SIL and Functional Safety – some lessons we still have to learn.

David Craig, Amec

This paper reflects AMEC's recent experience in undertaking functional safety assessments (FSA) (audits against IEC 61511) and in providing support to clients in developing their IEC 61511 compliant management and technical systems. It identifies and discusses some of the keys issues where companies are failing to manage risk in the most effective way because of a misapplication of the standard. The issues are split into two general themes: those which have a technical focus and those that relate to the "management system" which will be considered towards the end. These inevitably overlap. This paper is not intended to introduce new thinking. Instead it aims to assist those who are still trying to implement IEC 61511 by providing an overview of the standard and help in avoiding some of the often encountered errors.

For almost all organizations which consider integrating IEC 61511 into their company procedures there are pre-existing systems and structures which have some overlap with this standard. This is true for both operating companies and for engineering companies undertaking design, afterall who does not undertake a HAZOP on a new process? There are design principles and good practices used to design instrumentation loops, and Cause and Effect Diagrams (CED) are likely to exist for a process or a new project. For operating facilities, plant operating procedures, experience and training should ensure that personnel know what the trips do and the operations / maintenance people should test the trips based on some form of criteria.

Keywords: Functional Safety; IEC 61511; SIL; Implementation; lessons

Key Issues in Implementation

There are two common areas of ineffectual implementation of the standard. The first issue is a failure to understand that "SIL" is a risk reduction management system. The second area of concern is a failure to recognize that Functional Safety is a "process".

Implementing IEC 61511 therefore requires a clear understanding of the requirements of the standard and how its principles fit within existing structures and systems. Those new to the role, for example an instrument maintenance engineer with 2 – 3 days formal IEC 61511 training may feel exposed when faced with the task of "making it happen" for a site or project, particularly if there has been a delay between attending formal training and undertaking the process of implementation. It is often only at the implementation stage that detailed questions surface and further guidance is needed. For example, frequent questions have included:

- What is the difference between a Safety Instrumented Function (SIF) and the trip?
- What use is the CED to IEC 61511?
- What if a valve is not SIL (Safety Integrity Level) certified? And should procurement be limited to SIL certified valves as standard for all automatic isolation valves?
- Should every trip be tested every 6 months – and how much effort will this require and what supporting documentation should be prepared?
- How is process safety time estimated (process safety time is often defined as the time between the process parameter reaching the SIF action set-point and the occurrence of the hazardous event)?

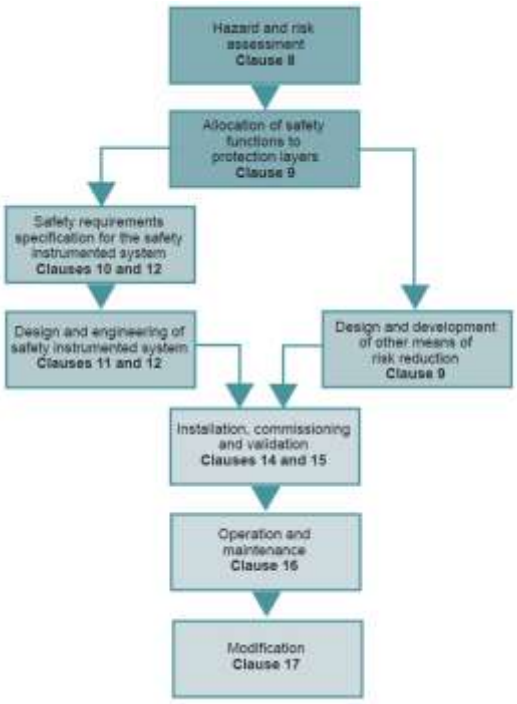
The above defines the general problem which can seem a complex task. The solution, in overall terms, is simply to follow to the structure of the standard. The standard is in essence a process for risk management, following generic risk assessment methodology as follows:

- Hazard identification, e.g. by HAZOP or similar tool;
- Consequence assessment, using some form of rating – in the process industries we usually only want to focus on infrequent high consequence events. This is usually done within the HAZOP process;
- Establishing existing risk controls. Again usually done as part of the HAZOP;
- Frequency assessment;
- Risk assessment & identification of additional controls to reduce the risk as required; and
- System to adequately maintain risk controls.

For the SIF there are additional key activities to maintain these risk controls:

- Installation and commissioning checks;
- Maintenance, inspection and testing; and
- Modifications.

The specific steps within IEC 61511 are given in the following figure.



- Hazard Identification
- Consequence assessment
- Establishing existing risk controls
- Frequency Assessment
- Risk Assessment & identification of additional controls to reduce the risk as required
- System to adequately maintain risk controls.

Initiating the IEC 61511 Implementation Process

The temptation may be to start where the site or a project has perceived strength. If the instrument engineer has this task then the perception could be that the CED may be the best place to start as it defines the actions for every trip system. This approach however has two key downfalls. First the CED contains a lot of non safety critical trips (for safety also read environmental or commercial impacts). Secondly the CED may not identify all the risk control measures required. To illustrate the point:

> Case A.
>
> A speciality chemical company has two complex reactor systems on a plant.
>
> CED Size: 40 inputs with 80 Outputs
>
> Inputs typically activate 6 or more outputs.
>
> Each output typically has 10 or so inputs.
>
> After a robust HAZOP and Layer Of Protection Analysis (LOPA) the SIF were defined as: 6 SIF with 1 input and 1 or 2 outputs. Of these 50% needed either a new input or new output (these were new instruments).

The number and size of the SIFs are much smaller than the CED, around 10% of the size. (For other process applications this may be a higher percentage).

Also new SIFs are needed which are not on the CED. This suggests that either:

- The earlier HAZOPs may have failed to identify some problems;
- The risk assessment (LOPA in this example) identified that further risk reduction measures were needed to meet the risk target which had not been identified in an earlier HAZOP (or similar process); or
- Process / plant changes had occurred and the change management procedures were not sufficiently robust to identify the increase in risk.

The above illustrates that the CED is not suitably sufficient in identifying SIF. Most critically it is not necessarily a good basis for risk management. The CED cannot identify new hazards or SIFs where these have not been identified before.

The above is a failure to recognize that functional safety is a "process". Like a chemical plant design project it has distinct steps which feed into one another and each must be well implemented or the complete project will fail. If the conceptual design has a flaw and it is only identified when it is commissioned then the effort to fix the problem may be considerable. Both plant design and 61511 are largely linear processes. Hence recognising the structure of IEC 61511 is important. Any existing assessments or studies are only useful if the input into the study is robust. Otherwise the old cliché is true: rubbish in; rubbish out.

Key learning point 1: the CED is often much larger than the SIF requirements and may not include all the SIFs dependent on the robustness of the HAZOP and risk assessment the CED is based on.

Key learning point 2: the implementation of IEC 61511 must follow the logical sequence in the standard.

Hazard identification and risk assessment

The level of detail and clarity of HAZOPs underpinning the process will have a significant impact on the quality of the implemented IEC 61511 system, and the efficiency with which it can be completed. Ideally in establishing the approach for a HAZOP, consideration should also be given to how it can best provide necessary input for IEC 61511 purposes. Adding consequence rating into the HAZOP, for example, enables HAZOP teams to easily identify the high hazard scenarios for further risk assessment using LOPA. The HAZOP needs to be sufficiently detailed to ensure that all the causes of a major accident hazard (MAH) are identified. This includes recording all valve and equipment tags. Identifying all the causes establishes the demand rate on the SIF.

Considerable efficiencies can be made in our experience when an integrated HAZOP / LOPA approach is used. Software is available which can be configured to copy data direct from HAZOP to LOPA worksheets for more detailed assessment. If the LOPA is undertaken within 2 to 3 weeks of the HAZOP using the same team, the time required for the LOPA can be dramatically minimised.

Key learning point 3: the HAZOP / LOPA processes should be fully consistent with each other (much of the HAZOP information is useful for the LOPA) and, where integrated significant time savings may be achieved.

The SIL Determination Process

The LOPA team is often best place to define the exact functionality of any SIF identified, if competent and well selected to represent all disciplines. The team should know exactly what it must do to make the process safe and this is an excellent opportunity to capture this requirement.

Two approaches are commonly used for SIL determination: Risk Graph and LOPA. Risk Graph is sometimes seen as a more rapid, screening tool but can lead to conservative estimations.

LOPA is often considered more rigorous but perceived to be time consuming by some. Measures can be taken to address some of these issues, for example Risk Graph (as described in IEC 61511) can be made more sophisticated but this simply makes it more time consuming and similar to LOPA. A very effective mechanism to reduce time is to integrate the HAZOP and SIL determination process.

The SIL determination process itself has limitations. The timing of the sessions is important, as are the nature of the hazards revealed by a HAZOP. There is little benefit undertaking a SIL determination if the design needs to be reviewed as a result of the HAZOP, nor can SIL determination contribute to scenarios where the cause is long term such as corrosion where the risk needs to be managed through a suitable asset integrity program rather than a SIF. In addition very high consequence or interdependent events need a more detailed risk assessment, possibly using Fault Tree or Quantified Risk Assessment methods. For example, appropriate consideration of potential escalations may not be possible within a SIL workshop due to the complexities involved. If a fire or explosion could result in subsequently large fires or explosions which consequence should be assessed, the initial event or the final event? The probability (and significance) of an escalated event occurring may depend on a range of factors such as wind speed and direction and can become too complex for the HAZOP/ LOPA team to assess, and may be best considered in more detail outside of the workshop environment.

This also introduces the question of how to deal with general mitigation measures such as fire and toxic gas systems and blow-down systems. In some simple cases these could be incorporated into the SIL determination. However, for large or high pressure gas and oil processes the effectiveness of these systems preventing an escalation event must be very carefully considered. Again the complexity of the scenario may prevent the HAZOP/ LOPA team being able to complete the assessment without more detailed subsequent analysis.

Key learning point 4: the scope and limitations of the SIL determination methodology must suit the processes being studied. Where fire and explosion risks are considered the issue of escalation events must be well thought through and consistently applied. It may be that detailed quantitative methodologies are more useful in considering the benefits of fire and gas detection systems.

Target Risk Criteria

One key feature of the SIL determination process is the Risk Target. It should be considered in appropriate detail, justifiable and clearly defined. If these criteria are not correctly calibrated then the SIL target for every SIF will either be too low or too high. These risk target values will depend on the regulatory environment and / or the corporate approach to risk.

Key learning point 5: the risk criteria used in the SIL determination should be well thought through, justifiable and clearly defined.

Effective Safety Requirement Specifications (SRS)

The next step is to define the Safety Requirement Specification (SRS). This is often omitted yet is critical for definition and communication. Two case studies below illustrate the need for the SRS.

> Case B.
>
> On a 15 year old plant an item of equipment is protected by a high temperature trip, low feed flow trip and two instrumented pressure relief systems (a very low differential pressure and materials of construction issues prevent the use of conventional pressure relief valves being used). A SIL verification PFD calculation is undertaken by an experienced instrument engineer who had been involved in the plant design. A risk reduction factor of 5 is estimated which is considered low (by by 2 orders of magnitude) by the site process engineer. The discrepancy arises because the instrument engineer assumes all four trips are needed to make the plant safe. The process engineer knows this to be incorrect and that only one trip system or one relief system is required to make the plant safe. Case B assumes site operation in the early 1990s before the SRS concept was in place at the site.
>
> Case C.
>
> The SIF design has occurred before the SRS had been fully generated. The process engineer specified that the response time should be 0.5sec. This led to a useful discussion between the process and instrument engineers.

In the first case the instrument engineer knew what the SIF did, understood the process in general terms but the degree of redundancy in the SIFs had not been clearly documented. A key function of the SRS is to define the SIF or SIFs that make the plant safe. The level of redundancy must be clear. Other actions may also be specified which are not part of the SIF.

In the second case the initial process safety time estimate was extremely low and had to be revisited by the process engineer. The SIF could not respond in the available time. If the SIF cannot be designed to achieve all the necessary requirements of the SRS the process design should be reviewed and alternative risk control options generated.

The SRS requires all the interested parties (process safety, process engineering, instrumentation, and production, maintenance) to document and agree what is required of the SIF. This includes response time and the operator interface: alarms, reset requirements etc. For SIF test intervals the “default” case for 1 year may not apply. Oil installations, steel works and some processes (e.g. sulphuric acid plants) only have a main shut-down every 2 to 3years.

Key learning point 6: use the SRS as a communication tool to agree the SIF requirements with all the stakeholders.

SIL Verification

The SIF loop design must comply with the SRS. Then the SIL verification can be undertaken.

This is generally well understood in concept and most formal courses examine this requirement. There is the need to ensure both requirements (PFD and Architecture) are included in the verification. Again this should be well documented for auditing purposes and for future modifications if required.

Installation and commissioning

Installation and commissioning activities should be designed to check that the SIF complies with the SRS. Does the system function correctly? This should consider not only the pre-commissioning conditions (ambient temperature and pressure with no process fluids) but also, as far as possible, normal process conditions. For example if a valve closes on a high pressure flammable gas pipeline, can the functional test be replicated at high pressure with an inert gas before the process gas is added? If a SIF has a relatively short process safe time, how quickly does the system respond during the commissioning? If the response time is a few seconds validating this needs to be considered carefully, especially if the instruments and isolation valves are physically far apart? There is also a need to check reset requirements work for all SIFs.

For a SIF everything should go into more detail from design through installation and commissioning to operations/testing and modification. Hence the SIF installation and commissioning checks should be significantly more comprehensive than other instrumentation.

Key learning point 7: installation and commissioning checks on SIFs should be comprehensive and establish the SIF complies with the SRS in conditions corresponding as closely as practicable to normal operating.

Risk management system

The above describes some of the technical issues which need to be addressed when implementing IEC 61511. However, of equal significance is the need to recognise that this standard is in effect a risk management tool. This immediately leads to three conclusions:

- It requires a management system – it needs competent people, procedures and to following the structure of a management system (e.g. HSG 65);
- It is not the only risk management tool. It should be used appropriately; and
- Risk reduction is the primary function of the standard - any other benefits are subordinate to this purpose. As engineers we gravitate to technical nuts and bolts and can critically miss the "big picture".

IEC 61511 covers a range of activities from process design and process safety (HAZOP, SIL determination) though to Instrument design and ultimately maintenance. Operations also need to be strongly involved in the system. The key features of the functional safety management system are:

- Structured and unified, not a collection of disparate procedures followed by individual engineering disciplines;
- Follows the "Deeming cycle": Plan, Do, Check, Act. The activities must be designed to be audited (functional safety assessment). Performance must be reviewed (e.g. via Process Safety Performance Indicators, PSPIs); and
- Seen as a continuing activity and not just a project with a discrete activity, e.g. "calculate a few SILs". Testing, maintenance and control of modifications all need to be integral to the whole process.

Other issues such as competency and communication must be addressed.

Key learning point 8: there is a need for a full management system and not just a procedure to determine the target SIL and then verify it.

Ownership

Ownership and responsibility of the management system is a difficult choice. "Safety Instrumented Systems" automatically suggests it falls within the scope of either the "Safety" or "Instrument" departments, probably the latter. However, it is very much a cross functional activity. It requires Process design, Process Safety (or Technical Risk Management), Instrument design, Operations and Instrument Maintenance. But for some sites these functions may be small with limited resource and level of competency.

Who should manage the system? The initial phases of IEC 61511 are process safety lead but the main design and on going activities are predominately instrumentation tasks. Who ever, is responsible for the functional safety management system must be senior enough to be able to influence all the disciplines affected by the requirements of the standard. The individual must also have a sufficient grasp of the entire scope of the standard and have a secure understanding of risk management.

The management system is required to ensure that all the necessary parties are involved at the correct time and in event of non-compliance that the right individual is informed to assess and correct the problem.

Critical to the overall effectiveness of the functional safety management system are clear consistent, unified procedures.

Key learning point 9: the functional safety management is a cross functional activity. No one individual will have the skill set to execute all the procedures involved. The management system must involve a range of functions at the correct time in the procedure.

Functional Safety Assessments

A Functional Safety Assessment (FSA) is in effect the audit process within the functional safety management system. It is intended to assess if each step of the process is compliant with IEC 61511. The fundamental requirement here is that there is sufficient documentation to justify and explain what has occurred. For operating sites or engineering projects there is often a tendency to document a result without detailing the method, demonstrating competency of those involved and listing the key inputs to a report. One simple example is that the scenario used in the LOPA should have the HAZOP scenario reference included demonstrating the link between the hazard identification process (HAZOP) and the risk assessment process (SIL determination).

Key learning point 10: the functional safety management processes should be sufficiently well documented that an external auditor (functional safety assessor) can assess compliance against the standard.

Conclusion

The above issues have been encountered at a range of facilities and both design and operational phases.

Each of the issues can be readily solved with structured planning and considered attention to the process.

The implementation of IEC 61511 must include all the elements of the standards. A management system must be developed to provide a consistent, unified approach which can be followed by all involved.

The various elements of the management system must be implemented in the sequence given in the standard. It may, however, be that this can be scheduled over a period of time providing the phases of implementation are in the correct sequence. Care must be taken to ensure that any modifications undertaken are suitably controlled and included in the functional safety management systems. For functional safety every activity must work or the desired risk reduction will not be achieved. The chain is only as strong as its weakest link.