UNITED ELECTRIC CONTROLS

LEADERS IN SAFETY, ALARM & SHUTDOWN

ViewPoint

The Safety Case for UE's One Series Safety Transmitter

UE's multi-functional Safety Transmitter adds diversity, independency and/or physical separation while providing breakthrough diagnostic coverage. Accelerated use of Independent Protection Layers can be adopted to provide added risk reduction and SIL achievement.

Keywords: SIS, SIL, Safety, Proven in Use, IEC 61511, IEC 61508, One Series Safety Transmitter

By Channing Reis - Sr. Regional Manager

Introduction

UE's multi-functional Safety Transmitter adds diversity, independency and/or physical separation while providing breakthrough diagnostic coverage. Accelerated use of Independent Protection Layers can be adopted to provide added risk reduction and SIL achievement. It can help diminish the Beta factor where traditional voting mechanisms are employed and it is effective across multiple layers of protection wherever process safeguards are in place, including SIS.

Issues

If you are a manufacturer of certified products like United Electric, one approach in presenting your product is to build a "Safety Case" that matches-up your product's attributes with what the standards say shall be done in order to comply. For example, IEC 61511 (Functional Safety –Safety Instrumented Systems (SIS) for the Process Industry Sector) says "diversity and physical separation" are preferred techniques for reducing common cause, common mode and dependent failure in Safety Instrumented Systems. Devices of similar design and construction, similar performance characteristics, and requiring similar proof and validation tests, pose a risk of simultaneous hardware and systematic failure extending to all instrumented functions in a process plant. I call this the "Achilles Heel" of Instrumented Protective Systems. It is a risk within and between all layers of protection, and is a problem not easily solved by simply adding redundant similar devices (as with process transmitters.)

In the Instrumented Protective Systems (IPS) world, process transmitters for a long time have been the only game in town when it comes to measuring devices. Most brands have similar characteristics, supplying a mA output in response to process changes. Process transmitters are dependent on the logic solver (PLC/DCS) for their functionality including power, diagnostics, safety variable output and ultimately the speed of response of the safety system either to process changes or fault detection. One could argue that process transmitters and PLCs have a mutual dependency (some would say over dependency) that adds common stress on all process safeguards across multiple layers of protection.

Redundancy can maximize availability of the process and safety system, but it leaves safety designers scratching their heads on how to reduce common cause, common mode or dependent failure. For that, diversity, independency or new systematic capability needs be introduced.

What would the introduction of a more diverse, independent and systematically capable architecture look like? In building our safety case, we try to demonstrate how our Safety Transmitter offers a breakthrough in all three of these areas.

Design & Construction

The design and construction of the One Series Safety Transmitter follows the requirements of the latest IEC 61508, ed. 2.0, 2010 standard which is substantively different than the first issue of the standard back in 2000. The updated version imposes a new level of traceability on the design process. It adds more robust EMC/EMI requirements. It spared no detail in requiring diversity and redundancy at the board or "element" level. This de-

composing of the safety sub-system right down the IC chips, board layout and sensor signal processing is recognition of the power of the "synthesis of elements" concept – the idea that reliability is built by aggregating and measuring the performance of discrete components. It represents another considered approach to root out weak links in safety instrumented systems.

The meaning to owner/operators and their safety designers is that they can have even greater confidence in hardware assessed under the latest IEC 61508 standard anywhere that hardware is used across the layers of protection in a plant. And, there are many: Safety Controls, Alarms, Interlocks (SCAI) includes not only SIS, but subsets of Safety Alarm, Permissive, Safety Critical Control, Safety Interlock, Emergency Shut Down and Detection & Suppression (see ISA 84.91.01-2012.)

The rigor in the new IEC standard shows up in the quantitative measures that assessors use to relate probalistic failure. UE's new Safety Transmitter has a Safe Failure Fraction (SFF) (98.8%) (See Table 1) which is now the highest among manufacturers of generic or safety certified transmitters for pressure, differential pressure and temperature. This reliability metric is an expression of how capable the device is in detecting faults using automatic, self-diagnostics. Assuming a product has been assessed to the new standard, it's a figure quants can trust. The first issue of IEC 61508 allowed SFF percentages to include failures that placed no demand on the safety system. This had the effect of "buffing up" the numbers for many process transmitters certified under the old standard. IEC 61508, ed. 2.0, 2010 eliminates those "no consequence failures" making the up-to-date SFF's all the more accurate and impressive.

Type B Complex Devices

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
<60%	Not	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

Table 1

The advantages can be summed up in two words: safety and availability. Proof tests can be more strategic, more efficient and less wasteful of the time and attention of O&M personnel, a major potential contributor to safety and productivity. Let the self-diagnostics do the work. Validate health and stability based the robust diagnostic software and circuitry which is scanning for faults and out-of-spec parameters every six seconds. Other manual efforts to validate health, stability, accuracy and operability are a waste of time because our unit is already doing the work.

Not all devices provide this level of assurance. A review of the Failure, Mode, Effects and Diagnostic Analysis (FMEDA) of several well-known brands of process transmitters shows SFFs that are considerably lower than UE's new Safety Transmitter (lower still when you strip out the "no consequence" failures.) The FMEDAs also report a metric called "Internal Fault Detection Time (worst case)" For some of the best known and most widely applied process transmitters, this can range from 30 seconds to <1 hour. This is a long time to report a fault! (e.g. loop power compliance, frozen impulse lines, over range, etc.) UE's Safety Transmitter reports faults in 6 seconds, worst case.

With the enhanced hardware reliability and systematic capability of UE's new Safety Transmitter, proof testing could evolve to a simple visual inspection. In other words, if you can be confident that the device ain't broke, there is neither need nor good reason to fiddle with it.

What It Does

The “what it does” (of our device) is unique as it supplies both analog and digital outputs. Each of our (4) outputs is assessed as a “Safety Variable” which gives designers new flexibility in building the output architecture of a safety instrumented or other protective system. For example, the signal going back to the PLC/DCS can be a digital input based on a programmed set point value, say 800 psig. The device is doing the translation of the process variable and telling the PLC in 100 mS or less. Sticking with this example of using a single UE Safety Transmitter, the designer can now add the device’s analog, 4-20 mA output, sending the current signal back to the PLC to add redundancy or another alarm or trip point. The UE Safety Transmitter will not eliminate the need or desire for redundant voting mechanisms, but its unique diversity and redundancy can provide designers with a significant contribution to SIL Achievement through higher Risk Reduction Factors, smaller Beta factors and lower PFDavg across the entire system.

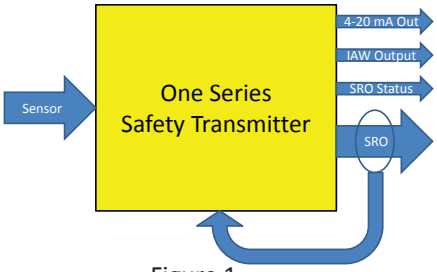

Figure 1

The UE Safety transmitter provides more than primary and redundant signals to the PLC. It has an on-board Safety Relay Output (SRO) rated 5A @ 250 VAC which can provide a high speed trip to a final control element at a programmed value. (See Figure 1) The introduction of this attribute allows designers to create Independent Protection Layers (IPLs) where the SRO acts directly on the actuator, relay or a start/stop circuit to control a final element like a valve or pump, without processing the trip signal through the PLC. All the while, the PLC can be informed of the trending or the action of the SIF via the device’s other analog or digital outputs.

This diversity, independence and physical separation are exactly what the standards encourage in order to reduce the common stress on the SIS. The processing time of our digital outputs is significantly faster
(typically ~60mS) which can mean the difference between a safe trip and a destroyed piece of rotating equipment such as a compressor or pump, the propagation of an environmental hazard or risk of injury to personnel. The UE Safety Transmitter is powered via the analog loop or independently with an external 24 VDC power supply if physical separation from on the PLC/DCS is necessary or desirable.

An example is the need in SIL 1 and SIL 2 remote, unmanned locations where a suitable protection may mean building an entirely redundant SIS with cabinets, PLC’s and redundant sensors. UE’s Safety Transmitter eliminates that need because of it can serve both sensor and logic solving functions out of the box.

Systematic Capability

Of course, we cannot ignore the issue of human capability in the adoption of new devices. Designers are faced with providing solutions that can be implemented and realized. In this area UE delivers what it has always delivered in its products: simplicity. This is perhaps best illustrated by comparing the weightiness of product & Safety Manuals: UE’s One Series Safety Transmitter product & Safety manual totals (40) pages in length. In contrast, one well-known brand of process transmitter has a product & safety manual supplement totaling some (240) pages.

from UE.

Summary

UE's Safety Transmitter can provide all this – 4-20mA output, soft programmable alarms or a hard, fast-acting safety relay output while providing breakthrough diagnostic coverage. The device adds diversity, independency and/or physical separation when it's needed and wanted or serves the role of a simple, affordable, certified transmitter for pressure, differential pressure or temperature. It makes possible the accelerated use of Independent Protection Layers to provide added risk reduction and SIL achievement. It diminishes the Beta factor where traditional voting mechanisms are employed. Last but not least, it can be highly effective migrating across multiple layers of protection wherever process safeguards are in needed including SIS.

More expensive process transmitters (typically $2x cost) cannot perform at this level. The devices certified under the older IEC 61508 standard are effectively "legacy systems" as far as IEC 61511 is concerned. But our Safety Case is not built on this basis. The real measure is embodied in the design, performance and systematic capability of our product, and the flexibility it provides to safety designers. State of the art safety critical elements challenge the status quo by introducing new architectural solutions for SIF at less cost.

To learn more about this topic and United Electric Controls (UE) capabilities, please contact the author at creis@ueonline.com or see us at ueonline.com.