contents

Measurement Best Practices for Safety Instrumented Systems

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

Mark Menezes
Measurement Business Manager (Canada)
Rosemount Inc.
Chanhassen, MN 55317

KEYWORDS

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

ABSTRACT

ANSI/ISA S84-1996 is migrating to a new international standard – the IEC 61511. Over the past few years, global CPI and HPI users have started to adopt this new standard, particularly for new installations. From these installations, "best practices" have started to emerge. Some of these, related to measurement, are documented here. The objective is to allow the user to comply with the new standards, while maximizing real-world safety and availability, and minimizing life cycle cost.

INTRODUCTION - STANDARDS AND TERMINOLOGY

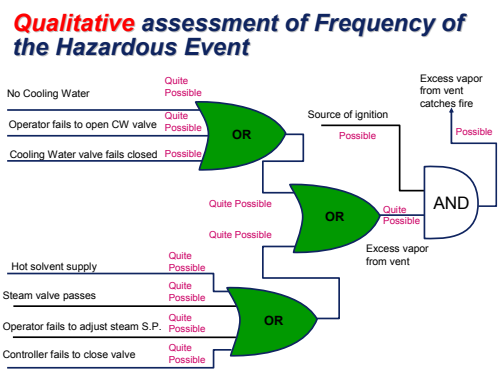
The ANSI/ISA S84-1996 standard has guided North American users for the past decade in designing safety instrumented systems. This standard is migrating to a new international standard – the IEC 61511 – with the new name ANSI/ISA 84.00.01-2004. Even where application of the new standard is not yet mandatory – for example, in jurisdictions governed by OSHA – global CPI and HPI users in particular have already started to apply the new standard to new installations, for three key reasons. First, global users recognize that adopting a single standard at all of their sites provides consistent engineering and maintenance practices, potentially reducing design, procurement and documentation costs. Second, users in most jurisdictions recognize that the standard will eventually become mandatory. For example, OSHA considers the standard to be "Recognized and Generally Accepted Good Engineering Practice" (RAGAGEP). As with the eventual adoption of S84-1996 by OSHA, complying with the standard now will minimize the need for future re-engineering. Finally, the new standard potentially provides users with flexibility to improve safety and availability, while reducing maintenance costs. For example, as will be detailed later, with the right equipment and installation, the new standard may allow the user to significantly stretch out inspection intervals.

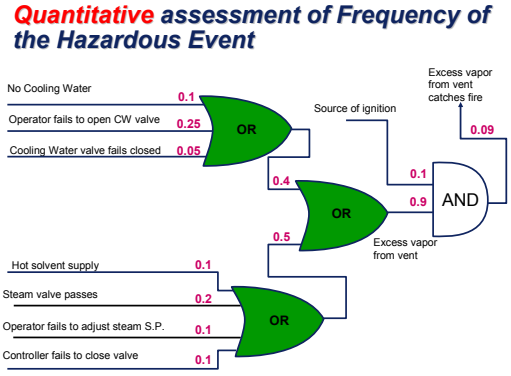
For *existing* safety systems that were designed to comply with ANSI/ISA S84-1996, the new standard includes a "grandfather clause" - "For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issue of this standard (e.g., ANSI/ISA-84.01-1996), the owner/operator shall determine that the equipment is designed, maintained, inspected, tested, and

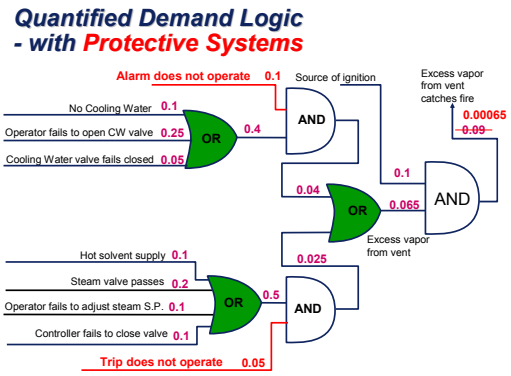
Presented at ISA EXPO 2005, 25-27 October 2005
McCormick Place Lakeside Center, Chicago, Illinois, www.isa.org

operating in a safe manner." The user does not necessarily need to upgrade non-certified logic solvers, transmitters or final control elements that are used in existing safety systems. However, they do need to perform a quantitative analysis of each Safety Instrumented Function (SIF) to verify that it meets the Safety Integrity Level (SIL) required, given the specified test interval.

For both new and existing applications, the need is for the user to take an analysis which in the past may have been mostly or entirely qualitative, and make it more quantitative. For example, in the HAZOPS, the user might define that a failure that was "very likely" has a risk of "0.1 events per year". In the Layer of Protection Analysis (LOPA), the user might need to estimate that the risk of the cooling water control valve used in the basic process control failing to open is 0.05 per year (alternative approaches to LOPA include the safety layer matrix method, and regular and calibrated risk[1]). Finally, the user needs to quantify the risks of dangerous failure of the devices used in the safety system. For measurements, a dangerous failure occurs when the process is operating in an unsafe region, yet the transmitter advises that it is safe. The relevant data is the "Probability of Failure on Demand" (PFD).







Presented at ISA EXPO 2005, 25-27 October 2005
McCormick Place Lakeside Center, Chicago, Illinois, www.isa.org

Methodologies for performing these calculations can be found in other sources[2], and spreadsheets and other tools are readily available from consultants. In practice, the challenge for most users is not in doing the calculations, but in obtaining **useful and relevant data**.

OBTAINING SAFETY DATA FOR MEASUREMENTS

The new standard describes two valid approaches for selecting devices and obtaining device data – the use of "validated/certified" devices, or "proven in use/prior use". Certified devices are designed and manufactured by the supplier to comply with IEC 61508, Section 2 (Hardware) and Section 3 (Software). Before applying the data, the user can either audit the supplier themselves – not usually practical – or rely on an independent third-party, such as Exida or TUV. "Proven in use/Prior use" is described in section 11.5.3 of ANSI/ISA 84.00.01-2004. The user documents operating experience from both SIS and basic process control applications, through the entire life cycle of the devices in question.

There are advantages and disadvantages to both approaches. Using certified devices transfers the burden of calculating and documenting device safety from the user to the supplier. This reduces cost, since the supplier can leverage their efforts and agency costs over many users. This advantage can be particularly important for small users who might not have available resources to perform their own Prior Use analysis. Unfortunately, data for certified transmitters is based on a "white paper" analysis, so it cannot quantify the impact of "real-world" effects. In the real-world, as opposed to the laboratory, there are many factors that can cause a transmitter to read either dangerously high or dangerously low, that might not be detected during normal operation. Some obvious examples include[3]:

- Pressure: plugged sensing lines, power supply variations, hydrogen permeation of diaphragm, severe over-pressure (pressure hammer) causing zero shift, mis-installation causing zero shift
- DP-Flow: eroded or mis-aligned primary element (orifice plate),
- Temperature: coated thermowell, well incorrectly located (so it does not register the peak)
- DP-Level: coated, leaking or deformed remote seal
- Coriolis: tube coating

Other examples can apply to any measurement technology. For example, the user might specify a device whose measurement uncertainty is greater than the "safety margin" – the difference between where the process normally operates, and where it becomes unsafe. Selection, installation and maintenance errors can also affect any technology, though some technologies are more "fool-proof" than others - for example, a flanged vortex meter is less likely to be mis-aligned than a wafer vortex meter.

These risks are application dependent – the risk of line plugging is obviously greater for a dirty application - so must be quantified by the user for each individual application. Also, identifying and quantifying real-world risk is much more important for field devices such as transmitters and valves than for logic solvers. Logic solvers used in SIS applications are typically installed in laboratory environments. In addition, "real-world" logic solver failures – those that appear under installed conditions but not during white paper or laboratory testing - normally manifest as safe failures. So, barring programming errors, real-world dangerous failure rates for logic solvers should be similar to the failure rates documented by white paper analysis.

While "real-world" effects must be separately quantified for each application when using the Certified approach, a comprehensive Prior Use analysis by definition accounts for these potential real-world

effects, since it is based on actual operating results from real devices in real, "similar" applications. The key downside of the Prior Use approach is that it is expensive and time-consuming, and must be done by the user, not the supplier. For smaller users, with a small installed base and limited resources, identifying a sufficient number of "similar" applications can be problematic. Many dangerous transmitter failures are caused by device software and firmware – how many users log this device-specific information when a failure occurs? Is it valid to assume that statistics gathered for an older generation of software and firmware apply to a newer device? Another key challenge is "management of change" – what happens if the user has collected all of their statistics using one version of a particular transmitter, and then the supplier makes a significant design change? The user needs to evaluate the design change, and verify that it will not negatively impact safety.

In practice, users are gravitating towards an approach which combines the best of both the "validated/certified" and Prior Use approaches. In this modified approach, the user starts with third-party validated data from the supplier for a Certified or non-Certified transmitter. This data applies to the hardware and software revision level of the specific device under consideration, and is supplied with a "Safety Manual" that specifies the installation and application conditions under which the data is valid. Then, based on their operating experience, gained from similar applications but not necessarily identical devices, the user de-rates that data to account for expected real-world effects.

Common Cause

Using either of the Prior Use or Certified approaches, it becomes apparent, particularly in applications where redundancy is employed, that the transmitter itself can be a trivial component of overall risk. To illustrate why, consider the case of redundant pressure transmitters with a risk of dangerous failure rate of, for example, 0.005 (meaning that if the user had 200 of these transmitters installed in similar applications, on average one would fail dangerously per year). Unfortunately, the two transmitters are connected to the process via a long, common set of impulse tubing, which might plug at a rate of 0.01. The dangerous failure rate of the measurement "system" is then:

$$PFD = (0.005)^2 + 0.01 \approx 0.01$$

In these cases, it is especially important for the user to quantify and minimize risk for the common cause, in this case the impulse tubing. Approaches the user should consider include:

"Best Practices" to Improve **Common Cause Strength** – Best practices evolve with technology. For example, newer smart transmitters allow the user to separate the sensor from the electronics, allowing the sensor to be directly connected to the process, with the electronics located at an accessible location. Obviously, a direct-connected transmitter is less likely to plug than one connected via long, narrow impulse lines.

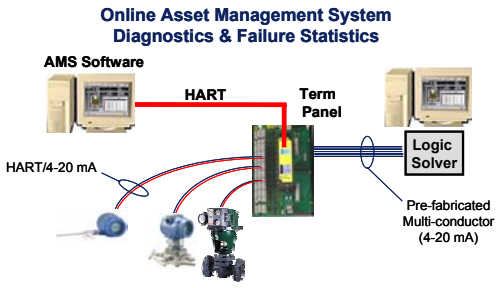
Diversity – While redundancy reduces the risk of random errors, diversity can minimize systematic, common-cause problems. One common application of diversity is the use of a Vortex or Coriolis Flowmeter to back up an orifice meter. Newer vortex designs are less likely to plug or coat than orifice plates and impulse lines. In addition, in contrast with DP-flowmeters or older vortex designs, there are no failure-prone gaskets or seals in contact with the process fluid, and no potential paths for leaks or fugitive emissions. With any inline meter, the user should ensure that any component that can fail –

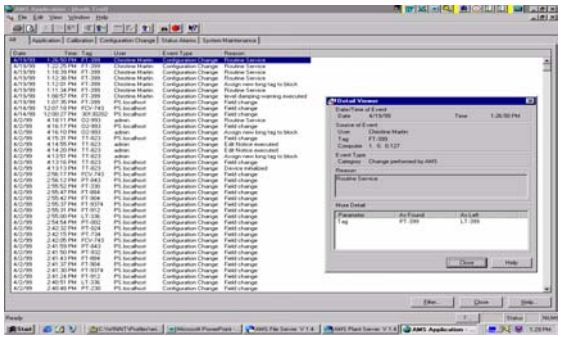
notably, the sensor – is located outside the process seal, so it can be replaced without shutting down the line. The user should also ensure that they determine the lowest possible flowrate that the flowmeter will be required to accurately measure, especially since most flow applications are unsafe at low, rather than high flows. A Vortex flowmeters will show "no flow" until it reaches some threshold. Unless the user has installed a newer "reducer" type meter, replacing an installed vortex meter with a smaller or larger meter requires significant, expensive piping changes.

Another widely-used approach is to back up a DP-Level meter with a top-down level technology, such as contacting or non-contacting radar. This protects against measurement errors caused by fluid density changes, and damage to the diaphragm seal itself.

Diagnostics – Internal diagnostics allow transmitters to diagnose themselves and their process connections. For example, a smart temperature transmitter might determine that its RTD has failed or has a loose connection. In the case of this critical fault, the transmitter output would fail to a fail-safe state (either high or low off scale). In the case of less critical faults – for example, a warning that the RTD is degrading and will fail "soon" - the transmitter would continue to provide a usable output, but would annunciate the impending failure at the LCD faceplate, and also via the HART output. If the logic solver can interpret HART diagnostics, it would immediately make this information available to the operator and/or maintenance, so the root cause can be corrected *before* it causes a shutdown. Otherwise, this can be provided by a parallel Asset Management System (AMS), shown below.

Another potential benefit of the Asset Management System is that it automatically collects an "Audit Trail" of failures and corrective actions. This can be useful in quantifying statistics for "real-world" safety and reliability, and developing and refining "Prior Use" data. The Audit Trail information is typically much more detailed than would normally be collected manually – device hardware and software revision level, materials of construction, range, etc – which can help the user identify problems with individual devices or material selection issues.





Test/Inspection Interval

As mentioned previously, one potential benefit of using the new standard is that is provides some flexibility in test/inspection interval. The safety data provided by the supplier should include a plot of PFD vs. time. As with any supplier data, the user needs to de-rate this to account for any identified time-dependent real-world common cause.

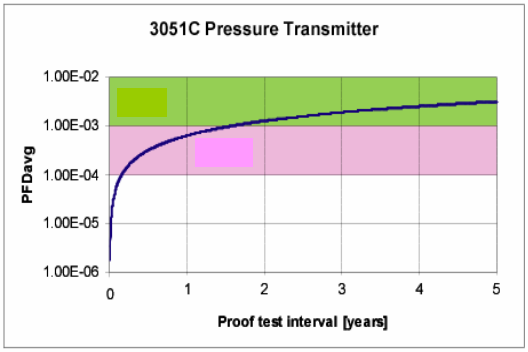


Figure 1 PFDavg values 3051C Pressure Transmitter

A transmitter with a safer design and more comprehensive diagnostics does not need to be inspected as frequently as another transmitter. *Two* transmitters – which provide continuously varying outputs that can be compared against each other – are inherently self-diagnosing, so are normally much safer than switches. As a result, the user can obtain comparable safety from switches only if they test/inspect much more frequently. This ignores the safety risks incurred by the testing itself – technicians can be injured, isolating valves can be left in the incorrect position after the test is complete, and the devices are usually unavailable during the test itself. So, less frequent testing of safe transmitters provides not only lower maintenance cost, but better real-world safety when compared with more frequent testing of less-safe switches.

Availability

Safety is not the same as availability – a system or device designed and certified for very high safety can suffer from low availability. For this reason, it is important for the user to avoid over-designing their safety system. While "you can never have too much safety", and "even one accident is too many" make for good safety posters, in real applications over-designed safety systems lead to spurious trips. Ironically, since processes are most unsafe during shutdown and subsequent startup – for example, the recent Texas City explosion occurred during equipment startup - over-designed safety systems can actually reduce **real-world** safety.

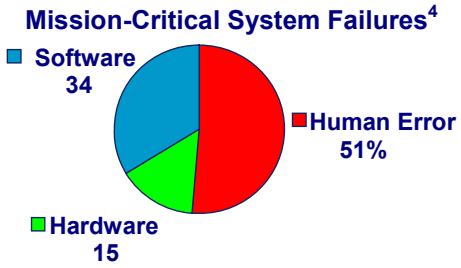
In critical applications that must not shut down, the user should consider adding one additional level of device redundancy beyond that needed to satisfy safety standards. As noted previously, adding redundancy to improve availability only makes sense after the user has first maximized common cause **strength** – robust, reliable devices, and in most cases the same “best practices” for selection, installation and maintenance that were used to achieve high real-world safety; **diversity** to improve resistance to systematic *safe* failures; and **diagnostics** that detect and alert the user to safe failures *before* they require process shutdown.

Consider redundancy of the “weak link” – in most temperature applications, both safe and dangerous failures are caused by the sensor instead of the transmitter. Instead of using two temperature

transmitters connected to a single RTD, consider a single transmitter connected to a dual-element RTD. Since the dual-element RTD is inserted into a single thermowell, and the transmitter continually monitors both sensors to ensure they match, this approach provides a significant improvement in safety and availability, at minimal increase in life cycle cost. For the most critical applications, the highest safety and availability is of course provided by *two* transmitters, each connected to a dual-element RTD.

Commonality and Human Error

Most failures of mission-critical systems are not caused by hardware or software. They are caused by human error – engineer, maintenance, operations.



Human errors can usually be attributed to lack of familiarity, illustrated by the "Automation Irony": "Engineers generally automate the tasks that are easy, leaving the hard jobs to people ... (who) … must carry out difficult tasks intermittently on unfamiliar systems - a sure recipe for failure."[5] Training is important of course, but even more important is maximizing **commonality**. For example, it may be tempting for the user to specify a unique transmitter for safety applications because that device boasts unique "safety features". While this new device may provide better safety and possibly reliability *on paper*, in the real-world it can suffer from four key problems when compared with more familiar devices:

- The user's engineers are not as familiar with specifying the new device and are more likely to make an error in the selection of the device, its materials, or its options
- The user's maintenance personnel are not as familiar with "best practice" installation and maintenance of the new device. In cases where the safety devices are only inspected very infrequently, say every 5 years, the technicians would only work on the devices at those intervals – or, sooner unfortunately, if the device caused an unscheduled shutdown.
- The supplier has not had as much run time with the new device to work out bugs in design or manufacture.
- The user incurs additional training and inventory costs.

Adding "safety options" to familiar, proven transmitters can provide significant user benefit in enhanced fault tolerance, diversity and diagnostics. Using a completely unfamiliar, unproven device in critical safety applications based solely on high laboratory safety, and possibly an impressive brochure, defies common sense.

So, the user should strive to use common or similar devices and practices for both basic process control and safety applications. This is not to say that the same actual device should be physically shared

between the basic process control and the safety system. While physically wiring one transmitter to both the basic process control system (BPCS) and the safety system (SIS) provides obvious savings in device costs, only a user who is very familiar with the standard should attempt to do so after careful analysis of the process safety risks and costs of added documentation. Per the standard – "Using a single sensor for both the BPCS and the SIS requires further review and analysis because … failure of this single sensor could result in a hazardous situation". Also – "A SIS is normally separated from the BPCS … to retain flexibility for changes, maintenance, testing and documentation relating to the BPCS." Finally – "Where a single sensor is used for both a BPCS and SIS function, the requirements … will normally only be satisfied if the sensor diagnostics can reduce the dangerous failure rate sufficiently and the SIS is capable of placing the process in a safe state within the required time. In practice this is difficult to achieve even for SIL 1 applications."

CONCLUSION – "Best Practices"

To comply with the emerging standards, and achieve the highest safety and availability at the lowest life cycle costs, users should:

1. Ensure that safety design on new processes comply with the latest relevant standard, namely ANSI/ISA 84.00.01-2004.

2. Perform a quantitative analysis to verify that existing safety systems provide the SIL required for each SIF, given the specified test interval.

3. To minimize hardware requirements, use either "Certified" or "Prior Use" devices. In practice, obtain the transmitter data from the supplier – validated by an accredited third party – and de-rate that data based on "real-world" safety risk which is unique to each specific application.

4. Common cause dominates real-world safety for measurements. Maximize common cause strength, employ diverse technologies and use devices with diagnostics. An Asset Management System makes diagnostic information more accessible and timely, and provides detailed statistics of failures and remedial action for future Prior Use analysis.

5. Transmitters require much less testing than switches, and hence achieve higher real-world safety.

6. Maximize availability to increase safety – use robust, reliable devices and practices, and employ redundancy of transmitters and/or sensors.

7. Minimize human error and life cycle cost by maximizing commonality between the BPCS and SIS. Use only devices which are familiar and proven, both by the user and the supplier.

8. Share actual components between the BPCS and SIS only after careful analysis of safety risk and costs to operational and maintenance flexibility.

Presented at ISA EXPO 2005, 25-27 October 2005
McCormick Place Lakeside Center, Chicago, Illinois, www.isa.org

REFERENCES

1. "Guidelines for Safe Automation of Chemical Processes", Chap. 7, Sec. 4, Center for Chemical Process Safety, AIChE.

2. ibid.

3. Menezes, M. and Brown, S., "Design Safety Instrumented Systems with Relevant Data", *Chemical Engineering*, July 2003.

4. Fox, A. and Patterson, D., "Self-Repairing Computers", *Scientific American*, June 2003.

5. ibid.