Selecting Sensors for Safety Instrumented Systems

Chad McGuire
Jessica Lo
Erik Mathiason
Emerson Process Management

A plant's safety instrumented system (SIS) is critical in preventing process safety incidents. Use this guide to help choose the proper sensors for your plant's SIS.

For plants in the chemical process industries (CPI), the safety instrumented system (SIS) is designed to be the last, and arguably most critical, layer of protection. Although the process control system's purpose is to keep the plant running and optimize profits, the SIS's job is to keep the process, the plant, and the company's reputation safe. The control system runs the plant to maximize profitability, whereas the SIS interrupts the control system if and when it is necessary to do so. To prevent a potentially catastrophic incident (and to keep that facility from becoming the headline of tomorrow's newspaper), the SIS will shut down the plant under certain conditions. The process control system and the SIS are two independent systems that should not share any common components. Unfortunately, this is not always the case in the real world, as the standards for safety instrumented systems can be open to interpretation.

Why do we need safety instrumented systems?

A SIS helps prevent serious and potentially deadly disasters. Three examples (Figure 1) demonstrate past incidents that have occurred due to a failure in the SIS. The first, and most well-known, is considered the world's worst industrial disaster. In 1984, a major gas release at a pesticide plant in Bhopal, India, exposed hundreds of thousands of people to methyl isocyanate and other chemicals.

The two other disasters occurred more recently. A hydrocarbon vapor cloud explosion occurred at a North American refinery in 2005, killing 15 workers and injuring an additional 170. In the third incident, several explosions at an oil storage depot in Europe injured more than 40 people; fortunately, there were no fatalities.

Each of these incidents portrays the inherent risks and potentially disastrous consequences associated with operations in the CPI. Implementing safety instrumented systems is all about reducing this risk.

Risk of what?

When it comes to designing systems to reduce risk, what risks are we talking about? In the design of SISs, risks are typically grouped into three major categories: risks to personnel, risks to the environment, and financial risks. The most talked-about risk associated with safety is the risk of personnel fatalities or injuries. However, other risks must also be considered. For example, it is important to account

Bhopal, India, disaster
and gas leak (1984)
Final death toll: over 15,000

Refinery explosion after
hydrocarbon vapors ignited (2005)
Deaths: 15, Injuries: 170

Buncefield, U.K., oil storage
terminal explosion and fire (2005)
Over 40 people injured

Figure 1. Implement a SIS to reduce the risk of a process safety incident. These three images are examples of the catastrophic events that have resulted after a failure in the SIS.

for incidents that could be catastrophic to the environment, or that expose the plant to permit violations or fines from government regulators, such as the U.S. Occupational Safety and Health Administration (OSHA). Companies also face many financial risks, including damage to equipment, business interruption, loss of company image, lost value for shareholders, and lost market share.

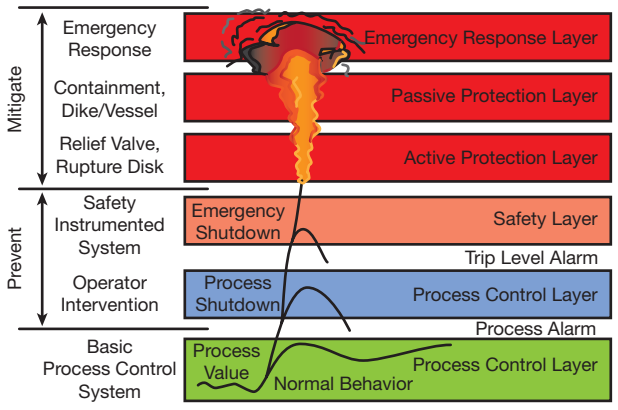
Along with facility operators, insurance companies and government agencies also strive to reduce risk.

Layers of protection

The SIS is designed to be the last layer of prevention against a safety incident. Consider a typical reactor. Given the right conditions in the vessel, a reaction could reach an unsafe state. Without layers of protection, prevention, and mitigation, the reactor could explode and cause significant damage. Figure 2 demonstrates the layers of protection to prevent and mitigate such an incident and where a SIS fits in.

The most basic layer — the process control system — keeps the operation running under normal conditions by controlling process variables. If the reaction were to move beyond safe operating conditions, the first prevention layer — operator intervention — would be activated. For example, an audible alarm might sound to alert the operator to manually shut a valve to stop the reaction. In case that does not work, the next prevention layer — the SIS — is in place to bring the measured variable under control before a catastrophic event, such as a tank explosion, occurs.

Mitigation layers are in place to reduce the damage caused by the event if both prevention layers were to fail. The first mitigation layer is often a relief valve designed to open before the tank ruptures. The next layer might be some type of additional containment device, such as a dike or vessel, designed to capture any material that escapes primary containment. If that fails or if a vapor is released into the atmosphere, the final mitigation layer — plant emergency response — would be implemented to ensure that the vapor does not cause further damage and to minimize contamination to the environment.



▲ **Figure 2.** Processes are protected by layers of protection that are designed to prevent or mitigate a catastrophic event. The SIS is the last prevention layer before mitigation actions are needed.

Components of a SIS

The CPI use IEC 61511, "Functional Safety — Safety Instrumented Systems for the Process Industry Sector," as the standard for the design, implementation, and operation of safety instrumented systems.

Multiple safety instrumented functions (SIFs) make up the SIS. Each SIF consists of three components: a logic solver, a final control element, and a sensor. These components are very similar to those in a distributed control system (DCS).

The logic solver is similar to a proportional-integral-derivative (PID) controller. The logic solver is programmed to perform a specific function that will return the process to its safe state in order to avert a dangerous condition. The final control element, commonly a valve, is designed to perform the action being driven by the logic solver. The third component, which is the focus of this article, is the sensor (also called a transmitter in a DCS). The sensor provides the logic solver with the information it requires to determine whether the SIF should be activated to move the process to a safe state.

Choosing the right sensor

Selecting the correct sensor for your application typically involves the following steps, which are detailed in the remainder of this article:

1. Determine the risk reduction factor for your process.
2. Determine the required safety integrity level (SIL) and probability of failure on demand (PFD) range.
3. Decide whether you will use a sensor that is IEC 61508 certified or a prior-use sensor.
4. Evaluate the sensor's failure rates, safe failure fraction, systematic capability, and random capability to ensure they comply with the required SIL.
5. Choose a mean repair time, mission time, and proof test interval, and calculate the PFD of the sensor.
6. Ensure that the PFD for the entire SIF falls within the PFD range established in Step 2.
7. Install the sensor and the remainder of the SIF.

1. Determine the risk reduction factor

Before you can choose the optimal sensor for your SIF, you must understand the level of risk reduction needed in your SIS to meet requirements set by the facility, company, and/or government.

The first step is to perform a process hazard analysis (PHA), such as a hazard and operability (HAZOP) analysis,

to determine the likelihood of a specific event occurring.

For example, a facility performs a hazard analysis and determines that the risk of a valve not closing is one event every year. However, the facility has selected an acceptable failure rate for this event of no more than once every 5,000 years. Therefore, it needs to reduce the risk of such a failure from 1.0/yr to 0.002/yr, which is represented as a risk reduction factor of 5,000.

2. Determine the required SIL and device PFD

Table 1, which is based on IEC 61511, shows how to translate the risk reduction factor into the SIF's required safety integrity level. For instance, if your risk reduction requirement is between 10 and 100, you need to design the SIF to a safety integrity level of 1, or SIL-1. If, as in the example, your risk reduction requirement is between 1,000 and 10,000, you need a SIL-3 SIF.

Table 1 also provides the range for the probability of failure on demand required for each safety integrity level. PFD is the chance that a device will be in failure mode when it is needed to return the process to a safe state.

Figure 3 illustrates the concept of probability of failure on demand. The orange bars on the top line represent events that require a process shutdown because some process variable is out of control. Over time, there will likely be multiple such events. In parallel to plant operations, the SIF sensor is running in the background. Each of the orange events requires the SIS to act and bring the plant to its safe state. However, there will be times when the sensor is in failure mode or is not operating as intended, which are represented by the red bars. The sensor's PFD is the chance of an event requiring a shutdown and a sensor failure happening simultaneously. The odds of this occurring are generally very small, but must be taken into account.

The PFD of the SIF is the sum of the PFD values of all of the components in the SIF (*i.e.,* logic solver, final control element, and sensor). Therefore, to design a SIF for a target SIL, you need to determine the PFD of each component in the SIF (as discussed later) and choose components whose overall PFD is within the range given in Table 1.

The facility in the example needs to reduce its risk by a factor of 5,000, which means it needs to design its system to a safety integrity level of 3 (SIL-3). According to Table 1, the target PFD range is 10^{-4} to 10^{-3}, and the aggregate PFD of all the SIF's components must not exceed 10^{-3}.

3. Pick a certified or prior-use sensor

IEC 61511 specifies that a sensor can be deemed safe for use in a SIS in two ways. The sensor must be either:

• compliant with IEC 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems"

• proven to work in a similar application with a good track record.

A sensor that is compliant with IEC 61508 has been certified by an accredited third-party rating agency (*e.g., exida* or TÜV) to meet stringent design and manufacturing requirements. Process instrumentation manufacturers closely follow this IEC standard to ensure that their products become certified for use in safety instrumented systems.

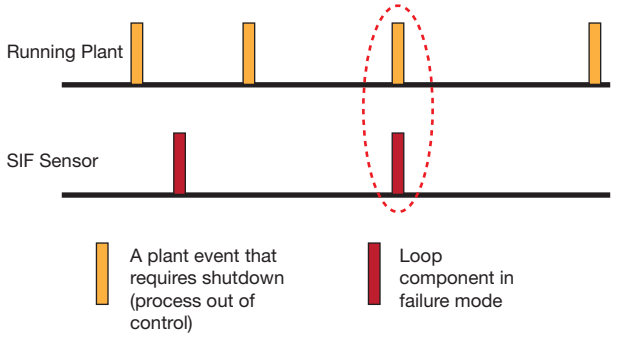
You may also choose a sensor that has not been IEC 61508 certified if it has a proven track record in a similar application. This is commonly referred to as a prior-use sensor. Proving that the sensor has been used in a similar application with a good track record requires rigorous monitoring and significant amounts of paperwork to record and track the sensor's failure data.

A prior-use sensor is an attractive option, because it is based on failure data recorded by the user. However, many facilities do not have a proper system to track failures and create the documentation needed to adhere to IEC 61511 standards. Prior-use is not an option for devices new to the market.

To demonstrate IEC 61508 compliance, manufacturers may engage a third party to perform a failure modes, effects, and diagnostic analysis of its sensors. An accredited third party offers expertise in this process, as well as an objective perspective. In this analysis, every possible error that can occur is evaluated, and the potential impact of each error on the safety function (*i.e.,* the analog output) is assessed.

Table 1. Use the calculated risk reduction factor to determine the required SIL for the SIF.

Risk Reduction Factor	Safety Integrity Level	Probability of Failure on Demand
100,000 to 10,000	SIL-4	10^{-5} to 10^{-4}
10,000 to 1,000	SIL-3	10^{-4} to 10^{-3}
1,000 to 100	SIL-2	10^{-3} to 10^{-2}
100 to 10	SIL-1	10^{-2} to 10^{-1}



▲ **Figure 3.** Probability of failure on demand (PFD) is the chance that a component failure in the SIS and an event requiring a safety shutdown occur simultaneously.

Article continues on next page

The failure modes analysis considers issues down to the component level. For instance, what happens if a particular capacitor on the sensor's board fails? What effect does this have on the sensor's output?

Another area examined with respect to failure rates is diagnostics that run automatically within the sensor during operation. Can a particular diagnostic detect certain failures? For example, if the sensor module fails, will the device output be driven to a specified state — either high or low — upon internal detection of a failure? Credit is given to the device if it is able to internally detect certain failure issues.

The failure modes analysis report includes all of the relevant safety data for the sensor, and describes the procedures to test it. These test procedures are used to verify that the sensor is functioning as expected and is in a like-new state. More importantly, successful testing provides additional assurance that the sensor is ready to perform, if needed, for a shutdown.

4. Evaluate the failure data

What sorts of failure-rate data are typically provided in a failure modes analysis report for a certified sensor? What data need to be monitored and recorded to justify implementation of a prior-use sensor? The answer: the sensor's failures in time (FITs) and safe failure fraction (SFF).

A failure in time is equivalent to one failure per billion operating hours. Four types of FITs are used to calculate SFF: safe detected, safe undetected, dangerous detected, and dangerous undetected. These standard terms may be more easily understood if you think of them as "safe and detectable," "safe even if undetected," "dangerous but detectable," and "dangerous and undetected." Figure 4 illustrates these different types of failures for an automobile tire.

Safe detected (λ_{SD}) refers to a failure that the sensor can detect and react to appropriately. For example, a tire pressure sensor in a vehicle detects low pressure in the tire due to cold temperatures, and alerts the driver. These failures are considered safe because they do not cause an on-scale failure. An on-scale failure occurs when the device is in a failure mode but the output of the sensor is still within 4–20 mA.

Safe undetected (λ_{SU}) failures are those that the sensor cannot detect, and therefore do not trigger an alarm to notify the user of failure. However, the failure does not cause a hazardous scenario. For example, a rock embedded in a vehicle's tire may cause a small change in tire pressure, but it does not damage the tire. This pressure change is not detected, but it does not impact the safety of the tire.

A dangerous detected (λ_{DD}) failure is an on-scale failure that the sensor's internal diagnostics can detect. Because the sensor can detect the failure, it will trigger an alarm. For example, if the driver runs over a nail, the tire pressure gage will detect that the tire pressure is dangerously low and send an alert to the driver.

A dangerous undetected (λ_{DU}) failure is an on-scale failure that cannot be detected by the sensor's internal diagnostics. It can only be detected by testing the sensor. In the tire example, a dangerous undetected failure might occur if the driver runs over a nail and the tire is ready to blow, but the driver is not aware of this fact. Without a tire pressure sensor, it would be difficult for you to detect the dangerous state of an impending blowout while you are driving.

▲ **Figure 4.** Four types of failures are used to calculate the safe failure fraction. In a safe detected failure, a tire pressure sensor detects low pressure due to cold temperatures and alerts the driver. In a dangerous detected failure, a tire pressure sensor detects low pressure due to a screw puncture in the tire and alerts the driver of this dangerous condition. In a safe undetected failure, a rock embedded in a sensorless tire may cause a shift in pressure, but does not pose a hazard to the driver. In a dangerous undetected failure, a sensorless tire is flat and may cause the driver to lose control.

The device's safe failure fraction describes the ratio at which a device experiences safe or detected failures, and is calculated by:

$$SFF = (\lambda_{SD} + \lambda_{SU} + \lambda_{DD}) / (\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU})$$

The SFF is used to evaluate whether or not a sensor will be safe enough for a specific SIS. Often, the SFF is given as a percentage. A SFF of 85% means that 85 out of 100 failures are safe or detected.

Systematic capability. The failure analysis report for a certified sensor also includes information on the manufacturer's systematic capability. If you are choosing a sensor for your SIF that is compliant with IEC 61508 (rather than a prior-use sensor), you must ensure that the manufacturer has a systematic capability for your required SIL level.

Systematic capability describes a manufacturer's

capability to produce a sensor that can be used up to and including the SIL noted on the certificate. The certifying organization evaluates all functional groups involved with design, development, manufacturing, and procurement to ensure that each of these areas meets the requirements to manufacture equipment that has a SIL rating. For instance, design and manufacturing personnel must be competent and trained on the processes and procedures that are required to comply with IEC 61508, and documentation must show that the product development and manufacturing procedures are robust.

IEC 61508 lists requirements that need to be followed for sensor design to allow their use at various SILs. The standard recommends the level of safety, or capability, for which the device can be used, based on the level of requirements met: SIL-1 is the easiest to achieve, and SIL-4 is the most challenging.

Ensuring that the manufacturer is able to achieve the requirements for systematic capability means that the manufacturer has supplied proof that the integrity of its software and hardware meet the requirements of the specified safety integrity level. Systematic capability information tells you the highest SIL for which a device can be used. Therefore, SIL-3 systematic capability indicates that the equipment can be used in applications up to and including SIL-3. In other words, a SIL-3 capable sensor can be used in a SIL-1, SIL-2, or SIL-3 application.

Redundancy and random capability. Occasionally, a sensor will be certified for a certain safety integrity level only if an extra, or redundant, sensor is implemented in the SIF. A sensor's random capability is a listing of its redundancy requirements for specific SILs. Information on the sensor's random capability is typically noted on the certificate of compliance to IEC 61508.

The random capability of a sensor for a specific SIL is determined using architectural constraint tables found in IEC 61508-2, such as the one shown in Figure 5. Find the SFF that is stated on the IEC 61508 certificate on the left of the table and the target SIL in that row, then read the corresponding hardware fault tolerance (HFT) at the top of that column to determine the number of redundant devices required.

Figure 5 demonstrates this concept for a common pressure transmitter. The sensor has a SFF of 91%, which falls into the range of the third row in the table. The HFT for this component for SIL-2 is 0, which means that a SIL-2 application requires no redundant sensors — just one sensor is sufficient. This is abbreviated as SIL 2 @ HFT = 0. You have the option to install just one sensor in your SIF.

Likewise, the HFT for a SIL-3 application is 1. This means that SIL-3 requires one redundant sensor, or two sensors total. This is denoted as SIL 3 @ HFT = 1. To achieve SIL-3, the SIF needs two sensors.

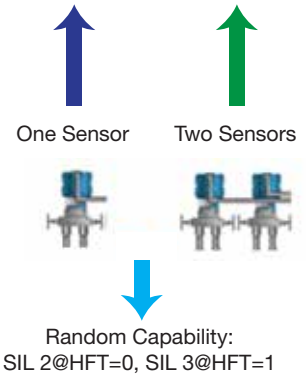
Depending on the criticality of the application or the other devices in the SIS, you might opt to install additional sensors beyond what is required for your SIL, which can improve system availability. In the SIL 3 @ HFT = 1 example, if one of the two devices fails, the process will shut down. However, if the system has an additional redundant sensor and one device fails, the process can continue to operate while the failed device is repaired or replaced.

5. Calculate the PFD of the sensor

Methods for calculating the PFD can be found in IEC 61508-6 or the International Society of Automation's equivalent standard, ISA 84. To calculate the PFD, you need to select a mean repair time, mission time, and proof test interval for the sensor based on the sensor's failure rate. Manufacturers of sensors that comply with IEC 61508 provide the failure rates for their devices; for prior-use sensors, the PFD value can be calculated based on documented failure rates.

The mean repair time is the amount of time that passes between the failure of a sensor in the SIF and the completed repair. The mission time is the length of time a particular SIF is installed and functioning. Because the PFD tends to increase over time, you should perform periodic proof tests to verify that the sensor is functioning in a like-new

Architectural Constraint Table for Type B Devices			
Safe Failure Fraction	**Hardware Fault Tolerance**		
	0	1	2
<60%	Not Allowed	SIL-1	SIL-2
60% to <90%	SIL-1	SIL-2	SIL-3
90% to <99%	SIL-2	SIL-3	SIL-4
≥ 99%	SIL-3	SIL-4	SIL-4



▲ **Figure 5.** Combining the safe failure fraction with the SIL allows you to determine the number of redundant transmitters required for the system. In this example, the sensor has a SFF of 91%, so it will require one redundant sensor for a safety integrity level of 3.

Table 2. A proof test consists of a series of steps to ensure that the device is operating properly. This is an example of a comprehensive proof test used for a common pressure sensor.

Step	Action
1	Bypass the safety function and take appropriate action to avoid a false trip.
2	Use HART communications to retrieve any diagnostics and take appropriate action.
3	Send a HART command to the transmitter to go to the high-alarm current output and verify that the analog current reaches that value.
4	Send a HART command to the transmitter to go to the low-alarm current output and verify that the analog current reaches that value.
5	Inspect the transmitter for any leaks, visible damage, or contamination.
6	Perform a two-point calibration of the transmitter over the full working range.
7	Remove the bypass and otherwise restore normal operation.

state. The sensor's safety manual or failure analysis report provides information regarding the steps that should be performed during the proof tests. Proof testing reduces the PFD. The proof test interval (the amount of time between proof tests) can be adjusted to help meet the target PFD.

The safety manual provides proof-test-coverage (PTC) data for both partial proof tests and comprehensive proof tests. The PTC is the percentage of dangerous undetected failures that are detected during that particular proof test.

A partial proof test is performed on a sensor that is installed in the process (an *in situ* sensor). A partial proof test typically does not require the user to actually activate the sensor — for example, to apply pressure to a pressure transmitter. In a comprehensive proof test, the sensor is activated to ensure that its mechanical components are functioning properly. Table 2 outlines the steps recommended for a comprehensive proof test of a typical pressure sensor, and Table 3 outlines the steps recommended for a partial proof test.

Figure 6 shows the relationship between partial and comprehensive proof tests. To truly validate that the sensor is functioning like new and to maintain a lower PFD, a comprehensive proof test may be required. The partial proof test provides a method to maintain a PFD through simpler proof testing. Combining partial proof tests and comprehensive proof tests reduces the maintenance complexity and helps

Table 3. This is an example of a partial proof test used for a common pressure sensor.

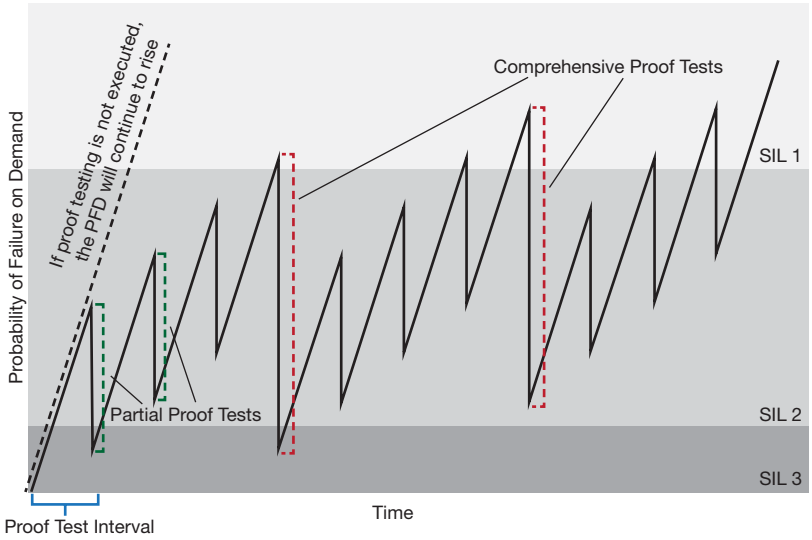
Step	Action
1	On HART host or communicator, enter the current value (in mA) representing a high-alarm state.
2	Use a reference meter to verify the mA output corresponds to the entered value.
3	Enter the current value (in mA) representing the low-alarm state.
4	Use the reference meter to verify the mA output corresponds to the entered value.
5	Document the test results per requirements.

to maintain the PFD required for a specific SIL.

Proof test coverage is a ratio, and it is not perfect. As dangerous undetected failures decrease, which typically occurs as new product designs develop an operating history, the PTC also tends to decrease. Lower proof test coverage is the result of the reduction in dangerous failures.

To understand the implications of this, it is important to realize that a perfect proof test is unlikely, and that one failure will remain undetected.

Table 4 describes two example sensors. The first design had nine dangerous undetected (DU) FITs. If we assume that proof testing is imperfect, and one FIT will remain undetected, the best PTC this proof test can achieve is 90%. The second sensor has an improved design with only four DUs. Assuming that one DU FIT will not be detected, *i.e.,* four of the five DUs can be tested, the best PTC a proof test can achieve would be 80%.



▲ **Figure 6.** A sensor's probability of failure on demand (PFD) increases over time. Proof testing a component helps to reduce the PFD and ensures that the SIF meets the required SIL.

Let's now look at how the calculation of PFD based on these factors is used in sensor selection. For example, imagine you must choose between the two sensors in Table 5, which have different numbers of dangerous undetected failures and different proof test coverages:

• a common sensor with a comprehensive proof test coverage of 95% and 34 dangerous undetected FITs

• a more-advanced sensor with a comprehensive PTC of 90% and 17 dangerous undetected FITs.

Assume the mean repair time, mission time, and proof test interval are equal for both sensors. Even though the first sensor has higher PTC, the second sensor has a lower PFD value, and would therefore be a better choice.

6. Ensure that the PFD for the entire SIF falls within the correct PFD range

Now that you have chosen a sensor for the SIF, you need to select the remaining components of the SIF in a similar way. Next, add the PFDs of the individual components to determine the PFD for the overall SIF. Then, verify that the overall PFD falls within the PFD range that was mandated by Table 1 in Step 2.

If the overall PFD does not fall within this range for the required SIL, then a different sensor must be chosen. Alternatively, you could add a redundant sensor or choose a shorter proof test interval to help reduce the sensor's contribution to the overall PFD.

Table 4. A sensor with a smaller number of dangerous undetected failures may have lower proof test coverage because of the ratio nature of the PTC.

	First Sensor	Second Sensor
Dangerous Undetected (DUs) FITs	9	4
Assume 1 DU will not be detected	1	1
Total DUs	10	5
Proof Test Coverage	90%	80%

Table 5. In this case, because the sensor with the lower PTC also has a lower PFD value, it would be a better choice to meet a higher SIL.

	Sensor 1	Sensor 2
PTC	**95%**	**90%**
λ_{DD} FITs	340	340
λ_{DU} FITs	34	17
RT	24 hr	24 hr
Lifetime	20 yr	20 yr
Test Interval	2 yr	2 yr
PFD	4.40×10^{-4}	2.92×10^{-4}

7. Install, validate, and maintain the sensors

When installing a sensor in a SIF, follow the instructions provided in the instrument's safety manual. Manufacturers are required to supply a safety manual for all certified devices. The manual provides the information you need to put the device into operation and meet any safety requirements.

Once the components in a SIF have been installed, perform a validation test for the entire loop. This validation should simulate the steps that a SIF would perform in the event of a safety incident, and should ensure that the process is able to reach a safe state, therefore ensuring compliance.

Finally, the IEC 61511 standard requires that SIFs be maintained properly to ensure that each component is available when it is needed. The frequency and type of maintenance performed is driven by the required PFD.

In closing

Safety instrumented systems are designed to prevent your facility from experiencing a major process safety incident. The design of a SIS is a very complex process that should be done in accordance with industry standards to ensure the facility's safe operation. This critical component is often the last barrier between a safe operation and a catastrophic event. Failure rates, proof tests, and maintenance frequency are key factors in achieving specified safety integrity levels.

Thus, instrumentation must be carefully chosen and evaluated to verify that the safety function meets or exceeds the requirements for the SIL. Many factors come into play when choosing the correct sensor, such as whether or not to use products that have demonstrated compliance for a specific systematic capability through compliance with IEC 61508 or through prior-use compliance with IEC 61511. CEP

CHAD McGUIRE is Director of Engineering and Design in Emerson Process Management's Pressure Business Unit. He has more than 20 years of experience in the manufacturing and design of Rosemount-branded products. He has a BS in mechanical engineering from the Univ. of Minnesota.

JESSICA LO is an electrical engineer with ten years of experience within Emerson's pressure design group. She has supported new product development and projects for compliance with IEC 61508; more recently, she has become involved in product reliability efforts aimed at growing and maintaining a product line that does not compromise quality and ensures reliability for the world's toughest measurement applications. She holds a BS in electrical engineering and an MS in management of technology from the Univ. of Minnesota. She is an active member of IEEE, the Society of Women Engineers, and the ISA 84 committee.

ERIK MATHIASON is a senior marketing engineer at Emerson Process Management with responsibility for pressure instrumentation. Specifically, he supports the growth and development of the Rosemount 3051S pressure transmitter, safety certified instrumentation, and new product development. He graduated from North Dakota State Univ. with a degree in mechanical engineering in 2010 and is an active member of ISA108, Intelligent Device Management.