Functional Safety – A Reality Check in the World of Projects!

By Nagappan Muthiah and Aracely Acevedo
Automation and Control - Wood Group Mustang

Paper presented at the 71st Annual Instrumentation and Automation Symposium for the Process Industry Industries, Texas A&M University, College Station, Texas, January 2016.

Introduction

Functional Safety Standard ISA84 / IEC 61511 is a performance based specification which allows operating companies a measure of freedom to determine their own methodology in meeting the targets set by the standard. However, this freedom also comes with its own challenges! The requirements of the standard can appear to be ambiguous as it does not offer a clear roadmap for implementation.

The goal of this paper is to identify techniques to translate the philosophical requirements of the standard into specific actions that can be implemented over a variety of projects. Being engaged with several projects aimed at ISA84 / IEC61511 compliance in the role of an engineering consultant; Wood Group Mustang found that operating companies face many issues in implementing the performance based concepts.

The primary challenge for these companies is defining a methodology to convert the Safety Lifecycle requirements of the standard into project or plant/operation specific requirements. Project teams need to realize that ISA-84 compliance requires a lifecycle approach and is not a one-time effort. Safety Lifecycle requirements should be addressed consistently by each project executed at a facility.

Additionally, Functional Safety deliverables are not simply reports for Process Safety Management (PSM) compliance. Data in these documents must be translated into usable information for operations and maintenance teams in order to provide a safe operating environment and improved process safety.

IEC-61511/ISA84 Functional Safety Standards

Functional Safety, per the International Electrotechnical Commission (IEC), "is the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs".[1] Functional safety focuses on the detection of a potentially dangerous condition and the subsequent implementation of a protective or corrective device or mechanism to prevent the development of a hazardous event into an unwanted consequence, or providing mitigation to reduce the potential severity of harm to people and/or the environment.

Functional safety is developed upon a body of performance based international standards of practice including IEC-61508 and IEC-61511/ISA 84.00.01 Parts 1-3 - with the latter specifically applying to the process industries. These standards allow operating companies to define Safety Instrumented System

[1] International Electrotechnical Commission, Functional Safety - IEC61508 Explained [Online] 2015.

(SIS) requirements based on their own risk criteria and do not define prescriptive requirements as many other legacy standards.

Functional safety is a life-cycle model that is integrated with established safety risk- management processes (e.g OSHA PSM) to provide a structured approach to defining safety requirements based on probability and severity of potential process safety events. The functional safety life-cycle includes all necessary activities involved for the implementation of Safety Instrumented Functions (SIF's) as part of the SIS. These activities begin at the concept design phase of a project and finishes when all of the SIF's are no longer available for use (decommissioned), including changes to the SIS/SIF during operation. The functional safety life cycle is a closed loop model that constantly identifies and assesses the risks, cultivates a design, then implements, verifies, and maintains that design.

Challenges – Paper to Reality

The ISA 84 / IEC-61511 standard allows operating companies the ability to determine their own methodology in meeting the targets set by the standard. The freedom derived from the non-prescriptive nature of the functional safety standards also comes with its own challenges!

Challenge 01 - Funding IEC-615111/ISA-84 Safety Life Cycle Approach

In the United States the Occupational Safety and Health Administration (OSHA) does not explicitly mandate that operating companies must comply with IEC-61511. Hence, during a project funding stage, the applicability of the standard is always challenged – "Show me where it says that we have to follow the IEC-61511 Functional Safety Lifecycle". The reality is that, even though the application of functional safety standards (IEC-61511/ISA 84.00.01 Parts 1-3) are not directly mandated, there is a regulatory basis for implementation in OSHA CFR 1910.119 for equipment associated with a covered process, including SIS, as documented below[2]:

1910.119(d)(3)(i)

Information *pertaining to the equipment in the process shall include:*

1910.119(d)(3)(i)(F)

Design codes and standards employed;

1910.119(d)(3)(i)(H)

Safety systems (e.g. interlocks, detection or suppression systems).

1910.119(d)(3)(ii)

The employer shall document that ***equipment complies with recognized and generally accepted good engineering practices (RAGAGEP)****.*

[2] OSHA, Standard Interpretations, Occupational Safety & Health Administration. [Online] November 29, 2005.

1910.119(f)(1)

The employer shall develop and implement written ***operating procedures that provide clear instructions for safely conducting activities involved in each covered process*** *consistent with the process safety information and shall address at least the following elements.*

1910.119(f)(1)(iv)

Safety systems and their functions.

1910.119(j)(4)

Inspection and testing.

1910.119(j)(4)(i)

Inspections and tests shall be performed on process equipment.

1910.119(j)(4)(ii)

Inspection and testing procedures shall follow ***recognized and generally accepted good engineering practices (RAGAGEP).***

Additionally the OSHA "General Duty Clause" states the following requirements

SEC. 5. Duties

(a) Each employer --

(1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;

(2) shall comply with occupational safety and health standards promulgated under this Act.

There is historical precedent of OSHA issuing Standard Interpretation letters where it recognizes ANSI/ISA 84.00.01 to be a "national consensus standard" and a "recognized and generally accepted good engineering practice" for SIS. An extract from one of these letters is provided below:

"*The PSM standard contains a number of requirements for equipment associated with a covered process, which may include Safety Instrumented Systems (SIS). OSHA considers the revised ANSI/ISA - S84.00.01-2004 Parts 1-3 (IEC 61511 Mod) to be recognized and generally accepted good engineering practices for SIS. Therefore, if an employer chooses to use S84.00.01-2004 Parts 1-3 as a basis ("code or standard employed") for SIS, and meets all S84.00.01-2004 Parts 1-3*[3] *requirements and other OSHA PSM*

[3] International Society of Automation, 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", Research Triangle Park : ISA, 2004.

requirements related to SIS, the employer will then be considered in compliance with OSHA PSM requirement for SIS" (2)

Therefore, in order to overcome the Funding Challenge, demonstration to management of the relationship between OSHA PSM compliance and the functional safety standards, as illustrated in Figure 1 below, is essential.

Figure 1. Functional Safety and OSHA PSM compliance

Challenge – 02: Safety Lifecycle vs. Projects

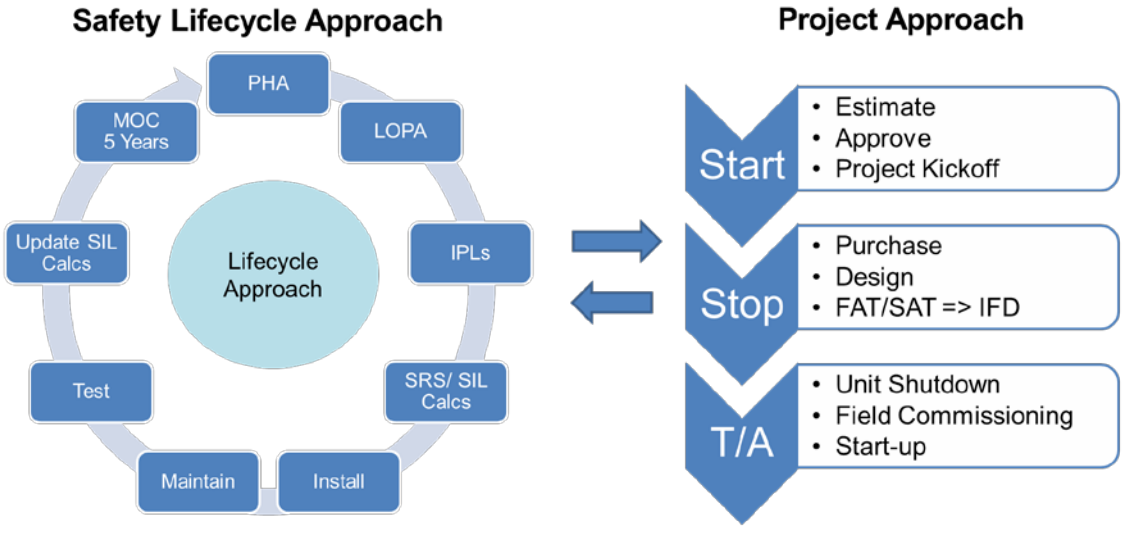

Figure 2. Functional Safety Lifecycle vs Projects

A principal success strategy in converting S84 requirements into project scope of work is to understand one primary, inherent, difference – the safety lifecycle is continuous – projects are not! Safety lifecycle activities traverse the entire life-span of the operating facility; while the individual IEC-61511 / S84 oriented projects have a finite life and finite budget.

Every project has a preliminary phase where the project is estimated and a proposal is generated. Management then reviews the proposal for validity of scope and budget and the project is approved. The project team takes this approved scope of work and moves into detailed design. At a certain point in the project the scope is frozen and the detailed design is implemented to completion. The project completion targets are most often tied to plant turnaround dates when a number of activities may be completed at once without the risk of affecting production.

A successful project finishes the scope of work on schedule, verifies and validates the design, and then completes commissioning during the plant turnaround window. A project team must understand that 100% perfection on paper and attempting to apply all safety lifecycle requirements within a single project at the cost of stalling all progress in field is not a success strategy. The authors have observed that, many times, even though a project's scope may increase, the scheduled turnaround (or implementation) dates usually do not move. Eventually the tendency is that the additional scope of work is completed at the cost of compromising the allocated time for verification, validation and testing – this is not acceptable from a functional safety perspective.

Hence, it is important to understand that the Safety Lifecycle requirements should be implemented as a series of projects (Project 01, Project 02 and so forth). A successful strategy is to prioritize work based on the risk being mitigated. Target a majority of the SIFs and implement them in the field. This typically results in improved process safety upon completion of the first project. The SIFs that could not be completed with the first project may be implemented with following projects. This allows for incremental improvements in functional safety while adhering to time constraints, as opposed to delaying all implementation until a suitable time can be scheduled to complete all SIFs at once. Essentially, one installed and functioning SIF is better than a hundred SIFs that only exist on paper and never implemented.

Challenge 03: Breaking the Silos

Functional safety standard ISA84 (S84) compliance requires the effective capitalization of the synergy between various project team members in order to produce functional results in each phase of the safety life-cycle. Figure 3 below shows the different project teams that are typically involved with S84 Compliance.

Figure 3. Typical FS Silos

The main characteristics of these project teams are typically[4]:

- There is a limited team life
- They produce non-repetitive, one-time outputs
- Require cross-functional knowledge, expertise, judgement
- Members disband or receive new assignments after project completion

These characteristics of project teams can result in a “silo” mentality of team members, with each team member considering themselves a singular unit with their own individual interests to be fulfilled at the completion of the team task. A method of breaking the walls of each of these “silos” needs to exist so that a more inclusive, cross-discipline strategy may be developed and implemented.

Breaking the Process Hazard Analysis (PHA) Silo

The first group of silos that typically need to be coordinated includes upper management and high-level company stakeholders (Plant Manager, Corporate Sponsor), PSM consultants and the PHA team (Figure 4).

[4] Eduardo Salas, Mary P. Kosarzycki, Scott I. Tannenbaum, David Carnegie, "Principles and Advice for Understanding and Promoting Effective Teamwork in Organizations"

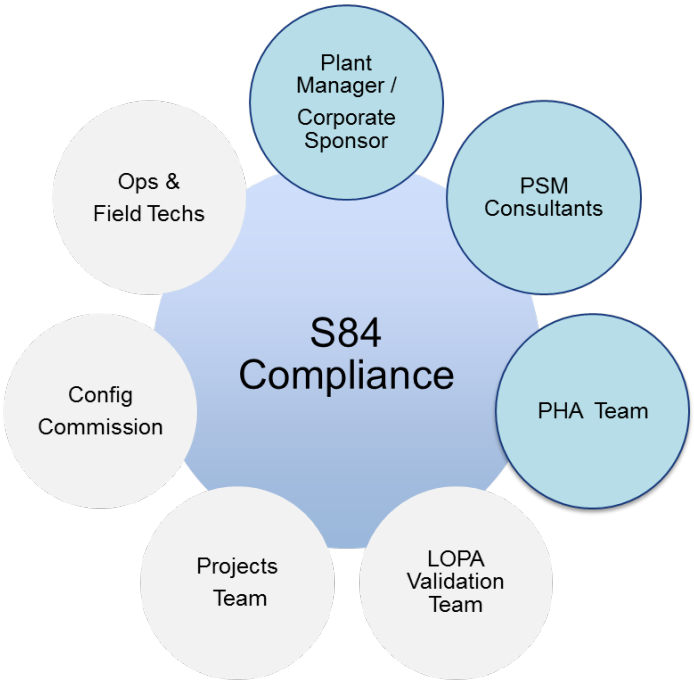

Figure 4. PHA Analysis Silos

An effective method to overcome this challenge includes establishing specific goals of PHA facilitation. Upper management must convey to the PSM consultants that the primary goal is to facilitate inputs from PHA Teams and not complete the analysis themselves.

The authors have found that during the implementation of this practice that there were situations where the PHA facilitators pre-populated the entire PHA scenario list themselves before the formal PHA began. This was done under the assumption that they were “saving time for the PHA team”. This intention of saving time for PHA team is noble; however it comes at the cost of deterring the brainstorming intent of the PHA. Once the PHA team sees the entire hazardous scenarios list pre-populated, there is a tendency for cognitive bias to take over where the PHA team does not question what already exists. The primary goal of conducting a PHA, as required by OSHA, is to identify and evaluate the hazards with equal participation from all members of PHA team including process, operations and safety representatives.

Successful Results:

- PHA has better coverage.
- Consequence categories identified better aligned with reality

1.1.1 Breaking the PHA and Projects Silo

The primary challenge here with the second group of silos is to get the PHA/LOPA teams to produce information that is conducive for defining the Functional Safety project scope.

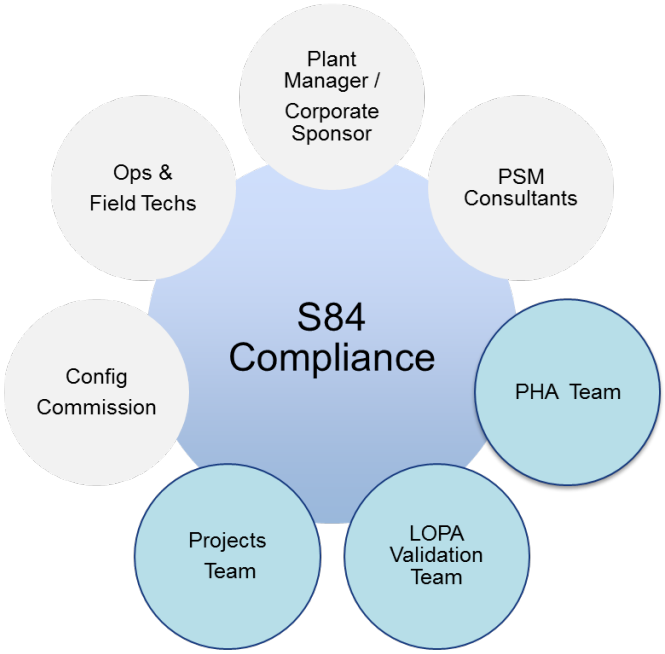

Figure 5. PHA and Projects Silos

An effective method to overcome these silos is establishing the following goals:

1) The PHA Team should understand that the PHA / LOPA documentation is not simply for passing OSHA audits. The documentation serves a much greater purpose of providing valuable information to the project team such that the project team can finalize a design that can be implemented in the field to mitigate any risk gaps.

2) PHA / LOPA documentation should be captured keeping Safety Lifecycle usability in mind.

Successful Results:

- Project teams understand requirements faster
- HAZOP scenarios validity not challenged
- Project scope is defined more effectively

Projects, Operations and Maintenance Teams Silo

The primary challenge here with the third group of silos is for the Project teams to ensure that their Safety Systems design meets the operability and maintainability requirements.

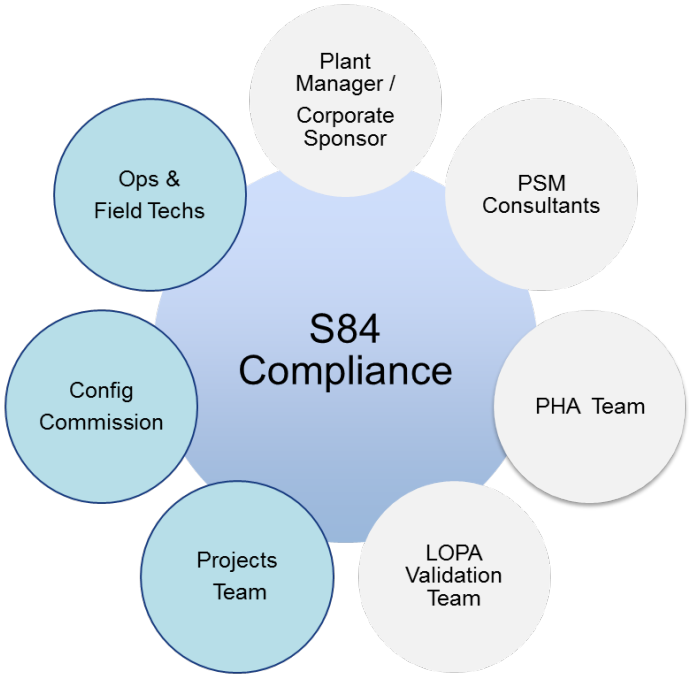

Figure 6. Project, Process and Operations Silo

An effective method to break the projects, operations and field technician team silos is to keep the following key aspects in mind:

1) Always involve Process and Operations during Safety Requirements Specification (SRS) development.
2) SIFs are not just about tripping a piece of equipment or stopping a process – plant availability is also important!
3) During SRS – SIF design, it's essential to fully understand and document the operability factors such as reset/restart requirements and special override bypass requirements in addition to the process trip specifications.
4) Spurious trip tolerances should be considered while deciding instrument voting architecture.

Successful Results:

- Improved SIF design that not only prevents the hazardous event from occurring, but ensures that operations can keep the unit running with minimal spurious trips.

Conclusion

With the listed techniques in this paper, the authors expect to provide the reader some clarity on how to convert the IEC-61511/S84 philosophical requirements into project scope of work. According to the authors' experience, Functional Safety practitioner role should not be limited to performing SIL determination and PFD calculations, but should also include acting as a facilitator to achieve the appropriate synergy between these multidiscipline team members in order to make Safety Life Cycle real-life implementation a successful experience. ISA-84 compliance requires the participation of multidiscipline teams who understand the need of others and are willing to improve their work process to achieve a common goal of improved process safety.

Bibliography

International Electrotechnical Commission, "Functional Safety - IEC61508 Explained", 2015.

OSHA, "Standard Interpretations, Occupational Safety & Health Administration", November 29, 2005.

International Society of Automation, 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", Research Triangle Park : ISA, 2004.

Eduardo Salas, Mary P. Kosarzycki, Scott I. Tannenbaum, David Carnegie, "Principles and Advice for Understanding and Promoting Effective Teamwork in Organizations".

Authors' Biographies

Nagappan Muthiah (Muthu) is the functional safety discipline technical authority for Wood Group Mustang's Automation and Control business unit. A Certified Functional Safety Expert and licensed Professional Engineer in the State of Texas with 12 years of process automation experience, he has worked on control systems expansion and upgrade projects for oil and gas, chemical, and fertilizer companies. Muthu is a voting member of ISA-84 for Wood Group Mustang and serves on the CFSE Process Safety Advisory Board.

Aracely Acevedo is a functional safety engineer in Wood Group Mustang's Automation and Control business unit. She holds an ISA84 Safety Instrumented Systems Expert Certification and has 12 years of instrumentation, control and functional safety experience. She has worked on basic and detailed design engineering projects for oil and gas transportation and refining. She is currently pursuing her Master of Science in safety engineering from the Mary Kay O'Connor Process Safety Center at Texas A&M University.