Session Seven
Functional safety and ageing assets

Shane Higgins
Principal Safety and Risk Engineer, HIMA Australia

Lyn Fernie
VP Global Consulting, HIMA Australia

Abstract
When designing a new facility, functional safety standards can be adopted at relatively low cost in order to reduce risks as low as reasonably practicable (ALARP), provided that standards are correctly specified and adopted from the earliest stages of a project. Practical ways to implement the standards for ageing assets are not immediately evident. The question often arises whether an existing plant or installation should be expected to comply with the same base standards as new assets. The functional safety standards provide a mechanism to determine an integrity requirement for a safety-related system based on the risk posed by hazardous scenarios. To enable a decision as to whether a retrofit is reasonably practicable, it is necessary to consider all the available options, assess the reduction in risk (benefit) provided by any new or modified safety functions/systems, and weigh that up against the cost of such improvements.

Introduction

The international standards IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) Safety-Related Systems (SRS) and IEC 61511, the daughter standard for the process industry sector, are increasingly expected to be adopted as the best practice approach for specification, design, procurement, installation, operation and maintenance of safety protection systems. However, the standards are voluminous, providing meticulous requirements whose implications can be daunting to the user. Practical ways to implement and comply with the standards are not immediately evident and the user is left to resolve numerous issues on how to implement the standards.

Development of Safety-Related Systems

The standards require the following steps to be undertaken when developing safety-related systems:

- Identify and analyse the risks
- Determine the tolerability of each risk
- Determine the risk reduction necessary to achieve a tolerable residual risk
- Specify the safety requirements for each risk reduction/safety function, including their safety integrity levels (SILs)
- Design the safety functions to meet the requirements
- Verify the safety functions as designed meet the requirements
- Implement the safety functions
- Validate the safety functions

Management of Functional Safety

Many users fall into the trap of jumping straight into risk analysis or specifying equipment, missing out one of the fundamental steps in the safety lifecycle, namely creating a framework within which to manage functional safety. Functional Safety Management (FSM) defines all activities required during the safety lifecycle phases of a product or process that are necessary for the achievement of the required level of functional safety. FSM also specifies the persons, departments, and organizations responsible for each safety lifecycle phase or for activities within each phase.

Developing a Functional Safety Management System (FSMS) is therefore an essential step for both new projects and existing assets. Decisions will need to be taken on the scope of the FSMS, which assets it will apply to, how it will be maintained, etc. A quality management system according to ISO9001 often provides a good starting point, but does not address all the requirements of a FSMS. Similarly, an existing Safety Management System (SMS) as required at Major Hazard Facilities (MHF) may also provide a basis on which an FSMS can be built and integrated. This also serves a secondary function of improving the awareness and understanding of FSM at the senior management level, the lack of which can be a major barrier to implementing an effective FSMS at any site.

The core element associated with the management of function safety is the creation of a Functional Safety Management Plan (FMSP); this document provides a road map to the FSMS. The FSMP either details the necessary activities to be performed to maintain the required level of functional safety or

provides reference to where the information can be found. A FSMP usually covers as a minimum:

- Policy & strategy
- Lifecycle management
- Roles & responsibilities
- Competency management
- Supplier management
- Configuration management
- Monitoring
- Documentation
- Functional safety auditing and assessment

Essential functions such as procurement activities, capability assessment of suppliers, and training of staff can also be undertaken through the FSMS framework.

Assessing compliance for an existing asset

The question arises whether an existing plant or installation should be expected to comply to the same base standards as for new assets, i.e. should full compliance with IEC61508 and IEC61511 be required for a plant that was built in the '70s, '80s, '90s (i.e. pre-dating the standards), or one that has been modified or expanded in the 00s?

When dealing with older assets, the costs associated with demonstrating that the facility meets the requirements of the functional safety standards can be significant, especially where a review indicates that equipment upgrades are required. Often in the mining industry, the upgrade requirements may extend far wider than the specific asset under consideration, for example where there are multiple machines operating on a particular facility or across a number of facilities, e.g. stackers, reclaimers, conveyors.

The functional safety standards provide a mechanism to determine an integrity requirement for a safety-related system based on the risk posed by hazardous scenarios. To enable a decision as to whether a retrofit is reasonably practicable it is necessary to assess the reduction in risk (benefit) provided by any new or modified safety functions/systems and weigh that up against the cost of such improvements. In the event that the cost of a retrofit cannot be justified in the short term, the process of assessing the requirements under the functional safety standards will often highlight other controls or methods that may allow significant improvements in plant safety at a relatively modest cost. This may be through providing better systems to manage existing controls, improving training and competency of staff on safety critical processes, changing out old or obsolete equipment that is identified as safety critical, or through implementing additional low-cost controls identified through the assessment process.

Case study – LNG facility built in the 80's and 90's

An LNG facility built in the '80s, with a Safety Instrumented System (SIS) that had been retrofitted in the '90s, undertook an assessment to determine the

requirements of a proposed replacement SIS as part of an overall control system upgrade.

As there were no recent records of hazard identification studies a Hazard and Operability (HAZop) study was carried out for each asset on the site with a focus on process safety and asset protection consequences, rather than operability issues. The study enabled an assessment to be made of the potential accident scenarios associated with the substances handled, the process used, and the equipment employed in the process.

The risk was assessed for each hazard using the Layers of Protection (LOPA) technique with the residual risk being allocated to the SIS wherever plausible Safety Instrumented Functions (SIF) could be implemented, defining the Safety Integrity Level (SIL) for each SIF. These studies were carried out without regard to existing safety 'trip' functions, except in providing an additional source of information, and the consequences and likelihoods of incidents were assessed in the absence of safety related layers. The results of these processes were fed into the development and allocation of safety requirements for the proposed system which was passed to the systems integrator and other parties responsible for the realization of the system.

At this stage in the project there was no overall functional safety management process in place and the understanding within the plant engineering team of the implications of adopting a functional safety methodology, both to the project lifecycle and to the overall plant safety lifecycle, was limited.

As is often the case it fell to those responsible for the design, implementation, installation, commissioning, verification, and validation of the system to put in place a Functional Safety Management System for the development phases. This required consideration to be given to the interfaces between the different areas of responsibility across both the project lifecycle and the overall plant safety lifecycle as well as the multiple parties involved. How would the required functional safety activities be coordinated across organisations and departments? How would functional safety be maintained as the plant transitions from commissioning to operations and maintenance, e.g. how will information from suppliers / designers / installers be translated into plant procedures and how would the functional safety of the system be monitored and audited throughout its lifetime?

Before the design process could begin it was necessary to review the existing field equipment including sensors and final elements as well as ancillary equipment such as interposing relays, cables, and pneumatics. Since plant documentation was not consistent with the existing plant an audit was conducted and drawings updated so that design decisions would be based on accurate information. The review was then performed to answer the following questions:

- What safety related interlocks are currently in place and do they match the required SIFs?
- Do any SIFs share sensors, final elements, or other critical components with the standard control system?
- Are installed components currently interfaced to the SIS or BPCS and are any changes required?

Following this safety assessments were conducted for each SIF allowing shortfalls to be identified against the requirements of the target SIL for each

SIF, to identify any missing SIFs and any existing functions performed by the safety control system that were not identified in the studies. Particular focus was given to the following:

- Are components to be retained suitable for use in a Safety Instrumented Function? Has the site gathered reliability data for components?
- Is the existing hardware fault tolerance (HFT) sufficient for the integrity required?
- Is the existing level of diagnostic coverage (DC) sufficient for the integrity required?
- Do the proposed SIFs achieve the required level of reliability (i.e. Probability of Failure on Demand (PFD) as determined through Fault Tree Analysis (FTA))?

Where shortcomings were identified, options were reviewed as to how to close the gap. Where it was practical to do so, these were resolved directly through changing out equipment for more suitable or more reliable components, installing additional elements for redundancy, or adding diagnostic features such as feedback monitoring of final elements or swapping digital signals for analogue. In some cases however, changing out of equipment (sensors or final elements) or addition of redundant elements could not be achieved without major changes to the plant or very large investments in hardware. In these cases other risk reduction options were considered including procedural measures, non-SIS safety functions (e.g. relief valves, bursting discs), hardwired interlocks, and short term measures (e.g. additional segmental proof testing). A practical approach to these types of issues was achieved through consideration of the ALARP (as low as reasonably practicable) principle. Any risk assessed as intolerable was addressed immediately as a reduction in risk was required, and cost considerations would not be deemed relevant. Risks in the tolerable region were deemed acceptable if they could be demonstrated to be ALARP, i.e. the cost of implementation of additional risk reduction measures was grossly disproportionate to the reduction in risk achieved. In some cases where it was deemed not to be practicable to implement changes as part of the current project a prioritized plan was put in place to systematically address and resolve issues over the following years.

Where installed elements were believed to be suitable but where insufficient data was available to demonstrate suitability (i.e. proven-in-use) this reinforced the need to implement a system to record and analyse reliability data on an ongoing basis. This, as well as other monitoring activities such as reviewing demands on the safety system, is a fundamental part of any functional safety management system.

Once the design issues for each SIF were resolved, proposed SIFs were reviewed for:

- Operability - will the SIF be invoked when the plant is not operating (i.e. will process variables exceed limits when not in operation or during start-up or shutdown)? Are additional signals required / available to reliably detect when a SIF should be active or enabled (enabling and disabling of SIFs may require different signals)?
- Maintainability - is there a requirement for bypasses, inhibits, overrides, or other functions to allow maintenance, calibration, or testing to be

performed during normal operation? What are the consequences of this for the safety of the system?

- Constructability - is infrastructure in place to allow SIFs to be implemented without major changes to plant? Where voting arrangements of sensors are employed; are they measuring the same parameter in the same place and is the existing variance between devices within the specified limits of the new system?
- Unintended consequences - can simultaneous activation of multiple SIFs (or other functions) result in a hazardous combination of outputs? Can spurious tripping of any function result in increased risk to plant? Do proposed changes increase the likelihood of spurious trips?
- Existing issues - will additional diagnostics unearth existing faults or issues that are currently managed outside of the control system or simply ignored? These may include the ability of the control system to maintain control within specified bounds, the ability of final elements to achieve feedback limits (sticky valves, play in actuators, instrument air quality), existing spurious trip conditions due to instrumentation issues, interference, process conditions, or environment/weather conditions. Will more rigidly implemented controls and interlocks lead to downtime or inability/difficulty to recover from faults?

Issues arising from any of these factors will typically be discovered at some point in the installation / commissioning or operation / maintenance stages and are generally easier and much less expensive to resolve if effort is made at early stages in the design to identify and resolve them.

Since the plant was required to operate near-continually and could not as a whole be taken out of service for any significant length of time the project presented significant challenges with maintaining process safety throughout the installation and commissioning stages. This required the team to simultaneously manage a combination of existing safety interlocks in the legacy safety system, newly implemented SIFs in the SIS, and an evolving series of temporary interlocks and hardwired signals between the two systems to facilitate interlocking functions that affected both cut-over plant and plant remaining on the legacy system. Comprehensive planning and risk assessment workshops were conducted to identify all hazards specific to the cut-over of each item of plant and put in place suitable controls to ensure that process safety was not diminished throughout the commissioning phase. These controls included procedural controls and changes to plant operating practices, partial plant isolations and minor shutdowns, and implementation of temporary interlocks.

In addition, careful adherence was required to configuration management and change control processes to reduce the risk of actions taken during later stages of commissioning affecting equipment that had already been commissioned, validated, and placed in service. Modular design (hardware and software) allowed testing or even modification, following rigorous change control procedures, with reduced effect on unrelated parts.

The challenge for the client was then to translate information from suppliers / designers / installers into plant procedures for operation and maintenance, and proof testing of critical components and functions as well as developing processes to effectively collect, record, analyse, and act upon safety critical data such as device reliability, initiating event frequency for SIFs, and spurious

trip frequency to ensure the plant performs as expected and is able to maintain functional safety throughout its operating lifetime.

Conclusion

Many industries in Australia are still getting to grips with what is required for compliance with the functional safety standards in an environment where regulators increasingly seek compliance with the standards as a means of demonstrating that hazards are adequately controlled.

A case study has been described, providing an overview of the practical application of these standards to new and ageing assets. As in all cases, having a Functional Safety Management System and Plan is an essential step towards compliance with the standard. Indeed, it is proposed that managing an imperfect safety-related system or SIS within a robust FSMP will provide a better outcome with regard to functional safety, than an asset having a fully compliant safety-related system which is no longer maintained through a functional safety framework.

For ageing assets, the decision as to whether to retrofit a safety-related system, or modify an existing one should be taken on the basis of the risk reduction benefit that such improvements will provide and the degree to which they are practicable, thereby reducing the asset's risk profile to as low as reasonably practicable (ALARP).