MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

18th Annual International Symposium
October 27-29, 2015 • College Station, Texas

ISA84/IEC61511 SIS Functional Safety Compliance: It's a Journey Worth Taking

Curt Miller, PE, CFSE
Partner/Principle Engineer, exida Consulting LLC
cmiller@exida.com

Dan Poston, PE, TÜV FS Eng
Global Engineering Services (GES), LyondellBasell
Daniel.Poston@lyondellbasell.com

Denise Chastain-Knight PE, CFSE
Senior Functional Safety Engineer, exida Consulting LLC
dchastainknight@exida.com

Abstract

Achieving full functional safety compliance at a plant will not just happen; it takes a focused effort from dedicated personnel and a supporting management staff. It's a lot of work, but the potential safety and reliability benefits are well worth the investment. This paper will walk through the steps employed at several sites in Texas and hopes to provide stimulus for others to follow suite.

The first ISA 84 (ISA 84.01-1996) functional safety standard initiated the safety lifecycle; the second, internationally adapted version, ISA 84 (ISA 84.00.01-2004) refined the process through the Functional Safety Management (FSM) plan and various other vital additions. Each helped provide a sturdy framework for an expected sustainable process for the remainder of the subject facility's life and are considered good practices by OSHA for PSM.

It is fully believed that if done properly, the end result of applying the ISA84 standard to complete compliance will be a safer and more cost effectively controlled process environment.

1. Functional Safety Management "It's All in the Plan"

The first ISA 84 (ISA 84.00.01-2004) objective is to specify safety lifecycle (SLC) management and technical activities needed to implement the safety instrumented system. It should designate responsibilities for each SLC phase and the activities within that phase.

The basic FSM tasks include:

1. Defining a safety lifecycle process. Most companies are already following this type of process for each safety system project. All that is usually still needed is to summarize the complete process, lay out the required inputs and outputs of each safety lifecycle phase so that everything is consistent, and adjust timing of some activities to provide inputs in a timely manner.
2. Developing a functional safety management procedure. For most companies, this will basically be the safety system installation's reference document. It will list the general installation structure - naming each of the safety lifecycle steps, identify the guidance documents that apply, establish roles and responsibilities, and define competency requirements.
3. Develop a project execution safety plan. Competent project managers know successful projects begin a project with good planning and only need to expand content to address the functional safety requirements. An example is shown below:

CLIENT NAME :						Page 2 of 8			
Project :						PSP No.: 01		Version: 01	
CLIENT ORDER No. :				exida REF :		DATE OF ISSUE:			
No.	Activity	Input	Process	Verification Record/ Output	Responsible Verifier	RESPONSIBLE			
						exida	CLIENT	VERIF. TYPE	Date
1.0	CLIENT Enquiry	CLIENT request	Sales procedures	Quotation File			A		
1.1	Prepare Quotation	Scope of Work	Quotation Preparation	Quotation File CLIENT Quotation		A			
1.2	Review Order against Quotation	Acceptable Purchase Order SRS	Order Acceptance procedures CHK-SRS-V1 SRS Review Checklist	Order File Verified SRS per IEC 61511	PM	R H			
1.3	Order Entry	CLIENT Order	Project Management	Computer Records		H			
1.4	CLIENT Kick-off Meeting	CLIENT Order Scope of Work	Project Management	Minutes of Meeting		H			
2.0	Produce Project Safety Plan	TEM-PSP-V1	PRC-FSM-V1 Functional Safety Management	Project Safety Plan for use throughout project Project Schedule	PM	A H	A	SM	

Table 1: Project Execution Safety Plan

Functional safety management (FSM) is specifically noted to act as an extension to existing monitored quality systems and processes. This quality-based philosophy of “plan, execute according to plan, verify, document, and improve based on the resulting experience” carries through the entire safety lifecycle.

1.1 FSM Issue #1: Management Must “Buy In” or the Process Will Fail

For a manager, the compliance requirements noted in this paper should only involve a moderate investment in time and resources. However, they do require a strong and ongoing philosophical commitment since that is where the benefits really build upon each other. As with most procedures and methods of organizing work, one can either drown in the paperwork or use it as a lifeline to cost savings and other improvements. The difference will come down to how well the process is managed. All documentation should provide a net value or else it should not exist.

1.2 Other FSM Issues Found in Functional Safety Management Implementation

The biggest issue found when trying to implement FSM is that many contractors employed to support SIS installations did not fully understand the requirements. Hence, such projects took their normal design path and many of the safety lifecycle requirements were not met in their logical order. In such cases, costly redesigns occurred where original equipment was

underspecified. In other situations, equipment was overspecified and more redundancy was procured than required.

Another issue found in meeting FSM compliance was completing the Functional Safety Assessment (FSA) after installation and commissioning and just before start-up. The hardest part of fulfilling this requirement is timing. One user stated “No way - it will never be obtained in practice. How can a company go through all the preceding safety lifecycle steps while operations is breathing down the FSA assessor’s neck?”[1] Having a strategy already in place that plans for the FSA in advance and incrementally doing the earlier stages will save a project considerable headache resulting from damaging, last minute mandated inclusions.

1.3 Example of Flawed FSM Execution

In one large installation, FSM practices were not applied in a systematic manner. After the facility started up, several near-misses resulted and a FSA audit team came in to review gaps. Since there were numerous infractions, the facility start-up was delayed for a significant period and deferred productions cost was estimated in the millions USD.

2. Completing Thorough PHAs

Process Hazard Assessment (PHA) follows the process design step in the functional safety lifecycle. New process plant design and existing facilities have included risk assessments associated with their unique processes for many years, it was not until 29 CFR 1910.119, Process Safety Management (PSM) for Highly Hazardous Chemicals [2] that it became a formal requirement in the U.S. Some equivalent requirements are usually present in other parts of the world, but not always.

2.1 HAZOPs

Most process plants use HAZOP or some variation; the key item is to make sure that there is a systematic way to identify all potential hazards so the risk team can determine how to manage each one. It is rather hard to protect against an unknown, undefined hazard. Although specialist advice may be required to determine which method may work best. Generally speaking, HAZOPs are favored for their thoroughness, since the whole plant is reviewed node-by-node, with a detailed set of guide words applied to each characteristic of the process.

The main advantage of a clear, concise PHA hazard identification review is through the information it provides to the SIL determination process. If the PHA is done and documented well, then the layer of protection analysis (LOPA) can be completed more efficiently and more accurately.

2.2 PHA Issues

A publication titled "Good practice and pitfalls in risk assessment" [3] notes the following instances of problems that have been witnessed in the US Gulf Coast process industry:

- Case Study 9: Not involving a team of people in the assessment/not including employees with practical knowledge of the process/activity being assessed
- Case Study 10: Ineffective use of consultants' (i.e. Not insuring that the staff within a company have a deep understanding of the risk assessment)

- Case Study 11: Failure to identify all relevant modes of operation' (i.e. All non-steady state operation modes)
- Case Study 12: Failure to consider common cause failures' (example - Four (4) pumps located close to a highway that were vulnerable to being hit by a vehicle)
- Case Study 16: Inappropriate use of generic failure data (i.e. Specific data to the product / application is always better for both risk analysis and safety system verification.)

With this key activity leading the rest of the safety lifecycle practices, risk assessments should always be performed carefully to avoid these types of mistakes.

2.3 Example of Flawed PHA

In a recent application, a truck loading node was not well defined during the design phase HAZOP and a temperature control failure was not captured. The second PHA revalidation team discovered that low temperature carbon steel piping embrittlement could result. Fortunately, the site had not seen such a failure, but the system was placed “out of service” until the design flaw was corrected.

3. SIL Determination

There are various graphical and numerical techniques to determine the required SIL value to achieve a tolerable risk. Those cited in ISA84/IEC61511 follow in Table 2.

Ref	Annex	Name	Origin
1	A	ALARP* (As Low as Reasonably Practicable)	UK **
2	B	Semi-Quantitative	USA
3	C	Safety Layer Matrix	USA
4	D	Calibrated Risk Graph: Semi-Qualitative	UK + Finland
5	E	Risk Graph: Qualitative	Germany
6	F	Layer of Protection Analysis	USA

Table 2: Comparison of different SIL Selection Methods

Each of these methods should give roughly the same answer if they're "calibrated" to the same tolerable risk. The real choice in technique depends more on what fits best with a company’s existing risk management philosophy and procedures. For each hazard, the SIL technique must take into account:

1. The corporations' tolerable limits
2. Full and mitigated consequences of each hazard
3. Root cause or initiating event frequency
4. Number and effectiveness of independent safeguards

If there's a gap between the tolerable and current hazard frequency (taking into account the applicable safeguards, but not the SIF), then added protection is required. It can be either a SIF or other layers of protection.

3.1 Issues with Combined PHA/SIL Determination

There are "pros and cons" about whether or not the SIL determination should be done simultaneously with the PHA or in a separate meeting. Such a debate was documented in an earlier paper titled "Joint PHA & SIL Facilitation – Successful Implementation Steps"[4]. On the whole, it is the authors' opinion that a combined PHA/SIL analysis can be done competently if the facilitator has the background in both risk identification concepts and functional safety, and the procedure structure supports intent. With such a background, the facilitator sees the "whole picture" and can efficiently utilize the PHA team to obtain key data for not only the PHA and SIL determination, but even go far enough to capture essential data for the SRS, PSV setpoints, and alarm rationalization.

3.2 Example where SIL Consistency was not Achieved

One client site that applied SIL determination had results for similar compressor applications that ranged from SIL0 to SIL3. Another had similar results for fired heater applications. It was found that the PHAs had considerable variance in consequence valuations and that each facilitator applied different IPL rule-sets. To reconcile the differences, the PHA and SIL determination teams had to reconvene which resulted in unnecessary resource cost. Management is now wary of the SIL determination process and the team must redeem itself on future applications.

4. Development of the Safety Requirement Specification (SRS) for SIFs

The safety requirements specification (SRS) is the primary reference for the remaining parts of the safety lifecycle. This document is especially important since it often marks the handoff of safety lifecycle responsibility from one company to another and is a key project communication document. Once these requirements are clearly laid out, they will significantly help the remaining design, installation, and operation phases of the safety systems lifecycle. The SRS addresses both functional and integrity specifications as stated below.

4.1 SRS Functional Requirements

The functional part of the SRS describes what the safety instrumented function does when harm from a given hazard is imminent. Required details include process inputs and their trip set-points, safety system outputs and their actions, and the logical relationship between each of them. This is a similar requirement for any control loop within the basic process control system, but in the SRS case, improved safety, not production, is the goal. Functional requirements that have been included in both editions of ISA 84 include:

ISA 84 Clause		**Stated Functional Requirement**
1996	**2004**	
5.3.1	10.3.1	Defined safe state
5.3.2&3	10.3.1	SIS process measurements and their trip points
5.3.4	10.3.1	SIS process output actions
5.3.5	10.3.1	The functional relationship between process inputs and outputs
5.3.7	10.3.1	Manual shutdown detail
5.3.6	10.3.1	Energize or de-energize to trip specification

ISA 84 Clause		Stated Functional Requirement
5.3.8	*implied*	Action(s) to be taken on loss of energy source(s) to the SIS
5.3.12	10.3.1	Method to reset the SIS after a shutdown

Table 3: SRS Functional Requirements

4.2 SRS - Integrity Specifications

The integrity part of the SRS describes "how well" the safety instrumented function needs to work when harm from a given hazard is imminent. In this part of the SRS, it must specify such things as the required SIL, as well as necessary diagnostics, maintenance, and testing. The specified integrity requirements that have been included in both editions of ISA 84 are included in Table 4.

ISA 84 Clause		Stated Integrity Requirement
1996	**2004**	
5.4.3	10.3.1	Proof test intervals
5.3	10.3.1	Response time for the SIS to bring process to safe state
5.4.1	10.3.1	SIL & operational demand mode (demand or continuous)
5.4.4	10.3.1	Maximum allowable spurious trip rate
5.3.10	10.3.1	Failure modes & desired response of the SIS (alarms, auto s/d)
5.3.11	10.3.1	All interfaces between the SIS and any other system (BPCS, ops)
7.7	10.3.1	The extremes of all SIS environmental conditions
5.4.2	*implied*	Requirements for diagnostics to achieve the required SIL

Table 4: SRS Integrity Requirements

4.3 SRS Pitfalls

There are multiple faults that can creep into a good SRS. Several include:

- Issues could start with the input where the SIL determination team may have been given a poorly executed PHA as an input
- Problem with SRS documentation control which include when it:
  - Is out of date because it was not maintained
  - Has no revision control
  - Is missing important requirements.

Having a "living" SRS and competent implementers overcomes such issues.

4.4 Examples of Flawed SRS Documentation

As might be expected, there are a number of frightening real life examples of SRS problems. Some direct quotes from system integrators [1] include the cases where:

1. "Change notes were verbally coming in, often by phone."
2. "Two companies sat down to go over their released-for-fabrication drawings, which were fully signed off, but the two sets of drawings were different."

3. “The SRS gaps that we regularly witness are where no function test intervals, test facilities, or spurious trip requirements are specified.”

It is for these reasons that a project team may want to incorporate a Functional Safety Assessment (FSA) at this point in the lifecycle to ensure that adequate information is available for design, especially for those critical SIL2 & SIL3 applications.

5. Confirm the SIF Conceptual Designs

The SIS conceptual design step involves taking the preliminary SIF list based on the SRS and investigating each SIFs makeup. Associated SIF components, voting configuration, and testing plan for each SIF are confirmed before being used in the SIL verification calculations.

5.1 Conceptual Design Issues

It is surprising how much time is required by a functional safety engineer (FSE) to validate a SIF’s conceptual design. Why? The problem is three-fold. First, the PHA hazard scenario is stated so vaguely that even the process engineer has a hard time specifying what is required to get to the safe state when reading the PHA post-facto. When reviewing cause and effects, a myriad of actions may be listed, but not all are required to remedy the hazard scenario as stated. It is paramount to get the sensing and actions correct to meet stringent SIL requirements. Any excesses will either not meet the SIL requirement or will become a burden for the maintenance phase of the safety lifecycle.

The second problematic issue with SIF conceptual design is accounting for all the components involved to meet the SIL target. In many cases, critical loops that have been verified using simplistic models are found deficient when all the mechanical and electrical diagrams have been reviewed. Interface components, especially non-SIL rated and programmed devices, could deliver one SIL level lower than what was originally thought true. It is always prudent to do SIF conceptual design homework upfront and accurately reflect the design intent in the models.

Finally, is the proposed SIF fully independent of the initiating cause and other IPLs? Care should always be included in designs that involve control valves since they normally involve some level of common cause. Such issues are compounded if the facilitator and team for the SIL determination session do not fully understand IPL requirements or mis-apply IPL credits. In other cases, the PHA team as a whole may not have addressed all causes and in such cases the concept design engineer must be familiar enough with the process to diagnose such issues.

5.2 Example of Flawed Conceptual Design

In a recent project, turbomachinery SIFs were being evaluated for a SIL2 application. All was thought to be fine since the system included SIL3 components for the sensors and logic solver and the final element was partial stroke tested. Unfortunately, late in the design cycle, an emergency trip device was discovered in the mechanical drawings that was critical to the SIF since it acted as an interface component for dumping the hydraulic power fluid. . The design team found an alternative solution to avoid adding an inline steam valve (estimated at $300k), but not every team is so fortunate.

6. SIL Verification Calculations ("Testing the Metal" of SIFs)

Each safety instrumented function (SIF) design must now be verified through probabilistic calculations. (See Clause 11.9.1) The key here is to do the probabilistic calculations for each SIF which will verify safety and spurious trip performance criteria as well as optimize design to economically meet the requirements for each different function. The spurious trip discovery could be quite significant for plant production where it has been stated that up to 18% of plant trips are associated with instrumentation.

Verification calculations are performed after the other conceptual design steps have been completed at draft level. (See Safety Instrumented Systems Verification -Practical Probabilistic Calculations [6] for more information on this subject.) If calculations show that the draft design does not meet the SIL target, the choices are:

1. Shorten the testing interval, but not beyond the practical point for operations
2. Select better technology/equipment.
3. Add redundancy or other IPLs

The conceptual design iterations will continue until the SIL or risk reduction target is met with the overall most economical system.

6.1 Issue #1 with Performing SIL Verification - Data

Finding data is a big issue in completing SIL calculations. If site generated data was available, naturally that would be the best option. In its absence, there are several industry databases being published by organizations like OREDA, AIChE, IEEE and others. This data often provides a total failure rate for an instrument type, but does not detail conditions or modes of failure. While the data in industry databases is not product specific or application specific, it does provide useful failure rate information especially for comparison purposes.

Another choice is utilizing "Failure Modes Effects and Diagnostic Analysis" data. This technique has been developed many years ago [6] specifically to obtain data needed for SIF verification calculations. A FMEDA is done by examining each component in a product. For each failure mode of each component, the effect on the product is recorded. The process is extremely detailed and systematic. FMEDA results can provide instrument specific failure rate data that can be far more accurate than generic database information. The method depends on electronic and mechanical component data [7] for its accuracy so it is important that the data be calibrated for the process industry environment. This is done by comparing results to actual field failure data [8].

6.2 Issue #2 with Performing SIL Verification - Meeting all SIL Requirements

Besides SIL (i.e. PFDavg) calculations, each safety function must meet a minimum hardware fault tolerance (HFT) based on the target SIL requirement listed in the architectural constraint table (11.4.1). This design element was included to provide an extra layer of protection to address the uncertainty in the failure rate of the various system components.

For example, the table from ISA 84.00.01-2004 shown below is used for field devices.

SIL	Minimum hardware fault tolerance
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

Table 5: Architectural Constraints for End Devices

Using this table for a SIL2 target, the design must use at least two final elements in a dangerous failure tolerant configuration (i.e. 1oo2) even if SIL verification results show an overall PFDavg of SIL2 with only 1 device is achieved.

One additional requirement is based on using “assessed” devices as safety components so that vender systematic flaws are minimized. Devices that are either certified to IEC 61508 or based on user "prior use" (Clause11.5.3) must be used to meet this requirement. Many functional safety engineers (FSEs) will choose certified components just because they don’t have a good device reliability database and the certified equipment comes with its own approved data. Either choice will require “usability” judgment based upon current installation time accumulated and specific application details.

6.3 Example on Value of FMEDA Derived Data

Many trusted devices lack certification and “prior use” justification is cumbersome. For example in steam turbine applications, data is rarely available for the trip and throttle valve. Rather than assume conservative data, one organization elected to perform a FMEDA on the device. Results supported a SIL2 attainment when using partial stroke testing and accounting for specific overspeed failure modes where a significant leak was required to fit the scenario stated.

7. Proof Testing Practices

Since OSHA 1910.119 Process Safety Management covered many of the operations and maintenance requirements, most companies are performing some level of tests. For many, the test is a full functional test from the sensor to the final device done a periodic basis that aligns with their scheduled shutdowns.

While this is still considered good practice, there may be benefits employed by utilizing upgraded diagnostic methods that are less invasive on the process. Given the capabilities of safety certified instrumentation, many of the functional proof test methods developed for relays and pneumatic instruments is not only less effective but very costly compared to more appropriate methods.

7.1 Proof Test Practice Issues

The biggest issue with proof testing is that no methods have 100% coverage of dangerous failures. To account for this discrepancy, replacement or “rebuild to new” (i.e. mission times) now must be specified for all equipment and they must be within the useful life of the component.

The second issue discovered when reviewing site test practices is that most procedures included the full functional test, but testing of the diagnostic routines was not completed. Since the associated SIFs verification included such diagnostics, such test practices had to be upgraded to

account for detection of faults, degraded failure architecture, and presentation of associated alarms.

7.2 Example of Optimized Proof Test Practice and Maintenance

As discussed in 7.1, no proof tests are 100% effective in detecting all covert faults. Due to such a limitation, turbomachinery specialists in one corporation inherently understood this issue and have been rebuilding their critical trip and throttle valves in every turnaround for years. This level of maintenance, coupled with optimized partial stroke testing techniques, has helped each site meet their SIL2 safety and production goals simultaneously.

Conclusion - Benefits of Following Compliance Plan

Executing an optimum functional safety plan will help the facility in multiple ways. A few extracted benefits from "Win/Win: A Manager's Guide to Functional Safety", include:

1. Lowering the cost of spurious trips by uncovering reliability issues
2. Proper front equipment selection and minimizing "overspecification" costs
3. More precise "realistic" PHA (Process Hazard Reviews)
4. A decrease in "specification errors" and resulting accidents
5. Universal, world-wide process standard efficiencies
6. Optimized proof test intervals
7. Impacts of production and corporate image losses can be quantified and included for a more accurate analysis

Thus each of these additive bottom line benefits, coupled with increased functional safety, can help justify the full ISA 84-2004 approach and make it a "journey worth taking". Try weighting them, putting in corporate estimates for both costs (spurious trips and different accident scenarios) and gains (manpower efficiency and production), and see if they result in good news to present to the senior management team.

References:

1. Miller, Curtis, Win/Win: A Manager's Guide to Functional Safety, 1st Edition, 2008
2. 29 CFR Part 1910.119, Process Safety Management of Highly Hazardous Chemicals, U.S. Federal Register, Feb. 24, 1992, http://www.osha.gov
3. Good practice and pitfalls in risk assessment, UK, Sheffield, Health and Safety Executive, 2003.
4. Miller, Curt and Crawford, Mike, Joint PHA & SIL Facilitation – Successful Implementation Steps, Mary Kay O'Conner Process Safety Center International Symposium, 2007.
5. Goble, W. M. and Cheddie, Harry, Safety Instrumented Systems Verification -Practical Probabilistic Calculations, NC: Research Triangle Park, ISA, 2005.

6. Goble, W. M. and Brombacher, A.C.,“Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems,” Reliability Engineering and System Safety, Vol. 66, No. 2, November 1999.
7. exida, Electrical & Mechanical Component Reliability Handbook, 2nd Edition, exida, PA: Sellersville, 2008, www.exida.com