

Critical Transmitters Improve Plant Safety and Reduce Costs

Paul Gruhn, P.E.
Safety System Specialist
Moore Process Automation Solutions
Houston, TX 77054
gruhnp@mpco.com

Abstract:

Safety instrumented (or interlock) systems (SISs) are designed to monitor a process for hazardous conditions and bring the process to a safe state if certain conditions are violated. Such systems consist of sensors, a logic box, and final elements (e.g., valves). In recent decades numerous companies have developed PLCs (programmable logic controllers) specifically for critical safety applications. While such improvements in logic box performance are certainly beneficial, a chain is only as strong as its weakest link. Improvements in field devices are also required. The primary criteria for safety related devices is *high diagnostics*.

This paper describes the limitations of certain sensors and configurations in safety applications, along with the benefits that may be achieved using a sensor designed from the ground up with very high levels of internal self-diagnostics.

Why Transmitters?

The traditional technology used for the logic solver portion of SISs was relays. The most appropriate sensor technology to match up with relays was discrete switches. While properly designed relays could be considered fail-safe (i.e., the likelihood of the relay contacts failing closed was minimal), the same could not be said of sensors. In other words, a pressure switch could just as likely fail closed as open. This represents a ‘dangerous’ failure, as the system will not respond when required. Non-redundant relay logic system can meet the highest safety requirements as defined in industry standards such as ISA, IEC and the AIChE. This is not the case for simplex field switches.

Many companies have replaced relay logic systems with programmable systems, such as PLCs (programmable logic controllers) and specialized redundant safety PLCs. While discrete switches can still be used with these systems, analog transmitters offer a number of benefits primarily in the form of diagnostics. Since a transmitter provides a dynamic, changing signal, it is easier to tell if the device is working properly. Unfortunately though, not all failures can be detected automatically.

Common Transmitter Problems

One common problem with transmitters occurs when extra resistance is added in the field cabling. When this occurs the transmitter is no longer able to overcome the added resistance and it cannot generate the appropriate output current. This also happens if the power supply begins to fail and goes to a voltage below its nominal value (ie 24Vdc degrades to 18Vdc). Another problem occurs when the internal circuitry, such as the analog to digital converter, fails ‘stuck’

(i.e., holding a certain value). Most transmitters cannot recognize these sort of problems. In fact, Moore has analyzed their standard pressure transmitter and found the diagnostic coverage level (i.e., the percentage of internal failures the transmitter can recognize automatically) to be around 35%. In other words, 65% of possible failures would remain undetected. (Note that estimating numbers such as these requires detailed analysis – it should not be based on a SWAG (Scientific Wild A** Guess).)

What is a Critical Transmitter?

The primary differentiating factors for a critical transmitter are a) diagnostics, b) redundancy and c) diversity.

Standard transmitters have diagnostic coverage factors ranging between 30 and 50%. The critical transmitter is certified by outside agencies as having over 98% diagnostic coverage. This is accomplished through both diverse redundancy and extensive self-testing. Dual, diverse components running diverse operating routines (e.g., A/D converters) provide a method of detecting whether any single component has failed. Reading back output currents and comparing them with the driving signals can test for power supply [problems](#) or [load resistance problems](#).

If internal failures are detected, the critical transmitter is designed to fail producing an output current of 3.7 mA. This failure range is defined in an international standard. The control system can detect this particular range and perform any predefined action (e.g., ‘hold last state’).

Performance Terms

In order to make comparisons of different systems, one must first have a meaningful way to measure system performance. (After all, if you can’t measure it, you can’t manage it.)

Safety systems may fail in either of two manners. They may suffer, or initiate, a nuisance trip and shut the plant down when nothing is actually wrong (generally called a ‘safe’ failure), or they may suffer an inhibiting, fail to function (or ‘dangerous’) failure, and fail to respond to an actual shutdown demand.

Nuisance trip performance

Many are familiar with the term ‘availability’ (uptime / total time). In terms of nuisance trip performance, what does an availability of 99.9% tell us? The number sounds good, but what does it *really mean*? A system that initiates a nuisance trip once a month, and is down for 40 minutes, has an availability of 99.9%. But, so does a system that initiates a nuisance trip once per year, but is down for 9 hours. And, so does a system that initiates a nuisance trip once every 10 years, but is down for 90 hours.

The term used in the ISA S84 standard for performance in this mode is MTBF_{sp}, or Mean Time Between spurious Failure (also called the nuisance trip rate). The difference between a system that causes a nuisance trip once every 6 months, versus once every 6 years, 60 years, or 600 years is readily apparent. Most users know how long their process will be down if such an event happens, they just want to know how *often* it might happen.

Safety performance

Different people use different terms for the safety performance of SISs. The ISA, IEC and AIChE documents use the concept of ‘safety integrity levels’ as a means to relate the required

safety system performance to the level of risk inherent in the process. Essentially, the greater the process risk, the better the SIS needed in order to control the risk. Table 1 summarizes the requirements using several terms which can all be directly related to one another.

Integrity Level	Safety Availability	PFD (Probability of Failure on Demand) 1 - S. Availability	RRF (Risk Reduction Factor) 1 / PFD
4	> 99.99%	< .0001	> 10,000
3	99.9 - 99.99%	.001 - .0001	1,000 - 10,000
2	99 - 99.9%	.01 - .001	100 - 1,000
1	90 - 99%	.1 - .01	10 - 100
0	Process Control - Not Applicable		

Table 1: IEC and ISA Performance Requirements

Note:

1. These numbers are intended to include the *entire system* (i.e., sensor, logic box, and final element).

Costs of Ownership

The purchase price of a transmitter is in the range of \$1,000, yet the *total* costs of ownership are much higher.

Users have reported that the initial installation for a transmitter in a new application can exceed \$8,000. This includes costs associated with design, drawings, permits, conduit & wire, labor, testing, etc.

Field devices must be periodically manually tested. A very common test interval is 1 year. The actual duration of testing a single transmitter can approach one hour when including all factors such as preparation, actual testing, documentation, etc. Assuming a labor rate of \$30/hr and a 15 year sensor life, total testing costs come out to \$450 per sensor (excluding such factors as interest, inflation, etc).

Therefore, the total ownership cost for a single transmitter can be estimated at \$9,450. This excludes such factors as lost production downtime, time value of money, etc. One could obviously include such factors, but the number of assumptions might be considered questionable for a simple, generic analysis.

One could assume the cost of a simple switch (in lieu of a transmitter) at \$200. Overall installation and testing costs would be similar, so the total overall cost of ownership over a 15 year period would be \$8,650.

For redundant transmitter arrangements, one can simply double or triple the installation costs, purchase price and testing costs (assuming both the critical transmitter and redundant transmitter arrangements are still be tested yearly). The critical transmitter has approximately a 35% higher initial purchase price. Total costs are summarized in Table 2.

Sensor Arrangement	Nuisance Trip Rate (years)	Risk Reduction Factor	Total Cost (\$)
Simplex Switch	100	200	8,650
Simplex Standard Transmitter	100	400	9,450
1oo2 Standard Transmitters	47	38,000	18,900
Simplex Critical Transmitter	100	9,000	9,800
2oo3 Standard Transmitters	1,000	170,000	28,350
1oo2D Critical Transmitters	1,000	170,000	19,600

Table 2: Summary of Performance and Cost

Notes:

1. A single sensor (or set of sensors) is assumed for both the nuisance trip rate and the risk reduction factor calculations. (MTBF = 100 years in both the safe and dangerous modes.) Logic box and final elements are not included in the modeling.
2. A standard transmitter is assumed to have 50% diagnostics, a critical transmitter 98%.
3. Dual standard transmitters are assumed to have 95% diagnostics (through comparison).
4. Triple standard and dual 1oo2D critical transmitters are assumed to have 99% diagnostics (through comparison).
5. Redundant devices are assumed to have 10% common cause related problems (i.e., a single failure effects multiple devices).
6. Performance calculations assume yearly testing and an 8 hour repair time.
7. Costs associated with lost production downtime (due to nuisance trips) are not included in the total costs.

Conclusions

Simplex discrete switches are unable to meet SIL 2 performance requirements (when including logic and final element portions of the system).

Depending upon the assumptions, standard transmitters offer questionable performance for SIL 2 (especially when including logic and final element portions of the system). In addition, no standard transmitters are independently certified for this level of performance. Differences in total costs between a discrete switch and a standard transmitter are negligible.

Dual 1oo2 standard transmitters offer safety performance appropriate for SIL 2 or 3, but at twice the cost of a single transmitter. (For just 20 sensors the benefit comes at a price of approximately \$180,000.) Such an arrangement is not attractive however due to the increase in nuisance trips (i.e., lost production downtime and increased risks associated with unnecessary shutdowns and startups).

Simplex critical transmitters are *certified* for SIL 2 performance, and offer an improvement in safety of one order of magnitude vs. a standard transmitter, all for the same overall cost as a standard transmitter. (Compared to the 1oo2 standard transmitter arrangement presented above, 20 simplex critical transmitters represent a *savings* of \$180,000!)

Triplicated standard transmitters or dual 1oo2D critical transmitters offer the highest nuisance trip and safety performance. (The 1oo2D critical transmitter however, is *certified* for SIL 3.) The 1oo2D configuration however, represents a potential total cost savings of approximately \$10,000 per sensor set. For 20 sensor sets, this represents a potential *savings* of \$200,000!

Author bio:

Mr. Gruhn is a Safety System Specialist with Moore in Houston. He is a senior member of ISA, a member of the ISA SP84 committee (Application of Safety Instrumented Systems for the Process Industries), the developer and instructor for ISA's 2-day class on safety shutdown systems (EC50), a co-author of ISA's textbook on Safety Instrumented Systems, and the developer of a commercial software package for evaluating different control and safety systems. He has a B.S. degree in Mechanical Engineering from Illinois Institute of Technology in Chicago, Illinois, and is a Licensed Professional Engineer in Texas.