Honeywell

THE POWER OF **CONNECTED**

Plant & Personnel Safety

2019 CONTROL ENGINEERING eBook Series

2019 PLANT ENGINEERING eBook Series

Contents

Process control safety and compliance advice

Process safety regulations, standards, and loss prevention practices are derived from a tangled web of documents and it's vital for a company to know the different agencies, standards, and other groups involved to reduce potential confusion.

Process safety regulations, standards, and loss prevention practices are derived from a tangled web of documents. Navigating references between entities can be convoluted to determine if a process safety system is in compliance with all of the associated parties. Over the years, many things have changed in the industry including products, standards, regulations, and equipment approvals. These changes have resulted in improved safety measures through risk avoidance and advancements in technology and products.

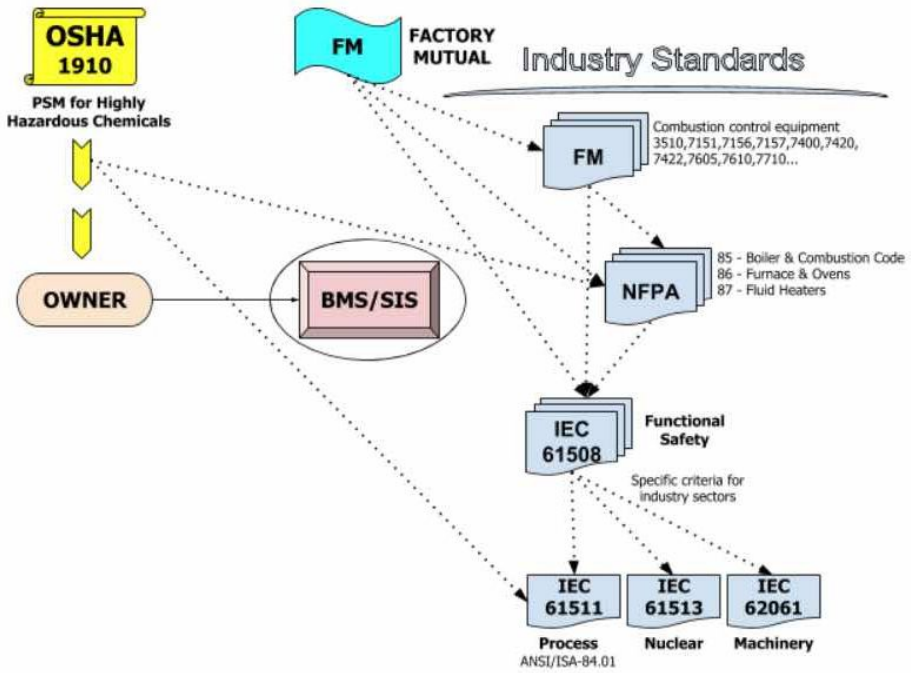
There are many government agencies, standards organizations, end-users, and other entities working to make the process industry safer. Knowing what their role is in identifying how a process safety system is to be designed, operated, and maintained over its lifecycle can help reduce some of the inherent confusion.

Occupational Safety & Health Administration (OSHA)

The United States Occupational Safety and Health Act 1970 created the Occupational Safety and Health Administration (OSHA), which is part of the United States Department Of Labor. The purpose of this administration is to assure the safe and healthy working condition for men and women by setting and enforcing standards, providing training, outreach, education and assistance. In 1992, OSHA created the Process Safety Management (PSM) regulation, which is composed of standards of organizational and operational procedures. Specifically, 29 CFR 1910.119 contains requirements for preventing or minimizing

the consequences of toxic, reactive, flammable, or explosive chemicals. US companies that contain 10,000+ pounds of hazardous material are required to adhere to the PSM documented regulations.

PSM is a performance-oriented standard which allows employers flexibility in complying with the requirements. The standard directly references and enforces Recognized And Generally Accepted Good Engineering Practices (RAGAGEP). These consists of widely adopted codes such as NFPA, consensus documents, non-consensus documents, and internal standards. In 2000, OSHA officially recognized the revised ANSI/ISA S84.01-1996 "Application of Safety Instrumented System for Process Industry" as a generally accepted good engineering practice.



Compliance with ISA S84.01 does not ensure compliance with PSM standards because the regulations cover a broader spectrum than just functional safety for the process industry sector. However, if a company can demonstrate an existing safety instrumented system

(SIS) designed to 1910.119(d)(3)(i)(F) (design codes and standards employed) complies with ISA 84 (technically now transitioning to IEC 61511) and meets all other OSHA PSM requirements related to a SIS, it shall be considered in compliance.

Factory Mutual (FM)

Factory Mutual (FM) is a global insurance provider and loss prevention engineering company that determines risk by engineering analysis versus actuarial approach. FM provides an extensive testing and approval process to ensure products meet quality, technical integrity, and performance for the purposes of property loss prevention. FM Approval is recognized and respected worldwide.

FM has developed an extensive set of combustion control standards used for testing and approval reference purposes. This includes automatic shutoff valves, flame sensors, flow and pressure switches, and other combustion control equipment. Specifically, FM 7605 is an approval standard that defines the requirements for programmable logic controller-(PLC) based burner management systems. This standard directly references compliance of both hardware and software to meet the requirements defined in IEC 61508 Standard on Functional Safety of Programmable Electronic Systems.

The figure below depicts the relationship between regulating bodies, the underwriter, and industry standards. Dotted lines represent direct references of the associated standard within the written documentation.

National Fire Protection Association (NFPA)

The National Fire Protection Association (NFPA) is a global nonprofit organization devoted to eliminating death, injury, property, and economic loss due to fire, electrical and related

hazards. This is accomplished by delivering codes and standards to minimize risk. In reference to the use of BMS, they have produced NFPA 85-Boiler and Combustion System Hazard Code, NFPA 86-Standard for Ovens and Furnaces, and NFPA 87-Standard for Fluid Heaters.

In 2015, the NFPA standards listed above were updated to invoke the concept of an SIS by referencing ISA 84/IEC 61511. The NFPA 85 standard is a prescriptive approach with specific requirements. This standard also states an end-user can utilize alternate solutions as long as one can demonstrate conformance to the ISA 84/IEC 61511 standard, which is a performance-based standard, and approval of the appropriate authority having jurisdiction.

American National Standards Institute/International Society of Automation (ANSI/ISA)

The American National Standard Institute (ANSI) oversees development, promotion, and safeguard standards and guidelines for the purpose of global competitiveness of U.S business and quality of life. This organization manages and coordinates a national consensus by standardizing and accrediting the procedures of the standards developing organizations. This means they confirm that the standards meet the institute's requirements for openness, balance, consensus and due process.

The International Society of Automation (ISA) is a nonprofit professional association that sets the standard for applying engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. ISA covers a broad range of concepts in the automation field and most of them have been recognized by ANSI. In reference to the content herein, the

ANSI/ISA 84 standard defines the standard and technical reports for use in applying Electrical/Electronic/Programmable Electronic System (E/E/PES) for use in process safety applications. This standard was created to supplement the PSM in implementing the instrumentation and controls necessary for safe operation. In general, the standard covers the safety lifecycle, which outlines a process from cradle to grave, and defines safety integrity level (SIL), which is a measurement of performance based on risk reduction.

International Electrotechnical Commission (IEC)

The International Standards Commission (IEC) is an international standards organization that prepares and publishes international standards for all electrical, electronic and related technologies.The commission developed IEC 61508 that outlines a global functional safety standard that applies to equipment manufacturers for developing products utilized in safety applications, which applies to all industry sectors. This standard ensures the quality and reliability of safety equipment providing an umbrella standard covering all industries.

Many countries around the world do not have regulating organizations such as OSHA to ensure safe working conditions. This led to the need to develop the IEC 61511 standard, which covers safety management, hazard analysis, design and implementation, pre-startup safety review, and training, which encompasses the life-cycle concept. Essentially, this standard outlines engineering practices to ensure the safety of industrial processes.

IEC 61508 has a narrow sector focus on the process industry and, more specifically, requires that an analysis is performed to remove any single failure of common equipment that can cause unsafe conditions. This concept was adopted by ANSI/ISA S84 and provides engineering concepts and strategies to meet the analysis requirements.

The standards outlined above identify some key attributes that define clear requirements for safety system compliance. This includes the use of input/output (I/O) modules approved or certified by an accredited body. No single failure of common equipment should be able to cause a process hazard. Also, independent or isolated safety functions from other basic process control logic must be protected from unintentional effects. This means burner management system (BMS) logic must be isolated from the standard combustion control logic. These details govern how systems are designed and applied. Many older systems do not comply with the new standard and the following section provides insight into the compliance of legacy systems.

The compliance of legacy systems

All over the US, hazardous industrial process systems have been running for decades. During the design and installation phase of these legacy systems, they may have complied with the existing safety standards. Unfortunately, over the years we have witnessed some safety failures that resulted in catastrophic incidents. These incidents have led to changes in the industry and an advancement in testing and quality assurance of the initiating and corrective devices, as well as a statistical risk-avoidance approach to the system design. Most legacy systems include non-safety rated components and/or controllers. These cases have led to OSHA including a grandfather clause within the PSM regulation released in 1992. Later ISA recognized that legacy equipment concern in the industry and included a grandfather clause within the ANSI/ISA 84 standard as well.

The grandfather clause (1.y) states the following: "For existing SIS designed and constructed in accordance with codes, standards, or practices, prior to the issue of this standard (for example, ANSI/ISA-84.01-1996), the owner/operator shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner".

Many existing legacy SIS installations utilize a run-to-fail strategy, which can have unpredictable consequences. The SIL concept provides a predictable failure rate during the useful life cycle of the device. However, once the device has exceeded the end of the life cycle it can have sporadic failures and the predictability no longer applies. Therefore the SIL rating of the associated Safety Instrument Function (SIF) can exceed the expected value causing exposure to additional unintended risk.

How "safe is safe enough" is a question every owner must determine. The grandfather clause listed above provides owners with the ultimate decision to determine if they meet the standards. OSHA defines very clearly in the PSM requirements that all safety systems must have safety specifications, operating procedures, personnel training, failure tracking, management of change, and audit records irrelevant to the installation date. Traditionally, when OSHA performs an investigation they compare to the current published good engineering practices regardless if the process was installed prior to issuance of S84.01-2004. So, determination of a "safe" system is up to the owner, but upon judgment day only current published standards will be referenced.

This gap between acceptance and judgment has prompted the ISA 84 committee to publish seven additional technical reports to further support the subjects around this topic. Technical Report, TR84.04, provides two steps to evaluating legacy systems include a hazard/risk analysis and the SIF to meet a predetermined risk level. The risk level can be determined by economic or asset protection as defined by the owner. The OSHA PSM regulation, as well as FM Global underwriters, utilize a risk-reduction approach to define a clear measurable risk level. The owner chooses how risk is determined, but it must be clearly documented with supporting evidence.

Process safety is a major concern to everyone, not just those that work in process facilities. For decades, many different methods and strategies have been deployed. OSHA has attempted to regulate the compliance to ensure standards are adhered to. The supporting sections above outline some of the major supporting standards and how each is referenced in an effort to clarify what exactly is the base reference.

Process owners are ultimately responsible to determine if they are truly "safe." While the way this is determined is optional, having data to support the claim is not. Risk avoidance is the best-published method known and alternative methods are acceptable, but providing the data to support an alternative method and convince the governing bodies is risky within itself. In most cases, the lack of concern for meeting the safety requirements is due to lack of understanding of the requirements.

Compliance can be a convoluted subject and requires extensive knowledge and analysis to determine. It is highly recommended to pull in third-party experts to accurately deduce whether you are in a comfortable risk zone.

Robbie Peoples, *integration manager, Cross Company. This article originally appeared on Cross Company online. Cross Company is a CFE Media content partner. Edited by Emily Guenther, associate content manager, Control Engineering, CFE Media, eguenther@cfemedia.com.*

Process safety systems: devices, instruments, and effective data analysis

Data analytics can now help you improve process safety, especially when supporting the entire safety lifecycle framework. Safety systems have identifiable stages and involve different specialized functions; know how each can help reduce risk.

Investments in process safety for the hydrocarbon and process industries are necessary not just to protect people and the environment, but also to facilitate profitable operations. A 2014 analysis by insurance broker Marsh found combined financial losses from the 100 largest accidents in the hydrocarbon industry since 1974 totalled over $34 billion, according to a March 19, 2014, news story posted by the Institute of Chemical Engineers.

Given this significant potential for losses, increasing understanding of the risks, growing regulatory demands and advances in automation, recent decades have seen a proliferation of safety interlocks in process plants. While this has significantly reduced the number of catastrophic incidents, it has also added to the number and complexity of safety systems that must be managed in the design and operating phases of the lifecycle.

As a consequence of the significant increase in the number of devices and instruments within the safety system, we have seen more formal processes for assessing, grading and implementing safety systems. We have also seen a massive increase in the data collected by the process historians, including an increase in the number of trip activations, both legitimate and spurious. And of course, there's the data from the maintenance systems.

Plants and their corporate leadership need a way to understand and harness this data.

Making sense of the safety lifecycle

Perhaps among the best ways of making sense of the complexity of process safety is to view it within the framework of a safety lifecycle. Just as the process and plant itself experiences a lifecycle that takes it through design to engineering and start-up and beyond, the safety systems has identifiable stages across different plant personnel functions:

→ The initial design and process hazards analysis (PHA) by process designers

→ The layer of protection analysis (LOPA) done by process safety engineers

→ Design of safety interlocks, including the safety requirements specification (SRS) by functional safety staff

→ Installation, testing and start-up

→ Operations, maintenance and periodic review, with the analysis feeding back to design revisions – beginning the lifecycle again.

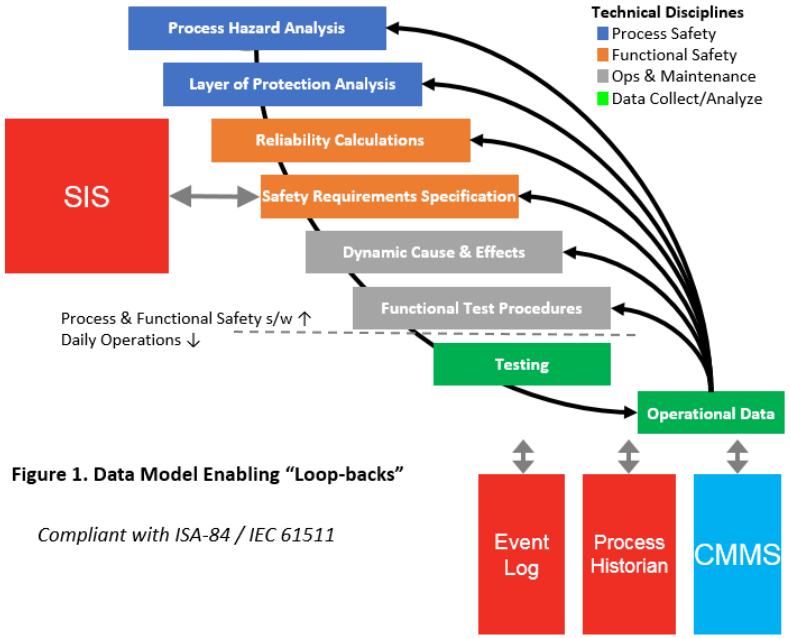


Figure 1. Data Model Enabling "Loop-backs"

Compliant with ISA-84 / IEC 61511

Figure 1: *The safety system lifecycle. All images courtesy: Honeywell*

This can be further broken down into the eight activities in Figure 1.

This view of the safety lifecycle has three major benefits: First, it makes it clear that process safety system design is an iterative process; indeed, the effectiveness of a safety system will inevitably degrade over time if it is not properly maintained and fails to adapt to changes in the process. Second, it illustrates the range of different functions involved. No single discipline can ensure an effective safety system; all must work together and the consequences of each discipline's decisions will be felt across the lifecycle.

Finally, it helps highlight the fact that there are multiple opportunities to improve the safety system. In particular, technology can bring enhancements each stage of the lifecycle and to the flow of data and transition between them.

This is most easily – and perhaps only – achieved by technology, which has significant scope to bring enhancements across each of the stages to make safety system design, maintenance and review more efficient and effective.

Starting on the right foot

As Figure 1 illustrates, safety system design at the outset (before the system is up and running) starts with the PHA, LOPA and then reliability calculations and SRS, during which safety integrity levels (SILs) for the key interlocks are determined. Advanced software has a significant role to play in these initial stages in smoothing and formalizing the process.

Traditionally, the PHA and LOPA done by the process safety functions would either be paper-based or use simple spreadsheet software, such as Microsoft Excel. Many people still do it this way, though nowadays specific software packages are often used for some of the steps.

By pulling these processes into an integrated software platform, such as Honeywell's Pro-

cess Safety Suite (PSS), that covers the whole lifecycle, plants can, first, structure the process; second, eliminate the need for rekeying data (and therefore the scope for error); and, third, smooth the data flow to the functional safety disciplines responsible for reliability calculations and the SRS. Both teams can use the same software, working on and from the same data.

The software also can be integrated with a configuration tool for the SIS Programming process, such as Honeywell's Safety Builder. After all, the logic has already been described in the SRS. This allows users to track changes and provides structure, guidance and compliance with industry standards: Helping design the plant's safety network, define the hardware set-up, design functional logic diagrams, upload the application and establish a live connection with the safety system. PSS can incorporate this data, and then the software can be used by automation engineers to identify and locate the precise transmitters, switches, valves, and other interlocks to be implemented.

The result overall is a more automated, structured efficient, and controlled process in the initial design and implementation of the safety system – with consistent data flowing seamlessly between the disciplines involved.

Another round

The more powerful application of such software, however, is seen once the safety system is up and running and starts to generate data. The PSA software can then use the time-stamped event data – which records all relevant process conditions and safety equipment data each time variables reached an alarm or interlock level – to continually feed back into each stage of the safety lifecycle. It also can be combined with analysis of historian data on equipment and process health from software, such as Honeywell's Uniformance® Asset Sentinel.

The result is a detailed view of the operation of shutdown systems and safety elements, as well as process safety risk in practice. This includes both leading indicators (before any incident or action occurs), with process or equipment changes and trends indicating a developing problem; and lagging indicator (after the incident or action), with analysis used to validate the performance of safety elements or identify the root causes of faults, if any.

This informs each stage of safety lifecycle, testing, validating, and refining the assumptions of the initial design against the real-world operational data:

→ Identifying and refining hazards for the PHA revalidation team according to those revealed in operation

→ Assessing the adequacy of the LOPA, whether protections worked in practice and what others may be required

→ Proofing and validating reliability calculations and SRS, revising these using data on the actual incidence of identified hazards, for example, and performance of safety elements in practice and providing real-world data on expensive issues like high spurious trip rates

Figure 2: *Three logical places to get started*

→ Assessing and refining operational maintenance procedures and tests. For example, if an emergency block valve worked perfectly during a power blip last week, does it need to be tested during next week's turnaround?

The software provides a consistent single data source and framework and allows data to seamlessly flow between teams and continually around the lifecycle (Figure 2).

Benefits

There are several benefits to such a structured, automated and technology-led approach to managing the safety lifecycle. Three are particularly worth highlighting:

→ Most obviously and importantly, it improves safety. A single source of data that flows consistently between each team and system significantly reduces the scope for errors. And the analytics engines compare the expectations with data coming back from the process historian to identify when something isn't working the way it was expected to.

→ It improves efficiency, not only in automating data capture and calculations, but also in eliminating unnecessary spending. Providing real-world analysis of the actual risks and performance of safety instrumented functions implemented, plants can direct spending on safety to areas where it is most effective.

→ It ensures compliance with standards like IEC 61511 / ISA 84.00.01 Functional safety - Safety instrumented systems and Recommended Practices like API RP 754 Process Safety Performance Indicators for the Refining and Petrochemical Industries. These call for methods to identify and inform appropriate personnel at various levels in an organization on key performance indicators (KPIs) in relation to safety (both leading and lagging indicators). IEC61511 also calls for periodic functional safety assessments of each installed safety instrumented system (SIS) after a few years of operation using KPIs to assess if it is performing as intended. The software facilitates this – and to an extent automates it.

These benefits are largely the result of two effects that technology have on the process.

First, it formalizes the design and review of the safety system over the lifecycle. It moves it from a rules-based, subjective approach to a data-based, objective process. The software informs the process with data specific to the plant's actual operation (rather than basing it on industry-wide standard failure rate data or manufacturers' specifications). This results in a more effective safety system. It also contributes to the increase in efficiency, since plants have sought to get this information in the past from reliability engineers and maintenance teams, but it is time consuming and difficult to put together. Constructing the LOPA, for example, there may be data on inspection results or repair history. However, it's time-consuming for a maintenance organization to report this in detail in its computerized maintenance management system (CMMS); it rarely provides the detail, such as the tag number of the particular instrument or valve involved, required to make a difference; and the information often does not make it back to the process safety teams responsible for the design – and if it does, it needs to be laboriously transcribed.

In capturing the required data and automating its integration in SIS design, plants make themselves less dependent on the opinions of maintenance representative and safety engineers, with the software automatically and proactively identifying safety issues. At the same time, it reduces the effort required to capture and use application-specific data, freeing scarce engineering expertise from laborious functional safety "data gathering" to concentrate on analysis and on fixing problems.

The second key characteristic of a technology-led approach, meanwhile, is that it democratises the process safety data. As well as providing consistent data across the lifecycle, the software can be deployed through the cloud to make this data and associated analysis

(securely) available across the organization and at different levels of the organization. That ensures that safety data can be made visible to relevant staff, wherever they are based, and also makes the best use of those with process safety expertise across the organization.

Key performance indicators to inform decisions can be tailored for each level of the organization: with detailed data focusing mostly on leading indicators at the facility, plant and shift level; and summary data, concentrating on lagging indicators, for corporate, business activity and business unit level (Figure 3).

Next steps

Both these facets of the technology also offer opportunities for future improvement in the process.

First, the data-driven approach not only leads to more objective, robust safety system design, but will soon allow predictive changes, anticipating problems that could cause shutdowns or safety issues in the future. Process safety engineers will not have to wait for event data to inform SIS design, but will be able to use the data analytics to predict the likelihood of initiating events. For example, if operations move closer to an interlock set point, then there may be an increased demand rate on that interlock. Statistical analysis of the process data can predict the future trip rate.

Second, the democratization of data is a two-way flow: Not only does it give access to the data that process safety experts need, wherever they are based; it also provides the ability for them to share their expertise with others in the organisation and tackle risks by driving best practice out into the field. Using intelligent wearables, for instance, field workers can access heads up displays with augmented reality (Figure 4) that can be used to provide information about procedures and checklists for maintenance tasks and safety checks. Risks and root causes identified through PSS that are either caused by field workers or can be addressed by them can be directly influenced. We can help them avoid making critical errors.

Finally, these developments help highlight perhaps the key benefit of seeing the SIS design in the context of the safety lifecycle: By continuously comparing their actual performance against their intended performance, looking for gaps, businesses have ample opportunity to aim for continuous improvement in safety across their plants.

Determine safety integrity level for a process application

Safety instrumented systems (SIS) are installed in process plants to mitigate process hazards and they must be assigned a target safety integrity level (SIL) during the process to determine what needs to be done next.

Safety instrumented systems (SIS) are installed in process plants to mitigate process hazards by taking the process to a "safe state" when predetermined set points have been exceeded or when safe operating conditions have been transgressed.

The SIS is one protection layer in a multi-layered safety approach since no single safety measure alone can eliminate risk. A layer of protection analysis (LOPA) is a method whereby all known process hazards and all known layers of protection are closely scrutinized. For each process hazard where the LOPA study concludes that existing protection cannot reduce risk to an acceptable or tolerable level, a SIS is required. Not all process hazards will require the use of a SIS. Each hazard that requires the use of an SIS must be assigned a target safety integrity level (SIL).

What are SIL levels?

SILs comes from two voluntary standards used by plant owners/operators to quantify safety performance requirements for hazardous operations:

→ **IEC 61508:** Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
→ **IEC 61511:** Safety Instrumented Systems for the Process Industry Sector.

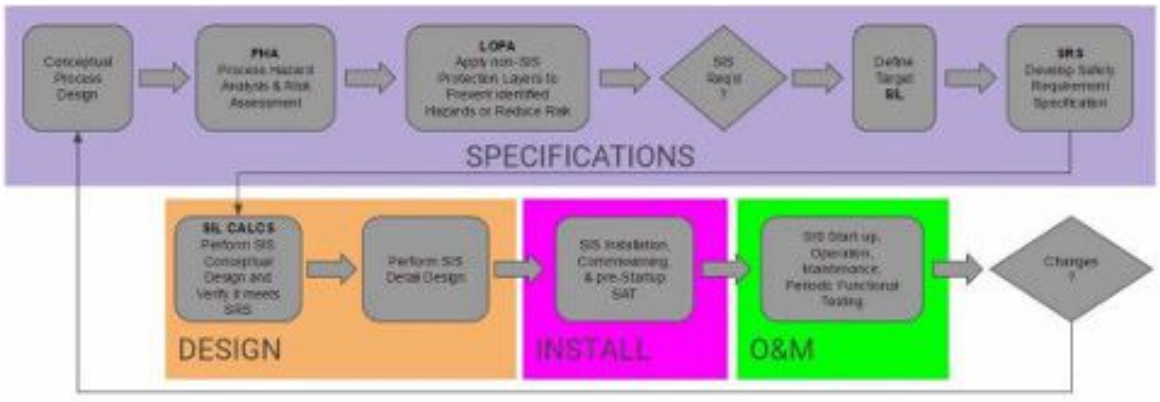
As defined in the IEC standards, there are four SIL Levels (1-4). A higher SIL Level means a greater process hazard and a higher level of protection required from the SIS. SIL Level is a function of hazard frequency and hazard severity. Hazards that can occur more frequently or that have more severe consequences will have higher SIL Levels.

To determine SIL Levels of process hazards, it is helpful to understand the safety lifecycle.

Safety lifecycle

The IEC standards define a concept known as the safety lifecycle, which provides a repeatable framework whereby all process hazards are identified and analyzed to understand which hazards require the use of a SIS for mitigation. By design, this is a cyclical process. Any changes in process design, operating conditions, or equipment requires cycling back to the beginning to ensure any changes are properly implemented.

There are many steps to follow to determine SIL Level and it starts with performing a process hazard analysis (PHA).



Example of a safety lifecycle model. Courtesy: Cross Company, adapted from IEC 61511

A PHA is a systematic assessment of all potential hazards associated with an industrial process. It is necessary to analyze all potential causes and consequences of:

→ Fires
→ Explosions
→ Releases of toxic, hazardous, or flammable materials, etc.

Focus on anything that might impact the process including:

→ Equipment failures
→ Instrumentation failures or calibration issues
→ Loss of utilities (power, cooling water, instrument air, etc.)
→ Human errors or actions
→ External factors such as storms or earthquakes.

Both the frequency and severity of each process hazard must be analyzed:

→ *How often could it happen?* Tank spills could happen any time there's a manual fill operation (multiple times a year)
→ *How severe is the result?* Localized damage, fire, explosion, toxic gas release, death.

Core to the PHA analysis is the fact that things can and do go wrong. Forget whether if it will happen and instead consider when it will happen. Each identified hazard is assigned an "acceptable" frequency. You cannot assume a hazard will "never" happen.

→ A hazard which results in simple First Aid could be considered "acceptable" if it could happen only once a year
→ An explosion and fire due to a tank rupture could have an "acceptable" frequency of once in 10,000 years.

The end result of the PHA is a list of all possible process hazards with each one assigned an acceptable frequency of occurrence. With the PHA complete, the next step in the safety lifecycle is the layer of protection analysis.

No single safety measure alone can eliminate risk. For this reason, an effective safety system must consist of protective layers. This way if one protection layer fails, successive layers will take the process to a safe state. As the number of protection layers and their reliabilities increase, the safety of the overall process increases. It is important to understand that each layer must function independently from the others in case one or more layers fails.

Some specific examples of protection layers include:

→ Fire suppression systems
→ Leak containment systems (dikes or double walls)
→ Pressure relief valves
→ Gas detection/warning systems.

For every process hazard identified in the PHA:

→ List all available non-SIS safety measures
→ Assign each layer its own hazard risk reduction factor
→ Calculate an effective hazard frequency with protection layers applied.

Example: A tank fill operation that happens 250 times per year – "could" experience an overfill event 250 times per year.

→ A protection layer in the form of a proper vent/drain system could reduce the danger by a factor of 100 (risk reduction factor)
→ The hazard resulting from tank overfill would have an effective frequency of 250/100 = 2.5 times per year.

After the effective hazard frequency of each hazard is known, the key question to ask is: "With non-SIS protection layers applied, is the effective frequency lower than the acceptable frequency?"

Once all process hazards are identified and protection layers assigned, if the PHA/LOPA study concludes that existing protection cannot reduce risk to an acceptable or tolerable level, a safety instrumented system (SIS) will be required. Not every process hazard, however, actually requires the use of a SIS.

Safety instrumented systems and functions

The purpose of a SIS is to take a process to a "safe state" when predetermined set points have been exceeded or when safe operating conditions have been transgressed.

The role of the SIS is to reduce risk by implementing safety instrumented functions (SIFs). Two example SIFs include:
→ **Hazard: Tank overfill. SIF:** The SIS stops the fill pumps at a predetermined safe level
→ **Hazard: High temperature. SIF:** The SIS opens a relay to cut power to a heater circuit at a predetermined safe temperature.

In any case, an SIF is a safety function implemented by the SIS to achieve or maintain a safe state. An SIF's sensors, logic solver, and final elements act in concert to detect a haz-

ard and bring the process to a safe state.

Each SIF serves as a protection layer to bring the effective hazard frequency down below the acceptable hazard frequency. To do this, each SIF must have a minimum risk reduction factor.

Target SIL level of the SIF

With the tank overfill example, it was determined that after applying non-SIS protection layers there was an effective frequency of 2.5 times per year. If the acceptable hazard frequency is once in 10 years, then the SIF must have a risk reduction factor (RRF) of at least 25.

→ Minimum RRF of SIF = Effective frequency w/o SIS / Acceptable frequency = 2.5/0.1 = 25.
→ The minimum required RRF of each SIF is used to determine the target SIL level of the SIF.

Target SIL Level is directly determined from the required RRF by using the table in Figure 3. Note the relationship between SIL Level and RRF. SIL1 has a minimum RRF of 10^1, SIL2 has a minimum RRF of 10^2, and so on.

SIL Required Risk Reduction Factor (RRF)

1	10 to 100 (10^1 to 10^2)
2	100 to 1,000 (10^2 to 10^3)
3	1,000 to 10,000 (10^3 to 10^4)
4	10,000 to 100,000 (10^4 to 10^5)

For the tank overfill example, the minimum RRF is 25, the target SIL level of the SIF is SIL1 and this is, therefore, an SIL1 hazard.

For each hazard identified by the PHA and LOPA that requires an SIF, a target SIL level is assigned using the same methodology. Note that it is likely you will have various target SIL levels. The next step in the process is to design a SIS capable of implementing the required SIFs and reaching the target SIL levels.

Achievable SIL level of the SIF

The SIS is a system comprised of numerous components such as:

→ Sensors for signal input
→ Input signal interfacing and processing
→ Logic solver with power and communications
→ Output signal processing, interfacing, and power
→ Actuators (valves, switching devices) for final control function.

An example SIF where the SIS de-energizes a relay to open a heater circuit upon high temperature could have any or all of the following loop components:

→ Thermocouple
→ Transmitter
→ Input signal conditioner or barrier
→ Analog input card
→ Communication card(s)
→ CPU

→ Discrete output card
→ Output signal conditioner or barrier
→ Heater circuit relay.

One must assume that a hazard will occur at some point. You cannot assume a hazard will "never" happen. Similarly, one must assume that any of the components of the SIF could fail to act upon demand.

One very common failure would be an isolation valve that remains open under normal process conditions. If this valve is required to close to achieve a particular SIF, it is possible that the valve could stick open and not close upon demand. For this reason, one must know the failure probability the SIF.

The overall failure probability of a given SIF is determined by performing SIL calculations (SIL calcs). SIL calcs are somewhat complex and are outside the scope of this article but essentially, the process is to gather failure rate data for the SIF components and account for factors such as test frequency, redundancy, voting arrangements, etc. The end result is that for each SIF, you end up with an overall probability of failure on demand (PFD).

Failure rate data for the numerous pieces of equipment that make up SIF loops are published by the equipment manufacturers. Companies frequently contract with consultants to determine failure rate values.

It is failure rate data that is required as an input to perform SIL calcs for an SIF, not SIL Level data. There is no such thing as an SIL-rated device. We don't buy SIL-rated transmitters or SIL-rated control systems.

Once the PFD of the SIF is known, then its RRF is simply the inverse of PFD (RRF = 1/PFD). You can then compare the SIF's RRF to the minimum required RRF. If the SIF's RRF is greater than the minimum RRF, then the SIF is sufficient to reduce the overall hazard level below the acceptable level.

Returning to our tank overfill example, let's assume the SIL calcs prove the SIF has an RRF of 300. Since this is greater than 25, then the SIF is sufficient. If the SIL calc had found an RRF of less than 25, then changing or rearranging the SIF components would be necessary. One way to increase the RRF is to install redundant transmitters in a voting arrangement or to purchase transmitters with lower published failure rates.

The relationship between SIL level, RRF, and PFD is demonstrated below.

SIL	PFD	RRF
1	1 in 10 – 1 in 100	10 to 100
2	1 in 100 – 1 in 1,000	100 to 1,000
3	1 in 1,000 – 1 in 10,000	1,000 to 10,000
4	1 in 10,000 – 1 in 100,000	10,000 to 100,000

Going back to the tank fill example, there was a minimum RRF of 25 (SIL1) with an SIF RRF of 300. The achievable SIL level of the SIF is SIL2. This means there's an SIL2-capable SIF being used to protect an SIL1 hazard. This is perfectly acceptable and is not unusual.

David Yoset *is a project manager with Cross Company. This article originally appeared on Cross Company's Integrated Systems blog. Edited by Chris Vavra, production editor,* Control Engineering, *CFE Media, cvavra@cfemedia.com.*

Bringing safety and security together for process control applications

It is important to understand the interaction between safety and security in process control applications to make better overall decisions.

Every production process comes with inherent risks. To achieve the greatest degree of safety and security, it is vital to implement an effective separation of the process control and safety systems, which is required for functional safety and cybersecurity standards. There is a lot at stake, including the employees' health, the company's assets, and the environment.

For a better understanding of the interaction between safety and security, it is helpful to clarify several terms. There are numerous definitions of safety. A general definition of safety is the absence of danger. This means a condition is safe when there are no prevailing hazards. It often is not possible to eliminate all potential risks; especially in complex systems.

A more common definition of safety is the absence of unacceptable risks. Reducing risks to an acceptable level is functional safety's task. An application's safety depends on the function of a corresponding technical system, such as a safety controller. If this system fulfills its protective function, the application is regarded as functionally safe.

This can be clarified with these two examples: oil flowing out of a pipeline and endangering people in the vicinity is a safety issue. A system that cannot prevent icing in a pipeline, even though that is supposed to be its task, and then a critical situation arises, is a functional safety issue. Functional safety systems protect people, facilities, and the environment and are intended to prevent accidents and avoid downtime of equipment or systems.

Separate layers reduce risks

The process industry increasingly is becoming aware of the importance of relevant standards for the safety and profitability of systems. Technical standard IEC 61511, Functional safety – Safety instrumented systems for the process industry sector, defines the best way to reduce the risk of incidents and downtime. It prescribes separate safety layers for control and monitoring, prevention and containment, as well as emergency measures (see Figure 1). Each of these three layers provides specific functions for risk reduction, and collectively they mitigate the hazards arising from the entire production process.

Figure 1: *IEC 61511 prescribes separate safety layers from control and monitoring, prevention and containment, as well as emergency measures. Image courtesy:* Control Engineering Europe/*Hima*

IEC 61511 also prescribes independence, diversity, and physical separation for each protection level. To fulfill these requirements, the functions of the different layers need to be sufficiently independent of each other. It is not sufficient to use different I/O modules for the different layers because automation systems also are dependent on functions in I/O bus systems, CPUs and software. To be regarded as autonomous protection layers in accordance with IEC 61511, safety systems and process control systems must be based on different platforms, development foundations, and philosophies. In concrete terms, this means the system architecture must, fundamentally, be designed so no component in the process control system level or the safety level can be used simultaneously.

Rising risk

In the last 10 years, the risk of cyber attacks on industrial systems has risen due to increas-

ing digitalization. In addition to endangering information security, these attacks increasingly pose a direct threat to system safety. System operators need to be aware of these risks and address them. This can be achieved in a variety of ways. Unlike functional safety systems, which are intended to protect people, these systems and measures protect technical information systems against intentional or unintentional manipulation as well as against attacks intended to disrupt production processes or steal industrial secrets.

Safety and security have become more closely meshed. Cybersecurity plays a key role, particularly for safety-oriented systems, because it forms the last line of defense against a potential catastrophe.

Standards define the framework

Compliance with international standards is necessary in the design, operation, and specification of safety controllers. IEC 61508, Functional Safety, is the basic standard for safety systems, which applies to all safety-oriented systems (electrical, electronic, and programmable electronic devices). IEC 61511 is the fundamental standard for the process industry and defines the applicable criteria for the selection of safety function components.

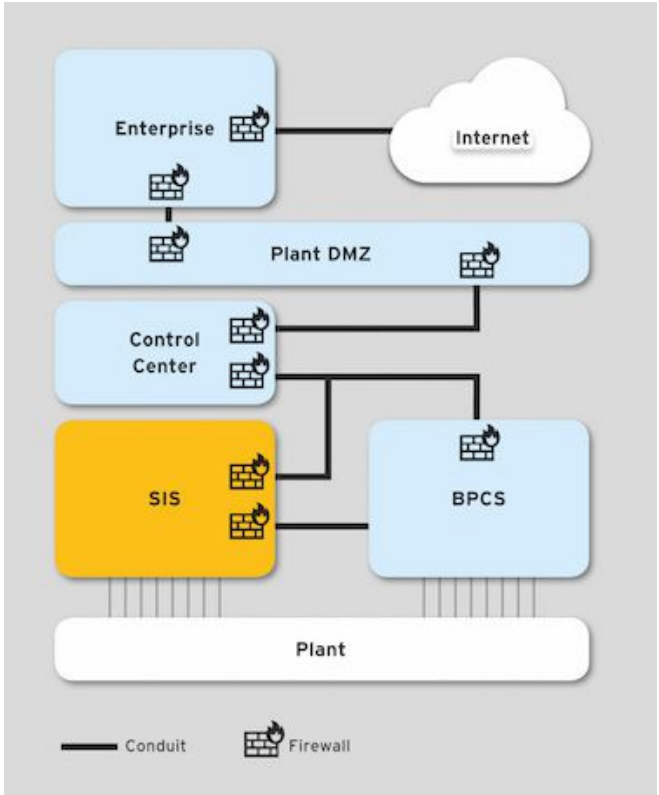


Figure 2: *IEC 62443 requires separate zones for the enterprise network, control room, SIS, and BPCS, each of which must be protected by a firewall to prevent unauthorized access. Image courtesy: Control Engineering Europe/Hima*

The IEC 62443 cybersecurity series of standards for information technology (IT) security in networks and systems must also be considered. It specifies a management system for IT security, separate protection layers with mutually independent operating and protection facilities, and measures to ensure IT security over the full life cycle of a system. It also requires separate zones for the enterprise network, control room, safety instrumented system (SIS), and basic process control system (BPCS), each of which must be protected by a firewall to prevent unauthorized access (see Figure 2).

Cybersecurity by design

Safety and security are closely related aspects of process systems, which must be considered separately and as a whole.

Standardized hardware and software in process control systems require regular updates to remedy weaknesses in the software and the operating system. However, the complexity of the software architecture makes it difficult or impossible to assess the risks analytically, which could arise from a system update. For example, updates to the process control system could affect the functions of the safety system integrated into the control system.

To avoid critical errors with unforeseeable consequences in safety-relevant processes as a result of control system updates, the process control system must be technologically separate from the safety system. For effective cybersecurity, it is not sufficient to upgrade an existing product by retrofitting additional software functionality. Every solution for functional safety must be conceived and developed with cybersecurity in mind, right from the start. This applies equally to the firmware and the application software.

Effective protection

An example of effective protection is a proprietary operating system specifically designed for safety-oriented applications and runs on autonomous safety controllers. It includes all functions of a safety PLC and excludes all other functions, making it immune to typical attacks on IT systems. The CPU and the communication processor need to be separate for operational security even in the event of an attack on the communication processor. The controllers allow several physically separate networks to be operated on a single communication processor or processor module. This prevents direct access to an automation network from a connected development workstation. In addition, unused interfaces can be disabled individually.

A common feature of the process industry standard and the cybersecurity standard is the required separation of the SIS and the BPCS. This independence of safety systems is a good idea from a practical and economic perspective. The SIS and BPCS have, for example, very different life cycles and rates of change. System operators are free to choose "best-of-breed" solutions from different manufacturers.

Systems independent of the process technology, which can be integrated into process control systems despite physical separation, offer the highest degree of safety and security for critical applications. They are the best way to increase the operational reliability and availability of process systems and improve the overall profitability of a production process.

Dr. Alexander Horch *is head of the R&D and product management business area at HIMA Paul Hildebrandt. This originally appeared in a September 10 article on the* Control Engineering Europe *website. Edited by Chris Vavra, production editor,* Control Engineering, *CFE Media, cvavra@cfemedia.com.*

Four overlooked aspects of risk management, process safety

Process safety trends in risk management and functional safety: The basic process control system (BPCS) focuses on optimizing the process for business continuity. Risks mitigated through "after-the-fact" measures try to minimize an event's impact. Between these strategies lies the very important layer of Safety Instrumented Systems (SIS). See four often overlooked aspects of risk management.

Automation can help people operate more safely, and that requires a proactive application of risk management techniques. Functional safety is a positive move and can help control engineers and those around them rest easier. Risk management has four often overlooked areas.

What is risk management?

Every engineered system has risks: to people, to the environment, and to equipment and/or facilities. These risks are here to stay, but the key to good risk management is to drive them down to as low as reasonably practicable (ALARP). Functional safety, the planned reduction of those risks through automated safety systems, is increasingly being specified as a requirement in the design and retrofit of processes. Safety Integrity Levels (SILs) are here to stay.

In the process sector, risks are prevented, controlled, and mitigated through layers of protection. At the fundamental level, the basic process control system (BPCS) focuses on optimizing the process for business continuity. However, the BPCS alone provides only a piece of the risk prevention and control strategy. Conversely, risks are mitigated through "after-the-fact" measures that try to minimize the impact of an undesirable event. In be-

tween these two strategies lies the very important layer of Safety Instrumented Systems (SIS).

Safety Integrity Level SIL	PFD_{AVG} Average Probability of Failure on Demand per year (Low Demand)	RRF Risk Reduction Factor	PFD_{AVG} Average Probability of Failure on Demand per hour (High Demand)
SIL 4	>= 10^{-5} to <10^{-4}	100000 to 10000	>= 10^{-9} to <10^{-8}
SIL 3	>= 10^{-4} to <10^{-3}	10000 to 1000	>= 10^{-8} to <10^{-7}
SIL 2	>= 10^{-3} to <10^{-2}	1000 to 100	>= 10^{-7} to <10^{-6}
SIL 1	>= 10^{-2} to <10^{-1}	100 to 10	>= 10^{-6} to <10^{-5}

Achieving a given safety integrity level (SIL) requires the satisfaction of three requirements: Probability of failure on demand (PFD), hardware fault tolerance (HFT), and safe failure fraction (SFF). All three must be achieved in concert to validate that the SIF in the safety requirements specification (SRS) are adequately realized. Image courtesy: Intertek

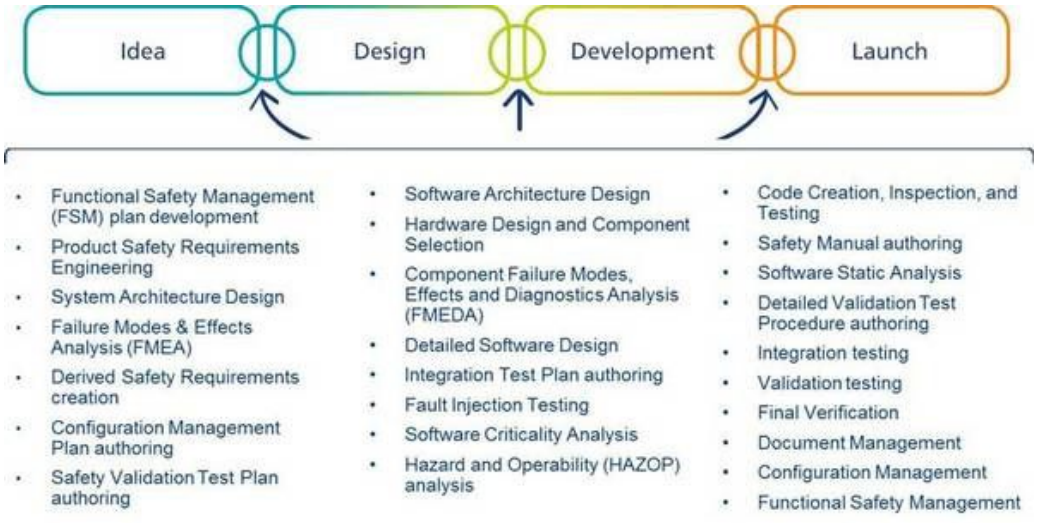
1. **Often overlooked is an initial risk assessment:** Conducting an initial risk assessment early in the process design is a critical and often missing element. Since everything relating to functional safety hinges on a proper risk assessment, re-using an old one or simply not conducting one at all hamstrings any further efforts. In fact, up to 40% of the failures in industrial accidents can be traced back to poor or lacking initial risk assessments and requirement specifications.

Meaning of SIS?

What is a SIS? A SIS is the last line of defense before calling the fire department and various three-letter government agencies. When all else fails, the SIS saves the day.

SIS can address specific needs expressed in the Safety Requirements Specification (SRS) as Safety Instrumented Functions (SIFs). These come out of a Process Hazard Analysis (PHA) or Hazard and Operability (HAZOP) study. Most processes will have several loops working simultaneously to bring risk to a tolerable level. Such systems can employ electronic, pneumatic, hydraulic, or combination control methods.

A SIS usually consists of one or more sensing elements reporting the state of the system, a logic processor to make decisions that keep the system in a safe state, and a suite of actuators to carry out the commands of the logic processor. The successful implementation of such a safety system can reduce residual risk by several orders of magnitude, with obvious benefits to safety as well as business continuity.



Part of driving down risk also means paying careful attention to risk throughout the development lifecycle, whether for a process or a product. So FSM is perhaps the most important part of any attempt at realizing reduced risk. A good FSM execution is documented, auditable, and verifiable by functional safety assessments, both internal and external. Image courtesy: Intertek

The best practices for the design, realization, operation, maintenance, and decommissioning of a SIS for the process sector are outlined by IEC 61511/ISA 84. Manufacturers of specific products, such as sensors, logic controllers, or actuators, are governed by IEC 61508. Understanding the similarities and differences between these two approaches is critical to the effective specification of components in the SIS.

2. Often overlooked is a requirements allocation: The importance of requirements allocation is often overlooked in SIS design. This vital step is where SIFs are delegated to hardware, software, or some combination of the two. Often designers are ready to

jump ahead in the process and start building the system before they have a good grasp on what the best architecture is to accomplish the required risk reduction. However, such a "leap before you look" mentality can lead to either an over-designed system that is also very expensive or, tragically, an under-designed system that exposes the operation to unacceptable risk.

Industry	Impact	Relevant Standards
Appliances	A temperature sensor used to detect unsafe temperatures during a wash cycle, which then activates a locking device on the access door	IEC 60335, IEC 60730
Medical	A flow-rate sensor used in an intravenous pump to monitor dosage given to a patient and throttled by software-controlled dispensers for tailored delivery	IEC 62304
Machinery	A light curtain used to detect when a person enters a dangerous area, which then causes the activation of a brake to hazardous rotating parts	IEC 62061, ISO 13849
Automotive	A sensor used to detect the position of a throttle pedal, which then uses software-enabled logic to select the appropriate acceleration curve to command to the engine	ISO 26262
Utilities	A thermocouple reports the temperature of a transformer to a supervisory control and data acquisition system, which then restricts current flow to extend transformer life	IEC 61511
Chemical	A level sensor, a pressure transducer, and a temperature sensor is used by a supervisory control and data acquisition to actuate valves to maintain a process within prescribed limits	IEC 61511
Railway	A proximity sensor is monitored by a logic processor to actuate a motorized railroad-crossing barrier	EN 50126, EN 50128, EN 50129
Aerospace	A pressure sensor and a radar altimeter are used with software-enabled voting logic to maintain altitude for safe separation distances between aircraft	US RTCA DO-178B, US RTCA DO-254
Nuclear	A safety-instrumented system is used to detect a seismic event, close isolation valves, and trip/isolate any supply systems that could overfill tanks	IEC 61513, IEC 60880, IEC 61238

Functional safety, the planned reduction of those risks through automated safety systems, is increasingly being specified as a requirement in the design and retrofit of processes. Image courtesy: Interlek

Achieving a SIL

How do you achieve an SIL? Both approaches above use SILs to quantify the trustworthiness of a SIS. Ranging in increasing confidence from SIL 1-4, each SIL represents an order of magnitude increase in the trustworthiness of the SIS to reduce risk to a tolerable level. This trustworthiness is measured by probability of failure on demand (PFD) calculations.

Achieving a given SIL requires the satisfaction of three requirements: probability of failure on demand (PFD), hardware fault tolerance (HFT), and safe failure fraction (SFF). All three must be achieved in concert to validate that the SIFs in the SRS are adequately realized.

3. Often overlooked is the use of available architectures: To streamline the process of achieving a SIL, it is helpful to leverage available architectures, which are often overlooked. Meeting the required PFD can be very onerous if using a one-out-of-one (1oo1) architecture. However, the design of redundancy in the system, such as with a two-out-of-three architecture (2oo3), can both increase the safety and reduce the overall cost

of the system. This can also help with the tradeoff between having a system that detects dangerous conditions while minimizing spurious trips (false alarms).

FSM importance

How important is functional safety management (FSM)? Part of driving down risk also means paying careful attention to risk throughout the development lifecycle, whether for a process or a product. So FSM is perhaps the most important part of any attempt at realizing reduced risk. A good FSM execution is documented, auditable, and verifiable by functional safety assessments, both internal and external.

4. **Often overlooked is the use of functional safety throughout the lifecycle:** Functional safety management needs to be the first thing started in the process and also the last thing completed. Waiting until after the design is finalized (or worse yet, after the system is built and ready to be commissioned) before thinking about FSM is a sure way to encounter schedule delays and cost overruns.

What's next for process safety?

Where will process safety progress? As societies around the world become increasingly risk averse, there is great opportunity to leverage automation to both make the world a safer place and maximize the benefit of our processes to the world. The key to achieving this will be a conscious posture shift toward risk management. Functional safety is an excellent step in this direction, and when diligently applied, can help control engineers and their communities sleep well at night.

Erik Reynolds, CFSE, PMP, *is a consultant at Intertek, a CFE Media content partner. Edited by Mark T. Hoske, content manager,* Control Engineering, *mhoske@cfemedia.com.*

Using a PHA for process valve safety

A detailed process hazard analysis (PHA) has to examine the human factors involved and identify, evaluate, and control potential hazards to prevent future process valve incidents from occurring.

On Nov. 22, 2016, an operator was working on a valve assembly at the ExxonMobil Refinery in Baton Rouge, La, when isobutane released. The resulting fire seriously injured four workers in the sulfuric acid alkylation unit.

There is always a technical reason for a failure, but anyone doing an analysis has to examine the human factors involved. A detailed process hazard analysis (PHA) on covered processes that identify, evaluate, and control potential hazards to prevent future incidents from occurring.

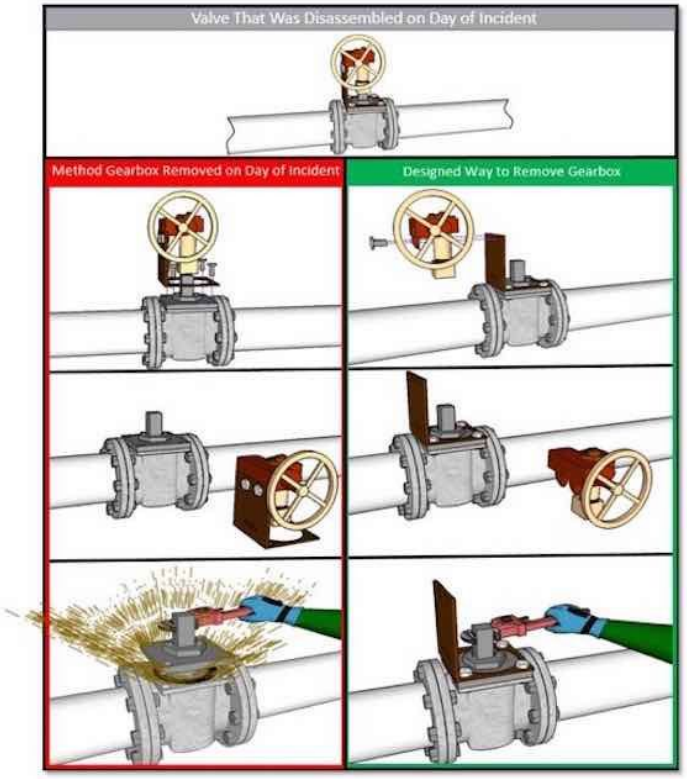
"You have to look at how you are handling human factors surrounding valve operation," said Mike Wingard, investigator at the Chemical Safety Board (CSB) during his presentation at the Mary Kay O'Connor Safety Center 2017 International Symposium, in College Station, Tex. "The valve design, the way the support bracket was set up, gave a false sense of security."

After the analysis incident and the CSB report, anyone could look at the incident and say why would anyone do this? But after you get into the details, it is possible to understand how and why the incident happened, Wingard said.

"There were four serious burn injuries, but it could have been worse," Wingard said.The plug valve in question is an open and close device that is manually controlled.

In this case, the operator took the entire valve handle assembly off. The proper way would have been to leave the assembly stem on and keep the four bolts in place. Instead, however, he took out all four bolts that tied the valve into the pipe.

The CSB learned there were long-standing reliability issues with gearboxes used to operate plug valves in the refinery's alkylation unit. When alkylation unit operators encountered a malfunctioning gearbox on a plug valve, it was an accepted practice for the operator to remove the gearbox to open or close the valve with a pipe wrench. Refinery management did not, however, provide alkylation unit workers performing this operations activity with a written procedure or training on safe gearbox removal from plug valves and its associated hazards.



Example showing how the alkylation unit plug valve with gearbox was removed and how it should have been removed. Image courtesy: ISSSource/ Chemical Safety Board (CSB)

While some operators felt comfortable performing this type of work, others did not and referred this work to maintenance personnel, who they felt were more qualified to remove the gearbox.

The Occupational Safety and Health Administration (OSHA) process safety management (PSM) standard requires companies to perform a detailed PHA.

In addition, the American Petroleum Institute (API) published a human factors tool that asks:

→ Is there any equipment that often does not work as designed?
→ How could human error cause an incident or unsafe condition?
→ Are routine duties well-defined?
→ Are the job aids adequate (including training)?

In its alkylation unit process hazard analysis (PHA), the Baton Rouge refinery did not document any consideration of human factors related to valve operational issues. Had the PHA human factors analysis prompted workers to discuss the removal of these gearboxes, the company could have identified the potential hazard of inadvertently taking the valve apart during gearbox removal.

Refinery operators said they frequently encountered situations where the handwheel did not turn the valve, Wingard said. Given the history of issues with these alkylation unit gearboxes, the refinery should have evaluated these operational difficulties, recognizing that this older valve design could result in unintentional disassembly of pressure-retaining components, which, as seen, can have catastrophic consequences.

"There was a lack of procedure," Wingard said. "There was no procedure detailing how to deal with different gearbox designs. There was no procedure on when to call maintenance. The operator had a choice to do it yourself or to call maintenance."

Gregory Hale *is the editor and founder of Industrial Safety and Security Source (ISSSource.com), a news and information Website covering safety and security issues in the manufacturing automation sector. This content originally appeared on ISSSource.com. ISSSource is a CFE Media content partner.*

Honeywell

THE POWER OF **CONNECTED**

Personal Gas Safety

Remote monitoring of the safety of lone workers

When can the process control system, safety system share field devices?

An SIS and BPCS can sometimes share components, but not without careful analysis.

Can a safety instrumented system (SIS) and a basic process control system (BPCS) share field devices? It could certainly save money; consider that a large cryogenic valve for an LNG plant can easily cost $500,000. But how can the SIS and BPCS share valves or other components and still comply with standards? This article will examine the relevant standards and show how it can be done—and how it shouldn't.

Applicable standards

SISs are generally designed to meet IEC 61511 in order to comply with the requirements of national regulations (ISA 84.00.01 is the U.S. version of IEC 61511). This standard states that it is permissible to share devices between safety and basic process control systems but also sets certain requirements for when sharing devices is and is not allowed. Those requirements are often misunderstood and frequently ignored. Ultimately the object is to avoid a single point of failure, a situation in which failure of a single device can cause the process to go out of control, creating a demand on the safety system, yet also simultaneously defeats the shut-down system by preventing it from responding properly.

To share field devices successfully, it is vital to understand the process under control—not just the safety equipment or the electronics, but the chemical processes that are being controlled. One must understand the process and how the devices are used, and understand how they fail and what will happen if they fail.

When can the process control system, safety system share field devices?

Consider the note to paragraph 8.2.1 of IEC 61511 relative to sharing devices:

"In determining safety integrity requirements, account will need to be taken of the effects of common cause between systems that create demands and the protection systems that are designed to respond to those demands."

This is not a normative requirement but states that careful thought is required before sharing components between the BPCS and the SIS to ensure that the overall risk is within allowable limits. In addition, paragraph 11.2.10 and its attached note offer more advice:

"A device used to perform part of a safety instrumented function shall not be used for basic process control purposes, where a failure of that device results in a failure of the basic process control function which causes a demand on the safety instrumented function, unless an analysis has been carried out to confirm that the overall risk is acceptable."

"NOTE: When a part of the SIS is also used for control purposes and a dangerous failure of the common equipment would cause a demand for the function performed by the SIS, then a new risk is introduced. The additional risk is dependent on the dangerous failure rate of the shared component because if the shared component fails, a demand will be created immediately to which the SIS may not be capable of responding. For that reason, additional analysis will be necessary in these cases to ensure that the dangerous failure rate of the shared equipment is sufficiently low. Sensors and valves are examples where sharing of equipment with the BPCS is often considered."

This means that one should not use a device in a safety instrumented function (SIF, essentially a control loop for safety purposes) if a failure of that device will cause a BPCS loop to place

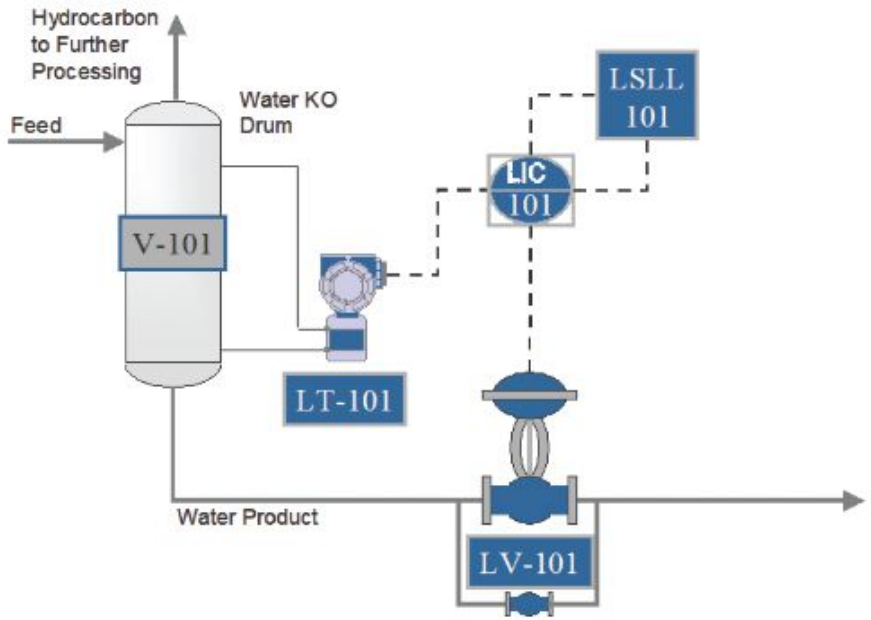


Figure 1: *The "ultimate" in sharing. Function block LSLL-101, the level limit, is supposed to provide the safety function, but failure of the level transmitter or control valve will constitute a single point of failure.*

a demand on the SIS and simultaneously cause that SIF to fail to a dangerous state. This clause is the origin of the requirement for preventing a single point of failure.

The 11.2.10 Note says that having a single point of failure is permissible as long as the frequency of such a failure is acceptably low. This requires a detailed quantitative analysis—a laborious process that many people do not do well, and often ignore. However, in most situations the mathematical analysis will reveal that sharing is not possible.

The FMEA process

Sharing will require a FMEA (failure modes and effects analysis) of the equipment to be shared. This means that for any shared equipment—a transmitter, a valve, or even an entire control loop—one must determine all of the different ways that each of the shared components can fail, and whether any failure mode constitutes a single point of failure. And while

the standard does not explicitly require it, we strongly recommend that the study be formally documented and verified.

The FMEA process begins with making a list of each item to be shared for a given loop or function. All the failure modes for each item should be listed, and for each failure mode the effect of the failure must be described. If a primary failure disables a safeguard, then that constitutes a single point of failure. The single points of failure must then be eliminated with a redesign or a quantitative analysis that demonstrates that the frequency of failure is low enough to be allowed should be performed.

Too much sharing

Figure 1 shows an example with a considerable amount of sharing. The process is a water knockout drum; the interface between hydrocarbon and water is monitored by level transmitter LT-101, which provides the process measurement to controller function block LIC-101 in the control system that adjusts the level control valve, LV-101, to hold the water level in the drum to the setpoint. Function block LSLL-101, the low-level limit, is providing the safety function in this example. Possible

Table 1: *Possible failure modes and consequences*

Table 1: Possible failure modes and consequences

Device	Failure mode	Effect	Safeguards	Notes
LT-101	Fail upscale	Controller output goes to zero, valve fully open	Overfill interlock - failed	Single point of failure
	Fail downscale	Controller output goes to max, valve fully closed	No shared interlock	
	Fail in place	Controller output goes fully open if setpoint is changed to a lower value.	Overfill interlock - failed	Single point of failure
LC-101	Fail upscale	Controller output goes to max, valve fully closed	No shared interlock	
	Fail downscale	Controller output goes to zero, valve fully open	Overfill interlock - failed	Single point of failure

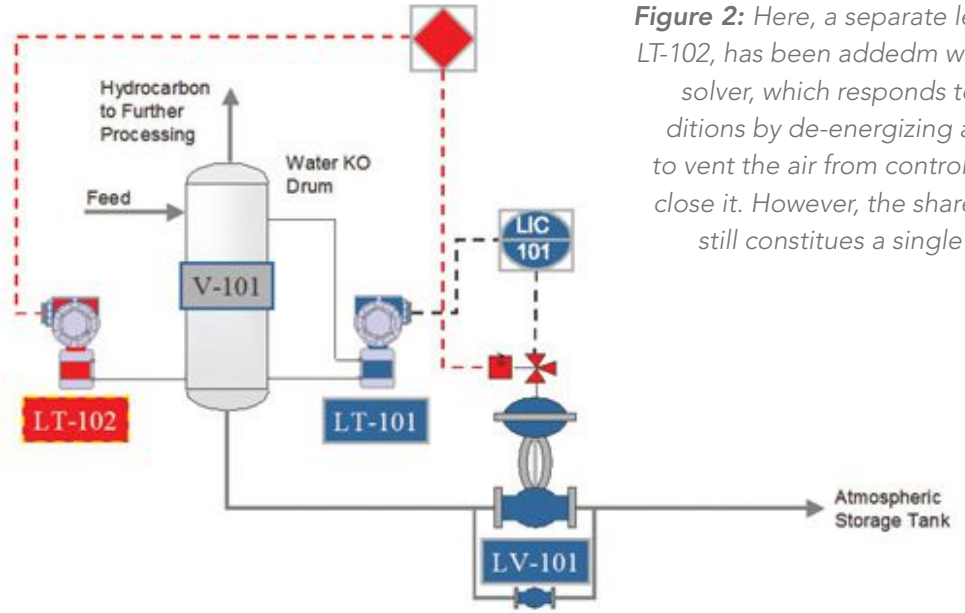


Figure 2: *Here, a separate level transmitter, LT-102, has been addedm with its own logic solver, which responds to low-level conditions by de-energizing a solenoid valve to vent the air from control valve LV-101 to close it. However, the shared control valve still constitues a single point of failure.*

failure modes and their consequences are tabulated in Table 1.

This example has been simplified and highlights only two shared components. In reality the DCS input card, the DCS CPU, the DCS output card, and the level valve are all shared and should be included in the failure analysis.

This arrangement clearly cannot be used, but what would happen if the safety function were separated out, at least in part? In Figure 2, a separate level transmitter, LT-102, has been added. This provides a level measurement signal to its own logic solver, which responds to low-level conditions by de-energizing a solenoid valve to vent the air from control valve, LV-101, causing it to close. In this scenario, the only shared component is the control valve. The failure mode analysis is tabulated in Table 2.

Once again, sharing of just the control valve provides insufficient protection.

Figure 3 shows the situation with an additional, separate shut-off valve. The analysis in this case is simple: there can be no single point of failure because there are no shared components.

Table 2: Better, but still not good enough

Device	Failure mode	Effect	Safeguards	Notes
LV-101	Fail open	Valve fully open	Overfill interlock - failed	Single point of failure
	Fail closed	Valve closed	No shared interlock	
	Fail in place	Pathway open to completely drain vessel if input rate drops	Overfill interlock - failed	Single point of failure
	Bypass open	Pathway open to completely drain vessel	Overfill interlock - failed	Single point of failure

Table 2: *Better, but still not good enough*

Sharing that works

For an example of a situation in which it permissible to share some components, consider a hydrocracker or a heavy oil hydrotreater. In these process units there will be a feed pump going from a low feed-system pressure, perhaps 100 psig, up to a very high reactor pressure of 1,000 to 2,000 psig. There is a shutdown system, illustrated in Figure 4, intended to detect that forward flow has been lost because of a pump failure.

The shutdown system will then close a shutoff valve to prevent the high-pressure reactor system from flowing backwards through the feed pump into the low-pressure feed system, potentially causing a pressure-relieving scenario. Upon pump failure, the flow controller on the discharge of the pump will respond to the low-flow condition by opening the control valve to try to increase the flow rate since the measured flow (zero) is below the feed flow setpoint. Therefore, a solenoid valve controlled by the shutdown system is provided on the

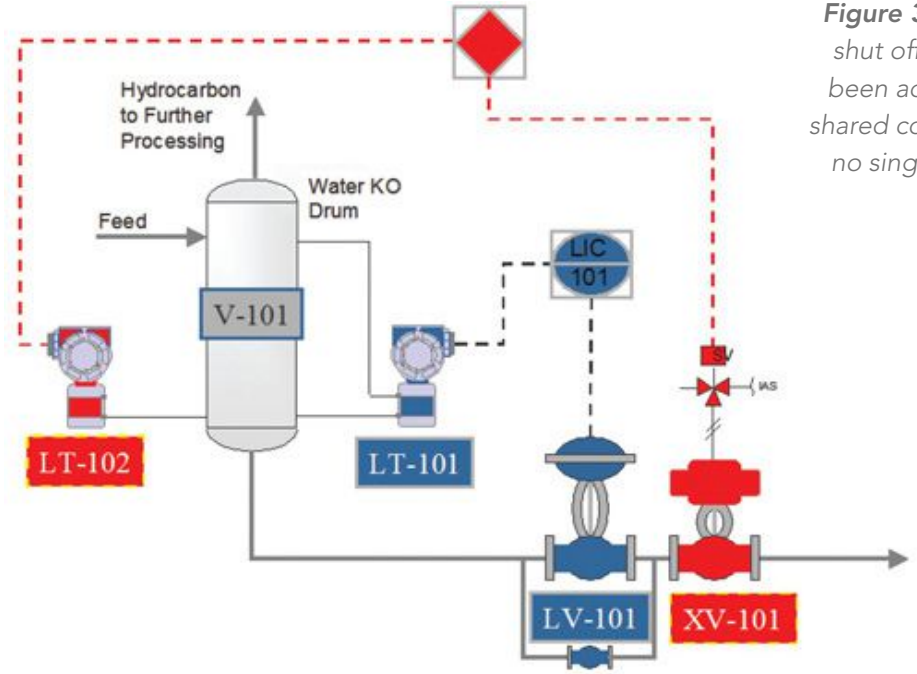


Figure 3: *Here, a separate shut off valve, XV-101, has been added. There are no shared compnents and thus no single points of failure.*

flow-control valve. If forward flow is lost, the shutdown system will de-energize the solenoid valve to close the control valve.

In this case, sharing the control valve is permissible because it does not constitute a single point of failure that both creates a demand and causes the protective function to fail dangerously. Failure of the flow controller cannot cause a reverse flow. The only thing that causes a reverse flow is pump failure. If the valve gets stuck in any position—in place, open, or closed—it will not cause a reverse flow if the pump continues to operate. The shutdown action is independent of the cause of the hazardous situation, so sharing the valve for both the safety purpose and the shutdown purpose is permissible. A separate shutdown valve is often provided to provide redundancy should the flow-control valve fail to close when the solenoid valve is de-energized, either due to a failure of the solenoid valve or if the control

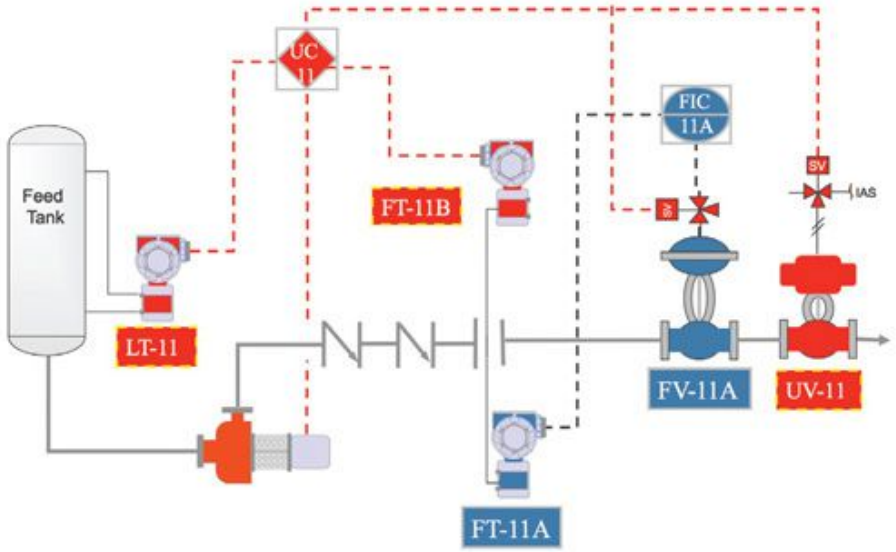


Figure 4: *This figure illustrates where sharing of the flow control valve is acceptable since it does not cause a single point of failure that creates the demand and causes the protective function to fail dangerously.*

valve is stuck.

We have not covered cases where a single point of failure is permitted. This requires a detailed mathematical analysis of the frequency of possible failures, an analysis that may be more costly than purchasing separate equipment.

In summary, IEC 61511 allows sharing of field equipment between the SIS and BPCS, but it has requirements that, if properly implemented, will prevent sharing in an unsafe manner. One of those requirements is a fairly complex analysis of the shared components, which is often misunderstood or done improperly. And finally, a documented and verified FMEA of all shared components should be performed.

Marszal *is president of Kenexis Consulting Corporation. Hawkins is global refining business consultant for Emerson Process Management.*

Plant & Personnel Safety

Thank you for visiting the Plant & Personnel Safety eBook!

If you have any questions or feedback about the contents in this eBook, please contact CFE Media at *customerservice@cfemedia.com*

We would love to hear from you!

Sponsored by

Honeywell

THE POWER OF **CONNECTED**