FUNCTIONAL SAFETY: SIL DETERMINATION AND BEYOND – A CASE STUDY FROM A CHEMICAL MANUFACTURING SITE

Jasjeet Singh and Neil Croft, HFL Risk Services Ltd, Manchester, UK

Industrial chemical processes increasingly rely on Electrical/Electronic/Programmable Electronic (E/E/PE) systems as safety systems. The proportion of automation places high reliability demands on components that make up these systems. Given the hazards associated with chemical manufacturing, reliability of systems which perform safety related functions is of the utmost importance. This aspect has drawn significant attention from the regulators who are encouraging compliance with the current functional safety standards IEC 61508 and IEC 61511 for E/E/PE systems. The process industry standard IEC 61511 follows a safety life cycle approach which begins with risk assessment. In the author's experience, a large number of operators who have completed, or are in the process of evaluating their control and safety system's reliability, do so to 'determine the SIL or the safety integrity level' only. However, the standard is much more than just SIL determination and techniques like Layer of Protection Analysis (LOPA) can do much more than 'determine' the SIL.

Functional safety is not only about SILs but encompasses the whole safety life cycle from the initial risk assessment to operations, maintenance and decommissioning. The vast majority of operators complete the SIL assessment and install the individual elements (sensors, valves etc.) rated for the SIL, and are under the impression that they have a SIL rated safety system in place. SIL is a property of the whole loop; installing the individual 'SIL rated' elements does not necessarily result in a SIL compliant loop. By following the safety life cycle approach, a true SIL compliant safety system is realised. Often some elements of the safety life cycle such as training are not considered at all or ignored. As per the standard, completion of all elements of the safety life cycle is necessary for true compliance. A 'SIL rated Safety Instrumented System (SIS)' on its own does not ensure compliance.

This paper uses an example of the risk assessment of a chemical process, which posed hazards of decomposition and thermal runaway, where the functional safety approach was used as a tool to improve the understanding of the process and its hazards. The risk assessment initiated further studies on reaction kinetics and calorimetery. These studies helped to identify the true hazards from the process which resulted in implementing inherent safety principles to some of its aspects, thus eliminating particular initiating events. Also a SIL rated SIS was designed and commissioned to reduce the risk from some initiating events where inherent safety was not practicable. Specially tailored training programs were delivered to ensure familiarity with the safety life cycle at all levels of personnel within the company and to promote further specific training. The paper discusses the use of Hazard Identification (HAZID) and LOPA which was done on the process with the aim of identifying those scenarios which posed significant risk. A further assessment was completed to identify risk reduction measures, including the safety instrumented functions (SIFs). The SIFs were implemented by a custom designed SIS which followed the safety life cycle approach. The result was a safer process with improved efficiency.

INTRODUCTION

A chemical manufacturing site was required by the Health and Safety Executive (HSE) to complete a 'SIL Determination' study on a reactor system. The site employed the engineering consultancy where the author is employed, to assist them with the exercise. The author is of the view that a comprehensive risk assessment was necessary to complete this exercise, and proposed that a Hazard Identification (HAZID) be carried out on the system. A Layer of Protection Analysis (LOPA) could then be used to identify the gap between the target risk reduction and risk reduction provided by the existing protection measures. These gaps could then be reduced to As Low As Reasonably Practicable (ALARP). The process would result in identification of the safety functions. Following that if the safety function(s) is allocated to an instrumented protective system(s) (IPS), it would then be designated as a safety instrumented function (SIF). The target integrity of the SIF, or it target safety integrity level (SIL) could then be estimated from the LOPA study.

The paper describes the various elements involved in such a study, and includes common misconceptions at various stages.

The objective of this paper is to raise awareness of the two concepts:

- LOPA is much more than SIL Determination – Hierarchy of risk reduction measures;
- Installing SIL certified components does not mean that a SIL rated 'loop' is achieved.

GENERATION OF SCENARIO – INITIATING EVENT PAIRS

The author is using a case study from a chemical plant which manufactures an organometallic speciality chemical compound used in pharmaceutical industries amongst others. The process involves reaction of magnesium with an alkyl halide in a flammable solvent – a Grignard reaction.

In the process plant, a reactor vessel is charged with a pre-determined quantity of a flammable solvent. Magnesium is then added via a chute. The contents are agitated to enable homogenous mixing. A small quantity of alkyl magnesium halide is then added to initiate the reaction. The system is injected with alkyl halide from cylinders. The resulting reaction is exothermic. The contents are continuously cooled. The injection process is critical to the reaction as it governs the heat generation. At the time of the study, the injection of alkyl halide was controlled by the operator using a manual valve. The system is illustrated in Figure 1.

A HAZID study on the system generated a number of potentially hazardous scenarios. The scenarios discussed in this paper are summarised in Table 1.

Both scenarios had other initiating events which are not discussed in the paper. Both these scenario – initiating event pairs were subjected to LOPA. The result is discussed in the next section.

'HAZARDS' BEFORE 'SIL' – USING LOPA EFFECTIVELY

The first concern when embarking on a 'SIL Determination' exercise is the tendency to put the 'cart before the horses'. Hazards, and the risks from these hazards, have to be identified with their initiating causes. Only then can the safety function be determined. Also, the 'risk tolerance criteria' must be known. Without this it is impossible to meaningfully identify the integrity requirements on the safety functions. However, it is not uncommon to see the target SIL allocated to a hazardous event based on the judgement of consequences alone. No consideration is given to the type and number of initiating events, and to other protection measures which do not rely on an instrumented system, or indeed, if feasible, inherently safer process design.

In the case study used as an example, the two scenario-initiating event pairs, amongst others, identified from the HAZID were subjected to LOPA. The analysis for each pair is discussed below.

SCENARIO A: A CASE FOR INHERENTLY SAFER PROCESS DESIGN

The scenario involved overheating of the contents due to the uncontrolled application of the heating medium. The contents were heated using steam during addition of Alkyl Magnesium Halide for initiation. Upon reaching the required temperature, steam is cut off. The vessel is then put on cooling for the remainder of the sequence. This sequence of steps was vulnerable to errors such as: valves failing to close; sequence failing to close the valve; or operator leaving the heating on when in manual mode.

In LOPA, all these scenario-initiating events were analysed independently. The analysis determined that the

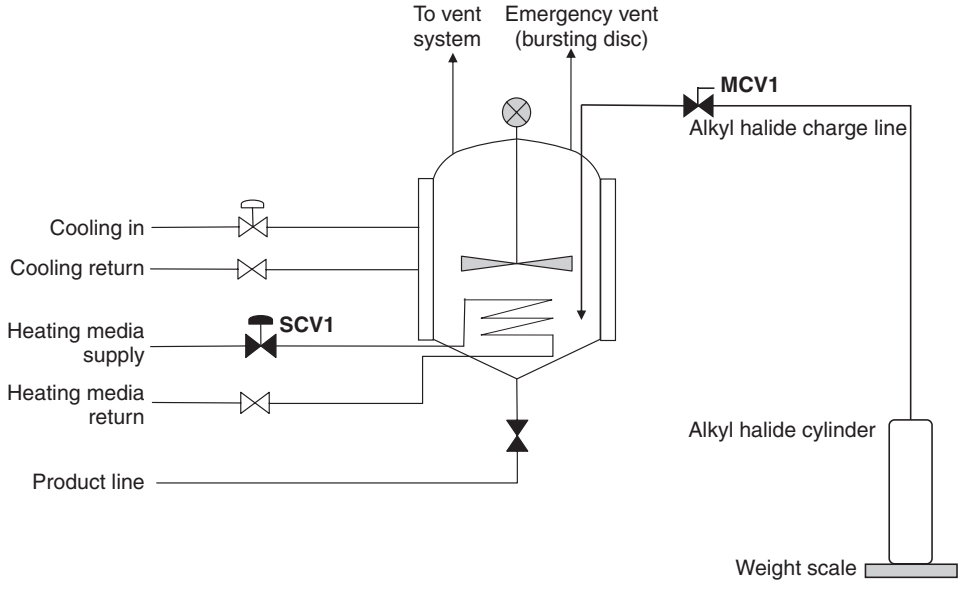

Figure 1. System illustration

Table 1. HAZID Scenarios

Scenario	Initiating event	Consequences
Scenario A: Overheating of the contents resulting in thermal runway and decomposition. Overpressure in the system and vessel catastrophic failure.	**A.1:** Failure of the steam control valve (SCV 1) resulting in steam being applied to the reactor. **A.2:** Failure of the control sequence to close the steam control valve (SCV 1) resulting in steam being applied to the reactor. **A.3:** Operator fails to close the steam control valve (SCV 1) when in manual mode resulting in steam being applied to the reactor.	Fire and explosion. Potential for fatalities.
Scenario B: Excessive injection of alkyl halide. High heat generation resulting in contents reaching thermal decomposition temperature. Rapid decomposition and overpressure in the system. Vessel catastrophic failure.	**B.1:** Human Error – Operator fails to close the manually controlled addition valve (MCV 1). **B.2:** Mechanical failure – failure of the addition valve (MCV 1).	Fire and explosion. Potential for fatalities.

target risk reduction by independent layers of protection was not achieved. Hence further risk reduction was required to demonstrate ALARP. When done correctly, the HAZID – LOPA process is straightforward. However, it is not unusual to find that when a hazard analysis team reaches this stage, there is a tendency to find 'local' or scenario specific solutions. For example, various ideas were put forward at this stage in the scenario being discussed. These included installation of a high temperature trip, interlocking heating control with cooling etc. However, the scenario was discussed further and the possibility of an inherently safer design was explored. The chemistry expert in the team informed that there is a high probability that the reaction would initiate without heating, without significantly affecting the batch time. It was recommended that further analysis be carried out on the reaction kinetics to determine if heating was actually necessary.

Following the study, the plant team conducted a detailed reaction kinetics analysis and concluded that for the particular product being synthesized, reaction initiation by heating was not necessary. The alkyl halide when introduced sub-surface reacted quickly without the formation of different layers etc. inside the vessel. Hence, application of heat was no longer deemed necessary. Trial runs proved this theory. The operations and the hazard analysis team then concluded that heating would be disconnected physically from the reactor vessel when manufacturing the product. This removed the possibility of various initiating events which could lead to the scenario of overheating identified in the HAZID. Hence, an inherently safer process design was achieved.

This example illustrates that LOPA is much more than a SIL determination exercise. The hierarchy of risk reduction starts with the principles of inherent safety. The team was able to think 'outside of the box', the box being 'install a SIL rated instrumented loop' to achieve the required risk reduction.

SCENARIO B: A CASE FOR FOLLOWING SIS SAFETY LIFE-CYCLE

The scenario involved excessive injection of the alkyl halide resulting in overheating of the contents. The rate and quantity of heat generated due to excessive injection of the controlled reactant, alkyl halide, even in small doses had the potential to cause thermal runaway.

The amount of the reactant injected was controlled using a 'dead man's handle' type valve. The operator had to monitor the temperature rise after each 'slug', and stop if the anticipated temperature profile was not observed. This procedure was vulnerable to errors such as: the valve failing to close or seal properly; failure of the temperature display resulting in false output to the display units, etc.

Again, in LOPA, all these scenario-initiating events were analysed independently. The analysis determined that the target risk reduction by independent layers of protection was not achieved hence further risk reduction was required to demonstrate risk reduction to ALARP. Following further analysis, calorimetric calculations to determine the quantity of alkyl halide necessary to cause thermal runaway were completed. The team revisited the LOPA, and recommended that a SIL 1 capable SIS to control the injection of alkyl halide should be installed to achieve the necessary risk reduction, in conjunction with other risk reduction measures. At this point, the SIS Safety Lifecycle has to be understood, with its requirements. Only then can true functional safety be achieved.

In the author's experience, a large number of small or medium scale chemical operations are yet to familiarise themselves with the full requirements of Functional Safety Management (FSM), and consequently do not adapt the concept of safety life cycle into their Safety Management Systems (SMS). The view that replacement of field elements with SIL rated counterparts achieves a SIL loop is widespread. The chemical operator in the case study faced similar concerns. Hence it became evident that a thorough

overview of the SIS Safety Life-cycle and the industry standard IEC61511 was necessary.

This brings us to the second objective of the paper – highlighting the fact that installing SIL certified components does not mean that a SIL rated 'loop' is achieved. The process industry standard on functional safety IEC 61511 describes various activities involved in designing, commissioning, operating and maintaining a 'SIL rated' SIS. In the author's experience many end users are not aware of the various activities involved in functional safety. The misconception that using 'SIL rated' components alone would yield a SIL loop is widespread. The industry regulator often accepts such loops as IEC compliant but this approach is changing rapidly as the knowledge around functional safety continues to improve.

The SIS safety life cycle has been designed such that it allows a clear and structured approach to Functional Safety Management. BS IEC 61511 Part 1 contains information of the safety life cycle. In brief, the safety life cycle:

- Provides the technical framework for the activities necessary for ensuring functional safety is achieved by the E/E/PE safety-related systems.
- Covers all activities from initial concept, through hazard analysis and risk assessment, development of the safety requirements, specification, design and implementation, operation and maintenance, and modification, to final decommissioning and/or disposal.
- Encompasses system aspects (comprising all the subsystems carrying out the safety functions, including hardware and software) and failure mechanisms (random hardware and systematic).
- Contains both requirements for preventing failures (avoiding the introduction of faults) and requirements for controlling failures (ensuring safety even when faults are present).
- Specifies the techniques and measures that are necessary to achieve the required safety integrity.

Figure 2 shows the safety life cycle and the functional safety assessment stages. Detailed discussion on the functional safety activities is not within the scope of this paper. However, the author considers the following as being crucial to achieving functional safety from the end user's perspective:

- Safety Requirements Specification (SRS) Generation;
- SIL Verification and SIS Validation;
- Personnel Training;

The importance of these activities is discussed briefly below:

SAFETY REQUIREMENTS SPECIFICATION (SRS) GENERATION

It must be emphasised that any risk assessment technique, including LOPA, cannot yield the exact requirements for a SIS. These assessments establish a required risk reduction and a preferred method to achieve it. When it is decided that a required safety function will be allocated to a safety instrumented system, LOPA aids in setting the 'target SIL'. The next step is the most crucial step but is also the step most often missed – SRS datasheet generation. The SRS translates the SIF identified by the risk assessment to an engineering design specification. The SRS also acts as an input for the loop designer to assist the generation of the detailed loop design. IEC 61511 clearly summarises the minimum contents of a SRS datasheet.

The SRS also acts as a reference when the loop is to be validated – another activity often missed. A properly generated SRS is a true reflection of the loop, summarising all its salient features which are essential for designing, operating and maintaining the loop. A SRS is also required to demonstrate compliance with the functional safety standards. For various validation activities that have to be performed before and after a SIS is put into operation, the SRS maintains a 'live' picture of the loop. Hence if the SRS is not properly maintained, or even worse not generated at all, demonstrating that the required functional safety has been achieved becomes almost impossible.

SIL VERIFICATION AND SIS VALIDATION

At every major stage of the SIS being realised, validation of the processes completed prior to that stage is recommended. The standard recommends that validation be carried out for SRS generation, Design and Realisation (Commissioning).

Assuming that installing SIL certified components, the target SIL has been achieved is the first step towards a false sense of safety and compliance. SIL certification for individual components only implies that the component is suitable for using in a SIS with corresponding SIL requirements. The important point to remember is that the SIL is a property of the 'whole loop' and NOT that of individual elements – the functional safety mantra is **"Loop, loop, the whole loop, nothing but the loop"**. A loop designer generally goes through an iterative process of designing the loop, choosing its architecture, choosing the various elements etc. and then verifies if the target SIL would be achieved. This could be a simple exercise or could be quite complex, depending on the SIF that has to be performed. For example, in this study, the SIF required a complex functional relationship between flow, pressure and temperature. Hence, a number of iterations became necessary. This further emphasises the importance of the SRS, since the functional relations are defined in the SRS and which are used by the designer as the basis for the whole loop.

When the end user simply procures and installs individual elements, functional safety cannot be achieved. This aspect of functional safety is often overlooked by end users.

Validation has to be carried out after installation and commissioning of the SIS has been completed. This involves the Factory Acceptance Test (FAT) and also a strict crosscheck against the SRS.

PERSONNEL TRAINING

Establishing functional safety on a plant requires the input of a cross discipline team. The responsibilities of the

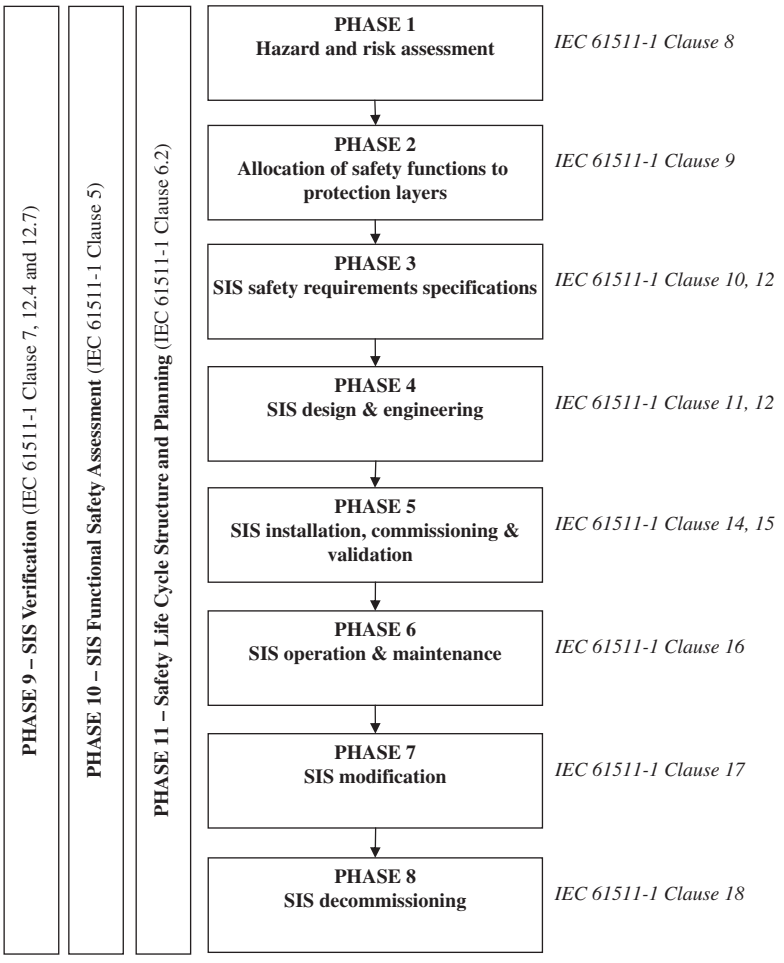

Figure 2. SIS safety life cycle

individuals have to be defined and clearly allocated. Hence personnel have to be trained to an appropriate level. Special emphasis has to be given on ensuring that all personal involved understand the basic concepts, and that SIS is a different breed of plant instrumentation.

Operations and maintenance teams occupy an important position in ensuring functional safety is maintained. Since the requirements for maintenance of such systems are quite stringent, routine maintenance practices cannot be used for SIS.

Even the personnel responsible for procurement for components used in the SIS have to be trained to an appropriate level. This is to ensure that they understand that SIS elements cannot be replaced with other relatively cheap alternatives.

The standard IEC61511 Part 1 clause 5 requires that all persons and/or departments which are responsible for carrying out and reviewing each of the Safety Life-cycle phases shall be identified and be informed of the responsibilities assigned to them.

As a guide to ensure competence of the individuals and departments involved in the FSM system, the items listed in Table 2 should be addressed. The items are listed in the standard as a minimum requirement to ensure competence compliance.

It is worth noting that this is just a brief overview of the SIS safety life cycle aimed at highlighting the fact that SIS involve much more than the "sensor – relay – valve" concept. The end users of these SISs, especially the small and medium scale chemical industry, are in the process of adapting the safety life cycle methodology. But more awareness is required to gain significant penetration.

CONCLUSIONS

SUMMARY

The author hopes that the two concerns that were raised at the start of this paper have been addressed:

- LOPA is much more than SIL Determination; and
- Installing SIL certified components does not mean that a SIL rated 'loop' is achieved.

The end users should not jump to designing 'SIL' systems without following the risk assessment methodology

Table 2. Minimum Competence Requirements

IEC 61511 Clause 5.2.2
a. Engineering, knowledge, training and experience – Process Application
b. Engineering, knowledge, training and experience – Application Technology
c. Engineering, knowledge, training and experience – Sensors & Final Elements
d. Safety engineering knowledge
e. Knowledge of the legal and safety regulatory requirements
f. Management and leadership skills for safety life cycle management
g. Understanding of the potential consequence of an event
h. SIL Determination for SIF
i. Novelty and complexity of the application and the technology

including the hierarchy of risk reduction measures – the safety systems.

It is essential to know the process completely first to understand the risks it presents. Only when the hazard is known explicitly, can a clear safety function be defined. When using techniques like LOPA, end users should not feel obliged to generate a requirement for a SIS. Only when it has been concluded that no other equally effective and reasonable alternative can be implemented, should the safety function be designated as a SIF.

Secondly, when a SIF or multiple SIFs have been allocated, simply buying components with SIL certificates and 'hardwiring' them does not equate to a SIL loop. Remember the mantra, **"Loop, loop, the whole loop, nothing but the loop"**.

End users should implement a Functional Safety Management system, and integrate it with their overall SMS.

THE STANDARDS ARE CHANGING

The technology has changed by orders of magnitudes in recent years. A high degree of penetration of computers into process control solved many problems, but also raised many concerns. After all, a hazardous reaction cannot be 'rebooted'. Hence with the advent of automated control and safety systems or E/E/PE systems, concerns have been raised about their reliability. Two decades ago most safety systems comprised of discrete sensors, usually a switch, discrete relay based logic acting on an on-off type field element. Currently, more and more people are using programmable logic controllers (PLC), smart transmitters etc.

Prescriptive standards cannot cover the details, the variation, and the complexity of systems in operation today. Hence, mostly due to industry initiatives, new performance based standards are taking over. Functional safety standards like IEC 61508 and IEC 61511 show this fundamental change. Hence, the way these standards have to be adapted should change as well. 'Cookbook' recipes for safety systems offer little benefit in today's chemical plant. Consideration has to be given to the whole life of the plant, from cradle to grave. Safety systems are no exception.

REFERENCES

1. BS EN 61808:2010, "Functional safety of electrical/electronic/programmable electronic safety related systems", Geneva: International Electrotechnical Commission.