General Factsheet

Safety Requirements Specification

Developing a safety requirement specification (SRS) prior to design and engineering

Challenges for end users within the functional safety marketplace:

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. Companies are now suffering from a loss of corporate memory as expertise has since fragmented.

However the expectations both from Industry and the regulators to improve both process and functional safety in light of recent significant industry incidents, has meant that the management of functional safety is an ever increasing imperative for the end users 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 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 IEC 61508 and IEC 61511 can support the end user in terms of FS management structure and deliverables that are robust and traceable.

Development of a Safety Requirements Specification:

Experience suggests that there is currently a significant disjoint 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 execution of a Safety Instrumented System (SIS).

When it comes to allocating risk reduction requirements to instrumented protective layers, it is the responsibility of the end user/operator to provide a SRS to the engineering - equipment supplier. This is identified as Phase 4, Overall Requirements, and Phase 9 for E/E/PES in the IEC 61508 safety lifecycle model.

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 industry, in IEC 61511 part 1 clause 10.3.1. Unless the performance and detailed information derived within the earlier safety lifecycle phases is interpreted in alignment with the IEC 61508 - 61511 recommended sections of an SRS development document, then this can have major consequences on safety performance when it is commercially released to the supply chain in additional issues relating to commercial, contractual and requirements creep.

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, performance criteria, size and complexity of the application (see table overleaf).

How ABB can help:

Developing an SRS is normally possible from utilising the essential information as found within the earlier hazard and risk assessment and aligning this with the performance criteria, reliability and expected operating regime of the end user organisation. ABB works with our clients to create a workable and robust SRS in line with the compliance requirements of the standards.

By supporting end users and - or EPC's develop the SRS document we provide the following benefits:

- Provision of a structured SRS document skeleton that can be reused
- Technical support in addressing any missing information - gaps in existing assumptions

Item	SRS Requirement
1	A description of all the safety instrumented functions necessary to achieve the required functional safety
2	Requirements to identify and take account of common cause failures
3	A definition of the safe state of the process for each identified safety instrumented function
4	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)
5	The assumed sources of demand and demand rate on the safety instrumented function
6	Requirement for proof-test intervals
7	Response time requirements for the SIS to bring the process to a safe state
8	The safety integrity level and mode of operation (demand/continuous) for each safety instrumented function
9	A description of SIS process measurements and their trip points
10	A description of SIS process output actions and the criteria for successful operation, for example, requirements for tight shut-off valves
11	The functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissives
12	Requirements for manual shutdown
13	Requirements relating to energize or de-energize to trip
14	Requirements for resetting the SIS after a shutdown
15	Maximum allowable spurious trip rate
16	Failure modes and desired response of the SIS (for example, alarms, automatic shutdown)
17	Any specific requirements related to the procedures for starting up and restarting the SIS
18	All interfaces between the SIS and any other system (including the BPCS and operators)
19	A description of the modes of operation of the plant and identification of the safety instrumented functions required to operate within each mode
20	The application software safety requirements as listed in section 12.2.2 of IEC 61511-1(2003-01)
21	Requirements for overrides/inhibits/bypasses including how they will be cleared; the specification of any action necessary to achieve or maintain a safe state in the event of fault(s) being detected in the SIS. Any such action shall be determined taking account of all relevant human factors
22	The mean time to repair which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints
23	Identification of the dangerous combinations of output states of the SIS that need to be avoided
24	The extremes of all environmental conditions that are likely to be encountered by the SIS shall be identified. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radio frequency interference(EMI/RFI), shock/vibration, electrostatic discharge, electrical area classification, flooding, lightning, and other related factors
25	Identification to normal and abnormal modes for both the plant as a whole (for example, plant start-up) and individual plant operational procedures (for example, equipment maintenance, sensor calibration and/or repair). Additional safety instrumented functions may be required to support these modes of operation
26	Definition of the requirements for any safety instrumented function necessary to survive a major accident event, for example, time required for a valve to remain operational in the event of a fire
27	Identification of security measures defined during hazard and risk analysis to prevent malevolent and unauthorised actions

Note: a number of these requirements are a pre-requisite to performing an accurate and complete SIL Achievement. Fundamentally, a well structured SRS allows for 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.

- Test key assumptions to reduce cost, complexity in design and installation and expected maintenance regimes to ensure adequate provision is in-built
- Provide clarification and reduce ambiguity to technical, management and integrity requirements
- Provide independent 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

ABB Safety Execution Centres supply a range of integrated engineering services in process industries, including, consultancy, project management and implementation to customers worldwide. We offer functional safety design and verification management and broader technical consultancy services. As part of our integrated automation engineering management portfolio we offer functional safety management consultancy services for new and existing assets.

Services include:

- Independent Functional Safety Authority for both new and brownfield projects
- Independent Functional Safety Assessment
- Independent Achieved SIL Assessment
- SIL Determination using ABB's Trip Requirement & Availability Calculator (TRAC) software tool
- Safety Instrumented System Auditing
- Development of Functional Safety Management Systems
- Design and execution of SIS projects in compliance with
- IEC 61508 - 61511 requirements via accredited TuV certified
- Safety execution centre, using TuV certified products and certified competent safety engineers

Our approach is holistic - we understand all the dimensions relevant to functional safety management, design and maintenance:

- Risk assessment
- SIS design and build
- SIS maintenance, inspection and repair
- Regulatory compliance and auditing
- SIS life extension or replacement migration
- Functional safety management, standards and procedures
- Sub-contractor management
- Competency and Independence

Our solutions are proven to deliver technical robustness, operational excellence and sustainable business improvement. We prefer to work in partnership with our customers where we deliver benefits together and we transfer relevant skills to our customer for ongoing improvement.

We have extensive experience of introducing improvements and technical solutions in organisations and in managing the necessary changes so our approach is to work alongside customers in fully implementing sustainable change.

Assured and certified products, services, delivery and execution.

For further information please contact:
ABB Safety Lead Competency Centre
Howard Road, Eaton Socon, St Neots
Cambridgeshire, PE19 8EU
Phone: +44 (0)1480 475321
E-Mail: oilandgas@gb.abb.com
www.abb.com/oilandgas