A United Electric Controls White Paper

UNITED ELECTRIC CONTROLS

Safety Instrumentation Simplified

The case for a hybrid safety transmitter

by: Wil Chin, Vice President of Marketing and Business Development at United Electric Controls
Rick Frauton, Senior Product Marketing Manager at United Electric Controls

The reliability of today's automation technology has moved from generic components into the high reliability, certified space. While there remains considerable variation in the quality of the sub-system infrastructure, there is increasing awareness of the risk, cost of ownership and sustainability of all elements of process safeguards, including, and especially, the Safety Instrumented System (SIS).

Traditional SIS components along with all instrumented protective systems (IPS) are under scrutiny for their role in either initiating or responding to hazardous events. Within the scope of the Basic Process Control System (BPCS), these instrumented functions are known collectively as SCAI – Safety Controls, Alarms and Interlocks per ISA 84.91.01-2012. (See Figure 1.) In the subset of SCAI known as Safety Instrumented Systems (SIS), these protective functions are managed under the guidance of IEC 61511 and ISA 84.00.01, two functional safety standards that have largely been accepted as best engineering practices.

Instrumented systems that provide process safeguarding usually consist of:

- Sensors, which read pressure, temperature and other process variables.
- Logic solvers which translate analog or discrete inputs from process variables or from diagnostic signals, and act on those values.
- Final elements, which are the last link in safeguarding the process. These elements can be valves and other interconnected equipment like a Motor Control Center (MCC).

The ultimate objective is to reduce the risk of a hazardous event by putting in place instrumented safeguards that are "available" to the BPCS, assuring that no demand is ever placed on the safety instrumented system or, in a worst case scenario, the safety instrumented system that brings the process to a safe state.

According to the ARC Advisory Group, more than 50 percent of safety system failures can be attributed to the final element, 40 percent to the sensor and 8 percent to the logic solver.

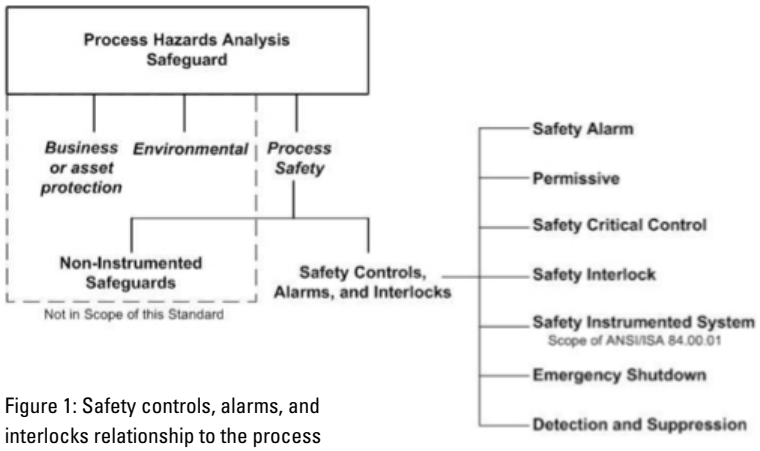


Figure 1: Safety controls, alarms, and interlocks relationship to the process hazards analysis (PHA)

Reference: ANSI/ISA 84.91.01-2012

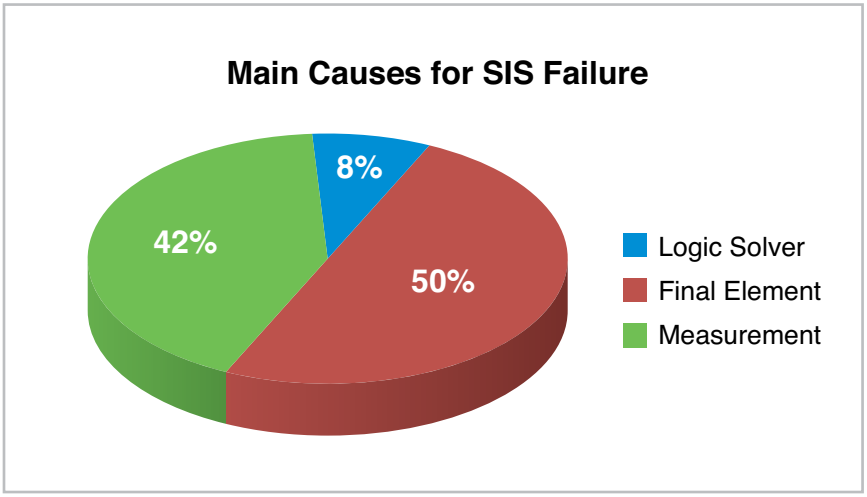
Furthermore, according to Health and Safety Executive, an organization which advises the British government on workplace regulatory matters, more than 85 percent of industrial accidents are caused by human error. Anything that can be done to guide best practices, simplify system architectures and automate operations will contribute to performance which is both safer and more cost-effective. Although industry standards IEC 61511 and S 84 are related, technical reports provide a fair amount of guidance regarding safety best practices. There is wide variance across the process sector regarding efforts to comply with such functional safety standards, which is not surprising given their complexity. In general, the industry is challenged with retiring expertise, a wide variety of equipment, and a kind of myopia that may limit consideration of newer, disruptive technology which may prove more cost-effective and technically supportable than traditional approaches. Main Automation Contractors (MACs) and Engineering Procurement Contractors (EPCs) who design and build the systems and the owner-operators who use them must be aware of the possibilities that new, largely hidden technology can enhance compliance with functional safety standards. The complexity manifests at the subsystem design, implementation and commissioning levels. It can boost the cost of a system, through installation of redundant SIS components necessary to achieve the target SIL, increasing TCO based on need for more proof testing, calibration and maintenance. Complexity can reduce operating efficiency, masking information about whether a targeted valve actually closed as instructed by the logic solver, for example. And, complexity can introduce greater cyber security vulnerability through multiple, unnecessary digital I/O, particularly in interfaced and integrated safety systems tied to with BPCS and enterprise systems that ultimately communicate via the Internet. Such complexity is an even more critical issue today, as many engineers who have learned the intricacies of the system are retiring and being replaced by inexperienced workers for whom the learning curve is already high.

How we got here

The first safety systems involved electromechanical process switches, which could be set to open or close valves or act on other final elements directly, based on an internal set point and out-of-range process variable. More sophisticated, programmable logic solvers were introduced to manage the increasingly complex relay logic. Since these systems lacked diagnostic coverage, voting mechanisms were introduced to provide higher levels of safety integrity and availability.

As "smart" process transmitter usage grew, they became the norm in the plant, and by default, the sensing elements for SIS systems. But once the networked process transmitter was configured for SIS, the digital communication

Figure 2: Causes for SIS Failure



Source: ARC Advisory Group

capability went unused, leaving the SIS unnecessarily vulnerable to cyber security threats. The digital protocols do provide the ability to reconfigure process transmitters remotely, which is ideal for process control applications, such as batch processing. This same capability, however, opens the SIS to tampering and must be disabled for maximum security. Process transmitters achieve high levels of accuracy necessary for custody transfer and ultimate process control. Conversely, process monitoring to determine whether safe parameters have been exceeded does not require such high accuracy. Increasing the accuracy of process transmitters, however adds to the price of the sensor, creating waste. And, since a safety system must have adequate layers of protection to meet SIL 2 or SIL 3 safety requirements, it may be necessary to deploy multiple transmitters, adding further to the cost.

This move toward complexity has resulted in SISs with the following less than desirable traits:

- Redundant sensors, each with higher cost and more capability than is actually needed to achieve the SIL target.
- Cabling that connects up to 20 sensors to a PLC.
- Complex voting logic and ESD decision algorithms that interpret the outputs provided by these redundant sensors.

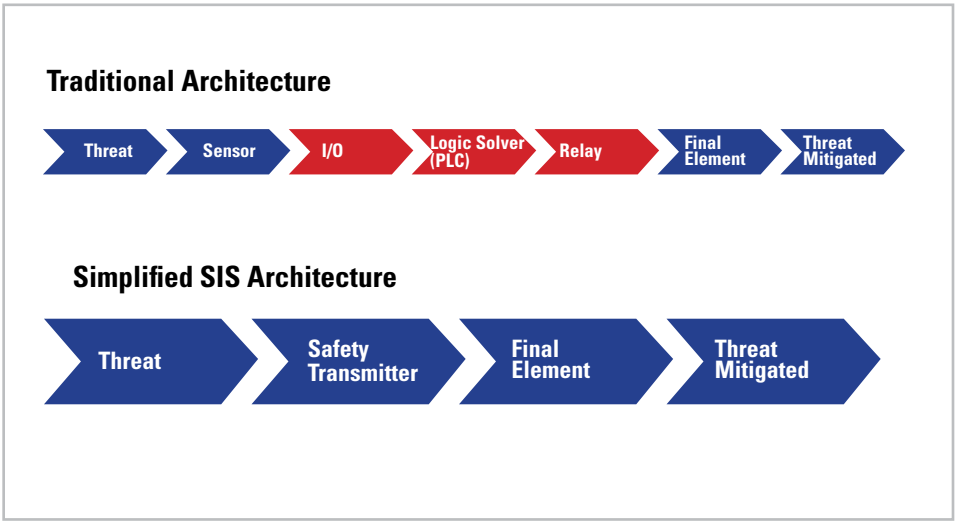
For smaller, less critical systems, this growing complexity isn't as much of a problem. But in large systems, which could involve hundreds of sensors, this arrangement adds unnecessary costs of implementation and ownership, vulnerability and confusion on the part of the operators and maintenance personnel.

Myth-busting

While many safety applications could benefit from a simpler safety architecture, SIS designers are instead deploying more technology layers, adding more complexity than is necessary. This stems from two false assumptions: That a safety PLC must always be the logic solver and the controller for switching the final elements and that smart process transmitters with high accuracy (and price!) are adding value to the system. Challenging these assumptions can result in a safer, more economical system. Let's look at each.

Instead of using a safety PLC to perform the logic solving function, for many safety applications, a safety transmitter with a built in safety relay can function as both sensor and safety logic solver. Eliminating an external connection from the sensor to the logic solver in this way reduces wiring and complexity while increasing reliability and speed of response. Safety transmitters that combine the sensor and logic solver functions and are certified by a third party for use in the SIS provide assurance that the product will perform the functions for which it was designed while providing extremely high safe failure fractions.

Figure 3



Blending BPCS and SIS components is another logic solver alternative. Some SIS designers attach multiple safety sensors to their BPCS logic solver. Conversely, the output from one process transmitter is provided for both the BPCS and the SIS logic solvers. When properly designed per the IEC 61511 standard, these two systems must be autonomous to ensure high reliability and availability and to avoid common mode failures. Common mode failures can, for example, occur when similar components from the BPCS and the SIS are subject to the same fault conditions, often resulting in a loss of both process and safety control.

Sensor sense

A transmitter that combines the functions of the sensor and a logic solver provides smart self diagnostics and decision making capability. The sensor monitors the process variable for abnormal conditions and the built-in logic solver makes the appropriate decision to manipulate the final element via the on-board safety relay. Safety transmitters manufactured by UEC (www.ueonline.com), for example, combine a transmitter with a programmable switch and configurable self diagnostics to provide the logic solver function.

The safety transmitter embeds a high-capacity safety relay to control the final element and a 4-20 mA signal for process trending, eliminating the need for a safety PLC or other logic solver.

Figure 4: One Series Hybrid Safety Transmitter

This saves money by reducing the number of safety components needed to achieve the SIL target and functionality. It also eliminates the additional premium paid for smart process transmitters, since the high accuracy and communications protocol is not likely to be used once the system is configured.

A large petrochemical plant in Dahej, India, for example, deployed the UE One Series hybrid transmitter-switch and reduced labor by 50 percent, commissioning time by 75 percent, logic solver programming and rewiring time by 100 percent. If smart process transmitters were used in place of these hybrid transmitters for these safety systems, implementation and TCO costs would have been estimated at 500 percent higher.

Furthermore, a hybrid transmitter-switch provides something that is not available in any other SIL-rated SIS sensor: the ability to verify and report if the instruction sent to the final element from the safety relay was actually executed.

The UE safety transmitter, for example, uses a feature called SRO Monitor to verify both the wiring integrity and instruction execution for the safety relay. The 4-20 mA analog signal is verified for accuracy and can indicate a fault by outputting 3.6 milliamps. Auxiliary discrete outputs provide set point status and diagnostics status, providing redundancy and facilitating voting logic schemes when a safety PLC is part of the SIS design.

A simpler, safer world

As mentioned earlier, a hybrid transmitter-switch design may not be appropriate for all SIS applications, but there are many SIL architectures that will benefit from this powerful yet simpler approach to SIS design.

- A refinery planning to implement a conventional SIS involving a process transmitter, trip amplifier, safety relays, distributed control system, wiring and all of the ancillary programming necessary to initiate an emergency shutdown, could achieve the same results with just a hybrid transmitter. Programming would be minimal and there would be no need for these separate components. Hybrid transmitter-switches that are certified for use in SIS applications functions as transmitter, switch, safety PLC and associated I/O, and by doing so eliminate the added cost, complexity, wiring and maintenance.

- A mothballed plant facing the need to upgrade their safety systems cost-effectively would avoid the need to implement a full-blown safety system, potentially reducing the time and expense to safe operation by as much as 75 percent. This could be even higher if design, analysis, and labor are included.
- A company in a low-margin industry that has to safely expand its operations to meet projected demand increase, but for which success depends on rigid cost control, could save as much as 60 percent over the cost of sensors, in addition to a reduction in the total cost of ownership.
- A refinery seeking to comply with IEC 61511 in order to update HAZOP and LOPA could benefit by implementing a hybrid safety transmitter at the FEED stage. If, for example, the analysis shows that one or more SIFs are needed to reduce the inherent risk, this can be accomplished by replacing legacy switches with hybrid transmitter-switches to provide or upgrade these SIFs.

In summary, combining sensor, logic solver and relay into one, factory-integrated, SIL-verified automation component contributes to safety and cost control initiatives by offering the following advantages over safety PLCs and smart transmitter based systems:

- Reduced purchase price
- Reduced wiring
- Reduced maintenance
- Reduced time for learning and programming
- Reduced spares management
- Reduced vulnerability to human error, by eliminating human touch points

And as the industry moves in the direction of even greater automation, the human factor in safety installations will become even less. We may not be at the point where we are automating the proof testing, but 10 years ago, very few people thought that driverless cars would be a good idea either.

Wil Chin is Vice President of Marketing and Business Development at United Electric Controls, in Watertown, Mass. Prior to that, he was a research director for the ARC Advisory Group covering asset performance management, condition monitoring, plant asset management, field devices, control valves, communication protocols, and wireless technology. He has also held technical and marketing positions at Krohne and Foxboro (now part of Schneider Electric). He can be reached at **wchin@ueonline.com**.

Rick Frauton is Senior Product Marketing Manager at United Electric Controls, where he is responsible for the One Series safety transmitter product line. Previously he held technical marketing positions at Polaroid Corporation. He can be reached at **rfrauton@ueonline.com**