Session Ten:

The importance of a clear Safety Requirements Specification as part of the overall Safety Lifecycle

Andy Crosland
SIS Business Development Manager, Europe – Emerson Process Management

Abstract

The need for specifying requirements clearly is recognised best practice for most automation projects, so it makes sense to be extra-vigilant when dealing with safety systems. Many project specifications cover functional and user requirements in great detail, but often miss the key safety considerations set out in IEC 61511. As well as the obvious benefits of a clear specification from the outset, the Safety Requirement Specification (SRS) is the essential reference document for the mandatory IEC 61511 Safety Lifecycle task of SIS Safety Validation. You will be shown the key SRS considerations, particularly why this information is so important at Validation time.

Introduction

Properly designed Safety Instrumented Systems (SIS) are made up of highly reliable components with a Probability of Failure on Demand which is very low indeed; low enough such that the risk reduction provided by these Safety Instrumented Systems brings down the risk in the processes we operate to a tolerable level. However, choosing reliable equipment is only part of the story. There are still many opportunities for human error in the specification, design, implementation and installation of all parts of a Safety Instrumented System.

Failures of the equipment are often referred to as Random failures; breakdown, wear-out or expiry of components within the equipment that lead to the sensor, logic solver or final element failing to either a safe or a dangerous state. Human errors however are referred to as Systematic failures.

Of course there are opportunities also for human/systematic failures in the design and manufacture of the standard product components we use within Safety Instrumented Systems. However, those components which have been designed and independently certified in accordance with the requirements of IEC 61508 should have minimised this risk by observing *Techniques and measures to control systematic failures caused by hardware and software design* given in IEC 61508-2 Table A.16, and specific measures for controlling safety-related software given IEC 61508-3. Devices which have correct evidence of Proven-in-Use reliability in accordance with IEC 61511-1 Clause 11.5.3 (prior use) also minimise this risk.

But even when the correct components are chosen with the required safety reliability, there remains significant potential for human/systematic failures in the way those components are brought together and configured.

In the UK, and in many other European Countries, the IEC 61511 standard is recognised as defining good engineering practice for the implementation of

Safety Instrumented Systems. This standard captures knowledge and experience from past projects, and by following IEC 61511, practitioners are guided to ensure that appropriate equipment is selected for the components of the SIS and with a system of procedures, checks and guidelines designed to minimise the potential for systematic failures or human error remaining undetected in the final SIS.

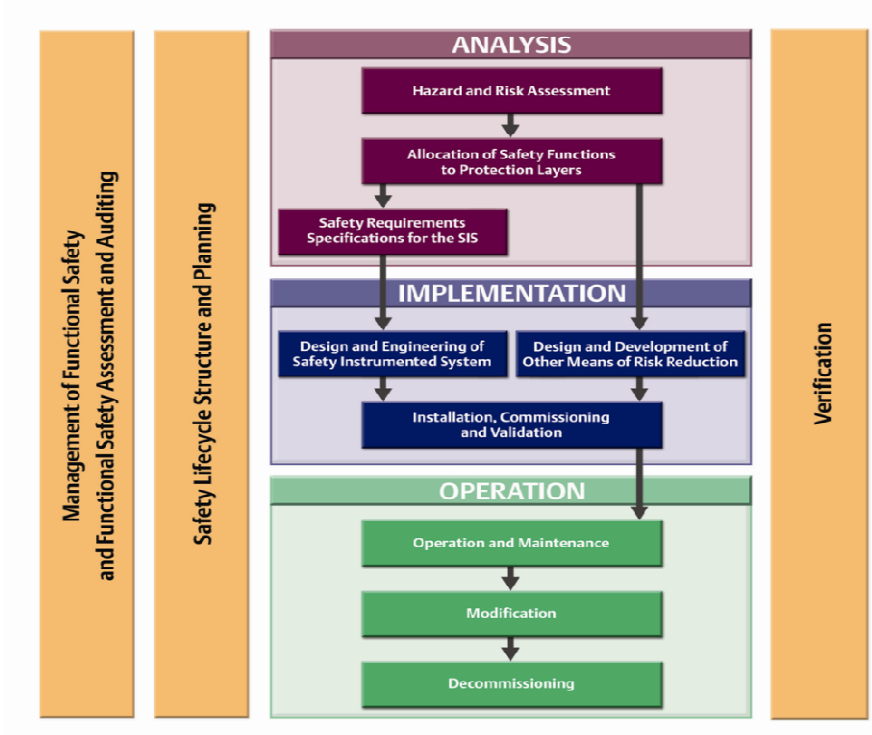
IEC 61511 sets out a number of key concepts, one of which being that of a Safety Lifecycle; a structured approach which the standard itself defines as:

> *necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the initial concept phase of a project, through design, implementation, operation and maintenance, and finishes when all of the safety instrumented functions are decommissioned and therefore no longer available for use*.

Within the Safety Lifecycle, a number of key Phases are defined, including:

- Hazard and Risk Assessment
- Allocation of Safety Functions to protection layers
- ***Safety Requirements Specification*** for the safety instrumented system
- Design and Engineering of the safety instrumented system
- Installation, Commissioning ***and Validation***
- Operation and Maintenance
- Modification
- Decommissioning

The SIS Safety Lifecycle is represented diagrammatically as shown below. This diagram is based on IEC 61511-1 Figure 8.



We can see clearly that the Safety Requirement Specification (SRS) is sufficiently important within the lifecycle to be represented as a complete lifecycle phase, and specific clauses of the standard dedicated to it. Further, we will discuss later in this paper the importance of the SRS when it comes to the mandatory task of SIS Safety Validation; the final checks that the SIS meets all safety requirements captured in the SRS before the identified hazards are introduced to the process.

Observations from a Safety Systems supplier

As manufacturers and suppliers of complete safety instrumented systems, our project teams have seen many specifications for a variety of projects around the world. As part of Emerson's certified processes for SIS implementation projects, a checksheet is used to work through the specification documents provided by the client, to check that the essential required elements of a Safety Requirement Specification have been covered by the documentation received.

Not surprisingly this checklist maps clearly onto the requirements for an SRS set out in the IEC 61511 standard, however it structured in a way that considers:

- Non-functional SIS Requirements, such as codes and standards and the environmental conditions
- General Functional SIS Requirements, applicable to all Safety Instrumented Functions (SIFs) within the SIS, and to the external and operator interfaces with the SIS
- Specific Functional SIF Requirements, for each SIF
- Basis of Design

As a general observation from our engineering teams, it is clear that this checksheet process often reveals deficiencies in the information provided. This usually prompts discussion between vendor and client to ensure that the key safety requirements relevant to the vendor's project scope are clarified and documented at the outset.

Vendors of Safety Instrumented Systems rarely receive an SRS which truly addresses all requirements of IEC61511. We are sometimes encouraged by documents which carry the title "Safety Requirement Specification", but are often disappointed by the detail within.

Specifications often focus heavily on the safety logic definition, which of course is one aspect which must be specified. However, documents such as Cause & Effect diagrams or Functional Logic Diagrams rarely address the points called for within the IEC 61511 specification for an SRS. Notes are often added to Cause & Effect diagrams in an attempt to clarify the requirements. However, multiple notes can lead to confusion and mis-interpretation, or in other words precisely the kind of systematic error the IEC 61511 standard tries to avoid.

Cause & Effect diagrams give a useful overall picture of the safety logic, but they do not align well with the SIF-based approach set out by the standard.

One common concern is that many specification documents with the title SRS or otherwise, contain large amounts of information which is not directly relevant

to functional safety. Whilst a detailed specification of HMI requirements on graphical representation of the SIS status, for example, is necessary for overall project implementation, it does not impact safety. Such detailed functional requirements are better left for other documents.

One final observation is that SRS's received from clients tend to focus heavily on the requirements for the logic solver. However the logic solver is only one part of the overall SIS. As we will see later, there are many requirements relevant to the sensor and final element parts, which have a very significant potential to impact on functional safety and therefore require documentation and attention. Whilst these requirements may not be directly relevant to a vendor who's scope is to design and build a SIS Logic Solver only, the safety lifecycle still requires that an SRS exists for the complete SIS, including sensors, logic solvers and final elements. Documents are often structured around contractual arrangements for delivery of each part of the overall SIS. But who delivered what means little from a safety lifecycle viewpoint during the 10-20 years or more operational phase.

What to include in a Safety Requirements Specification

The IEC 61511 standard sets out quite clearly within Clause 10 the requirements for creating a Safety Requirement Specification. Further requirements are specified within Clause 12.2 for a Software Safety Requirements Specification derived from the overall SRS; relevant only to programmable logic solvers, which of course form the heart of most modern safety systems.

The standard requests that the SIS requirements should be expressed and structured in such a way that they are:

- clear, precise, verifiable, maintainable and feasible; and
- written to aid comprehension by those who are likely to utilize the information at any phase of the life cycle

One of the important words missing here is the word "concise". Safety Requirements Specifications should also be concise, and should focus only on those topics that are relevant to achieving functional safety. Considerations such as HMI requirements, electrical wiring and tagging standards, cabinet dimensions, etc., are all distractions which have the potential to divert attention from the important safety topics. Such engineering details should be moved into a User Requirement Specification or Functional Design Specification, which is a different document with a different purpose.

Clause 10 of IEC 61511 lists a number of things which *shall* be included in the SRS; use of the word *shall* conveying the fact that these are mandatory requirements of the standard for every project. There are 27 requirements presented within Clause 10 as a bulleted list, and to repeat all of them here is not helpful. However, some of the common items which are often poorly addressed within client specifications are listed below:

- *a definition of the safe state of the process for each identified safety instrumented function*

- *a definition of any individually safe process states which, when occurring concurrently, create a separate hazard (for example, overload of emergency storage, multiple relief to flare system)*
- *response time requirements for the SIS to bring the process to a safe state*
- *requirements for overrides/inhibits/bypasses including how they will be cleared*
- *identification of the dangerous combinations of output states of the SIS that need to be avoided*
- *the extremes of all environmental conditions that are likely to be encountered by [all parts of] the SIS shall be identified*

Prior to the SRS development, a Hazard and Risk Assessment of the process should have been completed; often taking the form of a HAZOP (Hazard and Operability Study). Much of the documentation created within the HAZOP will not be relevant to the Functional Safety requirements. Firstly, many of the topics discussed are operability rather than safety issues. Secondly, of the Hazards identified, some will have risk reduction measures in place which are sufficient without the need for a Safety Instrumented System. However, for those Hazards which do require risk reduction from an SIS, there may well be valuable information about the nature of the hazard and the process and environmental conditions which may affect the SIS. This information, where relevant to safety, should be captured and consolidated within the SRS. Few projects refer back through the many pages of a HAZOP report at the design, build, test, install phases.

Re-stating the requirement from above, the SRS should be *written to aid comprehension by those who are likely to utilize the information at any phase of the life cycle.* The SRS seems a sensible place to consolidate safety-related data from the HAZOP where relevant to the SIS.

Following on from the Hazard and Risk Assessment, some form of analysis should have been carried out to determine which Hazards do indeed require instrumented safety for risk reduction; the Allocation of Safety Functions to protection layers (or SIL Allocation for short). One common form of assessment is the Layers of Protection Analysis (LOPA), but there are others such as Risk Graphs, etc. They key point is that these documents may also contain nuggets information which it is important to capture in the Safety Requirement Specification.

For example, the LOPA analysis might identify contributions to the overall risk reduction from BPCS or operator actions in response to alarms, as protection layers independent from but relevant to the SIS. Similarly, restrictions on access to hazardous areas to reduce occupancy, or availability of breathing apparatus in the event of a toxic gas release may be specified.

The Safety Requirement Specification is a good place to capture this information, so that these things can be checked at the time of SIS safety validation.

The Grey Area

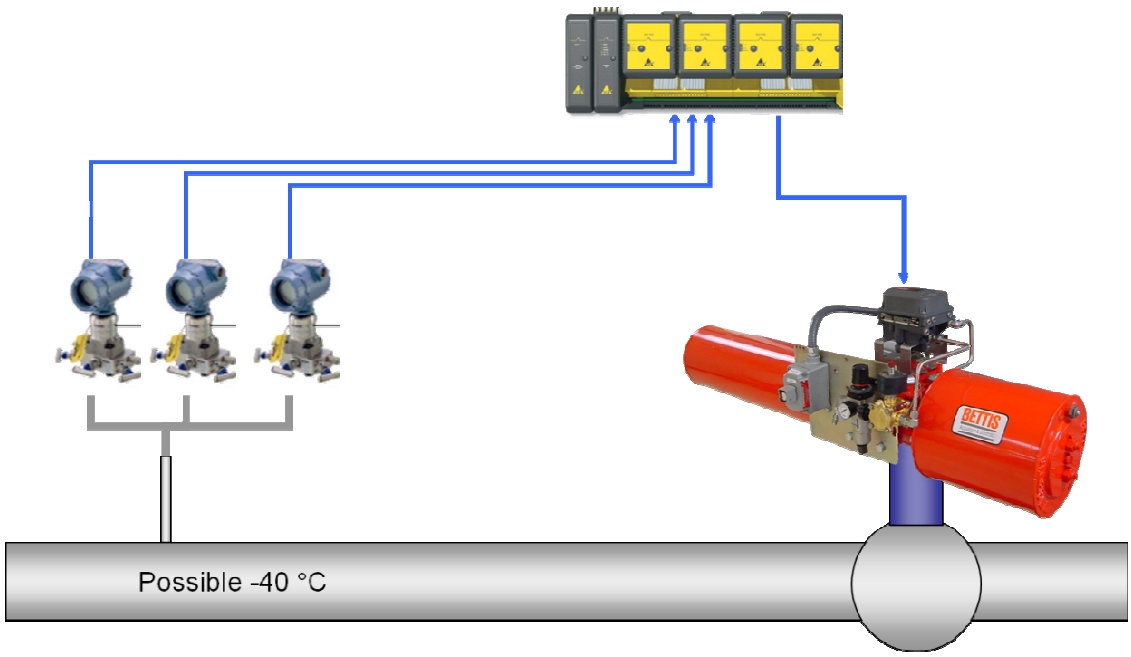
What is often the case is that project specifications leap straight into engineering details, following on from the Hazard Analysis (HAZOP) and SIL Allocation (e.g. LOPA) phases, leaving the important SRS phase as something of a grey area.

In reality, the practicalities of meeting project schedules often lead to engineering details being worked on in parallel with completion of the analysis phases. By creating a Safety Requirement Specification which consolidates the results of the Hazard Analysis and SIL Allocation once complete, this gives an opportunity to ensure that all safety requirements have been captured by any interim detail engineering. It also provides a basis for validation, to ensure that no errors have been made in the preliminary designs, and implemented in the SIS.

Examples

Let's take a look at a few examples to illustrate some of the issues of concern.

Consider first a simple safety function which measures pressure with 3 transmitters voted in a 2oo3 (2 out of 3) configuration, to close a valve if the pressure within a process pipe is higher than the trip point.



(1) First of all considering the environment, and in particular note that the process fluid (a gas stream) has the potential to go down to temperatures as low as *minus* 40 ℃. The process design specifies lagging on the pipe, to minimise condensation and ice formation. However the process engineer has commented that temperatures as low as -40 could cause failures of the valve to operate, and suggests not lagging the valve itself to mitigate against this.

Where should this important piece of information be captured? Hopefully it will be recorded as a note on one of the many instrument datasheets on the project and/or perhaps a note on the P&ID diagram. But even if those notes are there,

will they be seen by the appropriate people and will their relevance to safety be recognised?

By capturing the fact that the valve should not be lagged in the SRS, this can easily be added to the checklist when the valve is inspected during SIS Safety Validation. Further, the validation planning can consider whether it is feasible to test the valve's operation at the extreme process temperatures, or at least to acknowledge the limitations of tests at higher/ambient temperature.

(2) Now consider the Pressure Transmitters themselves. It is common practice to use impulse lines on pressure and DP flow service. These are small bore pipes that to connect the pressure sensor to the point in the process where pressure is to be measured. The use of impulse lines can cause problems which lead to an incorrect measurement. Problems include blockage or plugging of impulse lines either by high-viscosity liquids, entrained solids or perhaps in this case by freezing of condensed gases. This might lead to a complete inability to detect pressure change, or a delayed response. Either could cause a failure of the safety function, if the pressure transmitter cannot detect the high pressure within the required process safety time.

    To mitigate against this there are a number of potential strategies such as:

    (a) Use of a heat trace to maintain a higher ambient temperature, reducing the risk of condensate formation and/or freezing, or

    (b) Using an intelligent pressure transmitter which has the ability to detect plugging of impulse lines, thereby moving a potentially dangerous failure from un-detected to detected.

If the safety case relies on avoidance and/or detection of plugged impulse lines, then it is important that the heat trace is fitted and working, and that the diagnostics feature of the intelligent transmitter is enabled. Furthermore, the IEC 61511 standard will require that this diagnostic alarm shall be subject to appropriate proof testing and management of change along with the rest of the SIS, even if the alarm is generated by the BPCS.

The Safety Requirement Specification should record the requirements for avoidance of failures due to plugged impulse lines, so that the presence of these measures and the operation of any diagnostic alarm can be confirmed during validation.

(3) The diagram of our safety function suggests that the 3 pressure transmitters are connected to a common tapping point on the process pipework. This is an artificial arrangement to illustrate a point. In practice, multiple tappings (one per transmitter) are more likely. If the plant was built this way, the common tapping line could itself be vulnerable to impulse line plugging. If so, then we also have here an illustration of a Common Cause failure, since plugging of this common line would affect all three transmitters simultaneously.

One of the requirements in IEC 61511 is that the Safety Requirement Specification shall identify and take account of common cause failures. It may have been decided in one of the preceding design documents that individual tappings with separate impulse lines are necessary to avoid common cause.

This information may be buried as a note on one of many instrument datasheets. It seems clear that this should be documented within the SRS so that SIF design verification (SIL calculations) can take allocate an appropriate common cause β-factor, and that later at SIS Safety Validation phase the presence of separate impulse lines can be checked when the installation is inspected.

An Example of Fire Detection Systems

Let's consider a different example from a Fire and Gas application. There is often a debate as to whether Fire and Gas detection systems should have any SIL rating applied to them or not, but even so they are usually implemented as safety instrumented systems. In many cases, the primary purpose of a Fire and Gas system is to warn personnel to evacuate the facility, after a hazardous event has already occurred. This is not so easy, of course if the facility is an offshore oil and gas platform or vessel, such as an FPSO (Floating Production Storage and Offloading), where fire fighting could be essential to survival of the crew; abandonment being the last resort and one which carries its own risks.

On one such project, our engineers were presented with a Cause & Effect diagram as the specification for the project. This is quite typical, but experience shows that Cause & Effect diagrams cannot possibly address all of the requirements of a full Safety Requirement Specification. Often, there are many notes attached to the Cause & Effect chart, and the notes often grow in number as clarifications are discussed during project execution.

The fire water system on this project comprised a ring main which could be fed by multiple pumps in different locations. There are several off-takes from the ring main, delivering fire water to deluge affected process areas, controlled by the Fire & Gas system.

The Cause & Effect chart contained a simple note related to the fire water pumps which said "Pumps will start on demand". What this didn't convey was the requirement for the number of pumps to be started to be matched with the demand for fire water, depending on how many areas require deluge activation. If demand were to exceed available supply, due to pump failure, then demands should be isolated on a priority basis, with an operator override system to override the automatic selection if necessary. Further, there was a risk that if too many pumps were started, the fire water ring main could be damaged, which could potentially leave the fire water system unable to carry out its safety function. However, the operators should always be able to override the system's selection of which pumps to start.

As a result of clarifications, the simple "pumps will start on demand" note was expanded into a document of several pages, to clearly specify the requirements for the fire water system.

This example illustrates two other topics which are mandatory within an IEC 61511 compliant SRS, which are the need to consider if multiple demands could lead to an additional hazard (multiple fire pumps activating damages the fire water ring main), and the need for overrides to be clearly specified.

A structured approach to SRS development

To tackle the issues described above, a structured approach is proposed, whereby information that is available from preceding Safety Lifecycle phases and other design efforts can be collated into one consistent documentation set, known as the SRS. The SRS may indeed be a single document, or a collection of referenced documents.

The proposed structure for each SRS is outlined below:

First a **Project Overview** provides an introduction to the project and the process, and where appropriate may also contain a limited process description to aid with the understanding of the main processing units, their interconnection, the nature of operation (batch/continuous) and the most significant hazards present. Information regarding the process fluids or chemicals and their potential to harm people, equipment or the environment may also be captured.

Non-Functional Requirements are then documented, which capture such things as:

- which codes, standards and legislation may be applicable to the process and to the SIS implementation
- environmental conditions and any implications for the SIS equipment, plus utility supplies (power, instrument air, etc.)

General SIS Requirements capture all things which are relevant to the overall SIS, rather than to specific individual SIFs within the SIS. Topics include:

- process modes of operation (start-up, running, controlled / normal shutdown, emergency shutdown, maintenance, etc.)
- SIF modes of operation (demand / continuous), and the protection principle being used (de-energise to trip / energise to activate)
- sources of common cause failures
- instances of concurrently occurring safe states creating hazards
- describe in principle (not in detail) all interfaces between the SIS and other systems and the operators, including HMI for operation, maintenance and diagnostics, plus general requirements for manual shutdown
- actions necessary to achieve or maintain a safe state if the SIS detects a fault through diagnostics

SIF-Specific Functional Requirements should be captured in the form of a structured narrative which describes the hazard, describes how the hazard is detected and sets out the actions the SIS must take to bring the process to its defined safe state. The Safety Integrity Level (SIL) and the required response time should also be specified.

The role of the Consultant

The task of creating the Safety Requirement Specification is not only a documentation exercise. It is an opportunity for an independent consultant to

question the information available, and to clarify any points necessary, to make sure that the requirements for the safety instrumented system truly are well understood.

As one example, the SRS development process should include a systematic tag-by-tag review of the process and environmental conditions each field device is likely to encounter. Consider how extremes of temperature and pressure, or perhaps the corrosive or abrasive nature or other properties of the process fluid, might affect the device's ability to perform its safety function within the overall SIS.

The selection of an appropriate SRS author should be considered carefully. The task is often left to the controls engineer who wants to use existing design documents as much as possible and will focus on the solution and how it works. As safety engineers we should focus on how things can fail; quite a different approach. The process designers might not be the right people either, as they are to closely involved and may assume incorrect levels of knowledge in the reader of the SRS.

Often the protection means are to an extent designed in the SRS therefore the SRS author should understand the requirements of SIF Design and SIL Verification, considering fault tolerance with sufficient redundancy of equipment and actions to achieve the desired Safety Integrity Level.

The SRS is a special document about safety

It is common practice (and good practice) on many sites that access to safety systems equipment is controlled differently from non-safety equipment, such as the BPCS. Even with an integrated control and safety system, safety logic solvers are often installed in separate cabinets with different keys. The system should also make provision for different, restricted access controls to the safety system's configuration software, to prevent unauthorised changes.

Generally safety systems equipment is clearly labelled as such, often brightly coloured to let people know, just like in nature, that it is dangerous to interfere.

The same principle should be applied to safety system documentation, particularly those documents which have a potential to affect whether functional safety can be achieved. Documents such as the safety requirement specification should be given elevated status, as being safety-related. Whilst there may be many changes and revisions to normal project documents, modifications to the SRS need much more careful consideration.

SIS Safety Validation

At the end of the SIS implementation part of the project, when all of the detailed engineering has been completed to design, build and install the SIS, IEC 61511 requires a mandatory activity called SIS Safety Validation. This should be carried out after installation and commissioning of the complete SIS (sensors, logic solver, final elements), and before the identified hazards are introduced to the process.

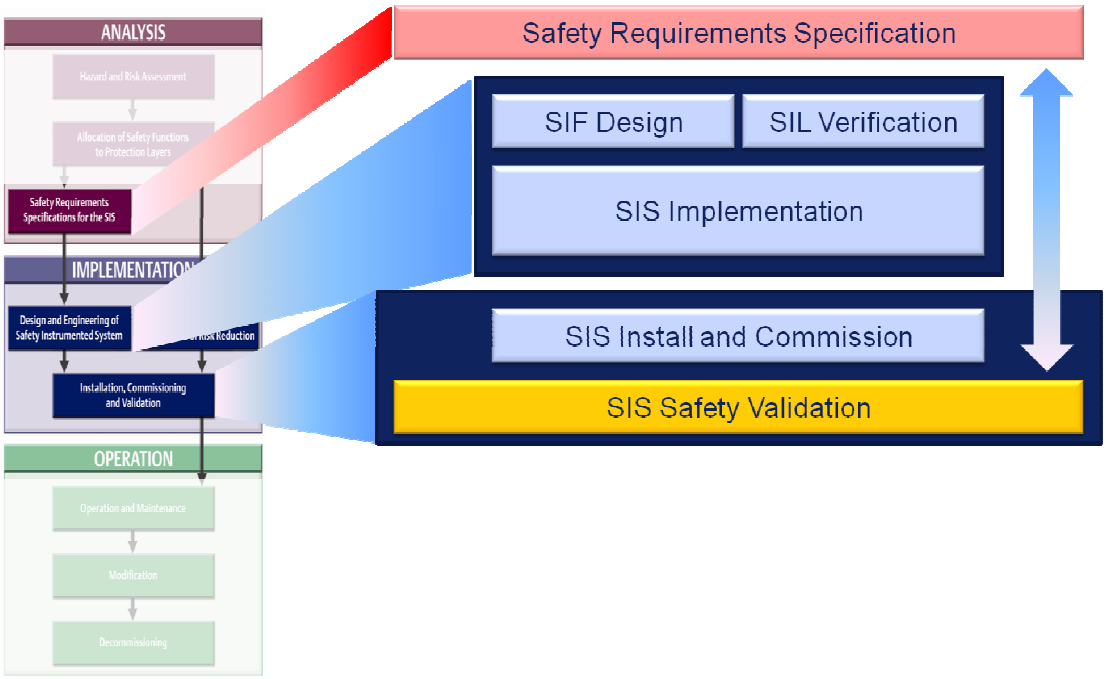
It is disappointing that the safety lifecycle diagram shown earlier has just one box for "Installation, Commissioning and Validation". This tends to

de-emphasise the "*and Validation*" part of the task. However, there are quite clearly two separate clauses within the text of the standard; Clause 14 dealing with Installation and Commissioning, and Clause 15 dealing with the mandatory task of SIS Safety Validation.

The standard tells us within Clause 15 that: "*The objective of the requirements of this clause is to validate, through inspection and testing, that the installed and commissioned safety instrumented system and its associated safety instrumented functions achieve the requirements as stated in the safety requirement specification.*"

So validation includes both inspection and testing of the SIS equipment, and it is important to note that our reference for Validation is the Safety Requirement Specification. No other documents are mentioned here, so we should not be referring to the HAZOP or LOPA study reports, or the Cause & Effect Diagrams, or any other detailed engineering documents.

The diagram below is an attempt to illustrate the importance of the Validation step referring back to the project Safety Requirement Specification, as a means to trap any errors which may have been made during the intervening detailed engineering stages. If we validate against lower level detail design documents, we are simply validating that the errors those documents may contain have been implemented in the SIS.



The SIS Safety Validation provides confirmation that the necessary risk reduction is in place prior to introducing the hazards, and it should do this with reference to the SRS which is a clear, concise, single source of all information relevant to functional safety. By carrying out these high-level checks in this way, any human error in lower-level design can be detected.

So in our examples listed earlier, several items were mentioned which should be included within the SRS and which should be checked at Validation time, these include, for our simple SIF example:

- Confirmation (by inspection) of the Heat Trace installation on the pressure transmitters, and of the process connection arrangements
- Testing of the Plugged Impulse Line diagnostic alarm
- Checks that the pipework lagging has not also encapsulated the valve, and where practical tests of the valve operation at process temperature extremes.

And for our Fire and Gas example:

- Checks on the pump selection logic, and
- Checks on the operator override mechanisms to force a pump to start or a deluge valve to open

Verification or Validation

One final topic is an attempt to clear up often-heard confusion between two words which are very similar in common use, but which have quite different meanings in the context of the IEC 61511 standard.

In common use, verification and validation both imply some form of checking or confirmation that something is correct. However, within IEC 61511, verification is something which must be done for all phases throughout the safety lifecycle, whereas validation is itself a lifecycle phase (and must therefore itself be verified).

The standard makes numerous references to requirements for verification within, and has a whole clause (Clause 7) specifically about the need for ongoing verification.

Indeed we mentioned earlier one specific, specialised verification task, known as SIL Verification. This is a confirmation using modelling and calculation techniques that the reliability of the equipment chosen, in the proposed configuration is sufficient to meet the target SIL level for the proposed SIF.

Validation is a specific activity at the end of the implementation phase of the project, to confirm that that the SIS is installed and functioning correctly.

SIL Verification and SIS Validation are clearly two very different activities, but with titles that understandably cause confusion.

The following definitions are taken directly from the IEC 61511 standard, and may help to clarify further:

validation

> *activity of demonstrating that the safety instrumented function(s) and safety instrumented system(s) under consideration after installation meets in all respects the safety requirements specification*

verification

> *activity of demonstrating for each phase of the relevant safety life cycle by analysis and/or tests, that, for specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase*

We see clearly that Validation is an activity that occurs once, at a specific time in the Safety Lifecycle; Verification is an ongoing activity for each phase of the lifecycle.

Conclusions

Even if we use reliable (certified, or proven in use) components, things can go wrong with the design and implementation of our SIS, due to human error during the project.

The international standard IEC 61511 is recognised good practice for the implementation of Safety Instrumented Systems in the process industry. By following this standard, the effects of human error can be minimised.
IEC 61511 sets out a safety lifecycle model within which the requirements for a Safety Requirement Specification are clearly defined. However, the detail of those requirements is often neglected in specification documents presented to SIS vendors as the basis for implementation.

The Safety Requirement Specification should consolidate information from preceding lifecycle phases where relevant to the functional safety provision by the complete SIS, including sensor, logic solver and final element parts.

The SRS should contain all information necessary as the basis for the mandatory lifecycle phase of SIS Safety Validation; an inspection and test of the installed SIS prior to introducing the process hazards. Validation should be based on the SRS, not on intermediate lower-level design documents, so that any errors which may have been made in the creation of those detail design documents are detected by the validation, rather than becoming a part of the installed SIS.

Validation should not be confused with Verification, which is an ongoing activity throughout all phases of the safety lifecycle.

Acknowledgements

Russell Cockman, SIS Consultant, Europe

Rafael Lachmann, SIS Implementation Manager, Europe

Glossary

SRS	Safety Requirement Specification
SIS	Safety Instrumented System, comprising of sensors, logic solvers and final elements
SIF	Safety Instrumented Function; an SIS implements one or more SIFs
SIL	Safety Integrity Level; each SIF has a target Safety Integrity Level, which is a number from 1 to 4, indicating increasingly stringent requirements for risk reduction
BPCS	Basic Process Control System; often called the DCS (Distributed Control System), or the PAS (Process Automation System). Basically, those parts of the overall system which are not qualified in accordance with the IEC 61511 standard.
HAZOP	Hazard and Operability study; a commonly-used form of Hazard Analysis
LOPA	Layers of Protection Analysis; one of several methods documented in IEC61511-3 for determining the required SIL level of a SIF during Allocation of Safety Functions to protection layers (SIL Allocation).

References

[1] IEC 61511 Parts 1, 2 and 3

[2] IEC 61508 Parts 2 and 3

[3] Detection of Plugged Impulse Lines Using Statistical Process Monitoring Technology, Dave Wehrs, Emerson Process Management