INL/EXT-13-29750

Digital Sensor Technology

Ted Quinn, Jerry Mauck, Richard Bockhorst; Technology Resources

Ken Thomas; Idaho National Laboratory

July 2013

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

INL/EXT-13-29750

Digital Sensor Technology

Ted Quinn, Jerry Mauck, Richard Bockhorst; Technology Resources

Ken Thomas; Idaho National Laboratory

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

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 (ANL) and Idaho National Laboratory (INL). This report was prepared under Work Package CT-13IN070307.

EXECUTIVE SUMMARY

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, reliability, availability, and maintainability. This report demonstrates these benefits in direct comparisons of digital and analog sensor applications. It also addresses the qualification issues that must be addressed in the application of digital sensor technology.

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. An example instrument loop uncertainty calculation for a pressure sensor application is presented to illustrate these improvements. This is a side-by-side comparison of the instrument loop uncertainty for both an analog and a digital sensor in the same pressure measurement application.

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.

Closely related to the concept of reliability, availability is the probability that the sensor will function on demand. Improvement in instrument loop availability with digital sensors is described again as a function of the continuous on-line monitoring. Advantages for digital sensors in maintainability are also discussed, highlighting improvements that reduce operational and maintenance burdens.

Notwithstanding the benefits of digital sensors, there are certain qualification and licensing 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). This is being addressed in a related Digital Technology Qualification project by the Oak Ridge National Laboratory.

Finally, the transition to more advanced sensor technology is described in terms of the measurement principles used in legacy analog technology, current digital sensor technology, and emerging sensor technology for the measurement of pressure, level, flow, temperature, and neutron flux. The emerging technologies promise even greater design and performance benefits for digital sensors.

Table of Contents

EXECUTIVE SUMMARY iv

ACRONYMS iix

1.0 Introduction 1

1.1 Purpose 1
1.2 Scope 2
2. Background 4

2.1 Barriers to Digital Technology Implementation in NPPs 4
2.2 The Challenge of Digital Technology Qualification for Plant Instrumentation 5
2.3 The Practical Effect on Digital Sensor Technology Implementation 7
3. Overview of Plant Process Instrumentation 9

3.1 Loops 9
3.1.1 Analog Instrument Loops 9

3.1.2 Digital Instrument Loops 10

3.2 Transmitters 10
3.3 Communication 11
3.3.1 Current 11

3.3.2 Digital 11

3.3.3 Wireless 12

3.4 Output Devices 12
3.5 Advantages of Digital Loops 12
4. Operational Advantages of Digital 14

4.1 Instrument Loop Uncertainty 14
4.2 Reliability 19
4.2.1 Importance of Sensor Reliability 20

4.2.2 Example Reliability Calculation - Temperature Transmitter 21

4.3 Availability 27
4.4 Maintainability 29
5. Qualification and Licensing Considerations 31

5.1 Qualification Considerations 32
5.1.1 Software Quality 32

5.1.2 Environmental, Seismic, and Electromagnetic Compatibility (EMC) Qualification 33

5.1.3 Reliability, including Software Common Cause Failure 34

5.1.4 Communications 36

5.1.5 Cyber Security 37
5.2 Licensing Considerations 38
5.2.1 Nuclear Plant Modifications under Licensee Control 38
5.2.2 Nuclear Plant Modifications under NRC License Amendment 39
5.2.3 Improvements in Plant Technical Specifications 40
5.2.4 Certification of New Nuclear Plant Designs 41
5.3 Summary of Qualification and Licensing Considerations 42
6.0 Transition to Advanced Transmitter Technology 43
6.1 Pressure Transmitters 43
6.1.1 Analog Pressure Technology 43
6.1.2 Digital Pressure Technology 45
6.2 Flow Measurement 46
6.2.1 Analog Flow Technology 46
6.2.2 Digital Flow Technology 47
6.2 3. Emerging Flow Technology 47
6.3 Level Measurement 47
6.3.1 Analog Level Technology 47
6.3.2 Digital Level Technology 48
6.3.3 Emerging Level Technology 49
6.4 Temperature 50
6.4.1 Analog Temperature Technology 50
6.4.2 Digital Temperature Technology 50
6.4.3 Emerging Temperature Technology 50
6.5 Neutron Flux Monitors 51
6.5.1 Analog Flux Technology 52
6.5.2 Emerging Flux Technologies 53
7. Summary 55
8.0 References 57
Appendix A: Nuclear Plant Transmitter Types 61
Appendix B: Uncertainty Terms 65
Appendix C High Pressurizer Pressure Calculation 67
Appendix D INPO Data Search for Instrument Failures 101
Appendix E Typical Nuclear Power Plants Units 1 and 2 104

Table of Figures

Figure 1 Typical Analog Instrument Loop 9
Figure 2 Typical Digital Instrument Loop 10
Figure 3 Parameter Normal Operating Range and Safety Limit Parameters 18

Table of Tables

Table 1 Example Pressure Loop Uncertainty for Reactor Trip 15
Table 2 Example Pressure Loop Uncertainty for Indication 15
Table 3 Typical Level Loop Uncertainty for Reactor Trip 16
Table 4 Typical Level Loop Uncertainty for Indication 17
Table 5 Transition to Advanced Transmitter Technology 44

ACRONYMS

AL	Analytical Limit
ATWS	Anticipated Transient Without Scram
BPC	Basic Processing Cycle
CCF	Common Cause Failure
CDA	Critical Digital Assets
D3	Diversity and Defense-in-Depth
DAS	Diverse Actuation Systems
DCD	Design Control Document
DCS	Digital Control System
EMC	Electromagnetic Compatibility
EMI/RFI	Electromagnetic and Radio Frequency Interface
EPRI	Electric Power Research Institute
ESF	Engineered Safety Function
ESFAS	Engineered Safety Function Actuation Systems
FMEA	Failure Modes and Effects Analysis
GT	Gamma Thermometer
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
IEEE	Institute of Electrical and Electronics Engineers
INERI	International Nuclear Energy Research Initiative
INPO	Institute of Nuclear Power Operations
ISA	International Society of Automation
LAR	License Amendment Request
LPRM	Local Power Range Monitor
LTSP	Limiting Trip Setpoint
M&TE	Measuring and Test Equipment
MEMS	Microelectromechanical systems
MTBF	Mean-Time-Between-Failure
MTTR	Mean-Time-To-Repair
NEER	Nuclear Engineering Education Research
NMS	Neutron Monitoring System

NGNP	Next Generation Nuclear Power Plant
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NTSP	Nominal Trio Setpoint
O&M	Operation and Maintenance
PFD	Probability of Failure on Demand
PIE	Postulated Initiating Event
PLC	Programmable Logic Controller
PRA	Probabilistic Risk Assessment
QA	Quality Assurance
RTD	Resistance Temperature Detectors
RTS	Reactor Trip System
RTS	Reactor Trip Subsystems
SAR	Safety Analysis Report
SCCF	Software Common Cause Failure
SDOE	Secure Development and Operational Environment
SL	Safety Limits
SMR	Small Modular Reactors
SSE	Safe Shutdown Earthquakes
TI	Test Interval
TIP	Traversing In-Core Probe
UFSAR	Updated Final Safety Analysis Report

1.0 Introduction

1.1 Purpose

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. [1]. 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.

For some nuclear plant instrument applications, there is no proven and qualified digital technology currently available, in part, due to the lack of commercial demand for the reasons cited above. In these cases, performance improvement using digital sensor technology is not an option.

The purpose of this report 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 report 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.

In regard to the first object, this project investigates the advantages of digital sensor technology as it improves performance in the areas of accuracy, reliability, availability, and maintainability. It describes the magnitude of the performance improvement with the digital instruments and asserts that it is very much in the interest of the commercial nuclear industry to find an acceptable solution to the issue of SCCF for digital instrumentation.

The second objective is the subject of an Oak Ridge National Laboratory related project for which the goal is to resolve the impediments to qualification of digital technology for nuclear power application to enable more extensive utilization of modern equipment in the full range of I&C systems at nuclear power plants. [2] More specifically, the project is developing an objective, scientific basis for determining necessary and sufficient mitigation of software common cause failure vulnerabilities.

Together, these projects will demonstrate the application of equipment, strategies, and methodologies to enable more extensive digital technology usage. This is further described in Section 1.3 Background.

As a point of clarification, the terms *sensor technology* and *instrument* (and variations) are used interchangeably in this report. In actuality, a sensor is the portion of an instrument that is in contact with and "senses" a process parameter (such as pressure or temperature). An instrument also has a transducer that converts the sensed parameter to a corresponding parameter that can be processed by the instrument, typically an electrical signal, a force, or a displacement. The instrument, in turn, either displays the value locally or transmits it to other devices as control or display inputs. For the purpose of this report, it is not necessary to distinguish between the terms *sensor technology* and *instrument* and therefore either is used depending on the context.

1.2 Scope

The scope of this project is nuclear plant performance improvement across all types of current and future nuclear power plants in the use of digital instrumentation. This includes the current U.S. light water reactor operating fleet, the new builds that are in the licensing and construction process now, small modular reactors (SMRs), and the next generation nuclear plants (NGNP).

The project focuses on several representative instrument applications that comprise the majority of instrument applications in a typical nuclear power plant (NPP). These are typical of what is available today and that illustrate typical values relative to performance improvement. Specifically, the instrument applications investigated in this project are pressure, level, flow, and temperature. These were selected because there are commercially-available digital instruments in these applications and this enables a rigorous comparison to their analog counterparts. Therefore, these projected performance benefits can be multiplied over the number of similar instruments in a plant.

Additional instrument applications not considered in this report also hold promise of performance improvement, but they are not yet available as commercial offerings and have not yet been proven in respect to performance characteristics for comparison to their analog counterparts. Examples would be such parameters as neutron flux, radiation monitoring, linear position, gas purity, etc. Some manufacturers report that they have not pursued digital counterparts to their current analog offering in these applications because there is no demand in their customer base. This is not surprising and is again indicative of the analog preference due to the regulatory uncertainty. The report highlights the need for commercial development in these instrument applications as well.

The organization of the major sections of the report is as follows:

Section 2 Provides background information on how the increased use of digital instrumentation increases the complexity of digital qualification.

Section 3 Provides an overview of instrument loop concepts and how performance is affected by legacy analog instrumentation technology.

Section 4 Demonstrates the operational advantages of digital instrumentation in the areas of accuracy, reliability, availability, and maintainability.

Section 5 Describes certain qualification and licensing considerations that are somewhat of a challenge with digital technology and that must be addressed in order to take advantage of digital instrumentation in nuclear power plant (NPP) designs.

Section 6 Describes legacy, current, and future instrumentation technology that will likely become available.

Section 7 Presents the conclusions of the project and describes future needs for research and development.

2. Background

2.1 Barriers to Digital Technology Implementation in NPPs

Digital technology has been implemented in nuclear power plants for several decades, however on somewhat a limited basis. 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. [3]

Recent experience in the industry has highlighted this difficulty. Of note is the recent Oconee Nuclear Station implementation of a digital reactor protection and engineered safeguard features actuation system that resulted in a prolonged regulatory review over the issue of diversity and defense-in-depth (D3. This analysis basically requires the assumption of a SCCF for highly-safety significant systems and demonstration of the ability to cope with this failure. This typically results in the requirement to implement a diverse actuation system (DAS) based on technology that is not subject to the same SCCF. This is an expensive and time-consuming solution and also introduces potential negative effects in the form of increased maintenance burden and the possibility of a spurious actuation of the DAS, resulting in a plant transient.

More recently, there has been an increased focus on digital upgrades primarily for non-safety control systems and, in a few instances, upgrades of safety systems. However, for the most part, these upgrades have not involved the extensive use of digital instrumentation, but rather are based on continued reliance of the analog instrumentation that was originally installed in the plants. Even for systems that are not highly-safety significant, there is still a substantial burden to demonstrate low probability of being affected by a SCCF. As an added concern, electronic components on which digital technology is based can be more susceptible to harsh environments and therefore cannot be located in some of the plant areas as their analog counterparts. These considerations are described in more detail in Section 5 of this report, Licensing and Qualification Issues.

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.

2.2 The Challenge of Digital Technology Qualification for Plant Instrumentation

Up to the present time, the SCCF issue has been mainly a concern of the protection and control systems, and not the instruments that supply the process signals into these systems, which have, for the most part, remained analog in both current and new plant designs. Including the instruments in this analysis would introduce a whole new dimension of complexity in the analysis if a SCCF had to also be assumed among the instruments. The analysis would affect both diversity and defense-in-depth.

Regarding diversity, a typical instrumentation design would have three or four redundant, independent channels for each safety-related process parameter in order to meet the regulatory-imposed single failure criterion and to allow for a channel to be out-of-service for testing or repair. Even for non-safety related instrument applications, especially those important to plant production, equipment protection, and personnel safety, redundant instrument channels are typically used to eliminate single failure vulnerability. In either case, it is common practice for the redundant instruments to be of the same manufacturer make and model number, in order to reduce the burden on design engineering, maintenance procedure development, number of spare parts, and number of technician qualification requirements.

For the use of analog instruments, common cause failures for design deficiencies, manufacturing errors, and maintenance errors do not have to be assumed for the purposes of single failure analysis. [4]

On the contrary, digital computers used in safety systems must consider the possibility of susceptibility to SCCF. [5] This requirement is applicable to nuclear plant safety-related instruments that are based on digital technology. Again, 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 D3 analysis would be to require an instrument signal diverse from these instruments on which to base a DAS to cope with a SCCF.

Regarding defense-in-depth, plant protection is based on four echelons of defense as described in the Nuclear Regulatory Commission (NRC) Standard Review Plan, NUREG-0800 Chapter 7 Branch Technical Position (BTP) 7-19 [6], which are listed as:

1. the control system
2. the reactor trip system
3. the engineered safety system
4. the monitoring and indicator system

The safety-related instruments supply signals to the reactor trip system and engineered safety system, as well as provide reliable indicators for operators to monitor the plant

and conduct manual actions. They also supply signals to the plant control system, which is not safety-related. This is achieved by splitting the signals and using isolators to ensure that failures in the control system cannot affect the reactor trip system, the engineered safety system, or the monitoring and indicator system.

The reasons for using common instruments are:

- It is very costly to design, implement, and maintain these instrument applications and therefore, the number must be minimized.
- It is difficult to physically locate multiple instrument sensors at the same plant location such that they are measuring the same process values. Otherwise, compensations factors would have to be used which would complicate the design and increase measurement uncertainty.
- It is desirable for all of these systems to operate on a consistent set of plant parameters so that the systems are not subject to measurement variations introduced by multiple instrument systems.

However, under this design concept, the safety-related instruments are common to all four echelons of defense and therefore they could all be affected by a SCCF.

Therefore, the use of common, safety-related instruments of the same manufacturer make and model number would impact both diversity and defense-in-depth. BTP-19 requires that:

- The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.
- If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function.

  Note: in the context of BTP-19, the term “common mode failure” is synonymous with the term software common cause failure (SCCF).

As stated in the second point, the remedy for a postulated SCCF would be to introduce a diverse instrumentation system. This would be quite problematic due to the cost, design complexity, and the difficulty of physically-installing additional instruments at the required plant system locations.

It is possible that devices of different manufacturers (or even different model numbers of the same manufacturer) could be used within the redundant channels of a given instrument function. However, as previously stated, this substantially drives up cost and long-term maintenance cost. It also results in slight performance differences among the redundant channels. In addition, there are few offerings for safety-grade digital instruments in the marketplace today, restricting the available choices for multiple devices for the same application.

On a plant scale, the few available choices of digital instruments would have to be used over and over again in various plant systems that compose the four echelons of defense, including supplying signals through isolators to the non-safety control systems. And this is the typical case in the operating plants today, where a given analog instrument is used in multiple instrument applications across many systems. An example would be the use of a Rosemount 1153 pressure transmitter used in pressure, level, and flow instrument applications supplying signals to the reactor protection and emergency core cooling systems. The result of assuming a SCCF on any given device would be to impair many systems at the same time.

2.3 The Practical Effect on Digital Sensor Technology Implementation

The current regulatory framework for SCCF does not provide a means for determining how much diversity in a design is sufficient. It is possible that within given manufacturer's make and model there could be sufficient diversity to minimize the probability of a SCCF due to other factors, including diverse software development. The manufacturers do not offer these options today because there are no objective criteria for determining how much diversity is enough, and therefore no objective way to credit this diversity in the analysis (as sufficient to preclude a SCCF).

As a result, the current operating fleet owners are reluctant to upgrade these instrument channels to digital counterparts, even where there is a digital counterpart of the same fit, form, and function. In these cases, the digital counterparts could reasonably be expected to fit into the same instrument panels without physical modifications. However, these upgrades would immediately invoke the requirement for D3 analysis, which would likely result in the DAS requirements described above. This is not a trade-off they would likely make to gain the performance benefits of the digital replacements.

It is similarly clear why nuclear plant designers involved in the new builds prefer analog safety-related instruments in spite of the potential performance gains with the digital counterparts. It is difficult enough to deal with this issue in the protection and control systems, without involving the instrument signal inputs into these systems. In addition, the nuclear plant designers have little incentive to pursue this in that it increases engineering and regulatory risk during what is a time-critical design and licensing period for new builds. They have no financial stake in the long-term maintenance costs for the plant. On the contrary, they stand to lose money if the design and regulatory approvals are delayed due to unresolved technical issues. Therefore, it is a less-risky path to stick with the familiar analog instrument technology.

The owner-operators could direct the new plant designers to pursue the digital instruments in order to gain the performance and maintenance benefits of the digital counterparts. However, it is not apparent that this sort of analysis has even been undertaken in order to determine the long-term cost benefits of using the digital

technology. The owner-operators seem satisfied to take the least-risk path during the licensing stage even if that means reduced performance of the instrument system and higher maintenance costs over the life of the plant.

Some in the industry have advocated a position that upgrades to digital instrumentation should be pursued as early plant modification following the initial licensing and plant start-up, thus eliminating the technical and regulatory risk during the plant design and construction period. However, this approach is clearly more expensive, delays the benefits, and still incurs sizeable regulatory risk and uncertainty whenever it does occur.

The intent of this project is to call attention to the substantial performance benefits afforded by digital sensor technology over the life of a nuclear power plant. As stated earlier, a related project to this one is being conducted by the Oak Ridge National Laboratory to address the issue of digital technology qualification, and in particular, the matter of SCCF, in order to develop an objective criteria for how much diversity in sufficient in a digital design. The hope is that these two efforts together can mount a compelling case for overcoming the barriers to the use of digital sensor technology and encourage plant designers, plant owners, and instrumentation suppliers to find practical solutions to the current impediments to obtaining these performance improvements.

3. Overview of Plant Process Instrumentation

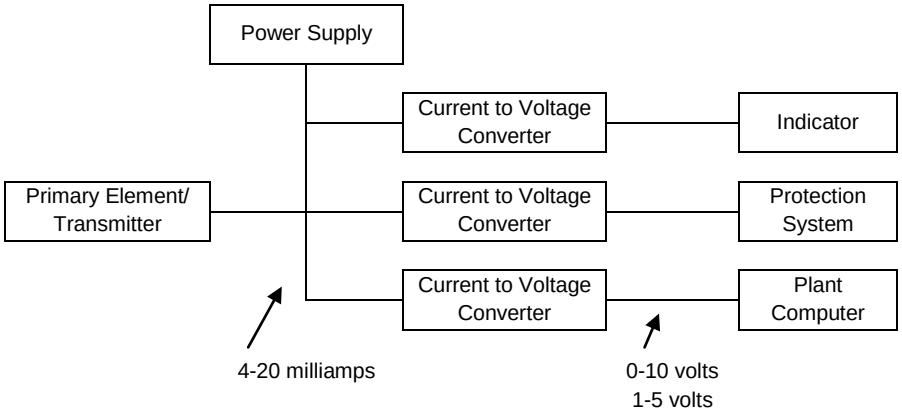
Nuclear plant instrumentation typically consists of a transmitter located close to the monitored process and a power supply and signal conditioning electronics located in the control room. Ideally, each instrument loop would precisely report the true value of the monitored process. Unfortunately, deviations in the signal from the true value occur. Each device in the loop is characterized by its specified accuracy that includes linearity, repeatability and hysteresis. Variations in the temperature where the equipment is located, long term stability, power supply regulation, calibration equipment and other factors can influence the indication. Taken together, these factors cause the indicated value to differ from the true value of the process. The degree to which this deviation may reasonably occur is the uncertainty of the indication.

3.1 Loops

3.1.1 Analog Instrument Loops

In order to communicate the potential benefits of digital instrumentation some background on analog instrument loops is useful. Figure 1 shows a typical configuration of an analog loop. An analog instrument loop consists of a power supply, a transmitter, current to voltage converters, and various output devices. The transmitter develops a 4 to 20 milliamp current proportional to the sensed process. For example, some electronic pressure transmitters convert the force applied to the transmitter into a change in capacitance that is subsequently measured and amplified into current that is conducted through a pair of wires to the control room. Each transmitter has a dedicated cable of several hundred feet that connects the transmitter to the control room components. In the control room, a series of current to voltage converters supply a voltage signal to the output devices. For the protection system, the signal from the transmitter (typically voltage) is compared to a preset voltage (setpoint) using an operational amplifier and if the signal voltage exceeds the setpoint value, protective action is initiated by a series of relay actuations. Protective actuations are typically initiated based on at least two out of three or two out of four logic.

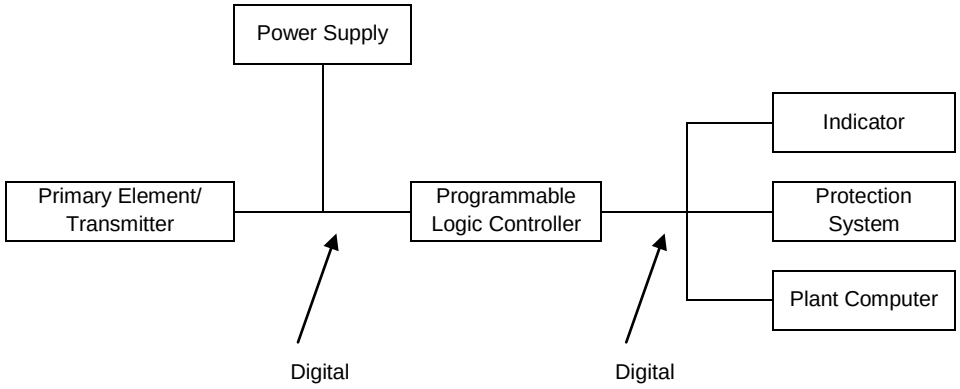
Figure 1 Typical Analog Instrument Loop



3.1.2 Digital Instrument Loops

Digital instrument loops are similar to analog loops in that a loop has a power supply, a transmitter and output devices. Measurement of many process parameters begin as an analog signal using the same technology as analog transmitters, such as a change in capacitance due to the force applied by the pressure. The significant differences in digital electronic transmitters are 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 errors introduced by analog signal processing. Digital signal transmission and processing typically does not introduce significant uncertainty. The data transmission from the transmitter to the Programmable Logic Controller (PLC) is typically a protocol such as Foundation Fieldbus. The transmission from the PLC to various other devices can be either a time-critical protocol or a non-time-critical protocol such as Ethernet.

Figure 2 Typical Digital Instrument Loop



3.2 Transmitters

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 may 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 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 2 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.

3.3 Communication

3.3.1 Current

Conventional analog field instruments typically transmit the signal via a twisted, shielded two conductor cable as a current between 4 and 20 milliamps. Since each transmitter has a unique value, it is necessary to use point-to-point wiring (one wire pair per device) and each two conductor cable is limited to carrying only the process variable signal. A current signal is used to minimize electrical interference issues. For transmitters located in the containment building, the signal cable is routed to a penetration assembly located in the containment wall. This cable is typically several hundred feet. Outside the containment wall, another similar cable is connected to the penetration assembly and is routed to the control room. In the control room, the signal is converted to a voltage signal typically either 0 to 10 volts or 1 to 5 volts.

3.3.2 Digital

Digital process instrumentation communicates with control devices using a digital communication protocol generally referred to as a fieldbus. There are a number of different fieldbus protocols. They communicate by modulating the current. A fieldbus may have multiple transmitters on a single cable since each device on the bus has a unique identification code. This allows multi-drop wiring where a number of unique devices can be connected on a single cable. The number of devices on a single cable varies based on the communication protocol, the communication speed requirements, and other considerations. Limiting the number of transmitters on a single cable to eight or so is a common practice.

Digital communication has encouraged the development of multivariable instruments. Since a single cable can handle multiple variables, transmitters that are capable of measuring two variables are available. For example, a digital differential pressure transmitter may also be capable of measuring the process temperature, permitting a more accurate measurement of the flow rate.

Digital communication networks are capable of two way communication. This permits the installation of transmitters that can be adjusted remotely. This can greatly reduce maintenance burden, and in some cases, worker radiation dose for devices located in such an environment.

3.3.3 Wireless

Wireless networks utilize communication protocols such as IEEE 802.11 to communicate information. For industrial applications, wireless networks are handicapped by the need to provide a permanent power source which requires a cable. Since a cable is required, the reliability of a fieldbus network is favored over wireless. Wireless communication has not been widely implemented in industrial applications. Some common applications that have been implemented are battery powered equipment monitoring devices and closed circuit television security monitoring.

3.4 Output Devices

Common output devices for instrumentation loops are control valves, motor control, indication, automatic component actuation, and input to information systems. The interface between analog loops and the output device is typically a specific type of device suitable for the type of output device being served. As an example, a control valve is typically operated by a current-to-pressure positioner. The positioner is supplied with a 4 to 20 milliamp signal from a controller. The controller is supplied with a signal from the analog instrument loop that is compared to the setpoint, conditioned by the proportional, integral and/or derivative values in the controller, and a conditioned signal is supplied to the positioner.

The interface between digital instrumentation loops and the output devices is typically a PLC or a distributed control system (DCS). Using the same example of valve control, the valve is still operated by a positioner. The positioner can either be digital or analog. The PLC or DCS can supply either a digital or analog signal to the positioner. The system can be arranged such that the digital transmitter can serve as a backup controller in the event of a loss of the normal control loop. Alternately, the digital transmitter can also serve as the controller and provide a signal to the positioner directly.

3.5 Advantages of Digital Loops

There are several significant differences between analog instrument loops and digital instrument loops. Since the signal transmission is digital multiple transmitters can be assigned to a single cable. In addition, many digital transmitters can transmit a second value such as temperature. Digital instrument loops offer improvements in the uncertainty associated with the signal. Transmitters can be re-calibrated and a different range can be established remotely and can perform self diagnostics and notification of problems identified.

Conventional analog field instruments use point-to-point wiring (one wire pair per device) so the wires are limited to carrying only one piece of information such as the process variable. A digital bus doesn't have that limitation since each device on the bus has a unique identification code. This allows multi-drop wiring where a number of unique devices can be connected on a single cable. The number of devices on a single cable varies based on the communication protocol, the communication speed requirements and other considerations.

Traditional analog and discrete devices have no way to tell you 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 may eliminate the need for some routine checks and helps detect failure conditions before they cause a major process problem.

4. Operational Advantages of Digital

In addition to the design advantages of digital discussed in the previous section, there are a number of operational advantages of digital instrument loops. Reduced instrument uncertainty may provide increased operating margin as well as improving the safety margin. Benefits may also be realized with improved reliability, availability and maintainability. Each of these factors is discussed in the following sections.

4.1 Instrument Loop Uncertainty

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 [7] which endorses Part 1 of ISA-67.04-1994 [8]. The principal uncertainty terms which are typically considered are as follows. Other terms may also be applicable.

- Accuracy (linearity, hysteresis, repeatability)
- Drift (long term stability)
- Calibration uncertainties (setting tolerance, measuring and test equipment)
- Environmental temperature (temperature effect on device accuracy)
- Power supply (effect of power supply variations on device accuracy)
- Radiation (radiation effect on device accuracy)
- Seismic (earthquake effect on device accuracy)
- Process considerations (differences between the condition at the location of the sensor and the point of interest)

The ISA standard describes the method of combination of uncertainties that are random, independent, and approximately normally distributed as using the square root of the sum of the squares. Uncertainties that do not meet this standard are typically combined algebraically. This ISA standard defines several terms relevant to the determination of setpoints that provide assurance that nuclear plant safety limits are not violated. Appendix A provides a listing of some of the terms.

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 is shown in Appendix C. 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 summarizes the results of the Appendix C calculation. This example calculation shows a reduction in the total loop uncertainty by a factor of 3.

Table 1 Example Pressure Loop Uncertainty for Reactor Trip

Term	Analog	Digital	Reference (Appendix C)
Sensor Accuracy	0.2500%	0.0300%	7.1.1.1
Sensor Drift	0.4500%	0.1875%	7.1.4.1
Sensor M&TE	0.4240%	0.0300%	7.1.2.1
Sensor Temperature Effect	1.3750%	0.2250%	7.1.5.1
Sensor Power Supply	0.0131%	0.0131%	7.1.10.1
Rack Accuracy	0.7650%	0.0000%	7.1.1.2
Rack Drift	0.5580%	0.0000%	7.1.4.2
Rack M&TE	0.2000%	0.0000%	7.1.2.2
Rack Temperature Effect	0.1125%	0.0000%	7.1.5.2
Sum of squares	3.285E-04	8.775E-06	
Square root	±1.81%	±0.296%	
Process Considerations*	0.3000%	0.3000%	7.2.10
Uncertainty	±2.11%	±0.596%	8.1

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.

Table 2 provides a similar comparison of digital to analog loop for an indication output for the same loop. Since the rack components for a digital loop simply re-transmit the digital signal from the transmitter there is no additional uncertainty associated with them.

Table 2 Example Pressure Loop Uncertainty for Indication

Term	Analog	Digital	Reference (Appendix C)
Sensor Accuracy	0.2500%	0.0300%	7.1.1.1
Sensor Drift	0.4500%	0.1875%	7.1.4.1
Sensor M&TE	0.4240%	0.0300%	7.1.2.1
Sensor Temperature Effect	1.3750%	0.2250%	7.1.5.1
Sensor Power Supply	0.0131%	0.0131%	7.1.10.1
Rack Accuracy	1.0308%	0.0000%	7.1.1.3, .4
Rack Drift	1.7678%	0.0000%	7.1.4.3, .4
Rack M&TE	0.1369%	0.0000%	7.1.2.3, .4
Rack Temperature Effect	0.2670%	0.0000%	7.1.5.3, .4
Rack Power Supply	0.3715%	0.0000%	7.1.10.3, .4
Indicator Readability	0.5000%	0.0000%	7.1.11.4
Sum of squares	7.001E-04	8.775E-06	
Square root	±2.65%	±0.296%	

Process Considerations*	0.3000%	0.3000%	7.2.10
Uncertainty	±2.95%	±0.596%	8.1

A second summary example for steam generator level is shown in Tables 3 (reactor trip) and 4 (indication and control). The significantly improved performance of digital transmitters allows two pressure transmitters, one connected to each upper and lower level tap, to be used in place of a single differential pressure transmitter. The two transmitters are connected electrically with one of the transmitters performing calculations to convert the two pressure values into a digital level value that is transmitted to the control room. To simplify the calculation, the calibrated span and upper range limit are assumed to be the same (150”). From this example calculation, the uncertainty for the digital level system is approximately a factor of 8 more accurate than the traditional analog system. This improvement is due to the improved performance of digital transmitters and, for this application, elimination of the reference leg.

Table 3 Typical Level Loop Uncertainty for Reactor Trip

Term	Analog	Digital	Reference (Appendix C)
Sensor Accuracy	0.250%	0.078%	Typical
Sensor Drift (30 months)	0.200%	0.125%	Typical
Sensor M&TE (typical)	0.250%	0.078%	Typical
Sensor Temperature effect (50ºF)	0.500%	0.140%	Typical
Sensor power supply (1 volt)	0.005%	0.005%	Typical
Sensor Static Pressure span effect (1000 psi)	0.500%	N/A	Typical
Sensor Static Pressure zero effect	0.660%	N/A	Typical
Rack Accuracy	0.765%	0.000%	7.1.1.2
Rack Drift	0.558%	0.000%	7.1.4.2
Rack M&TE	0.200%	0.000%	7.1.2.2
Rack Temperature Effect	0.113%	0.000%	7.1.5.2
Sum of squares	2.050E-04	4.742E-06	
Square root	±1.432%	±0.218%	
Process Consideration	+1.17%	N/A	Typical
Reference Leg Temperature (150", ±50ºF)	-0.500%		Typical
Positive Uncertainty	+2.602%		
Negative Uncertainty	-1.932%		
Uncertainty, two transmitters		±0.308%	

For the digital level indication system there is no uncertainty due to static pressure shift since this uncertainty is unique to differential pressure transmitters which are not implemented in the digital case. Since the rack equipment is merely re-transmitting and displaying the transmitted digital value, there is no uncertainty associated with the

indicator. Finally, since there is no reference leg, the uncertainty due to reference leg temperature variations is deleted.

Table 4 provides a comparison between analog and digital indication outputs for the steam generator level example. For the indication, the digital loop in this example is over 7 times more accurate.

Table 4 Typical Level Loop Uncertainty for Indication

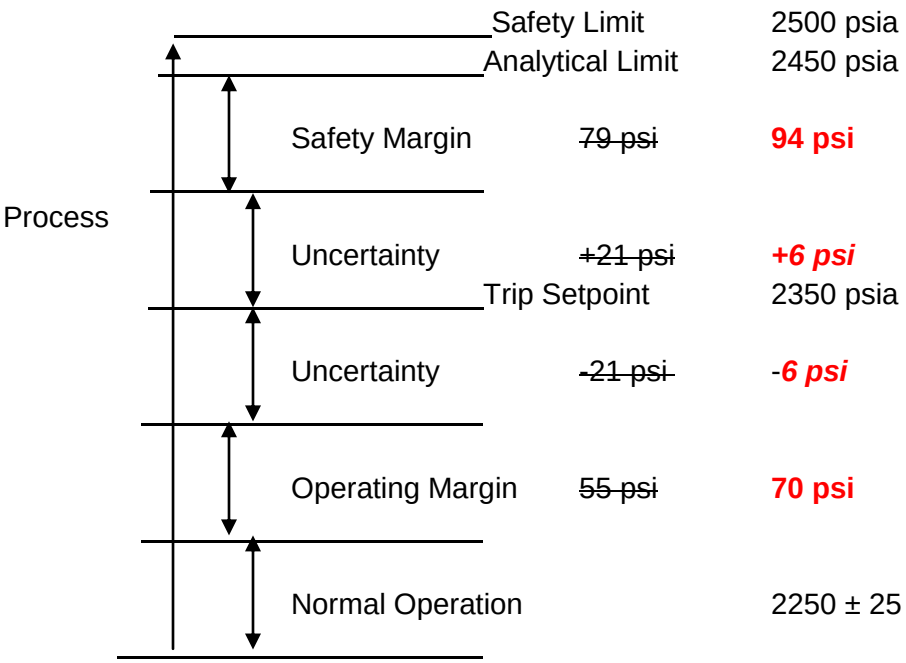
Term	Analog	Digital	Reference (Appendix C)
Sensor Accuracy	0.250%	0.078%	Typical
Sensor Drift (30 months)	0.200%	0.125%	Typical
Sensor M&TE (typical)	0.250%	0.078%	Typical
Sensor Temperature effect (50ºF)	0.500%	0.140%	Typical
Sensor power supply (1 volt)	0.005%	0.005%	Typical
Sensor Static Pressure span effect (1000 psi)	0.500%	N/A	Typical
Sensor Static Pressure zero effect	0.660%	N/A	Typical
Rack Accuracy	1.031%	0.000%	7.1.1.3, .4
Rack drift (typical)	1.768%	0.000%	7.1.4.3, .4
Rack M&TE (typical)	0.137%	0.000%	7.1.2.3, .4
Rack temperature effect (typical)	0.267%	0.000%	7.1.5.3, .4
Rack Power Supply	0.372%	0.000%	7.1.10.3, .4
Rack readability (typical)	0.500%	0.000%	7.1.11.4
Sum of squares	5.766E-04	8.742E-06	
Square root	±2.401%	±0.296%	
Process Consideration	+1.17%	N/A	Typical
Reference Leg Temperature (150", ±50ºF)	-0.500%		Typical
Positive Uncertainty	+3.571%		
Negative Uncertainty	-2.901%		
Uncertainty, two transmitters		±0.418%	

The capabilities of various digital transmitters differ. All will contain an analog-to-digital conversion. A digital transmitter may also include linearization, temperature compensation and damping to improve the accuracy and stability of the transmitter. Combined with the elimination of analog components to regulate the 4 to 20 milliamp signal, these features result in significantly improved accuracy, reduced influence of the environmental temperature and improved long term stability.

So what does all this mean in practical applications? During upset conditions the instrument channel uncertainty is key in defining the margin between the maximum (or minimum) value at which protective action will occur and the values assumed in the plant safety analysis that assure the relevant safety limits are not exceeded. It also establishes the margin between normal and transient process operating values and the minimum (or maximum) value at which automatic protective action might be expected.

Figure 3 is a diagram that illustrates the relationship between the normal operating range for a parameter and the safety limit for that parameter. The safety analysis for the plant establishes an analytical limit for a parameter that provides assurance that the safety limit for that parameter will be observed. The margin and instrument uncertainty is subtracted (or added depending on whether the process is increasing or decreasing toward the safety limit) to establish the trip setpoint. As can be seen from this diagram, the uncertainty has a direct impact on the margin between normal operating values and the safety limit as well as the margin between the normal operation values and the trip setpoint. A reduction in the instrument uncertainty can increase the safety margin, increasing the operating margin to a trip or both.

Figure 3 Parameter Normal Operating Range and Safety Limit Parameters



Appendix C is an example setpoint calculation for a nuclear unit that is reasonably representative of an actual setpoint calculation for high pressurizer pressure. In this example calculation the following values are used. (The referenced section numbers from Appendix C are shown in parentheses.)

Safety Limit	2500 psia	(8.1)
Analysis Limit	2450	(8.1)
Trip Setpoint	2350	(8.1)
Calibrated Span	1000	(7.1)
Loop Uncertainty	±2.1% or ±21 psia	(8.1)
Nominal Operating Value	2250	(8.3)
Operating Band	±25	(8.3)

For this example, the safety margin is equal to the analysis limit less the sum of the uncertainty and the trip setpoint. In equation form,

Safety Margin = Analysis Limit – (Trip Setpoint + Loop Uncertainty)
Safety Margin = 2450 – (2350 + 21)
Safety Margin = 79 psi

The operating margin is difference between the lowest value for the trip setpoint and the sum of the highest normal operating value and the indication uncertainty.

Operating Margin = (Trip Setpoint- Setpoint Uncertainty)– (Nominal Operating Value + Operating Band + Indication Uncertainty)

Rearranging,

Operating Margin = Trip Setpoint– Nominal Operating Value – Operating Band - Setpoint Uncertainty – Indication Uncertainty

The setpoint uncertainty and indication uncertainty can be combined using square root of the sum of the squares.

Operating Margin = $2350 – 2250 - 25 – (18^2 + 9.7^2)^{1/2}$ (8.3)
Operating Margin = 75 – 20.5
Operating Margin = 54 psi

In the Appendix C example, the values for the analog instrument were replaced with values for a digital loop.

Safety Limit	2500 psia	(8.1)
Analysis Limit	2450	(8.1)
Trip Setpoint	2350	(8.1)
Calibrated Span	1000	(7.1)
Loop Uncertainty	±0.6% or ±6 psia	(8.1)
Nominal Operating Value	2250	(8.3)
Operating Band	±25	(8.3)

For this example implementing a digital instrument loop would increase the safety margin by 15 psi (21 – 6) from 79 psi to 94 psi and increase the operating margin by 15 (20 – 5) from 55 psi to 70 psi. These revised figures are shown in red in Figure 3.

4.2 Reliability

Nuclear safety is largely dependent on the reliability of the components that make up the important systems of a nuclear power plant. 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 [9] and IEEE-7-4.3.2-2003 [5].

Reliability is defined in IEEE-352 [10] 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 principles, as stated in IEEE-352, are applicable to the analysis of the effects of components failures on safety system reliability. This is a cornerstone to reactor safety in the regulatory and technical design principles of reactor design around the world. The principles are applicable during any phase of the system lifetime. They have their greatest value during the design phase. During this phase, reliability engineering can make the greatest contribution toward enhanced safety.

4.2.1 Importance of 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.

This affects a variety of critical plant functions – the automatic protection system, the automatic control system, manual operator actions, and the fidelity of alarms. Even in systems that have redundant instrument channels (e.g. 2 out of 4 logic), the actuation logic is degraded and might result in a spurious operation. When there is a single sensor for a particular parameter and it is out of service, the parameter must be obtained in some other way.

Alarms are affected in two ways when sensors fail. Alarms depending on correct sensor functioning might not work. Others could cause a nuisance alarm when plant conditions actually don't warrant the alarm. Nuisance alarms distract the operator and create a false indication in the control room by triggering alarm lights. Nuclear control rooms generally maintain what is referred to as a "dark or black board concept" in the control room, meaning that only valid alarms should be lit. When a false indication will likely be present for an extended period of time, temporary modifications are typically made to the alarm circuitry to extinguish the alarm lamp.

All of these problems result in operator workarounds, meaning that an alternate method of accomplishing a function must be developed and documented. The operators have to be briefed or even trained on the alternate method. The workarounds can add substantially to the mental workload of the operators during design basis events and so they must be analyzed in aggregate and maintained below a level that does not create an undue operator burden.

Also, unreliable plant sensors result in excessive maintenance, which is both expensive and can result in maintenance-induced faults. In other words, frequent maintenance on troublesome components can induce further problems as these components are excessively handled, manipulated, and tested. A good example of this is disconnecting instrument tubing over and over, which leads to fitting wear and future tubing leaks. Therefore, unreliable sensors result in more frequent maintenance, which becomes a

vicious cycle by providing more opportunity for maintenance-induced faults. This problem is described further in Section 4.4 Maintainability.

A search of the Equipment Performance Information Exchange (EPIX) System, maintained by the Institute of Nuclear Power Operations (INPO) confirms that sensor reliability is a common plant problem and the cause of many plant disturbances. The results of this search are found in Appendix D INPO Data Search for Instrument Failures. This search returned hundreds of relevant sensor problems relate to just a portion of the common instrument types (e.g. pressure transmitters). This information confirms that sensor reliability remains a significant concern for safe and productive plant operations. The most common types of failures were:

- Failed capacitors in the power supplies
- Failed sensing lines; due to damage, corrosion, plugging and air intrusion
- Degraded contacts for relays and circuit cards
- Failed terminal lugs
- Failed bellows or diaphragms in pressure sensors
- Leaking or failed fittings for sensing lines

It is notable that most of these failure causes are related to analog sensors. While current digital sensors do share some of the same subcomponents, emerging sensor technologies will eliminate many of them. (Section 6.0 provides a description of the more notable emerging sensor technologies.) This underscores the importance of the nuclear industry transitioning to new digital sensor technologies that are not susceptible to these common, chronic problems.

The reliability of sensors is also an input to the system and component level reliability analysis each nuclear plant performs under INPO AP-913, Revision 2 [11]. This provides a basis for both validation of existing surveillance and maintenance frequencies originally provided by the vendor, and also provides the basis for surveillance extensions if the reliability of the components can be shown to be adequate. Unreliable sensors thus preclude an opportunity to reduce maintenance workload, conserve spare parts, and reduce overall plant operating costs.

4.2.2 Example Reliability Calculation - Temperature Transmitter

A quantitative analysis is typically performed to calculate the predicted reliability or availability (or both) of safety components to ensure they perform their safety functions over specified surveillance periods. A key measure of reliability used by the nuclear industry is the Average Probability of Failure on Demand or PFD_{avg}. The PFD_{avg} is a function of Mean-Time-Between-Failure (MTBF) and the Proof Test (or Surveillance) Interval.

Typically the component supplier will establish the MTBF value for a component based on analysis and operating history, usually following the processes in the following documents.

- Mil-HDBK-217F, "Reliability Prediction of Electronic Equipment” [12]

- ANSI S84.01-1996 “Application of Safety Instrumented Systems for the Process Industries” [13]
- IEEE 352-1987, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems [10]
- IEEE 577-2004, IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities [14]

For the owner-operator, this analysis includes pertinent system interactions and sufficient detail to establish proof test intervals, which are the same as surveillance test intervals. These are set up to be consistent with the operating goals for the system.

Many suppliers base the predicted MTBF upon MIL-HDBK-217F. [12] The vendor has the counts of populations of shipped modules. The published failure rate should result in a predicted number of returns of failed modules. Since suppliers typically track returns and test them for their failure, an actual failure rate can be established and then the vendor can back-calculate the actual MTBF for the population.

To illustrate the reliability improvements afforded by digital sensors over analog, a simple reliability analysis of an analog temperature transmitter is presented followed by an analysis of a digital temperature transmitter associated with a digital control system (DCS). The more complicated digital reliability analysis references Attachment E, which provides the basis for the increased reliability that is gained with a DCS network capable of on-line monitoring and diagnostics, thereby significantly reducing the time to detect transmitter problems.

Digital System Temperature Transmitter Reliability Example Calculation

The reliability of a specific instrumentation design can be quantitatively determined in accordance with IEC 61508 [15] 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. The basic concept in a Markov model is to identify the state of a system and the transitions that occur between such states. A sample calculation is provided in Attachment E, which uses a Markov model to determine the reliability of a digital temperature transmitter as a sensor input to a distributed control system (DCS).

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. Again, the measure of this is the PFD_{avg}. 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 PFD_{avg} 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 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 PFD_{avg}. This capability can also be used to justify longer surveillance intervals.

Examples of the types of monitoring credit in a field-bus application include:

1. The fieldbus communications execute every basic processing cycle and failures are reported, so online monitoring and checking for failures is continuous.
2. The configured channels in each communications processor are polled as determined by the input/output control block attached to that channel and on the time period determined at configuration time.
3. Network connections from the communications processor are monitored in the system monitor. Loss of communication (for any reason) is alarmed.
4. Network switches are able to be monitored using a separate program.
5. Communications links report their health on the processing period that they are configured.
6. Workstations and servers are able to be monitored by staff.

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 [15] 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.

Table 1 in the typical reliability calculation shown in Appendix E depicts all failures for this particular DCS design, separating those that are dangerous from those that are safe. In addition, those that are detected (by online monitoring), can be separated from those that cannot be detected. Approvals for use of the monitoring credits are obtained from nuclear power product testing organizations (such as the European TÜV).

The example digital system reliability calculation in Appendix E illustrates the case of a Markov model for a DCS Programmable Logic Controller (PLC) logic solver with an input string using a typical digital temperature transmitter. The following steps are performed in this analysis utilizing PLC spreadsheets as shown in Appendix E.

1) Select the most significant safety instrumented function for the configuration using system documentation (Logic Diagrams, Input/Output Listings and simplified block diagrams). In this case, it is the referenced temperature transmitter.

2) Select the spreadsheet for the PLC configuration (1 out of 2, 2 out of 3, 2 out of 4, etc.). Develop new spreadsheets for special cases (For example Dual 2 out of 3 PLC configuration).

3) Enter Input/Output module information, proof test interval and mean time to repair into each spreadsheet.

In this 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 the calculation. 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, represented in Figures 3-1 of Appendix E, 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.

From Section 8 of the calculation in Appendix E, the PFD_{avg} of the temperature transmitter is conservatively set at 1×10^{-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 PFD_{avg} 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 PFD_{avg} of the PLC logic solver is also computed and found to be 5.99×10^{-5} over 18 months for a fully integrated DCS (PLC logic solver) with temperature sensor input, as described in Attachment E, Section 8.

The combined PFD_{avg} of the PLC logic solver and temperature transmitter input string are found as follows:

$$PFD_{AVG\text{-}TOTAL} = PFD_{AVG\text{-}LOGIC\ SOLVER} + PFD_{AVG\text{-}TEMPERATURE\ TRANSMITTER}$$
$$PFD_{AVG\text{-}TOTAL} = 5.99 \times 10^{-5} + 1 \times 10^{-7}$$
$$PFD_{AVG\text{-}TOTAL} = 6.00 \times 10^{-5}$$

It should be noted that the PFD_{avg} 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 $PFD_{avg.}$ 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. And since there is no monitoring capability to perform an automatic sensor cross-channel comparison, a single sensor is considered. 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.

On this basis, the PFD_{avg} calculation is somewhat simpler as follows:

$$PFD_{avg} = (1/MTBF)^2 \times TI^2$$

$$PFD_{avg} = (1/73.98)^2 \times 1.5^2$$

$$PFD_{avg} = 4.11 \times 10^{-4}$$

With no on-line monitoring, this is the best PFD_{avg} 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 PFD_{avg} 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 PFD_{avg} to be in the 10^{-5} range.

Implications for Improved Sensor Reliability

At the sensor level, the PFD_{avg} 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 PFD_{avg} is 1×10^{-7} versus the analog sensor PFD_{avg} of 4.11×10^{-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 PFD_{avg} for the temperature function can be calculated as follows:

$$PFD_{AVG\text{-}TOTAL} = PFD_{AVG\text{-}LOGIC\ SOLVER\ (digital)} + PFD_{AVG\text{-}TEMPERATURE\ TRANSMITTER\ (analog)}$$
$$PFD_{AVG\text{-}TOTAL} = 5.99 \times 10^{-5} + 4.11 \times 10^{-4}$$
$$PFD_{AVG\text{-}TOTAL} = 4.71 \times 10^{-4}$$

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 PFD_{avg} value of 5×10^{-5} for an analog instrument design with credited channel checks is assumed with the following results:

$PFD_{AVG\text{-}TOTAL} = PFD_{AVG\text{-}LOGIC\ SOLVER\ (digital)} + PFD_{AVG\text{-}TEMPERATURE\ TRANSMITTER\ (analog)}$
$PFD_{AVG\text{-}TOTAL} = 5.99 \times 10^{-5} + 5.00 \times 10^{-5}$
$PFD_{AVG\text{-}TOTAL} = 1.10 \times 10^{-4}$

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.

4.3 Availability

From a practical standpoint, availability means that a given component is operational or "available for use." The complement term is "unavailability" or the time that the component is "not available for use." The concept of availability is related to reliability as presented in Section 4.2. Obviously, the more reliable a component is, the more it is available. However, actual availability as measured by utilities would also be adjusted for the time a component is taken out of service for preventive maintenance and testing when it is actually in good working order (not having to be repaired).

Availability is a very important concept in the operation of nuclear plants because the plant is at its maximum safe configuration when all components are available, both safety and non-safety. As described in Section 4.2.1, formal operator workarounds are typically imposed when important plant components are unavailable, unless they are specifically designed for this using redundancy. Also, in the case of sensors being unavailable, trip logic for important safety functions could be reduced raising the possibility of spurious operations and resultant plant transients.

Availability is defined in IEEE 352-1987 [10] as follows:

> Availability - the probability that an item or system will be operational on demand.
> (1) steady-state availability is the expected fraction of the time in the long run that an item (or system) operates satisfactorily.
> (2) transient availability (or instantaneous availability) is the probability that an item (or system) will be operational at a given instant in time. For repairable items, this will converge to steady-state availability in the long term.

Standards such as IEEE-603 [9] and IEEE 7-4.3.2 [5] provide guidance that reliability and availability goals should be established. Additionally, availability is analyzed to a high degree, based on plant specific data, following the guidance of INPO AP-913 Revision 2. [11] In Section 2 Equipment Reliability Process Instructions of AP-913, the plant staff is to assemble data based on availability, reliability or condition. Availability is an important performance indicator of system and component health and is typically used to trigger corrective actions if it is not meeting pre-established performance targets.

Similarly, availability is a performance measure often used to support compliance with the NRC's "maintenance rule" or 10 CFR 50.65. This states that license holders will monitor the performance of systems, structures, and components to ensure that they are capable of fulfilling their intended functions. When components such as sensors have poor availability, they can impact the overall availability of important safety systems, which at a certain point, would be considered non-compliance with the regulation. This could lead to adverse regulatory actions.

A quantitative analysis is performed to calculate the predicted availability of the equipment to ensure it performs its safety function over an expected surveillance period. This is usually provided by the manufacturer and is developed as a typical in the example below.

For the vendor, the analysis is performed at a component level to establish the Mean-Time-Between-Failure (MTBF) value for the component based on analysis and operating history and usually follows the processes referenced in Section 4.2.2. For the owner-operator, this analysis includes pertinent system interactions and sufficient detail to establish proof testing intervals, consistent with the operating goals for the system.

A simple availability analysis of the typical analog temperature transmitter referenced Section 4.2.2 is provided below. The analog temperature transmitter has an MTBF of 73.98 years, as noted in Section 4.2.2. The availability is calculated as follows:

$$\text{Availability} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

Where:
MTBF – Mean Time Between Failures
MTTR – Mean Time to Repair (A common value used for MTTR is 4 hrs.)

Therefore:

$$\text{Availability}_{\text{TT-Analog}} = \frac{73.98 \text{ yrs} \times 8760 \text{ hrs/yr}}{(73.98 \times 8760) + 4} = \frac{648064.8}{648068.8} = 99.9993\%$$

It should be noted that this is just the availability of the temperature transmitter (sensor) and not of the entire instrument loop. The actual loop availability will likely be lower due to the availability of the other components in the loop.

As noted in Section 4.2.2, the reliability and availability of a digital sensor can be improved due to continuous on-line monitoring of the health of the device. Again, a MTTR of 4 hours is assumed. Using the example of the same typical digital temperature transmitter that was referenced in Section 4.2.2, the availability can be determined as an inverse relationship of the previously calculated PFD_{avg} of 1×10^{-7} as follows:

$$\text{Availability}_{\text{TT-Digital}} = \frac{1}{(1 + PDF_{avg})} = \frac{1}{(1 + 1 \times 10^{-7})} = 99.99999\%$$

The results indicate improvement in availability for the digital sensor compared to the analog sensor, although both are obviously very good availability numbers. This is because both sensors are highly reliable as indicated by their MTBF values. The actual availability for an entire instrument loop or string would likely indicate an even greater advantage for the digital sensor because it is often the other components in an analog instrument loop that are more prone to failure.

4.4 Maintainability

Maintainability is a measure of the relative burden to keep systems and components in good working order. More than just the direct testing and maintenance, maintainability broadly encompasses the efforts of the entire plant and support organization to ensure that the systems and components will continue to perform their design basis functions.

There are thousands of plant sensors and related components in a typical nuclear plant, making this a very expensive and labor consuming effort. For this reason, improvement in performance that would lead to reduced testing and maintenance requirements would be highly beneficial.

Nuclear plants conduct a very structured program for surveillance testing and preventative maintenance for plant sensors. The surveillance testing for safety-related sensors consists of three levels as required by the plant's Technical Specifications:

> Channel Checks – a qualitative assessment of channel behavior, comparing the channel indication or status with other indications of independent instrument channels measuring the same parameter. These are typically performed every shift or daily.
>
> Analog Channel Operational Test (ACOT) – the injection of a simulated signal into the channel to verify operability of alarm, interlock, and/or trip functions, including making adjustments as needed to set points such that they are within the required range and accuracy. These are typically performed every quarter.
>
> Channel Calibration – the adjustment of the channel such that it responds within the required range and accuracy to known values of input. It encompasses the entire channel including alarm, interlocks, and/or trip functions and may be performed in by any series of sequential, overlap, or total channel steps such that the entire channel is calibrated. These are typically performed every refueling outage.

For non-safety sensors that are not subject to the Technical Specifications, similar surveillances are set up in accordance with good practice and operating experience, such that a sufficient degree of reliability is obtained. The Electric Power Research

Institute is one source of preventative maintenance templates that are based on best industry practice and experience.

Digital instrumentation offers the potential of significant reduction in surveillance testing. Their self-diagnostic capabilities may provide justification to eliminate or at least reduce the frequency of the cross channel comparisons. Likewise, digital instrumentation may permit longer intervals between channel calibrations due to the improved long term stability.

Corrective maintenance is conducted whenever a failure of a component occurs or there is some operating abnormality with the component. Sometimes a modification to a component is needed to correct design problems or upgrade the components because spare parts are no longer available.

Corrective maintenance consists of troubleshooting and repair. For hard failures, the troubleshooting and repair times are relatively minimal. Many hard failures can be identified and repaired in a day. Identification of the source of intermittent problems is a more difficult and time-consuming task. Self-diagnostic features permit early detection and repair of some failures and greatly simplify troubleshooting. Likewise, self-diagnostic capability may identify intermittent failures without time-consuming troubleshooting.

There is a considerable effort expended by the plant support staff to support the instrumentation and control maintenance program. This is typically the largest technical group in the plant's maintenance organization. In addition, the volume of this work is a key driver of the size of the work planning and scheduling organizations. And, it contributes significantly to the workload of other support functions such as safety tagging, quality control, nuclear risk management, operations support of maintenance, and engineering.

The amount of sensor testing and maintenance drives a corresponding workload in Engineering to review the as-found set points for trending, concerns on operability, and possible changes in the frequency of testing. This information is typically analyzed shortly after the maintenance is performed and is documented in the plant's system health program.

Frequent testing of safety-related sensors puts the plant at increased risk of spurious plant trips and other safety feature actuations. This is because the sensor channels that are being tested must be put in a trip condition (except when the plant can "bypass" the channel under the requirements of NRC Regulatory Guide 1.47 [16]) which typically satisfies half the logic for an actuation. This means that if there is a momentary excursion on a redundant channel that exceeds the setpoint, the safety actuation will occur. Sometimes this occurs due to a "wrong component" event, when the maintenance crews unwittingly work on two redundant channels.

A key advantage to less-frequent testing and maintenance is the avoidance of maintenance-induced failures. Unfortunately, an appreciable percentage of sensor channel failures are due to faulty maintenance practices, in spite of all the efforts to control the quality of the work. The maintenance organization typically tracks this as "rework." Another contributor is the early failure of newly-installed spare parts, due to some inherent manufacturing defect. And, just performing work on the devices can cause wear and damage, such as disassembling and reassembling instrument tube fittings, which are then prone to leakage.

In terms of maintaining a highly-competent maintenance and support workforce, a transition to digital sensors will enrich jobs and produce a better alignment to the knowledge and skills being taught in technical schools. This is a concern today when the utilities have to assume the entire burden of job skill training for dated technologies. Job skill development for maintaining modern digital sensors, including the advanced test equipment, will be an important factor in attracting and retaining a highly-qualified and motivated workforce in the future. Otherwise, engineers and technicians will be concerned that their technical knowledge and job skills are falling behind marketplace demands and that their personal marketability is declining.

In summary, digital sensors offer significant benefits in regard to the maintainability of the plant instrumentation and control systems in the areas of plant work reduction, cost reduction, safer operations, and improved job satisfaction. These benefits continue for the life of the nuclear plant and should support the business case the make this digital transition.

5. Qualification and Licensing Considerations

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 burden over what is required for analog sensors is potentially significant and can cause cost increases and delays in plant upgrades or new designs. Further work to reduce these burdens is needed so that the long-term benefits of using digital sensors in nuclear power plants are reasonably obtainable. The major areas of consideration are:

Qualification Considerations:

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

- Cyber Security

Licensing Considerations:

- Nuclear Plant Modifications under Licensee Control
- Nuclear Plant Modifications under NRC License Amendment
- Improvements in Plant Technical Specifications
- Certification of New Nuclear Plant Designs

The sections below provide a discussion of these qualification and licensing considerations and address issues and concerns that need resolution to encourage greater use of digital sensors.

5.1 Qualification Considerations

Qualification is the process of demonstrating that a component or system meets its specified requirements. The requirements are derived from the design bases of the various systems of the nuclear plant, which in turn rest on system performance objectives, regulatory requirements, consensus standards, and other forms of technical criteria. Certain qualification topics are either specific to, or have special considerations for, digital systems, including digital sensors.

5.1.1 Software Quality

Each nuclear plant is required to have a Quality Assurance Program for safety-related systems and components, with the program conforming to 10 CFR 50 Appendix B Quality Assurance Criteria for Nuclear Power, Plants and Fuel Reprocessing Plants [17]. In addition, 10 CFR 50.55 a(h) requires that protection and safety systems comply with IEEE-603-1991. [9] This standard endorses IEEE 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems on Nuclear Power Generating Stations [5], as the most general statement of requirements for use of digital in safety-related designs. It, in turn, references a number of other IEEE standards that are concerned with various stages of the software development and implementation life-cycle. IEEE 7-4.3.2 requires a software quality program consistent with the requirements of IEEE/EIA 12207.0-1996 for all software that is resident at run time.

The Quality Assurance Plan must address the special quality requirements particular to digital systems.

The NRC's Standard Review Plan, NUREG-0800, Chapter 7, Branch Technical Position (BTP) – 14, entitled *Guidance for Software Reviews for Digital Computer-Based Instrument and Control Systems* [18], provides a description of the software development process for the programmable based (digital) sensors. The software development process is a requirement of the Quality Assurance Program under 10 CFR 50 Appendix B Criterion III, Design Control. A graded approach to the software development process is normally used to take into account the complexity of the software being implemented within the digital sensor. Simple programs would require less depth when compared to complex programs. However, this is very difficult to judge

and can lead to regulatory concerns. Great care should be taken during the judgment of the complexity of the software. Justification for this decision should be substantial.

5.1.2 Environmental, Seismic, and Electromagnetic Compatibility (EMC) Qualification

Sensor qualification is mainly concerned with three major topics:

- environmental
- seismic
- electromagnetic compatibility (EMC) qualification

The environmental, seismic, and EMC qualification for digital based sensors is basically the same qualification process as used for the qualification of analog sensors. The objective of equipment qualification is to demonstrate that the safety sensors are capable of performing their specified safety functions during and following a postulated event. For sensors, the analysis should determine whether they are capable of performing their functions in both normal and accident environments.

Digital sensors typically have a greater susceptibility to environmental factors compared to their analog sensors due to the more sensitive electronic components within the sensor. This can restrict where the sensors can be located.

The safety-related sensors must be qualified to the requirements of IEEE Std. 323-2003 [19], as augmented by NRC Regulatory Guide 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants. [20] When a components is to be located in a harsh environment, where qualified heating, ventilation, and air conditioning (HVAC) is not provided, the qualification is performed by a heat rise test and a subsequent analysis using linear temperature data extrapolation. The analysis must demonstrate, using extrapolated test data, that individual component and equipment temperature specifications are not exceeded within the sensor housing when exposed to the environmental conditions as specified.

In addition, radiation qualification must be performed for sensors located in a harsh environment. The radiation levels are determined by radiation measurements or historical data taken for the respective area. Normal radiation qualification is based on analysis for mild areas, where sensors are preferred to be located if the design can accommodate it. However, sensors that have to be located in areas of the plant that could be exposed to higher levels of radiation during design basis events require more stringent radiation testing.

For seismic qualification, safety-related sensors must be qualified by test, analysis or a combination of both methods in accordance with IEEE Std. 344-2004 [21], as endorsed by RG 1.100 [22]. Functional operability tests must be conducted during seismic qualification tests with the equipment energized using simulated inputs and interfaces.

The safety I&C system sensors must be qualified for EMC in accordance with MIL Std. 461E Requirements for the Control of Electromagnetic Interference Characteristics for Subsystems and Equipment [23] and IEC 61000 Part 4 Series [24] as augmented by

NRC Regulatory Guide 1.180 [25]. EMC testing of the equipment is performed for both conducted and radiated signals as follows:

- EMI/RFI emissions
- EMI/RFI susceptibility / immunity
- Surge withstand capability

These tests are performed on each sensor in various modes of operation such that successful completion of the test demonstrates that the safety system function has not been compromised and the sensor performs within its design specifications. The selection of the specific tests and operating envelopes (test level, applicable frequency and limitations) is based on NRC Regulatory Guide 1.180. For digital based sensors, this could be a harsher environment.

Due to the difficulty of qualifying digital sensors based on sensitive electronic components for harsh environments, the commercial offerings currently available are for mild environments. At the present, the nuclear plant designers and owners are apparently satisfied to continue to use analog sensors in safety-related harsh environment applications rather than pursue this option with the sensor suppliers. This qualification work must ultimately be undertaken by either the sensor suppliers or the plant owners if the full value of digital sensors is to be obtained.

5.1.3 Reliability, including Software Common Cause Failure

Safety-related sensors must be designed for high reliability using qualified sensor equipment. The reliability of these system configurations to perform their safety functions is demonstrated via a reliability analysis and a Failure Modes and Effects Analysis (FMEA).

The reliability analysis is a quantitative analysis using the same quantitative process as used for analog sensors. Software is not part of this analysis as software is not assigned a quantitative value for reliability. The FMEA is a “qualitative” evaluation which identifies various failure modes that can occur to the components of interest, such as sensors. The FMEA identifies significant single failures and their effects or consequences on the system’s ability to perform its functions.

The reliability analysis and the FMEA are performed for protection systems' sensors in conjunction with the remaining portions of the instrument string, including the bistable/coincidence and actuation logic. The FMEA is prepared conservatively assuming that one protection instrument string including the sensor is already bypassed for maintenance.

An unavailability analysis is performed on the sensors to assess their unavailability when they are requested to perform their function. The analysis quantifies the probability that the sensors would fail to provide a trip or actuation signal when required. As noted above, these analyses are similar to those used for analog sensors.

The possibility of software common cause failures (SCCFs) of more than one echelon of defense is the primary concern in considering postulated failures within the echelons

including sensors used for defense-in-depth. These failures can be caused by interdependencies between these echelons. The problem becomes one of specifying the degree of dependencies, as it is impossible to have four completely independent echelons when certain features must be shared due to the commonality of the architecture and personnel. Physical and electrical independence is only one of the dependencies under analysis. The second is the CCF caused by shared hardware features such as power supplies, sensors or other equipment. The third and the one under consideration in the D3 assessment is shared software between digital based equipment such as sensors that leads to a SCCF between and within the echelons. This is of particular concern where sensor information is shared between echelons such as the RTS, ESFAS and control as well as indicators used by the operator to establish successful manual control in the mitigation of a postulated event. In other words, all four echelons could be compromised by the same SCCF due to the sharing of digital sensor output between the echelons.

The selection of digital based sensors with either firmware or programmable software leads to an analysis of the SCCF concern. This is considered to be one of the major licensing differences between analog and digital based sensors.

The installation of a digital based protection sensor that includes the Reactor Trip System (RTS) functions and the Engineered Safety Feature Actuation System (ESFAS) functions presents a licensing concern that a postulated SCCF of this digital sensor might propagate in such a fashion that could defeat the required safety functions. A Diversity and Defense-in-Depth (D3) evaluation must be performed that demonstrates that there is sufficient defense-in-depth and diversity to cope with a postulated SCCF to the digital based sensors in the RTS, ESFAS including the credited control and Diverse Actuation Systems (DAS), which must include diverse sensors. Where the concern of SCCF cannot be eliminated, the RTS and ESFAS functions must be ensured by the addition of a DAS using diverse sensors that automatically actuates reactor trip and engineered safety feature functions using a select group of input parameters.

The NRC has established a methodology and acceptance criteria for D3 evaluations that are to be used when digital based systems, including sensors, are implemented in the RTS and ESFAS at operating nuclear power plants and for new plants. The NRC's Standard Review Plan, NUREG-0800, Chapter 7, Branch Technical Position (BTP) – 19, Guidance for Software Reviews for Digital Computer-Based Instrument and Control Systems [26] and NRC NUREG/CR-6303 [27] document the methodology and acceptance criteria.

1. *The applicant/licensee should assess the diversity and defense-in-depth of the proposed instrumentation and control system to demonstrate that vulnerabilities to common mode failures have been adequately addressed.*
2. *In performing the assessment, the vendor or applicant/licensee shall analyze each postulated common mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate*

methods. The vendor or applicant/licensee shall demonstrate adequate diversity within the design for each of these events.

3. *If a postulated common mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common mode failure should be required to perform either the same function or a different function that provides adequate protection. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.*
4. *A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in Items 1 and 3 above.*

Points 1, 2, and 3 of the following Nuclear Regulatory Commission (NRC) position discussed in BTP 7-19 apply to digital sensor modifications to nuclear plants. Point 4 also applies in that the display information has to be from a diverse sensor.

The simplicity of the software used within the digital based sensor can become a significant factor in the D3 analysis process. However, to prove simplicity for this analysis, exhaustive software testing (all paths used and unused unless terminated) is required. Achieving complete testability is discussed in BTP 7-19. This can be very difficult to achieve except in the simplest of digital sensor designs.

5.1.4 Communications

Digital based sensors are able to take advantage of advanced digital communication technology such as HART, Field Bus, ProfiBus, and other such industry standards. However, such usage raises the question of compliance with the NRC's Digital Interim Staff Guidance (ISG) – 04 [28], Digital communication links offer capabilities that could conflict with certain requirements specified in 10 CFR 50.55 a(h) (namely IEEE 603-1991 and IEEE 7-4.3.2) in regard to the requirements of separation and independence of redundant instrument channels. These are applicable to safety digital sensors transmitting information to the protection systems and the control systems through isolators.

To clarify, the NRC's position is that an ISG does not create requirements, but is a summary of existing requirements and provides guidance to the NRC staff in reviewing licensee designs and design changes subject to those requirements. More importantly, an ISG can be taken as a summary of the NRC's interpretation of those requirements. ISG-04 is composed of four basic areas of interest:

1. interdivisional communications: communications among different safety divisions or between a safety division and a non-safety entity
2. command prioritization: selection of a particular command to send to an actuator when multiple and conflicting commands exist

3. multidivisional control and display stations: use of operator workstations or displays that are associated with multiple safety divisions and/or with both safety and non-safety functions
4. digital system network configuration: the network or other interconnection of digital systems that might affect plant safety or conformance to plant safety analysis assumptions (interconnections among safety divisions or between safety and non-safety divisions should also satisfy the guidance provided for interdivisional communications)

The first and fourth areas are the most applicable to the implementation of digital sensors.

Digital sensors are also subject to the requirements stated in 10 CFR 50 Appendix A, General Design Criteria [17]. This guidance specifically addresses issues related to interactions among safety divisions and between safety-related equipment and equipment that is not safety-related. This guidance also addresses non-safety digital control systems that might affect the plant conformance to safety analyses (accident analyses, transient analyses, etc.).

Digital sensors are most beneficial when implemented with digital communications technology, even though most commercial digital sensors are able to interface to conventional analog communications technology such as 4-20 mA current loops. However, the use of the digital communication technology is admittedly encumbered with this additional analysis and potential regulatory review.

5.1.5 Cyber Security

Unlike their analog counterparts, digital sensors must be protected from cyber attacks. Regulatory requirements for cyber security are found in 10 CFR 73.54 [29], which requires a cyber security program and a cyber security assessment of all critical digital assets to determine if any cyber vulnerabilities exist.

The security assessment consists of two parts; computer security and cyber security. Computer security is established during the design phase and primarily uses the guidance provided in NRC Regulatory Guide 1.152 [30], which provides guidance for compliance with cyber security requirements during the development life cycle phases such that the digital hardware and software are developed in a secure environment. It is better if this is performed by the digital sensor vendor during the component design and manufacturing process, but could be verified by the licensee or a third party after the design if the right processes were followed and adequate quality records were available for audit. In any case, the nuclear plant licensee is the party that is legally responsible for the accuracy and completeness of this assessment, and therefore must provide oversight of this process.

NRC Regulatory Guide 5.71 [31] addresses cyber security for the testing, operational, and retirement life cycle phases, which provides guidance on how to protect critical digital assets (CDA) from cyber-attacks. A CDA is a subcomponent of a critical system that consists of or contains a digital device, computer or communication system or

network. In turn, a critical system is an analog or digital technology-based system in or outside of the plant that performs or is associated with a safety-related, important-to-safety, security, or emergency preparedness function.

The industry has developed a template for an industry standard cyber security program to comply with the NRC's cyber security requirements through an effort sponsored and facilitated by the Nuclear Energy Institute (NEI). This template was published as NEI 08-09 [32], which was subsequently endorsed by the NRC. NEI 08-09 provides guidance on the necessary elements of a cyber-security plan, how to analyze digital computer systems and networks for cyber-vulnerabilities, and how to establish, implement, and maintain a cyber-security program.

Safety-related and important-to-safety digital sensors would be categorized as CDAs and would therefore fall under the requirements of the licensee's cyber security program. This would require an analysis of wide range of potential mitigation strategies and the implementation of those that are determined to be applicable. This requirement is yet another reason that nuclear plant designers and plant owners have been reluctant to use digital sensors in applications that would be subject to these requirements. Therefore, additional efforts are needed by or on behalf of the industry to resolve these issues in a cost-effective manner.

5.2 Licensing Considerations

5.2.1 Nuclear Plant Modifications under Licensee Control

In order to upgrade existing analog sensors to digital, a regulatory analysis must be performed to determine under which regulatory process the change must be conducted, either under licensee control or under NRC license amendment as described in Section 5.2.2.

The requirements in 10 CFR 50.59 [17] define the criteria that establish when a license amendment is required before implementing plant changes. The criteria of 10 CFR 50.59 apply to sensor modifications for both safety and non-safety systems.

If the criteria are met for the change, no license amendment is required. If not, the change can only be implemented after receiving a license amendment under the requirements and process specified in 10 CFR 50.90 [17]. Nuclear Energy Institute NEI 01-01 [33] provides guidance to licensees on performing 10 CFR 50.59 evaluations for digital upgrades such as digital sensors. NEI 01-01 was the co-publication of the Electric Power Research Institute (EPRI) TR- 102348, Revision 1, Guideline on Licensing Digital Upgrades [34]. Regulatory Issue Summary (RIS) 2002-22 [35] communicated the NRC's endorsement of NEI 01-01 for use in determining the appropriate regulatory process for digital upgrades such as digital sensors. RIS 2002-22 also specifies certain staff positions on several aspects of the digital design and licensing processes.

One particular screening criterion for a digital upgrade is whether it requires a change to a nuclear plant's Technical Specifications. Such changes can be made only under a license amendment. However, upgrades usually would not require a Technical Specification change as long as the change was maintained the same design. In other words, the current design is maintained if just the sensors themselves were being upgraded on a like-for-like basis and there were no changes in how the design was configured or functioned (such as changes to the set points or number of channels).

However, if a reduction in the surveillance requirements specified in the Technical Specifications was desired to take advantage of digital sensor capabilities, then a license amendment would be required. (Refer to Section 5.2.3)

Consideration of software common cause failure (SCCF) is required regardless of the safety significance of the digital sensor. This can be a key factor in determining whether the criteria of 10 CFR 50.59 are met, meaning that a license amendment is not required. Two of the most applicable criteria to this question are:

> Criterion 2: Does the activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of a SSC (system, structure, or component) important to safety?
>
> Criterion 6: Does the activity create a possibility of a malfunction of an SSC important to safety with a different result?

In this context, consideration of SCCF involves the determination that failure due to software is "sufficiently low," that is, much lower than other failures that are considered in the nuclear plant's Updated Final Safety Analysis Report (UFSAR). Regarding the possibility of a malfunction with a different result, this is not necessarily a new type of malfunction, but a malfunction that is not bounded by those already evaluated in the UFSAR.

The NEI 01-01 guidance indicates that, for digital upgrades to systems that are highly safety-significant, licensees should perform a defense-in-depth and diversity analysis as part of the design process to ensure that the plant has adequate capability to cope with software common-cause failure vulnerabilities. (Refer to Section 5.1.3)

In summary, the guidance of NEI 01-01 must be carefully applied in the upgrade of analog sensors to digital to ensure that the change is made under the correct regulatory process. Due to the special considerations of a software-based plant component, there is extra burden on making this determination and the regulatory consequences of failing to obtain a license amendment when it is required can be quite high. And so, the additional burden and regulatory risk to correctly assess these special digital issues is potentially a factor in a plant owner's decision to either stay with analog sensor technology or to upgrade to digital sensor technology.

5.2.2 Nuclear Plant Modifications under NRC License Amendment

For cases where the 10 CFR 50.59 [17] criteria results in the need for NRC review and approval of the plant change, a license amendment for the nuclear plant must be obtained. The requirements for this are stated in 10 CFR 50.90. [17] Depending on the

scope of the license amendment, the process can be lengthy and costly, with no certain outcome as to approval. In fact, there is some risk that the NRC will impose additional design and testing requirements that were not accounted for in the original project estimate.

To ensure a more consistent and predictable process for a license amendment for digital upgrades, the NRC issued ISG – 6 [36] to provide detailed guidance for all phases of the process. ISG – 6 is currently in a pilot project evaluation phase as it is being used on a large highly-safety significant digital upgrade at a large U.S. nuclear plant. While this upgrade project is not yet complete, ISG – 6 is currently available for use by any of the domestic nuclear plants and represents the best regulatory approach for cases where the implementation of digital sensors requires a license amendment.

The need for a license amendment for the upgrade of analog sensors to digital would be a formidable barrier for a number of nuclear utilities, due to the cost, time, and risk involved. Therefore, this is yet another impediment to obtaining the benefits of digital sensors. This highlights the importance of the Oak Ridge National Laboratory project to provide objective criteria for how much diversity is sufficient to resolve the SCCF question, and thereby reduce the number of digital sensor upgrades that would potentially require a license amendment.

5.2.3 Improvements in Plant Technical Specifications

One major advantage with the implementation of software-based digital sensors is the ability to use on-line diagnostics including self-monitoring and self-calibration. Digital sensors have the capability to perform self-checks by continuously monitoring sensor health and then automatically annunciating or indicating when sensor problems arise. As a result, traditional test provisions for analog sensors may not be needed for the digital sensors because of these automatic diagnostic design capabilities. These diagnostic capabilities may be used to reduce the surveillance testing stated in the Technical Specifications. This could be of great benefit in reducing operations and maintenance costs without impacting nuclear safety. This could include channel checks, functional testing, and calibrations.

However, precautions are necessary to ensure that the requirements of the Technical Specifications are maintained. Unless granted on a generic basis, the approval for surveillance extensions must be granted on a plant-specific basis. The critical area for Technical Specification relief is the crediting of the on-line monitoring feature provided by the digital sensor. This would involve checking the output of the digital sensor to determine if performance criteria are being met. This includes whether it is operating inside or outside of acceptable limits and whether self-calibrations are sufficient to replace manual calibrations of the sensor. This can provide relief on channel check frequency or even a total replacement and perhaps relief on the frequency of transmitter calibrations, saving a considerable amount of plant personnel time. Of course, this is all dependent on maintaining TS requirements and meeting regulatory requirements.

There are many benefits to this monitoring capability, including non-intrusive continuous testing, decrease in radiation exposure, and a continuous evaluation of the sensor

installation and process conditions. However, there are certain features that have to be analyzed, such as the safety level of the on-line monitoring capability, the annunciation of fault conditions or out-of-tolerance conditions either through automatic or manual means, and the bypass and inoperability alarms.

Provisions for digital sensor and network diagnostics as well as the measurement of channel drift history, can be credited according to NEI 04-10 Rev 1 [37] to address the extension of surveillance test intervals for equipment covered by Technical Specifications. The NRC has authorized licensees to make changes to Technical Specification surveillance intervals in its Safety Evaluation Report for NEI 04-10, Rev 1 [38]. This program establishes a Surveillance Frequency Control Program (SFCP) which ensures that surveillance requirements specified in the Technical Specifications are performed at intervals sufficient to assure the associated Limiting Conditions for Operation are met. The regulatory programs for Maintenance rule (10 CFR 50.65), as well as corrective action programs identified by 10 CFR 50 Appendix B, require monitoring of test failures and require action to be taken. The approach for changing surveillance frequencies uses existing Maintenance Rule guidance as well as Regulatory Guide 1.175 [39], to develop risk-informed test intervals for equipment covered by Technical Specifications. In Section 4 of NEI-04-10 Rev 1, Step 7, credit can be taken for benefits of early detection of potential mechanisms (as is provided in digital system online monitoring and diagnostics) and degradations that lead to common cause failures. This and other potential credits are inputs to the risk analysis and Probabilistic Risk Assessment (PRA) for each nuclear plant, which can be used to justify the extension of Technical Specification surveillances.

5.2.4 Certification of New Nuclear Plant Designs

For new nuclear plants, the NRC has provided a more streamlined plant licensing process as compared with the process that was used in the first generation of plants, which formerly required first a construction license and then an operating license at the time the plant was completed. The new process is known as a Combined Operating License (COL), for which the requirements are found in 10 CFR 52 [40].

However, for technical requirements, 10 CFR 52 refers to many of the same standards and regulatory guidance that are applicable to the currently operating nuclear fleet. This includes the NRC's Standard Review Plan, NUREG-0800, and in particular Chapter 7 for I&C concerns. Therefore, requirements for qualification of digital designs, including SCCF, remain the same.

Under 10 CFR 52, plant designers apply for approval of a Design Certification Document (DCD), which can be referenced by any prospective plant owner/operator in their application for a COL. Recognizing that a number of design details would not be known at the time of DCD submittal, the NRC provided for concept of Inspections, Tests, Analysis, and Acceptance Criteria (ITAAC), and a special subset of ITAAC known as Design Acceptance Criteria (DAC). This was especially important for digital designs in that certain aspects are not yet known at the time of general plant design certification.

This way, the NRC can verify them later in the process to avoid holding up the general design certification.

This concept under 10 CFR 52 reduces regulatory risk in the licensing of new nuclear plants because it because questions about new digital sensors would not necessarily hold up the overall plant certification, assuming that the outstanding information was granted either DAC or ITAAC status by the NRC.

5.3 Summary of Qualification and Licensing Considerations

It is evident that there are substantial burdens in implementing digital sensors that must be overcome if the industry is to obtain the long-term operational benefits of digital sensors. So far, these factors in various combinations have been a significant impediment to the use of digital sensors in both operating plants and new reactor designs, especially for safety-related applications,

The following is a summary of the key areas where the burden needs to be reduced through the efforts of digital sensor suppliers, nuclear plant designers, and nuclear plant licensees if there is to be wide-spread adoption of digital sensors.

- Methodologies for determining software quality
- Environmental hardening (temperature, pressure, radiation, electro-magnetic)
- Objective criteria for determining how much diversity is sufficient to alleviate SCCF concerns
- Clear acceptance criteria for special digital concerns such as digital communications and cyber security
- Enhanced guidance for 10 CFR 50.59 evaluations with respect to SCCF
- Proven process for digital license amendments that is consistent and predictable, thereby allowing the reasonable management of project cost, schedule, and risk.

Two positive considerations for digital sensor implementation in the licensing area are also noted. There is a proven process under NEI 04-10 for obtaining improvement in Technical Specification surveillance intervals, thereby providing the means to capture the benefit of digital sensors in applications governed by the Technical Specifications.

Also, for new plant designs, the DAC and ITAAC processes reduce regulatory risk to the overall plant certification for certain issues that cannot be determined or resolved at the time of Design Certification application. This factor can make it more attractive to pursue the long-term benefits of digital sensors without incurring undue risk to the Design Certification schedule.

6.0 Transition to Advanced Transmitter Technology

There is constant improvement in sensor technology for nuclear power plants as a result of ongoing discoveries by research organizations, new products by instrument suppliers, and new requirements arising out of nuclear operating experience. One particular driver is the need for increased sensor performance characteristics to support advanced reactor designs. This would include qualification for higher temperature and tolerance of chemically harsh and corrosive environments. Operating experience is another such driver. For example, the Fukushima-Diiachi accident in Japan will likely drive the development of instruments that can operate in severe accident environments.

This continuous improvement in sensor technology will inevitably result in improved product offerings for the existing sensor applications in the operating fleet and the new nuclear plants currently under licensing and construction. This will favorably impact the major benefits of improved sensors in the areas of accuracy, reliability, availability, and maintainability as described in this report. Some of these developments will make favorable impacts for both analog and digital sensors alike, in that they improve the conversion of the process parameter to a representative signal. Others are more suited to digital application.

Table 5 depicts a survey of certain sensor types that comprise the majority of nuclear plant sensor applications. It presents pressure transmitters, level transmitters, flow transmitters, temperature transmitters, and neutron flux monitors that are described in this section in three categories:

- Analog Sensor – existing analog sensor technology in nuclear plant, qualified in accordance with 10 CFR 50 Appendix B and associated environmental and seismic qualification references (including harsh environment)
- Latest Digital Sensor – existing digital sensor technology in nuclear plants qualified in accordance with 10 CFR 50 Appendix B and associated environmental and seismic qualification references (not harsh environment)
- Emerging Technology – new sensor technology in the R&D stage or in applications outside of the nuclear industry that have potential benefit in accuracy, reliability, availability and maintainability if deployed in nuclear plants.

6.1 Pressure Transmitters

6.1.1 Analog Pressure Technology

Analog electronic pressure transmitters are widely used in various safety and non-safety applications in nuclear power plants. The transmitters are used in both gage and absolute pressure modes with gage pressure applications predominating. These electronic pressure sensors generally use a diaphragm, piston, bourdon tube, or bellows to measure strain or deflection due to applied pressure. The effect of the pressure is converted to a current, typically 4 to 20 milliamps, and transmitted to the control room or

Table 5 Transition to Advanced Transmitter Technology

Sensor Type	Analog Sensor	Latest Digital Sensor	Emerging Technology
Pressure	• Electromagnetic • Capacitance (Strain gauge) •	• Digital capacitance)	• Optical • Potentiometric • Resonant Devices
Flow	• Mechanical • Pressure • Thermal	• Mechanical Capacitance • Ultrasonic	• Vortex • Electromagnetic • Optical • Coriolis
Level	• Capacitance – D/P • Bubblers • Displacers	• Digital Capacitance • Ultrasonic • Radar	• Nuclear • RF/Admittance/Capacitance
Temperature	• RTD's • Thermoucouples (T/Cs)	• Digital Temperature Transmitters(in conjunction with RTD or T/C	• Ohio State Research Task – Fiber Optic • Johnson Noise Thermometry
Flux	• Proportional Counter • Compensating Ion Chamber • Uncompensated Ion Chamber	• Not found	• Silicon Carbide Based Flux Monitors • Solid-State Neutron Flux Monitor • Fuel Mimic Power Monitor • Scintillation-Based Measurements • Gamma-Thermometer for incore measurements

other environmentally controlled area. A pressure instrument loop typically consists of a power supply, transmitter, current-to-voltage converters, output devices and interconnecting cabling. There is a wide variety of technologies employed to provide commercially available electronic pressure transmitters. The principal technologies employed in nuclear plants are based on force balance, capacitive, and strain gage principles.

Electromagnetic pressure measurement

Pressure is applied to a bourdon tube or force bar which results in deflection. As the bourdon tube moves out of position due to this applied force, a highly sensitive electromagnetic sensor detects it and causes an electronic amplifier to send a different amount of electric current to a force coil. The force coil presses against the bourdon tube which pivots to counteract the initial motion of the force bar. When the system returns to equilibrium, the milliampere current through the force coil will be a direct, linear representation of the process fluid pressure applied to the diaphragm capsule.

Capacitive pressure measurement

The principle of capacitive pressure measurement is based on the measurement of the capacitance of a capacitor, which is dependent upon the plate separation. The principle of capacitive pressure measurement is realized using a main body with a metallic diaphragm, or one coated with a conductive material, which forms one of the two plates of a dual-plate capacitor. If the diaphragm is deflected under pressure, the plate separation of the capacitor decreases, which results in an increase in its capacitance. An example of an industry-typical digital pressure instrument using capacitive pressure measurement is analyzed in the instrument uncertainty calculation in Appendix C.

Strain gauge pressure measurement

The sensor uses a wire that is welded to a Bourdon tube and cantilever beam. Increased internal pressure applied to the Bourdon tube tends to straighten the tube, which in turn bends the cantilever beam proportionally. Motion of the free end of the beam applies tension to one gage, increasing its resistance, and compression to the other, decreasing its resistance. The two gauges are connected to form two active arms of a bridge circuit. The bridge output signal is conditioned and converted to a 4-20 mA or 10-50 mA output signal by the transmitter electronics.

6.1.2 Digital Pressure Technology

Capacitance Pressure Measurement

A variation of the analog capacitance pressure measurement addressed in the above section is the digital version exemplified by the industry-typical digital pressure sensor, analyzed in the instrument uncertainty calculation in Appendix C. This provides a high degree of accuracy as well as incorporates the improvements in online monitoring diagnostics that are available with a digital transmitter to reduce the percentage of failures that are dangerous and undetected, as addressed in Section 4.2 of this report.

6.1.3 Emerging Pressure Technology

Optical pressure measurement

Techniques include the use of the physical change of an optical fiber to detect strain due to applied pressure. This technology is employed in challenging applications where the measurement may be highly remote, under high temperature, or may benefit from technologies inherently immune to electromagnetic interference.

Potentiometric

This technology uses the motion of a wiper across a resistive media to detect the force cause by the applied pressure.

Resonant Devices

These devices use changes in resonant frequency in a sensing mechanism to measure stress, or changes in gas density, caused by applied pressure. This technology may be used in conjunction with a force collector, such as those in the electromagnetic pressure measurement category above. Alternatively, resonant technology may be employed by exposing the resonating element itself to the media, whereby the resonant frequency is dependent upon the density of the media. Sensors have been made out of vibrating wire, vibrating cylinders, quartz, and silicon microelectromechanical systems (MEMS). Generally, this technology is considered to provide very stable readings over time.

6.2 Flow Measurement

There are a number of different types of instruments for measuring flow that can be grouped into broad categories, mechanical, pressure, thermal, and electronic. Examples of each type are as follows in the categories of analog, digital, and emerging technologies.

6.2.1 Analog Flow Technology

Mechanical

Mechanical flow meters are flow meters that depend on mechanical means to measure volume either by a rotating part or displacement. Examples of mechanical flow meters in use at nuclear units are turbine flow meters and rotometers.

Pressure

Pressure-based flow meters depend on an obstruction in the flow path such as an orifice plate that develops a pressure drop as a result of the flow. As described by Bernoulli's equation, flow is proportional to the square root of the differential pressure so a signal proportional to the flow rate can be displayed. Examples of mechanical flow meters in use at nuclear units are Venturi or an orifice plate with a differential pressure transmitter. An example of this is the Rosemount Model 1153 analog transmitter (capacitance technology) configured as a differential pressure transmitter. [41]

Thermal

Since the heat transfer coefficient is affected by flow, flow can be measured using thermal devices. These devices typically have a heater and temperature measuring device to develop a signal proportional to flow. Thermal mass flow meters are most commonly used to measure gas flow.

6.2.2 Digital Flow Technology

Capacitance

The digital capacitance technology has been incorporated in the Rosemount 3051. [42] This technology offers the higher level of accuracy and also online monitoring diagnostics that can benefit in overall system reliability. It has been qualified for mild environments in accordance with 10 CFR 50 Appendix B.

Ultrasonic

The ultrasonic measurements have been incorporated in nuclear plants in systems such as feedwater flow measurements to provide a more accurate measurement used in the secondary calorimetric calculation and adjustment of neutron monitors. This has provided a very important benefit in allowing the increase in reactor power, concurrent with the increased accuracy of the flow measurement. Ultrasonic flow transmitters are typically digital and are mounted externally to the pipe so no pressure drop device such as an orifice plate is required.

6.2 3. Emerging Flow Technology

Electronic

A number of different types of flow meters use electronic means to measure flow. Examples of these types of flow meters are vortex, electromagnetic, optical, and Coriolis flow meters. All of these methods depend on detecting a physical characteristic that varies with flow rate electronically. A number are in use in commercial industries due to requirements in accuracy and cost performance.

6.3 Level Measurement

As with flow measurement, a number of different technologies are available to measure level. Almost all of the level measurements in nuclear power plants are for measuring water level or a liquid similar to water. Some level measurement applications are for pressurized vessels while others are at atmospheric pressure.

6.3.1 Analog Level Technology

Differential Pressure (D/P)

This device does not really measure level. It measures the head pressure that the diaphragm senses due to the height of the material in the vessel multiplied by a second variable, the density of the product. This gives you the resultant force being exerted on the diaphragm, which is then translated into a measurement of level. A primary benefit of a D/P transmitter is that it can be readily installed on a vessel. It can also be easily isolated using block valves. D/P transmitters are subject to errors due to density

variations of the liquid and pressure drops when flow is present in the vessel. One instrument supplier offers a level monitoring system consisting of two pressure transmitters linked together electronically eliminating the traditional reference leg. One of the sensors calculates the differential pressure and transmits the value digitally. This arrangement eliminates issues related to reference legs such as temperature effect on the reference leg, maintaining the reference leg completely full or completely dry, flashing in the reference leg, and leaks.

Bubblers

This simple level measurement has a dip tube installed with the open end close to the bottom of the process vessel. A flow of gas (usually air) passes through the tube and when air bubbles escape from the open end, the air pressure in the tube corresponds to the hydraulic head of the liquid in the vessel. The air pressure in the bubble pipe varies proportionally with the change in head pressure. The system consists of a pipe, an air supply, a pressure transmitter and a differential pressure regulator. The regulator produces the constant gas flow required to prevent calibration changes. Accuracy depends on a stable air supply and is limited by the regulator.

Displacers

When a body is immersed in a fluid, it loses weight equal to the liquid weight displaced (Archimedes Principle). By detection of the apparent weight of the immersed displacer, a level instrument can be devised. If the cross sectional area of the displacer and the density of the liquid is constant, then a unit change in level will result in a reproducible unit change in displacer weight. Displacers are affected by changes in density. Since the displacement of the body (its weight loss) is equal to the weight of the fluid displaced However, changes to the specific gravity changes affect the weight of the displaced material, thus changing the calibration.

6.3.2 Digital Level Technology

Capacitance

The digital capacitance technology has been incorporated in the industry-typical digital pressure sensor, addressed in the instrument uncertainty calculation in Appendix C. This technology offers the higher level of accuracy and also online monitoring diagnostics that can benefit in overall system reliability. It has been qualified for mild environments in accordance with 10 CFR 50 Appendix B.

Ultrasonic/Sonic

Ultrasonic transmitters work on the principle of sending a sound wave from a peizoelectric transducer to the contents of a vessel. The device measures the length of time it takes for the reflected sound wave to return to the transducer. A successful measurement depends on reflection from the process material in a straight line back to the transducer. There are various influences that affect the return signal, such as dust, heavy vapors, surface turbulence, foam and even ambient noise. Temperature can also be a limiting factor in many process applications.

Radar

The sensor emits a microwave pulse towards the process material. This pulse is reflected by the surface of the material and is detected by the same sensor which now acts as a receiver. Level is inferred from the time of flight (transmission to reception) of the microwave signal. Microwave “echoes“ are evaluated by sampling echoes and building up a retained profile of the echoes. This non-contact technology produces highly accurate measurements in storage tanks and some process vessels. The pressure ratings on the radar antenna are limited. Some applications for nuclear plant fuel pool level measurement are now being offered.

6.3.3 Emerging Level Technology

Nuclear

Nuclear level controls are used for continuous measurements, typically where most other technologies are unsuccessful. Radioisotopes used for level measurement emit energy at a fairly constant rate and in a random fashion. Gamma radiation, which is present in high-energy short-wave lengths produce a great penetrating power and are used for level measurement. Different radioactive isotopes are used, based on the penetrating power needed to “see” through the process vessel. The radiation from the source penetrates through the vessel wall and process fluid. A detector on the other side of the vessel measures the radiation field strength and infers the level in the vessel. The percentage of transmission decreases as the level increases. Licenses, approvals, and periodic inspections are required. Radiation sources are expensive and disposal is difficult. There are some other considerations regarding the accuracy, linearity, and rate of response, which are generally not as good as other technologies.

RF Admittance/Capacitance

A constant voltage is applied to a rod or cable (sensing element) in the process. The resulting radio frequency current is monitored to infer the level of the process material. The theory of operation for an RF Admittance level transmitter is similar to that of capacitance transmitters, but with two important circuit additions. The oscillator buffer and chopper drive circuits permit separate measurement of resistance and capacitance. Since the resistance and capacitance of any coating are of equal magnitude (by physical laws), the error generated by a coating can be measured and subtracted from the total output. RF Admittance/Capacitance of are by far the most versatile technologies for continuous level measurement and handles a wide range of process conditions anywhere from cryogenics to 1000 degrees F and from vacuum to 10,000 psi pressure. Aside from the electronic circuit technology, sensing element design is very important to handle these process conditions. There are no moving parts to wear, plug, or jam. There is only a single tank penetration, usually at the top of the tank, above the actual process level. Smart transmitters are available that need no calibration, since they constantly re-calibrate themselves, based on the dielectric constant monitoring.

6.4 Temperature

6.4.1 Analog Temperature Technology

In nuclear plants, there are a variety of temperature sensors used in I&C systems. The most common ones are thermocouples and resistance temperature detectors (RTD's). These devices convert temperature into very small variable electrical voltages (thermocouples) or varying electrical resistance (RTD's). These sensors are generally field mounted devices that may be placed directly in contact with the item to be measured or in thermowells that protrude into a fluid system.

An example of a current day analog temperature transmitter used in many nuclear plants in the U.S. is the Weed Instrument Model N7000 Temperature Transmitter [43], which is fully qualified to all U.S. nuclear requirements and provides an accuracy of ± 0.1% of calibrated span.

6.4.2 Digital Temperature Technology

One of the great advantages of a digital solution, as represented by the Caldon LEFM 2010 RCT Reactor Coolant Temperature Meter [44], is the ability to measure the bulk average temperature to a much higher accuracy with multiple inputs, which adjusts for stratification and variations in flow. This can greatly reduce the total uncertainty for the measurement and increase the plant operating margin. Additionally, monitoring and diagnostic capabilities are added as preventive diagnostic indicators. Any detected error will generate a message on a display, providing a higher degree of reliability of operation and reducing the probability of failure on demand.

6.4.3 Emerging Temperature Technology

During the last several years, newer type sensors are being considered for temperature measurement including the following.

Fiber Optic Temperature Sensor

Fiber optic sensors are being investigated to determine the prospects for potential applications for nuclear power plant measurements. Fiber optic sensors have a high degree of immunity to electromagnetic and radio frequency interference (EMI/RFI), so they can be used in strong EMI/RFI environments. Other potential advantages are higher sensitivity, smaller size, less weight, larger bandwidth, and ease of multiplexing. Therefore, if they can be demonstrated to have sufficient environmental compatibility, they can be a promising new sensor type for measuring temperature in nuclear power plants. Ohio State University has performed R&D on this sensor type and documented the benefits of moving to commercially available product lines. [45]

Johnson Noise Thermometry

Johnson Noise Thermometry is being considered by U.S. and Korean research teams for primary flow-loop temperature measurement because the values derived are

inherently drift free. Also, Johnson noise is insensitive to the material condition of the sensor and, consequently is immune to the contamination and thermo-mechanical response shifts that plague thermocouples and RTD's. This is being considered for commercialization for increased accuracy in primary-loop temperature measurement with the added benefit of reduced calibration requirements.

Transition to Digital Technology for Temperature Measurement

The use of a higher level of computerization in temperature measurement provides the possibility for inclusion of new functionality, such as data validation, new algorithms, process performance evaluation (heat exchanger performance), diagnostics and prognostics, and a much higher assignment of failure detection due to online monitoring. Algorithms such as subcooled margin, which requires both temperature and pressure, and conversion through interpolation in the steam tables, can be developed in software to meet the plant requirements for indication and operator interface. Additional cross channel calibration and online monitoring can support calibration and functional test interval extensions through analysis in accordance with programs such as NEI 04-10 [37], which has been NRC approved. Long term trending can now be handled automatically, for both evaluation of sensor degradation as well as contributing to the monitoring of critical parameters that impact on efficiency of operation.

6.5 Neutron Flux Monitors

Digital application in conjunction with some of the emerging flux technologies listed above can provide higher accuracy and at the same time, improved reliability, availability and maintainability for the sensor string and safety function performed. The migration to digital technology has been slow in this area due to the acceptance of existing analog licensing background and robust design for the current offerings, particularly in consideration of the daily calibrations that occur on neutron flux channels, as adjusted from the secondary calorimetric values. For these cases, early detection of degradation provides a high degree of reliability in the existing designs.

A number of different technologies are applied to neutron flux measurement. The Nuclear Power Reactor Instrumentation Systems Handbook [46], published in 1973 by the U.S. Atomic Energy Commission, still provides a good overview of the sensing systems employed in early and current nuclear power plants. Usually, three ranges in nuclear instrumentation are used to monitor and control and power level of a reactor through the full range of reactor operation.

Source Range

The source range makes use of a proportional counter. Source range instrumentation usual consists of a high-sensitivity proportional counter and associated signal measuring equipment. These channels are typically used over a counting range of 0.1 to 10^6

counts per second, but vary based on reactor design. Their outputs are displayed in terms of the logarithmic of count rate.

Intermediate Range

The intermediate range makes use of a compensated ion chamber in most cases. Intermediate range nuclear instrumentation consists of a minimum of two redundant channels. Each of these channels is made up of a boron-lined or boron gas-filled compensated ion chamber and associated signal measurement equipment of which the output is a steady current produced by the neutron flux.

Power Range Nuclear Instrumentation

The power range makes use of an uncompensated ion chamber. Power range nuclear instrumentation normally consists of four identical linear power level channels which originate in eight uncompensated ion chambers. The output is a steady current produced by the neutron flux. Uncompensated ion chambers are utilized in the power range because gamma compensation is unnecessary; the neutron-to-gamma flux ratio is high. The output of each power range channel is directly proportional to reactor power and typically covers the range from 0% to 125% of full power but varies with each reactor.

6.5.1 Analog Flux Technology

The legacy and current technologies applied to these detectors is included in the following:

Proportional Counter Circuitry

Proportional counters measure the charge produced by each particle of radiation. To make full use of the counter's capabilities, it is necessary to measure the number of pulses and the charge of each pulse. A single detector includes a capacitor and preamplifier. The capacitor converts the charge pulse to a voltage pulse. The preamplifier amplifies the voltage pulse.

Compensating Ion Chamber

Ionization chambers are electrical devices that detect radiation when the voltage is adjusted so that the conditions correspond to the ionization region. The charge obtained is the result of collecting the ions produced by radiation. Compensating for the response to gamma rays extends the useful range of the ionization chamber. Compensated ionization chambers consist of two separate chambers; one chamber is coated with boron, while the uncoated chamber is sensitive only to gamma rays. Instead of having two separate ammeters and subtracting the currents, the subtraction of these currents is done electrically, and the net output of both detectors is read on a single ammeter.

Uncompensated Ion Chamber

For reactors operating near peak power, neutrons are the dominant radiation, and almost all of the current is due to neutrons. These chambers are used at high reactor power levels and are referred to as uncompensated ion chambers. The uncompensated

ion chamber is not suitable for use at intermediate or low power levels because the gamma response at these power levels can be significant compared to the neutron response.

6.5.2 Emerging Flux Technologies

Newer technologies are now being considered for neutron monitoring including the following:

Silicon Carbide Flux Monitor

Silicon carbide neutron flux monitors offer the potential to combine the functions of current three-range flux monitoring into a single system and further offer the potential to eliminate the added complexity of a separate gamma compensation system. Silicon-carbide-based flux monitors depend upon the production of a few-micron-thick, charge-depleted silicon carbon layer on top of a silicon carbide substrate – generally a Schottky barrier type device. A layer of LiF is deposited across the top of the device to convert incident neutrons into charged particles. The chief advantages of this emerging sensor technology is that silicon carbide shows considerable radiation hardness. It also offers high temperature tolerance while permitting high speed operation. Disadvantages may include application primarily as a point source in a local area versus a wide range monitoring capability.

Solid-State Neutron Flux Monitor

A solid-state flux monitor is has been evaluated as part of the International Nuclear Energy Research Initiative (INERI) project jointly sponsored by U.S. Department of Energy and the Korean Ministry of Science and Technology. [47] [48] This flux monitor is based on the flux-induced change in electrical resistance of a Group III nitride solid. Because the detector is a solid, no gas seals are required as for conventional technologies. The detector is also expected to be mechanically robust, highly temperature tolerance, and inexpensive.

Fuel Mimic Power Monitor

The fuel mimic power monitor has been developed and demonstrated through the U.S. Department of Energy Nuclear Engineering Education Research (NEER) program and EPRI funding. [47] [48] The instrument represents a unique sensing technology in that it provides a direct measurement of the nuclear energy deposited into a fuel mimic mass. The fuel mimic power monitor is based on the addition of heat through resistive dissipation of input electrical energy to a small mass of reactor fuel or fuel analogue. The main advantage of this type of sensor is that it provides a close analog to the actual physical process of interest (cladding temperature). The major concerns about the technology relate to its sensitivity to its heat transfer environment. The device also relies on accurate temperature measurement.

Scintillation-Based Measurements

This emerging technology is directed at obtaining a more accurate, reliable, cost-effective determination of in-core power density to facilitate higher fuel burn-up, more efficient core loadings, and uniform power distributions. Scintillation-based measurements have been targeted at the higher core temperature reactor designs(such as the modular helium reactor). The primary deficiency in this technology preventing its use for in-core measurements has been the lack of an effective technique for measuring light within reactor core environments and the rapid darkening of fiber optic light pipes in high radiation fields.

Gamma Thermometer for Incore Measurement

Current Generation I and II Boiling Water Reactors utilize a Traversing In-Core Probe (TIP) for calibration of the Local Power Range Monitor (LPRM). The LPRM is a miniature fission chamber in-core neutron detector composed of U235 and U234 (used to breed more U235). After exposure to significant exposure to neutron flux (8-10 full power years), the amount of fissionable U235 left in the detector decreases which reduce the sensitivity of the LPRM detectors. The LPRM system is calibrated periodically (currently with the TIP) to adjust the gain to compensate for this phenomenon. In general a LPRM detector exhausts the usable U235 to the point where the detector has to be replaced, usually 8 to 10 years of use at full power (directly proportional to detector sensitivity) is not sufficient for reactor protection system. LPRM sensitivities drop over time. The TIP system is a mechanically complex component of the neutron monitoring system (NMS), requiring high maintenance. This complexity, coupled with the reactor containment penetration required for withdrawal of detectors, provides a need for an improved system for LPRM calibration.

In Generation III reactors, the TIP system may potentially be replaced by a Gamma Thermometer (GT). [49] The GT is a fixed in-core detector that will significantly reduce the operating and maintenance costs associated with the neutron monitoring system. Additionally, dose to personnel is reduced because the irradiated tip TIP detectors are replaced by GTs. This can eliminate the “pig” (shielded unit for detector storage) that the TIPS are stored in outside containment. The shear valve (a breach in the containment wall) is also eliminated by use of the GT system. Using this method, surveillance testing of the shear valve is eliminated or reduced. This system design is being licensed with the GE-Hitachi ESBWR design certification.

The GT sensor provides a signal that is proportional to gamma flux. This gamma flux can be used to calculated reactor power, at steady conditions, and thus provides a means of reference for the calibration of LPRMs.

7. Summary

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.

The currently-operating nuclear power plants are faced with aging and reliability issues in their current instrumentation and control systems. Replacing the current analog sensors with digital counterparts provides the double benefit of resolving the operational problems while also improving safety margins and lowering maintenance costs.

For new nuclear facilities, including small modular reactors SMRs, there is an opportunity to design these plants in a way that ensures higher instrument performance and lower operating costs over the life of the plant. The advantage of doing this in the initial design, as opposed to a back-fit by plant modifications, is that projected operational and maintenance support requirements will be lower throughout the life cycle of the plant and thereby contribute positively to the economics case for the plant.

This project outlines the benefits of digital sensors in four 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.

Availability – similar to reliability, the digital sensors will perform on demand for a higher percentage of time. This means that there would be less operator workarounds to compensate for sensors out of service.

Maintainability – there is less maintenance support and cost required due to the longer service intervals between planned maintenance, lower failure rates, and the assistance of on-board diagnostics to reduce troubleshooting efforts when there are failures.

There are certain qualification and licensing considerations that must be addressed in the implementation of digital sensors, particularly in regard to safety-related applications. One significant barrier to the implementation of digital instrumentation is software common cause failure under licensing requirements. This must be addressed by demonstrating that there is adequate diversity and defense-in-depth in the design to accomplish the plant safety functions when SCCF is assumed for all like digital devices.

There are currently no objective criteria for how much diversity is sufficient to preclude a SCCF. This is being addressed in a related project by the Oak Ridge National Laboratory.

There are some environmental qualification issues with digital instrumentation that must also be addressed. These include electromagnetic compatibility, radiation, and temperature. Some digital instruments cannot match the environmental qualification of their analog counterparts. The resolution of this problem is somewhat hampered by the lack of market for the digital instruments, providing low incentive to suppliers to improve the environmental qualifications of their digital offerings.

Therefore, further work is needed in several 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 Digital Technology Qualification project at Oak Ridge National Laboratory is an important step in providing objective criteria for how much diversity is enough. There might be an opportunity to collaborate with new nuclear plant designers, especially of a SMR design, to see how the use of digital sensors can be accommodated in the addressing SCCF for all levels of digital control and protection systems.

- 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. This project has provided representative examples of performance improvement by digital instruments. The multiplied effect of these performance improvements across the many plant systems would result in considerable cost savings and would likely support a business case for a transition to digital sensors.

- 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. This is primarily an issue of electronic components embedded in the digital sensors. Other industry sectors have had success in hardening electronics, notably military and space applications. It is recognized that a market for these improved digital instruments must develop for this to be attractive to the suppliers.

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. Further work can address these barriers and thereby enable the nuclear power industry to obtain these benefits by incorporating digital sensors whenever opportunities are presented.

8.0 References

1. Quinn, E., Mauch, J., & Thomas, K., (2012) Digital Technology Qualification Task 2 – Suitability of Digital Alternatives to Analog Sensors and Actuators, INL/EXT-12-27215, Idaho Falls, ID: Idaho National Laboratory
2. Wood, R., Pullam, L., Smith, C., Holcomb, D., Korsah, K., Muhlheim, M., Common Cause Failure Mitigation Practices and Knowledge Gaps, NEET/ASI/ORNL/TR-2012/01, Oak Ridge, TN: Oak Ridge National Laboratory
3. Thomas, K. and Hallbert,B., (2013), Long-Term Instrumentation, Information, and Control Systems (II&C) Modernization Future Vision and Strategy Revision 2, INL/EXT-11-24145, Idaho Falls, ID: Idaho National Laboratory
4. Institute of Electrical and Electronics Engineers, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," IEEE Std. 379-2000, Piscataway, New Jersey, 2000
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. U.S. Nuclear Regulatory Commission, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," Branch Technical Position 7-19, Washington, D.C., 2007
7. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.105 Revision 3, Setpoints for Safety-Related Instrumentation, Washington, DC, December, 1999
8. American National Standard ANSI/ISA S 67.04 Part 1-1994, Setpoints for Nuclear Safety-Related Instrumentation, 1994
9. 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
10. 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
11. Institute of Nuclear Power Operations (INPO), AP-913 Revision 2, Equipment Reliability Process Description, Atlanta, Georgia, December 2007
12. U.S. Department of Defense, MIL-HDBK-217F, Reliability Prediction of Electronic Equipment, Washington, DC, January 1990
13. ANSI S84.01-1996 "Application of Safety Instrumented Systems for the Process Industries"
14. Institute of Electrical and Electronics Engineers, IEEE 577-2004, IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities, Piscataway, New Jersey, 2004
15. International Electrotechnical Commission, IEC 61508 - 2009, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, Parts 1 through 6.

16. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.47 Revision 1, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems, Washington, DC, February, 2010

17. 10 CFR Part 50, Domestic Licensing of Production and Utilization Facilities, U.S. Nuclear Regulatory Commission, Washington DC

18. U.S. Nuclear Regulatory Commission, Standard Review Plan, NUREG-0800, Chapter 7, Branch Technical Position (BTP) – 14 Revision 5, Guidance for Software Reviews for Digital Computer-Based Instrument and Control Systems, Washington, DC, March, 2007

19. Institute of Electrical and Electronics Engineers, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," IEEE Std. 323-2003, Piscataway, New Jersey, 2003

20. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants, Washington, DC, March 2007

21. Institute of Electrical and Electronics Engineers, "Seismic Qualification Electric and Mechanical Equipment for Nuclear Power Generating Stations," IEEE Std. 344-2003, Piscataway, New Jersey, 2003

22. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.100, Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment of Nuclear power Plants, Washington, DC, May 2008

23. U.S. Department of Defense, MIL-STD-461E, Requirements for the Control of Electromagnetic Interference Characteristics for Subsystems and Equipment IEC 61000 Part 4, Washington, DC, August 1999

24. International Electrotechnical Commission, IEC 61000 - 2009, Electromagnetic Compatibility, Part 4

25. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, Washington, DC, October 2003

26. 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

27. U. S. Nuclear Regulatory Commission, NUREG/CR 6303, Method for Performing Diversity and Defense-In-Depth Analyses of Reactor Protection Systems, Washington, DC, December 1994

28. U. S. Nuclear Regulatory Commission, Interim Staff Guidance, DI&C-ISG-04, Highly-Integrated Control Rooms - Communications Issues, Washington, DC, September 2007

29. 10 CFR Part 73, Physical Protection of Plants and Materials, U.S. Nuclear Regulatory Commission, Washington DC

30. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.152 Revision 3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, Washington, DC, July 2011

31. U. S. Nuclear Regulatory Commission, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, Washington, DC, January 2010

32. Nuclear Energy Institute (NEI), NEI 08-09 Revision 6, Cyber Security Plan for Nuclear Power Reactors, Washington, DC, April, 2010

33. Nuclear Energy Institute (NEI), NEI 01-01, A Revision of EPRI TR 102348 to Reflect Changes to the 10 CFR 50.59 Rule, Washington, DC, March 2002

34. Electric Power Research Institute (EPRI), TR 102348 Revision 1, Guideline on Licensing Digital Upgrades, Washington, DC, March 2002

35. U. S. Nuclear Regulatory Commission, Regulatory Issue Summary 2002-22, Use of NEI/EPRI Joint Task Force Report, "Guideline on Licensing Digital Upgrades: EPRI TR 102348, Revision 1, NEI 01-01: A Revision of EPRI TR 102348 to Reflect Changes to the 10 CFR 50.59 Rule", Washington, DC, November 2002

36. U. S. Nuclear Regulatory Commission, Interim Staff Guidance, DI&C-ISG-06, Licensing Process, Washington, DC, January 2011

37. Nuclear Energy Institute (NEI), NEI 04-10 Rev. 1, Risk-Informed Technical Specification Initiative 5b, Risk-Informed Method for Control of Surveillance Frequencies, Industry Guidance Document, Washington, DC, April, 2007

38. U.S. Nuclear Regulatory Commission Safety Evaluation Report on NEI 04-10, Rev 1, dated Sept 19, 2007

39. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.175, An Approach for Plant-Specific Risk-Informed Decision-making: Inservice Testing, Washington, DC, August 1998

40. 10 CFR Part 52, Licenses, Certifications, and Approvals for Nuclear Power Plants, U.S. Nuclear Regulatory Commission, Washington DC

41. Rosemount 1153 Series D Alphaline Nuclear Pressure Transmitter Product Data Sheet 00813-0100-4388 Revision BA, January 2008

42. Rosemount 3051S Series of Instrumentation Product Data Sheet 00813-0100-4081 Revision RA, January 2013

43. Weed Instrument N7000 Series RTD and Thermocouple Temperature Transmitter

44. Caldon LEFM 2010 RCT Reactor Coolant Temperature Measurement, Datasheet ML-279 Rev. 1

45. Email from Chris Petrie of Ohio State University (OSU) to Ted Quinn, 5/15/2013, entitled, Request for Information for INL NEET Program Task – OSU Input

46. U.S. Atomic Energy Commission (AEC), Nuclear Power Reactor Instrumentation Systems Handbook, 1973 (VOL I and II)

47. U.S. Nuclear Regulatory Commission, NUREG/CR-6812, Emerging Technologies in Instrumentation and Control, Washington, DC, March 2003

48. U.S. Nuclear Regulatory Commission, NUREG/CR-6888, Emerging Technologies in Instrumentation and Control: An Update, Washington, DC, January 2006

49. IEC Draft Standard 62584, Nuclear Power Plants – Instrumentation Important to Safety – Application of Gamma Thermometer (GT) for Local Power Range Monitor (LPRM) Calibration

Appendix A: Nuclear Plant Transmitter Types

Typical Nuclear Plant Significant Instrumentation Table B6-1		
Parameter	System	Sensor Type
Turbine Vibration	Turbine	Accelerometer
Pressurizer Safety Valve Position	PWR	Acoustic pickup
Main Generator Current	Main Generator	Current meter
Main Generator Field Current	Main Generator	Current meter
Differential Protection Relays	Electrical	Current relay
Overcurrent Protection Relays	Electrical	Current relay
Accumulator Tank Level	PWR	Differential pressure transmitter
Auxiliary Feedwater Flow	PWR/BWR	Differential pressure transmitter
Charging Flow	PWR	Differential pressure transmitter
Component Cooling Water Flow	PWR/BWR	Differential pressure transmitter
Condensate Storage Tank Level	PWR/BWR	Differential pressure transmitter
Containment Spray Flow	PWR/BWR	Differential pressure transmitter
Core Spray System Flow	BWR	Differential pressure transmitter
Drywell Spray Flow	BWR	Differential pressure transmitter
Drywell Sump Level	BWR	Differential pressure transmitter
Feedwater Heater Level	Secondary	Differential pressure transmitter
Heater Drain Tank Level	Secondary	Differential pressure transmitter
High Level Radioactive Liquid Tank Level	PWR/BWR	Differential pressure transmitter
HPCI Flow	BWR	Differential pressure transmitter
HPSI Flow	PWR	Differential pressure transmitter
Isolation Condenser System Shell Side Water Level	BWR	Differential pressure transmitter
Letdown Flow	PWR	Differential pressure transmitter
LPCI System Flow	BWR	Differential pressure transmitter
LPSI Flow	PWR	Differential pressure transmitter
Main Feedwater Flow	PWR/BWR	Differential pressure transmitter
Main Steam Flow	PWR/BWR	Differential pressure transmitter

Moisture Separator Drain Tank Level	Secondary	Differential pressure transmitter
Pressurizer Level	PWR	Differential pressure transmitter
Quench Tank Level	PWR	Differential pressure transmitter
RCIC Flow	BWR	Differential pressure transmitter
RCS Flow	PWR	Differential pressure transmitter
Reactor Vessel Level	PWR/BWR	Differential pressure transmitter
RHR/SDC System Flow	PWR	Differential pressure transmitter
RWST Level	PWR/BWR	Differential pressure transmitter
SLCS Flow	BWR	Differential pressure transmitter
SLCS Storage Tank Level	BWR	Differential pressure transmitter
Steam Generator Level	PWR	Differential pressure transmitter
Steam Generator Level	PWR	Differential pressure transmitter
Suppression Chamber Spray Flow	BWR	Differential pressure transmitter
Suppression Pool Water Level	BWR	Differential pressure transmitter
Volume Control Tank Level	PWR	Differential pressure transmitter
Neutron Flux	PWR	Fission chamber
Neutron Flux	PWR	Fission chamber
Drywell Drain Sumps Level	BWR	Float switch
Containment and Drywell Hydrogen Concentration	BWR	Hydrogen cell
Containment Hydrogen Concentration	PWR/BWR	Hydrogen cell
Boron Concentration	PWR/BWR	Ion chamber
Accumulator Isolation Valve Position	PWR	Limit switch
Containment Isolation Valve Position	PWR/BWR	Limit switch
Emergency Ventilation Damper Position	PWR/BWR	Limit switch
Isolation Condenser System Valve Position	BWR	Limit switch
Containment and Drywell Oxygen Concentration	BWR	Oxygen cell
Diesel Load	Diesel	Power meter
Accumulator Tank Pressure	PWR	Pressure transmitter
Condenser Vacuum	Secondary	Pressure transmitter
Containment Pressure	PWR/BWR	Pressure transmitter
Diesel Lube Oil Pressure	Diesel	Pressure transmitter

Drywell Pressure	BWR	Pressure transmitter
Drywell Pressure	BWR	Pressure transmitter
Main Steam Isolation Valve Leakage Control System Pressure	BWR	Pressure transmitter
Pressurizer Pressure	PWR	Pressure transmitter
Quench Tank Pressure	PWR	Pressure transmitter
Radioactive Gas Holdup Tank Pressure	PWR/BWR	Pressure transmitter
Steam Generator Pressure	PWR	Pressure transmitter
Turbine First Stage Pressure	Turbine	Pressure transmitter
Turbine Lube Oil Pressure	Turbine	Pressure transmitter
Diesel Speed	Diesel	Proximity probe
RCS Flow	PWR	Proximity probe
Turbine Speed	Turbine	Proximity probe
Condenser Air Removal Effluent Radioactivity	PWR/BWR	Radiation detector
Containment Effluent Radioactivity	PWR/BWR	Radiation detector
Containment Radiation	PWR/BWR	Radiation detector
RCS Coolant Radioactivity	PWR/BWR	Radiation detector
Containment Sump Level	PWR/BWR	Reed switch
Control Rod Position	PWR/BWR	Reed switch
Feedwater Heater Level	Secondary	Reed switch
Power Supply Status	PWR/BWR	Relay
Pressurizer heater status	PWR	Relay
RCP Status	PWR	Relay
Component Cooling Water Supply Temperature	PWR/BWR	Resistance temperature detector
Containment Cooling Heat Removal	PWR/BWR	Resistance temperature detector
Containment Sump Water Temperature	PWR/BWR	Resistance temperature detector
Feedwater Temperature	Secondary	Resistance temperature detector
Pressurizer Temperature	PWR	Resistance temperature detector
Quench Tank Temperature	PWR	Resistance temperature detector
RCS Temperature	PWR/BWR	Resistance temperature detector
RCS Temperature	PWR/BWR	Resistance temperature detector
RHR/SDC Heat Exchanger Outlet Temperature	PWR	Resistance temperature detector
Suppression Pool Water Temperature	BWR	Resistance temperature detector
Incore Neutron Flux	PWR/BWR	Self-powered neutron detectors
Containment Atmosphere Temperature	PWR/BWR	Thermocouple
Core Exit Temperature	PWR/BWR	Thermocouple

Drywell Atmosphere Temperature	BWR	Thermocouple
Main Generator Stator Temperature	Main Generator	Thermocouple
Reactor Vessel Level	PWR/BWR	Thermocouple
RCP Undervoltage Relays	Electrical	Undervoltage relay
Safety Bus Undervoltage Relays	Electrical	Undervoltage relay
Diesel Voltage	Diesel	Voltmeter
Main Generator Voltage	Main Generator	Voltmeter
RCS Subcooling	PWR	
SG Safety Valve Position	PWR	

Appendix B: Uncertainty Terms

Safety Limit

Nuclear power plants and nuclear reactor facilities include physical barriers that are designed to prevent the uncontrolled release of radioactivity. Safety limits (SL) are chosen to maintain the integrity of these physical barriers. Safety limits can be defined in terms of directly measured process variables such as pressure or temperature. Safety limits can also be defined in terms of a calculated variable involving two or more measured process variables, such as departure from nucleate boiling ratio.

Analytical Limit

The Analytical Limit (AL) is the value of a given process variable at which the safety analysis models the initiation of the instrument channel protective action. ALs are documented in the safety analysis calculations and/or the Updated Final Safety Analysis Report (UFSAR). Performance of the safety analyses with conservative ALs demonstrates that the established SL and other acceptance criteria are not exceeded during normal plant transients, Anticipated Operational Occurrences, and other design basis transients. Note that only specific trip functions and/or safeguards features are required to operate for each postulated event.

Trip Setpoint

The limiting trip setpoint (LTSP) is the least conservative value of the nominal trip setpoint that still protects the AL. The nominal trip setpoint (NTSP) can be more conservative than the LTSP due to plant conditions or as a compensatory action.

Accuracy of the loop components

Accuracy reflects the intrinsic ability of the component to translate the input to the component into an output. The principal components of component accuracy are linearity, repeatability and hysteresis.

Environmental temperature and humidity changes

Environmental temperature changes typically result in variations in the output of a loop component. The effect of temperature and humidity changes in an environmentally controlled area is not excessive, however they can become dominate in areas exposed to accident environments.

Power supply variations

While power supply effects need to be considered, they are typically insignificant compared to other uncertainty terms.

Cable leakage

Cable leakage is a function of the applied voltage and the insulation resistance of the cabling and connections. During normal environmental conditions, the effect of cable leakage is negligible. When the cabling and connections are exposed to accident environmental conditions, the effect of cable leakage can be significant.

Drift

Drift is the variation in sensor or instrument channel output that may occur between calibrations that cannot be related to changes in the process variable or environmental conditions. Drift is typically regarded as time dependent however this may or may not be accurate. Allowances for drift are typically significant for loops under normal environmental conditions.

Calibration setting tolerance

The calibration setting tolerance is the range of values at the conclusion of a calibration allowed by the calibration procedure.

Measuring and test equipment requirements

Calibration procedures contain requirements on the parameters that affect the uncertainty of the equipment used to calibrate installed plant equipment. Typically, the equipment used to calibrate plant equipment is required to be at least as accurate as the plant equipment.

Integrated radiation effects

The effect of integrated radiation exposure is typically insignificant under normal environmental conditions but may be significant for post accident environments.

Seismic events and vibration

The effect of vibration is typically negligible. Seismic effects are typically negligible for low level seismic events however calibration checks may be required following significant seismic events.

Process Measurement Effects

The calibration of transmitters is typically based on the value at the sensing point. If the value at the point of interest may be different due to effects such as elevation differences or flow induced pressure drops, this difference needs to be considered.

Appendix C High Pressurizer Pressure Calculation

ENGINEERING CALCULATION COVER PAGE	CALCULATION NO. *P102*	CHANGE NO.	PAGE **1**	TOTAL NO. OF PAGES **37**
	CALCULATION. REV.	UNIT	CONVERSION:	
	CALCULATION SUBJECT: High Pressurizer Pressure Example			

Document Impact ☐ Yes ☐ No	ENGINEERING SYSTEM NUMBER/PRIMARY STATION SYSTEM DESIGNATOR BBA		Q-CLASS *II*
	CONTROLLED PROGRAM OR DATABASE	PROGRAM/DATABASE NAME(S)	VERSION/RELEASE NO.(S)
Site Programs Impact ☐ Yes ☐ No	☐ PROGRAM	☐ ALSO, LISTED BELOW	
10CFR50.59 / 72.48 Review:	☐ DATABASE		

1. BRIEF DESCRIPTION:

INITIATING DOCUMENT Rev.

2. OTHER AFFECTED DOCUMENTS;

☐ YES ☒ NO OTHER AFFECTED DOCUMENTS EXIST AND ARE IDENTIFIED ON ATTACHED FORM.

3. APPROVED BY:

ORIGINATOR (Print name/sign/date)
Qualification Verified: Initial _____

FLS (Signature/date)
Qualification Verified: Initial _____

IRE (Print name/sign/date)
Approval requires PQS EN-PQ14 Qualification Verified: Initial _____

4. CONVERSION DATE _____

TABLE OF CONTENTS

PURPOSE……3
SCOPE……4
INTRODUCTION…….. 5
LOOP DIAGRAM……..6
ASSUMPTIONS……7
DESIGN INPUT……9
METHODS/ERROR ANALYSIS……15
CALCULATIONS/CHANNEL ANALYSIS……31
CONCLUSIONS……..37
REFERENCES……38

1.0 PURPOSE

1.1 To determine the uncertainty of the high pressurizer pressure instrument loop based upon recommended changes to the calibration procedures and M&TE calibration practices and evaluates the following:

- Loop error impact on setpoint design margin
- Loop measurement accuracy
- Adequacy of setpoint value selection
- Values to be used for Setting Tolerance, and Measurement and Test Equipment accuracy test procedures and in calibrating the Measurement and Test Equipment for these same procedures
- Values to be used for determining loop operability during the calibration cycle and the functional testing cycle.

2.0 SCOPE

2.1 This calculation is performed as a bounding calculation based upon recommended changes to the current surveillance procedure practices. Since the surveillance procedures, calibration devices, and device tolerances should be identical for all divisions of a loop function, this calculation applies to the following instrument loops:

Instrument Loop Number	Function
Channel A, Loop P-0102-1	High pressurizer pressure
Channel B, Loop P-0102-2	High pressurizer pressure
Channel C, Loop P-0102-3	High pressurizer pressure
Channel D, Loop P-0102-4	High pressurizer pressure

2.2 This calculation applies to margin verification for normal operating conditions and excludes error attributed to accident environmental conditions.

2.3 Loop P-0102-1 was selected as the bounding loop for this calculation since the environmental parameters, loop devices, calibration procedures, and mode of operation appeared to be identical for all of the 102 loops. A bounding nominal trip setpoint, allowable value and rack allowance are desirable, to simplify calibration and to ensure a consistent application of the principles of loop operability.

The setpoint methodology assumes that the transient time for "turning" the process variable, including loop response time, has been considered in the plant safety analysis. Therefore, no consideration of response time errors will be considered in this calculation.

3.0 INTRODUCTION

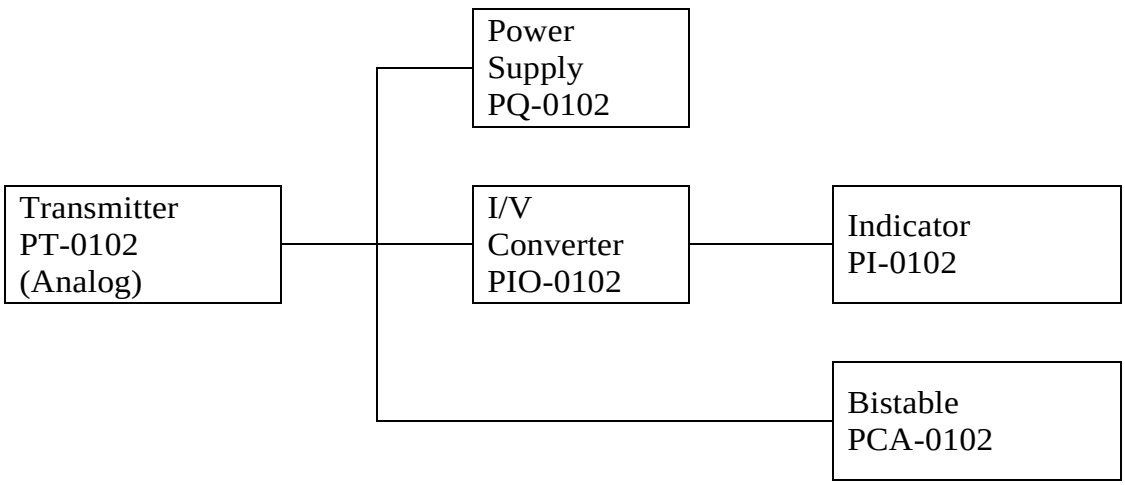
The 102 loops have multiple output signals including bistables and indicators. This calculation will only evaluate the signal to the RPS trip units for high pressurizer pressure. The high pressurizer pressure bistable operation is not required to mitigate any accident which creates an accident environment in the location of the loop components.

The high pressurizer pressure trip is designed to protect the reactor coolant system from over-pressurization. The present technical specification setpoint for high pressurizer pressure is 2400 psia which is 100 psi below the nominal safety valve setting of 2500 psia. The 2400 psia value is based upon a 2450 psia value assumed in the Safety Analysis.

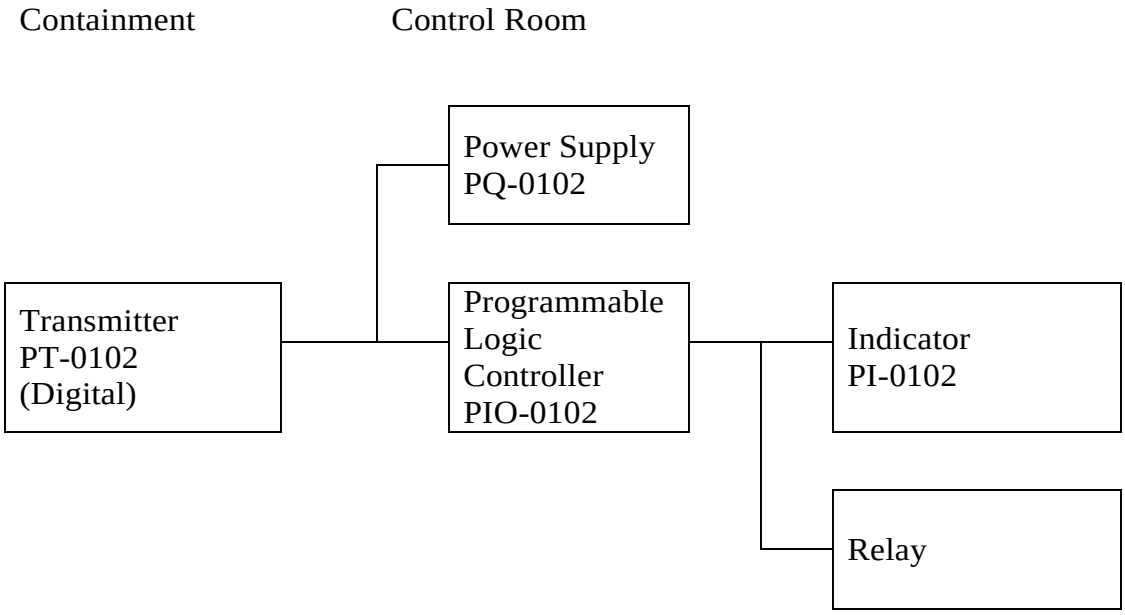
This calculation determines the error that could exist in the High Pressurizer Pressure loop function based upon recommended changes to the surveillance test procedure and to the M&TE calibration practices. This calculation is based upon the tolerance changes recommended in the conclusions section of this calculation. This calculation does not represent the current error of any loop but the maximum error which could be obtained using the procedures with the recommended changes. Because worst case loop errors are used, and tabulated in Section 8.0, this is a bounding calculation for the high pressurizer pressure trip function.

4.0 BLOCK DIAGRAM

Typical Analog Instrument Loop
Figure 4-1



Typical Digital Instrument Loop
Figure 4-2



5.0 ASSUMPTIONS

5.1 A positive (+) bias offsets a loop measurement to a higher value. A negative (-) bias offsets a loop measurement to a lower value.

5.2 All values are assumed to be in process units unless otherwise noted.

5.3 All data is assumed to be 2 sigma values with a 95% confidence level. This assumption is in accordance with the setpoint methodology. (Ref. 10.11)

5.4 1 YR = 365.25 days • 24 hours/day

1 YR = 8766 HRS

1 MO = 31 days • 24 hours/day

1 MO = 744 hours

5.5 This calculation is based on normal environmental conditions, no accident effects are considered in the calculation. Environmental conditions are based upon Reference 10.3, and Reference 10.10, the temperature study.

5.6 Containment temperatures will vary between 70 ºF and120 ºF during plant operation, based on the temperature study (Reference 10.10).

5.7 Atmospheric pressure is approximately 14.7 psi.

5.8 The density of the borated water is nearly the same as pure water so no correction will be used.

5.9 All error components will be assumed to be random unless otherwise stated. The assumption of error components being random is in accordance with the setpoint methodology Ref. 10.11

5.10 For this calculation the setting tolerances for the devices have been set equal to vendor stated device accuracy. Likewise, the total uncertainty to the M&TE used to calibrate the high pressurizer pressure instrumentation must be equal to or better than the device being calibrated.

5.11 The pressure transmitters are gauge and therefore the final absolute pressure reading of the 102 loops will be affected by the variations in the atmospheric pressure.

5.12 A containment pressure spike and subsequent trip is not part of the accident scenario that is bounded by a high pressurizer pressure trip. The affects of containment pressure variations will be limited to the Tech Spec LCO of 3 psig. Local atmospheric pressure variations which reduce the pressure will push the setpoint in a more conservative direction and are not considered in this calculation. Head correction of + 13.59 psi is added to transmitter calibration for conservatism. Specific drawings were not available to determine the as-built elevation for the process taps and the instrument installation. To ensure that this calculation is conservative, additional head correction calculations should be performed to ensure that the 13.59 psi envelopes the head correction for all four channels of the pressurizer pressure function.

5.13 Historical plant survey information for this plant area defines the normal radiation level at <25 mR/hr. Due to this low dose rate, radiation effects are assumed to be zero. (Ref. 10.3)

5.14 Loop P-0102-1 was assumed as the bounding loop for this calculation since the environmental parameters, loop devices, calibration procedures, and mode of operation appeared to be identical for all of the 102 loops.

5.15 Reference 10.8 defines the power supply effect for the transmitter as 0.005% per volt. A variation of plus or minus 0.5 volts is assumed.

5.16 10 CFR 75 allows a variation for the time of performance of technical specification surveillance. The yearly, refueling, or monthly requirements may be performed within 25% of the time period specified. This calculation assumes that the 25% allowance will be used and therefore multiplies all surveillance time periods by 1.25 to ensure conservatism.

5.17 All process devices are assumed to be calibrated in place, therefore the calibration temperature will be assumed to be equal to the minimum temperature for the device location. This assumption provides the most conservative device temperature errors.

5.18 The technical specifications limit Control Room temperature to 105°F to protect panel equipment from temperatures not to exceed 120°F. This limiting condition is assumed to be based on the potential loss of HVAC and is established as a criterion for technical specification action. This calculation assumes that this does not represent normal conditions in the Control Room. Normal Control Room temperatures are assumed not to exceed 75°F and louvered panel temperature buildup is assumed to be no greater than 10°F above that value.

6.0 DESIGN INPUT

6.1 Methodology

The following Loop Uncertainty equations from Reference 10.11 will be used as the basis for this calculation. The methods for calculating the values associated with these variables are fully explained in Reference 10.11.

Device specific errors are combined based upon the following formulas to determine the total loop error (TLE), loop drift (LD), and rack drift (RD). These values will then be used to determine three values: the nominal trip setpoint (NTSP), this is the maximum value where plant can set the trip setpoint for the bistable, other values more conservative than this value may be used for the actual plant setting, the allowable value (AV), this is the maximum value for the loop as-found during the refueling cycle calibration, and the rack drift allowance (RA), this is the maximum as-found value for the rack components during the channel functional check. Exceeding this value does not require that a report be generated but further evaluation should be performed to ensure that the loop is still operable.

$$TLE = (A+D+M+SPE+R_N+T_N+H_N+P+PCR)^{1/2} + PCN$$

$$LD = (A+D+M)^{1/2}$$

$$RD = (A_R + D_R + M)^{1/2}$$

Where:

TLE	=	Total Loop Error Allowance
LD	=	Loop Drift Allowance
RD	=	Rack Drift Allowance
A	=	Accuracy Allowance (Where setting tolerance is greater than device accuracy the setting tolerance is used in place of accuracy) Ref. 10.11
A_R	=	Accuracy Allowance for the components tested during the functional test (Rack Accuracy)
D	=	Drift Allowance
D_R	=	Drift Allowance for the components tested during the functional test (rack drift)
M	=	Maintenance and Test Equipment Allowance
M_R	=	Maintenance and Test Equipment Allowance for the components tested during the functional test (rack M&TE)
V	=	Setting Allowance
R_N	=	Radiation Effects Allowance (normal)
T_N	=	Temperature Effects Allowance (normal)
H_N	=	Humidity Effects Allowance (normal)
SPE	=	Static Pressure Effects Allowance
P	=	Power Supply Effects Allowance
PCR	=	Random Process Consideration Allowances
PCN	=	Non-random Process Consideration Allowances

The values for TLE, LD and RD calculated above are combined in the following manner to determine the nominal trip setpoint (NTSP), the allowable value (AV), and the rack allowance (RA). Since the setpoint is for an increasing process the total loop error will be subtracted from the analytical limit to determine the nominal trip setpoint. The loop drift term and the rack drift terms are each then to be added to the calculated NTSP to determine the allowable value and rack allowance, respectively. The AV term is to be used to determine if the calibration for the loop is acceptable. **If** the as-found to as-left difference between the present and previous calibrations exceeds the loop drift value or the setpoint is determined to be above the AV, then the loop must be further evaluated for operability. The RA term is to be used to determine if the functional check for the loop is acceptable. **If** the as-found to as-left difference between the present and previous functional test exceeds the rack drift value or the setpoint is determined to be above the RA, then the loop must be further evaluated for operability.

$NTSP_{MAX}$ = AL- TLE

Where:

AL	=	Analytical Limit
TLE	=	Total Loop Error

AV = NTSP + LD

Where:

$NTSP_{MAX}$ = Nominal Trip Setpoint (calculated above)

LD = Loop Drift

RA = NTSP + RD

Where:

NTSP = Nominal Trip Setpoint (calculated above)

RD = Rack Drift Allowance

6.2 Given Conditions:

6.2.1 Loop ID Number: 102 bounding case for high pressurizer pressure loops (Assumption 5.15)

6.2.2 Loop Function: high pressurizer pressure trip

6.2.3 Loop Instrument List: Ref. 10.6

P-0102-1 ~~PCA-0102-1~~ PIO-0102-1 PI-0102-1

This bounding calculation is also applicable to

P-0102-2 ~~PCA-0102-2~~ PIO-0102-2 PI-0102-2

P-0102-3 ~~PCA-0102-3~~ PIO-0102-3 PI-0102-3

P-0102-4 ~~PCA-0102-4~~ PIO-0102-4 PI-0102-4

6.2.4 Device Dependency:

Device dependency is used to determine where a common external stimulus may cause instrument error effects to not react in a random manner. Where the same letter appears in a column for both instruments then the error effects are dependent and combined in accordance with the setpoint methodology (Ref. 10.11) for dependent errors.

Device	Environment Ref. 10.7.b	Power Ref 10.6	Calibration Ref. 10.7.a	Rad Zone Ref 10.7.b
P-0102 -1	A	A	A	A
~~PCA-0102-1~~	~~B~~	~~A~~	~~B~~	~~B~~
PIO-0102-1	B	A	C	B
PI-0102-1	B	A	D	B

6.2.5 Process Considerations and Insulation Resistance

Type (PC/IR)	Magnitude (%Span)	Instrument Dependency	Uncertainty Dependency	Sign +/-
PC	0.3	Assumption 5.12		NP

This process consideration accounts for the three psi difference allowed for containment pressure variation. This three psi is a primary measurement error for the transmitter. The NP is an abbreviation for a non-random positive error or bias. Local plant atmospheric variations are assumed to be enveloped by the containment pressure variation (Assumption 5.12}.

6.2.6 Calibration Conditions:

Device	Temp °F (Ref. 10.10) (Assumption 5.6)	Static Pressure (psig) Ref. 107.a 5.12)	Atmospheric Pressure (psig) (Assumption	Calibration Period (Months) Ref. 10.7.a
P-0102-1	72.4	14.2	14.2	18.000
~~PCA-0102-1~~	~~75~~	~~N/A~~	~~N/A~~	~~1.000~~
PIO-0102-1	75	N/A	N/A	1.000
PI-0102-1	75	N/A	N/A	1.000

6.2.7 Design Input Information:

Calibrated Span	1500.00 to 2500.00 psia	Reference 10.7.a
Analytical Limit	2450.00 psia	Reference 10.1
Process Max Operating Pressure	2500 psig	Reference 10.3
Operational Time Required After Accident	0.00	Reference 10.7.b

6.2.8 Device Specific Information:

6.2.8.1 Device 1: P-0102-1 Reference 10.6

Plant Room:	Containment	
Power Supply ID:	PQ-0102-1	
Instrument Manufacturer:	Unidentified	
Model Number:	~~Analog~~	***Digital***
Surveillance Test Procedure:	IC-ST-P102	Ref. 10.7.a

6.2.8.1.1 Vendor Data Reference 10.8 and 10.12

Model	~~Analog~~	***Digital***
Tech Manual	~~Analog~~	***Digital***
Upper Range Limit	~~3000~~	***4000*** psia
Calibrated Span	1500 to 2500.00 psia	
Seismic	Accuracy within ±0.5% of upper range limit during and after a disturbance defined by a required response spectrum with a ZPA of 7g.	
Temperature	~~0.75% of URL + 0.50% for each 100 °F change~~ ***±(0.025% URL + 0.125% calibrated range) per 50 °F***	
Humidity (Steam)	Accuracy within ±(4.5% upper range limit + 3.5% span) during and after exposure to steam at the following temperatures and pressures: 420 °F (215.6 °C), 95 psig for 3 minutes 350 °F (176.6 °C), 120 psig for 7 minutes 320 °F (160 °C), 70 psig for 8 hours 265 °F (129.4 °C), 24 psig for 67 hours	
Pressure	N/A	
Radiation	Accuracy within ±(1.5% of upper range limit +1.0% span) during and after exposure to 5.5 x 10^7 rads, total integrated dosage.	
Power	~~0.005% of span for each 1 volt variation in power supply~~	

	Less than ±0.005% of calibrated span per volt
Drift	~~0.20% of URL for 30 months~~
	±0.125% of URL for five years
Accuracy	~~.25% of span~~
	±0.0075 * URL / CS % of Calibrated Range

6.2.8.1.2 Location Data Reference 10.7.b and.10.10

Room	Containment
Room Name	Containment Sector J
Harsh Environment	No
Temperature (Maximum normal)	Assumption 5.6
Humidity (Maximum normal)	100 % RH
Pressure (Maximum normal)	3 psig
Radiation (Background)	0.0025 R/hr
Seismic Response Spectrum	0.000 ZPA

6.2.8.1.3 Calibration Data Reference 10.7.a

M&TE devices used	~~0-200 mADC scale~~
	0-3000 scale
Calibrated input span	1500 to 2500 psia
Calibrated output span	~~4 to 20 Madc~~ ***Same (digital)***
Setting Tolerance	~~0.04 Madc or 0.25% of Span~~
	± 0.3 psi (equal to reference accuracy)

6.2.8.2 Device 2 PCA-0102-1 Reference 10.6

Rack/Panel	PNL-31A
Power Supply ID	PQ-0102
Instrument Manufacturer	G063
Model Number	BISTABLE
Surveillance Test Procedure	IC-ST-P102

6.2.8.2.1 Vendor Data Reference 10.9 and 10.13

Vendor Tech Manual	
Range	4 to 20 Madc
Seismic	Not provided
Temperature	0.009% of range per op change
Humidity	Not provided, Assumed = 0
Pressure	Not applicable
Radiation	Not applicable
Power	Not provided, Assumed = 0
Drift	0.5% of range for 1.4 months
Accuracy	0.612% of range

6.2.8.2.2 Location Data Reference 10.7.b

Room	PNL-31A
Room Name	Control Room
Harsh Environment	No

Temperature	75-85ºF Assumption 5.18
Humidity	65 % RH
Pressure	0.0 psig
Radiation	0.0000 R/hr
Seismic Response Spectrum	0.000 G ZPA

6.2.8.2.3 Calibration Data Reference 10.7.a

M&TE devices used	DVM 0.02% R @ FS 40 VDC scale
Calibrated input span	1.00 to 5.00 VDC
Calibrated output span	Not Applicable Switch
Setting Tolerance	0.031 Vdc or 0.765% of Span

6.2.8.3 Device 3 PIO-0102-1 Reference 10.6

Rack/Panel	PNL-31A
Power Supply ID	PQ-0102
Instrument Manufacturer	G063
Model Number	Current to voltage converter
Surveillance Test Procedure	IC-ST-P102

6.2.8.3.1 Vendor Data Reference 10.9 and 10.13

Supplier	Tech Manual
Input Range	4 to 20 Madc
Output Range	0 to 10 volts
Seismic	±0.1% of span
Temperature	±0.50% of span over 50 ºF
Humidity	Not provided, Assumed = 0
Pressure	Not applicable
Radiation	Not applicable
Power	±0.20% of span for ±5% DC voltage variations
Drift	±1.00% of span over 18 months
Accuracy	±0.25% of span

6.2.8.3.2 Location Data Reference 10.7.b

Room	PNL-31A
Room Name	Control Room
Harsh Environment	No
Temperature	75-85ºF Assumption 5.18
Humidity	65 % RH
Pressure	0.0 psig
Radiation	0.0000 R/hr
Seismic Response Spectrum	0.000 G ZPA

6.2.8.3.3 Calibration Data Reference 10.7.a

M&TE devices used	
Transmitter simulator	± (0.045 % FS + 0.01 % RDG ± 1 LSD) FS = 22 mA
Calibrated input span	4 to 20 Madc
Calibrated output span	0 to 10 volts

Setting Tolerance	No additional allowance required

6.2.8.4 Device 4 PI-0102-1 Reference 10.7.a

Rack/Panel	PNL-41A
Power Supply ID	PQ-0102
Instrument Manufacturer	G063
Model Number	Indicator
Surveillance Test Procedure	IC-ST-P102

6.2.8.4.1 Vendor Data Reference 10.9 and 10.13

Supplier	Tech Manual
Input Range	0 to 10 volts
Output Range	1500 to 2500 psia
Seismic	± 1.00% of span
Temperature	0.03% of span per 1.8 ºF change
Humidity	Not provided, Assumed = 0
Pressure	Not applicable
Radiation	Not applicable
Power	± 0.05% per 1% of voltage change
Drift	±1.00% of span over 18 months
Accuracy	±1.00% of span
Readability	± 0.5% of span

6.2.8.4.2 Location Data Reference 10.7.b

Room	PNL-31A
Room Name	Control Room
Harsh Environment	No
Temperature	75-85ºF Assumption 5.18
Humidity	65 % RH
Pressure	0.0 psig
Radiation	0.0000 R/hr
Seismic Response Spectrum	0.000 G ZPA

6.2.8.4.3 Calibration Data Reference 10.7.a

M&TE devices used	
Transmitter simulator	± (0.045 % FS + 0.01 % RDG ± 1 LSD) FS = 22 mA
Calibrated input span	0 to 10 volts
Calibrated output span	1500 to 2500 psia
Setting Tolerance	No additional allowance required

7.0 METHODS/ERROR ANALYSIS:

7.1 Calculation of Device Uncertainties

7.1.1 Basic Accuracy (a):

a = va / CS * PS Reference 10.11

Where:

va = Vendor Stated Accuracy

CS = Calibrated Span
PS = Equivalent Process Span (1000.000 psia)

7.1.1.1 P-0102-1

~~va = 0.25% of Span~~

va = ±0.0075 * URL / CS %

va = ± (0.0075 * 4000 / 1000) %

va = ± 0.03% span

Substituting:

~~a_1 = 0.0025 * 1000~~

~~a_1 = 2.50000 psi~~

a_1 = 0.0003 * 1000

a_1 = 0.3 psi

NOTE: For errors expressed in terms of calibrated span, CS/cs term is not shown, for clarity.

7.1.1.2 PCA-0102-1

va = 0.612% of Range
cs = 4.000
R = 5.000

Substituting:

a_2 = (.00612 * 5) / 4 * 1000
a_2 = 7.65000 psi

7.1.1.3 PIO-0102-1

va = 0.25% of span
cs =10.000
R = 10.000

Substituting:

a_3 = (0.0025 * 10) * 1000 / 10
a_3 = 2.50 psi

7.1.1.4 PI-0102-1

va = 1.00% of Range
cs = 10.000
R = 10.000

Substituting:

a_4 = (0.0100 * 10) * 1000 / 10
a_4 = 10.00 psi

7.1.2 Maintenance and Test Equipment accuracy: (m)

m = Error / CS • PS

Where

Error = M&TE error
CS = Calibrated Span
PS = Equivalent Process Span (1000 psia)

7.1.2.1 Device 1; P-0102-1

Accuracy of the M&TE used for the calibration of the transmitter must be equal to or better than the device being calibrated (Assumption 5.10). For the purposes of this calculation it is assumed that the total uncertainty for each M&TE device will be equal to or better than ~~0.1%~~ ***0.30 psi***.

Total M&TE error for the transmitter is;

m_1 = SRSS (Multimeter error, Gauge error)

m_1 = SRSS (0.001 * 20 * 3000 / 20, 0.001 * 3000)

m_1 = SRSS (3.00, 3.00)

m_1 = 4.24 psi

m_1 = SRSS (Multimeter error, Gauge error)

m_1 = SRSS (0.00, 0.30)

m_1 = 0.30 psi

7.1.2.2 PCA-0102-1

Since only the bistable trip point is of interest for this calculation a DVM calibrated to 0.02% of the 0-40 VDC scale is used. The error is equivalent to 0.2% of process device span. Assumption 5.10

Error = 0.2% of span

Substituting

m_2 = 0.002 • 1000

m_2 = 0.002 * PS

m_2 = 2.000 psi

7.1.2.3 PIO-0102-1 and PI-0102-1

The current to voltage converter and the indicator are calibrated as a unit. A transmitter simulator is used to provide and input current between 4 and 20 milliamps and the meter output is read. Since the uncertainty terms of the indicator are addressed separately, they do not need to be included in the M&TE term.

Error = ± (0.045 % FS + 0.01 % RDG ± 1 LSD) * 1000 / 16

FS = 22 mA

RDG = 20 mA

LSD = .01 mA

Substituting

m_{3-4} = ± (0.045 % FS + 0.01 % RDG ± 1 LSD) * 1000 / 16

m_{3-4} = ± (0.045 % 22 + 0.01 % 20 ± 0.01) * 1000 / 16

m_{3-4} = ± (0.0099 + 0.0020 ± 0.01) * 1000 / 16

m_{3-4} = ± (0.0219) * 1000 / 16

m_{3-4} = 1.36875 psi

7.1.3 Device Setting Tolerance (v):

v = st / CS * PS

Where

st = Device Setting Tolerance

CS = Calibrated Span

PS = Process Span

7.1.3.1 P-0102-1

Setting Tolerance is reduced to be equal to vendor's specified accuracy for the process device of 0.25% of calibrated span. Assumption 5.10

~~st_1 = 0.25% of span~~

st_1 = 0.03% of span

Substituting

~~v_1 = 0.0025 * 1000~~

~~v_1 = 2.50000 psi~~

v_1 = 0.0003 * 1000

v_1 = 0.30 psi

7.1.3.2 PCA-0102-1

Setting Tolerance is defined to be device vendor stated accuracy of 0.612% of range. Assumption 5.10

st = 0.612% of Range

R = 10

cs = 10

Substituting

v_2 = (0.00612 * 5) / 4 * 1000

v_2 = 7.65000 psi

7.1.3.3 PIO-0102-1 and PI-0102-1

Setting Tolerance is defined to be device vendor stated accuracy of the largest value in the serial string that is being calibrated or 1.00% of range. Assumption 5.10

st = 1.00% of Range

R = 10

cs = 10

Substituting

$v_{3\text{-}4}$ = (0.0100 * 10) / 10 * 1000

$v_{3\text{-}4}$ =10.00 psi

7.1.4 Vendor Drift (d):

d = 1.25 * tc * vd * PS / CS Reference 10.11

Where;

tc = Instrument Calibration Period (months)

vd = Vendor Drift Specification per month

CS = Calibrated Span

1.25 = Allowance given on Tech Spec. Time Requirements (10 CFR 75) Assumption 5.17

PS = Equivalent Process Span (1000.000 psia)

7.1.4.1 P-0102-1

tc = 18.000

~~vd = 0.2% * URL / 30~~

~~URL = 3000 psia~~

vd = 0.125% * URL / 60

URL = 4000 psia

Substituting:

~~d_1 = 1.25 * 18 * (0.002 * 3000 / 30) * 1000 / 1000~~

~~d_1 = 4.50 psi~~

d_1 = 1.25 * 18 * (0.00125 * 4000 / 60) * 1000 / 1000

d_1 = 1.875 psi

7.1.4.2 PCA-0102-1

tc = 1.000

vd = 0.5% * R / 1.4

R = 5.00

CS = 4.000

Substituting:

d_2 = 1.25 * 1 * (.005 * 5 / 1.4) *1000 / 4

d_2 = 5.5803571 psi

7.1.4.3 PIO-0102-1

tc = 18.000

vd = 1.00%

PS = 1000 psi

CS = 10.0 volts

Substituting:

d_3 = 1.25 * (0.0100 * 10) *1000 / 10

d_3 = 12.5 psi

7.1.4.4 PI-0102-1

tc = 18.000

vd = 1.00%

PS = 1000 psi

CS = 10.0 volts

Substituting:

d_4 = 1.25 * (0.0100) *1000 / 10

d_4 = 12.5 psi

7.1.5 Device Temperature Effects (t_N)

Normal Conditions: Reference 10.11

t_N = (N-C) * VTE * PS / CS

Where:

N = Normal Maximum Temperature

C = Calibration Temperature

VTE = Vendor Temperature Effect

URL = Upper Range Limit

CS = Calibrated Span

PS = Equivalent Process Span (1000.000 psia)

7.1.5.1 P-0102-1

N = 120.00 Assumption 5.6

C = 70.00 Assumption 5.6

~~URL = 3000~~
CS = 1000
~~VTE = ± (0.0075 * URL + 0.0050 * CS) / 100~~
~~VTE = ± (0.0075 * 3000 + 0.0050 * 1000) / 100~~
~~VTE = ± 0.275 psi / °F~~
URL = 4000
VTE = ± (0.00025* URL + 0.00125* CS) / 50
VTE = ± (0.00025 * 4000 + 0.00125* 1000) / 50
VTE = ± (2.25) / 50
VTE = ± 0.045 psi / °F
Substituting:
~~t_{N1} = (120 – 70) * (0.275) * 1000 / 1000~~
~~t_{N1} = ± 13.75 psia~~
t_{N1} = (120 – 70) * (0.045) * 1000 / 1000
t_{N1} = ± 2.25 psi

7.1.5.2 PCA-0102-1
N = 85 °F Ref. 10.7.b
C = 75 °F Assumption 5.18
VTE = 0.009% * R / 1
R = 5
CS = 4
Substituting:
t_{N2} = (85 – 75) * (0.00009 * 5 / 1) * 1000 / 4
t_{N2} = 1.125 psi

7.1.5.3 PIO-0102-1
N = 85 °F Ref. 10.7.b
C = 75 °F Assumption 5.18
VTE = 0.50%/50 ºF * R * PS / CS
R = 10
PS = 1000
CS = 10
Substituting:
t_{N3} = (85 – 75) * (0.50%/50 * 10) * 1000 / 10
t_{N3} = 1.00 psi

7.1.5.4 PI-0102-1
N = 85 °F Ref. 10.7.b
C = 75 °F Assumption 5.18
VTE = 0.03%/1.8 ºF
R = 10
PS = 1000
CS = 10
Substituting:

t_{N4} = (85 – 75) * (.005 * 10) * 1000 / 10
t_{N4} = 1.67 psi

7.1.6 Device Humidity Effects (h_N):
Normal Conditions Reference 10.11
h_N = (N-C) * VHE * PS / CS
Where:
N = Normal Maximum Humidity
C = Calibration Humidity
VHE = Vendor Humidity Effect
CS = Calibrated Span
PS = Equivalent Process Span (1000 psia)

7.1.6.1 P-0102-1
N = 100.000 Ref. 10.7.b
C = 0.000
VHE = 0.00000
CS = 1000.000
Substituting:
h_{N1} = 0.00000 psi

7.1.6.2 PCA-0102-1, PIO-0102-1, PI-0102-1
N = 65.000 Ref. 10.7.b
C = 0.000
VHE = 0.00000
CS = 40.000
Substituting:
h_{N2-4} = 0.00000 psi

7.1.7 Device Radiation Effects (r_N)
Normal Conditions Reference 10.11
r_N = VRE * PS/CS, or
r_N = VRE * 1.25 * 744 * tc * N * (1 * 10-6) * PS / CS
(second equation applies if VRE is expressed per megarad)
Where:
N = Normal Radiation Dose Rate (R/hr)
tc = Calibration period
VRE = Vendors Radiation Effect
CS = Calibrated Span
744 = Hours in a month (31*24)
PS = Equivalent Process Span (1000.000 psia)
1.25 = Allowance given on Tech Spec Time Requirements (10 CFR 75)

7.1.7.1 P-0102-1
N = 0.0025 Assumption 5.13 and Ref. 10.3
TID = 0.000
tc = 18.000

VREN = 0.5% * R for Radiation < 0.035 MRads
VREN = 0.00000 Assumption 5.13
CS = 1000.000
Substituting:
r_{N1} = 0.00000 psi Assumption 5.13

7.1.7.2 PCA-0102-1, PIO-0102-1, PI-0102-1
N = 0.000 Ref. 10.3
TID = 0.000
tc = 1.000
VREN = Not Applicable
CS = 40.000
Substituting:
r_{N2-4} = 0.000 psi

7.1.8 Device Seismic Effects (s):
s = VSE * PS/CS, or
s = VSE * SRS * PS/CS Ref. 10.11
(Second equation applies if VSE is expressed per g)
Where:
VSE = Vendors Seismic Effect
SRS = Seismic Response Spectrum
CS = Calibrated Span
PS = Equivalent Process Span (1000.000 psia)

7.1.8.1 These devices are not required to function for a seismic event, therefore seismic error is 0.00. Assumption 5.5
s_{1-4} = 0.0000

7.1.9 Device Static Pressure Effects (spe):
Static Pressure Effect applies only to instruments in direct contact with the process. Additionally, static pressure effect does not apply to instruments other than differential pressure devices where both sides are in contact with the process. Since the loop's transmitter is not a differential pressure device, this loop has no device static pressure effects. (Reference 10.11)
spe_{1-4} = 0.00000

7.1.10 Device Power Supply Effect (p)
p = PSS * VPSE * PS/CS
Where:
PSS = Power Supply Stability
VPSE = Vendor Power Supply Effect
CS = Calibrated Span
PS = Equivalent Process Span (1000.000 psia)

7.1.10.1 P-0102-1
PSS = 2.627 Attachment 3
VPSE = 0.005% * CS Assumption 5.15
CS = 1000.00

VPSE = 0.00005 * 1000
VPSE = 0.05 psi / volt
Substituting,
p_1 = PSS * VPSE * PS/CS
p_1 = 2.627 * 0.05 * 1000 / 1000
p_1 = 0.13135 psi

7.1.10.2 PCA-0102-1
PSS = 2.627 Attachment 3
VPSE = Not Provided
Substituting,
p_2 = 0.000 psi

7.1.10.3 PIO-0102-1
PSS = 2.627 Attachment 3
VPSE = ±0.20% of span for ±5% DC voltage variation
VPSE = ±0.20% / (±5% * 45 VDC) per volt
VPSE = ±0.09% per volt
Substituting,
p_3 = VPSE * PSS * CS
p_3 = ±0.09% * 2.627 *1000
p_3 = ± 2.335 psi

7.1.10.4 PI-0102-1
PSS = 2.627 Attachment 3
CS = 1000 psi
VPSE = ± 0.05% per 1% of voltage change
VPSE = ±0.05% / (±1% * 45 VDC) per volt
VPSE = ±0.11% per volt
Substituting,
p_4 = VPSE * PSS * CS
p_4 = ±0.11% * 2.627 *1000
p_4 = ± 2.890 psi

7.1.11 Indicator Readability (re)

7.1.11.1 P-0102-1
Not applicable

7.1.11.2 PCA-0102-1
Not applicable

7.1.11.3 PIO-0102-1
Not applicable

7.1.11.4 PI-0102-1
CS = 1000 psi
I_{READ} = ± 0.5% of span
Substituting,

re_4 = I_{READ} * CS

re_4 = ±0.50% *1000

re_4 = ± 5.00 psi

7.2 Calculation of Combined Loop Effects

7.2.1 Accuracy Allowance (A)

A = $(a_1^2 + a_2^2 + \ldots a_N^2)$

Recalling the device accuracies from Section 7.1.1

a_1 = ~~2.50 psi~~ ***0.30 psi***

a_2 = ~~7.65 psi~~ ***0.00 psi***

a_3 = ~~2.50 psi~~ ***0.00 psi***

a_4 = ~~10.00 psi~~ ***0.00 psi***

Substituting for the loop to the bistable,

A ~~$= (2.5)^2 + (7.65)^2$~~ ***$= (0.3)^2$***

A ~~$= 6.25 + 58.5225$~~ ***$= 0.09$***

A ~~$= 64.7725$~~ ***$= 0.09$***

A_R ~~$= (7.65)^2$~~ ***$= 0.0$***

A_R ~~$= 58.5225$~~ ***$= 0.0$***

Substituting for the loop to the indicator,

A ~~$= (2.5)^2 + (2.5)^2 + (10)^2$~~ ***$= (0.3)^2$***

A ~~$= 6.25 + 6.25 + 100$~~ ***$= 0.09$***

A ~~$= 112.50$~~ ***$= 0.09$***

A_R ~~$= (2.50)^2 + (10)^2$~~ ***$= 0.0$***

A_R ~~$=6.25 + 100$~~ ***$= 0.0$***

A_R ~~$= 106.25$~~ ***$= 0.0$***

7.2.2 Drift Allowance (D)

Independent device drift uncertainties are combined as;

D = $(d_A^2 + d_B^2 + \ldots d_F^2)$

Where the subscripts A through F represent the device drift effects in each independent loop segment.

Independent device uncertainties;

$d_A = d_1$

Dependent device uncertainties;

d_B = $(d_2 + d_3 + d_4)$

Recalling device drift from Section 7.1.4

d_1 ~~$= 4.50$ psi~~ ***$= 1.875$ psi***

d_2 ~~$= 5.58$ psi~~ ***$= 0.0$***

d_3 ~~$= 12.5$ psi~~ ***$= 0.0$***

d_4 ~~$= 12.5$ psi~~ ***$= 0.0$***

Substituting for the bistable loop,

D ~~$= (4.5)^2 + (5.5803571)^2$~~ ***$= (1.875)^2$***

D ~~$= 20.25 + 31.14$~~ ***$= 3.156$***

D ~~$= 51.39$~~ ***$= 3.156$***

D_R ~~$= (5.5803571)^2$~~ ***$= 0.0$***

D_R ~~$= 31.14$~~ ***$= 0.0$***

Substituting for the indicator loop,

D ~~$= (4.5)^2 + (12.5)^{-2} + (12.5)^{-2}$~~ ***$= (1.875)^2$***

D ~~$= 20.25 + 156.25 + 156.25$~~ ***$= 3.156$***

D ~~$= 332.75$~~ ***$= 3.156$***

D_R ~~$= (12.5)^2 + (12.5)^{-2}$~~ ***$= 0.0$***

D_R ~~$= 156.25 + 156.25$~~ ***$= 0.0$***

D_R ~~$= 312.5$~~ ***$= 0.0$***

7.2.3 M&TE Allowance (M):

Independent device M&TE uncertainties are combined as;

M $= (m_A^2 + m_B^2 + \ldots m_F^2)$

Where the subscripts A through F represent the device M&TE effects in each independent loop segment.

Independent device uncertainties;

$m_A = m_1$

Dependent device uncertainties;

$m_B = (m_2 + m_3 + m_4)$

Recalling device M&TE from Section 7.1.2,

m_1 ~~$= 4.24$ psi~~ ***$= 0.30$ psi***

m_2 ~~$= 2.00$ psi~~ ***$= 0.0$***

$m_{3\text{-}4}$ ~~$=1.369$ psi~~ ***$= 0.0$***

Substituting for the bistable loop,

M ~~$= (4.24)^2 + (2)^2$~~ ***$= (0.30)^2$***

M ~~$= 17.98 + 4$~~ ***$= 0.09$***

M ~~$= 21.98$~~ ***$= 0.09$***

M_R ~~$= (2)^2$~~ ***$= 0.0$***

M_R ~~$= 4.00$~~ ***$= 0.0$***

Substituting for the indicator loop,

M ~~$= (4.24)^2 + (1.369)^2$~~ ***$= (0.30)^2$***

M ~~$= 17.98 + 1.874$~~ ***$= 0.09$***

M ~~$= 19.85$~~ ***$= 0.09$***

M_R ~~$= (1.369)^2$~~ ***$= 0.0$***

M_R ~~$= 1.873$~~ ***$= 0.0$***

7.2.4 Setting Allowance (V):

Independent device setting tolerance uncertainties are combined as;

V $= (v_A^2 + v_B^2 + \ldots v_F^2)$

Where the subscripts A through F represent the device setting tolerance effects in each independent loop segment.

Independent device uncertainties;

$v_A = v_1$

Dependent device uncertainties;

$v_B = (v_2 + v_3 + v_4)$

Recalling device setting tolerance from Section 7.1.3,

v_1 ~~= 2.500 psi~~ ***= 0.30 psi***

v_2 ~~= 7.650 psi~~ ***= 0.0***

v_{3-4} ~~=10.00 psi~~ ***= 0.0***

Substituting for the bistable loop,

V ~~$= (2.5)^2 + (7.65)^2$~~ ***$= (0.30)^2$***

V ~~$= 6.25 + 58.5225$~~ ***$= 0.09$***

V ~~$= 64.7725$~~ ***$= 0.09$***

V_R ~~$= (7.65)^2$~~ ***$= 0.0$***

V_R ~~$= 58.5225$~~ ***$= 0.0$***

Substituting for the indicator loop,

V ~~$= (2.5)^2 + (10.00)^2$~~ ***$= (0.30)^2$***

V ~~$= 6.25 + 100.00$~~ ***$= 0.09$***

V ~~$= 106.25$~~ ***$= 0.09$***

V_R ~~$= (10.00)^2$~~ ***$= 0.0$***

V_R ~~$= 100.00$~~ ***$= 0.0$***

7.2.5 Temperature Effect Allowance

Independent environmental temperature effects are combined as follows: There are no temperature dependent process concerns.

Normal, $T_N = (T_{NA}^2 + T_{NB}^2 + \ldots T_{NF}^2)$

Where the subscripts A through F represent the combined device temperature effects in each independent plant environment.

Independent device temperature effects; Normal:

Normal, $T_{NA} = t_{N1}$

Dependent device temperature effects;

Normal, $T_{NB} = (t_{N2} + t_{N3} + Pc + IR)$

Recalling device temperature effects from Section 7.1.5,

t_{N1} ~~= 13.75 psi~~ ***= ± 2.25 psi***

t_{N2} ~~=1.125 psi~~ ***= 0.0***

Substituting for the bistable loop,

T_N ~~$= (13.75)^2 + (1.125)^2$~~ ***$= (2.25)^2$***

T_N ~~$= 189.0625 + 1.265625$~~ ***$= 5.0625$***

T_N ~~$= 190.328$~~ ***$= 5.0625$***

Substituting for the indicator loop,

T_{NR} ~~$= (13.75)^2 + (1.00 + 1.67)^2$~~ ***$= (2.25)^2$***

T_{NR} ~~$= (13.75)^2 + (2.67)^2$~~ ***$= 5.0625$***

T_{NR} ~~$= 189.0625 + 7.1289$~~ ***$= 5.0625$***

T_{NR} ~~$= 196.191$~~ ***$= 5.0625$***

7.2.6 Humidity Effects Allowance (Hn):

Independent environmental humidity effects are combined as follows:

There are no humidity dependent process concerns.

Normal, $H_N = (h_{NA}^2 + h_{NB}^2 + \ldots h_{NF}^2)$

The subscripts A through F represent the combined device humidity effects in each independent plant environment.

Independent device humidity effects;
Normal, H_{NA} = h_{N1}
Dependent device humidity effects;
Normal, H_{NB} = (h_{N2} + h_{N3} + Pc + IR)
Recalling device humidity effects from Section 7.1.6,
h_{N1} = 0.00000
h_{N2-4} = 0.00000
Substituting and grouping according to device environmental dependency, process concern and insulation resistance dependency.
H_N = 0.00000 ***(No change)***

7.2.7 Radiation Effects Allowance (R)
Independent environmental radiation effects are combined as follows: There are no radiation dependent process concerns.
Normal, R_N = (r_{NA}^2 +r_{NB}^2 + … r_{NF}^2)
Where the subscripts A through F represent the combined device radiation effects in each independent plant environment.
Independent device radiation effects;
Normal, R_{NA} = r_{N1}
Dependent device radiation effects;
Normal, R_{NB} = (r_{N2} + r_{N3} + Pc + IR)
Recalling device radiation effects from Section 7.1.7,
r_{N1} = 0.00000 psia
r_{N2-4} = 0.00000 psia
Substituting and grouping according to device radiation dependency, process concern and insulation resistance dependency.
R_N = 0.000 ***(No change)***

7.2.8 Seismic Allowance (S):
Independent device seismic uncertainties are combined as;
S = (s_A^2 +s_B^2 + … s_F^2)
The subscripts A through F represent the device seismic effects in each independent loop segment.
Independent device uncertainties;
s_A = s_1
Dependent device uncertainties;.
s_B = (s_2 + s_3 + s_4)
Recalling device seismic uncertainties from Section 7.1.8,
s_1 = 0.00000 psia
s_{2-4} = 0.00000 psia
Substituting and combining according to device location dependency;
S = 0.0000 ***(No change)***

7.2.9 Power Supply Allowance (P):
Independent device power supply uncertainties are combined as;
P = (p_A^2 +p_B^2 + … p_F^2)

The subscripts A through F represent the device power supply effects in each independent loop segment.

Independent device uncertainties;

$p_A = p_1$

Dependent device uncertainties;

$p_B = (p_2 + p_3 + p_4)$

Recalling device power supply uncertainties from Section 7.1.10,

p_1 ~~$= 0.13135$ psi~~ ***$= 0.13135$ psi***

p_2 ~~$= 0.00$ psi~~ ***$= 0.00$***

p_3 ~~$= 2.335$ psi~~ ***$= 0.00$***

p_4 ~~$= 2.890$ psi~~ ***$= 0.00$***

Substituting for the bistable loop,

P ~~$= (0.13135)^2 + (0.00)^2$~~ ***$= (0.13135)^2 + (0.00)^2$***

P ~~$= 0.0173$~~ ***$= 0.0173$***

P_R ~~$= (0.00)^2$~~ ***$= (0.00)^2$***

P_R ~~$= 0.00$~~ ***$= 0.00$***

Substituting for the indicator loop,

P ~~$= (0.13135)^2 + (2.335)^2 + (2.890)^2$~~ ***$= (0.13135)^2 + (0.00)^2 + (0.00)^2$***

P ~~$= (0.0173) + (5.4522) + (8.3521)$~~ ***$= 0.0173$***

P ~~$= 13.8216$~~ ***$= 0.0173$***

P_R ~~$= (2.335)^2 + (2.890)^2$~~ ***$= (0.00)^2 + (0.00)^2$***

P_R ~~$= (5.4522) + (8.3521)$~~ ***$= 0.00 + 0.00$***

P_R ~~$= 13.8043$~~ ***$= 0.00$***

7.2.10 Process Concerns (PC)

Process Concerns can affect the form of the calculation in any of three possible ways depending on whether or not the process concerns are random or non-random and the dependency of random process concerns.

For Non-Random Process Concerns

$PC = pc$

For Random, Non-Dependent Process Concerns

$PC = pc^2$

For Random, Dependent Process Concerns

$PC = pc$

Random Process Considerations:

Recall the Random Process Considerations and IRs which are not dependent on environmental or radiation conditions.

0.00000 psia

PCR = 0.00000

Non-Random Process Considerations:

Recall the Non-Random Process Considerations and IRs

3.00000 psia

PCN = 3.00 ***(No change)***

7.2.11 Static Pressure Allowances (SP)

There are no device static pressure effects associated with this loop, therefore

SP = 0.0000 ***(No change)***

7.2.12 Readability (I):

Independent device power supply uncertainties are combined as;

$I = (i_A^2 + i_B^2 + \ldots i_F^2)$

The subscripts A through F represent the device power supply effects in each independent loop segment.

Independent device uncertainties;

$i_A = i_1$

Dependent device uncertainties;

$i_B = (i_2 + i_3 + i_4)$

Recalling device power supply uncertainties from Section 7.1.10,

i_1 ~~= 0.00 psi~~ ***= 0.00 psi***

i_2 ~~= 0.00 psi~~ ***= 0.00***

i_3 ~~= 0.00 psi~~ ***= 0.00***

i_4 ~~= 5.00 psi~~ ***= 0.00***

Substituting for the bistable loop,

I ~~$= (0.00)^2 + (0.00)^2$~~ $= (0.00)^2 + (0.00)^2$

I ~~$= 0.00$~~ $= 0.00$

I_R ~~$= (0.00)^2$~~ $= (0.00)^2$

I_R ~~$= 0.00$~~ $= 0.00$

Substituting for the indicator loop,

I ~~$= (0.00)^2 + (0.00)^2 + (5.00)^2$~~ $= (0.00)^2 + (0.00)^2 + (0.00)^2$

I ~~$= (0.00) + (0.00) + (25.00)$~~ $= 0.00$

I ~~$= 25.00$~~ $= 0.00$

I_R ~~$= (0.00)^2 + (5.00)^2$~~ $= (0.00)^2 + (0.00)^2$

I_R ~~$= (0.00) + (25.00)$~~ $= 0.00 + 0.00$

I_R ~~$= 25.00$~~ $= 0.00$

8.0 CALCULATION/CHANNEL ANALYSIS

8.1 Error Combination, Bistable Loop

The errors are combined based upon the following formulas to determine the total loop error (TLE), loop drift (LD), and rack drift (RD). These values will then be used to determine three values:

the nominal trip setpoint (NTSP), this is the maximum value where plant can set the trip setpoint for the bistable, other values more conservative than this value may be used for the actual plant setting,

the allowable value (AV), this is the: maximum value for the loop as-found during the refueling cycle calibration, and

the rack drift allowance (RA), this is the maximum as-found value for the rack components during the channel functional check. Exceeding this value does not require that an Incident Report be generated but further evaluation should be performed to ensure that the loop is still operable.

$TLE = (A+D+M+SPE+R_N+T_N+H_N+P+PCR)^{1/2}+PCN$

$LD = (A+D+M)^{1/2}$

$RD = (A_R +D_R+ M_R)^{1/2}$

Where:

TLE = Total Loop Error Allowance

LD = Loop Drift Allowance

RD = Rack Drift Allowance

A = Accuracy Allowance (Where setting tolerance is greater than device accuracy the setting tolerance is used in place of accuracy)

A_R = Accuracy Allowance for the components tested during the functional test (Rack Accuracy)

D = Drift Allowance

D_R = Drift Allowance for the components tested during the functional test (rack drift)

M = Maintenance and Test Equipment Allowance

M_R = Maintenance and Test Equipment Allowance for the components tested during the functional test (Rack M&TE)

V = Setting Allowance

R_N = Radiation Effects Allowance (normal)

T_N = Temperature Effects Allowance (normal)

H_N = Humidity Effects Allowance (normal)

SPE = Static Pressure Effects Allowance

P = Power Supply Effects Allowance

PCR = Random Process Consideration Allowances

PCN = Non-random Process Consideration Allowances

Substituting;

Only the larger of accuracy or setting tolerance is used in the calculation (Ref. 10.11). Setting tolerance has been set equal to vendor basic accuracy as one of the recommendations for this calculation, therefore, Setting Tolerance is not considered. Humidity (H), Radiation (R), Static Pressure Effect (SPE), and random Process Concerns (PCR) have all been justified to not be

applicable to the loop function or calculated to be zero. The remaining factors are therefore considered.

A	~~= 64.77~~	***= 0.09***	(7.2.1)
D	~~= 51.39~~	***= 3.156***	(7.2.2)
M	~~= 22.00~~	***= 0.09***	(7.2.3)
V	~~= 64.77~~	***= 0.09***	(7.2.4)
T_N	~~= 190.328~~	***= 5.0625***	(7.2.5)
P	= 0.0173	***No change***	(7.2.9)
PCN	= 3.000	***No change***	(7.2.10}
A_R	~~= 58.5225~~	***= 0.0***	(7.2.1)
D_R	~~= 31.14~~	***= 0.0***	(7.2.2)
M_R	~~= 4.000~~	***= 0.0***	(7.2.3}
V_R	~~= 58.5225~~	***= 0.0***	(7.2.4)

TLE $= (A+ D + M + T_N + P)^{1/2} + PCN$

~~TLE $= (64.77 + 51.39 + 22.00 + 190.328 + 0.0173)^{1/2} + 3$~~

~~TLE $= (328.5053)^{1/2} + 3$~~

~~TLE = 18.12 + 3~~

~~TLE = 21.12 psi~~

TLE $= (0.09+ 3.516+ .09 + 5.0625 + 0.0173)^{1/2} + 3$

TLE $= (8.775)^{1/2} + 3$

TLE = 2.962 + 3

TLE = 5.962 psi

LD $= (A + D + M)^{1/2}$

~~LD $= (64.77 + 51.39 + 22.00)^{1/2}$~~

~~LD $= (138.17)^{1/2}$~~

~~LD = 11.75 psi~~

LD $= (0.09 + 3.516 + 0.09)^{1/2}$

LD $= (3.696)^{1/2}$

LD = 1.922 psi

RD $= (A_R + D_R + M_R)^{1/2}$

Since only the bistable trip is checked on the monthly functional the rack accuracy term is limited to the accuracy, drift, and M&TE for the bistable.

~~RD $= (58.5225 + 31.140385 + 4.000)^{1/2}$~~

~~RD $= \{93.662885)^{1/2}$~~

~~RD = 9.68 psi~~

RD = 0.0

8.2 Determining NTSP, AV, and RA for the bistable loop

The values for LE, LD and RD calculated above are combined in the following manner to determine the nominal trip setpoint (NTSP), The allowable value (AV), and the rack allowance (RA). Since the setpoint is for an increasing process the total loop error will be subtracted from the Analytical Limit to determine the nominal trip setpoint. The loop drift term and the rack drift term are each then is added to the calculated NTSP to determine the allowable value and rack allowance, respectively.

$NTSP_{MAX}$ = AL- TLE

Where:

~~AL = Analytical Limit (2450 psia)~~

~~TLE = Total Loop Error (21.87 psia)~~

~~$NTSP_{MAX}$ = 2450 – 21.12~~

~~$NTSP_{MAX}$ = 2428.88~~

AL = Analytical Limit (2450 psia)

TLE = Total Loop Error (5.90 psia)

$NTSP_{MAX}$ = 2450 – 5.96

$NTSP_{MAX}$ = 2444.04

This represents the maximum nominal trip setpoint. The existing nominal trip setpoint is 2350 psia. Since the existing trip setpoint is less than the maximum nominal trip setpoint, the existing nominal trip setpoint is acceptable.

AV = $NTSP_{MAX}$ + LD

Where:

NTSP = Maximum Nominal Trip Setpoint (~~2428.88 psia~~) ***2444.04***

LD = Loop Drift (~~11.75 psi~~) ***(1.826 psi)***

Substituting;

AV = $NTSP_{MAX}$ + LD

~~AV = 2428.88+ 11.75~~

~~AV = 2440.63~~

AV = 2444.04 + 1.922

AV = 2445.96

RA = $NTSP_{MAX}$ + RD

Where:

$NTSP_{MAX}$ = Maximum Nominal Trip Setpoint (~~2428.88 psia~~) ***2444.04***

RD = Rack Drift Allowance (9.68 psi) ***(0.00)***

Substituting;

RA = $NTSP_{MAX}$ + RD

~~RA = 2428.88 + 9.68~~

~~RA = 2438.56~~

RA = 2444.04 + 0.00

RA = 2444.04

The current Technical Specification setpoint is 2400 psia, and the current plant setting is 2350 psia. The Calculated Nominal Trip setpoint value of ~~2438~~ ***2444.04*** indicates that there is sufficient margin for the Technical Specification setpoint and the current plant setting to account for all accuracies determined in the calculation.

8.3 Error Combination, Indicator Loop

The errors are combined based upon the following formulas to determine the total loop error (LE), loop drift (LD), and rack drift (RD) for the indicator loop. These values will then be used to determine

TLE = $(A+D+M+SPE+R_N+T_N+H_N+P+PCR)^{1/2}+PCN$

LD = $(A+D+M)^{1/2}$

RD = $(A_R+D_R+M_R)^{1/2}$

Where:

TLE = Total Loop Error Allowance

LD = Loop Drift Allowance

RD = Rack Drift Allowance

A = Accuracy Allowance (Where setting tolerance is greater than device accuracy the setting tolerance is used in place of accuracy)

A_R = Accuracy Allowance for the components tested during the functional test (Rack Accuracy)

D = Drift Allowance

D_R = Drift Allowance for the components tested during the functional test (rack drift)

M = Maintenance and Test Equipment Allowance

M_R = Maintenance and Test Equipment Allowance for the components tested during the functional test (Rack M&TE)

V = Setting Allowance

R_N = Radiation Effects Allowance (normal)

T_N = Temperature Effects Allowance (normal)

H_N = Humidity Effects Allowance (normal)

SPE = Static Pressure Effects Allowance

P = Power Supply Effects Allowance

PCR = Random Process Consideration Allowances

PCN = Non-random Process Consideration Allowances

Substituting;

Only the larger of accuracy or setting tolerance is used in the calculation (Ref. 10.11). Setting tolerance has been set equal to vendor basic accuracy as one of the recommendations for this calculation, therefore, Setting Tolerance is not considered. Humidity (H), Radiation (R), Static Pressure Effect (SPE), and random Process Concerns (PCR) have all been justified to not be applicable to the loop function or calculated to be zero. The remaining factors are therefore considered.

A	~~= 112.500~~	***= 0.09***	(7.2.1)
D	~~= 332.75~~	***= 3.516***	(7.2.2)
M	~~= 19.850~~	***= 0.09***	(7.2.3)
V	~~= 106.25~~	***= 0.09***	(7.2.4)
T_N	~~= 196.191~~	***= 5.0625***	(7.2.5)
P	~~= 13.822~~	***= 0.0173***	(7.2.9)
PCN = 3.000		***(No change)***	(7.2.10}
A_R	~~= 106.250~~	***= 0.0***	(7.2.1)
D_R	~~= 312.500~~	***= 0.0***	(7.2.2)
M_R	~~= 1.873~~	***= 0.0***	(7.2.3}
V_R	~~= 100.00~~	***= 0.09***	(7.2.4)

$TLE = \pm (A + D + M + T_N + P)^{1/2} + PCN$

~~$TLE = \pm (112.500 + 332.75 + 19.850 + 196.191 + 13.822)^{1/2} + 3$~~

~~$TLE = \pm (675.113)^{1/2} + 3$~~

~~$TLE = \pm 25.983 + 3$~~

~~$TLE = +28.983$ psi~~

TLE = ± (0.09 + 3.516+ 0.09 + 5.0625 + 0.0173)$^{1/2}$ + 3
TLE = ± (8.775)$^{1/2}$ + 3
TLE = ±2.962+ 3
TLE = +5.962 psi

Three channels of pressurizer pressure instrumentation are used to monitor pressurizer pressure to avoid an un-needed reactor trip. The random portion of the indicator loop uncertainty can be divided by the square root of the number of independent channels or the square root of three.

$TLE_{3\ CH}$ = TLE_{RANDOM} / (Number of channels)$^{1/2}$ + PCN

~~$TLE_{3\ CH}$ = 25.983 / (3)$^{1/2}$ + 3~~
~~$TLE_{3\ CH}$ = 25.983 / 1.732 + 3~~
~~$TLE_{3\ CH}$ = 15.001 + 3~~
~~$TLE_{3\ CH}$ = 18.001 psi~~
$TLE_{3\ CH}$ = 2.962 / (3)$^{1/2}$ + 3
$TLE_{3\ CH}$ = 2.962 / 1.732 + 3
$TLE_{3\ CH}$ = 1.710 + 3
$TLE_{3\ CH}$ = 4.710 psi

The normal operating pressure is 2250 psia ± 25 psi. The maximum normal operating pressure can be calculated as follows.

Maximum normal operating pressure = Nominal pressure + band + $TLE_{3\ CH}$

~~Maximum normal operating pressure = 2250 + 25 + 18.001~~
~~Maximum normal operating pressure = 2293.001 psia~~
Maximum normal operating pressure = 2250 + 25 + 4.710
Maximum normal operating pressure = 2279.710 psia

The operating margin can be calculated by subtracting the bistable uncertainty and the maximum normal operating pressure from the nominal trip setpoint. Calculating the uncertainty of the bistable only,

TLE_{BS} = $(A+D+M+SPE+R_N+T_N+H_N+P+PCR)^{1/2}+PCN$

~~A = (7.65)^2 = 58.5225 (7.2.1)~~
~~D = (5.58)^2 = 31.1364 (7.2.2)~~
~~M = (2)^2 = 4.00 (7.2.3)~~
~~V = (7.65)^2 = 58.5225 (7.2.4)~~
~~T_N = (1.125)^2 = 1.266 (7.2.5)~~
~~P = (0)^2 = 0 (7.2.9)~~
~~PCN = 0 (7.2.10)~~
~~TLE = ± (A + D + M + T_N + P)$^{1/2}$ + PCN~~
~~TLE_{BS} = (58.5225 + 31.1364 + 4.00 + 1.226 + 0)$^{1/2}$ + 0~~
~~TLE_{BS} = (94.925)$^{1/2}$ + 0~~
~~TLE_{BS} = 9.743 psi~~
A = (0.00)^2 = 0.00 (7.2.1)
D = (0.00)^2 = 0.00 (7.2.2)
M = (0.00)^2 = 0.00 (7.2.3)
V = (0.00)^2 = 0.00 (7.2.4)
T_N = (0.00)^2 = 0.00 (7.2.5)

P = (0.00)^2 = 0.00 (7.2.9)

PCN = 0.00 = 0.00 (7.2.10}

TLE = ± (A + D + M + T_N + P)$^{1/2}$ + PCN

TLE_{BS} = (0.00 + 0.00 + 0.00 + 0.00 + 0.00)$^{1/2}$ + 0.00

TLE_{BS} = (0.00)$^{1/2}$ + 0.00

TLE_{BS} = 0.00 psi

Operating margin = $NTSP_{ACTUAL}$ - TLE_{BS} – (maximum operating pressure + $TLE_{3\ CH}$)

Rearranging,

Operating margin = $NTSP_{ACTUAL}$ – maximum operating pressure - TLE_{BS} - $TLE_{3\ CH}$

Since TLE_{BS} and $TLE_{3\ CH}$ are random, independent and approximately normally distributed, they can be combined using the square root of the sum of the squares.

Operating margin = $NTSP_{ACTUAL}$ – max operating pressure – (TLE_{BS}^2 + $TLE_{3\ CH}^2$)$^{1/2}$

~~Operating margin = 2350 – 2275 – (9.743^2 + 18.001^2)$^{1/2}$~~

~~Operating margin = 75 – (94.925 + 324.045)$^{1/2}$~~

~~Operating margin = 75 – (418.970)$^{1/2}$~~

~~Operating margin = 75 – 20.469~~

~~Operating margin = 54.531 psi~~

Operating margin = 2350 – 2275 – (0.00^2 + 4.710 ^{2})$^{1/2}$

Operating margin = 75 – (0.00 + 22.187)$^{1/2}$

Operating margin = 75 – (22.187)$^{1/2}$

Operating margin = 75 – 4.710

Operating margin = 70.290 psi

9.0 CONCLUSIONS

The requirement of the high pressurizer pressure is to trip at or below 2450 psia as assumed in the accident analysis. The current plant setting of this trip is 2350 psia. This calculation used the limiting errors based upon recommended changes to the calibration procedures for the process devices and plant standard procedures for calibration of the M&TE devices. This calculation demonstrates that the current process instrumentation specifications are sufficient to perform the function required, and that only the calibration procedures require modification. Analysis of the operating margin calculates that a minimum pressure of ~~54.531~~ ***70.290*** psi is available to avoid an un-needed reactor trip.

10.0 REFERENCES

10.1 [Plant name deleted] Technical Specifications

10.2 Not used

10.3 [Plant name deleted] Updated Safety Analysis Report

10.4 Not used

10.5 Not used

10.6 Drawing [number deleted] Revision 61

10.7 Documents

a. Calibration Procedures [procedure titles deleted]

b. [Specific document reference deleted]

10.8 Transmitter Technical Manual [Supplier name deleted]

10.9 Technical Manual [Supplier name deleted]

10.10 A-E Temperature Study [A-E name deleted]

10.11 [Company name deleted] Engineering Design Standard "Instrument Selection and Uncertainty Analysis"

10.12 Vendor Calculation [Vendor name deleted]

10.13 Vendor Letters [specific reference deleted]

Appendix D INPO Data Search for Instrument Failures

INPO Data Search for Instrument Failures

The Equipment Performance Information Exchange (EPIX) System, maintained by the Institute of Nuclear Power Operations (INPO), was search for relevant instrument failures over the time period 1997 – 2012, a 15 year period. Nuclear utilities are obligated to enter all component failures that meet a certain criteria into this data base so that a comprehensive set of information can be accumulated for trend analysis and specific component histories.

A number of relevant search terms for plant sensors were entered into the EPIX System yielding a large number of recorded failures. Typical failures for some of the search terms are listed below. In addition, a summary is provided of the most common causes of instrument loop failures.

Search Term – "Pressure Transmitter" – Search results 293 documents

Typical Failures:

- Failure of pressure transmitter for Control Room pressure indication and control.
- Failure of sensor in Feedwater System diaphragm sensor/transmitter that supports feedwater system indicator.
- Failure of sensing line in Leak Monitoring System diaphragm sensor/transmitter that supports RCIC pump.
- Failure of circuit board/card in Essential Service Water System dielectric/capacitive sensor/transmitter.
- Failure of capacitor(s) in Containment Spray System (PWR) AC:DC electronic power supply that supports Containment Combustible Gas Control System, axial-single stage compressor VXAHARFA.
- Failure of electrical termination (lug/connector) in RPS pressurizer pressure channels.
- Failure of tube in Reactor Coolant System (PWR) bourdon tube sensor/transmitter.
- Failure of Closed/Component Cooling Water System bellows sensor/transmitter. The transmitter's sensing lines were clogged.
- Failure of potentiometer in RPS steam generator pressure channels.

Search Term – "Temperature Sensor" – Search results 116 documents

Typical Failures:

- AP-913 high critical component failure due to failure of switch and electrical termination (lug/connector) in Chilled Water System temperature bistable/switch.
- Outage impacted due to failure of thermistor in Cntl. Bldg./Complex Environ. Cntl. Sys. flow bistable/switch that supports Control Room A/C Equipment Cooling Blower 2HVC*ACU1B.
- Supplemental Diesel Generator M-1005 tripped on high coolant temperature when load was removed. Failed coolant temperature sensor needed replacement. failure of the RTD temperature element.

- Automatic reactor scram due to failure of subcomponent bimetallic sensor/transmitter of Main Generator Output Power System power step-up transformer Main Transformer X1. The unit remained shut down for approximately three weeks to replace the main XFMR with an on-site spare. The inappropriate actuation of the XFMR deluge system was caused by failure of a bimetallic temperature detector near the transformer that is used to detect a rapid increase in temperature, symptomatic of a fire.
- Failure of switch in Cntl. Bldg./Complex Environ. Cntl. Sys. bistable that supports Control Room A/C Equipment Cooling Blower 210.1-120.

Search Term – "Speed Sensor" – Search results 35 documents

Typical Failures:

- Emergency Diesel Generator Failed to Start due to A3 Speed Pick-up Sensor Amphenol Connector Found Disconnected.
- Failure of circuit board/card in RPS reactor coolant pump speed channels that supports RPS high local power density/low DNBR channels CPCICALC0001-C.

Search Term – "Level Instrument" – Search results 237 documents

Typical Failures:

- Automatic reactor scram due to failure of Containment Isolation Control System level bistable/switch. The level instrument had been successfully isolated and calibrated prior to the event. When restoring the instrument to service, a pressure fluctuation occurred coincident with opening of the reference leg isolation valve, causing the other instruments on the shared reference leg to indicate false high reactor level, resulting in the reactor scram.
- Failure of sensing line in Condensate Storage and Transfer System sensor/transmitter LT00812A. During this event on 12/09/10, a freezing situation occurred causing the level transmitter to malfunction.
- Failure of circuit board/card in Steam Generator Blowdown System (PWR) diaphragm sensor/transmitter.
- Failure of Essential Service Water System float sensor/transmitter that supports Essential Service Water System centrifugal - axial pump 1SW-E017.
- Failure of amplifier in Containment Spray System (PWR) indicator.
- AP-913 failure event due to failure of electrical termination (lug/connector) in RPS steam generator level channels. Red Channel Steam Generator 'A' Level signal isolator LM-461A failed low because the connector pin was not fully inserted. The apparent cause of this event appears to be that the pin was not locked into the connector housing by the manufacturer.
- Failure of Standby Liquid Control System (BWR) tank/accumulator. Crystalline deposits caused a false level to be transmitted to the Control Room instrumentation.

Search Term – "Flow Transmitter" – Search results 359 documents

Typical Failures:

- Failure of bellows in Plant Protection System diaphragm sensor/transmitter 1-NFP-222. AS FOUND data for 1-NFP-222 (Reactor Coolant Loop 2, Cold Leg Channel III, Reactor Protection Flow Transmitter) was found out of calibration tolerance.
- Failure of electrical termination (lug/connector) in RPS reactor coolant flow channels 2DWRDTU3.
- Failure of sensing line in Reactor Core Iso. Cooling Sys. (BWR) dielectric/capacitive sensor/transmitter that supports *RCIC Pump 2ICS*P1. The effect of the pressure pulses is amplified by air in the lines leading to the flow transmitter failure.
- AP-913 high critical component failure due to failure of capacitor(s) and none identified by investigation in RPS reactor coolant flow channels that supports *Rctr Clnt Pump 22RCP.
- Failure of Essential Service Water System diaphragm sensor/transmitter. The apparent cause of the incorrect flow indication and the flow differential alarm was a failed outlet flow transmitter and an out of calibration square root extractor.

Most common failure causes, for all instrument types:

- Failed capacitors in the power supplies.
- Failed sensing lines; due to damage, corrosion, plugging and air intrusion.
- Degraded contacts for relays and circuit cards.
- Failed terminal lugs.
- Failed bellows or diaphragms in pressure sensors.
- Leaking or failed fittings for sensing lines.

Typical Nuclear Power Plant Units 1 and 2

Project Code _____

Subproject Code _____

Subproject Name _____

Design Phase Engineering

Specialty N/A

Document Title Typical Unit 1 & 2 1E RPS Reliability Analysis

Serial Number _____

Prepared by _____

Reviewed by _____

Reviewed by _____

Approved by _____

Table of Contents

1.0 Purpose
2.0 Summary of Results
3.0 Input and Design Criteria
4.0 Assumptions
5.0 Method of Analysis
6.0 Reliability Calculations
7.0 References
8.0 Conclusions

1.0 Purpose

The purpose of this calculation is to document the methodology and results of the Reliability Analysis, where applicable, for the safety system architecture as defined by a typical nuclear power plant including the temperature sensor input string.

The intent of the Reliability Analysis is to provide a quantitative evaluation of the reactor trip system (RTS) and the Engineered Safety Features Actuated (ESFAS). The goal is to demonstrate that the electronic hardware portions of the RTS and ESFAS achieve an unavailability factor and an $MTTF_{spurious}$, as required by the utility. The unavailability parameter calculated is the average probability of failure on demand (PFD_{avg}).

This is a NUCLEAR SAFETY RELATED document.

2.0 Summary of Results

The PFDavg is calculated for the eight PLCs in the Reactor Trip Subsystems and the four Train PLCs that perform the ESFAS safety functions. The PFDavg is computed for a proof test interval (TI) of 18 months. The requested unavailability value (PFD_{avg}) of 5.99×10^{-5} (from Section 8), as per IEEE-352 and IEC-61508, are achieved for the RTS systems for a proof test interval of 18 months for the logic solver portion and crediting online diagnostics and online monitoring for the temperature sensor string (see Section 8).

The analysis conservatively selected the worst case bounding functions (Most Significant Safety Instrumented Function) based on the number of I/O modules used in an RTS and ESFAS function and also considering the normally energized and de-energized channel to channel and channel to train communications for some ESFAS functions (discussed in Section 3.2). The Most Significant Safety Instrumented Function for the RTS is the RCP Flow function. The Most Significant Safety Instrumented Function for the ESFAS is the SI & CIA function

The following Chart 1 summarizes the results of the reliability analysis for the worst case redundant PLCs configurations in the RPS. The TI used in the analysis is 13,140 hours (18 months) for the Dual ESFAS Train System and for the two Reactor Trip Subsystems PLC portion. The results address the reliability of the specific configurations utilized for the typical nuclear design. The temperature sensor string unavailability results are included in Chart 2 and show that with cross channel comparison of triple redundant temperature transmitters in online monitoring, the input string supports the logic solver unavailability when combined to meet the 5.99×10^{-5} PFDavg.

The PLC configurations for the RT and Train Subsystems are provided in the next section on Inputs and Design Criteria.

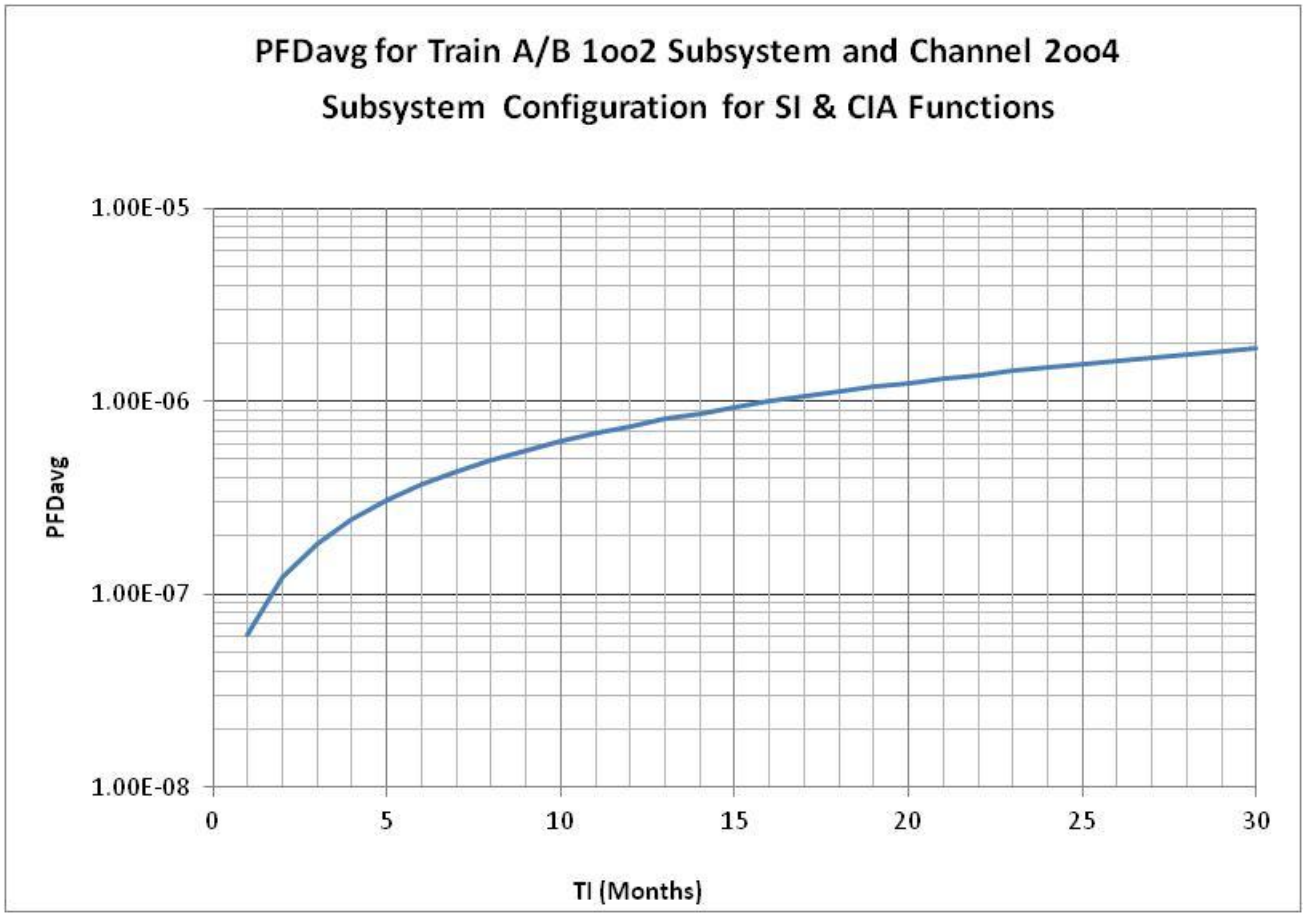


Chart 1 - PFD_{avg} vs TI for Train and Channel Configuration for SI & CIA Function

3.0 Input and Design Criteria

3.1 Reactor Protection System Block Diagrams

The following block diagrams in Figures 3-1, represents the basic PLC configuration for circuits controlling engineered safety function actuation systems (ESFAS) with PLMs and Train A subsystem 1 and Train B subsystem 1 that perform ESFAS dual 1oo2 safety functions.

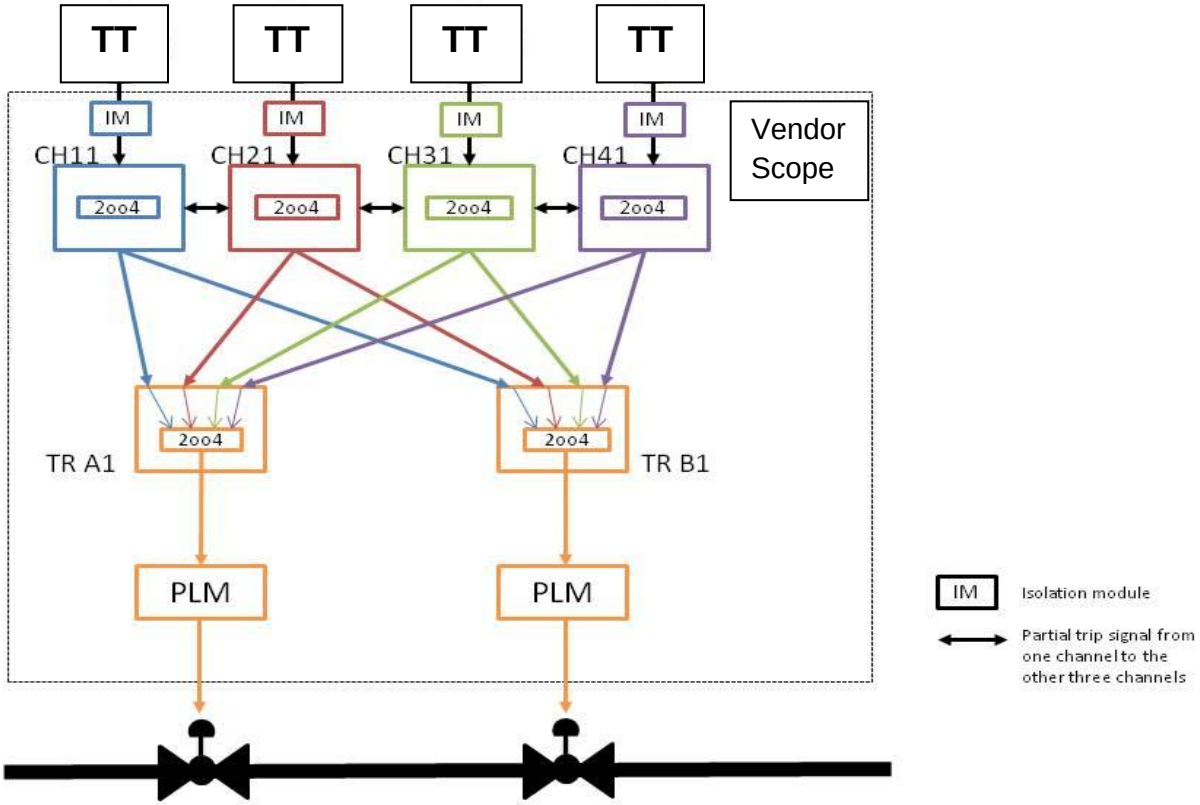


Figure 3-1 - Block diagram of the PLC for an ESFAS function using PLM outputs

3.2 PLC Component Failure Rates

Failure rates are calculated per MIL-HDBK-217F where available. Where not available, failure rates were computed using Bellcore Issue 6 database, parts count method (method I case 1), assuming nominal 40 degrees C junction temperature, 50% electrical stress, ground benign, controlled environment, quality class II. The “parts count” or “Black Box” method is very similar to and was modeled from the MIL-HDBK-217 standard. Although the Bellcore/Telcordia standard was originally developed for the telecommunications industry, it is also widely accepted in industrial and process automation as it is considered to match specific application conditions closer to those actually experienced than the MIL-HDBK-217 values. Typically the military standard has more conservative failure rates than Telcordia. However, depending on the actual device design Telcordia in certain cases gives the more conservative values.

Failure Mode and Effect Analysis quantified the Diagnostic Coverage and the Safe Failure Fraction in accordance with IEC 61508-6 Annex C.

Typical

Typical

Typical

Typical

MODULE FAILURE RATES

	Total Failure Rate	Fraction Safe Failures	Safe Failure Rate	Diagnostic Coverage Safe	Safe Detected Failure Rate	Safe Undetected Failure Rate	Dangerous Failure Rate	Diagnostic Coverage Dangerous	Dangerous Detected Failure Rate	Dangerous Undetected Failure Rate
Main Processor	1.5688	0.652	1.0223	0.989	1.0112	0.011082	0.5466	0.985	0.5386	0.008025
Digital Input Module Leg (32pt)	1.2461	0.500	0.6231	0.990	0.6168	0.006231	0.6231	0.990	0.6168	0.006231
Digital Input Common Processing (32pt)	0.4813	0.500	0.2407	0.990	0.2383	0.002407	0.2407	0.990	0.2383	0.002407
Digital Input Circuit (32pt)	0.0239	0.500	0.0120	0.990	0.0118	0.000120	0.0120	0.990	0.0118	0.000120
High Density Digital Input Module Leg (64pt)	1.4669	0.562	0.8242	0.990	0.8160	0.008242	0.6427	0.990	0.6362	0.006427
HD Digital Input Common Processing (64pt)	0.8980	0.601	0.5398	0.990	0.5344	0.005398	0.3582	0.990	0.3546	0.003582
HD Digital Input Circuit (64pt)	0.0089	0.500	0.0044	0.990	0.0044	0.000044	0.0044	0.990	0.0044	0.000044
NG Diff. Analog Input Module Leg (32pt)	4.2363	0.500	2.1182	0.967	2.0485	0.069640	2.1182	0.967	2.0485	0.069640
NG Diff. Analog Input Common Processing (32pt)	2.4229	0.500	1.2115	0.950	1.1509	0.060573	1.2115	0.950	1.1509	0.060573
NG Diff. Analog Input Circuit (32pt)	0.0567	0.500	0.0283	0.990	0.0281	0.000283	0.0283	0.990	0.0281	0.000283
NG High Density Analog Input Module Leg (64pt)	4.4107	0.559	2.4649	0.990	2.4403	0.024649	1.9458	0.990	1.9263	0.019458
NG HD Analog Input Common Processing (64pt)	2.5675	0.601	1.5433	0.990	1.5279	0.015433	1.0242	0.990	1.0139	0.010242
NG HD Analog Input Circuit (64pt)	0.0288	0.500	0.0144	0.990	0.0143	0.000144	0.0144	0.990	0.0143	0.000144
IAI/TC Module Leg (16pt)	2.8459	0.500	1.4229	0.974	1.3863	0.036586	1.4229	0.974	1.3863	0.036586
IAI/TC Common Processing (16pt)	1.1179	0.500	0.5589	0.950	0.5310	0.027946	0.5589	0.950	0.5310	0.027946
IAI/TC Circuit (16pt)	0.1080	0.500	0.0540	0.990	0.0535	0.000540	0.0540	0.990	0.0535	0.000540
NG 24 VDC DO Module Leg (32pt)	2.7236	0.500	1.3618	0.990	1.3482	0.013618	1.3618	0.990	1.3482	0.013618
NG 24 VDC DO Common Processing (32pt)	1.8703	0.500	0.9352	0.990	0.9258	0.009351	0.9352	0.990	0.9258	0.009351
NG 24VDC DO Switch (32pt)	0.0200	0.500	0.0100	0.990	0.0099	0.000100	0.0100	0.990	0.0099	0.000100
115 VAC DO Module Leg (16pt)	1.3535	0.500	0.6767	0.990	0.6700	0.006767	0.6767	0.990	0.6700	0.006767
115 VAC DO Common Processing (16pt)	0.4297	0.500	0.2149	0.990	0.2127	0.002149	0.2149	0.990	0.2127	0.002149
115 VAC DO Switch (16pt)	0.0433	0.500	0.0217	0.990	0.0214	0.000217	0.0217	0.990	0.0214	0.000217
Analog Output Common Processing (8pt)	1.3309	0.500	0.6654	0.990	0.6588	0.006654	0.6654	0.990	0.6588	0.006654
Power Supplies	0.5000	1.000	0.5000	1.000	0.5000	0.000000	0.0000	1.000	0.0000	0.000000
Pulse Input Module Leg (8pt)	1.8178	0.500	0.9089	0.968	0.8794	0.029479	0.9089	0.968	0.8794	0.029479
Pulse Input Common Processing (8pt)	1.0195	0.500	0.5097	0.950	0.4843	0.025487	0.5097	0.950	0.4843	0.025487
Pulse Input Circuit (8pt)	0.0998	0.500	0.0499	0.990	0.0494	0.000499	0.0499	0.990	0.0494	0.000499

Note: 1) Total failure rates were computed using Bellcore Issue 6 failure rate data. All failure rates are in failures per million hours.

2) The diagnostic coverages were derived from Annex C in IEC 61508-6.

Table 1- PLC Version 10.5 Module Failure Rates

3.3 Common Cause β factors

These factors are applied in accordance with the IEC 61508-6 Annex D for quantifying the effect of hardware-related common cause failures.

3.4 Typical Temperature Transmitter Failure Rates

A typical digital temperature transmitter has a mean time between failure of 71.2 years in accordance with Reference 7.4.18. The dangerous undetected failure rate is estimated to be 50% of the total failure rate, based on past vendor experience and methods approved by Technischer Überwachungs-Verein (TÜV). (TÜV, or *Technical Inspection Association* in English, is composed of German companies who validate the safety of various types of products.) This typical temperature transmitter (TT) is combined with its associated sensor for the calculation of total PFD_{avg}. The typical TT PFD_{avg} calculation should also take into account the sensor redundancy. Chart 2 shows the typical TT PFD_{avg} vs. TI for Triple Sensor configurations.

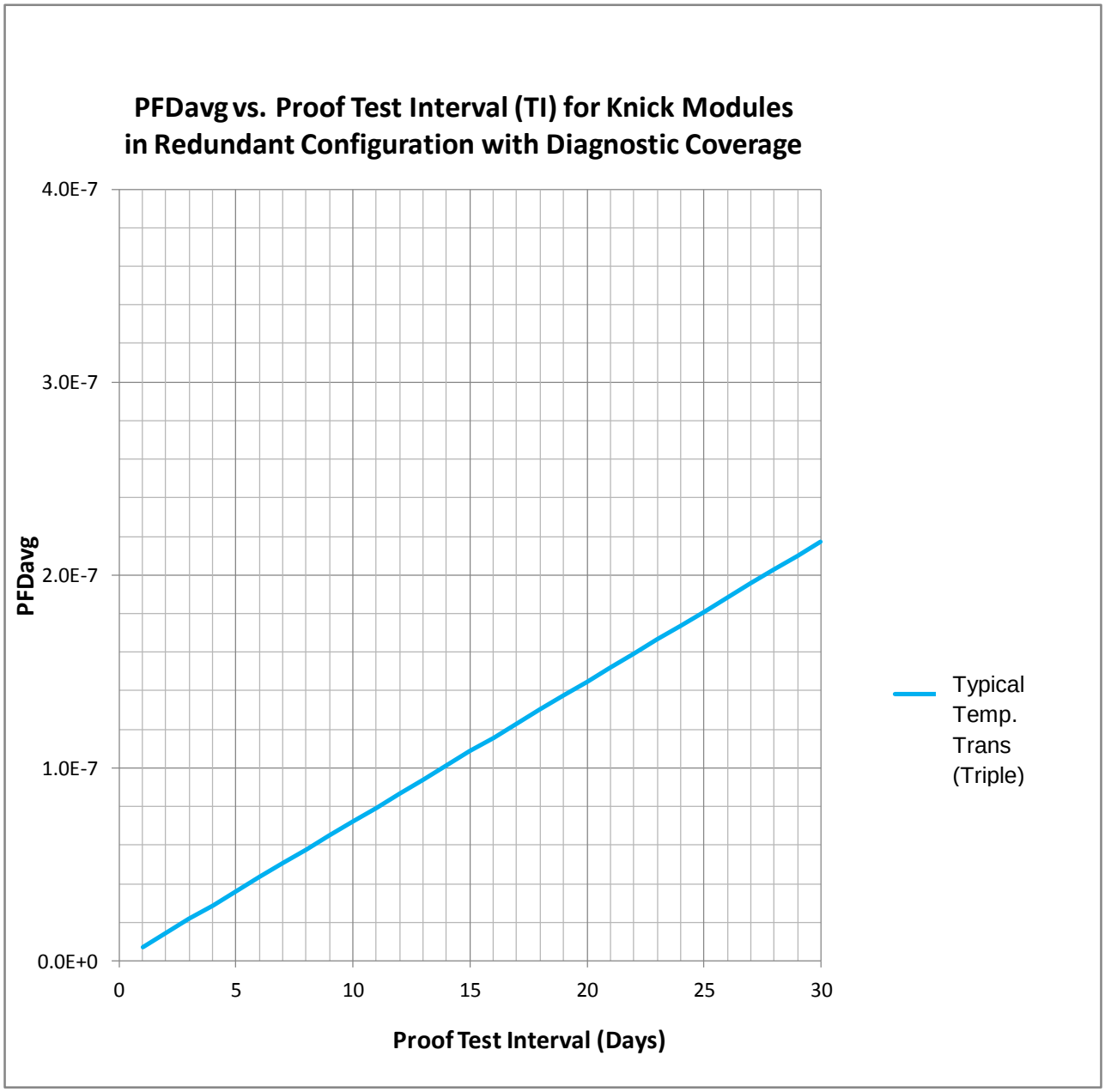


Chart 2 - PFDavg vs. Proof Test Interval (TI) for Triple Knicks

3.7 Acronyms and Symbols

The following is a list of the various acronyms used in this document:

AI	– Analog Input
AO	– Analog Output
Avg	– Average
BOM	– Bill of Material
CCF	– Common Cause Failure
CIA	– Containment Isolation Phase A
DD	– Dangerous Detected
DI	– Digital Input
DO	– Digital Output
DU	– Dangerous Undetected
FMEA	– Failure Modes and Effects Analysis
FPH	– Failures per Hour
FPMH	– Failures per Million Hours
IEC	– International Electrotechnical Commission
IEEE	– Institute of Electrical and Electronics Engineers
ESFAS	– Engineered Safety Features Actuation Systems
I/O	– Input/Output
IOC	– I/O Communication
MooN	– M out of N Architecture (i.e. 2oo4)
MP	– Main Processor
MTBF	– Mean Time between Failures
MTTF	– Mean Time to Failure
$MTTF_{spurious}$	– Mean Time to Fail Spurious
MTTR	– Mean Time to Repair
$MTTR_{ol}$	– Mean Time to Repair-On Line
PFD	– Probability of Failure on Demand
PFD_{avg}	– Average Probability of Failure on Demand
RO	– Relay Output
RPS	– Reactor Protection Systems
RT	– Reactor Trip
RTB	– Reactor Trip Breaker
RTS	– Reactor Trip System
SI	– Safety Injection
SD	– Safe Detected
SU	– Safe Undetected
SFF	– Safe Failure Fraction
SIF	– Safety Instrumented Function
SIS	– Safety Instrumented System
SIL	– Safety Integrity Level
TI	– Periodic Offline Test or Proof Test Interval
TMR	– Triple Modular Redundant
TÜV	– Technischer Überwachungs-Verein

3.8 Definitions of Key Terminology

3.8.1 Availability

Availability is the characteristic of an item expressed by the probability that it will be operational at a randomly selected future instant in time. This metric assumes unplanned down time associated with a component failure and average MTTR only. It does not take into account planned down time such as: preventive maintenance activities, planned upgrades, and planned down-time.

3.8.2 Average Probability of Failure on Demand (PFD_{avg})

The PFD_{avg} is the average probability of failure on demand for an individual SIF (Safety Instrumented Function) for the defined Test Interval. IEC 61508 / IEC 61511 and ANSI S-84.01 require that the SIL (Safety Integrity Level) calculation for each individual SIF include the PFD_{avg} of the Logic Solver. Typically, a SIF will comprise of approximately 3 to 8 I/O points, and the PLC Logic Solver will be shared by several SIF. By using the I/O for the most complex SIF (worst case), the PFD_{avg} value obtained for the Logic Solver can conservatively be used for each individual SIF. The PFD_{avg} obtained is an appropriate value to be used in the QRA (Quantitative Risk Assessment) validation process of the SIL for each independent SIF. Note that the calculation of PFD_{avg} is conservative for all SIF architectures. As a result, the calculation for MooN can be more conservative than the calculation for 1oo1. (MooN refers to a voted M out of N SIF architecture, as defined in IEC61508. 1oo1 refers to single-channel SIS architecture.)

3.8.3 Common Cause Failure

A failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure.

3.8.4 Dangerous Failure

A failure which has the potential to put the safety instrumented system in a hazardous or fail-to-function state.

3.8.5 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.

3.8.6 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.

3.8.7 Dangerous Systematic Failure

An error that results in a dangerous failure that originates during specification, design, implementation, commissioning or maintenance actions. This failure exhibits a non random pattern of failures that exist at a discrete time 0 and remain failed throughout the full mission time of the SIS.

3.8.8 Detected

In relation to hardware failures and software faults, detected by the diagnostic tests or through normal operation. This does not include hardware failures and software faults identified during proof testing.

3.8.9 Diagnostic Coverage

The percentage of the total failure rate of the component or subsystem that is detected by built in diagnostic tests. Diagnostic coverage does not include any faults detected by proof tests.

3.8.10 Fault

An abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.

3.8.11 MooN

A safety instrumented system, or part thereof, made up of “N” independent channels, which are so connected, that “M” channels are sufficient to perform the safety instrumented function.

3.8.12 Mean Time between Failure (MTBF)

The Mean Time between Failures is the average time between successive failures of a system which can be repaired or restored through the replacement of a failed component. This differs from MTTF (Mean time to Failure) in which the system/component repair/restoration time (MTTR) is not a consideration.

3.8.13 Mean Time to Fail Spurious ($MTTF_{spurious}$)

The $MTTF_{spurious}$ relates to the nuisance or spurious trip rate of the SIS (Safety Instrumented System). All the “Safety Critical” I/O modules are included in the $MTTF_{spurious}$ section of the spreadsheet. Enunciator points and other I/O that will not trip the process automatically are not included. Power supplies are considered in the $MTTF_{spurious}$ calculation of de-energize to trip safety systems, as a false trip can occur if the power fails. By considering the total number of chassis', we account for the dual logic power supplies. Field power supply failures are accounted for separately when the calculations are done for the whole SIF including field elements (this is not part of the logic solver reliability calculations). The MARKOV model based reliability calculation tool developed by PLC vendor and reviewed by TÜV provides the PFDavg and the $MTTF_{spurious}$ calculations for the Logic Solver, including the three Main Processors, the Logic Power Supplies, all the chassis and all the conventional TMR safety related I/O modules. The Mean Time to Fail Spurious is the average time between successive events triggered by detected faults in a safety instrumented system.

3.8.14 Mean Time to Repair (MTTR)

The Mean Time to Repair is that time required on average to detect a failed component within the system and complete those actions necessary to restore full system function. The times listed assume:

- Repair by replacement.
- Availability of at least one on site spare for each listed component.

MTTR includes the time necessary to diagnose the fault, stabilize the system prior to component swap out as well as the time to bring the system back on line to full functionality. In cases where a system or subsystem is comprised of multiple components, the MTTR for the system or subsystem will be comprised of the worst case MTTR of the components comprising the system or subsystem.

3.8.15 Proof Test

A test performed to reveal undetected faults in a safety instrumented system so that, if necessary, the system can be restored to its designed functionality. Note: Also known as Periodic Offline Test.

3.8.16 Probability of Failure on Demand (PFD)

The probability that safety instrumented system is in a functional state in the event of a process demand necessitating a transition to a safe-state.

3.8.17 Probability of Failure on Demand (PFD) Analysis

PFD analysis techniques employ systematic methodologies that decompose a complex system into its basic components. The performance and interactions of these basic components are combined into reliability models (such as simplified equations, fault trees and Markov models) to determine the overall system safety availability.

3.8.18 Redundancy

The use of multiple elements or systems to perform the same function; redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy).

3.8.19 Safe Failure

A failure which does not have the potential to put the safety instrumented system in a hazardous or fail-to-function state.

3.8.20 Safe Detected Failure

A detected failure which does not have the potential to put the safety instrumented system in a hazardous or fail-to-function state. Safe detected failures do not include hardware failures and software faults identified during proof testing.

3.8.21 Safe Undetected Failure

An undetected failure which does not have the potential to put the safety instrumented system in a hazardous or fail-to-function state.

3.8.22 Safety Integrity

Safety integrity is defined as “The probability of a Safety Instrumented Function satisfactorily performing the required safety functions under all stated conditions within a stated period of time.” Safety integrity consists of two elements: 1) hardware safety integrity and 2) systematic safety integrity. Hardware safety integrity can usually be estimated by modeling the component failure rates and the associated architecture (1oo1, 1oo2 etc). The result of this analysis yields a resulting PFD value which can be contrasted with the target (or specified) failure measure. Systematic safety integrity is difficult to quantify due to the diversity of potential causes of failure. Systematic failures may be introduced during the specification, design, implementation, operational and modification phases and may impact hardware as well as software.

3.8.23 Spurious Failure

The definition is the same as a safe failure. A failure which does not have the potential to put the safety instrumented system in a hazardous or fail-to-function state.

3.8.24 Undetected

In relation to hardware and software faults not found by the diagnostic tests or during normal operation.

4.0 Assumptions

4.1 Overall System Assumptions

The analysis assumes:

- The Isolators and temperature transmitters are part of the sensor subsystem and are not included in the logic solver reliability analysis. They are included in the analysis of the portion of the sensor string provided by the vendor in Section 3.
- The PLMs are part of the final element subsystem and are not included in the logic solver reliability analysis.
- The PLCs being evaluated are designed, installed and maintained in accordance with ANSI/ISA-84.01-1996
- Component failure and repair rates are assumed to be constant over the life of the component.
- Once a component has failed in one of the possible failure modes it cannot fail again in one of the remaining failure modes. It can only fail again after it has been repaired.
- The analysis assumes the same independent failure rates for identical redundant components
- The logic solver failure rate included input modules, logic solver, output modules and PLC power supplies.
- The Proof Test Interval (TI) is assumed to be shorter than the Mean Time to Failure (MTTF).
- Proof testing and repair of components (e.g...Replacement of modules) in the system are assumed to return the system to a perfect or “as new” condition.
- All PLC components have been properly specified based on the process application.
- All power supply failures are assumed to be in the de-energized state.
- All Failure rates will be per 10^6 hours unless otherwise specified.
- Field power supplies are not included in the reliability analysis.

4.2 Mean Time between Failure (MTBF) Assumptions

The analysis assumes:

- Failures are independent of each other
- Failures occur randomly at a constant rate over time.
- Repairs/replacements return the system to a “good as new” condition
- 35C max ground benign environment (unless otherwise noted)
- Component failure rates as listed in the Telcordia standard unless otherwise specified. These failure rates are assumed to be conservative relative to failure data from returns to Vendor.
- Wiring, interconnects, nests, racks and similar components are not considered in this analysis because their failure rate is much lower than the components on the modules.
- The typical Temperature Transmitter (TT) MTBF estimates are addressed in Section 7.4.

4.3 Mean Time to Repair (MTTR) Assumptions

The analysis assumes:

- Repair by replacement.
- Personnel will be available to repair all failures within 4 hours.
- Availability of at least one module on site as spare for each module type. Additional modules may be required if they have a high failure rate and/or the time to replace used spares is significant.

- MTTR includes the time necessary to diagnose the fault, stabilize the system prior to component swap out as well as the time to bring the system back on line to full functionality.
- In cases where a system or subsystem is comprised of multiple components, the MTTR for the system or subsystem will be comprised of the worst case MTTR of the components comprising the system or subsystem
- Since the MTTR = 4 hours, the reliability analysis assumes the detected failures being repaired can be ignored.

4.5 Train PLC Reliability Assumptions

The assumptions used to calculate the reliability for the Train PLC configurations are:

- The TI is 13, 140 - hours (18 months).
- The Mean Time to Repair - Online (MTTRot) is 4 hours.
- The Most Significant Safety Instrumented Function used for the Fail-to-Function calculations requires 4 DI modules and 6 DO modules representing the Safety Injection (SI) and Containment Isolation Phase A (CIA) functions from typical Loop Sheet in reference 7.2.5 and the vendor terminations listings.
- The Fail - Safe Calculations assume all I/O modules are used for safety functions.
- The common cause Beta factors are Beta_2oo3 = 1.5% for the individual PLCs.
- Common cause factors are also applied to the redundant Train 1oo2 configurations.
- The Train A Server and Train B Server PLCs are not included in the analysis since they are not safety critical.

5.0 Method of Analysis

5.1 Overview of PFDavg Methodology

IEC 61508 (Reference 10) and IEEE-352 (Reference 16) describes methodologies for PFDavg calculations. The following steps are performed in this analysis utilizing PLC spreadsheets similar to Spreadsheet 1 in this analysis.

1) Select the most significant safety instrumented function for the configuration using system documentation (Logic Diagrams, I/O Listings and simplified block diagrams).

2) Select the spreadsheet for the PLC configuration (1oo2, 2oo3, 2oo4, etc.). Develop new spreadsheets for special cases (For example Dual 2oo3 PLC configuration).

3) Enter I/O module information, proof test interval and mean time to repair into each spreadsheet.

In accordance with the referenced methodology (IEEE-352 and IEC-61508), the reliability values for sensor string values (Isolation Module and Knick Transmitter) are to be combined with the sensors (provided by client) 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 represented in Figures 3-1, including the relays and PLM are to be 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 a safety function.

6.0 Reliability Calculations

The reliability calculations for the worst case ESFAS function as per the methodology described in Section 5.

Typical

Typical

Typical

Typical

CONTROLLER - PFDavg & PFH CALCULATION

NUCLEAR POWER PLANT UNITS 1 & 2 (Train A Subsystem 1)

CONFIGURATION DATA (Most Significant Safety Instrumented Function)

Number of 32 point Digital Input Modules (nsf)	4	Mean Time to Repair- Online (MTTRot)	4	Hours
Number of Digital Input Points per Module (ndipts)	0			
Number of 64 point HD Digital Input Modules (nhdsf)	0			
Number of HD Digital Input Points per Module (nhddipts)	0			
Number of 32 point Diff. Analog Input Modules (nasf)	0			
Number of Diff. Analog Input Points per Module (ndaipts)	0			
Number of 64 point HD Analog Input Modules (nahdsf)	0			
Number of HD Analog Input Points per Module (nhdaipts)	0			
Number of 16 point IAMTC Modules (niaisf)	0	Periodic Offline Test Interval (TI)	13140	Hours
Number of IAMTC Points per Module (niaipts)	0			
Number of 32 point 24 VDC Digital Output Modules (msf)	6			
Number of 24 VDC Digital Output Points per Module (ndopts)	0			
Number of 16 point 115 VAC Digital Output Modules (mhvsf)	0	Common Cause - Beta Factor (Beta)	1.5%	
Number of 115 VAC Digital Output Points per Module (nhvdopts)	0			
Number of 8 point Analog Output Modules (maosf)	0			
Number of 8 point Pulse Input Modules (npsf)	0			
Number of Pulse Input Points per Module (npipts)	0			

Typical

FAIL - TO - FUNCTION

PFDavg	5.994E-05
Safety Availability	99.9940%

Spreadsheet 1 ESFAS PLC Train A Subsystem 1 - Fail-to-Function

7.0 References

The following are referenced within this document or were used to develop this document:

7.1 DCS Contract

1. Typical NNP DCS System Contract

7.2 DCS Design Information

2. Typical Nuclear Power Plant Project
3. Typical PLC Configuration by System.
4. Typical Loop Drawings XXXXXXXXXX-DI-0000
5. Typical System Manual RPR Reactor Protection System Chapter 6.2 Logic Diagram Not used

7.3 Reliability Methodology

6. Telcordia (Bellcore) TR-NWT-000332, Issue 6 December 1997, "Reliability Prediction Procedure for electronic equipment."
7. Relex version 7.7 for calculation of component data
8. IEC 61513 - 2001, "Nuclear Power Plants-Instrumentation and Control for Systems Important to Safety-General Requirements for Systems."
9. IEC 61508, 2009, "Functional safety of electrical/electronic/programmable electronic safety-related systems" Parts 1 through 6.
10. MIL-HDBK-217F, "Reliability Prediction of Electronic Equipment, Method I case 1 (parts count) to generate failure rate.
11. ANSI S84.01-1996 “Application of Safety Instrumented Systems for the Process Industries”
12. ANSI/ISA TR84.00.02-2002 “Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques Part 2: "Determining the SIL of a SIF via Simplified Equations”.
13. Modern 2oo4 processing architecture for safety systems, Prof. Dr-Ing.Habil.Josef Borcsok,Hima, Bruhl, Germany
14. IEEE Standard No.762 “Definitions for Use in Reporting Electric Generating Unit Reliability, Availability and Productivity.
15. IEEE Standard352-1987,IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems.
16. IEEE Standard 577-2004, IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities

7.4 Vendor component specifications and reliability data

17. E-mail / Quotation-- Request, Reliability values for Typical digital temperature transmitter which includes the following:
    - Failure rate/ mean time between failures:
    - MTBF: 623,333 h MTBF:
    - 71.2 years Failures in time:1604 FIT
    - Conditions: stationary operation in well-kept rooms, average ambient temperature 40°C, no ventilation, continuous operation.

8.0 Conclusion/Discussion

The reliability analysis for the scope of supply in this typical nuclear plant has been performed and documented in this calculation based on the Input and Design Criteria in Section 3, the assumptions in Section 4, the Method of Analysis in Section 5 and the References in Section 7. The results are documented in Section 2, Summary of Results and in Section 3, Input and Design Criteria, for each component analyzed in the vendor scope of supply.

The PLC subsystems represented in Section, have been analyzed for both the worst case configuration and the results are shown in Section 2, Tables 1. The reliability analysis calculations show that the redundant Reactor Trip Subsystems can attain the requested unavailability of 5.99×10^{-5} (from Spreadsheet 1) for off-line proof testing of 18 months for the logic solver portion. The Temperature Transmitter of interest in this analysis has a PFD_{avg} of 1×10^{-7} associated with a proof test interval of 14 days, as interpolated in Chart 2. With the use of online monitoring, the actual proof test or surveillance interval can be credited in as low as a few minutes using built in diagnostics to compare the signals from the triple redundant Knick temperature transmitters.. Therefore the 1×10^{-7} value for PDF_{avg} is highly conservative.

In accordance with the referenced methodology (IEEE-352 and IEC-61508), the reliability values for sensor string values (Isolation Module and Temperature Transmitter) are to be combined with the sensors (provided by client) 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 represented in Figures 3-1, including the relays and PLM are to be 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 a safety function.

As a result, the summation of the individual elements of PFD_{avg} for both the logic solver and the Temperature Transmitter is as follows:

$$PFD_{AVG\text{-}TOTAL} = PFD_{AVG\text{-}LOGIC\ SOLVER} + PFD_{AVG\text{-}TEMPERATURE\ TRANSMITTER}$$

$$PFD_{AVG\text{-}TOTAL} = 5.99 \times 10^{-5} + 1 \times 10^{-7} = 6.00 \times 10^{-5}$$

In accordance with the referenced methodology (IEEE-352 and IEC-61508), the reliability values for sensor string values (Isolation Module and Temperature Transmitter) are to be combined with the sensors (provided by client) 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 represented in Figures 3-1, including the relays and PLM are to be 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 a safety function.