Lessons Learned on SIL Verification and SIS Conceptual Design

72nd Annual Instrumentation and Automation Symposium for the Process Industries

January 26-28, 2017

aeSolutions Technical Team
aeSolutions, Greenville, South Carolina, USA

Abstract:

There are many critical activities and decisions that take place prior to and during the Safety Integrity Level (SIL) Verification and other Conceptual Design phases of projects conforming to ISA84/IEC61511. These activities and decisions introduce either opportunities to optimize, or obstacles that impede project flow, depending when and how these decisions are managed. Implementing Safety Instrumented System (SIS) projects that support the long-term viability of the Process Safety Lifecycle requires that SIS Engineering is in itself an engineering discipline that receives from, and feeds to, other engineering disciplines.

This paper will examine lessons learned within the SIS Engineering discipline and between engineering disciplines that help or hinder SIS project execution in achieving the long-term viability of the Safety Lifecycle. Avoiding these pitfalls can allow your projects to achieve the intended risk reduction and conformance to the IEC 61511 Safety Lifecycle, while avoiding the costs and delays of late-stage design changes. Alternate execution strategies will be explored, as well as the risks of moving forward when limited information is available.

Keywords:

IEC 61511, Safety Instrumented Systems (SIS), Independent Protection Layers (IPL), Functional Safety Assessment (FSA), Safety Requirement Specification (SRS), Safety Lifecycle, Functional Safety Management Plan (FSMP), Project Execution Plan (PEP), SIS Front-End Loading (SIS FEL), Layer of Protection Analysis (LOPA), SIL Verification

Introduction:

ISA 84 (IEC 61511 mod) was released in 2004 as a performance-based standard for implementing SIS in the process industry. Since then, numerous end users, system integrators, EPCs, etc. have executed projects involving the implementation of the guidelines presented in the standard. With each implementation comes more experience and lessons learned on how to improve process work flows.

Through this white paper, the authors will discuss several facets that can have significant impact on overall total installed cost and schedule based on their experience. With case studies, the paper will present how skipping Functional Safety Assessment (FSA) stages 1 and 2 delays project; how not thinking of proof test philosophy during early project stages can lead to late project changes; and how overlooking process safety time and SIF response time during SIL Verification calculations can lead to designing a SIF that may not be effective in preventing hazards for which it is credited.

As shown in Figure 1, SIS Conceptual Design commences after the completion phases of Risk Assessment (SIL Selection), and ends with the issuing numerous deliverable packages used for SIS detailed design. Detailed design, in regards to SIS Conceptual design involves a combination of process engineering, electrical engineering, control panel design, SIS hardware design, software configuration, and instrumentation design and specification.

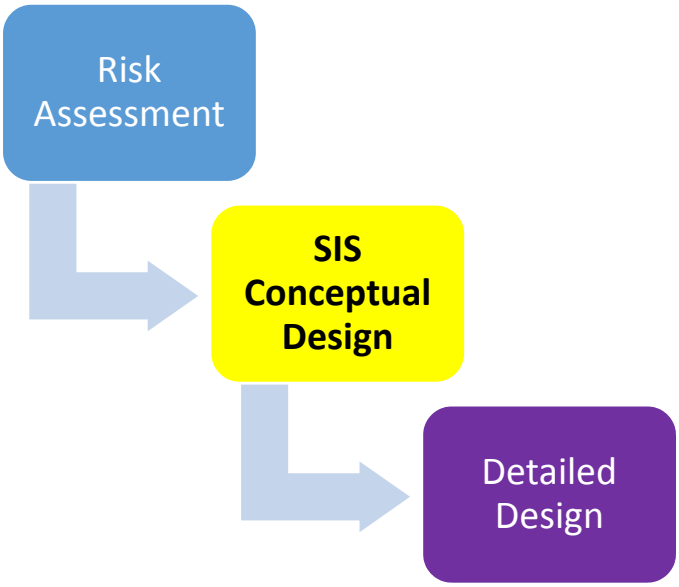

Figure 1: The Span of SIS Conceptual Design

For the full Safety Lifecycle, refer to Figure 8, in Clause 6 of ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), referred to in this document hereafter as simply "IEC 61511". As more process industry end-users strive for compliance to IEC 61511, the greater the need for competent individuals and project teams to execute projects that inherently incorporate the Functional Safety Management Plan (FSMP). This ensures the scheduling of the recommended and required stages of Functional Safety Assessment (FSA), and other key process safety activities. These requirements, as well as the ramifications of running projects without them considered in a timely manner, will be discussed in the sections below.

The cost-saving activity of LOPA validation referred to as "IPL Select" will be explored, that intersects Safety Instrumented Function (SIF) and Independent Protective Layer (IPL) conceptual design in the final stages of Risk Assessment. IPL Select is an up-front investment from a SIS FEL perspective that can provide a significant payback, minimizing potential rework and schedule delays.

The ability to successfully integrate key activities of Safety Instrumented System (SIS) conceptual design into capital projects, grandfathered processes, and process upgrades is paramount in reducing process risk to a tolerable level. Designing and installing IPL that satisfy the sustainability aspects of IEC 61511 requires personnel competence and strategic planning within the SIS Engineering discipline, and between disciplines.

SISs are often regarded as having a very high initial and maintenance costs. However, as the late Trevor Kletz stated: "There's an old saying that if you think safety is expensive, try an accident. Accidents cost a lot of money. And, not only in damage to plant and in claims for injury, but also in the loss of the company's reputation." The cost of a process incident, SIS design and installed costs, and costs of spurious trips are considered in SIS benefit-to-cost ratio calculations. But the costs of company reputation and potential long-term lost revenue is nearly impossible to quantify. A properly design, installed, tested, and maintained SIS reduces the likelihood of process risk and ensures the sustainability of the SIS Safety Lifecycle.

In this document, projected project cost savings and schedule delays will be presented for various case studies. The values and delays expressed are in terms of the specialty SIS engineering firm labor and the client engineering labor. The estimated costs of EPC rework is taken into account where noted. All other 3rd party labor, travel, and expenses are not included in these case studies. The estimated return on investment therefore is estimated at reasonable minimum. The cost of design changes that propagate can increase costs and schedule delays by multiple factors. The case studies are calibrated based on SIS project experience to an SIS project with 24 SIL1 and SIL2 SIF, and 72 non-SIF protective layers.

It should be noted that the project samples used in the calibration applying the principles and recommendations in this white paper range from over 15 years' experience and involvement in large projects with greater than 100 SIF, medium-sized projects, and small projects with less than 10 SIF. Implementing recommendations herein can reduce EPC and specialty engineering firm re-work and change orders.

SIS Engineering – an engineering discipline

SIS Engineering in itself is an engineering discipline that combines numerous facets of engineering into one. It is not imperative to have an "SIS Engineering" department within a large EPC firm, but EPCs, integrators, OEMs, and end-user organizations should fully understand what the SIS Engineer's function is in the project. As with all engineering disciplines, an error or delay in the propagation of engineering data flow, misinterpretation, or insufficient data, can inflict costly changes and delays in design, installation, and start-up. With SIS Engineering not yet established as a curriculum in universities, SIS Engineers develop from the fields of process controls, process engineering, or electrical engineering backgrounds. There are several organizations that provide course work that can introduce the requirements and intricacies of SIS Engineering (ISA, Exida, and TuV). But, as true with all else, practice makes perfect. Careers focused on projects requiring conformance to IEC 61511 enable those responsible for filling roles in the safety lifecycle to apply lessons learned and envision obstacles and challenges that other project disciplines may not.

A Project Execution Plan that integrates Functional Safety

A project is most successful when the Project Execution Plan (PEP) and the Functional Safety Management Plan are coordinated and synchronized. Not considering the inter-related process safety data flow and activities can render an SIS project requiring re-work, assuming oversight and reviews of the design recognize these errors. If not recognized, process risk gaps may covertly be developing. The roles of different organizations that are critical to the success of a project (the end-user, the Process Safety firm, the EPC, and/or OEM), as well as the individuals within these firms, must be understood and agreed-to by all parties and documented in the PEP in its roles and responsibilities matrix. Stage gates and deliverable freeze-points must be established to maintain control and prevent rework. For example, two large SIS projects in the Oil & Gas industry did not have well defined SIS roles and responsibilities, stage gates, and freeze points established between the end-user, the EPC, and the process safety contractor. Communication paths were not established to transfer prompt notification of changes between the EPC and the SIS Engineering firm. This resulted in substantial (6-digit) project overruns and change orders. After implementing new project workflow changes, which included stage gates and strategic freeze points, the 3rd and 4th projects executed in the series experienced a significantly increase in the recognized contribution of the process safety engineers, and reduced the amount of change orders and overall project implementation costs significantly.

Lesson Learned: Integrate SIS Engineering deliverables into the Project Execution Plan. Not doing so will render costly overruns and schedule delays, especially on large projects.

Where SIS Front-End Loading begins

We'll assume the methodologies of Hazard and Operability Study (HAZOP) and Layer of Protection Analysis (LOPA) are the risk assessment methodologies employed in this paper, whether applied to greenfield processes (new installations), or brownfield processes (existing processes).

Historically, the SIS Engineering discipline begins after risk assessment, however experience has shown that an intermediate step can save a significant amount of time, potential re-work costs, and avoid downstream schedule delays. This intermediate step referred to as of "LOPA Validation" and "IPL Select" assesses and refines the existing and proposed credited protection layers in closing the process risk gaps for each high hazard consequence of concern.

What is LOPA Validation and IPL Select, and where does it fit in regards to the Safety Lifecycle?

IEC 61511 clause 9.5.1 specifies "The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode, and dependent failures between protection layers and the BPCS are sufficiently low in comparison to the overall safety integrity requirements of the protection layers."

LOPA Validation and IPL Select includes the participation of a senior Risk and SIS FEL individuals (well versed in the allocation of protective layers) to work with the LOPA team to:

- verify that the hazard scenarios are clearly documented and follow client and RAGAGEP standards. This includes initiating cause, consequence, and IPLs to close any gaps.
- verify that the target risk reduction assigned to the SIFs in each LOPA scenario is accurate and generally achievable with a reasonable test interval before the SIF engineering effort commences
- assist in providing alternative solutions for gap closure
- assist in confirming the IPL requirements of dependability, auditability, independence, diversity and physical separation of IPLs against initiating events and other IPLs on the same cause-consequence scenarios
- assist in providing process safety times and IPL response times are adequate to ensure the IPLs will prevent the hazard
- identify potential common cause failures that may require alternative means of risk reduction calculations or selection of other IPLs
- identify lower cost IPLs if available
- obtain the buy in and support from the end-user's operations staff on the planned credited IPLs.

Figure 2 below depicts the LOPA Validation and IPL Select activity as an intersection of Risk Assessment and SIS Conceptual design.

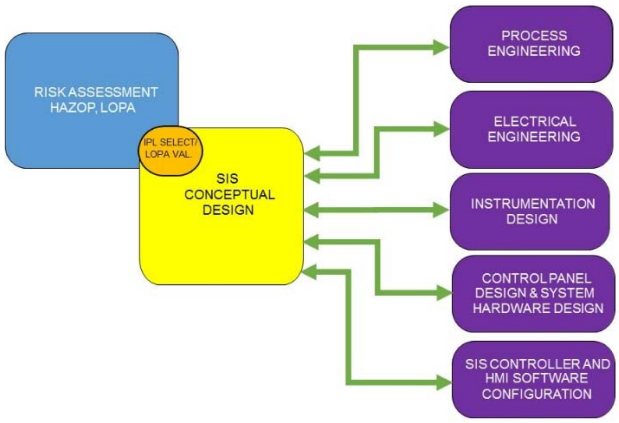

Figure 2: LOPA Validation and IPL Select – Where SIS Front End Loading intersects Risk Assessment

By involving the SIS Engineering Lead in the LOPA Validation and IPL Select review, the SIF functionality and integrity requirements are further refined, proving a smoother transition of project data flow.

In the case of the SIS project originally encompassing 24 SIL1 and SIL2 SIFs, and 72 non-SIF protective layers defined from the PHA/LOPA, we assume that reconvening of the LOPA and subsequent changes invoke the following changes: 6 SIFs are added, 6 SIFs are modified, and 12 non-SIF IPLs are added. The anticipated minimum level of effort savings and schedule impact would be:

Estimated cost (hrs) and schedule benefit of performing IPL Select:	
Hours of downstream rework due to invalid or modified IPLs:	426.0
Hours of IPL Select - 3-day including end-user labor:	-166.0
Potential savings (not including EPC):	260.0
Potential startup delay avoided (in weeks, not including EPC):	4.1

It should be noted that the LOPA Validation and IPL Select stage gate meets most of the requirements of the first portion of FSA Stage 1:

- FSA Stage 1 - After the hazard and risk assessment has been carried out, the required protection layers have been identified and the safety requirement specification has been developed.

Therefore, if the end user chooses to implement LOPA Validation and IPL Select, then the FSA Stage 1 team will spend a minimal amount of time reviewing the Risk Assessment and protective layers. The same can be said of FSA Stage 2 and Stage 3.

Lesson learned: Performing LOPA Validation and IPL Select will reduce the rework of SIL Calculations, SRS and supporting documents, and can significantly impact detail design and installation/commissioning as the SIS design progresses.

Project-Impacting assumptions or decisions in LOPA Recommendations

A LOPA Report typically consists of the LOPA worksheets, an IPL List (which includes SIFs, which are by definition, IPLs), and LOPA Recommendations List. We'll focus on the Recommendations List. The LOPA Recommendations List consists of uniquely numbered recommendations that must be taken into account to follow up and validate the assumptions made in the LOPA, and to ensure that protection layers receive the intended IPL credit they are awarded. The assigned end-user management, engineering, and operations staff must follow up and either confirm or reject recommendations. The Recommendations list almost always has impact on IPL credits and also defines the integrity and functional requirements of the SIFs and other IPLs.

Executing Functional Safety Assessments

The first 3 stages of FSA as defined by IEC 61511 are executed at different stage gates of SIS project execution:

- Stage 1 - After the hazard and risk assessment has been carried out, the required protection layers have been identified and the safety requirement specification has been developed.

(Authors' note: It should be noted that SIL Verification calculations and SRS support documents are also within the scope of this assessment.)

- Stage 2 - After the safety instrumented system has been designed. (Authors' note: design is verified to meet requirements of the SRS.)
- Stage 3 - After the installation, pre-commissioning and final validation of the safety instrumented system has been completed and operation and maintenance procedures have been developed.
- Stage 4 - After gaining experience in operating and maintenance.
- Stage 5 - After modification and prior to decommissioning of a safety instrumented system.

(FSA Stages 4 and 5 are post-startup, and not addressed within the scope of this document.)

Only FSA Stage 3 is considered a shall (required) by IEC 61511, however the consideration of FSA Stages 1 and 2 is highly recommended. Holding off until Stage 3 (post-installation) can prompt late changes in Risk Assessment, SIL Verification calculations, the SRS, detailed design and installation.

Take the case of the same sample SIS project, originally encompassing a quantity of 24 SIL1 and SIL2 SIFs (combined), and 72 non-SIF protective layers defined from the PHA/LOPA as above. The anticipated minimum level of effort savings and schedule impact for Implementing FSA Stage 1 would be:

Estimated cost (hrs) and schedule benefit of performing FSA Stage 1:	
Hours of downstream rework due to invalid or modified IPLs:	578.0
Hours of FSA Stage 1; 6-day including end-user labor:	-188.0
Potential savings (not including EPC):	390.0
Potential startup delay avoided (in weeks, not including EPC):	5.5

Skipping FSA Stage 1 and performing FSA Stage 2 (which would also invoke Stage 1), but after SIL Calculations and SRSs have been developed renders a higher risk of rework and impact on schedule:

Estimated cost (hrs) and schedule benefit of performing FSA Stage 2:	
Hours of downstream rework due to invalid or modified IPLs:	1308.0
Hours of FSA Stage 2; 9-day including end-user labor:	-402.0
Potential minimal savings (including estimated EPC design):	906.0
Potential startup delay avoided (in weeks, not including EPC):	10.0

Skipping FSA Stage 1 and FSA Stage 2, and only performing FSA Stage 3 (which would also invoke Stage 1 and 2, but after SIL Calculations and SRSs have been developed and the installation of the SIS, prior to startup renders an even higher risk of rework and impact on schedule:

Est. potential cost (hrs) and schedule delay waiting to perform FSA Stage 3:	
Hours of downstream rework due to invalid or modified IPLs:	1468.0
Hours of FSA Stage 3: 13-day including end-user labor:	-348.0
Potential savings (not including EPC):	1120.0
Potential startup delay avoided (in weeks, not including EPC):	22.0
Estimated Equipment and installation costs:	$118,260

Lesson learned: Waiting on the first FSA being performed at Stage 3 can have significant impact on startup and rework. Discovery of risk assessment and design errors before startup can invoke costly delays – of several weeks.

Consideration of Process Safety Time

According to the CCPS Guidelines for Safe and Reliable Instrumented Protective Systems Process Safety Time (PST) is "the time period between a failure occurring in the process or its control system and the occurrence of the hazardous event." Whereas IPL Response Time is "the time necessary for the IPL to detect the out-of-limit condition and complete the actions necessary to stop the progression of the process away from the safe state." Per ISA-TR84.00.04, it is recommended that the required IPL Response Time be no more than half the PST.

If the PST calculations are not performed prior to the Issue for Design (IFD) SRS, then a SIF may be fully designed, only to find out that its response time is not adequate in preventing the hazard. This would also be true for any other IPL that was credited in the same hazard scenario and typically involves an alarm with operator response. Under these circumstances, the LOPA Team would have to be reconvened, and additional IPL(s) would require significant conceptual design rework.

The rework cannot be accurately estimated for the process safety specialists, and the cost of re-design is based on the alternate design solutions to be put into place.

Note that a less drastic measure may be by adjusting the SIF trip point closer to the process control trip point, providing a greater process safety time, thus allowing more time for the SIF to respond and be proven effective. The same applies to alarm-type IPLs, BPCS interlock IPLs and SIFs: adjusting the trip/alarm point closer to the process control setpoint will provide the operator more time to respond to the alarm. This may not be feasible in some cases.

Lesson Learned: PST must be calculated which drives the IPL Response Time requirements for the IPL. These calculations are often delayed due to notification of the end-user process engineering for data. It is critical that these calculations are performed before SRSs are finalized. Concentrate first on the fast-moving processes – (eg. gas blow-by, knockout pot carryover, small vessels with relatively large

volumetric turnovers, and accumulation of unburned fuel in a firebox). Communicate the requirements after risk assessment so that the SIF components (sensor response time, sampling times, and valve actuation) can properly be addressed.

Proof Testing isn't an afterthought

Developing manual and automatic proof test procedure guidelines after the SRS has been developed can render functions untestable (e.g. turbine over-speed, high level in a vessel where level switch is side-mounted), invoke lower proof test coverage, and impede the sustainability of your SIS. Clause 16 (of 19 total) of IEC 61511 can mislead a junior SIS designer into believing it is one of the last steps in the Safety Lifecycle. But proof testing philosophies should be established before SIL Verification calculations and must be established before or during initial SRS development. Proof testing philosophies should be vetted with the end-user when other aspects and parameters of SIL calculations are being established.

Recall that a SIF is made of a sensor subgroup, a logic solver subgroup, and a final element subgroup. And many SIFs share the same final elements; for example, a number of SIFs for a boiler take action by closing main and pilot fuel valves. Since IEC 61511 allows segmented testing, identifying common subgroups between SIFs can be an opportunity to more efficiently test the final elements. There is no better function test than a full end-to-end SIF proof test, because it tests the functionality of all components in the system including relays that may be between the logic solver and field devices. But in most cases, full end-to-end proof tests are disruptive to the process while it is running. Therefore segment proof testing, which requires carefully managed bypasses, is often required.

Plant turnaround intervals are also important because offline proof testing, which may account for the majority of final elements of many SIFs, must be performed during these outages. Automatic testing is often employed to detect a proportion of dangerous failures in between full function tests. Automatic testing is usually established as a requirement during SIL Verification calculations.

Assessing the availability of offline "Train" testing (e.g. Compressor Train A is down and isolated from the process while Compressor Trains B and/or C are running) can provide opportunities for testing in between major turnarounds.

Lesson Learned: Integrate proof testing into the thought processes of SIL Verification and integrate the test philosophy of the SIF into SRS development. Obtain end-user operations and maintenance approval of testing and initial templates for both full function and device-level functions.

Other Sustainability requirements of the IEC 61511 Safety Lifecycle

The IEC 61511 Safety Lifecycle is a series of processes that circle back to the Hazard Analysis and Risk Assessment, as categorized below:

- Historical Testing data and Demands on SIFs:
    - Proof test data to update the assumed failure rates used in SIL Verification calculations. This affects the Probability of Demand (PFD_{avg}) achieved by SIFs that should be entered back into the LOPA IPL credit.

    - Demand frequencies of initiating events assumed in the LOPA
    - Demand frequencies on SIFs
- Management of change
    - Requires an assessment of whether or not the process change(s) invoke new hazards
    - If hazards are introduced, then gather PSI and loop back to PHA/LOPA and repeat the lifecycle
- PHA Revalidation
    - On a 5-year interval revalidate your entire process covered by 29CFR119.1910 – which also means gather PSI and loop back to PHA/LOPA and repeat the lifecycle.
- record SIF sensor bypass information,
- determine your overall health of process risk that takes into account observed failure rates, bypassing, and late proof testing

Lesson Learned: Feedback data is difficult to manage without appropriate infrastructures in place. IEC 61511 requires that this feedback is taken into account, and proper action taken to reduce process risk. Electronic tools are becoming available to manage the feedback data and integration.

Last but not Least: Ensuring Competency in the Safety Lifecycle

Clause 5 of IEC 61511 clarifies that "Persons, departments or organizations involved in safety life-cycle activities shall be competent to carry out the activities for which they are accountable."

This requires not only the technical aspects of SIS conceptual design, but also in project planning, and one of the most important aspects is the synchronization of planning.

Additionally, the ability to recognize obstacles early in any project execution is key in removing or reducing the impact of those obstacles. This ability comes with experienced teams that have depth in the various phases of the Safety Lifecycle, and the interconnections of these phases.

Significant efforts can be applied to all phases of the safety lifecycle, but the ramifications of not ensuring the competency in the assigned roles within the safety lifecycle can have devastating impacts on project costs, schedule, and unrealized process risk. After an SIS project is complete, unrealized process risk is manifested in invalid protective layers and/or testing procedures that do not fulfill the assumed credit, functionality, and integrity assigned in risk assessment. The cost is a higher likelihood of an incident and not managing the process hazards to a company's tolerable risk. The incident itself can be estimated using formulas, but the impact to people and an end-users financial well-being and reputation cannot be quantified within a high degree of accuracy.

Conclusion:

Topics addressed in this paper were learned from experience in operations, control systems integration, controller and HMI configuration, instrumentation, risk assessments, maintenance, plant management, and SIS Engineering. Some come from personal experience, training, incident and near miss reports, Chemical Safety Board publications, and various other sources. Many in the chemical and petrochemical industry have learned from their own and others' mistakes.

This paper summarizes a portion of the lessons learned in implementing SIS and other protective systems in the chemical, petrochemical, oil & gas, food & beverage, power, and pharmaceutical industries. The intent of this white paper is to assist readers in reducing the costs of rework, avoiding schedule delays, delivering projects that meet IEC 61511 sustainability requirements, and ultimately minimize process hazard risks to a tolerable level for owners and operators.

References

1. ISA. *Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Parts 1 - 3*, International Society of Automation, Research Triangle Park, North Carolina, 2004.
2. ISA. *TR84.0.04 Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod), Part 1.* International Society of Automation, Research Triangle Park, North Carolina, 2005.
3. *CSB Video Excerpts from Dr. Trevor Kletz*. Dr. Trever Kletz. 13 Nov. 2013. Web.
4. OSHA. *29 CFR Part 1910.119, Process Safety Management of Highly Hazardous Chemicals*. U.S. Federal Register. Feb. 24, 1992. Web.
5. CCPS. *Layer of Protection Analysis: Simplified Process Risk Assessment.* Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2001.
6. CCPS. *Guidelines for Safe and Reliable Instrumented Protective Systems.* Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2007.