Decoding SIS: Are You Doing What's Necessary to Prevent Disasters?

Emily Henry, PE(SC), CFSE
aeSolutions
Greenville, SC
emily.henry@aesolutions.com

aeSolutions Technical Team

Prepared for Presentation at
American Institute of Chemical Engineers
2024 Spring Meeting and 20th Global Congress on Process Safety
New Orleans, LA
March 24-28, 2024

Decoding SIS: Are You Doing What's Necessary to Prevent Disasters?

Emily Henry, PE(SC), CFSE
aeSolutions
Greenville, SC
emily.henry@aesolutions.com

aeSolutions Technical Team

Keywords: Safety Instrumented Systems, Safety Integrity Level, Risk Reduction Factor, Probability of Failure on Demand, Process Safety Management (PSM), IEC 61511, IEC 61508, Risk Assessment

Abstract

When your facility is tasked with industry safety standard compliance, where do you start? What do all those SIS acronyms mean? For OSHA PSM-covered facilities, adherence to a functional safety lifecycle can be a critical step in overall SIS performance assurance.

What is hiding under the radar of a plant SIS? Risk assessments define hazard consequences with assumed initiating event frequencies. How do we prevent these consequences? By verifying the reliability and availability assumptions of SIL Verification design parameters. Without understanding the design parameters your SIS is based upon, or without proper maintenance of your SIS equipment, your risk assessment gap closure may be incomplete.

What factors into the assumptions of an SIS design?

- Are your safety devices replaced at their specified asset life, tested at the interval, and tested with the necessary rigor to uncover dangerous failures as specified in your calculations?

What does following the Functional Safety Lifecycle entail?

- Does your facility have a Functional Safety Management Plan, perform Functional Safety Assessments on your SIS Design, and keep records of device failures to evaluate field performance against assumed reliability?

This paper will illustrate the real consequences of failing to uphold SIS design assumptions or follow the Functional Safety Lifecycle.

1 Introduction

It is all too easy to become laser-focused on plant chemical processes or day-to-day mechanical issues of operating a facility while Safety Instrumented System (SIS) design parameters (by all accounts to some just numbers on a page) and requirements of the Functional Safety Lifecycle are denied their due respect. Those design parameters, however, aren't just numbers on a page and understanding them can prove to be the difference between acceptable/unacceptable system performance and reliability. Proof test coverages, asset life values, and test intervals are all critical design assumptions that relate to your SIS's real-life performance and reliability. SISs can **and will** fail in an unsafe manner if they are not properly maintained and operated. Functional Safety standards and regulations have been put in place to create a safer world for us all. Integrating the Functional Safety Lifecycle into facility process safety culture is critical for compliance with industry safety standards. Only then can you operate and maintain your SIS as designed to prevent disasters. This paper addresses various critical SIS design parameters and the importance of training to fully understand and implement the Functional Safety Lifecycle.

2 The Wide World of Functional Safety

2.1 When do the Major Standards / Regulations Apply?

When must a facility follow SIS standards for the process industry? For professionals new to the field of process safety, it may not be abundantly clear how different standards or regulations get applied to your site in the first place. You could work for years in a process facility without the proper training or guidance and not fully understand the key standards you should be following to operate safely. Let's discuss a few of the main standards and regulations and how they relate to each other with regard to process safety – OSHA 29 CFR 1910.119, IEC 61508, and IEC 61511.

The Occupational Safety and Health Administration's (OSHA) Process Safety Management (PSM) regulation is OSHA 29 CFR 1910.119. It states that there are two possibilities for the regulation applying to a facility:

> i) A process which involves a chemical at or above the specified threshold quantities listed in Appendix A to this section;
>
> ii) A process which involves a Category 1 flammable gas (as defined in 1910.1200(c)) or a flammable liquid with a flashpoint below 100 °F (37.8 °C) on site in one location, in a quantity of 10,000 pounds (4535.9 kg) or more.[1]

The OSHA 29 CFR 1910.119 regulation requires compliance with PSM practices including documentation of process safety information, mechanical integrity inspection and testing, correction of equipment deficiencies, and quality assurance. There is an appendix in the

regulation which offers recommendations and guidance for compliance with the PSM requirements.

The IEC 61508 standard *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems* outlines requirements for electrical/electronic/programmable electronic safety-related systems. IEC 61508 is more typically utilized by device manufacturers rather than end users, as shown in Figure 1 below.[2]

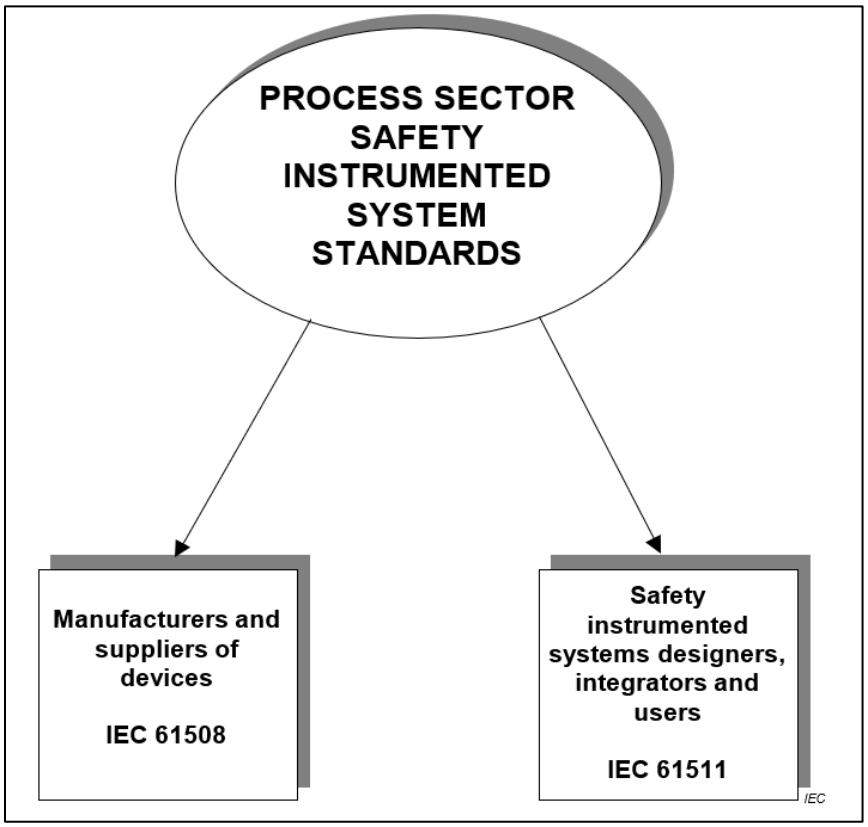

Figure 1. Relationship between IEC 61511 and IEC 61508

How do you know you're following RAGAGEP (Recognized and Generally Accepted Good Engineering Practices) in order to comply with applicable regulations like OSHA 29 CFR 1910.119? One generally accepted good engineering practice specifically written with regard to SIS is IEC 61511 *Functional Safety - Safety Instrumented Systems for the Process Industry Sector*. Originally written as ANSI/ISA 84.00.01-2004, Parts 1-3 (IEC 61511 Mod), the IEC 61511 standard is a "process sector Implementation of IEC 61508:2010."[3] IEC 61511 applies to a wide variety of industries within the process sector including chemicals, oil and gas, pulp and paper, pharmaceuticals, food and beverage, and non-nuclear power generation. These standards do require a licensing fee to access. If your facility does not have access to the standard at present, there are still free resources available to help educate process safety professionals about IEC 61511 terms. aeSolutions is one such entity that publishes a free SIS terms glossary (found here https://www.aesolutions.com/glossary).[4] The glossary page encourages process safety

professionals to seek out the full standard to ensure understanding of all applicable definitions and standard requirements.

2.2 Importance of Process Safety Culture in the Functional Safety Lifecycle

It takes significant effort and training to instill the proper safety culture at a site to appropriately operate and maintain a SIS. If the functional safety lifecycle is properly followed and infused as a part of site culture, major incidents can and have been prevented from occurring. If all levels of personnel at a site are invested in closing risk gaps by implementing a SIS, it makes following the safety lifecycle much less of an uphill battle. If any group of personnel at a site is not invested or devoted to the purpose and criticality of any portion of the safety lifecycle, this opens up possibilities for failure and potential injury.

Operating with a culture of process safety means educating all personnel groups on the true hazards against which the SIS is designed to protect. When all personnel groups comprehend the underlying basis of the SIS target reliability, it is much more likely that they will step up to the challenge of operating and maintaining the SIS as designed. Following the functional safety lifecycle is one way to uphold your documented SIS design parameters. What happens when site personnel do not follow the safety lifecycle? SIS performance may be adversely affected by directly impacting three of the key SIS design parameters discussed in more detail in Section 4.

- Understandably facilities need to manage operations expenses and don't want to purchase new equipment more often than required. However, if management is not educated on the criticality of replacing or refurbishing SIS devices at their specified **asset life** interval, it becomes easy to adopt a "run to failure" method of operating the facility. This invalidates the assumed reliability of the safety devices in your SIS when they are kept in operation past their useful life.
- When periodic functional proof tests are executed at the prescribed **proof test interval** in the SIS design, you discover a percentage of failures which otherwise could have gone unnoticed. If the proof tests are not executed at the prescribed test interval, latent failures still exist since no repairs or testing have been done. In that scenario, your SIS holds itself together by a thread. It is no longer as reliable as your design originally required per the risk assessment.
- If maintenance technicians do not understand the reasoning behind the extensive test steps for safety devices, it is easier to shrug off those requirements in order to shorten outage durations and get a process unit up and running. However, if maintenance technicians are educated on the purpose of **proof test coverage** and how that factors into your SIF reliability, they can then justify the extra time or steps necessary to complete that proof test as written.

A priority can be shifted or moved down a list of other priorities. Values are core aspects of a culture. In this case, PSM needs to function as a value within the facility culture so that your SIS receives the priority it deserves. If upper management considers PSM and the SIS safety lifecycle requirements as a priority rather than a core value, it is more difficult to adhere to the design assumptions in the SIS documentation.

The BP Texas City Refinery explosion in 2005 is one example of process safety culture not being considered a value at an organizational level. The Chemical Safety Board (CSB) investigation report into this incident describes how:

> "BP Texas City lacked a reporting and learning culture. Personnel were not encouraged to report safety problems and some feared retaliation for doing so. The lessons from incidents and near-misses, therefore, were generally not captured or acted upon."[5]

Fostering a positive process safety culture in an organization or facility requires being open to reporting and learning from near-misses or process incidents. If those who report known issues or potential safety concerns are met with negativity or even apathy, there is no incentive to continue improving the site's process safety performance. This was the case with BP Texas City refinery's safety culture which contributed to the explosion at the Isomerization (ISOM) unit in 2005.

3 What's Hiding Under the Radar of Your SIS?

3.1 Functional Safety Management Plan - Yes, You Do Need One

A Functional Safety Management Plan outlines all responsible parties in your plant who interact with the SIS. Those parties need to be knowledgeable about the purpose and criticality of the SIS. They need to be trained directly on the tasks for which they are responsible in the Safety Lifecycle. This training should be particularly focused on how Safety Lifecycle tasks differ from typical non-SIS plant tasks. Plant personnel turnover, the loss of senior engineers and influx of green engineers, or the inaugural installation of an SIS are all opportunities for personnel to encounter an SIS for the first time. This requires a concerted effort to educate personnel on effective management of the safety lifecycle to maintain safety and comply with applicable standards.

A Functional Safety Management Plan (FSMP) can serve as a road map for facility teams to follow throughout the Functional Safety Lifecycle. It is a document in which teams can agree upon how the facility will conform to the clauses laid out in the performance-based IEC 61511 standard. For example, you can determine where your site will store documentation records of your safety lifecycle activities, such as proof tests or functional safety assessments. If a database or network file location is publicly known to all personnel interacting with the SIS, that could be your choice for maintaining these records. Then you are able to train personnel new to supporting your SIS on where this information is stored and maintained.

An FSMP also contains a responsibility matrix. This matrix lays out all key tasks in the functional safety lifecycle and a place to determine which roles in your facility are responsible for carrying out those tasks. The term "RACI" is used in reference to assigning task responsibilities in the responsibility matrix. There may be some roles in your facility that are directly **R**esponsible for completing a functional safety task. However, another personnel role could be directly **A**ccountable for ensuring that the responsible person performs said task. Other roles may be **C**onsulted only during task completion. Finally, some roles in the facility may only need to be **I**nformed of the task taking place. Calling out the different responsibilities for each facility role (site manager, engineer, auditor, etc.) in following the safety lifecycle can help

prevent tasks from slipping through the cracks and being missed altogether. Figure 2 below provides one such example of a SIS task and some plant roles which would interact with the task.

	Process Controls Engineer	Maintenance & Reliability Manager	Maintenance Supervisor	Instrument Technicians
Maintenance (IEC 61511 Clause 16)				
Proof Test Execution	I	A	C	R

Figure 2. Example Responsibility Matrix

3.2 Functional Safety Assessments - Audit Doesn't Have to be a Dirty Word

Functional Safety Assessments (FSAs) are a major piece of the safety lifecycle which span the entire life of a SIS from design to commissioning to operation to decommissioning. Figure 3 below shows each point in the lifecycle of a SIS when a different FSA should be performed. FSAs are designed to be completed by a completely independent person from the SIS design team. A cold set of eyes is necessary for discovering any hiding discrepancies at various stages in the lifecycle of a SIS. Where a PSM audit addresses compliance with regulations at the facility safety program level, a FSA addresses compliance of a specific SIS design per documented risk assessment hazard scenario mitigations.

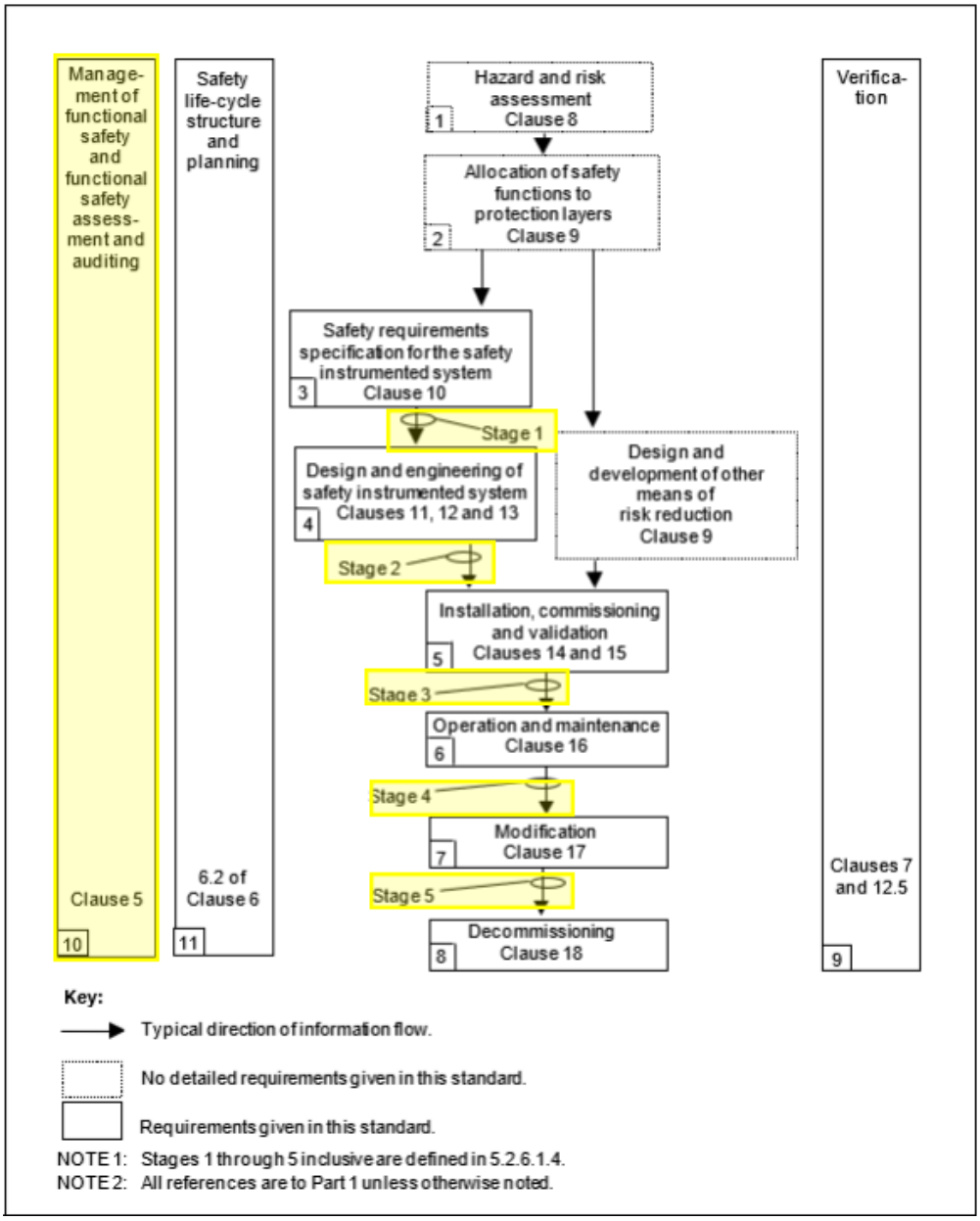

Figure 3. FSA Stages of the Functional Safety Lifecycle[6]

Employing an effective independent functional safety assessor makes it possible to find and resolve systematic errors before they are even introduced in your plant. Examples of the systematic errors the FSA process could identify include but are not limited to: incorrect instrument calibrated ranges, incorrect SIF trip setpoints per the defined risk assessment hazard, SIF response times that do not meet the requirement of the hazard process safety time (PST), and incorrect configuration of safety logic solver hardware to meet defined required Safety Integrity Level (SIL). Once items are flagged as recommendations in a FSA report, there is an opportunity to correct the design or implementation of the SIS. This allows for operating the SIS at the level of risk reduction required by its risk assessment.

Addressing and correcting findings from an FSA or a PSM audit is critical to operating the SIS per its design. A functional safety assessor can do their job to identify errors in SIS design or installation. However, if the assessor's recommendations are not resolved by the facility operating the SIS, the problem still exists. This can lead to process safety incidents like the BP Texas City refinery explosion discussed above. BP Texas City refinery PSM audit teams found in 2004 that "process safety action item resolution was still a problem for the refinery (20 percent of open action items were overdue), and that changes were still being made before MOC sign-offs and action items had been resolved."[7] If proper PSM audit action item closeout had been mandated at the site, mitigations could have prevented the ISOM unit explosion in 2005.

A less practiced piece of the safety lifecycle is recording device failures. Any SIS device failure must be recorded to verify that your assumed reliability in the SIS design is achieved in practice in the field. It is good practice to assess device failures using root cause failure analysis methods to identify and correct potential systematic errors plaguing your plant operations and maintenance activities. Learning from identified and recorded failures is one way to prevent them in the future.

4 SIS Design Parameters & How They Can Trip You Up

How do you know what's important in the stack of documents that you now must adhere to regarding the SIS you support? There are Safety Integrity Level (SIL) Verification Calculations, Safety Requirement Specifications (SRS), Proof Test Procedures, and even more to digest. There are a few key data points in the design documentation of your SIS, which, if not adhered to, could invalidate your SIS's designed reliability.

4.1 Asset Life

Failure rates of devices are defined as an average probability that is relatively constant or slowly declining value over the useful life of a device. Useful life is the key term in that definition. This term defines the portion of a device's lifecycle after which it has survived the infant mortality phase and before reaching the phase of age-related wear out. Useful life is one of the main values utilized to calculate the device's average probability of failure on demand (PFDavg). Figure 4 below shows the simplified equation and variables used to calculate a single device's probability of failure.

Essentially, PFDavg details the probability that when the device is called upon to perform its safety function as designed it will fail. This PFDavg value can only be assumed to be constant during the device's useful life period. If the device is not replaced prior to wear out age, this assumed constant PFDavg is no longer valid.

$$PFD_{avg} = C_{PT}\left(\frac{\lambda * TI}{2}\right) + (1 - C_{PT})\left(\frac{\lambda * LT}{2}\right)$$

Figure 4. Simplified PFDavg Equation for 1oo1 Device[8]

In Figure 4,

- λ = the failure rate
- C_{PT} = percentage of failures detected by the proof test
- TI = period test interval
- LT = lifetime (or useful life) of the device

Does useful life always mean you have to replace the device? If you choose to "refurbish to like-new condition," what does that entail? Refurbishing a device to "like-new" condition means ensuring all the device failure modes (identified either by the vendor-published information or by a Failure Modes & Effects Diagnostic Analysis (FMEDA)) are repaired sufficiently. Making repairs for all known failure modes would then reset the device PFDavg back to the PFDavg value assigned at the device's start of useful life. This implementation of repairs effectively resets detectable and undetectable failures back to their initially installed probability of occurring during the operating life of the device. Depending on the types of failure modes defined for the device (internal materials wear out, electronics degradation, sensor drift, etc.), an effective refurbishment could require a detailed overhaul of device subcomponents to ensure that they operate in like-new condition. A quick trip to the maintenance shop for visual inspection without replacing subcomponents may not truly repair the device to "like-new" condition and "like-new" PFDavg value in your SIF.

Does your SIS design use generic industry standard failure rate data (FRD) or vendor-specific FRD for the SIF PFDavg calculation? This is a key detail to know when you must replace a failed device in your SIS – you must install a device with equal or better FRD than the data used in the SIL Verification Calculations. Some SIL Verification Calculations utilize industry-collected "generic" FRD which ensures the risk reduction factor (RRF) achieved by your Safety Instrumented Function (SIF) is conservative regardless of which SIL-certified hardware you install in the field. Other SIL Verification Calculations may utilize "manufacturer-specific" FRD to call out a device make and model directly for use in the SIF. This can be useful if your facility wishes to standardize on a specific model of equipment for use in your SIS and a program exists to ensure these devices are stocked as spares on site and properly identified when replacement of a field SIF device is necessary. However, if "manufacturer-specific" FRD is utilized and the field device is replaced with a device that does not match or exceed the FRD assumed in the SIL calculation, it is possible to degrade your SIF RRF to an unsafe level.

Take, for example, a SIF composed of a single differential pressure sensor, a generic SIL 2 rated logic solver, and a single generic ball valve final element with a generic rack and pinion actuator and generic three-way solenoid. What happens to the overall RRF of the SIF when the sensor FRD changes in the field? In Table 1 below, note that the first differential pressure sensor with generic data has an entire order of magnitude worse PFDavg than the vendor-specific data. Vendor 1 differential pressure sensor has a better PFDavg than the generic data sensor, but still somewhat worse than the Vendor 2 differential pressure sensor PFDavg.

Table 1. Sensor PFDavg Effect on SIF RRF Achieved

Sensor Installed	Sensor PFDavg Value	SIF SIL Achieved Value	SIF RRF Achieved Value
Generic Pressure Transmitter	1.63E-02	1	17
Vendor 1 Pressure Transmitter	4.87E-03	1	21
Vendor 2 Pressure Transmitter	2.39E-03	1	23

If your risk assessment assigned this imaginary SIF a RRF target of 22, then your SIF would only pass the risk reduction target if the Vendor 2 differential pressure sensor is installed in the field. If the differential pressure sensor fails in the field and a maintenance technician does not replace it in-kind, but with a similar-looking device (one that may even be SIL rated) the SIF could then fail to meet the hazard scenario risk reduction for which it is credited.

Knowing which vendor devices are SIL-certified versus not SIL-certified is critically important. For example, in some vendor model number codes, the SIL-certified version only differs by one option code entry. In your facility's instrument storage, a maintenance tech could see what at first glance appears to be an identical transmitter to the safety transmitter. However, it's missing two characters in the model number, and it is actually not SIL-certified. If they aren't trained to know the difference in the model code identifiers (or your site doesn't actively steward storage of verified safety equipment in a specific location), this would mean an uncertified device is installed in your SIS after the attempted repair. Now, the assumed SIF reliability is no longer valid, and the facility is operating with an unmitigated hazard risk gap.

4.2 Proof Test Intervals

Many process safety professionals have experienced the scenario of upper management requesting to extend test intervals in a SIS with the goal of extending the operational run time of a critically valuable process unit. If your plant teams request to defer these critical proof tests beyond the prescribed test interval, one small process issue or upset on top of an undiscovered failure could result in the SIS not doing its job – preventing a known hazard consequence. It is imperative to perform a detailed assessment of the risk incurred by extending a safety-critical device test interval beyond what was assumed in the SIL calculation.

When has deferring safety proof testing resulted in a process incident? One example is the ExxonMobil Torrance refinery Fluid Catalytic Cracker (FCC) unit Electrostatic Precipitator (ESP) explosion in February 2015. Per the Chemical Safety & Hazard Investigation Board (CSB) investigation of this event, several weaknesses existed in the ExxonMobil Torrance site's PSM system. One of those weaknesses was operating the FCC spent catalyst slide valve (SCSV), a piece of safety-critical equipment, beyond its useful life. The purpose of the SCSV is to create a plug seal between the hydrocarbon/reactor side of the FCC unit and the air/regeneration side of the FCC unit. Per the CSB's ExxonMobil Torrance Refinery Investigation Report, the SCSV,

when closed, is used to "prevent undesirable mixing of air and hydrocarbons, which is an explosion hazard."[9] According to the CSB report:

> "An Equipment Degradation Document predicts the probability of failure of the SCSV due to erosion, based upon a four- to five-year run length of the FCC unit between turnarounds. To ensure effective operability of the valve, ExxonMobil assigned it a testing interval of every four years to make sure the valve could function as required to prevent a flow reversal during normal operation."[10]

Due to a change to typical turnaround intervals at the Torrance site, the SCSV was intended to operate for a period of greater than six years - well beyond its safe operating life. The key detail here was that the ExxonMobil Torrance team did not carry out an appropriate risk evaluation to determine the possible consequence of operating a safety-critical device beyond its useful life. The CSB report states "ExxonMobil operated FCC unit equipment beyond its predicted safe operating life. The failure of the equipment allowed hydrocarbons to reach the ESP."[11]

Not only was the equipment test interval of the SCSV in the ExxonMobil Torrance refinery incident improperly managed, but the rigor of proof testing was also insufficient. "To meet the four-year testing requirement, ExxonMobil periodically partially closed the SCSV while the unit operated to verify that the mechanical valve components functioned properly. While an important mechanical testing strategy, this testing method did not evaluate whether the valve was eroded, or test whether the SCSV could close and seal."[12] This limited partial stroke testing was not thorough enough to uncover all the major failure modes of the slide valve internals. Whatever level of risk reduction the Torrance refinery FCC team assumed this safety-critical valve would provide against "undesirable mixing of air and hydrocarbons"[12] was no longer achieved due to insufficient proof testing.

4.3 Proof Test Coverage

Proof Test Coverage (PTC) is defined as "a measure of how many undetected dangerous failures are detected by the proof test."[13] It measures the percentage of dangerous failures (failures which would lead to the inability of the SIS to perform when demanded) a device's proof test procedure will find when performed. Typically during the safety certification process, devices undergo a Failure Modes and Effects Diagnostics Analysis (FMEDA) to determine all possible failure modes of a device. The PTC tells us how rigorous a proof test is by its ability to reveal those failure modes of a device during testing.

Carrying out proof tests which adhere to the documented PTC in the SIS design is essential for ensuring the reliability and safety of complex systems. For example, if a PTC of 95% is documented in the SIL Verification Calculation, that implies that an extremely rigorous proof test will be conducted in order to uncover 95% of dangerous undetected failures. Are your proof test procedures rigorous enough to meet that assumed PTC by uncovering 95% of failures detailed in the FMEDA? If the proof test is not thorough enough to reveal the documented percentage of failures, there will be undetected dangerous failures waiting to degrade the performance of your SIS.

Again, the BP Texas City Refinery explosion in 2005 is one example of a process incident which

manifested in part due to a lack of rigorous proof testing. Inadequate testing protocols left crucial safety systems and equipment insufficiently inspected and maintained, which led to a buildup of flammable materials and eventual catastrophic failure. The failure of the ISOM unit raffinate splitter section at the BP Texas City Refinery was proven to be a result of several instrument failures, mainly due to inadequate maintenance and testing.[14] Incorrect data in equipment specification sheets, such as inaccurate specific gravity values for process hydrocarbons, led to critical instruments being miscalibrated in the field.[15] Instruments with a history of failures were not flagged for corrective action, and site practices didn't ensure proper testing and repair of the instruments prior to unit startup. Improper testing methodology and test procedures were used to assess instrument functionality, including the functionality of a blowdown drum high level alarm. These proof testing integrity issues resulted in starting up the raffinate splitter tower without functioning critical safety devices.

The BP Texas City Refinery explosion shed light on the vital importance of thorough testing. These tragic events show the serious consequences that can result from neglecting proper testing and maintenance procedures. They remind us of the crucial role that careful testing plays in keeping complex systems reliable and safe. Looking ahead, it's crucial for industries to make comprehensive testing a priority, ensuring all necessary steps are taken to identify and address potential faults or failures before they turn into disasters. Testing per documented proof test coverage minimizes risk by converting undetectable failures to detectable failures. It allows facilities to adhere to PSM regulatory testing requirements, and, most importantly, safeguards the well-being of people and the environment.

5 Conclusion

Disaster lies waiting around every corner; waiting for you to slip up and underestimate the importance of adhering to your SIS design assumptions. Conforming to safety standards and regulations will ensure your SIS can prevent process incidents. By weaving the Functional Safety Lifecycle into the very culture of a facility it becomes natural to execute SIS-related tasks with the level of rigor required to uphold your SIS design.

Several things could be hiding under your SIS radar, but there are direct steps to take so that those things won’t hinder your SIS. These steps include implementing SIS-specific training, alignment of facility stakeholders on SIS task responsibilities, and spreading knowledge of the Functional Safety Lifecycle requirements. Executing the Functional Safety Assessments throughout the entire lifecycle of the SIS will also help you stay on the right track along your SIS journey by detecting systematic errors early to reduce unnecessary risk.

Be careful not to trip on your SIS design parameters. Similar to a new car driving off the dealership lot, SIS certified devices immediately decline in reliability as they age. Over time due to wear-out and other failure modes, your devices can underperform if they are not properly maintained and tested. This can lead to your SIS failing to do its job – protecting you, your colleagues, and nearby populations. Ensuring SIS devices are properly tested and replaced (or refurbished to like new condition) when specified will help guarantee everyone in the facility returns home safely every day.

6 References

[1] OSHA 29 CFR 1910.119, *Process Safety Management of Highly Hazardous Chemicals*. OSHA; 2024; 331 p.

[2] IEC 61511-1, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements*. IEC; 2016; 10 p.

[3] IEC 61511-1, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements*. IEC; 2016; 9 p.

[4] Exida. *Functional Safety Term Glossary*. https://www.exida.com/resources/glossary . Accessed January 17, 2024.

[5] U.S. Chemical Safety and Hazard Investigation Board. *BP Texas City Refinery Investigation Report No. 2005-04-I-TX*. 26 p.

[6] IEC 61511-1, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements*. IEC; 2016; 38 p.

[7] U.S. Chemical Safety and Hazard Investigation Board. *BP Texas City Refinery Investigation Report No. 2005-04-I-TX*. 140 p.

[8] Goble WM, Cheddie H, *Safety Instrumented Systems Verification, Practical Probabilistic Calculations*. ISA – Instrument Society of America, Research Triangle Park, NC; 2005; 56 p.

[9] U.S. Chemical Safety and Hazard Investigation Board. *ExxonMobil Torrance Refinery Investigation Report No. 2015-02-I-CA*. 2017. Section 3.4.

[10] U.S. Chemical Safety and Hazard Investigation Board. *ExxonMobil Torrance Refinery Investigation Report No. 2015-02-I-CA*. 2017. Section 5.3.2.

[11] U.S. Chemical Safety and Hazard Investigation Board. *ExxonMobil Torrance Refinery Investigation Report No. 2015-02-I-CA*. 2017. Section 1.

[12] U.S. Chemical Safety and Hazard Investigation Board. *ExxonMobil Torrance Refinery Investigation Report No. 2015-02-I-CA*. 2017. Section 5.3.1.

[13] Goble, William. *How to Calculate Proof Test Coverage*. (2014) https://www.exida.com/blog/how-to-calculate-proof-test-coverage . Accessed February 17, 2024.

[14] U.S. Chemical Safety and Hazard Investigation Board. *BP Texas City Refinery Investigation Report No. 2005-04-I-TX*. 133 p.

[15] U.S. Chemical Safety and Hazard Investigation Board. *BP Texas City Refinery Investigation Report No. 2005-04-I-TX*. 321 p.