A NEW WORLD OF SAFETY

Based on Proven Digital Technologies, a smart SIS Architecture Spans the Enterprise to Provide Manufacturers a Global View of Plant Safety
Can groundbreaking pressure instrumentation really make your plant run safer and more profitably?

You better believe it. Now, for the first time ever, you can get world-renowned Rosemount reliability in a safety-certified instrument. The scalable Rosemount 3051S Series is TÜViT-certified to IEC 61508 safety standards, meaning you can use the same proven pressure instruments in both basic process control and critical safety instrumented systems. This innovation simplifies safety standard compliance while reducing documentation requirements and proof testing. All of which can save you over 60% in total lifecycle costs. So it’s not just better instrumentation, it’s your path to better measurement practices that lead to a more profitable future. See it for yourself at Rosemount.com/Safety
Of all the issues facing today’s process manufacturers, ensuring safe operations and guaranteeing shutdown when necessary are paramount. Digital technologies now exist to help process manufacturers better address these critical issues. The same proven digital plant technology that powers our PlantWeb® architecture has now been extended to create the industry’s first smart safety instrumented system (SIS) solution. This smart SIS spans the entire loop from sensor, to logic-solver, to final control element.

This architecture uses the information available in intelligent field devices to allow the process industries to operate more safely. Electronics have been added to proven field devices to permit their use in Safety Integrity Level (SIL) 1-3 safety-rated operations. The combination of these elements into SIS provides users with a reliable, flexible, easy-to-use tool. The new, scalable, DeltaV SIS, which integrates seamlessly into our DeltaV system, is now available. This smart SIS solution provides users with a global view of their enterprise that spans the entire facility yet maintains the degree of separation of the safety critical elements from the basic process control system (BPCS) that is required by the IEC 61508 and 61511 standards. The traditional approaches to safety instrumented systems have now been superseded by this integrated-loop approach to safety management.

These new smart SIS solutions are built on the proven PlantWeb technologies—including intelligent field devices, predictive diagnostics and digital communications—which are today delivering results in thousands of process manufacturing facilities around the world. In addition, experienced, certified Emerson safety personnel and service organizations worldwide are ready to assist customers with process system hazard analysis and risk assessment along with smart SIS design, implementation and commissioning. Find all the details on Emerson’s new smart SIS solution at www.EasyDeltaV.com/SIS.

TOWARD AN INTEGRATED SAFETY CONTROL ARCHITECTURE

TOM SNEAD, PRESIDENT, PROCESS SYSTEMS & SOLUTIONS DIVISION
EMERSON PROCESS MANAGEMENT

S-4 A PROCESSORS’ GUIDE TO SAFETY
PROTECTING PERSONNEL, PLANT ASSETS AND COMMUNITIES STARTS WITH A PROPERLY DESIGNED SAFETY INSTRUMENTED SYSTEM

S-7 MONITORING CRITICAL VALVES
SMART FIELD DEVICES AND TESTING SOFTWARE PROVIDE A MAJOR LEAP IN SAFETY VALVE RELIABILITY

S-9 INTEGRATED YET SEPARATE
NEW LOGIC SOLVERS INTEGRATE SAFETY SYSTEMS DIRECTLY INTO CONTROL SYSTEM ARCHITECTURE

S-11 A ROADMAP TO SAFETY
STANDARDS HAVE PAVED THE WAY FOR SYSTEM LIFECYCLE SUPPORT BUT WATCH OUT FOR THE POTHOLES

S-13 BEST OF BOTH WORLDS
EMERSON’S SAFETY-CERTIFIED TRANSMITTERS PROVIDE BOTH COMPLIANCE AND COMPREHENSIVE DOCUMENTATION
A PROCESSORS’ GUIDE TO SAFETY

PROTECTING PERSONNEL, PLANT ASSETS AND COMMUNITIES STARTS WITH A PROPERLY DESIGNED SAFETY INSTRUMENTED SYSTEM

“A little neglect may breed mischief,” Benjamin Franklin once wrote. “For want of a nail the shoe was lost; for want of a shoe the horse was lost; and for want of a horse the rider was lost.”

Perhaps this maxim should hang in the control rooms of oil refineries, oil and gas production platforms, chemical plants and other industrial facilities where even the smallest hiccup in a volatile process can lead to catastrophe. In these industries, stuck valves, errant meter readings and other seemingly insignificant control glitches have led to fiery explosions, the release of toxic emissions and, in the case of more than one major U.S. refiner, cat crackers failing.

During the past few decades, systems and instrumentation vendors have developed sophisticated safety instrumented systems (SIS) to shut down potentially dangerous out-of-control processes before they do damage and to help plant personnel identify potential sources of these problems. Whereas basic process control systems (BPCS) control the making of on-spec product, to isolate them from the problems that they’re intended to identify and prevent. The three basic elements include:

1. Sensors, which monitor the state of an ongoing process.
2. Logic Solvers, which collect and analyze data from the sensors to determine whether emergency conditions exist, and how to respond (e.g., ignore, initiate a “safe” shutdown of the process, etc.) Typically, these are safety-rated electronic controllers.
3. Final Control Elements. Typically, these are pneumatically actuated valves.

A well-designed SIS not only reduces risks from out-of-control processes; it can also help users meet regulatory demands. A well-designed system can also increase plant availability by reducing the number of spurious “trips” caused by an SIS that fails to properly evaluate a safety situation and unnecessarily shuts down a process.

A Knowledgeable Source

While users can take the “best of breed” approach by purchasing components of an SIS from separate suppliers, many users are opting for the benefits that accrue by relying on a single, knowledgeable SIS supplier that has deep industry knowledge and an extensive portfolio of products and services. With its long experience as a leader in control products, systems and services, Emerson Process Management is just such a supplier. Offering products such as Emerson’s FIELDVUE SIS digital valve controller, SIL-PAC actuator solutions and SIS safety transmitters and valves. The DeltaV SIS system is at the heart of a tightly integrated, high-value system that

Table 1: Risk Based on Frequency

<table>
<thead>
<tr>
<th>Risk level</th>
<th>Descriptor</th>
<th>Frequency of Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Frequent</td>
<td>One per year</td>
</tr>
<tr>
<td>4</td>
<td>Probable</td>
<td>One per 10 years</td>
</tr>
<tr>
<td>3</td>
<td>Occasional</td>
<td>One per 100 years</td>
</tr>
<tr>
<td>2</td>
<td>Remote</td>
<td>One per 1,000 years</td>
</tr>
<tr>
<td>1</td>
<td>Improbable</td>
<td>One per 10,000 years</td>
</tr>
</tbody>
</table>

SISs are intended to protect people, product and the environment by enabling a safe shutdown of the process if control is lost.

Safety instrumented systems consist of basic technologies that are separate and distinct from a plant’s BPCS.
will help process manufacturers design and implement plants with maximum safety and availability.

**Standards and Safety-Related Concepts**

Two international standards govern the design and implementation of safety instrumented systems. The International Electrotechnical Commission’s (IEC) standard commonly referred to as IEC 61508, is targeted at suppliers of safety-related equipment and defines a set of standards for functional safety of electrical/electronic/programmable electronic safety-related systems. (In the United States and Canada, ANSI/ISA S84.01 essentially mirrors the IEC standard.) Among the stipulations in the IEC standard is the use of separate logic solvers and sensors from those in the BPCS, the provision of mean-time-to-failure data to users; and the use of dedicated wiring from each SIS field device to the system’s I/O.

IEC 61511 is aimed at safety system users. The standard comprises formally collected best safety practices and addresses all safety life-cycle phases from initial concept, design, implementation, operations and maintenance modification, through to decommissioning.

The IEC standards include several concepts that are vital to determining the level of risk in a plant and selecting an SIS to meet the facility’s safety needs. The first of those concepts is Safety Instrumented Function (SIF), which is defined as a single set of actions that protects against a specific hazard. Safety instrumented system are comprised of one or more SIFs.

Another important concept addressed by the standards is that of Safety Integrity Levels—SILs—which define the levels of protection needed for a particular SIF. The IEC standards describe four possible discrete SILs, while the ISA standard defines only the three that are most applicable to the process industries. SILs are determined by multiplying the risk level factors based on frequency (Table 1) by the risk level factors based on severity (Table 2) to obtain a product between 1 and 25. If the product falls between 15 and 25, the risk is considered high and indicates a need for SIL 3 protection; if the product is 6 or less, the risk is low, requiring SIL 1 protection. A product between 7 and 15 indicates a need for SIL 2 protection.

**Table 2: Risk Levels Based on Severity**

<table>
<thead>
<tr>
<th>Risk level</th>
<th>Descriptor</th>
<th>Potential consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Catastrophic</td>
<td>Multiple deaths</td>
</tr>
<tr>
<td>4</td>
<td>Severe</td>
<td>Death</td>
</tr>
<tr>
<td>3</td>
<td>Serious</td>
<td>Lost time accident</td>
</tr>
<tr>
<td>2</td>
<td>Minor</td>
<td>Medical treatment</td>
</tr>
<tr>
<td>1</td>
<td>Negligible</td>
<td>No injury</td>
</tr>
</tbody>
</table>

Once the SIL level of a given SIF has been calculated, the standard defines the acceptable probability of failure on demand (PFD) of the associated SIS. A SIF with a high SIL rating will require the use of a low system with a low average PFD (Table 3). An important factor in determining the PFD is the frequency of system testing, including the stroking of its valves. The longer the time between tests, the higher the PFD. As we will see, testing itself poses its own potential safety risks and other problems. Fortunately, Emerson has solutions that all but eliminate these difficulties.

**Design and Selection Challenges**

Based on these “cut and dried” standards, selecting a safety instrumented system would seem to be a straightforward process. However, many users are opting for the benefits that accrue by relying on a single, knowledgeable SIS vendor that has deep industry knowledge and an extensive portfolio of products and services.
exercise. However, this process is far more subtle and requires companies and their consultants to face a number of challenges and make choices about how to deal with them. For starters, identifying SIFs can be a tricky undertaking that, if not conducted properly, can be unnecessarily costly to users. Exida is a leading safety systems consulting firm, and Bill Mostia, one of its engineers, notes that some loops that appear to be SIFs are not. "A SIF is normally associated with life-and-limb protection," Mostia recently wrote. "However, when a SIF operates, there may be related actions that occur at the same time that place portions of the process in desirable operating states to minimize startup time, loss of inventory, process equipment problems, etc. Operating companies sometimes fall into the trap of considering these related actions as part of the SIF."

The result, says Mostia, is that companies wind up identifying too many SIFs—each of which has to conform to relevant safety standards—thus imposing unnecessary burdens on the plant’s owner.

Keep It in Context
Examining system performance data outside its proper context is another pitfall implementers must avoid. As Mark Menezes, an Emerson Process Management engineer, and Dupont engineer Steve Brown recently pointed out in a co-written article, system and component data supplied by vendors—even when validated by an independent third party—reflects lab results "and can be an order of magnitude too optimistic for usage in the field."

At the same time, "proven-in-use" data, which takes into account real-world failure causes, tends to be conservative because the data covers the whole range of a plant’s technology over a long period. Results from older, less reliable equipment can skew the results. According to Menezes and Brown’s article, “The net results to the user are overdesign, overtesting, increased spurious trips and needless capital expenditures.”

In addition, they noted that safety system design involves trade-offs that must be evaluated. For example, designers must typically strike a balance between a system’s ability to provide safety and its availability. If a designer tilts too far in the direction of safety, plant availability suffers as a result of frequent spurious trips; if he or she tilts too far in the other direction, that person runs the risk of increasing availability at the price of reduced safety.

In the rest of this publication, we’ll take a detailed look at how implementers meet these challenges, how safety system components protect plant safety, and how selecting Emerson Process Management as a partner can help you implement a reliable system to keep your plant, your personnel and your community safe, while providing you with maximum plant availability.
Of the three major elements in a safety instrumented system—sensors, logic solvers and final elements—the latter are usually the ones that give plant engineers the most headaches. Studies have shown that 40–50% of safety-related problems occur in an SIS’ final elements, which typically include shutdown valves, venting valves, isolation valves and critical on-off valves.

Fortunately, a new generation of intelligent instrumentation and software—including Emerson’s FIELDVUE instruments, SIL-PAC Valve Automation Solutions and AMS™ Suite: AMS ValveLink software—dramatically improves valve reliability through remote automated performance monitoring and testing. Positive results include:

- Increased reliability of the safety instrumented system and, as a result, greater confidence in the system.
- Improved worker safety as a result of being able to perform valve tests without sending personnel into hazardous areas.
- More frequent safety valve testing.
- Spotting potential trouble spots in need of maintenance attention by capturing digital diagnostic data about safety system components.

Exercise: Key to Valve Health

Similar to the cause of many physical ailments in people, not enough exercise is a leading cause of valve problems. While humans can resolve the problem by spending less time on the couch and more time in the gym, remedies aren’t nearly that simple in process manufacturing facilities. In continuous processes such as those one finds in oil refineries, chemical plants and power plants, safety valves generally remain set in one position. The lack of movement—or valve exercise—combined with harsh plant conditions can cause valves to stick. In a worst-case situation, operators won’t discover a valve is malfunctioning until an emergency occurs, and the device fails to move into a safe state.

The only way to ensure that a safety system valve will function when it’s needed is to periodically test it. In fact, the length of time between tests has a major effect on the safety system’s Probability of Failure on Demand (PFD) and, thus, can affect a system’s SIL rating. Lengthening the interval between tests has a linear effect on the PFD, so if the length of time between tests is doubled, the PFD is doubled as well.

“Therefore, it is imperative that these valves be tested frequently in order to reduce the PFD and meet the target SIL rating,” says Riyaz Ali, development manager for Emerson’s Fisher FIELDVUE instruments.

Ideally, operators would be free to test the full range of the valve (0–100%, or full-open to full-close) frequently. However, in most cases this is not practical because fully stroking a shutdown valve generally requires shutting down the process. Consequently, plants usually schedule full-stroke tests during planned shutdowns, which typically take place once every 2–3 years. However, Ali notes that improved preventive maintenance and system reliability have resulted in less frequent shutdowns and thus fewer full-stroke tests.

The SIL-PAC solution is used for emergency shutdown applications.

Fortunately, engineers have come up with a way around this situation, based on the fact that full stroking of the valve isn’t necessary to determine whether the instrument is stuck. By stroking the valve by as little as 10%, plant personnel could improve its reliability in an emergency situation. In this test, a small ramp signal, too small to disrupt the process, is sent to the valve to trigger a small movement, thus confirming that the valve can be moved.
Nevertheless, even this solution presents problems. The most popular method of partially stroking valves involves using mechanical limiting devices, such as a pin, valve stem collar or a valve handjack, that restrict a valve’s movement. If an emergency occurred during testing or a limiting device was inadvertently left affixed to the valve after a test, then the valve would likely not be able to perform its intended function. In addition, this testing method requires the physical presence of personnel—in locations where hazardous conditions can frequently exist—to install and remove the limiting devices and conduct test procedures. In fact, manual partial-stroke testing is inherently unsafe because the safety shutdown function is not available during testing.

A New Generation

However, a new generation of smart field devices, software for testing and analysis, and digital communications protocols is eliminating these problems and increasing safety system reliability while reducing costs.

Smart positioners have grown increasingly popular in recent years. These microprocessor-based, current-to-pneumatic digital valve controllers provide internal logic for control of valves while also using the HART communications protocol to provide plant personnel with details about the instrument’s condition.

In a typical installation, a smart positioner is installed in a four-wire system. A logic solver provides two separate outputs: a 4–20 mA output serves as the primary control signal and is used to control the valve position during partial-stroke testing. The same pair of wires is also able to transmit valve diagnostic information back to the operator via a HART digital signal superimposed on the 4–20 mA signal. The second output from the logic solver is a 24–VDC signal, connected to a solenoid valve. This serves as an independent means of sensing an SIS command to the safety valve, should the analog connection to the valve fail. This arrangement is known as a 1-out-of-2 (1oo2) failsafe configuration.

Instruments such as Emerson’s Fisher DVC6000 Series Digital Valve Controllers with AMS ValveLink software for emergency shutdown solutions do not require the presence of personnel in the field during testing because of the technology’s inherent communication capabilities. Initiating the automated routine test does not require the technician to remove the instrument’s cover or be near the valve. The simplicity of this automated procedure eliminates costly, labor-intensive routines and allows for more frequent online testing. Another benefit of Emerson’s smart SIS solution over manual partial-stroke testing is that if a command directing shutdown is issued during a partial-stroke test, the valve will immediately close.

The new generation of digital valve controllers and diagnostic software delivers a wealth of information about the valve’s condition that enables operators and maintenance personnel to spot points of failure that might not otherwise be apparent. AMS ValveLink software can maintain “signature” files showing the ideal state of the instrument, which are then compared with results acquired during partial-stroke testing. Thus, plant personnel can quickly spot conditions such as packing problems (through friction data), leakage in the pneumatic, pressurized path to the actuator (through the pressure vs. travel graph); valve sticking, actuator spring rate and bench set. ValveLink also creates a time-stamped audit trail of testing that can be reviewed, analyzed and used for regulatory compliance purposes.

AMS ValveLink also includes its Batch Runner tool and can be used to automate diagnostic testing. It provides the capability of running multiple tasks back-to-back with no operator intervention necessary. In addition, the software’s Event Messenger is able to notify key personnel via email and/or pager when a specified alert occurs, thus enabling quick response to potential problems.

So, while final control elements have been the weak link in SIS in the past, Emerson is using advanced technology to enable users to spot potential problems easily and cost-effectively.
The logic solver is the “brains” of the SIS. Logic solvers receive data inputs from the system’s sensors and evaluate that data to determine whether a shutdown is warranted. The logic solver then sends the output to the system’s final elements, such as safety valves and relief valves.

Until now, implementing, programming and maintaining logic solvers has been anything but easy and routine. Logic solvers typically are very expensive components. Programming and maintaining them is extremely labor intensive. Integrating data into basic process control systems typically requires complex interfaces and gateways, and SIS architectures have made required testing and maintenance time-consuming and costly.

In addition, logic solvers are monolithic, centralized units with large footprints. Although well suited for large-scale operations with uniform SIL requirements, traditional logic solver technology has lacked the scalability and flexibility processors need to cost effectively deal with an expanding range of safety integrity needs.

**Barriers Removed**

Emerson has removed many of those obstacles with the release of DeltaV SIS, which includes DeltaV SLS 1508 logic solver. Unlike many logic solvers that must be “bolted” on to the basic process control system (BPCS) via extensive integration, the DeltaV SLS 1508 was developed as an integral component of Emerson’s PlantWeb architecture. In addition, the DeltaV SLS 1508 is modular, enabling users to efficiently scale the system to meet process control and safety objectives.

The DeltaV SLS 1508 can be configured as a simplex system, or users can increase the availability of their SIS loops with a redundant pair of solvers. Both architectures are certified as suitable for SIL 3 applications.

In addition, the DeltaV SLS 1508 uses the HART protocol to deliver rich communications from devices in the field to operators and software in the plant’s control room. Through the use of HART function blocks the safety system is able to deliver diagnostic information that provides technicians with details about a malfunction in sensors, transmitters, and final elements and enables them to conduct preventive maintenance as well.

“With the DeltaV SLS, you’re using the same engineering tools as with the DeltaV BPCS, but with different security accesses,” says Emerson Product Manager Gary Law. “While the standards require that you must not be able to write to the safety system from the BPCS, you can read any process data you want via an operator interface. We’ve designed it so that you can access our safety system data or control strategy from a single operator interface in exactly the same way you would access it from the DeltaV controller.”

More important, he says, is the elegance and simplicity the DeltaV logic solver brings to programming safety systems. For example, it’s not uncommon for a plant to change the programming or configuration of a safety system to accommodate new devices, or a change in the product. However, says Law, safety standards create procedures that can complicate the task.

“The standards dictate that, anytime you’re making a change in the system from the operator interface, one has to perform a repeat-confirmation step, which essentially means that you have to send commands twice to the logic solver to ensure that it has properly received the changes,” says Law.
“To do that with any other safety system on the market means that you have to have double engineering in the operator interface, gateways and the logic solver. It can be a daunting process. But we just built that whole process into our system. You can make changes merely by using a wizard that sets up the whole repeat-confirmation process automatically while remaining compliant with the standard.”

In addition, Emerson has simplified the task of programming the logic solver. The company offers a full palette of TÜV-certified smart function blocks designed specifically for SIS functions. As a result, tasks that can take many pages of ladder logic to engineer and an extensive effort to test, commission and maintain, can be accomplished in the DeltaV system through drag-and-drop configuration.

For configuring the system, Emerson has also simplified the use of Cause and Effect Matrices (CEMs). “In most systems, you have a front-end engineering tool that you use to create the CEM. That system then generates logic that you download into your logic solver. Until recently, those systems required that you do your functional testing on the logic underneath, which looks nothing like the matrices you used to create your requirements,” says Law.

In the DeltaV SIS, CEM diagrams are directly deployed in the controller using an approved function block. This executes as it is presented, without programmers having to dig into the underlying logic to test it. In fact, there is no logic other than check boxes, so the standard is demonstrably adhered to.

Scalability Provides Flexibility
The scalability of the DeltaV logic solver offers a distinct advantage by making it far easier and more cost-efficient to configure the system for a given plant situation at what Law refers to as a “granular level.” As an example he describes a typical plant situation where three reactors, each with 10 I/O points, would all require separate logic solvers to meet safety demands.

“In the case of many safety systems, putting separate logic solvers on each reactor just isn’t economically feasible; the devices are too expensive,” says Law, who explains that a single logic solver is a possibility, but that solution would still require separate I/O cards for each reactor.

“Emerson’s logic solver handles 16 I/O points, and that means we can put the logic solver on the controller backplane that looks after the reactor. By installing three logic solvers we’ve created a cost effective distributed safety system that meets safety requirements because there’s no common point between the three. By being able to dedicate processing in small chunks and distribute it among the logic solvers, we provide users with an economic advantage.”

Using relatively small distributed logic solvers also gives users increased flexibility says Law. “By being able to dedicate separate logic solvers to specific SIFs throughout a plant, each solver can be configured for a specific SIL level.”

The DeltaV SIS takes advantage of PlantWeb’s HART capabilities to enable rich communications among all system components. In multi-vendor systems, the logic solver is also capable of communications via OPC and Modbus as required. So, regardless of the PLC or DCS that users employ for basic process control, they can increase plant availability by using the advanced diagnostics in Emerson’s SIS.

The DeltaV SIS facilitates compliance with environmental and health regulations. Its Device Audit Trail automatically details changes to a device’s configuration and records a wealth of relevant event data.

To help users meet safety standard requirements and management of change, the system features an electronic signature function that can be configured to prohibit any system changes without the appropriate permissions.

Emerson has developed an SIS logic solver that can benefit virtually any plant that needs to ensure safe operations and maximize plant availability. For plants already using Emerson’s PlantWeb architecture, the DeltaV SIS provides tight integration with the basic process control system. At the same time, users of other vendors’ basic process control systems and components can obtain many of the same benefits by interfacing between the two with standard protocols such as Modbus, OPC and HART.
How safe is “safe enough” when it comes to potentially hazardous processes in chemical plants or oil refineries? What steps should a plant take in evaluating risks and initiating protective measures? How do you ensure that a safety system will function when it’s needed? How do you protect against inadvertently compromising the integrity of your safety system?

Consider the Consequences

When one considers the consequences of a safety system failure, the gravity of these questions becomes apparent. For that reason, major standards-setting bodies—the IEC in Europe and ANSI/ISA in the U.S.—have spent the past two decades developing comprehensive standards for the design, implementation and lifecycle management of industrial safety systems. Over time, these standards have taken hold in a growing number of process plants, and the standards organizations continue to revise them to keep up with changing needs and advancing technology.

Nevertheless, one safety system expert cautions that companies wishing to implement systems that comply with the standard must rely on knowledgeable, experienced personnel to do the job correctly.

Not Rocket Science But Close

“It’s not rocket science, but you really need to know what you’re doing,” says Bill Mostia, who has spent more than two-dozen years applying safety, instrumentation and control systems in process facilities.

The development of safety system standards can be traced back to the mid-1970s, when two devastating industrial accidents occurred. In 1974, a chemical plant explosion in Flixborough, England took 28 lives. Two years later, a chemical plant explosion in Seveso, Italy released a cloud of dioxin over a wide area, causing serious health and environmental problems.

At about the same time, process manufacturers began replacing some of the electro-mechanical controls in their plants with newly developed programmable logic controllers (PLCs) and distributed control systems (DCSs), giving rise to concerns about their performance in emergency situations.

“People just started having fears that these systems might be dangerous,” says Mostia, who today works for exida, a consulting firm that helps companies design and implement control systems. “They felt the need to bring these systems under control.”

A Guide For Manufacturers

As a result, IEC and ISA began work on standards intended to guide manufacturers in the design and use of control systems for safety applications. IEC created two landmark standards, the first of which, IEC 61508—“Functional Safety of Electrical/Electronic/Programmable Electronic Safety Systems”—was begun in the mid 1980s.

“IEC 61508 is an umbrella standard, designed to cover
multiple industries. The vision was–and still is—that industry sectors would write their own standards based on IEC 61508 and add their own particular perspectives and definitions,” says Mostia.

Later, the organization developed IEC 61511, intended as the safety system standard for the process industries. In general, IEC 61508 is considered to be the standard that governs the manufacturers and suppliers of safety systems and devices, while IEC 61511 is considered most applicable to systems designers, integrators and users.

IEC 61511 addresses all safety lifecycle phases, including initial concept, design, implementation, operations, maintenance and modification.

Basic But Necessary Steps
While the details of every safety system implementation will vary, the basic steps companies must go through to comply with the industry standards are the same:

• Identify hazards and safety functions for each process
• Allocate safety to layer of protection. Develop safety requirements
• For each loop, determine the level of risk reduction/level of safety
• Design the SIS (hardware, software)
• Select the loop sub-components
• Install, commission, operate and maintain

The first three steps involve a risk analysis study of the plant, which is generally done using a hazard and operability analysis.

“Basically, the designers divide up the plant into small pieces and use a group of guide words like ‘too much,’ ‘too little,’ and ‘not enough,’ when looking at the hazards and potential risks in each of these plant ‘nodes,’ ” says Mostia.

As part of the second step, designers consider the passive protections that already exist, such as dikes to retain spills, over-engineered vessels, etc. The presence of these elements reduces the amount of risk for that section of the plant. “The result is that you come up with a safety system requirement and target SILs,” says Mostia.
Formal Design Stage
At that point, plants go into the formal design stage, which generally consists of two steps:
1. Conceptual design, in which the plant decides on the safety system architecture (e.g., redundant sensors and/or logic solvers; the amount of redundancy warranted, etc.) based in large part on the SIL requirements.
2. Detailed design, in which designers combine the conceptual design, safety requirements and the plant’s engineering specifications.

Potential Potholes
While the process is straightforward from a high-level viewpoint, Mostia cautions that there is a number of potential potholes that safety system designers and process engineers should be aware of throughout the lifespan of the safety instrumented systems they are planning to create.

• Overdesign: “If you don’t do your SIL selection properly, you could wind up with too high a SIL for everything. As a result, you wind up with more complex, expensive systems than you need,” says Mostia.

• Underdesign: On the other hand, you need to make sure that you don’t underestimate your SIL needs and install a system that won’t deliver the protection you need in an emergency. “Sometimes, you get into a project environment where people are worried about spending, so they tend to drive the SIL down to rationalize not putting in sufficient safety systems. You have to find a middle ground between the two extremes,” Mostia contends.

There is a number of potential potholes that safety system designers and process engineers should be aware of.

• Treating safety systems as a patch: Many companies are tempted to treat a safety system as an add-on patch to their basic process control systems that can be installed and then largely ignored. Mostia notes that S84 and IEC 61511 address the entire lifecycle of the SIS, including ongoing maintenance and testing. In addition, they have to ensure that their maintenance technicians are properly trained to ensure that the system is operating properly.

• Grandfathering: As noted earlier, the newest version of ANSI/ISA S84 will be identical to IEC 61511, essentially creating a global standard. The revision also calls for existing systems compliant with S84 to be “grandfathered” under the new version of the standard. However, grandfathering should not be interpreted as meaning that “whatever’s in place is okay without any further effort,” says Mostia. “The intent is that you go back to make sure that your safety systems were built to the standards of the day. There’s a formal process for doing that and documenting the process.”

To ensure that the organization doesn’t hit one of these potholes, Mostia says it is vital that plants employ knowledgeable and experienced safety system designers. If a company has suitable internal resources it should deploy them, but if it doesn’t have the in-house expertise, then the company should consider hiring a consulting firm specializing in safety system design and implementation.

Finally, companies should ensure that their system designers are vendor-neutral so that they’re sure they’re buying the systems and components best-suited for their needs rather than being won over by advisors’ vested interests.
When it comes to selecting transmitters for safety instrumented systems, SIS designers are between the proverbial rock and a hard place, says Dale Perry, pressure transmitter marketing manager for Emerson Process Management’s Rosemount division.

IEC and ANSI/ISA safety system standards dictate a plant has two choices if it wants to be compliant, says Perry: It has to use transmitters that have been certified as compliant, or it has to be able to produce rigorous historical documentation proving that a non-certified transmitter is safety system-capable. “Well, most users simply don’t have the documentation necessary in order to use non-certified devices, and the selection of certified devices right now is very slim,” he says.

The result, he adds, is that many companies opt to use uncertified transmitters with which they’re familiar and over-engineer and over-test the systems—a very expensive way to ensure the performance of a safety system.”

A Familiar Answer

Emerson has provided an answer to this dilemma with the release of the 3051S pressure/differential pressure transmitter and the 3144P temperature transmitter. Emerson has added SIS electronics to both devices, which have been TÜV-certified as IEC 61508-compliant for SIL 2 use. As a result, SIS users have the best of both worlds. They can select instruments for their safety systems with which they are already familiar and which are certified for SIS use.

In addition, users no longer have to overcompensate with too much testing and redundancy, because Emerson has documented the instrument’s loop testing and calibration needs. Users can be confident that the system will meet their safety and plant availability needs cost-effectively.

Because the devices are the source of information about the status of a process, transmitters play a unique role in the SIS. Your logic solver can be absolutely top-notch, and your safety valves can function flawlessly when called upon in an emergency, but if your system is receiving inaccurate information on the state of the process from faulty transmitters, you will be operating in an unsafe condition. Worse, in instruments that haven’t been rigorously tested, proven and certified to function in particular conditions, some of those faults can be hidden, leaving operators and technicians unaware that anything is amiss.

Among potential covert transmitter problems:
- Poor installed repeatability that exceeds safety margins.
- Coated RTD thermowells.
- Corrosion and hydrogen permeation in pressure transmitters that can cause gradual drift.
- Rapid and severe overpressure in differential pressure transmitters than can cause a zero shift, detectable only during calibration and/or inspection.
- Abrasion of electrodes in magnetic flowmeters, causing noisy flow measurements and electrode failure.

That is why IEC 61508 imposes a strict set of conditions under which an instrument can be deemed acceptable for safety systems and on the way that sensing elements in the system must be configured, says Perry.

Certifying this compliance requires that manufacturers put the device through extensive third-party testing to see how it reacts to a wide range of process conditions, whether it produces errors under those circumstances, whether those changes can be routinely detected and whether the changes are safe or unsafe, says Perry. Testing is rigorous and expensive, and there are relatively few safety-certified transmitters available to users, he adds.

The alternative to using a certified instrument is for users to select instruments that are “proven-in-use.” “To gain proven-in-use approval, your vendor has to prove that it has a quality system in place. Then, you have to show that you have the same transmitter operating in your basic process control system (BPCS) under conditions similar to those in the safety system, and you have to document usage and failure history to determine mean
time between failures (MTBF). Once you have all that, you can use the transmitter in your SIS,” says Perry.

The problem: few users are capable of or willing to meet those extensive demands for prior-use documentation, and many are unwilling to select transmitters from the limited pool of certified devices. As a result, says Perry, many companies simply “throw up their hands,” use the same transmitters employed in their BPCS, and compensate for uncertainty by installing redundant devices and frequently testing and calibrating them. By following this route, plants typically run up enormous and unnecessary costs, he says.

“For example, with our new certified pressure transmitter, we’ve documented a need for a loop test every five years and calibration every 10 years. But some plants using transmitters that are not certified or proven in use for SIL 3 applications are calibrating them every six months. In other words, they’re doing 10 times more than they might need to with a certified instrument,” says Perry.

In addition, plants typically over-engineer and overbuild their systems using uncertified and unproven transmitters. This involves the installation of redundant transmitters on safety loops, despite the fact that redundancy might not be required with the use of some safety-certified instruments. Here, too, the basic cost of the hardware and ongoing lifecycle costs can be significant, says Perry.

Proven and Certified

With its release of its safety-certified 3051S and 3144P transmitters, however, Emerson has provided users with the tools to implement systems that meet functional needs while providing them with the confidence that allows them to avoid unnecessary costs.

First, Emerson is the industry’s leading supplier of instrumentation, with hundreds of thousands of transmitters in place around the world. Among its most-used products in basic process control systems are the 3051 and 3144 transmitters, both of which are proven with billions of hours of operation. Consequently, many plants already have the knowledge and capability to use and maintain the safety instruments, both of which have been certified as IEC 61508-compliant by TÜV.

“Leveraging existing Rosemount commissioning, maintenance and training procedures can create significant cost savings. Now everyone in the maintenance shop is qualified to work on SIS instrumentation,” says Perry.

A study by exida, a major consulting firm involved in the evaluation of safety devices and design of safety systems, shows that 36% of the sensing devices in safety applications are pressure transmitters and 19% are temperature transmitters. “In light of the fact that the pressure transmitter can also perform level and flow measurements, these two devices potentially cover nearly 85% of safety system applications,” says Perry.

In addition, Emerson Process Management ships its safety-certified transmitters with all necessary documentation involving all aspects of their use in safety systems, including testing and maintenance requirements. Users are not required to test and calculate SIL limits, probability of failure on demand or prior use. Simple and less time-sensitive proof testing lowers SIS maintenance costs by reducing unscheduled plant shutdowns.

Both transmitters have been certified for use in SIL 2 applications (SIL 3 applications when used redundantly) and, in applications involving “clean” fluids, safety standards permit fault tolerances that will allow many users to reduce instrument redundancy. Also, the 3051S and 3144P transmitters use the same parts as their BPCS counterparts.

“In essence, we’ve simply taken the existing transmitter and inserted a supervisory electronic circuit board to make it compliant with IEC 61508 standards,” says Perry. “So, in many instances, plant engineers won’t have to buy an enormous number of new transmitters for their company’s safety systems. They’ll simply be able to stock circuit boards and install them in transmitters already in their inventory.”
Safe enough?

Finally, a smart approach.

Introducing DeltaV™ SIS, the first safety system for your safety applications to use digital communications and field intelligence to help you achieve increased availability—with the ease you expect from the DeltaV system. And, it easily scales and distributes to fit safety applications of any size.

It’s a core element in Emerson’s digital PlantWeb® architecture and the world’s first Smart SIS. Every aspect of the safety loop is integrated into each safety function—from sensor through logic solver to final control element—using the power of digital field intelligence, diagnostics, and automated proof testing.

Integrated. Reliable. Easy-to-use. Now you can better manage your safety efforts throughout the entire IEC 61511 safety lifecycle.

For more on a smarter approach to safety, visit: EasyDeltaV.com/SIS