The importance and impact of a good SRS - it's not just about the cause & effects

John Walkington, Suresh Sugavanam, Stuart R Nunns

Safety Lead Competency Centre Manager, ABB UK, john.walkington@gb.abb.com, Safety Lead Competency Centre Functional Safety Consultant, ABB UK, suresh.sugavanam@gb.abb.com, Safety Lead Competency Centre Managing Consultant, ABB UK, stuart.nunns@gb.abb.com

Keywords: Safety Requirements Specification.

Abstract

This paper will review the implications arising from the release of the safety requirements specification (SRS) to the supply chain relating to issues such as safety functionality/integrity, assumptions made or not made, contractual and requirements creep and where one such implication is that a functional specification based on just a cause effect is not sufficient for compliance to the recommended safety standards.

1 Introduction

Defining what's required to deliver optimised safety instrumented systems (SIS) in process industry projects can be incredibly complex, whether they're new builds, upgrades or expansions (see figure 1). Accordingly, while everyone is keen to ensure that whatever's in place, at the end, the process presents as little risk as is practicable. Precisely, what that means in terms of safety system requirements at the outset of the project, can lead to potential 'gaps' in critical information requirements, that may manifest themselves in a detrimental way at a later date in the project delivery lifecycle or eventually whilst the plant is in the operational phase.

For example, the hazard identification study of a proposed project might identify the possible danger from a flammable storage tank overfilling with the potential to result in a pool fire and/or explosion. As a result of the related risk assessment of the hazardous scenario(s) identified, Instrumentation engineers will naturally be expected to provide suitable instrumented protection to prevent that happening in accordance with some form of target safety integrity and functional performance.

In the past, an individual engineer might well have used a particular type of high-level prevention system based on a previous safety instrumented function (SIF) project design as a default solution. This might for instance, include a proof test frequency based on previous Asset Owner maintenance expectations that aligned with practical resource availability from within the on-site maintenance team.

Invariably due to time and resource pressures, the temptation may well be to simply use the same 'prescriptive' approach in any new project, but by doing so, this could well result in an expensive mistake further down the line.

If safety systems are over-specified, they're likely to cost more upfront, and the extra complexity they introduce will require more operational management and maintenance once commissioned, pushing up the OPEX running costs over the lifetime of the plant.

By contrast, the consequences of under-specification can be much more serious because the safety system may well be inadequate and unable to provide the correct level of risk reduction and one that has the potential to result in a hazardous incident.

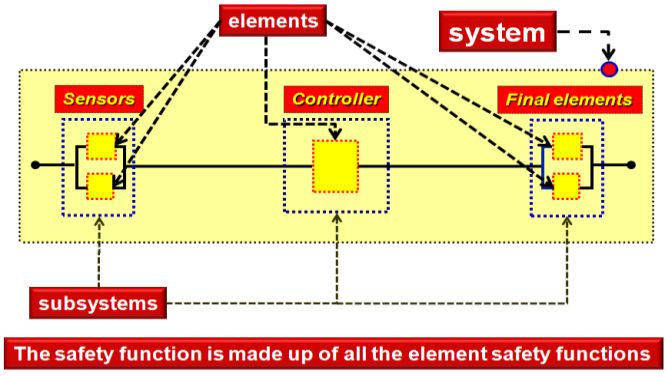

Figure 1 Designing the SIS and SIF's

2 Developing a safety requirements specification prior to design and engineering:

A key technical management requirement for the Asset Owner is the potential mis-match between the hazard and risk analysis information and the development of the safety requirements specification prior to the design and engineering of the safety related system.

The introduction of Edition 2 of the IEC61508:2010 [1] functional safety standard gives a higher priority to defining a suitable, dedicated safety requirements specification (SRS) for each project. It introduces a formal phase (Phase 9)

between the conclusion of the hazard analysis phase of a project and specifying particular SIS requirements prior to the design and engineering phase.

The SRS is intended to bring together all the information necessary to make sure that any SIS provides the right level of performance and risk reduction without being overly complex or expensive.

However from the authors' experiences to date, many Process Owners and Engineering Contractor organisations continue to omit the sort of information that needs to be included in a detailed SRS especially if it is to meet 'due diligence' requirements regarding traceability and any assumptions made i.e. as a minimum it needs to comply with expected 'industry good practice' requirements.

In some cases, project scheduling activities tend to force the supply chain into making formal bid responses well ahead of any detailed technical discussions based on a qualified and accurate SRS and therefore it could be argued at this stage in the proceedings, the intent for the SIS is to 'design by assumption'. Here the technical outline of SIS requirements against a very basic automation philosophy document (that again can be agreed 5-6 months before the project Hazop actually commences) is confirmed in principle before any detailed hazardous scenarios are identified (what about the correct derivation of the Target SIL for each SIF you ask?)

This is even more noticeable for large multi-contractual projects where the tendency is to worry about the SIS requirements further down the project plan as part of the overall project deliverables. Even so, such larger capital projects where the duration of the project lifecycle can span several years, it will be essential that the SRS can be prepared for different stages of the project's technical/commercial process and become an iterative safety related document. This can typically constitute an initial stage SRS where only preliminary SIS requirements about the safety system are available from the Asset Owner/EPC highlighting the generic system requirements to meet safety philosophy and operations and maintenance requirements and where the detailed technical (SIS) information may not be available, i.e. usually only coarse functional specifications will exist based on process engineering data sheets.

At this early stage of the project, the purpose of the preliminary SRS is to seek safety requirements information that will enable a basic sizing of the safety system. Further into the project timescales, additional revisions of the SRS document will be needed to complete a detailed specification when Target SIL's and individual safety instrumented functions are further detailed. Either way, the SRS becomes a working document to support the development of the SIS during the capital project lifecycle.

Typically the SIS usually forms a very small part of the larger project automation scope of supply in terms of the cost to the project, but what is often missed completely during this stage of the decision making process is that the small cost of getting it right at the front end of the safety lifecycle, can be a significant ratio/multiplication factor (in terms of incident costs) and more (in terms of loss of operations) in the future to the Asset Owner if the SIS where to fail on demand.

There's no formal template for what constitutes a comprehensive and 'fit for purpose' SRS, although IEC61508 and IEC 61511[2] (see also ISA 84[3]) require something in the region of twenty six pieces of separate safety instrumented functional information that should be considered in any detailed SRS.

That may sound like a huge information-gathering burden, but most of the information should be readily available, albeit in a number of separate documents, especially if a thorough hazard analysis and SIL determination risk assessment has been previously carried out.

When it comes to allocating risk reduction requirements to instrumented protective layers, it is the responsibility of the Asset Owner/operator to provide an SRS to the engineering/equipment supplier to correctly design the safety functionality and safety integrity requirements for the desired safety instrumented system (SIS). This is identified as Phase 3 of IEC 61511 and Phase 9 of IEC 61508 for E/E/PES in the IEC 61511/61508 safety lifecycle models. See figure 2 below as an example within IEC 61511.

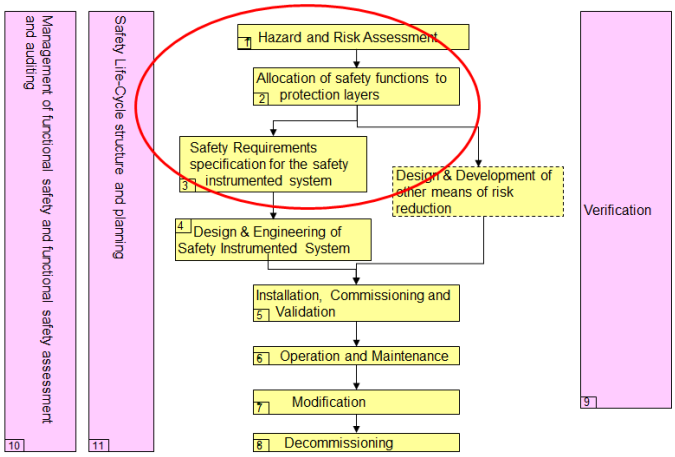

Figure 2 - IEC 61511 Safety Management Lifecycle

Unless the performance and detailed information derived within the earlier safety lifecycle phases is interpreted in alignment with the IEC 61508/61511 recommended sections i.e. highlighting Industry good practice SRS development documentation, then as highlighted earlier, this can have potential major consequences on safety performance as well as implications on the initial capital (CAPEX) costs deployed and lifetime operating costs (OPEX) associated with the conceivable over, or under design, of the required solution.

3 The challenges for Asset Owners

Dedicated functional safety resources can be difficult to source within operating companies in today's lean manufacturing operations. In many cases, dedicated functional safety (FS) specialists just do not exist and the halcyon days of 25 years ago when teams of engineers were available in-house are no longer the norm. Such in-house functional safety specialists have since either moved on, or retired and have not been replaced. Asset Owner operating companies are now suffering from a loss of corporate memory as expertise has since fragmented.

However the expectations from Industry and the Regulators alike are to improve both process and functional safety technical requirements in light of recent significant industry incidents. This has meant that the management of functional safety is an ever increasing imperative for the Asset Owners to continue to operate their plants safely under their duty of care requirements.

Fundamental to supporting the basis of safe operation is the need to have systems and procedures in place that can develop appropriate layers of protection (and by association a methodology to develop safety requirements specifications) so as to reduce the operating risk to a minimum, or 'As Low as Reasonably Practicable' (ALARP). Alignment with Industry good practice standards such as IEC61508 and IEC61511 can support the Asset Owners in terms of FS management structure and deliverables that are robust and traceable.

4 Development of a Safety Requirements Specification

Experience suggests that there is currently a significant disjoint or tangible 'gap' (pictorially as shown in figure 3) between the current processes of hazard and risk assessment leading to the derivation of the Target SIL and the development of a robust and meaningful (SRS) for the design, and implementation of a Safety Instrumented System (SIS).

If we consider Industry good practice expectations, unless the performance and detailed information derived within the earlier safety lifecycle phases are interpreted in alignment with the IEC 61508/61511 recommended sections of an SRS development document; this may have consequences on safety performance when it is commercially released to the supply chain i.e. in addition to issues relating to commercial, contractual and requirements creep.

Broadly speaking, SRS requirements fall into four notional categories: performance, integrity, operations & maintenance and service & repair.

The 'performance' requirements cover the range of considerations that make sure that the safety instrumented system is fit for the specific purpose for which it's designed i.e. can it meet the required process safety time (PST), for instance from detecting a problem within the process to carrying out an action to make it safe, takes time, especially if there are large, slow-moving items of equipment involved within the end to end design of the SIF, such as a large ESD valve.

'Integrity' is all about making sure that the safety system is working properly when you need it most. The required level of integrity for a particular safety system, and if we are following Industry expectations on this expressed as a safety integrity level (SIL), will depend on a combination of the likelihood of the action being needed and the definition of what constitutes a safe state, including aspects such as the likely safety element architectures deployed and the operating environmental conditions for the SIF.

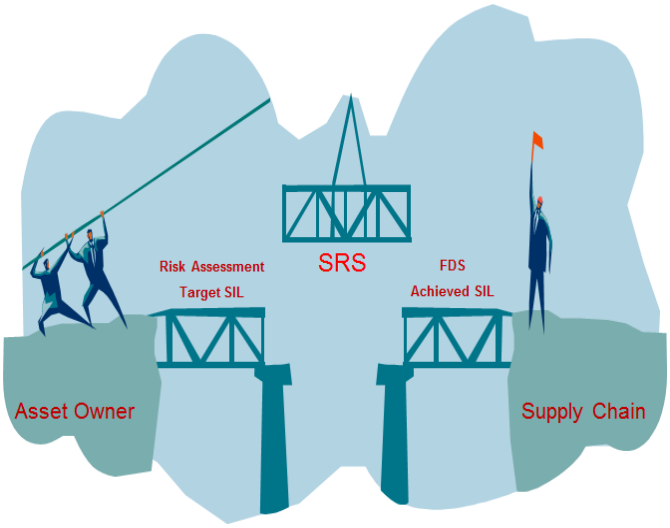

Figure 3 - bridging the gap between the Asset Owner and the Supply Chain

'Operations and maintenance' requirements cover the need for designing into the SIF operational features such as inhibits or overrides, shutdown modes, system re-starts, response times and critical information about actions associated with alarms. This is essentially about making sure that you have the right (management and engineering) regime in place to look after the SIS equipment and have confidence that it will work properly throughout its declared operational lifetime. How often do you need to carry out proof testing, for instance? Do you know the difference between proof test and functional test? Do you have the right functional safety management structure in place to guarantee, that vital checks will not be missed or forgotten? And how is system performance reported and the 'bad actors' assessed?

In order to review the requirements highlighted above, the SRS needs to be developed in conjunction with a number of identified disciplines and related core competencies providing the necessary contribution. It is not simply the Instrument engineer's problem to deliver the SRS once identified; the SRS will typically require input and development from roles such as the process safety engineer, EHS manager, project

manager, commercial manager and ideally the end user operations and maintenance staff.

A key question to ask responsible organisations managing SRS requirements, relates to the training and awareness of the commercial and purchasing teams to meet safety lifecycle management requirements. Again the authors' experiences to date would suggest, this functional group are often left out of awareness training and competency development when it comes to understanding the key drivers for safety requirements and getting this part of the project right from the outset.

Finally, the SRS should also include information relating to maintaining system security, servicing, repairs and controlling modifications. It's really about ensuring that the performance of the safety equipment is not altered in a detrimental way at some point after it's installed, i.e. perhaps by an uncontrolled modification, use of a non-certified spare, or a potential security threat that enters the system via external communications.

Guidance is provided in IEC 61508 Ed 2 Part 2 clause 7.2.3 regarding the content of the Safety Requirements Specification (this is strengthened, for the process industries, in IEC 61511, see part 1 clause 10.3.1).

5 Impact of the SRS into the Supply Chain from the Project Commercial Team?

In spite of the introduction of the new safety requirements step in Edition 2 of IEC 61508, experience to date identifies that in many issued SRS documents, these are still not comprehensively detailed, leaving safety system suppliers second-guessing about many of the specific criteria that process operators and contractors are looking for.

What is important for all to understand is that the Asset Owner/EPC community should recognise that the contractual necessities for safety system requirements should not be attempted to be resolved too early in the project lifecycle/FEED study; and that commercial and technical discussions with the supply chain should start in earnest wherever practicable only after the development of the detailed SRS and as based on the information provided from the earlier output of the hazard and risk assessment processes.

At a time when project owners and their main Contractors may not have dedicated functional safety expertise in-house, some project owners may seek advice and the available expertise from within the wider supply chain to understand the functional and reliability targets set by the risk assessment and therefore provide assistance in such matters.

As such, responsible suppliers with a demonstrable track record for competency assurance and proven technology solutions of SIS will generally be a good place to start when trying to bring this information together. The SRS development methodology may form part of a wider suite of functional safety management (FSM) system procedures that can be utilised as part of the broader safety lifecycle management requirements for compliance to the safety standards e.g. an accredited certified FSM system assessed by a recognised third-party organisation such as TüV [4, 5].

In doing so, a competent supplier will typically support Asset Owners and Contractors to develop the SRS by providing a structured SRS document skeleton that can be used to identify any gaps in the existing information and assumptions. This exercise can be conducted using independent resources to provide a common SRS platform (using any supporting tools as necessary) ahead of any commercial discussion.

In this way, once the SRS has been formally released, the SIS supplier can test key assumptions and spot if there's an opportunity to safely reduce complexity in design and installation and the expected maintenance regimes whilst optimising the overall cost of safety.

For the commercial and responsible supply chain teams involved during a typical invitation to tender and bid process, a detailed SRS issued as part of the commercial negotiations will allow for greater transparency against requirements and provide a vehicle to test key assumptions to reduce cost, complexity in design and installation and expected maintenance regimes, to ensure adequate provision is in-built i.e.

- Provide clarification and reduce ambiguity to technical, management and integrity requirements
- Provide commercial assurance that the SRS meets the intended risk reduction to be afforded by the SIS
- Establish the basis for traceability and audit trail throughout later lifecycle phases

This level of detail will provide the necessary integrity and traceability required to ensure that the correct functional design is taken forward through the safety lifecycle process e.g. the correct development of the functional design specification (FDS) for the SIS.

So when the detailed SRS is available and can be commercially released to the supply chain, the specification should no longer be just the focus of compliance to a basic prescriptive re-usable functional description as based on a legacy solution, or a loosely defined *'low cost wins'* approach. What is required to provide adequate risk reduction is a comprehensive data capture reflecting the requirements for functionality and reliability linked to the identified individual hazard scenarios and therefore should be based on much more *"than just the cause and effects diagram''*.

In addition, by following the requirements found in the safety standards, a number of these SRS requirements are a pre-requisite to performing an accurate and complete SIL Achievement/Verification exercise later during the design and engineering activities.

Fundamentally, a well-structured SRS allows the suppliers of the intended SIS solution to correctly interpret the requirements to drive the system architecture, design, implementation, and testing activities, necessary to meet the SRS intent via appropriate functional safety assessments (FSA) and achieved SIL reporting.

9 Conclusions

In summary, the overarching premise is that well specified safety requirements reduce the risk of under, or over specification, affecting both safety risk reduction requirements and capital to be deployed. This means that the system requirements specification meets the desired scope, optimised cost of solution, performance and maintenance criteria, size and complexity of the application.

Experience to date suggests that an invite to tender (ITT) or request for quotation (RFQ) from the project owner or EPC partner does not necessarily come with a full SRS in accordance with the relevant and recommended Industry good practice safety standards leading to the potential for:-

- Misinterpretation of ITT solution responses by the project owners commercial team during comparison analysis of response content
- Project schedule slippages, due to time spent in clarifying TQs & PQs, performing impact analysis for every change in the specification i.e. design by TQ
- Potential for expensive re-engineering of the solution at factory acceptance testing (FAT) based on misinterpretation of requirements regarding baseline assumptions, which invariably impacts on resources and costs
- The potential that a safety system that does not meet the necessary risk reduction could be approved for design
- Lack of demonstrable traceability to Industry good practice standards
- Potential exposure to liabilities both corporately and professionally

References

[1] IEC 61508: “Functional safety of E/E/PE safety-related systems, Edition 2”, (2010-02)

[2] IEC 61511: “Functional safety – safety instrumented systems for the process industry sector. Edition 1”, (2003-01)

[3] ISA 84 Functional Safety: “Safety Instrumented Systems for the Process Industry Sector”. (ANSI/ISA-84.00.01-2004)

[4] TüV Rheinland and TüV Sud: “Global Functional Safety Management Certification Programme”

[5] ABB Safety Lead Competency Centre UK: “Accredited TüV Certified Functional Safety Management System for the Design & Engineering of SIS”