



The Link Between PSM & Functional Safety: Risk Reduction is Key

In my September 2008 column, I mentioned three years ago, the United States Occupational Safety & Health Administration (OSHA) accepted and recognized the ANSI/ISA – S84.00.01 / IEC 61511 Functional safety - Safety instrumented systems for the process industry sector standard as good engineering practice. More specifically, this meant that employers who met the ANSI/ISA – S84.00.01 / IEC 61511 requirements related to Safety Instrumented Systems (SIS) would then be considered in compliance with OSHA Process Safety Management (PSM) requirements for SIS.

OK, but what is Functional Safety and HOW does it fit into a PSM program?

Functional Safety

Distilled down, there are two key concepts outlined within the ANSI/ISA – S84.00.01 / IEC 61511 standard – Safety Integrity Levels (SIL) and the Safety Lifecycle.

Safety Integrity Level is defined as a relative level of risk reduction provided by a safety function, or it can specify a target level of risk reduction required. SIL is a measurement of performance, using an order of magnitude metric, required for a Safety Instrumented Function (SIF). The higher the SIL value, the more reliable the SIF is. While IEC uses four categories for SIL, ISA only uses SIL 1, 2 and 3.

validate, operate, maintain, and continuously improve their SIS.

While these are fairly straightforward concepts - Safety Integrity Levels (SIL) and the Safety Lifecycle, the ANSI/ISA – S84.00.01 / IEC 61511 standard itself is not an easy read. Being performance based, the standard focuses on what must be done, rather than on how it should be done. Owner/operators, faced with an environment whereby their peers are adopting these standards, struggle with the standard, find it difficult to implement and do not really fathom all the implications which continue after SIS start-up and commissioning. Areas of confusion include establishing their own performance / risk targets, implementing a Functional Safety plan, recording and documenting the steps involved, auditing that the program is working, validating that Functional Safety is still intact and implementing a management of change program to incorporate Functional Safety.

More often than not, this challenge is compounded when the owner/operator delegates managing the Safety Lifecycle to the Instrumentation and Controls group. Though Operations, Process, and Project managers have a stake in the evolution of the design and management of SIS, organizations typically believe the I&C group is the best equipped to lead the charge.

Consequently, unless corporations have individuals in-house who have demonstrated

ty Management program with involvement of all disciplines.

The Center for Chemical Process Safety (CCPS) “Business Case” identified Risk Reduction as one of four tangible benefits of adopting PSM in companies. Specifically, Risk Reduction pertaining to preventing human injury and avoiding significant losses and environmental damage.

Risk reduction is also a cornerstone principle in Functional Safety. By using the concept of SIL to establishing how much Risk Reduction is required to mitigate identified process risks, designers of process plants accomplish the identical goal of preventing incidents and impacts on people, assets, the environment and corporate reputations.

Now that we’ve established that Risk Reduction is common to both PSM and Functional Safety, let’s revisit the realities of bringing Functional Safety “alive” in companies.

The management of Functional Safety or SIL programs is a corporate responsibility, as it involves Hazard / Risk Identification and Risk Reduction. Risk managers, HSE managers and Asset Integrity managers are among those responsible for managing PSM programs. The same people are instrumental in committing to managing Functional Safety.

ACM created the Simplified Quad Model for Functional Safety (See Graphic 1) to present key concepts within the ANSI/ISA – S84.00.01 / IEC 61511 Safety Lifecycle to managers and non-technicians. Since without the buy-in from senior corporate decision makers within organizations, Functional Safety initiatives will not thrive, it is critical to demystify a rather complex and confusing standard.

The Quad model reflects what most Functional Safety enthusiasts already know and understand. A quick review of the Simplified Quad model starts with the top right hand quadrant (Q1). In Q1, the concepts of the facility or upgrade are developed. Design Basis Memorandums (DBM) are developed. During this project stage, Hazard and Risk Analysis (i.e. HAZID, HAZOP) is completed, as is the Allocation of Safety Functions to Protection Layers (i.e. SIL Determination). Risks are identified and assessed. The requirement for additional safeguards is determined.

SIL	Risk Mitigation	Protection Layer	Performance
Safety Integrity Level	Risk Reduction Factor (RRF)	Probability of Failure on Demand (PFD)	Reliability (1 – PFD)
1	10 to 100	10 ⁻¹ to 10 ⁻²	.9 - .99
2	100 to 1,000	10 ⁻² to 10 ⁻³	.99 - .999
3	1,000 to 10,000	10 ⁻³ to 10 ⁻⁴	.999 - .9999
4	> 10,000	10 ⁻⁴ to 10 ⁻⁵	.9999 - .99999

Table 1: Safety Integrity Levels - Relationship between RRF, PFD & Reliability.

Safety Lifecycle means the design and management requirements for Safety Instrumented Systems, from initial concept, design, implementation, operation, and maintenance through to decommissioning. Once it is deemed that a SIS system is required, a robust SIS management system should define how an owner/operator plans to assess, design, engineer, verify, install, commission,

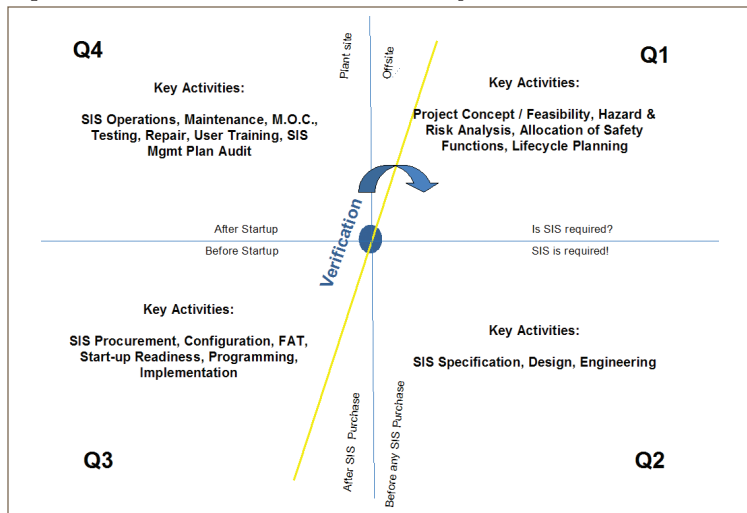
experience in interpreting and applying the ANSI/ISA – S84.00.01 / IEC 61511 standard, there can be considerable reluctance to venture into an area where it is not clear how they will tackle Functional Safety. However, once organizations understand that all disciplines can and should participate, they typically modify their approach and integrate Functional Safety into a broader Process Safe-

If additional safeguards or protection layers are required, then the bottom right quadrant (Q2) specifies the functionality and performance required for the additional safeguards, the architecture, and the system(s) required. It specifies both hardware and software requirements for the additional safeguard systems. Q2 involves design and specification. No equipment is purchased. Cost estimates are finalized, and approvals for purchasing the additional safeguard systems are confirmed.

On project approval, the bottom left hand quadrant (Q3) is where procurement occurs. Equipment is purchased. Fabrication and con-

to the facility's process are made, then Q1 defines the concepts of the change, the risks presented by the change, and determines if the existing safeguards are acceptable. Another series of HAZOP and SIL Determination studies may be required.

The yellow line, rotating clockwise, illustrates that as the quadrants are completed, a verification step is required to document such. This exercise demonstrates that the inputs and outputs of each step are complete. Verification includes a thorough review of all relevant documentation and records to prove the steps were completed within each quadrant.



Graphic 1: ACM Simplified Quad Model for Functional Safety

struction plans are developed and executed, detailed programming and configuration for the safeguard systems occur, and systems are readied for start-up with extensive testing during assembly and software development. Field work is completed including power, HVAC, cabling, cabinets and infrastructure systems. A pre-start check confirms the readiness for start-up.

Once safeguard systems are proven ready for start-up, the top left hand quadrant (Q4) is where start-up occurs and final system acceptance takes place. The Functional Safety requirements specified in Q2 are validated through testing. Results are recorded. The timeline for Q1 to Q3 can be months. However, Q4's timeline is measured in years, as Q4 is where the normal operations, maintenance and testing occurs. This is where safeguard systems are monitored, audited, documented and reported on according to a comprehensive SIS management plan. Once operational, if additions or modifications

The Simplified Quad model shown above illustrates that the Safety Lifecycle plan has a flow and simplicity if distilled down to it's basic elements. For interested readers, ACM can provide a more detailed Quad model which incorporates clauses within the ANSI/ISA – S84.00.01 / IEC 61511 standard. Just give us a call.

With a clearer understanding of the link between PSM and Functional Safety, organizations now can see a path whereby Functional Safety can be an integral part of any PSM program.



Readers can contact the author, Ken Bingham of ACM Facility Safety, a division of ACM Automation Inc. for more information by email: ken.bingham@acm.ab.ca and by phone at 403.264.9637.