

Selecting Transmitters for Safety Instrumented Systems

Stephen R. Brown
Control Systems Engineer
DuPont Fluoroproducts
Parkersburg, WV 26102

Mark Menezes
Manager – Pressure & PlantWeb (Americas)
Rosemount Inc.
Chanhassen, MN 55317

KEYWORDS

Safety, availability, transmitters, IEC, proven-in-use, safety integrity level, common cause, diagnostics

ABSTRACT

Users design safety systems to mitigate the risk of identified process hazards within tolerable levels, using application-specific risk models, defined user inspection schedules, and safety data for the devices under consideration. Some suppliers provide safety data for their devices. However, supplier data, even when validated by a third party, reflects laboratory results, and can be an order of magnitude too aggressive for field devices. “Proven-in-use” data includes real-world failure causes; however it tends to be conservative, since it must cover the whole range of the category, from 20-year-old pneumatics to the latest smart technology. Moreover, proven-in-use data is often aggregated for a given technology: for example, “pressure transmitter = dangerous failure rate of once in 50 years”. This aggregate data often does not isolate failure causes, so it does not allow users to take credit for improvements in technology or user practices intended to minimize the impact of specific failures. The net result to the user can be over design, over-testing, increased spurious trips and needless capital expenditures.

This paper will present recommended “best practices”, which allow the user to quantify the impact of real-world failure causes, and take credit for improvements in system design. This will improve safety and availability, and minimize life cycle cost.

STANDARDS AND TERMINOLOGY

The process industries are leading the charge to adopt existing and emerging standards that define methodologies for documenting system safety and availability. These standards include ANSI/ISA S84.01 and draft standard IEC-61511 for end users, and IEC-61508 for manufacturers. Although the focus of this paper is on selecting and maintaining transmitters, this cannot begin until the user first determines the required level of risk mitigation for each particular safety instrumented function (SIF). The user should consult other sources for details of this methodology¹, which determines the safety required - “safety integrity level (SIL)” - for each individual loop, or “safety instrumented function”.

Once the SIL requirement for a particular loop is determined, the user selects and maintains sub-systems, including logic solver, control valve(s) and transmitter(s), to achieve the loop/SIF SIL. Again, this methodology is well documented². Generally, improving the safety of the least-safe devices will have the most significant impact on overall loop risk reduction. Where measurements significantly impact loop safety, steps should include:

- Replace discrete switches with **transmitters**.
- Improve common cause **strength**
- Use **diversity**
- Use **diagnostics**
- Add **redundancy**

Each of these steps can include improvements in technology and/or user selection, installation and maintenance practices. For example, to improve resistance to the common cause of high ambient temperature, the user can purchase more robust transmitters (strength), install the transmitters further away from the hot environment (practices), or employ transmitters or software which might predict impending failure due to high temperature (diagnostics). Where redundancy is justified, the user should choose a backup technology that is more resistant to high temperatures (diversity).

Each approach can involve tradeoffs between safety and life-cycle-cost. For example, a user who upgrades an existing transmitter with one that is more stable will, for a fixed calibration/test interval, improve safety. Alternatively, the same user can choose to lengthen the calibration/inspection interval, with no sacrifice in safety. The key is to maximize “**Safety-ROI**” with upgrades to technology and practices that yield the largest improvement in safety, with the smallest increase in life cycle cost.

To determine measurement safety, some users rely on data provided by suppliers, usually validated by independent third parties such as FM and/or TÜV. This data includes the impact of strength, diversity and diagnostics, but in a laboratory environment. For control systems, this laboratory safety may provide a useful predictor of real-world **installed safety**. However, it has been the experience of the authors that, for field devices such as transmitters, real world installed safety is always much worse. Only by quantifying installed safety can users evaluate the real world safety and life-cycle-cost impact of specific technology and user practice alternatives.

EVALUATING INSTALLED SAFETY FOR TRANSMITTERS

Why does laboratory safety predict installed safety for a logic solver, such as a control system, but not for a field device, such as a transmitter? A covert failure for a measurement occurs when the loop is operating in an unsafe condition, yet the transmitter shows the loop to be operating safely. In rare cases this can be caused by software or electronics - quantified during a laboratory safety evaluation. In most cases, the authors have found that measurement covert failures are caused by:

- **Transmitter performance:** Can uncertainty in the measurement - caused by poor installed repeatability – exceed the safety margin?

- **Process interfaces:** What is the likelihood that pressure transmitter impulse lines will plug or freeze, or the RTD thermowell will coat? What is the likelihood that the shedder bar or sensor for a vortex flowmeter will coat?
- **Transmitter and sensor robustness and quality control:** Corrosion and hydrogen permeation can eventually cause overt failure of a pressure transmitter. However, for a period of time leading up to this failure, the measurement will suffer a gradual, covert drift.

For DP transmitters, a rapid and severe over-pressure can cause a zero shift, which is covert and detected only during calibration/inspection. Unfortunately, many over-pressures occur when the technician does not correctly equalize line pressure during re-installation *after* calibration, so this error may not be detected until the *next* calibration/inspection.

For a magnetic flowmeter, abrasion of the electrodes can initially cause noisy flow measurement, and ultimately complete electrode failure, yielding an onscale low flow reading.

- **Selection, installation and maintenance practices:** Can an engineer specify an uncompensated differential pressure or vortex flowmeter in a gas or steam application with widely varying fluid density? Can an incorrectly installed grounding strap cause a magnetic flowmeter to provide a noisy flow measurement? Can the same technician calibrate all transmitters using a biased reference?

QUANTIFYING COMMON CAUSE STRENGTH - INSTALLED REPEATABILITY

All users operate their hazardous processes with a safety margin between normal operation and where the hazard can occur. How can the user determine if the uncertainty associated with a given measurement will exceed this safety margin? Consider, for example, a DP transmitter with “0.1% reference accuracy” installed on an orifice plate – will the complete measurement system provide 0.1%, 1% or 10% flow repeatability? The first step is to identify factors that will cause a transmitter to be less accurate and repeatable outside of a laboratory. For a DP transmitter, key factors include:

- **Ambient Temperature Variation:** In the vast majority of “real-world” flow measurements, the transmitter can operate at a very different ambient temperature than the one at which it was calibrated. These variations can have a significant effect, which is easily simulated on the bench – blow warm air over a transmitter, and watch its output change.
- **High Static Line Pressures:** The DP transmitter used to infer flow could be significantly affected by a high line pressure. To simulate this effect on the bench, the user should apply a small DP across a transmitter. Then, add several hundred pounds of additional static pressure to *both* sides of the transmitter. In theory, the measured differential pressure should not change. In reality, it does.
- **Drift/Stability:** The output of any analog component will vary over time. As with the ambient temperature effect described above, this can affect all flow technologies. Better, smart transmitters are more stable, requiring less frequent calibration than older, analog transmitters or transducers, without any sacrifice in accuracy and repeatability.

Next, quantify the impact of these real-world conditions for the given application and transmitter of interest, using specifications published by the supplier. While these errors may seem small at 100% flow, since the errors are fixed over the entire transmitter range, and $DP \propto \text{flow}^2$, small errors at 100% - and small differences in transmitter accuracy - are **magnified** at lower flowrates, as seen in Figure 1.

<u>Flowrate (scfm)</u>	<u>DP (inH2O)</u>	<u>"Better" .075%</u>	<u>"Worse" .075%</u>	<u>Analog</u>
1000	100	0.09%	0.21%	0.65%
750	50	0.16%	0.38%	1.30%
500	25	0.37%	0.85%	2.60%
250	6.25	1.46%	3.40%	10.40%

FIG. 1 – FLOW ERROR (%) FROM DIFFERENTIAL PRESSURE TRANSMITTER³

Two observations from this typical application:

- Flow applications typically become unsafe at low rather than high flows. If the safety margin is set to less than 10%, at a 25% flow the analog transmitter can either miss a real trip, reducing safety, or cause a spurious trip, reducing availability.
- The “reference accuracy” of the transmitter is not useful for predicting installed repeatability. From Figure 1, when installed the two “0.075%” transmitters differ by nearly 2%.

Software tools are available from suppliers that allow users to quantify installed repeatability for specific transmitters in specific, user-defined application conditions⁴.

MINIMIZING COMMON CAUSE – DIVERSITY

Redundancy is most useful when the backup uses a different technology from the primary, minimizing the risk that a single failure mode will affect both. Of course, the diverse, backup technology should be strongly resistant to the failure modes that affect the primary technology. Consider, for example, an application where the primary is an orifice meter. Plugging of the impulse lines can affect any number of pressure transmitters connected to the orifice plate. To protect against this failure mode, the user might consider using a vortex meter as a backup. However, the vortex meter selected must be immune to coating itself, with a non-clogging design (no ports or crevices). To simplify periodic inspection, the vortex meter’s sensor should be removable without removal of the entire meter body from the line.

Diversity should also be applied to user practices. Ideally, a different technician would specify, install and maintain the primary and backup measurements, to minimize the risk of faulty practices.

DETECTING COVERT FAILURES – PERFORMANCE DIAGNOSTICS

Basic device diagnostics have been available for years to diagnose overt and covert component failures. While these diagnostics provide some value, for most users they offer diminishing returns by making an extremely safe device even safer – how often do users observe *onscale* failures of microprocessors? More powerful diagnostics are now available which go beyond detecting component failures to evaluate the **performance** of the complete measurement system, including common process interface problems that can cause onscale failures. In general, these diagnostics are made possible by the dramatic increases in computing power in modern microprocessors. Surprisingly to many users, most of these diagnostics can only be performed in the field devices themselves, and *not* higher-level expert or “Abnormal Situation Management” systems, because they require extremely high speed, resolution and accuracy.

Specific performance diagnostics have been described in the literature⁵ – some planned, some available in products shipping today - including:

- Pressure: Plugged impulse line detection and prediction
- Pressure-Level: Leaking diaphragm seal detection
- Temperature: Fast, predictable detection of failed RTD or thermocouple, sensor drift
- Vortex Flow: Detection of application changes (viscosity, density, etc)
- Magnetic Flow: Detection of faulty ground or electrodes, high process noise
- Coriolis Flow: Detection of slug flow, tube coating
- pH: Detection and prediction of faulty electrodes

To take safety credit, the user needs to estimate the likelihood of the failure and the effectiveness of the diagnostic. For example, suppose that impulse line plugging causes 50% of dangerous failures for a given pressure measurement, leading to an observed $MTTF_d$ of 50 years. If a diagnostic allows the user to detect this condition 80% of the time, the rate of dangerous failure can be reduced by 40%, with a corresponding improvement in $MTTF_d$ from 50 to 83 years. In the case of redundant measurements, the diagnostic can also improve availability if, after being alerted, maintenance can correct the root cause before it affects the *redundant* device.

To minimize delay due to user response time, a catastrophic fault – for example, failure of an RTD – should cause the transmitter output to immediately fail to a high (>20 mA) or low (<4 mA) state, whichever represents a “safe” condition. Ideally, the transmitter should be configured to fail to some specific off-scale output if it diagnoses a specific fault – for example, “21.4 mA = RTD failed” – which the logic solver would be configured to interpret. For a less severe fault - for example, a partially plugged impulse line – the transmitter should continue to provide a usable output. However, an alert should appear on the transmitter’s local display, and also at an “Asset Management System” (AMS) maintenance terminal. This will ensure safety, while minimizing spurious trips.

The vast majority of smart transmitters used in safety applications use the HART protocol. For this “hybrid” protocol, the process variable to the control system is standard analog 4-20 mA, while diagnostic alerts are communicated via the superimposed digital signal. The AMS strips off the digital information without interfering with the 4-20 mA signal used by the logic solver. Corrective actions made from the AMS are automatically logged, creating an as-found/as-left audit trail. This can simplify

both regulatory compliance and the collection of “proven-in-use” statistics. All-digital “fieldbus” protocols – including FOUNDATION fieldbus and Profibus-PA – are not at present used in safety systems. However, diagnostics in fieldbus transmitters are still worthwhile, as better diagnostic coverage in the process control system – for example, the DCS – can increase the likelihood that a hazard will be contained before it reaches the SIS. This can reduce the required SIL in the SIS.

EVALUATING TRANSMITTER AND SENSOR ROBUSTNESS AND QUALITY CONTROL

Many users attempt to compare and quantify **robustness** and **quality control** for different manufacturers by evaluating designs and the vendors’ professed commitment to concepts such as continuous improvement, ISO 9000, etc. Unfortunately, such comparisons typically degenerate into “dueling slideshows” that are not useful for decision-making. Equally worthless are mean-time-between-failure (MTBF) values provided by suppliers when they are based on “user-reported failures”. Since of course most users do not report all failed transmitters, this inflates MTBF, and actually penalizes suppliers with better customer service and communications. The most useful method is “Highly-Accelerated Life-Cycle Testing” (HALT)⁶ – however, this requires the destructive testing of many transmitters, and is prohibitively expensive for all but the highest-volume suppliers.

Since MTBF cannot be usefully compared, the best predictor of installed reliability is **experience** – in general, Serial #100 of a device will be much less robust and of lower quality than Serial #100,000. The question to the supplier therefore becomes – “how many thousands of devices, or devices of similar design, have been installed in similar applications – and please provide references.”

BEST PRACTICES FOR SELECTION, INSTALLATION & MAINTENANCE

Users try to use “best practices” wherever possible to minimize both overt and covert failures. However, as technology evolves, so do best practices. For example, users historically:

- Installed pressure transmitters with long impulse lines, to facilitate access. Today’s modern transmitters, however, are so much more reliable than older transmitters, that users find that most maintenance is due to the impulse lines themselves. Using short, horizontal impulse lines where possible will reduce maintenance, eliminate hydrostatic head errors and improve dynamic response.
- Balanced capillary lengths for a remote seal system on a pressurized vessel, to “balance out” ambient effects. Experience has shown, however, that the best repeatability, fastest dynamic response and lowest cost are obtained by direct-connecting the lower seal.
- Calibrated all safety-related transmitters on a fixed schedule – for example, every year. Instead, the user should quantify the calibration frequency that will provide the desired repeatability. In some cases, the necessary frequency will be much shorter than one year, in others, much longer.

The user can minimize their risk of sub-optimal selection, installation and maintenance by working with suppliers who can bring to bear substantial measurement expertise and experience, and strong local technical support. The supplier should offer a wide variety of technologies so they can propose diversity

where appropriate. And of course, users themselves should only select devices with which they have their own substantial experience, ideally gained in non-critical process applications.

SAFETY “CERTIFICATION”

Finally - it is important to reiterate that a SIL applies only to a particular SIF – there is no “entity approval”, as with intrinsic safety. The user must calculate risk reduction for the **entire loop**, and combining a logic solver, transmitter and valve – each with “SIL-2” certification – does not ensure a SIL-2 loop. Despite this, some suppliers promote their devices as “certified” to a particular SIL by a third party such as FM or TÜV. It is the view of the authors that a SIL certification for a field device such as a transmitter has little relevance, and may mislead the user into a false sense of security, because:

- As detailed above, the SIL that a transmitter achieves in a laboratory does not predict the measurement’s risk of covert failure under installed conditions. Use of this laboratory failure data may lead to the design of a SIF that in practice has a lower SIL than required.
- A transmitter is only one component – SIL must be calculated for the entire loop/SIF.
- Most importantly – to achieve certification, some suppliers have developed entirely new devices, which have not been extensively proven in the field by either suppliers or users.

When reputable suppliers introduce new products, including those that have undergone extensive laboratory and “beta” testing, they recommend users install the devices in non-critical applications so that both user and manufacturer can gain experience and correct “bugs” not discovered in the laboratory. Specifying an unproven device, solely on the basis of favorable laboratory testing - and possibly an impressive slide show - for the most safety-critical applications in a plant contradicts common sense.

CONCLUSION

In conclusion: when selecting transmitters for use in safety instrumented systems, users need to:

1. Follow the guidance provided in relevant safety system standards.
2. Consider and where possible quantify factors that can cause installed safety and availability for transmitters to be worse than expected from laboratory calculations.
3. Select devices, utilize performance diagnostics and apply selection, installation and maintenance best practices to quantify and minimize these real-world factors.

On an ongoing basis, users need to maintain detailed records of the root causes of observed dangerous and safe failures, noting whether the failures were discovered during system testing or normal operation. These records will allow them to take credit for improved technology, diagnostics or practices intended to minimize those specific root causes. This will ultimately improve safety and availability, and reduce life cycle costs.

REFERENCES

1. Guidelines for Safe Automation of Chemical Processes, published by the Center for Chemical Process Safety of the AIChE, provides an example using 2 such methods in chapter 7, section 4.
2. *ibid*, chapter 5.
3. Menezes, "Calculating and Optimizing Repeatability of Natural Gas Flow Measurements", Pipeline & Gas Journal, July 2001.
4. *ibid*.
5. Menezes, "Improve Plant Safety through Advanced Measurement Diagnostics", Chemical Engineering, Oct/2000.
6. Kececioglu, D., Reliability & Life Testing Handbook, Vol. 1, page 191.