Define your requirements and optimise safety

The latest safety standards recognise that it's important to define exactly what you need upfront in order to optimise safety systems through the lifetime of a process installation. John Walkington and Stuart Nunns explain what's involved and why it matters.

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's in place at the end of the process presents as little risk as is practical, precisely what that means in terms of safety system requirements has often been defined too loosely until now.

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 has the potential to result in an incident.

IEC 61508 Edition 2

The introduction of Edition 2 of the IEC61508:2010 functional safety standard gives a higher priority to defining a suitable, dedicated safety requirements specification (SRS) for each project. It introduces a formal stage between the conclusion of the hazard analysis stage 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.

But many process owners and contractors continue to omit the sort of information that needs to be included in an SRS if it's going to comply with industry good practice requirements. There's no formal template, although some organisations involved in functional safety, including ABB, may have their own procedures to ensure that their clients cover everything they need to.

IEC61508 and IEC 61511 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 has been carried out.

What's involved?

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

Performance covers the range of considerations that make sure that the safety instrumented system 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 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 safety instrumented function (SIF).

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 SIL level - will depend on a combination of the likelihood of action being needed and the definition of what constitutes a safe state, including aspects such as the likely operating environmental conditions for the SIS.

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?

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, or a potential security threat that enters the system via external communications.

Industry experience

In spite of the introduction of the new safety requirements step in Edition 2 of IEC 61508, ABB's experience is that many SRS documents 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 assessment, it's often not as tricky as process 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 expertise in-house, the best advice is to use the available expertise in the supply chain. Responsible 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 end users 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. 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 optimizing the overall cost of safety.

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

John Walkington is Department Manager and Stuart Nunns is Principal Managing Consulting at ABB's Safety Lead Competency Centre.