INL/CON-14-33917
PREPRINT

Digital Sensor Technology

9th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human Machine Interface Technologies (NPIC&HMIT 2015)

Ken D. Thomas, Edward L. Quinn, Jerry L. Mauck, Richard M. Bockhorst

February 2015

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Digital Sensor Technology

Ken D. Thomas
Idaho National Laboratory
2525 Fremont Ave.
Idaho Falls, ID 83415
kenneth.thomas@inl.gov

Edward L. Quinn, Jerry L. Mauck, Richard M. Bockhorst
Technology Resources
23292 Pompeii Drive
Dana Point, CA 92629
tedquinn@cox.net, jerrymauck@verizon.net, r_bockhorst@hotmail.com

ABSTRACT

The nuclear industry has been slow to incorporate digital sensor technology into nuclear plant designs due to concerns with digital qualification issues. However, the benefits of digital sensor technology for nuclear plant instrumentation are substantial in terms of accuracy and reliability.

Improved accuracy results from the superior operating characteristics of digital sensors. These include improvements in sensor accuracy and drift and other related parameters which reduce total loop uncertainty and thereby increase safety and operating margins.

Similarly, improved sensor reliability is illustrated with a sample calculation for determining the probability of failure on demand, an industry standard reliability measure. This looks at equivalent analog and digital temperature sensors to draw the comparison. The results confirm substantial reliability improvement with the digital sensor, due in large part to ability to continuously monitor the health of a digital sensor such that problems can be immediately identified and corrected. This greatly reduces the likelihood of a latent failure condition of the sensor at the time of a design basis event.

Notwithstanding the benefits of digital sensors, there are certain qualification issues that are inherent with digital technology and these are described in the report. One major qualification impediment for digital sensor implementation is software common cause failure (SCCF).

Key Words: digital, actuator, software common cause failure, nuclear power

1 INTRODUCTION

The nuclear industry has been reluctant to incorporate digital sensor technology into nuclear plant designs due to concerns with the licensing of digital systems and the potential complication of designs to incorporate sufficient diversity to address software common cause failure. There is also a degree of familiarity and comfort with the analog sensor technologies for both plant designers and plant owners such that they are willing to forego the acknowledged benefits of digital technology in favor of tried and true solutions for plant instrumentation.

The purpose of this paper is to demonstrate that the benefits of digital sensor technology can be significant in terms of plant performance and that it is worthwhile to address the barriers currently holding

back the widespread development and use of this technology. This topic is more fully described in a related report entitled Digital Sensor Technology, produced under the Department of Energy's Nuclear Energy Enabling Technologies Research Program [1]. This paper addresses two important objectives in pursuit of the beneficial use of digital sensor technology for nuclear power plants:

1. To demonstrate the benefits of digital sensor technology over legacy analog sensor technology in both quantitative and qualitative ways.
2. To recognize and address the added difficulty of digital technology qualification, especially in regard to software common cause failure (SCCF), that is introduced by the use of digital sensor technology. It outlines additional research that is needed to find practical means of achieving this qualification.

Digital actuator technology has been available to the nuclear industry for many years. During this time, other industries have made extensive use of it to improve the reliability of their operations and to lower costs. In the face of competitive pressure, these other industries have been able to derive positive business cases to invest in these technologies. In fact, such technologies have proven to be a competitive advantage in managing production costs.

A major impetus for increased use of digital actuators is that it is a means of reducing operating costs. As discussed in Section 2.0, digital actuators offer performance and maintainability benefits. They offer significant diagnostic and health reporting capabilities that can also reduce plant support costs and provide earlier warning of impending failures. The avoidance of failures that could result in costly plant shutdowns and adverse regulatory actions is a significant indirect cost benefit.

For the current operating fleet, the legacy analog I&C systems have been difficult to upgrade for a number of reasons, including licensing risk, cost, and the difficulty in changing the operating and support infrastructure such as procedures, defined maintenance plans, training programs, and other large investments in plant documentation.

While the new plants are making extensive use of digital control and protection systems, they are not incorporating digital instrumentation and communication technologies to any appreciable degree, especially for safety-related applications. The concerns for new plants remain the same of regulatory risk, environmental limitations, and the difficulty of dealing with qualification, especially in resolving the software common cause failure concern.

2 ADVANTAGES OF DIGITAL INSTRUMENT LOOPS

Digital instrument loops are similar to analog loops in that they both have a power supply, a transmitter, and output devices. Measurement of most process parameters begin as an analog signal, such as a change in capacitance due to the force applied by a pressure. The significant difference for a digital transmitter is that the transmitter contains a microprocessor, memory, analog-to-digital conversion component, and digital communication components. The electrical signal is converted to a digital value and is then transmitted over a cable to another digital device, such as a programmable logic controller, and then re-transmitted to the output devices. Conversion of the analog signal to a digital value as close to the process as possible reduces in accuracies inherent in analog signal processing. Digital signal transmission and processing typically does not introduce significant inaccuracies. Inaccuracies introduced by the instrument loop result in some degree of uncertainty regarding the true value of the analog signal.

There are several uncertainty terms that may be substantially improved by implementing a digital transmitter in place of an analog transmitter. The terms that typically dominate the instrument loop uncertainty are drift, harsh environmental effects, and process measurement effects. Digital transmitters significantly reduce the drift terms of the loops since, once the signal is digitized, drift of downstream components is no longer an issue. To date, no digital transmitters have been qualified for harsh

environmental effects so a definitive statement about improvement in this term is speculative. However, since the transmitter may also be able to communicate the environmental temperature at the location of the transmitter, the possibility of compensating for the environmental temperature is available. In some applications, implementing digital and/or updated technology transmitters may reduce or eliminate the process measurement effects term. For example, some digital level applications eliminate the reference leg (for a pressure or level instrument) so uncertainties associated with the reference leg become zero.

Digital transmitters also offer improved performance. The accuracy of digital transmitters is typically a factor of two better than analog transmitters. The stability from environmental conditions is significantly improved, e.g. a factor of 3 or better, for digital transmitters. Digital transmitters also allow remote modification of the range of the transmitter. Since the signal is digitized at the transmitter, the balance of the loop does not impact the accuracy of the signal.

Traditional analog and discrete devices have no way to indicate if they're operating correctly, or if the process information they're sending is valid. As a consequence, technicians spend a lot of time verifying device operation. Digital devices can tell if they're operating correctly, and if the information they're sending is good, bad, or uncertain. This eliminates the need for some routine checks and helps detect failure conditions before they cause major process problems.

3 IMPROVEMENT IN SENSOR ACCURACY

The Nuclear Regulatory Commission requires nuclear plants to have detailed calculations to support safety-related setpoints. Calculation of safety-related setpoints for nuclear power stations is guided by USNRC Regulatory Guide 1.105 [2] which endorses Part 1 of ISA-67.04-1994 [3].

To illustrate the potential reduction in instrument uncertainty by using digital instrumentation, a typical calculation of the instrument loop uncertainty for a pressurizer pressure loop was conducted. The uncertainty values for a digital instrument loop have been added to the calculation to show the potential improvement that may be realized with digital. Since the digital transmitters have not been qualified for post-accident environments, only values for normal operating conditions are considered. Table 1 below summarizes the results of the calculation. This example calculation shows a reduction in the total loop uncertainty by a factor of three.

Table 1 Example Pressure Loop Uncertainty for Reactor Trip

Term	Analog	Digital
Sensor Accuracy	0.2500%	0.0300%
Sensor Drift	0.4500%	0.1875%
Sensor M&TE	0.4240%	0.0300%
Sensor Temperature Effect	1.3750%	0.2250%
Sensor Power Supply	0.0131%	0.0131%
Rack Accuracy	0.7650%	0.0000%
Rack Drift	0.5580%	0.0000%
Rack M&TE	0.2000%	0.0000%
Rack Temperature Effect	0.1125%	0.0000%
Sum of squares	3.285E-04	8.775E-06
Square root	±1.81%	±0.296%
Process Considerations*	0.3000%	0.3000%
Uncertainty	±2.11%	±0.596%

For the digital pressure loop, the values for sensor accuracy, sensor temperature effect, sensor power supply, and sensor drift are taken from published specifications. Since the electronic signal is converted to a digital value by the sensor, a number of analog electronic components that provide the signal processing do not degrade the signal. Therefore, the values for accuracy, temperature, and drift are lower. Also, the rack components do not contribute to additional uncertainty since they are simply re-transmitting a digital value received from the sensor.

4 IMPROVEMENT IN SENSOR RELIABILITY

The reliability of sensors in a nuclear power plant is highly-important to safe operations. The sensors are virtually the only way the operators know about the operating conditions of the plant in that, for the most part, the plant cannot be monitored visually. Without properly operating sensors, the condition of the plant is unknown. When sensors are not functioning correctly or are out of service for repair, the plant is in a degraded configuration.

It is therefore a requirement in the design of a nuclear plant to conduct reliability analysis for certain safety-related components in accordance with IEEE-603 [4] and IEEE-7-4.3.2-2003 [5].

Reliability is defined in IEEE-352 [6] as follows:

The characteristic of an item or system expressed by the probability that it will perform a required mission under stated conditions for a stated mission time.

The reliability of a specific instrumentation design can be quantitatively determined in accordance with IEC 61508 [7] using a Markov Model, including the reliability data for individual components combined in the manner in which they support performance of the safety function. This analysis is based on the proof or surveillance test intervals, repair rates of components, and the plant specific configuration that is performing the safety function.

In traditional analog sensor designs, certain failure modes of sensors could go undetected until the next scheduled testing at the end of the current surveillance interval. Therefore, the device would be in a latent failure state and it would not operate correctly if called upon for its design basis function. Since the failure might have happened at any time during the surveillance interval, the predicted reliability of the instrumentation system would have to take this into account. The measure of this is the average probability of failure on demand or PFDavg. Surveillance intervals for many safety-critical sensors are often 18 or 24 months, corresponding to a refueling cycle, and therefore the time period over which a failure could go undetected could be quite significant. Some sensors have even longer surveillance intervals.

Obviously, if the sensor health could be confirmed on a more frequent basis, the PFDavg of the instrument design would be reduced (improved). Digital systems are able to do this by performing continuous monitoring of the sensor health. However, this capability depends on the sensor being part of a digital system that can perform this monitoring, such a distributed control system (DCS). In this case, the digital system can obtain significant information on the health of the instrument as well as the signal communication circuit and this can be credited in the determination of the PFDavg. This capability can also be used to justify longer surveillance intervals.

A key consideration in the crediting of monitoring is the treatment of what is termed dangerous detected and dangerous undetected failure fractions, which are established to provide input to the Markov reliability model for the device and the associated system. IEC-61508 defines these as follows:

Dangerous Detected Failure - A detected failure which has the potential to put the safety instrumented system in a hazardous or fail-to-function state. Dangerous detected failures do not include hardware failures and software faults identified during proof testing, represented by the plant's surveillance testing.

Dangerous Undetected Failure - An undetected failure which has the potential to put the safety instrumented system in a hazardous or fail-to-function state. Dangerous undetected failures do not include hardware failures and software faults identified during proof testing.

The failure fraction refers to the relative proportion of both the detected and undetected failures, expressed as a fraction of one. Thus, dangerous detected failure fraction of 0.93 means that 93 out of 100 dangerous failures are detected by the monitoring capability. The role of the monitoring capability is to detect as many of the total possible dangerous failures of the system and related devices as possible, with the monitoring credit being proportional to the fraction. Note that there are other failures that are designated as safe, meaning they do not threaten the reliability of the system.

In one particular example, three digital temperature transmitters are used as parallel redundant channels so that the on-line monitoring capability can conduct cross-channel checks to verify that the devices are functioning properly. This is just one among many health checks performed by the monitoring capability.

The actual computation is very complex and is performed by a computer program based on the data inputs to the various tables that are found in a sample calculation [1]. In accordance with the referenced methodology (IEEE-352 and IEC-61508), the reliability values for sensor string values (isolation module and temperature transmitters) are combined with the interfacing components to establish the complete reliability values for the input string and to provide a basis for the required proof testing of the sensor inputs. Similarly, the output string is combined with the respective output actuators to establish the reliability and to provide the basis for the required proof testing of the output string required to perform the safety function.

The PFDavg of the temperature transmitter is conservatively set at 1 X 10-7 based on a surveillance interval of 14 days (as depicted in Chart 2 of Appendix E). In actuality, the surveillance interval is every few minutes, which is the cycle time for the continuous on-line monitoring. This shows a significant effect on the PFDavg as a result of the on-line monitoring, because it has a dangerous detected failure fraction of 0.99.

The on-line monitoring capability helps in two distinct ways. It detects almost all of the dangerous failures and it does this check very frequently. Therefore, almost any dangerous failure would be detected immediately and the plant operators could take compensatory action before the device might fail to perform in a possible design basis event. In short, the design is highly reliable.

As a separate part of the calculation, the PFDavg of the PLC logic solver is also computed and found to be 5.99 x 10-5 over 18 months for a fully integrated DCS with temperature sensor input.

The combined PFDavg of the PLC logic solver and temperature transmitter input string are found as follows:

PFDAVG-TOTAL = PFDAVG-LOGIC SOLVER + PFDAVG-TEMPERATURE TRANSMITTER
PFDAVG-TOTAL = 5.99 x 10-5 + 1 x 10-7
PFDAVG-TOTAL = 6.00 x 10-5

It should be noted that the PFDavg for the temperature transmitter is two orders of magnitude lower than that of the PLC logic solver, meaning that it makes a negligible contribution to the total PFDavg. Again, this is possible only by the use of a digital sensor combined with an effective monitoring capability (very high dangerous detected failure fraction).

Analog Temperature Transmitter Reliability Example Calculation

For comparison purposes, a reliability calculation for a typical analog temperature transmitter is presented. This transmitter has a MTBF of 73.98 years as determined by the supplier's experience and represents a highly reliable device. In this case, the proof test or surveillance interval (TI) is 18 months or 1.5 years, based on a normalized plant refueling cycle.

Unlike the digital counterpart, this analog sensor does not have the capability to be monitored on-line. Therefore, the full dangerous undetected failure fraction must be assumed. Put another way, the dangerous detected failure fraction is 0.00 compared to 0.99 for the digital counterpart. So for this device, no monitoring credit can be given. And since there is no monitoring capability to perform an automatic sensor cross-channel comparison, a single sensor is considered.

On this basis, the PFDavg calculation is somewhat simpler as follows:

$PFDavg = (1/MTBF)^2 \times TI^2$
$PFDavg = (1/73.98)^2 \times 1.5^2$
$PFDavg = 4.11 \times 10\text{-}4$

With no on-line monitoring, this is the best PFDavg that can be credited to the instrument based on industry standards. [10] The result is also consistent with the reliability values of most of the current analog technology installed in nuclear plants today. In fact, a value of PFDavg in the 10-4 range is representative of a robust design as stated in IEC-61508 and IEEE-352.

This can however be improved with the addition of manual cross-channel sensor comparisons (or "channel checks") performed by operators on a shift or daily basis. These channel checks can detect gross failures and are typically required by the plant's Technical Specifications. However, they are not always credited in the instrument reliability calculations. Even with the channel checks, the dangerous detected failure fraction would still be considerably lower than that of a digital monitoring system because the channel checks cannot detect certain types of failures. They can, however, improve the PFDavg to be in the 10-5 range.

Implications for Improved Sensor Reliability

At the sensor level, the PFDavg is improved by several orders of magnitude by the use of digital sensors instead of the analog counterpart. Specifically in this example, the digital sensor PFDavg is 1 x 10-7 versus the analog sensor PFDavg of 4.11 x 10-4. Even with the addition of the channel checks, the improvement in the reliability of the sensors is dramatic.

At a system level, this means for the digital sensor design, the contribution of the sensors to the probability that the system will not function properly on demand is negligible. This is not the case for the analog sensor design (with channel checks), where the sensors and the logic solver make nearly co-equal contributions to the probability that the overall system will not function properly on demand.

This leads to the consideration of a hybrid analog-digital design that is typically seen in the industry today for operating nuclear plants as well as new plants. This is the case where a modern digital control system, such as a DCS, is combined with traditional all-analog sensor inputs.

Using the combined numbers from both the digital and analog reliability calculations presented above, the total PFDavg for the temperature function can be calculated as follows:

PFDAVG-TOTAL = PFDAVG-LOGIC SOLVER (digital) + PFDAVG-TEMPERATURE TRANSMITTER (analog)
PFDAVG-TOTAL = 5.99 x 10-5 + 4.11 x 10-4
PFDAVG-TOTAL = 4.71 x 10-4

In this case, the reliability of the total system for this temperature function has been degraded to the approximate level of the analog sensor. In other words, the improved reliability of the digital logic solver has essentially been lost and the reliability of the total system, for this temperature function, is reduced by over an order of magnitude compared to an all-digital design.

Even considering the effect of the channel checks, the reliability is still reduced. In this case, a mid-range PFDavg value of 5 x 10-5 for an analog instrument design with credited channel checks is assumed with the following results:

PFDAVG-TOTAL = PFDAVG-LOGIC SOLVER (digital) + PFDAVG-TEMPERATURE TRANSMITTER (analog)
PFDAVG-TOTAL = 5.99 x 10-5 + 5.00 x 10-5
PFDAVG-TOTAL = 1.10 x 10-4

The probability of this temperature function failing on demand is roughly twice as high compared to the all-digital design. This illustrates how the reliability benefits of a modern digital control or protection system are substantially negated when combined with traditional analog sensors as the process inputs.

5 QUALIFICATION CONCERNS

Additional burden is imposed on the use of digital sensors in the areas of qualification and licensing due to the fact that they are based on either software or firmware for their processing logic. Software-based digital systems have long been recognized as having failure susceptibilities that are not present with their analog counterparts. Also, digital systems reside on electronic components, which can be more susceptible to environmental influences than traditional electro-mechanical technology.

The additional qualification and licensing burden over what is required for analog sensors is potentially significant and can cause cost increases and delays in plant upgrades or new designs. The major areas of consideration are:

- Software Quality
- Environmental Effects on Electronics
- Reliability, including Software Common Cause Failure (SCCF)
- Digital Communications
- Cyber Security

Digital computers used in safety systems must consider the possibility of susceptibility to SCCF. If redundant channels use devices of the same manufacturer make and model number, as is typically the case, there would be no diversity in this set of instruments relative to SCCF susceptibility and it is conceivable that a software fault would simultaneously affect all channels and cause the design function to fail, in spite of the redundancy. For highly safety-significant instrumentation, the effect of the regulatory-required Diversity and Defense-in-Depth (D3) analysis [8] would be to require an instrument signal diverse from these instruments to cope with a SCCF.

These factors have been a significant impediment to the use of digital sensors in both operating plants and new reactor designs, especially for safety-related applications, and must be overcome if the industry is to obtain the long-term operational benefits of digital sensors.

6 CONCLUSIONS

Digital sensor technology represents an unrealized potential to significantly improve long-term operations for both operating and future nuclear plants. It provides both design and operational advantages over analog in such ways as improved technical performance, improved safety margins, and reduced maintenance cost. This has advantages for both current and future nuclear plants.

This paper outlines the benefits of digital sensors in two important areas:

Accuracy – significant reduction in total loop uncertainty (TLU), resulting in greater safety and operational margins, and reducing loop drift, allowing longer periods of time between calibrations. This means less maintenance burden for the plant and particularly less work in outages.

Reliability – significant reduction in the probability of failure on demand due to the credit for undetected failure fraction resulting from continuous verification that the device is functioning. The means less periodic testing can be justified.

In summary, there is considerable performance improvement available to the industry if digital instrumentation is adopted on a wide-scale. Several barriers must be addressed for this to be a practical option for the nuclear industry. Therefore, further work is needed in the following areas to promote the widespread use of digital instrumentation as follows:

- A reasonable solution to the SCCF must be found such that a failure all similar sensors does not have to be assumed.
- The industry would benefit by a case study on long-term plant economic benefits related to widespread use of digital sensors. This study would capture the plant-wide performance improvement and cost savings related to accuracy, reliability, availability, and maintainability.
- Instrument suppliers need to qualify, and harden if necessary, the digital sensor alternatives, so that they can be used in safety-related applications located in harsh environments.

7 ACKNOWLEDGMENTS

The U.S. Department of Energy (DOE) Office of Nuclear Energy (NE) established the Advanced Sensors and Instrumentation (ASI) technology area under the Nuclear Energy Enabling Technologies (NEET) Program to coordinate the instrumentation and controls (I&C) research across DOE-NE and to identify and lead efforts to address common needs. As part of the NEET ASI research program, the Digital Technology Qualification project was established based on collaboration between Oak Ridge National Laboratory (ORNL) and Idaho National Laboratory (INL). This paper has been developed with the funding provided for the Digital Technology Qualification project, and is derived from a related project report entitled Digital Sensor Technology (INL/EXT-13-29750). The authors would like to thank Ms. Suibel Schuppner of the U.S. Department of Energy, Program Manager for the NEET ASI research program, and Dr. Bruce Hallbert of the Idaho National Laboratory, Technical Director for the NEET ASI research program.

8 REFERENCES

1. Quinn, E., Mauck, J., Bockhorst, R., & Thomas, K., Digital Sensor Technology (INL/EXT-13-29750), Idaho National Laboratory, July 2013
2. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.105 Revision 3, Setpoints for Safety-Related Instrumentation, Washington, DC, December, 1999
3. American National Standard ANSI/ISA S 67.04 Part 1-1994, Setpoints for Nuclear Safety-Related Instrumentation, 1994
4. Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std. 603-1998, Piscataway, New Jersey, 1998
5. Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," IEEE Std. 7-4.3.2, 2003, Piscataway, New Jersey, 2003
6. Institute of Electrical and Electronics Engineers, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems, IEEE 352-1987, Piscataway, New Jersey, 1987
7. International Electrotechnical Commission, IEC 61508 - 2009, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, Parts 1 through 6.
8. U. S. Nuclear Regulatory Commission, Standard Review Plan, NUREG-0800, Chapter 7, Branch Technical Position (BTP) – 19 Revision 6, Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems, Washington, DC, July 2012