ARC VIEW

JANUARY 30, 2014

An Affordable Option for Safety and Security

By Paula Hollywood

Keywords

Process Safety, Safe Failure Fraction, Cyber Security, exida Certification

Summary

Texas City Refinery, Buncefield Terminal, and Deepwater Horizon are all examples of recent catastrophic industrial accidents. Could new safety technology have prevented or at least mitigated these disasters? Over the last couple of years, many regulatory agencies have shifted their focus from reactive to proactive approaches for preventing major accidents. This has created a new sense of urgency for end users to become proactive in their process safety endeavors.

The best way to reduce risk is to design inherently safe processes. However, inherent safety is rarely achievable. A realistic alternative is to employ diversity in safety systems to increase system reliability and avoid common mode failures.

United Electric Controls, a market leading provider of safety switches, recently briefed ARC Advisory Group on its new One Series Safety Transmitter. The company believes that its safety transmitter represents groundbreaking technology offering unprecedented performance at an affordable price. Key findings include:

- Despite advancements in technology and more rigorous standards, the process industries continue the struggle to ensure plant safety.
- Leading automation system safety testing organization, exida, bestowed its highest ever Safe Failure Fraction (SFF) rating per IEC 61508 to the One Series Safety Transmitter.
- The One Series Safety Transmitter is designed to deliver both process and cyber security.

SIS Technology Trends

Safety instrumented systems (SIS), consisting of sensors, logic servers, and final control elements, are intended to implement one or more safety in-

strumented functions (SIF). The goal of an SIS is to prevent or mitigate hazardous events by taking the process to a safe state when predefined conditions occur. IEC 61511, the international SIS standard for the process industries, mandates the process control system and SIS remain separate, independent, and autonomous. The hazard and risk analysis utilizes the concept of protection layers and specifies the safety integrity level (SIL) concept developed by the IEC 61508 standard.

ARC believes the best way to reduce risk is to design inherently safe processes. However, inherent safety is rarely achievable as risks prevail wherever hazardous or toxic materials are stored, processed, or handled. A more realistic alternative is to employ diversity in safety systems to increase system reliability and avoid common mode failures. Recent ARC research on safety systems in the process industries revealed that owner/operators are exhibiting an increased focus on system reliability and availability (rather than architecture). Increasingly, they understand the importance of safety lifecycle management; the need for greater integration of safety and security systems as they pose comparable threats; and adoption of lower cost, fit-for-purpose safety devices and systems.

Designed Solely for Safety Applications

The design engineers at United Electric must have been paying attention to these trends and responded with a SIL-certified transmitter designed solely for safety, alarm, and shutdown applications. The device was designed to fill functional gaps of currently available solutions. According to the company, it is more reliable, faster, minimizes nuisance trips, is suitable for both greenfield and brownfield installations, and is cyber secure -- all at an affordable cost.

FROM	TO
Process	Safety
Accuracy	Reliability
Fast response	Faster response
High cost	Affordable
Nuisance trips	Minimal trips
Transmitter	Transmitter & Switch
Convenience	Security

Design Goals of UE's Once Series Safety Transmitter

The IEC 61508 standard specifies the criteria that suppliers must follow to claim a SIL certification for devices. SIL requirements for hardware are based on a probabilistic analysis of the device. Devices must meet targets for maximum probability of dangerous failure and minimum safe failure fraction (SFF) to achieve a given SIL rating, a minimum SFF for SIL2 is > 90 percent and for SIL3 > 99%. Major safety assessment and certification organizations include the various TÜV organizations, exida, and Factory Mutual. Currently, exida has certified the

One Series Safety Transmitter for use in SIL2 safety systems, with SIL3 capability. Both pressure and temperature versions of the device received an SFF rating of 98.5 percent, the highest the organization has ever bestowed on a piece of equipment. SFF is an indication of fault tolerance and establishes the minimum level of redundancy required in a safety instrumented function.

UE's One Series Safety Transmitter

A typical safety loop consists of sensors, logic solvers, and final elements. A typical process SIL-rated pressure transmitter requires 300 ms to communicate with the logic solver and as much as 500 ms for the logic solver to send a signal to the final element (valve). As a result, the total elapsed time may not be fast enough for critical applications. When directly connected to the final element, the One Series Safety Transmitter cuts signal speed to 100 ms, a significant time savings in a disaster. In applications such as compressors, blowers, and pumps the One Series can comprise a complete safety system with a self-contained sensor, logic solver, and final element (switch) capable of SIL2 without additional safety instrumented function (SIF) components.

United Electric considers its technology as groundbreaking because the One Series Safety Transmitter is suitable for both brownfield and greenfield installations. The transmitter offers multiple outputs. This makes it suitable for both legacy systems that employ electromechanical switches and new safety systems that utilize digital devices such as pressure transmitters. Priced at less than half the cost of many SIL-rated process measurement transmitters, the One Series Safety Transmitter offers lower total cost of ownership by minimizing nuisance trips, requiring only annual proof testing, and reducing inventory requirements to support multiple generations of installed safety systems.

The company's patented IAW (I Am Working) algorithm detects faults before they become process control problems. Detected faults are reported on the digital display while the switch fails safe open and the 4-20 mA analog output saturates beyond 4 and 20 (per NAMUR standards) to provide remote fault indication. The intelligent and configurable IAW diagnostics allow the device to provide a significantly higher SFF, while providing plug port detection in pressure models.

Cyber Security

Industry and government concern regarding security of critical infrastructure continues to rise. The Cisco 2014 Annual Security Report released earlier this month indicated a 14 percent year-over-year increase from 2012 in cyber attacks and malicious traffic. The report further stated that while energy, oil & gas, pharmaceutical, chemical, electronics manufacturing remain prime targets; attacks in the mining, and agriculture have escalated. The report stated that a decline in customer confidence in product integrity contributed to an erosion of trust in the ability of providers to ensure security.

As safety and security become more inextricably linked, the need to ensure trust in safety devices increases exponentially. UE has made its One Series Safety Transmitters "hack proof," to help ensure cyber security. As a safety-only device, the transmitter is not integrated with distributed control systems nor does it utilize bi-directional communication or allow wireless connectivity. Digital integration with host systems is not required as transmitter health status is communicated via the display, analog signal, and status outputs.

Conclusion

ARC believes the best way to reduce risk in an industrial facility is to design inherently safe processes. Realistically, accidents can never be totally designed out of systems, but they can be managed. As the process industries become more proactive than reactive in ensuring safety, device reliability becomes a priority. ARC expects owner/operators will take advantage of new technologies and approaches to make plants safer. For plants with existing SIS systems, it is likely to be far more cost effective to choose an upgrade path that utilizes many of the existing system components.

IAW (I Am Working) is a registered trademark of United Electric Controls.

For further information or to provide feedback on this article, please contact your account manager or the author at phollywood@arcweb.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.