatic approach to making a judgement about suitability.
- IEC 61511 points to IEC 61508 for many aspects of hardware and software conformance. Without a detailed knowledge of IEC 61508, an assessment of conformance can be difficult.
- With the advent of cyber-security issues, further new standards have been added to the list of cross-referenced standards. Any duty holder employing modern smart and programmable elements must now also consider the security requirements of these additional standards.

- Each clause of IEC 61511 contains numerous sub-clauses, and in some cases, there are sub-sub clauses and lists of bullet-point items to check. In total there are over 590 sub-clauses and bullet-point items to work through in the fifteen clauses.
- Some requirements are similar in scope, and they are often interlinked between one clause and another.
- For some types of system implementation, there will be requirements that do not apply. Sifting these out from the ones which do apply is not trivial.

The only practical way of demonstrating conformance to IEC 61511 is to implement the requirements of clause 5; management of functional safety. Two specific sub-clauses are entitled functional safety assessment (abbreviated FSA in this paper and in IEC 61511) and functional safety audit and revision (abbreviated FSAR in this paper).

Functional Safety Management

A central element of the SIS safety life-cycle is a functional safety management (FSM) system. A good FSM system will ensure that each person responsible for completing and signing off functional safety activities is competent in the part of the life-cycle they are responsible for. It will provide effective policies, planning and procedures to control life-cycle activities.

As part of the management piece, IEC 61511 edition 2 now requires the competence of individuals to be actively managed in a competence management system (CMS). The standard does not fully elaborate on what this involves, but there are several public sources, including the UK Health & Safety Executive [HSE_2007] which provide sound guidance.

The CMS for functional safety may be just a part of overall competence management and need not be separated. The CMS should set the competency standard for each safety life-cycle role. It should include the role context, tasks, and attributes that the ideal candidate must fulfil to deliver what is required in their role. The levels of attainment for each task and attribute should be clearly specified. A competent assessor should be assigned to verify the individual against the required standard in each role.

Functional Safety Assessment (FSA)

Functional Safety Assessment is one important FSM activity which is proposed at five stages in the SIS safety life-cycle (as shown in Figure 1) and mandated in IEC 61511 to be carried out at least once prior to start-up of an SIS. The activity must be led by a senior competent person, who is not involved with the step or steps being analyzed.

The end expectation of FSA is that a judgement is made as to the functional safety and safety integrity achieved by every SIF within the system(s) being assessed.

The hope is that duty holders will implement FSA planning at the outset of a new project or modification process, and ensure that every organisation involved in delivering functional safety equipment or services knows their individual responsibilities.

With the correct planning and competence in place, it should be clear what evidence will be expected to satisfy the FSA at its various advisory stages, and most importantly at the key mandatory stage before the system enters or re-enters into service with the hazard.

If an FSA is conducted effectively from as early as the SIL determination and specification stage, the clear intent is that this will result in far fewer problems later in the design and validation of the SIF and SIS.

A more recent change in the emphasis of FSA has come with edition 2 of IEC 61511. This now requires periodic FSA during the operation and maintenance phase of the life-cycle. Although the period itself is not specified, the intent is stated as follows:

> *"to ensure that maintenance and operation are being carried out according to the assumptions made during the design and that the requirements within IEC 61511 for safety management and verification are being met."* IEC 61511-1, clause 5.2.6.1.10

FSA planning

Any organisation looking to conduct an effective FSA must first create a plan. The plan is a critical document to make it clear to all project members how the FSA will be approached. Here is an outline list of how a typical FSA plan could be structured:

The plan should include:

- A scope which makes it clear both what is to be included and excluded from the assessment, and which systems are under consideration;
- A clear indication of the lead assessor and their independence from the project;
- The expected roles of different parties in assisting the FSA;
- An estimate of the resources required to complete the FSA;
- The standards and guidelines to be referenced;
- The expected input documents;

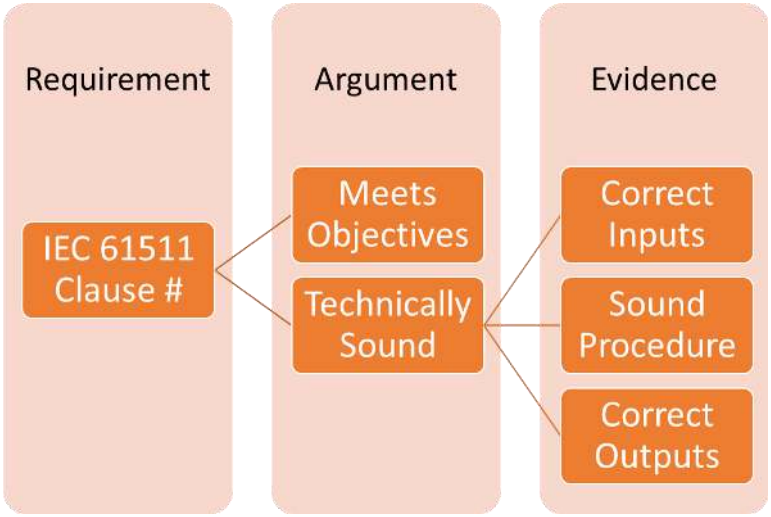
- The FSA methodology;
- The planned deliverables and expectations for repeat FSA after modifications;
- The expected timeline.

FSA preparation

The exact method of how to conduct an FSA in detail is not provided in IEC 61511. The level of depth and overall approach of the FSA will, therefore, be largely down to the lead assessor of the project, with the agreement of the project team.

The author of this paper suggests that the FSA is best conducted by aligning each requirement in IEC 61511 to arguments that the objectives of requirements have been met, and evidence that supports each argument. This requirement, argument, evidence chain was first proposed as a systematic approach to managing safety cases by Timothy Kelly [Kelly_1998].

Figure 2: The link between requirements, arguments and evidence. Adapted from [Kelly_1998].



The challenge of this approach to FSA is that it is very time-consuming when first conducted. Starting with a blank sheet of paper, the development of an FSA checklist which cross-references all the required IEC 61511 clauses, and creates typical arguments, is probably several person-weeks of effort for someone already competent with the subject standards.

The good news is that once an FSA checklist has been created, most of it can be re-used for multiple projects. It should only require an update when the standards themselves are updated.

FSA input documents

When a suitable FSA checklist has been developed, there needs to be a painstaking task of looking for evidence that supports the argument claims.

Experience with conducting several FSA's suggests that delivering the FSA plan is not necessarily a trivial exercise, even for a relatively small SIS project. It might at first seem that the number of uniquely designed SIF plays an important role in determining the level of effort, but in practice, the FSA time estimate relates more to the number of documents, their complexity, and the stage in the project at which the FSA activity is first started. Table 1 highlights the likely number of key documents for review at FSA stages 1 to 3.

Table 1: Estimated number of documents at key FSA stages.

Life-cycle stage	Estimated Number of Key Documents
FSA 1	10 + Number of drawings
Recommended after process hazard and risk analysis and the safety requirements specification has been produced.	
FSA 2	All FSA 1 + 15 + Number of SIS & SIF FAT RECORDS
Recommended after the SIS has been designed and factory acceptance tested.	
FSA 3	All FSA 1 + FSA 2 + 10 + Number of SIS & SIF VALIDATION RECORDS
REQUIRED after installation, commissioning, and validation testing. Operation and maintenance manuals have been developed.	

What is clear from Table 1 is the gathering number of documents that will need to form part of the FSA review as the timeline of a project progresses. Any project which leaves the FSA activity to the mandatory FSA 3 stage required by IEC 61511 may be facing a large and complex effort, almost irrespective of the total number of unique SIF and SIS in the project.

FSA methodology

There is no specific methodology mandated by IEC 61511 for conducting the FSA activity after planning. The precise approach is open to interpretation, but in this author's view the method must include some key activities as follows:

- Collection and initial review of documents.
- Stakeholder initial meeting.
- FSA plan.
- Detailed document review and completion of the FSA checklist.
- Interview of key project personnel.
- The witness of sample validation testing at a site (FSA 3).
- FSA report.
- Stakeholder close-out meeting.

In practice, a real-world project may involve several FSA meetings over several weeks or months, depending on project complexity and scope. It is also likely that interim reports will be produced rather than a single final report, especially if the FSA finds problems in early stages.

FSA results

With an FSA report as a final deliverable, it should be expected that there will be some conformance issues given the sheer number of IEC 61511 requirements, possible selection of techniques and other complexity issues raised earlier in this paper. Only the FSA lead assessor can make the judgement on how important non-conformance items are in practice.

When finalising the FSA checklist, it has been shown to be useful for the lead assessor to segregate non-conforming issues into at least two categories as follows:

A. Requirements, if not fulfilled, that should lead to aborting the start-up of the SIS.

B. Requirements, if not fulfilled, that require a recommendation for improvement.

Whatever the final report shows, the duty holder must make the ultimate decision on whether to start up an SIS once the FSA report has been produced with any non-conformances.

Functional Safety Audit and Revision (FSAR)

Functional safety audit and revision (abbreviated FSAR in this document, but not in IEC 61511) is intentionally separated from FSA in the IEC 61511 standard. The idea is that FSAR is an audit of procedures and records to determine whether an appropriate functional safety management system is in place and being followed.

However, the distinction between FSA and FSAR may be somewhat overplayed if an FSA is already being planned or conducted on a project. The person leading any FSA activity must take account of the detailed life-cycle phases of the stages being assessed. By definition, every stage of the life-cycle includes management, planning and verification activities, so the FSA must take these into account. In this sense, FSA's already include elements of an audit.

One thing that is clear about the distinction between FSA and FSAR is that FSAR does not have the specific goal of making a judgement about the functional safety achieved by each SIF design, whereas FSA does have that goal.

Somewhat like a Quality or Gap audit, an FSAR cannot be conducted until functional safety procedures are in place, and they have in place long enough to produce sufficient evidence documents about whether the procedures are being followed. However, it is entirely feasible that some procedures will be put in place and followed at least once during an SIS project development, meaning an FSAR alongside an FSA activity is an entirely valid prospect even for a new-build.

An FSAR also involves the important aspect of making recommendations for improvement, including possible revising of procedures or systems under management-of-change control. From experience, this is no different in an FSA given that non-conformances would lead to an action for change.

Experiences of FSA and FSAR issues in real-world projects

FSA and FSAR Take-up

On new-build SIS projects where IEC 61511 conformance is a contractual obligation, it is becoming more of a norm to see some formal activity of assessment or audit. Unfortunately, experience from several projects suggests that FSA is not very well understood by all parties, is often poorly planned into the project schedule, and is subsequently left until far too late in the project. This leads to surprise changes and costly re-work if the FSA exercise is taken seriously.

For significant modifications to existing systems, there seems to be some acknowledgement that FSA applies, but this seems to be far less the case for systems which pre-date IEC 61511 and are not undergoing significant change. Experiences of FSA at stage 4 are therefore less commonplace.

FSAR as a stand-alone exercise is something that may be taking place more commonly with duty holder internal resources, but from experience of a few of these exercises as an independent assessor, they are often arranged around the same time as FSA during an SIS modification.

Experience of FSA and FSAR non-conformances

Table 2 highlights some non-conformances that have been experienced in real-world FSA projects. The names of projects and the companies involved are withheld for confidentiality reasons. These experiences have come from several different projects where FSA was completed up to the stage 3 assessment. Mention of aspects relating to FSA 4 (after a system has been installed) are mentioned where applicable.

In each case of non-conformance, a suggested project impact is highlighted in Table 2. In some cases, it should be noted that there may be multiple impacts which can be more far-reaching than the example ones listed here.

For each example non-conformance, some pragmatic recommendations are provided as examples of things that can be done to avoid or limit non-conformance problems. In some cases, the suggested recommendation may not immediately impact a project (e.g. competence improvement), so in practice, the improvement may need to be very project-specific for a more immediate impact.

Table 2: Real-world non-conformances, their possible impact and recommendations.

Non-conformance	Possible impact	Recommendations for improvement
MANAGEMENT, planning and verification (Clauses 5, 6, 7)		
Functional safety management plan is either not produced or not followed by project parties.	Key stage-gates of verification may be missed or incomplete. It is highly possible that the FSA itself will be impacted if it is started too late in the project.	Project planning should ensure that a dedicated functional safety plan is produced and followed by all parties. Key stage gates should include review by a competent functional safety leader.
Lack of a competence management system.	Personnel with unknown functional safety competence working on the project. Possibility for poor decisions which may impact functional safety. If approval is by non-competent persons then verification activities are questionable.	A competence management system should be implemented and maintained for functional safety.
Lack of a clear responsibility matrix.	Unclear responsibility determination at the level of detail required for all life-cycle tasks. This can lead to missed activities or missed verification stages.	Life-cycle planning should include a clear responsibility assignment such as RACI matrix - responsible, accountable, consulted, informed.
Poorly defined or incomplete procedures for key life-cycle tasks.	Inconsistent approaches by project teams in the delivery of key aspects such as hazard and risk assessment, SIL determination, system specification, equipment and software selection, system design and validation testing. For FSA at stage 4, discovery of poor operation and maintenance procedures can mean that key records such as proof testing and failure/event recording are not available or are severely lacking.	Duty holders should produce and approve their own procedures to manage the safety life-cycle and ensure these are used by all project teams.
No check of sub-contractor competence with functional safety.	Personnel with unknown functional safety competence working on the project. Possibility for poor decisions which may impact functional safety. If approval is by non-competent persons then verification activities are questionable.	Project managers should ensure that equipment and service suppliers provide appropriate evidence of functional safety competence prior to selection.
Closure of action items without clear justification.	In all projects, there are action items created during different stages of the design. Where actions are closed without a record of justification, this can lead to significant later issues with understanding how the action was logged as completed.	Project teams should receive clear training on how actions are to be handled and what is required to be documented before actions are closed out.
Process hazard and risk assessment (Clause 8)		
Poorly recorded hazard studies (e.g. HAZOP).	Can cause multiple issues. Lack of qualitative risk ranking at an early stage may mean subsequent studies need to re-assess consequence severity. This may have a significant impact on traceability of SIF back to the hazards identified.	Implement risk ranking during studies like HAZOP, including clear description and assignment of consequence. Ensure proposed IPL and SIF are traceable by means of line numbering and tag references.
No cyber-security risk assessment.	Possible threats to the SIS from cyber-attacks are not identified. Subsequent stages of secure design are not implemented.	Conduct cyber-security risk assessment when system architecture is clear (new projects), or after review of existing system assets and network architecture (existing plants).

Non-conformance	Possible impact	Recommendations for improvement
Allocation of risk reduction to IPL (Clause 9)		
Lack of a clear duty-holder procedure for Layer of Protection Analysis - LOPA.	Where the duty holder accepts a procedure from a third party, they are reliant on that procedure being robust and complete. This is not always the case, and from project to project will produce significant inconsistencies.	The duty holder should produce a clear and concise procedure for SIL determination (by LOPA or any other method) and ensure it is used by all parties on all projects consistently.
Conditional modifiers in LOPA incorrectly applied.	Where a factor is incorrectly applied this can lead to a resulting incorrect SIL determination. If discovered late in the FSA activity this can lead to costly re-work.	
Only considering safety to personnel during SIL determination.	This is a missed opportunity. In some projects it may be highly important to assess environmental and commercial drivers for integrity.	
Incorrect or misleading assumptions about operator effectiveness as an IPL.	Projects which accept the results of SIL determinations which include incorrect assumptions about operator effectiveness as an IPL may subsequently make incorrect decisions about equipment and software requirements. If discovered late in the FSA activity this can lead to costly re-work.	Ensure LOPA results are reviewed by an independent competent person prior to finalisation of the safety requirements specification (independent review may be part of FSA 1).
SIS safety requirements specification (Clause 10)		
Missing or incomplete SIS hardware requirements.	This can lead to numerous critical project issues, depending largely on the requirements concerned. In the worst cases, a poor or missing initial requirement specification may mean that purchased SIS equipment is unable to perform the required safety function. This can involve very costly re-work.	Implement a safety requirements specification checklist and review procedure (independent review may also be part of FSA 1).
Poorly defined detail in SIS application program requirements.	SIS application program specifications which lack detail can lead to later issues over how the SIS should respond under fault conditions and many other aspects that can affect safety. This is usually easier to fix than hardware mistakes, but only if the SIS logic solver has appropriate capabilities for alteration.	
Poor definition of interfaces to/from the SIS, such as human-machine interface (HMI).	When interfaces such as the operator workstation view of SIS status and alarms are not clearly specified early in the project, it may be subsequently difficult to engineer what is needed to be displayed.	
Process Safety Time not fully defined, and SIF response time “assumed” to sufficient.	The SIF design may not meet the required process safety time, meaning a hazardous event may subsequently occur before the SIF can react.	

Non-conformance	Possible impact	Recommendations for improvement
Manual shutdown or bypass requirements poorly specified.	When manual shutdown or bypass capability has not been considered carefully in the SRS, it is subsequently difficult to engineer at later stages. This can lead to costly re-work.	
SIS design and engineering (Clause 11)		
Selection of SIS devices with little or no evidence of SIL capability.	If devices are selected without enough evidence of SIL capability then this can lead to difficult justification, putting the onus on the SIS designer or duty holder to provide equipment justification for the application.	Clear equipment selection rules should be created, with a list of authorised devices.
PFDavg (average probability of failure on demand) calculations do not meet the required SIL allowing for reasonable real-world conditions.	This can lead to a requirement to re-assess SIL considering additional IPL, restrictions placed on the duty holder for higher frequency proof testing, or reduced turn-around requirements for SIF overhaul.	The procedure for conducting appropriately rigorous probability of failure calculations should be created and followed.
No BPCS / SIS design assessment for cyber security.	Possible that cyber-attacks could compromise safety, with no way of knowing how resilient the system will be to attack.	Conduct cyber-security vulnerability testing. For existing systems this can be during turn-around (when the SIS is not in service).
SIS Application program development (Clause 12)		
Mixing safety and non-safety functions in the same SIS application program.	Mixing safety and non-safety functions can create an ongoing issue for management of change, as the entire application program will be treated with the highest SIL requirement. This will require costly re-validation testing for any changes in functionality.	Ensure designers follow segregation of safety and non-safety functions from the outset.
Development of custom function blocks which have not been IEC 61508 assessed.	Custom function blocks can create hidden failures and will require separate IEC 61508-part 3 assessment if they have been configured using any full variability language (FVL).	Do not allow custom function block development.
Not following application program restrictions in the logic solver safety manual.	A poor implementation of application program can lead to the introduction of dangerous systematic errors which may not be immediately apparent through testing.	Ensure designers follow safety manual restrictions.
Factory Acceptance Testing (Clause 13)		
Test setup not fully recorded.	For FAT to be an effective, albeit limited in nature, it is important to know exactly what the test setup is. If this is not recorded then it may lead to more time-consuming testing at site when the pressure to complete is typically much higher. This can lead to mistakes or incomplete testing.	Review FAT test specifications for completeness prior to witnessed testing.

Non-conformance	Possible impact	Recommendations for improvement
Pass/fail criteria not specified.	A test without pass/fail criteria has limited or even zero value as evidence of a test.	
Failed tests not re-tested.	Any failure during an FAT should lead to creation of a corrective action. If not, this failure is carried forward to site and may be missed or create further problems for subsequent validation.	Do not allow sign-off of FAT without review of open problems.
Logic solver application program not uniquely identified at the conclusion of FAT.	The application program at FAT must be compared with the version at site, and have any changes identified for review. This is to ensure re-testing is completed where required.	
Installation, commissioning and validation (Clauses 14, 15)		
Poor planning for validation.	When validation planning is inadequate, the validation itself cannot proceed. An SIS must never enter service without full validation, so this is a significant re-work item.	Ensure validation planning and test specifications are fully reviewed and approved by competent persons before commencing validation testing.
Wrongly identified document revisions at testing.	If a test records the wrong revision of document, then someone competent needs to review if the correct revision would have any impact on the test.	Improve validation test team training to include encourage and reward the finding of errors. Stress the importance of document revision accuracy, following as-written tests (provided it is safe to do so), and recording of all anomalies.
Validation test procedure not followed, or validation record is missing.	If a validation test is not followed or is missing then the test is incomplete and invalid. If the test procedure is wrong then this needs update by someone competent. If the test was missed in error then it must be completed, and records produced.	
Missing or incomplete operation and maintenance procedures and training.	An SIS entering service without adequate training or information for the operations and maintenance personnel is a potential significant safety issue.	Produce operations and maintenance manuals and conduct training or re-training prior to SIS start-up.

Conclusion

In the early years of functional safety and attempts at SIL conformance, there was a definite over-emphasis on purchasing "SIL certified" equipment, and somehow this would ensure a safe working system. This is a clear over-simplification of the challenge that awaits duty holders with IEC 61511 conformance.

The technical aspect of calculating "probability of failure" was also an attractive one for engineers to get embroiled with, but sadly it hid far more important but less technically appealing issues. Although achieved failure probabilities are certainly part of the requirement for demonstrating integrity, the achievement of specific numerical failure targets is only a very small piece of the functional safety picture.

The IEC 61511 standard has several hundred requirements that must be fulfilled for a duty holder to claim conformance. Non-conformances have been repeatedly experienced during independent FSA's conducted across multiple projects and applications as highlighted by the examples in Table 2 of this paper. This does not necessarily mean that unsafe systems were ultimately implemented, but it often resulted in significant time overrun and additional cost.

It should be noted that non-conformances will occur, and they will not all be fixed before an SIS is put into service, or back into service if it is a modification project. There will always be a judgement that must be made, and that judgement should be based upon a detailed justification that can only be produced by conducting FSA.

Any duty holder embarking on a functional safety project today would be well advised to put much more emphasis on management, personnel competence, appropriate procedures, project setup, assessment and audit activities.

References

[IEC 61508_2010] International Electrotechnical Commission, 2010, Functional safety of electrical /electronic /programmable electronic safety-related systems.

[IEC 61511_2016] International Electrotechnical Commission, 2016, Functional safety of safety instrumented systems for the process industry sector.

[HSE_2007] Health & Safety Executive, Institution of Engineering Technology and the British Computer Society, 2007, Managing competence for safety-related systems (2 parts).

[Kelly_1998] Kelly. T.P., 1998, Arguing safety - a systematic approach to managing safety cases.