

Safety functions and SIL verification



Meeting the challenge of ensuring the integrity and regulatory requirements for your specific safety application.

With increasing acceptance and implementation of 'smart' safety automation technologies, the process industries are experiencing a rapid evolution of the techniques and measures to apply in order to meet their Functional Safety Management (FSM) requirements. Given the increasing focus on safety and cyber security performance improvement, end users now require closer integration of their safety and control systems, safety functions at varying process states, and flexibility, scalability, and re-usability of their safety devices.

With a wide variety of options available to the end user, the challenge to determine the safest, most reliable and cost effective Safety Instrumented System (SIS) appropriately. However as the end users delegate their functional safety management obligations into the supply chain, there is a need to ensure that the various elements of the safety and security lifecycle are delivered in compliance with industry good practice.

Even before selecting the devices for a safety system, it is first important to understand what safety related data is required.

Ultimately for end users to demonstrate compliance to industry good practice standards such as IEC 61508, IEC 61511 and IEC 62443, they will need to ensure that the SIS systems that are about to be installed meet in all respects the specific details of the safety and Security Requirements Specifications (SRS) established at the outset of the project.

What we offer

In terms of IEC 61508 - 61511 SIL capability, each element should have the following information available:

- Safe Failure Fraction (SFF)
- Hardware Fault Tolerance (HFT)
- Type classification (A or B)
- Target failure measure, expressed as either: PFDavg, or dangerous failure rate (hour)
- Systematic capability

The objective of gathering the data above for each device of the logic solver sub-system and the corresponding field instrumentation, is to enable the SIL verification process to be fully undertaken for the end to end safety function and in doing so provide demonstrable evidence that SIL has (or in some cases, has not) been achieved.

Consideration must be given to the availability and supportive evidence of these parameters for each device when selecting those devices on the basis of their functional safety suitability.

A validated claim that the devices supplied have the claimed parameters should be a key verification activity. Sound judgement should be used in the selection of devices in accordance with IEC 61508 Ed. 2 and IEC 61511 Ed. 2 'routes to compliance' for equipment that is supplied with supporting substantiated data and assessment reports.

The demonstration of SIL verification for a safety function could be considered ineffective if devices are selected that have unproven or inconsistent safety data sets and little in the way of meaningful user application certification reports and device safety manuals. In such circumstances, the question could be asked as to why the device was originally selected for design at the outset? and typically the answer provided is, "because it was the cheapest."

Benefits

- Technical support in addressing any missing information gaps in existing safety device data sets
- Test key assumptions and calculations against the SRS requirements to ensure individual SIF's will provide the correct level of performance and integrity
- Provide clarification and reduce ambiguity to technical, management and integrity requirements
- Provide independent assurance that the achieved SIL assessment meets the intended risk reduction to be afforded by the complete SIS

Why ABB?

ABB can support the project during the FEED study, detailed SIS design stages, or as part of a modification management of change process, for setting out the requirements for SIL verification linked to your safety and SRS documentation.

ABB works with our clients to create a workable and robust achieved SIL report in line with the compliance requirements of the standards. By supporting end users and/or EPC's develop the necessary SIL verification documentation.

ABB supplies a range of integrated engineering services in manufacturing operations and engineering, including, consultancy, project implementation and management, to customers within the process industries worldwide.

We offer functional certified safety design and verification management and broader technical consultancy services. As part of our integrated automation engineering management portfolio we offer FSM consultancy services for new and existing assets.

Our approach is holistic - we understand all the dimensions relevant to FSM, design and maintenance including:

- HAZOP and risk assessment
- Cyber security and risk assessment
- SIS design and build
- SIS maintenance, inspection and repair
- Regulatory compliance and operational benchmarking
- SIS life extension or replacement migration
- FSM, standards and procedures
- Industry leading functional safety training
- TÜV Rheinland functional engineering expert and engineer competency and independence

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.