WHITE PAPER

Simplifying Plant Safety Instrumentation

UNITED ELECTRIC CONTROLS

www.ueonline.com

Simplifying Plant Safety Instrumentation

Safety implementation typically is done by a group that includes plant instrument engineers and technicians, who are charged with finding simple and reliable solutions. Often, these situations involve the question of when to shut a process down. Such decisions frequently hinge on key process variables such as flow, level, temperature and pressure. These must be in a specified range at various locations within chemical and petrochemical plants, refineries and power plants, including everything from critical process vessels to eye wash stations.

For such point safety applications, a properly designed and implemented digital switch with self-diagnostics can be an important part of the answer. As an element of a multiple technology solution, a digital switch-based approach can help eliminate common-mode failures, significantly improve response time, achieve needed safety integrity levels (SILs), and simplify plant safety instrumentation.

Switch background

Years ago, many switches were blind mechanical devices actuated electromechanically or by pneumatics. They offered no indication of reliability, such as success or failure in response to a command. This lack of feedback was particularly worrisome in safety applications. The result could be catastrophic, should a malfunction occur in place of the proper response to a tripped pressure or temperature alarm.

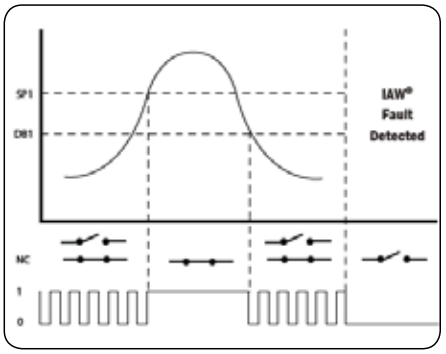
Partly because of this possibility, there has been a general trend toward other solutions. In particular, one popular implementation has been to use a transmitter together with a dedicated control system, one that is separate and distinct from the basic process control system. A benefit of this approach is that transmitters can convey a great deal of relevant process information, which can be useful for safety, control and process optimization. This technology also ensures that connections are active and the transmitter is working, two critical requirements for any safety application.

In such setups, transmitters provide continuous process data, and an alarm or protection system acts upon this information. Informal surveys have shown that somewhere between 25 and 33 percent of transmitters today are in such loops. Thus, nearly a third of the time, the result is a point safety solution offering binary, on-off action at the control room that is effectively equivalent to what had been provided by a traditional switch.

While transmitters have been evolving, switches have been undergoing their own revolution. Switches now are digital, with programmable set points and deadbands. They offer such capabilities as self-diagnostic solid-state electronics, plug port detection and nuisance trip filtering. They also have fail-safe-open programming modes that eliminate the problem of undetected failure.

An example of how this capability can be implemented is found in United Electric Controls' One Series of digital pressure and temperature switches. When conditions are normal, the switch pulses at 20 Hz between a 1 and 0, sending a continuous heartbeat signal easily detected by a controller. A process upset will be marked by closing the switch and the output of a continuous 1. If

the instrument detects a fault, the switch opens and the output drops to a steady 0, the same result as is the case for a wiring fault. In this arrangement, both success and failure are clearly indicated.



a. When process and instrument conditons are normal, a pulsed output indicates so.
b. When a set point is reached, the switch closes.
c. As conditons return to normal, pulsed output resumes
d. A detected instrument fault causes the switch to open and stay open.

Voting for an improved Safety Integrity Level

Digital switch technology also satisfies requirements needed to achieve a given SIL, which is a measure of the relative risk-reduction provided by a safety function. As defined by the International Electrotechnical Commission's standard IEC EN 61508, SIL includes both a hardware and system component. On the hardware side, integrity is determined by a probabilistic analysis of the device, with particular SIL ratings shown in the table below for discrete or low demand operation.

SIL	Probability of failure on demand	Risk reduction factor
1	0.1-0.01	10-100
2	0.01-0.001	100-1000
3	0.001-0.0001	1000-10,000
4	0.0001-0.00001	10,000-100,000

In the case of high demand or continuous operation, the following table applies.

SIL	Probability of failure on demand	Risk reduction factor
1	0.00001-0.000001	100,000-1,000,000
2	0.000001-0.0000001	1,000,000-10,000,000
3	0.0000001-0.00000001	10,000,000-100,000,000
4	0.00000001-0.000000001	100,000,000-1,000,000,000

Determining the SIL for a system is a multi-step process. It begins with a rigorous risk analysis of the system, followed by calculations with the SIL, or preferably raw failure probability data, for the devices determined to be in the critical path. From that an overall reliability figure is determined, which then yields the system SIL.
Knowing this provides methods needed to achieve a given SIL. For instance, a voting scheme involving three SIL 2-compliant components can lead to a SIL 3-system, as demonstrated by the following:

Probs=Prob1 x Prob2 x Prob3

where Probs is the probability of system failure in a voting scheme based on independent components and Probx is the probability of component x failing

Since the ratio of one SIL to another is 10:1, three component voting raises the system SIL from one level to the next. It also is the minimum number of components needed to break ties.

Point safety applications

So what are some of the applications that demand a given SIL and a point safety solution? Examples can be found in processing plants, transportation and worker safety.

The first group involves active processing, with instances found in chemical and petrochemical plants, refineries, and oil and gas facilities. In such situations, there is at least one, and possibly several, critical process vessel, in which a reaction occurs that must be monitored for level, flow, pressure, temperature, or a combination of these.

In petrochemical refining, for example, incoming crude oil undergoes distillation with the output processed through an isomerization unit to alter its structure before emerging as a fuel. Isomerization often involves heating product in the presence of a catalyst, such as platinum or another metal. The combination of heat and a chemical reaction can spiral out of control, ruining product and possibly leading to an explosion. The same is true for the sulfur removing hydrotreater units found in multiple places within a refinery. Thus, the temperature and pressure must be monitored at many locations, and, if need be, the process stopped.

A second set of applications involves transportation or storage of flammable materials. Examples can be found in grain elevators and power plant coal dust conveyors. In the first case, grain must be moved into and then within a structure, which is accomplished by a grain elevator. However, any fine airborne suspension of organic material is combustible. For that reason, stones and metallic fragments are removed before grain is transported or milled. Still, the elevator itself can be a source of heat or sparks. Thus the temperature within the mechanism has to be monitored and transport halted if dangerous conditions develop. The same situation prevails in power plants or other facilities with coal dust conveyors. If a conveyor bearing or roller begins to overheat and the safe threshold exceeded, this must be detected and the conveyor shut down.

An example of a final application category can be found in eye wash or safety stations. These are installed to ensure worker safety and must function flawlessly when needed. Consequently, it is critical that the wash solution be cool enough not to scald and warm enough not to freeze. These stations are situated in industrial settings, where temperature extremes are possible. Thus, a method to monitor the situation and signal a critical alarm is important, in the event that the wash temperature is too high or low.

Considerations

As these examples show, there often is a requirement to monitor and react to critical process variables, such as temperature and pressure. In implementing a solution, engineers should keep in mind that multiple technologies are better than one, speed can save, and that safety systems must be independent of the basic process control system.

The first point is important because multiple technologies avoid common-mode failures. Take the case of a transmitter-controller loop versus a switch. The former will suffer from the potential of a common-mode failure due to the reliance on a possibly distant controller for action. Because it is self-contained, the switch continues to work regardless of what happens to some other component.

A switch is also significantly faster. For instance, the One Series has a response time of less than 60 mS, five times better than what can be done with a transmitter. Any time savings can be crucial in preventing or mitigating an unsafe condition. The self-contained nature of a switch also ensures that the safety system can be independent of the control system. A switch will take its own readings of temperature and pressure, for example, and then react in response to its own programming.

However, it is important that this independence not be total. That is, any safety instrument must be able to report on its own condition and interface with the rest of a plant network. In the case of the One Series, this is done through self-diagnostics that allow extensive fault detection, including plugged ports and power supply out-of-range conditions. It also offers multiple outputs, with both a switch function and a 4-20 mA analog output. Finally, it reports faults locally on its own display and remotely via multiple outputs.

A final and imperative consideration for any technology involves determining the SIL rating for an entire system. As discussed earlier, the use of voting can allow SIL 2 components to create a SIL 3 system. In such arrangements, a critical piece of information is independent verification of safety ratings. Part of such verification will include failure modes, effects and diagnostics analysis. FEMDA data is part of the IEC EN 61508 certification and can be used in calculating overall system SIL.

Conclusion

As has been shown, advances in technology have made switches capable of monitoring temperature and pressure while conducting self-diagnostics, thereby removing the perils of blind mechanical action. These developments constitute good news for engineers who today want to simplify instrumentation in point safety applications common in petrochemical plants, coal dust transportation, critical line or vessel protection, or eye wash safety stations. Such switches offer improved solutions through avoidance of common mode failures, faster response times, independence from basic process control systems, and the ability to achieve desired SIL via a voting scheme.

###