Define your functional safety and cyber security requirements to optimise safety & security
Overview

The latest safety and security standards recognise that it’s important to define exactly what you need upfront in order to optimise and secure Industrial Automation Control Systems (IACS) and in particular for safety instrumented systems throughout the lifetime of a process installation.

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. And while everyone is keen to ensure that whatever is in place at the end of the process presents as little risk as is practical. Precisely, what that means in terms of safety and cyber security system requirements has in many cases being too loosely specified, which can invariably cause issues, errors and omissions as to exactly what is required, to achieve the necessary levels of risk reduction and security for the processing facility.

For example, the hazard analysis of a proposed project might identify a possible danger from a flammable storage tank overfilling with the potential to result in a fire or explosion. Instrument engineers will naturally be expected to provide suitable instrumented protection to prevent that happening.

In the past, an individual engineer might well have used a particular type of high-level prevention system based on a previous project design as a default solution. This might include a proof test frequency based on previous maintenance expectations, for instance. The temptation will be simply to use the same approach in any new project, but that could well be an expensive mistake.

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, pushing up running costs over the lifetime of the plant. And, of course, the consequences of under-specification can be much more serious, because the safety system may be inadequate and unable to provide the correct level of risk reduction that may have the potential to result in an incident.
The introduction of edition 2 of the IEC61508:2010¹, IEC 61511:2016² functional safety standards and the linkages to IEC 62443 series of IACS security standards³, gives a higher priority to defining a suitable, dedicated Safety Requirements Specification (SRS) for each project or systems modification.

It introduces a formal stage between the conclusion of the hazard analysis and risk assessment stage (functional safety and cyber security risk assessments) of a project and specifying particular SIS requirements leading into 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. It either includes the necessary information or is further supported by a dedicated report regarding the requirements for meeting any cyber security requirements e.g. identified countermeasures from the cyber security risk assessment results.

Specifically, for functional safety, the IEC61508 and IEC 61511 standards require over 26 pieces of information that should be considered in any SRS. That may sound like a huge information-gathering burden, but most of the information should be readily available, especially if a thorough hazard analysis and risk assessment process has been carried out.

---

3. IEC 62443-2-1 "Requirements for an IACS security management system", (2010)
What’s involved?

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

**Performance**
Performance covers the range of considerations that make sure that the Safety Instrumented System (SIS) is fit for the specific purpose for which it’s designed. Can it meet the required process safety time, for instance? From detecting a problem, carrying out an action to making it safe takes time, especially if there are large, slow-moving items of equipment involved within the end to end design of the Safety Instrumented Function (SIF).

**Integrity**
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 - expressed as a safety integrity level 'SIL', will depend on; a combination of the likelihood of action being needed and the definition of what constitutes a safe state. This includes aspects such as, the likely operating environmental conditions for the SIS and the considerations of other associated dependencies such as, cyber security measures to ensure successful operation.

**Operations and maintenance**
Operations and maintenance requirements cover the need for inhibits or overrides, shutdown modes, system re-starts, response times and critical information about actions associated with alarms. This is about making sure that you have the right regime in place to look after safety equipment and have confidence that it will work properly throughout its lifetime. How often do you need to carry out proof testing, for instance? Do you have the right safety management structure in place to guarantee that vital checks will not be missed or forgotten?

**Service and repair**
For service and repair, the SRS should also include information relating to maintaining system security e.g. patch management, 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, or a potential security threat that enters the system via external communications.
Industry experience

In spite of the introduction of the focused safety requirements step, within the safety standards from 2010 onwards. ABB’s experience is that many SRS documents even today 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.

However, between the suppliers and the findings in the project team’s hazard analysis and risk assessment, it’s often not as tricky as asset owners and contractors may think to put together an effective SRS.

At a time when project owners and their main contractors may not have dedicated functional safety and security expertise in-house, the best advice is to use the available expertise in the supply chain. Responsible and industry recognised competent suppliers of SIS will generally be a good place to start when trying to bring this information together.

Responsible suppliers such as ABB will typically support asset owners and contractors to develop the SRS by providing a structured SRS technical document that can be used to identify any gaps in the existing information and assumptions.
Conclusions

In this way, 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 and security.

Such an approach will provide the level of integrity and traceability required to ensure the correct functional design is taken forward through the safety and security lifecycle process.