Expected and Unintended Effects of Instrumented Safety Protections

Edgar Ramirez
Safety Instrumented Systems Specialist, ABB Inc.

John Walkington
Safety Lead Competency Centre Manager, ABB Ltd.

Abstract

As Industry seeks to reduce risk within processes through the operation of Safety Instrumented Systems (SIS) in accordance with good practice requirements, different levels of effectiveness and compliance with lifecycle management have been observed:

- Compliance with safety standards via systematic performance that enables effective risk reduction
- SIS equipment capable for Safety Integrity Levels is sourced but is not engineered / operated to meet the necessary risk reduction requirements
- Modern device technology is used to implement safety protections according to management practices that have not evolved to meet current industry good practice requirements

Unfortunately incidents leading to harm for personnel, the environment, and affecting operating companies ability to sustain their business still continue to happen in spite of existing and new safety systems being introduced and operated within facilities to support risk management.

In addition to safety impacts, effects include disruptions to plant availability from unwanted and potentially frequent spurious trips. In this paper, results and effects from SIS projects and operations are discussed so as to point out the importance and benefits of systematic functional safety measures, assessments and effective lifecycle management as per the industry good practice standards IEC 61508, IEC 61511 (ISA 84.01) and IEC 62061.

Introduction

Programmable safety related systems have been standard elements of process industries automation for more than three decades. There is a general awareness of their importance through industry standards that have prescribed their use to achieve the necessary risk reduction when implemented in applications such as Emergency Shutdown Systems, Burner Management Systems, and similar protective requirements.

Instrumented safety functions have previously been engineered and operated predominantly with a focus on achieving redundancy and maintaining hardware safety integrity of the logic solver, but our understanding of what it takes to make safety systems effective and sustainable for their purpose has evolved. After the release of the functional safety standards IEC 61508 and IEC 61511 the focus is
shifting towards requirements for overall safety instrumented functions and the processes needed to achieve safety functionality, safety integrity, and systematic capability.

Yet in several instances the practices for safety systems projects and operations still reflect the previous focus on logic solver hardware architecture and the calculation of a failure rate measure in the belief that this constitutes the answer to the integrity requirements. Adoption of the good practice functional safety standards requirements has progressed very slowly. Often the rapid pace of projects has forced implementation of safety instrumented systems that do not comply fully with requirements as found in the safety standards. Unfortunately, gaps and non-compliant engineering and management practices have led to implementation errors and the potential for failures of safety-related systems. There are well documented incidents associated with safety and control systems that have failed to act on demand due to systematic errors introduced particularly during the engineering and/or operations activities.

Within this paper, attention is drawn towards the safety lifecycle management elements that enable the various engineering and operating teams to conduct their activities according to the requirements in the functional safety standards. An area of special interest is how reduction of errors during the engineering and operational lifecycle phases of safety systems helps prevent systematic failures.

The relevance of functional safety assessments as a validation mechanism on the integrity of safety instrumented functions is also discussed.

**Expected Effects of Safety Instrumented Functions**

A basic principle in the IEC 61508 standard is that safety-related systems can be used to achieve tolerable risk in the context of where they are applied; this likely is a goal amongst end users of such systems.

To accomplish the necessary risk reduction and meet tolerable risk targets, the functional safety standards provide a general guideline to implement safety functions throughout several lifecycle phases that can be explained briefly as:

1. Understanding the hazards and the risks they pose
2. Allocating and specifying performance of safety functions to protect against those known risks
3. Designing, engineering and building safety functions that satisfy risk reduction performance requirements
4. Operating and maintaining safety function at the required performance levels throughout the entire lifetime of the SIS
5. Managing the activities above as a lifecycle approach, incorporating processes for competency, verification and validation
The Safety Lifecycle proposed in the standards IEC 61508 / IEC 61511 summarizes activities during implementation and use of SIS. The Safety Lifecycle concept (a topic covered in Functional Safety training courses, see Figure 2) is well known by many SIS project engineers, but operations and senior management personnel are perceived to have received less of an opportunity to raise their levels of awareness and understanding.

A most relevant requirement in the functional safety standards is that companies involved in SIS projects and operations must implement a safety lifecycle to manage activities in which they are directly involved.

The steps towards adoption of a safety lifecycle within all organizations include:

- Identification of the set of activities during SIS projects and operations in which the company is involved, including the requirements for managing their supply chain partners with the same management requirements / rigour
- Preparation of procedures, techniques, measures and tools required for the activities identified
- Formal adoption of the safety lifecycle within the company to ensure systematic implementation and operation of safety-related systems in compliance with the safety standards
Figure 2. Safety Lifecycle according to standard IEC 61511

Operational safety functions are intended to reduce the frequency of specific hazardous events occurring, but their performance relies on the activities defined in the earlier phases of the safety lifecycle.

The implementation of the safety lifecycle depends largely on the commitment of companies to dedicate and manage the resources required. However with economic and time constraints always being a main factor within modern manufacturing, full adoption of the safety lifecycle has been slow and in many cases there is not a full awareness or understanding of this requirement at various levels including senior management / stakeholder level. This is a significant problem that has been observed to result in activities missed or poorly
executed leading to failure-prone safety functions and companies being ill prepared to operate safety protections.

According to the safety standards, management of the safety lifecycle is required for the correct derivation and implementation of safety instrumented functions in order to ensure that the necessary activities take place in a logical, structured and systematic way. The lack of functional safety management methodologies could lead to loosing visibility of essential activities required to implement or operate safety functions correctly, and some activities may end up not being conducted at all. Evidently the resulting safety functions lack compliance with the standards, and impacts may manifest further as the missing engineering activities can affect safety function operational performance and availability to act on demand.

The overall risk reduction capabilities can therefore be affected or impaired due to poorly informed decisions, and when the risks have been identified as significant, the consequences of failure on demand could be equally devastating.

**Consequences of Engineering and Operations Errors**

Several cases of failures of control and safety systems have originated in issues that have developed from errors or omissions in earlier lifecycle management activities – including hazard and risk assessment, SIS design and engineering. Also, the detailed requirements for engineering and operations of safety instrumented functions are often deficiently described from the outset.

**Consequences from problems during risk identification and specifications phases**

The main input for engineering of safety systems is the ‘Safety Requirements Specification’ (SRS), based on the information produced during the ‘Hazard and Risk Assessment’ and subsequent ‘Allocation of Safety Functions’ safety lifecycle phases. SRS are expected to describe performance parameters, target integrity, and other aspects of individual safety instrumented functions necessary to reduce risk to tolerable levels.

Errors during hazard and risk assessment activities can lead to flawed specifications and systems that do not have capabilities to accomplish risk reduction targets. The case study below elaborates on the issue of poor Safety Instrumented Functions (SIF) specification, design and further inadequacies associated with a lack of proof testing:

**Case 1.** An incident developed in a refinery isomerization plant where a level transmitter designed as part of a safety function for alerting operators to the issue of high level in a hydrocarbons distillation tower failed to operate. Here the level transmitter that was used in the plant was required to provide the necessary alert and subsequent safe trip when the high level limit was reached and exceeded, however during a plant startup the level increased much more that the high level setting should have allowed, while the transmitter no longer provided the required high level alarm. The specification should have required the safety function to be proof tested on a predetermined frequency and to be maintained accordingly.
The incident root cause was a covert failure of the level transmitter that led to the SIF failure on demand.

The above issue and other factors in this plant combined to cause a loss of containment that resulted in catastrophic plant damage due to the explosion caused by the leaked flammable hydrocarbons, and several fatalities.

Hazard and risk analysis and specifications are part of the early safety lifecycle phases and are necessary activities to identify and prevent intolerable risks. Correct analysis should identify the need for a SIF or number of SIF’s to reduce the frequency of a specific hazardous event occurring. What is then paramount after installation is that the SIF’s are proof tested and maintained to ensure the basis of safety is valid and assured. According to the IEC 61511 Safety Lifecycle (Figure 2) there are three phases that lead to the preparation of safety requirements specifications (SRS):

1. Hazard Analysis and Risk Assessment
2. Allocation of safety functions to protection layers
3. Detailed safety requirements specifications for the safety instrumented system

In addition to understanding and addressing risk reduction targets, there needs to be awareness of the consequences of safety function effects to ensure these do not lead to intolerable risks themselves. Omissions in specifications can lead to safety functions that whilst accomplishing a notional risk reduction target, they are designed solely on the basis of a probability of failure on demand. What should not be forgotten is that they can also trigger unwanted consequences onto the plant operating envelope for when plant disturbances occur. As such they have the potential to reduce manufacturing availability by introducing undesirable and frequent spurious plant shutdowns, which affect the profitability bottom line of the operation.

According to IEC 61511, Safety Requirements Specifications must also describe what potential consequences of safety instrumented functions actions need to be prevented / managed, including:

- A defined spurious trip rate
- Description of desired response action upon faults including the required safe state to be achieved
- Equipment / plant safe states that combined with other equipment / plant safe states could result in a dangerous condition
- Start-up and restart requirements for safety instrumented functions
- Actions and additional safety measures to be implemented when running in degraded mode

The importance of these requirements and of the information produced within the Hazard & Risk Assessment and Specification phases is highlighted in the safety standards. Planning is also a key requirement and needs to be effectively managed to ensure timely completion of SIS projects. Information produced in
these activities becomes the baseline evidence with respect to demonstrating forwards and backwards traceability for the safety case rationale and necessary due diligence to effectively reduce risk through the actions of safety protections.

The above activities need to be managed to ensure that the resources and outcome are adequate. To prevent errors from being introduced during the engineering activities, the teams involved need to be competent for their assignments, and use a management process and certified/calibrated tools that have been proven to deliver correct results. IEC 61508 identifies this type of engineering errors as a source of ‘Systematic Failures’ that need to be prevented through the use of appropriate techniques, measures, verification & validation, and supporting tools by demonstrable competent personnel. It goes on further to introduce the concept that prevention of systematic failures is identified as a necessary SIL capability e.g., Systematic Capability SIL 1–4. In other words: SIL can only be achieved when demonstrating the corresponding Systematic Capability.

Consequences from problems during design, engineering and testing phases

According to IEC 61511 the SIS engineering activities need to rely on the detailed information from the Hazard and Risk Assessment lifecycle phases, and in particular the derivation of the Safety Requirements Specification. This is the key input to system integrators for transposing safety requirements into SIS design and engineering deliverables.

The expected outcome from the SIS design & engineering activities are safety instrumented functions that:

- Are implemented according to requirements in the Safety Requirements Specification
- Satisfy SIL compliance and verification requirements as detailed within the safety standards IEC 61511 / IEC 61508
- Meet a systematic capability commensurate to the target SIL for individual SIFs

Verification requirements include a determined test frequency, proof testing methods and results reporting of SIF tests so as to demonstrate that the appropriate action will be executed when the process conditions generate a demand. To better seek risk reduction objectives each SIF must be proven to perform according to the safety requirements.

Prevention of errors during all implementation phases should be a paramount objective of those responsible for managing the safety requirements into their scope of supply. Errors seeded during engineering and manufacturing of safety instrumented systems can result in faulty implementation, deviations from specifications, and hidden faults that are “engineered” into safety systems inadvertently; all of which can later manifest unexpectedly during the operations phase when the safety functions are required to act in earnest. Verification is one of the mechanisms aimed to detect and remediate errors during all SIS
implementation and operations phases, thus the importance of processes for consistent and systematic verification throughout projects and operations.

Some of the issues during design and engineering phases include:

- Selection of inadequate (SIL capable or not) components for safety instrumented functions
- Lack of, or inadequate review activities – deficient design review and SIL verification
- Reliance on ISO 9001 processes that are not adequate for functional safety requirements instead of safety lifecycle processes
- Lack of, or inadequate testing
- Lack of impact assessment and management of change processes
- No demonstrable evidence of systematic capability in line with the target SIL

Case 2. Consider the incident in a fuel storage depot where overfill prevention systems were engineered to be used relying on human intervention in combination with automatic alarming. During normal operation a high level condition developed within a fuel tank leading to overfill and loss of containment, followed by a huge fire that lasted several days and destroyed most of the site with over 40 people injured. The operator, systems integrator and the suppliers of safety-related components for the protection systems were found jointly responsible for the failure of the layers of protection to operate when required.

The revealed causes for the above incident included mal-operation of the dedicated high level alarm functionality, and engineering of a safety protection that did not provide sufficient risk reduction.

Many different activities take place during the overall design and engineering of safety instrumented systems due to the need to integrate measurement instruments, logic solvers and final control elements. Engineering of logic solvers requires hardware engineering and software development by multiple team members and disciplines and in some cases multiple supply chain partners. Complexity of SIS design and engineering can be considerable as there is a need to ensure competency of team members and adequacy of management processes and tools.

Systematic failures are more likely to be originated from errors or omissions developed during the design and engineering phases if the project teams lack demonstrable competencies and processes to manage functional safety requirements and support their safety related engineering activities. Competency of project teams and functional safety management are requirements within the safety standards; although their importance is not always understood, the lack of them explains the occurrence of some of the engineering errors and systematic failures that can lead to safety functions failing to act when required.

Some of the engineering errors such as application software errors and deviations from specifications in assembly can be detected during project testing.
and design review activities; this highlights the need to have proven safety lifecycle management processes in place:

- Robust specifications
- Robust test planning, test methods and reporting
- Management of change and impact assessment
- Verification – review and resolution mechanisms covering normal and abnormal testing / activities

Development of SIS engineering teams and the processes and tools required for SIS projects requires focus and commitment. Execution of SIS projects requires engineering teams of suppliers and End Users to learn about the requirements of IEC 61508 / IEC 61511 in order to fully understand the importance of this industry good practice. To fulfill Functional Safety Management (FSM) requirements, and ensure use of recommended techniques and measures, companies must dedicate significant efforts and funding as required to establish and maintain a structure with the required capabilities for safety instrumented system projects.

Remember that what is spent in a short duration project ‘verification’ lifecycle requirement (typically 2-6 weeks) will affect over 20 years of future operating life. This is clearly about investing in the additional safety verification activities identified within IEC 61508/IEC 61511 that affect the sustainability and profitability of the plant. This is often overlooked, or no one is appointed to manage, or completely misunderstood by both stakeholder and budget holders alike regarding the significance and importance of FSM during the early project detailed engineering, and commissioning / modification activities i.e. Capex resourcing and costing requirements.

**Consequences from problems during operations and maintenance of safety instrumented systems**

The expected outcome of operational safety instrumented functions is to prevent the identified hazards and the risk they pose from taking place within the facility.

Automated safety protections usually do not require operator intervention (unless a credit is being taken for a highly managed alarm in accordance with ISA18.2/EEMUA 191) to take the programmed actions and bring the plant to a safe condition for when there is a demand placed on the SIS. Performance therefore depends on the ability of the End User to maintain the integrity of the safety instrumented functions.

Several industrial incidents have been found to originate in errors during operation of safety systems; poor practices for management of change during modifications have been found to be a frequent cause of some of the incidents studied. Errors during operations and maintenance can result in safety systems with degraded capabilities that can render protections unavailable. Modifications without understanding risk reduction and potential impact to safety integrity can lead to safety protections that are affected or become unavailable to operate when required.
These situations can be caused by constraints or from misunderstanding the need to manage resources for activities (particularly verification activities) in the safety lifecycle. Two cases of incidents due to problems during operations that have been analyzed in greater detail are presented:

**Case 3.** Failures in operations and maintenance practices allowed faulty level instruments to be used in a distillation column of an oil refinery contrary to procedures. During a plant start-up, data from the level instruments was not accurately reflecting the level inside the tower; operations teams were unaware of this fact, and thus failed to prevent the level in the distillation tower from increasing. A subsequent loss of containment, explosion and fires caused extensive destruction in the plant, 15 fatalities and over 170 major injuries.

**Case 4.** A storage tank was being filled with hydrocarbon materials and some of the existing product had to be diverted to a secondary overfill tank. During this activity, the operators failed to gauge and monitor the tank according to procedures and arrived to discover it was overflowing. The high level trip on the tank was not working and the resulting explosion killed one man, injured 23 others, and caused other adjacent tanks to catch fire resulting in the complete loss of the terminal.

Systematic failures derived from deficiencies in or lack of procedures, and issues with competency of personnel (linking to the subject of human factors) are at least partially responsible for some of the incidents analyzed and others that are still occurring within the industry today. The lack of commitment to manage a safety lifecycle is a fundamental issue that can lead to other problems.

Operations and maintenance activities teams therefore need to be considered in safety management systems in order to maintain safety integrity, provided that the safety functions have been designed and engineered in accordance to requirements identified from the earlier hazard and risk assessments.

With this lifecycle support in place End Users within the operational phase of a SIS can benefit from key information and processes to manage and maintain integrity of safety functions:

- Traceability from risks identified in hazard and risks assessments, through to allocation of safety protections, safety requirements specifications, and safety instrumented functions that are implemented in the safety systems operating within the facility
- Guidelines to implement processes and tools required by teams during operations, testing and maintenance of safety instrumented functions
- Functional safety assessment processes to validate if safety integrity is achieved and maintained
- Modification impact assessment and management of change to determine if safety integrity is affected and to ensure SIS performance is maintained during modification
• Competency management guidelines – operations and maintenance teams need to develop competencies to operate and maintain safety protections

Over recent years the safety systems supply chain has been evolving towards compliance with requirements in the functional safety standards and currently manufacturers of safety related elements are supporting such requirements with the supply of ‘certificated SIL capable’ compliant equipment. The trend among End Users and engineering contractors is in the same direction, with most projects including specifications for safety instrumented systems that require compliance with the relevant functional safety standards.

Yet with the abundance of modern plant operational activities that require attention, and the continued business pressures focusing on increasing profitability from systems optimization, the ability to monitor and maintain the integrity of safety instrumented functions is under pressure, i.e. to reduce the effort and resources used. Sadly, incidents continue to happen on a too regular frequency, and the difficulties to understand and deploy processes and resources for functional safety are still one of the primary causes of such plant failures as they are often hidden from stakeholder view given the nature of their use and ‘on demand’ requirements.

How to assess if safety integrity is achieved

Functional Safety Assessments (FSAs) as mandated in the safety standards are a valuable validation activity to help End Users, engineering and operation teams assess and maintain safety protection robustness. Through a structured and independent review of requirements, design, engineering, installation and operations activities, the FSA process is geared to maintain integrity of safety instrumented functions. Upon conclusion of Functional Safety Assessments, a judgment is made of whether safety functions integrity is achieved, and corrective actions are needed to improve performance.

Safe Operations and the Safety Lifecycle

Error prevention
IEC 61508 identifies the implications of errors in design, engineering, management and operations as potential causes of SIS failures. Failures in safety-related systems are categorized as either Systematic Failures or Random Hardware Failures. Therefore it follows that:

• Engineering activities for SIS design, implementation and operations need to undertake specific verification actions as a means to reduce errors in such activities.
• Appropriate Techniques and Measures which are proven in practice for engineering and management activities are required to match the level of ‘Target SIL’.
Engineering teams that do not adhere to these guidelines need to ensure (and at some point demonstrate) that their techniques and measures are valid to achieve safety function and safety integrity. It also means that compliance with the safety standards will be harder to achieve and so may inhibit their ability to verify a SIS compliant solution i.e. a demonstrable Systematic Capability for their scope of supply.

The IEC 61511 safety lifecycle provides the sequence of activities adopted as good practice by industry for implementation of safety instrumented systems. In addition to implementation and operations activities the safety lifecycle highlights the need for Verification and Functional Safety Management throughout the entire process.

Companies that engage in safety instrumented system projects in compliance with the safety standards are expected to define a safety lifecycle that includes the activities to be conducted by them. Increasingly, End Users are seeking supply chain partners that can demonstrate capabilities to manage functional safety requirements via third party certification e.g. TÜV accredited certification. More comprehensive support is needed in companies to promote adoption by operations teams.

Adoption of a safety lifecycle into a compliant functional safety management system (FSMS) provides a mechanism to identify all roles, responsibilities, activities and interactions describing the starting and end points, sequences, flow of information, and the need for processes and tools that are used throughout the lifecycle. During the definition of the safety lifecycle the End User companies should mandate from within their own FSMS the activities that allow prevention and control of systematic failures not only for themselves, but the requirements of their supply chain partners to the applicable extent.

At the systems integrators level, implementation of the safety lifecycle via a FSMS enables the assurance of a compliant SIS project execution methodology and corresponding risk reduction capabilities.

Implementation of the safety lifecycle enables key benefits to be realized for safety instrumented systems and in particular for operations teams for:

- When appropriate hazard and risk assessments and safety requirements specifications are available these documents provide the key information to understand the reasons for the safety instrumented functions to be used, and why they should be maintained operating at the required integrity level.
- When functional safety assessments are conducted in support of the project and into the operational lifecycle phases, independent validation mechanisms are enabled for assessment of safety integrity at any stage within the safety lifecycle. This information provides demonstrable evidence that functional safety has not been compromised and that any corrective actions are identified and closed out accordingly.
Summary and Suggested Measures

The use of Safety Instrumented Systems in the process industries has been consolidated and is a common requirement in most specifications for new projects and those that involve modification or evolution of existing safety protections. The functional safety standards IEC 61508 / IEC 61511 are recognized as global good practices and most companies acknowledge the importance of following their requirements as a means of demonstrating due diligence.

Engineering teams are developing functional safety competencies and understanding of requirements in the referred safety standards through individual management systems / methodologies, training and certification schemes. Leading organizations in the functional safety arena have implemented accredited TÜV certified functional safety management systems as a method to systematically deploy processes, tools and develop competencies of personnel; these schemes have been used initially for SIS engineering and in some instances extending to operations support.

Those responsible for the operations and maintenance of SIS need to ensure that safety integrity is maintained through the lifetime of the instrumented safety protections, as the continued occurrence of incidents has evidenced this is not always the case. Adoption of a safety lifecycle according to guidelines as found within the safety standards can enable mechanisms to support operational safety systems. Implementation of the safety lifecycle and a compliant FSMS lead to activities, processes and documentation to support safety instrumented functions when these go into operation.

Some of the hurdles remaining today within the safety lifecycle are related to the correct delivery of safety requirements specifications. We are still on the way to fully realizing the benefits from correctly describing and transposing requirements into design. It is still to be managed more effectively how to capture and describe the requirements to provide the operational benefits in terms of Capex, Opex, profitability, sustainability and above all, a safe place to work once SIS are installed at site.

A key requirement that has not received sufficient attention is the need to reduce Systematic Failures during SIS engineering and operations. Manufacturers of equipment, project and operational teams still have pending assignments to ensure that their processes, competencies and safety management systems are developed in compliance with safety standards, and proven to prevent errors that can lead to systematic failures of safety-related systems.

In addition, Functional Safety Assessments of operational safety systems have the potential to give users assurance on the integrity of safety functions. Through periodic analysis and validation of safety integrity achieved / maintained, End Users can act to keep risk reduction measures fully available within the facilities where they are required.

Broader benefits expected from the use of safety instrumented systems can only be achieved when the safety lifecycle is fully implemented, yet in several
instances only partial implementations have been realized. Requirements and preparations to achieve safety integrity are often seen as a burden (when in fact they should be recognized as invaluable activities that will assist successful and sustainable operations over the lifetime of the operation), and limitations imposed in projects and operations end up affecting capabilities of safety functions.

If requirements for safety integrity are relaxed by the End User, then the supply chain will usually deliver solutions according to the market conditions and there is no guarantee that the final product will be adequate as per the requirements of the functional safety standards. Safety protections that do not meet demonstrable safety function, safety integrity and systematic capability requirements cannot be relied upon to prove and support the necessary risk reduction requirements to key stakeholders and regulators alike. In this context no SIL claims are valid in spite of the use of components that are purported to be ‘SIL rated’, as the activities or components that do not satisfy requirements become dominant contributors and make safety instrumented functions become non-effective.

From an operations perspective the result in these less robust situations are usually safety protections that are more likely to fail on demand and therefore the risks that remain are still within the intolerability levels for the manufacturing facility.

References