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

20th Annual International Symposium
October 24-26, 2017 • College Station, Texas

Functional Safety Management Planning

Denise Chastain-Knight†, R. Butz, W. Donaldson
Mary Kay O'Connor Process Safety Center
Artie McFerrin Department of Chemical Engineering
Texas A&M University
College Station, Texas 77843-3122

† Presenter E-mail: dchastainknight@exida.com

Abstract

Successful implementation of the Functional Safety standards, IEC-61508 and IEC-61511 (or ANSI/ISA 84), begins with robust management planning. The Functional Safety Lifecycle includes activities at all stages of a process lifespan, including conception of a project, hazards identification, specification, design and implementation, verification and validation, operation and maintenance, and modification and decommissioning. Each phase of the lifecycle has specific requirements for the activities that must be completed, goals to be achieved by those activities and expectations of the documentation. The standards are performance based, so for a turnkey project, the path to compliance is defined by the project engineering management firm. A written Functional Safety Management Plan (FSMP) defines the desired path and success metrics to ensure functional safety objectives are met at all stages of the lifecycle. This paper will review the requirements for functional safety management planning, and share the experiences of one large capital project where the lifecycle planning and execution failed expectations.

Keywords

Project Management Procedures and Controls, Interlocks & Safety, Safety Instrumented Systems (SIS), Residual Risk Management, Alarm and Instrument Management, Automatic SIS System

Introduction

Modern functional safety standards were first issued in the late 90s and are now evolving to second generation. Regrettably, nearly 20 years later, industry is still learning to apply them effectively. IEC-61511, adopted in the United States as ANSI/ISA 84 - 2004, defines practices intended to ensure the safety of industrial processes through use of Safety Instrumented Systems (SIS) to reduce risk. OSHA has cited ANSI/ISA 84 as a Recognized And Generally Accepted Good Engineering Practice (RAGAGEP) for implementation of SIS. End users expect engineering teams to be as expert in implementation of functional safety standards as they are with any other RAGAGEP standard. Unfortunately, flaws exist in project execution that saddle end users with non-compliant systems and un-mitigated risk.

ANSI/ISA 84-2004 (IEC61511 Mod) states "Safety planning shall take place to define the activities that are required to be carried out along with the persons, department, organization or other units responsible to carry out these activities. This planning shall be updated as necessary throughout the entire safety life cycle".[1] Unfortunately, many organizations do not include development of an overall Functional Safety Management Plan (FSMP) in scope, so capital projects often lack big picture guidance. Even in the absence of an FSMP, adherence to the balance of the engineering design standards is expected, but is often not delivered. The engineering design firms' project, to design and construct a green-field nitrogen fertilizer plant in Iowa, is an example. This paper will share some of the lessons learned and how gaps may have been avoided with a comprehensive FSMP.

Background

The project, to engineer, procure and construct a world scale, green-field, nitrogen fertilizer facility in Iowa, was structured with a common project execution model. Contracted by a global producer of fertilizers and industrial chemicals, a project management team and multiple engineering design firms were to deliver a turnkey facility. Contract documents include two requirements key to the discussion in this paper: 1) the project is to comply with ANSI/ISA 84-2004 and 2) a four-year shutdown cycle for maintenance is expected. The technology providers had primary process design responsibility and a small team from corporate operations provided project reviews. Design responsibilities were distributed between technology providers based upon process area. The design basis was fixed (e.g. Rev 0 or higher P&IDs), and construction in progress when the site operations team was assembled.

Prior to start-up the site operations team completed a thorough review of the design documents, conducted a HAZOP of record, and subsequent LOPA. These efforts identified potential gaps raising questions about the adequacy of the SIS. Specific concerns included potential for previously unidentified risk, insufficiently mitigated risk, and incomplete implementation of the functional safety lifecycle.

Requirements of the Standard

ANSI/ISA 84-2004 is an adoption of IEC 61511 edition 1.0, with a minor modification to the scope. IEC 61511 was written by end users for end users. It is a non-prescriptive, performance-based standard that states requirements, but does not explicitly define how to implement them. Clause 4, Conformance to this International Standard, states:

"To conform to this International Standard, it shall be shown that each of the requirements outlined in Clauses 5 through 19 has been satisfied to the defined criteria and therefore the clause objective(s) has(have) been met."[2]

Clauses 5 -18 describe the objectives and requirements for the phases of the lifecycle. Clause 19 describes the objectives and requirements for information and documentation. To achieve compliance, users must understand the requirement of the standard and define their own procedures and process to meet the requirements.

Clause 5 introduces the lifecycle and includes the general requirement of the standard, including;

- Requirement for a management system
- Organization, responsibility and resource competency
- Risk evaluation and risk management
- Planning
- Implementation and monitoring
- Assessment, auditing and revision
- Configuration management

Clause 6 details the functional safety lifecycle model, which organizes required activities into phases, illustrates the relationship between the phases, and establishes five assessment points within the lifecycle. Figure 1 illustrates the lifecycle phases.

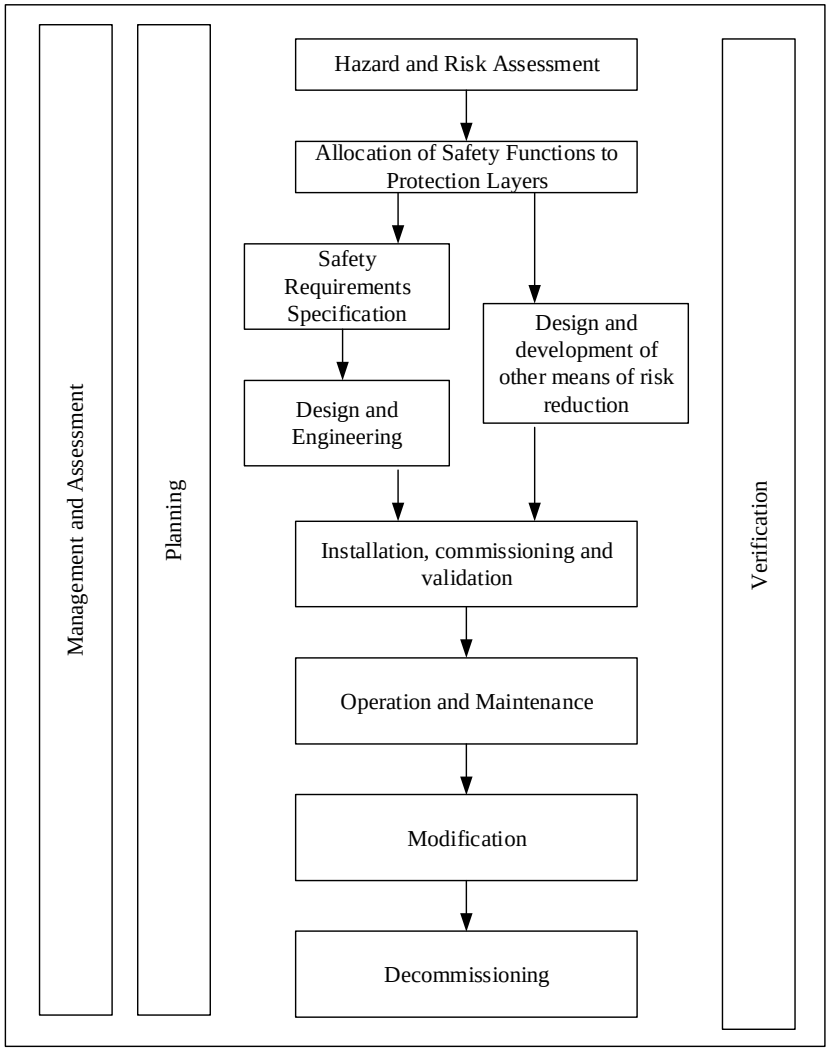

Figure 1. SIS Safety Lifecycle Phases

Clause 6 also includes a table that defines objectives for each phase, identifies clause (8-18) where requirements are stated, and summarizes the information and documentation inputs and outputs for the phase.

Planning is a required activity for all phases of the lifecycle and is a key step to establishing the scope, methodology, tools and acceptance criteria that characterize compliance. The objective of the planning process is to assure the activities of each phase of the lifecycle meet the requirements of the standard. This includes:

- the design basis and performance requirements and specification documentation;
- system testing and maintenance to assure continued reliability; and,
- documentation and analysis of performance records to confirm safety integrity is achieved.

When lifecycle activities are executed over a long period of time and by multiple teams, as is typical in large capital projects, the planning and execution activities will be recorded in many documents. In addition, there will be numerous procedures, work instructions, forms and records that support implementation of the plan. Periodic assessments (Functional Safety Audit) are required to confirm compliance. Table 1 is a summary of documents an assessor would expect to find as supporting evidence of lifecycle activities.

Document Type	**Examples : Characteristics**
Policy level Plan	Functional Safety Management Plan Philosophy: Defines the high level criteria for compliance such as applicable standards, roles and responsibilities, competency requirements, methodology & tools, workflow, schedule, documentation requirements, acceptance criteria and metrics. This document should set detailed parameters where they are important for detailed design. (e.g. proof test interval, maintenance philosophy)
Project Plan(s)	Project Execution Plan(s), Quality Management Plan(s), Risk Management Plan, Testing, Verification & Plan, Construction Management Plan: Defines the execution plan and quality control approach for parties conducting scope of work associated with the Safety Instrumented System (SIS).
Procedures	Process Hazard Analysis (PHA) Procedure, Safety Integrity Level (SIL) Selection Procedure, SIL Verification Procedure, Document Control Procedure: Detailed procedures for executing specific activities supporting the plan. Some will be global to be used by all (e.g. SIL verification procedure), others may be specific to a particular party (e.g. document control).
Work Instructions	Factory Acceptance Test (FAT) Procedure, Site Acceptance/Integration (SAT/SIT) Test Plan, Proof Test Procedures: Detailed instructions for executing a particular task, in a specific situation. Some are developed for a single use (e.g. FAT), while others are developed for repeated use (e.g. proof tests).
Specifications	SIF Safety Requirements Specification (SRS), Logic Solver SRS, Instrument and valve data sheets, equipment data sheets, typical installation details: Documents that specific the design, purchasing and installation requirements for the SIS and it's components.
Forms & Records	P&IDs, Logic Diagrams, verification reports, audit reports, inspection and proof test logs, training & competency records, non-conformance resolution log: Documents that record the basis for design (a.k.a. process safety information), conformance to requirements (e.g. training & competency logs) and records that document the testing and performance of the SIS and its components.

Table 1. Lifecycle Planning and Execution Documentation

Five functional safety assessment stages are identified in the standard; however, in ISA 84-2004, only one is required. The stage 3 assessment is conducted between the Installation, Commissioning and Validation and the Operating and Maintenance phases. All phases of the lifecycle prior to operation and maintenance are evaluated for compliance. Management and Assessment, Planning and Verification phases are evaluated for full compliance with prior phases, and planning requirements for future phases. The compliance criteria of a stage 3 assessment, is applied to the project observations within the balance of this paper.

Hazards Identification, SIL Assessment and SRS Development

The first three steps in the functional safety lifecycle are hazards identification, allocation of safety functions to protection layers, and preparation of a SRS. In this project the methods utilized in the first two steps were accepted methods, but not necessarily the best choices to establish Safety Instrumented Function (SIF) requirements for a highly integrated continuous process. The third step, SRS development was entirely omitted.

A SIS is comprised of a logic solver and many SIF interlocks. Individual SIFs are designed to mitigate the risks associated with a particular hazard scenario. Successful implementation of a SIS begins with SIL selection and establishment of the SIL target for each SIF. There are a number of methods available, each with strengths and weaknesses. A FSMP and/or supporting procedures should define what methods are to be used, and stipulate risk assessment criteria. The choice of SIL assessment method may have an influence on the SIL verification method/criteria, so a lifecycle view should be taken to pair methods appropriately. For example, a semi-qualitative method of SIL assessment should be paired with a SIL verification approach setting a minimum threshold within the SIL band (i.e. 30%).

Project phase HAZOPs and SIL Selection were completed by the two technology provider teams with corporate operations participation in all process reviews. HAZOP and SIL assessment reports for four process areas and numerous machine packages identified SIFs during the project. Operation HAZOPs and SIL Selection were completed 3-3.5 years after the project reviews with a fresh team. Operations HAZOP methodology was consistent with the project HAZOP. Both teams used different, but still acceptable SIL assessment methods, each having their own advantages, disadvantages, and verification considerations.

The project SIL assessment was performed by the engineering firms used a semi-qualitative four parameter, calibrated risk-graph method. Each parameter is divided into 2-6 rank groups considering consequence (4), occupancy (2), avoid-ability (2) and frequency of hazard (3, 6). Users assign parameter rank for each group to scenarios then step through a decision tree, similar to the one in Figure 2, to assign SIL target. The method has the advantage of being easy to use. The disadvantages are:

- the method is applied to individual cause/consequence pairs;
- assessment of safeguard effectiveness is minimal; outcome consistency relies on subjectivity of the users; and,

- results indicate SIL band but not relative position within the band.

For this reason, the assessment method should be paired with an appropriate SIL verification threshold to assure risk reduction targets are met.

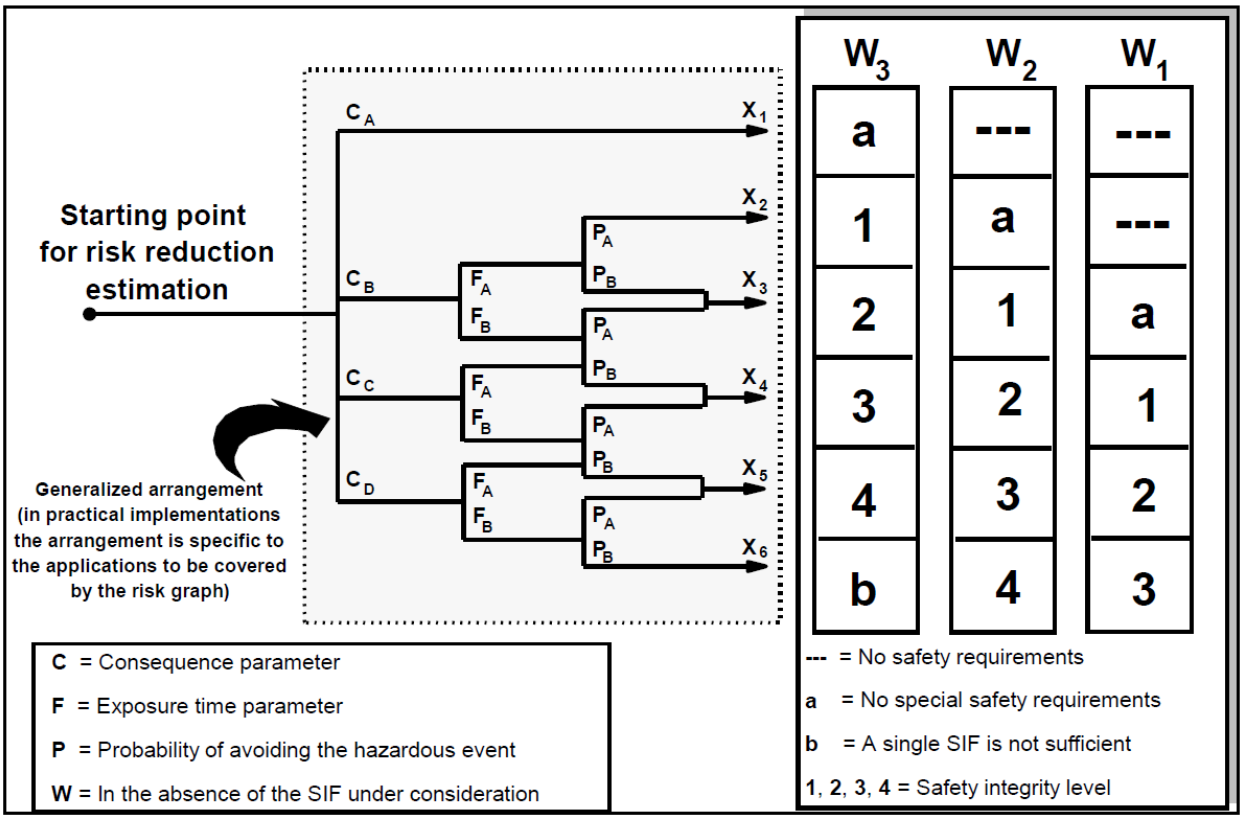

Figure 2. Example Risk-graph[3]

The site operations team elected to use quantitative Layer of Protection Analysis (LOPA) methodology for SIL assessment. This method is consequence based and considers multiple scenarios with the potential for a common consequence together. For a given consequence, a matrix is prepared listing potential initiating events (causes) vs. safeguards based on the HAZOP record. LOPA:

- defines individual probability for the initiating events;
- evaluates each safeguard for independence;
- assigns a probability of failure (PFD) for the independent protection layer (IPL); and,
- applies to the causes where the IPL may be effective.

The method is best applied by a trained team with calibrated rules for assigning frequency and probability. Key advantages of the method are that it delivers a SIL target with specified residual risk reduction factor (RRF) and the cumulative SIF demand rate is determined based on all potential causes. SIL verification is provided with a quantitative demand rate and specific PFD

target. Figure 3 illustrates a LOPA with three Initiating Events (IE), one IPL applicable to all IEs, an IPL and Conditional Modifier (CM) that apply to a single IPL each. Frequencies for IEs are set, PFDs for IPLs and CMs are assigned, then PFD for the SIF is calculated to reduce risk to the tolerable frequency. This example yields a SIF with PFD of 8.5E-3, or a SIL 2 SIF with minimum required RRF of 118.

Description

SIF 007 TAHH-9876 Process Cooler High Temperature

	Target Frequency	Calculated Frequency	Required RRF
S	0.0001	0.0001	0

People

Initiating Events	Frequency [YR^{-1}]	IPLs			CMs	Intermediate Frequency [YR^{-1}]	Comments
		SIF 007 TAHH-1234B	Turbine high steam temperature trip (turbine T-555 PLC)	TIC-1234C	Installed spare cooling water pump		
Fouling in process side of C-123	0.08	0.0085	0.1	0.1	NA	6.8E-06	Initiating Frequency set based on team judgement
TIC-1234A fails open	0.1	0.0085	0.1	NA	NA	8.5E-05	
Loss of cooling water pump	0.1	0.0085	0.1	NA	0.1	8.5E-06	

Figure 3. Example LOPA

During the operations LOPA the team defined a class of IPL identified as a Critical Protection Interlock (CPI). A CPI is an interlock that performs as an IPL, with a maximum PFD of 0.1, and is executed in the Basic Process Control System (BPCS) or a package control logic solver. CPIs are non-SIF IPLs. Application of CPIs in the LOPA reduced the number of SIFs significantly. Differences in the HAZOP team perspective, and the SIL assessment methodologies, coupled with the definition of CPI, resulted in a significant change in the SIF count and SIL target levels. SIL target distribution for the two teams are summarized in Table 2.

	Method	SIL 3	SIL2	SIL1	CPI	Total
Project	Risk-graph	5	44	159	0	208
Operations	LOPA	0	19	53	108	180

Table 2. SIL Target Distribution

Applying the LOPA approach to SIL targeting highlighted a discrepancy in determination of SIF mode. Demand is the frequency at which condition(s) may occur that cause the SIF to initiate. Frequency of proof test, or Proof Test Interval (PTI), must also be considered when determining SIF operating mode. SIFs may operate in low demand, high demand or continuous modes. Mode of operation dictates different verification, operation and maintenance requirements. Risk-graph method considers single cause/consequence pairs so SIFs are commonly assumed to be operating in low demand mode, based upon the frequency assigned to the initiating event. The project team

evaluated the design based on an annual PTI and used the risk-graph method. Initiating events were considered separately, so all SIFs were identified as low demand. The operations team considered multiple initiating events in the LOPA and set PTI based on the planned 4 year operating shutdown schedule. This resulted in the operating team identifying a number of high demand SIFs that were unrecognized by the project team. In addition, many SIFs were determined to have residual RRF requirements, some quite significant (e.g. SIL 2 RRF 303). Table 3 summarizes SIF mode and residual risk requirements identified by the LOPA.

	SIL 2	SIL 1	Total
Low Demand	3	24	27
Low Demand with residual RRF	5	2	7
High Demand	0	7	7
High Demand with residual RRF	11	20	31

Table 3. SIF Mode Distribution

The operations SIL assessment effort resulted in a reduction in the SIF count, separation of SIFs into two categories (SIF and CPI) and identification of high demand mode SIFs. In addition, the sensor and final elements included in the interlock definition of safe state was updated. ANSI/ISA 84 (IEC-61511) requires that a SRS be developed to define requirements for each function and the overall SIS performance. The standard includes an extensive list of items that are to be specified. The project team prepared the SRS for the logic solver performance, but only defined a few of the requirements for each SIF. Examples of SRS detail that were missing include:

- the requirements for common cause failure,
- SIF response time,
- process safety time,
- manual shutdown,
- reset, and
- override/inhibit/bypass function.

The SRS is used to assure suitable devices can be selected for SIF service, and it defines acceptance criteria for verification and validation activities. To address this gap, site operations separately commissioned the development of SIF SRS prior to startup. Unfortunately, the SRS was developed long after the design and procurement was complete, and construction was in an advanced stage, so implementation is a costly re-work effort.

Design and Engineering

Since SRS documents were not prepared to describe SIF design requirements, the requirements were not fully incorporated into the design. For example, the instrument and valve data sheets simply indicate something like ‘transmitter shall be SIL 2 certified’, or contain no indication of SIL requirements at all. This resulted in the procurement of unsuitable devices, which had to be

replaced, or required proven in use justification. Logic diagrams and loop sheets do not differentiate between safety and non-safety functions, therefore, the logic is not separated, so all logic in the SIS "shall be treated as part of the SIS and comply with the requirements for the highest SIL"[4]. Treating all logic in the SIS to the highest rigor will add cost to all future maintenance and modification efforts. In addition, the SIF requirements were not communicated to package vendors so multiple package systems failed to meet reliability targets.

In absence of a FSMP and SRS, SIL verification was performed inconsistently across the project areas; one team used a simplified methodology, and the other used Markov models. Both teams assumed 1 year proof test intervals, even though the plant is intended to operate on a 4 year turnaround cycle. Verification parameters, such as proof test interval, proof test coverage and time to restore, varied significantly and was often overly optimistic. Project documentation had no specific criteria noted to vet reported failure rate data for reasonableness and seek evidence that 'certificates' were prepared by an entity accredited in the IEC 61508 certification methodology.

Site operations decided to have verification calculations repeated using a single methodology and consistent basis. Three hurdles must be met in SIL verification; probability of failure (PFDavg or PFH), Hardware Fault Tolerance (HFT) (redundancy), and systematic capability. More than half the SIFs failed to meet target SIL or HFT on initial recalculation. Systematic capability was rarely achieved due to the number of non-certified devices requiring proven in use justification. Immediate corrections were made where possible. Where corrective action required more time to implement, a short term mitigation plan was developed to allow production to be started using the devices procured by the project. Complete mitigation will require a shutdown within the first year to implement the long-term mitigation plan. Costs for replacing components and completing an early shutdown will pale in comparison with the cost of the lost revenue.

Functional safety scope for the project includes three SIS logic solvers, housing a final total of 72 SIFs with 267 unique tags. Each tag represents a field device assembly made up of 2-5 components per assembly. (For example, a valve tag assembly includes the solenoid, actuator, valve and sometimes a positioner.) Seventy-seven percent of the procured components are not certified. Non-certified devices will be replaced with certified devices, where necessary (and possible). Proven in use justification must be prepared for remaining non-certified devices. The long-term mitigation plan includes:

- Replace transmitters, solenoids, actuators and valves assemblies with certified devices
- Certify valve and/or valve/actuator assemblies
- Perform a Failure Mode, Effects & Diagnostic Analysis (FMEDA) to determine model specific failure rates and complete proven in use justification for valve and/or valve/ actuator assemblies
- Add new certified transmitters, solenoid, actuator and valves to provide redundancy
- Rebuild selected large valves at increased intervals
- Certify or proven in use for multiple vendor package PLCs
- Perform proven in use justification for non-certified devices

Action plan to certify or perform FMEDA on a device does not guarantee all issues will be resolved. Should these devices not perform to the required reliability level, then additional mitigation may be necessary. For non-certified devices, proven in use justification[5] must be developed to document that the device failure rate and mode is consistent with expectations. Device performance history must be tracked and vendor input is often required. Developing a proven in use justification requires significant effort, and it may take years to develop an appropriate sized dataset.

Installation, Commissioning and Validation

A FSMP is to include planning for SIS verification, testing and validation. In absence of a FSMP, important testing activities, such as logic solver site acceptance test, site integration test and proof tests were not included in the installation, commissioning and pre-startup schedule. Proof test procedures were not included in the project turnover and had to be developed by site operations. Contract assistance was necessary to prepare proof test procedures on a fast track timeline so they would be available for pre-startup validation.

Commissioning efforts included bench tests and continuity tests. Logic was being modified during commissioning to address disconnects. To assure the proper performance of the SIFs, the site maintenance team completed proof tests and performed full-function trip tests. SIF response times were recorded and compared to the process safety times to validate adequate SIF response rate. Proof test calibrations discovered devices that were incorrectly calibrated, which indicated that bench calibration was inadequate. A number of SIF devices failed initial proof tests or failed soon after startup. In one case the percentage of devices that suffered early failure was uncomfortably high and the model (multiple devices, of the same model) was identified for replacement in all SIF applications.

While the site maintenance team was performing the validation proof and trip test, they compiled component information that will be needed for operations and maintenance phases, and clearly tagged all components as safety devices.

Operation and Maintenance

The Iowa facility is in the first few months of operations and has little site specific maintenance history at this point. Initial training was completed for operating and maintenance personnel. SAP asset, reliability and maintenance systems have been populated including proof test scheduling. A Preventative Maintenance asset management system has been developed with SIF devices classified at the highest level of criticality for safety inspection compliance. The system documents proof tests inspection and repair information, which will begin to build proven in use documentation.

Operation and maintenance planning is a work in progress. Once validation was completed, the site teams turned their attention to setting up systems to schedule and execute periodic proof

tests, capture and analyze data on system demand and device performance, and manage change. Implementation of the long-term mitigation plan is in progress including development of a modification and decommissioning plan. Remaining gaps are being closed as they are identified. Development of a comprehensive site FSMP for future use, and establishment of an assessment and auditing program are on the horizon. Much work remains for the operations and maintenance teams to completely close the remaining functional safety lifecycle gaps.

Conclusion

End users rely upon engineering contractors to complete comprehensive planning, provide expert technical guidance and deliver projects that comply with standards and RAGAGEP. In the absence of a comprehensive FSMP and failure to follow the safety lifecycle, a project can experience costly gaps in functional safety management and fail to reduce process risk. Correcting the deficiencies in project execution is costly, time consuming, and may leave a facility with unmitigated risk for a considerable time. The IEC 61511 committee recognized industry is falling short and has strengthened the planning and execution requirements in the second edition. The changes include more specific language on the supplier responsibilities for planning and procedures, quantification of random failure, software development and testing, competency management, hardware fault tolerance, functional safety auditing, verification, traceability and cyber security. Hopefully the enhancements to the standard and experience lessons, such as those shared here, will encourage industry to increase focus on functional safety management planning at the project stage and improve compliance with functional safety standards in the future.

Glossary

BPCS	Basic Process Control System
CM	Conditional Modifier
CPI	Critical Protection Interlock
FAT	Factory Acceptance Test
FMEDA	Failure Mode, Effects & Diagnostic Analysis
FSMP	Functional Safety Management Plan
HAZOP	HAZards and OPerability (study)
HFT	Hardware Fault Tolerance
IE	Initiating Event
IPL	Independent Protection Layer
LOPA	Layer of Protection Analysis
OSHA	Occupational Safety and Health Administration
P&ID	Process & Instrumentation Diagram
PFD	Probability of Failure on Demand
PHA	Process Hazard Analysis

PLC	Programmable Logic Controller
PTI	Proof Test Interval
REGAGEP	Recognized and Generally Accepted Good Engineering Practice
RRF	Risk Reduction Factor
SAT	Site Acceptance Test
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented Systems
SIT	Site Integration Test
SRS	Safety Requirements Specification

References

[1] Instrument Society of America (ISA), *ANSI/ISA-84.00.01-2004 part 1 (IEC61511-1 Mod) Functional Safety: Safety instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*. ISA, Clause 5.2.4.

[2] Instrument Society of America (ISA), *ANSI/ISA-84.00.01-2004 part 1 (IEC61511-1 Mod) Functional Safety: Safety instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*. ISA, Clause 4.

[3] Instrument Society of America (ISA), *ANSI/ISA-84.00.01-2004 part 3 (IEC61511-3 Mod) Functional Safety: Safety instrumented Systems for the Process Industry Sector – Part 3: Guidance for the Determination of the Required Safety Integrity Levels – Informative. ISA, Figure D.1*

[4] Instrument Society of America (ISA), *ANSI/ISA-84.00.01-2004 part 1 (IEC61511-1 Mod) Functional Safety: Safety instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*. ISA, Clause 11.2.2.

[5] Iwan van Beurden and Rachel Amkreutz, "'Proven in use' criteria for safety instrumented systems. Use these guidelines to qualify equipment.," *Hydrocarbon Processing* November 2004.

Author Information

Denise Chastain-Knight, PE, CFSE, CCPSC
exida
80 North Main Street
Sellersville, PA, 18960, USA
dchastainknight@exida.com

Ralph Butz
Iowa Fertilizer Co
3546 180th Street
Wever, IA 52658
ralph.butz@iowafertilizer.com

William Donaldson
Iowa Fertilizer Co
3546 180th Street
Wever, IA 52658
william.donaldson@iowafertilizer.com