INL/EXT-12-27215

Digital Technology Qualification Task 2 – Sustainability of Digital Alternatives to Analog Sensors and Actuators

Ted Quinn
Jerry Mauck
Ken Thomas

September 2012

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

INL/EXT-12-27215

Digital Technology Qualification Task 2 – Suitability of Digital Alternatives to Analog Sensors and Actuators

Ted Quinn, Jerry Mauck; 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

Executive Summary

The next generation reactors in the United States (U.S.) are an opportunity for vendors to build new reactor technology with advanced Instrumentation and Control Systems (control rooms, distributed control systems, etc.). The advances made in the development of many current generation operating reactors in other parts of the world are being used in the design and construction of new plants. These new plants are expected to have fully integrated digital control rooms, computerized procedures, integrated surveillance testing with on-line monitoring and a major effort toward improving the operations and maintenance (O&M) and fault survivability of the overall systems. In addition the designs are also incorporating major improvements in the man-machine interface based on lessons learned in nuclear and other industries.

Digital technology is available or emerging that can eliminate dependence on such legacy analog devices, with their attendant inaccuracies, limited reliability, and maintenance burdens. However, the nuclear industry has been slow to adopt these improved technologies due to lack of familiarity, licensing risk, and diversity concerns for safety significant applications. Without a resolution of this deficiency in the qualification basis for digital technologies, new plants and advanced designs may be constrained to continue reliance on legacy technologies for sensors and actuators rather than employ fully digital I&C systems.

The recommendations presented in this report will be used as input to I&C research programming for the implementation of lessons learned during the early phases of new build both for large light water reactors (LWR) and also small modular reactors (SMR). This report is intended to support current research plans and provide user (vendor, owner-operator) input to the optimization of these research plans.

Acknowledgement

We would like to thanks the following staff of NSSS and instrument vendors who participated in the data survey:

Steve Seaman - Westinghouse
Mike Dougherty - Fisher Rosemount
Rich Miller - GE-Hitachi
Brian Arnholt - MPower
Chris Doyel - AREVA
Michael Miller - Duke Energy (Retired)/Consultant Sargent & Lundy

Acronyms

ABWR	Advanced Boiling Water Reactor
ACRS	Advisory Committee on Reactor Safeguards
ALS	Advanced Logic System
AMSAC	Anticipated Transient without Scram Mitigating System Actuation Circuitry
ATWS	Anticipated Transient without Scram
BOP	Balance of Plant
BTP	Branch Technical Position
CFR	Code of Federal Regulations
CIM	Component Interface Module
COT	Channel Operational Test
D3	Defense-in-Depth and Diversity
DAS	Diverse Actuation System
DCD	Design Certification Document
DCS	Distributed Control System
EMI	Electro-Magnetic Interference
EPR	European Pressurized Reactor
EPRI	Electric Power Research Institute
ESBWR	Economic Simplified Boiling Water Reactor
ESFAS	Engineered Safety Features Actuation Systems
FAT	Factory Acceptance Test
FFB	Foundation Field Bus
FPGA	Field Programmable Gate Array
GE	General Electric
GEH	General Electric Hitachi
HART	Highway Addressable Remote Transducer
HICB	Instrumentation and Control Systems Branch
HMI	Human Machine Interface
I&C	Instrumentation and Control
INL	Idaho National Laboratory
INPO	Institute of Nuclear Power Operation
I/O	Input/Output
ISG	Interim Staff Guidance
LAR	License Amendment Report
LWR	Light Water Reactor
mA	Milli-amps
MESH	Invensys Switched Ethernet Network
MWe	Mega-Watts electric
NAS	National Academy of Science
NEI	Nuclear Energy Institute
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam System Supplier
O&M	Operations and Maintenance
PLC	Programmable Logic Controller
PG&E	Pacific Gas and Electric
PPS	Plant Protection System
PRA	Probabilistic Risk Assessment
PROFIBUS	Process Field Bus

PWR	Pressurized Water Reactor
QA	Quality Assurance
R&D	Research and Development
RFI	Radio Frequency Interference
RPS	Reactor Protection System
RTD	Resistor Temperature Detector
RTIS	Reactor Trip Isolation System
SBWR	Simplified Boiling Water Reactor
SMR	Small Modular Reactor
SRP	Standard Review Plan
SSLC	Safety System Logic Controller
STP	South Texas Project
SWCCF	Software Common Cause Failure
TVA	Tennessee Valley Authority
US	United States
VDU	Visual Display Unit

TABLE OF CONTENTS

List of Figures

List of Tables

1. Introduction

The purpose of this report is to identify legacy analog sensor and actuator technologies that are being incorporated in new plant designs and will likely result in unnecessary inaccuracies or excessive maintenance demands based on operating plant experience. Digital technology is available or emerging that can eliminate dependence on such legacy analog devices, with their attendant inaccuracies, limited reliability, and maintenance burdens. However, the nuclear industry has been slow to adopt these improved technologies due to lack of familiarity, licensing risk, and diversity concerns for safety significant applications. Without a resolution of this deficiency in the qualification basis for digital technologies, new plants and advanced designs may be constrained to continue reliance on legacy technologies for sensors and actuators rather than employ fully digital I&C systems.

For both operating plant modernization efforts and new plant designs, the focus in the instrumentation and control area has been in the implementation of digital platforms to be used as signal conditioners, bistables and logic devices by replacing them, albeit at a slow pace, with digital based programmable logic controllers (PLCs) adapted with digital communication networks. However, there appears to be very limited use of digital based smart sensors and actuators. There has been occasional use of smart sensors and communication networks involving sensors and actuators for non-safety systems. Presently the opportunity to replace the existing analog based sensors and actuators designs has not been acted on for the most part for both operating and new plant designs.

Perpetuation of these legacy technologies into new plant designs will preclude the benefits of modern digital technologies in control and protection applications, including higher availability, reliability, repeatability, accuracy and improved time response. Digital controls are not as susceptible to the inherent problems of analog designs such as signal attenuation, setpoint drift, and sub-component failure. These benefits would result in more accurate control of plant systems and improved safety margins for protection systems.

Legacy analog I&C technologies also require more maintenance and testing than their modern digital counterparts. Because of setpoint drift, these activities occur much more frequently and involve more components for an equivalent digital control loop. Troubleshooting to find a defective component is much more difficult than with digital components that have on-board diagnostic and communication capability.

The first phase of this research involves determining what sensor and actuator technologies are being incorporated into new plant designs and reactor concepts. It also identifies the equipment that results in unnecessary inaccuracies or excessive maintenance demands based on operating plant experience. Based on the initial findings, future work in this project will explore the problems associated with these legacy analog technologies and propose digital alternatives that meet the availability, reliability, and qualification requirements of safety-significant nuclear power plant (NPP) I&C systems

2. Hybrid Designs – Analog and Digital

As noted earlier, new plant designs are incorporating digital control and protection systems for the logic processing portion of these systems. However, by continuing to rely on analog sensor and actuator technology, the reliability and maintainability of the total systems is inferior to end-to-end digital systems. In other words, the modern digital systems are sandwiched between analog sensors and actuators, which dominate the overall reliability and performance of the systems.

Figure 1 below shows an example of a safety system function in the Engineered Safety Features Actuation System (ESFAS) on a new plant design (figure courtesy of Invensys Corporation), utilizing digital technology as the logic solver, but employing analog technology for the sensors and output actuators performing the required safety function.

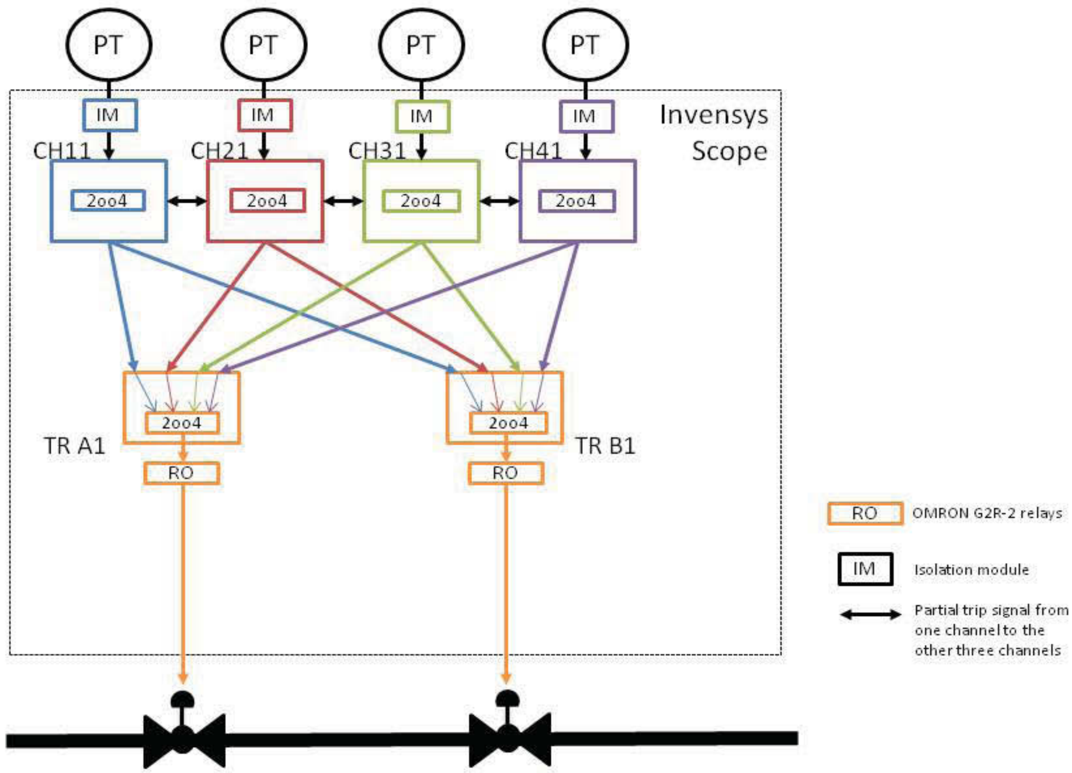

Figure 1 Safety System Architecture Utilizing Digital and Analog Technology

This figure clearly illustrates a hybrid design of both analog and digital technology in a given plant protection function. Hybrid designs are also typical of control systems. In fact, suppliers of digital control and protection systems make it easy to interface analog sensing and actuation circuits to their processing functions. This takes a variety of forms that are discussed in this report.

Figure 2 provides a more detailed example of a hybrid control function. In this case, the only digital portion of the function is the control logic processor, shown as the digital control system. This diagram is representative of a typical PLC digital design, using a flow transmitter (FT) as a feedback signal to throttle a control valve. Analog instruments and transmitters are used on the sensing side of the control function, converting some physical force to an electrical signal, with a 4-20 mA current loop running on twisted-pair copper conductors as the means of accurately transmitting the signal from the field process location to the control logic processor.

A similar arrangement is used on the output (actuator) side of the control function. A demand value is generated by the control logic processor as a digital output and is then converted to an analog electrical signal, which is in turn supplied to another 4-20 mA current loop to transport it to the field location. Depending on the type of actuator, this electrical signal in the current loop is usually converted to some other form of signal. For control valves, this is typically pneumatic control, using instrument air as the motive force. Figure 2 is greatly simplified in this regard, but the electrical signal is converted to a pneumatic signal (E/P controller) to produce an equivalent air pressure (typically 3 – 15 psi), which in turn is used to position the control valve with the air pressure acting against a calibrated spring pressure in the valve operator. For some types of large control valves, such as steam turbine driven feedwater pumps, the motive force is hydraulic oil pressure rather than air pressure.

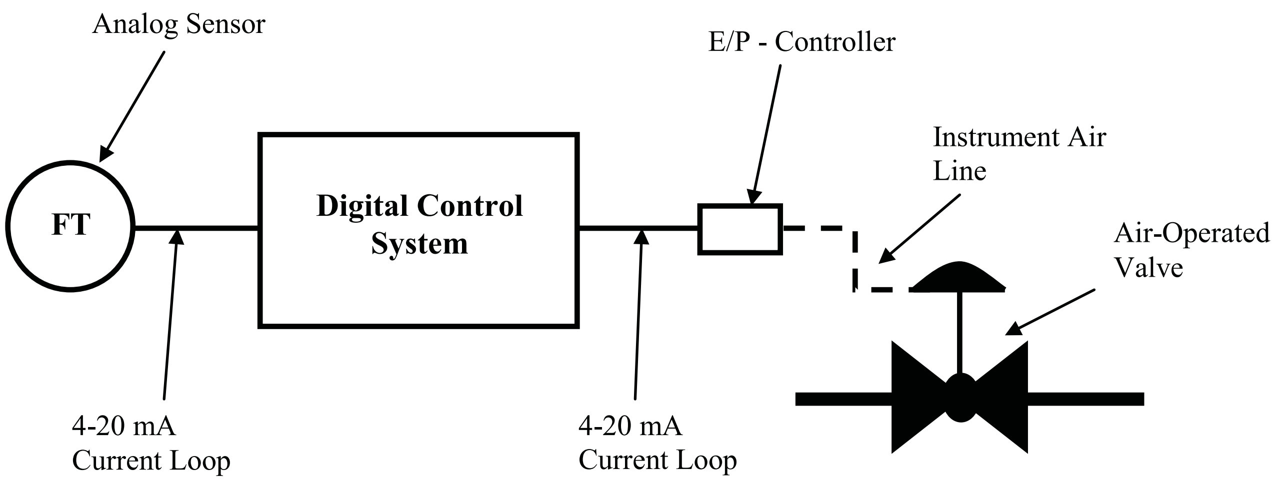

Figure 2 Example of a Hybrid Control Function, Using Digital and Analog Components

The inherent drawback of such a hybrid design is that the overall accuracy and repeatability of the control function is dominated by the more imprecise analog components, essentially negating the benefit of having a digital control system. Unlike the digital portion of the control scheme, the analog components are subject to a variety of factors that degrade their accuracy. One such factor is a deadband in electromechanical components where a certain amount of force is needed to overcome the friction in the device. Other factors include line losses, conversion inaccuracies, hysteresis, leakage (air or oil losses), set point drift, and environmental impacts (e.g. temperature. A digital signal is not subject to these factors to an appreciable degree.

Continue reliance on these analog components imposes a significant performance penalty on control functions as compared to end-to-end digital designs. There are also much greater maintenance burdens with these legacy analog technologies. Therefore, it is highly desirable for new plant designs to have qualified digital options for these components in order to achieve much-improved control performance at a lower on-going maintenance and testing cost.

3. Why Analog Technology Is Being Deployed in New Plant Designs

New plant designs such as the AP1000, European Pressurized Reactor (EPR), APR1400, Advanced Boiling Water Reactor (ABWR), Economic Simplified Boiling Water Reactor (ESBWR) and others including the new modular reactors are, for the most part, implementing legacy sensors and actuators in the new plant designs. While not surprising for actuators, it is thought that sensors would be more advanced, using the latest smart sensor technology. The use of legacy sensors and actuators are known to be easier to license and their use is quite familiar to plant designers and plant operators. This approach may prove to be shortsighted in that it will result in performance penalties and additional maintenance burden being placed on the plant operators in the long run. This could also cause a necessary redesign as analog technology further declines in the marketplace.

3.1 Licensing Risk

With the benefits of digital I&C systems, there are associated risks. A number of issues have been identified related to the use of digital computer-based equipment in safety systems as follows:

- Potential for common cause failure due to software errors
- Use and control of the tools used for configuring computer-based systems
- Sensitivity to environment Electro Magnetic Interference/Radio Frequency Interference (EMI/RFI)
- Potential for unexpected behavior
- Commercial grade dedication concerns
- Cost and difficulty of managing and maintaining software
- Documentation requirements are onerous due to difficulty in proving high quality for safety software
- Cyber security concerns

For the regulator, digital systems present a number of challenges. The most difficult issue to resolve is the use of common software in redundant trains of safety-related equipment and the resulting potential for a common cause failure due to a software fault. While there has been considerable focus on the large integrated control and protection systems, the issue of common cause failure affecting a large number of digital sensors and actuators has not been fully vetted.

The NRC position as stated in BTP 7-19, Defense-in-Depth and Diversity (D3), is required to be followed and met by licensees and vendors and implies that it is only applied to digital systems/equipment located in the Reactor Protection System, those given credit in the Chapter 15 Safety Analysis. The guidance in BTP 7-19 makes it somewhat difficult to implement digital based technology in either the sensors or the actuators for certain plant safety functions. Providing digital based sensors and actuators for safety injection and certain neutron flux parameters could require providing diverse sensors and actuators to overcome the software common cause failure (SWCCF) concern. This adds complexity and cost to I&C designs which is contrary to stated plant design goals.

To further complicate this scenario, it is not clear at this time to what degree SWCCF analysis is required for non-safety related systems. It is clear that some determination of susceptibility to SWCCF must be included in license applications and 10 CFR 50.59 reviews. This is in addition to demonstrations of software quality by providing to the NRC software documentation as listed in NRC Interim Staff Guidance (ISG-06), which is quite burdensome.

Recent precedents of the licensing effort for the Oconee digital Reactor Protection System (RPS), Wolf Creek Field Programmable Gate Array (FPGA) for feedwater isolation, and others have somewhat chilled the industry's appetite for digital projects that need regulatory approval. This has had something of a carryover effect into the new plant licensing efforts albeit not for the digital based control and protection systems. The licensing procedure for new plants (Part 52) was predicated on the idea that licensing would be relatively short and predictable (originally thought to be about 42 months). Given the new concepts that were introduced in the overall reactor and safety designs (e.g. passive plants), it is evident that plant designers were not willing to risk additional schedule delays or technical design issues based on emerging I&C technologies for sensors and actuators.

The primary issues associated with using digital equipment licensing in safety-related I&C systems include the following:

- Common mode failure by software: Failure of similar or identical software running on identical hardware in multiple trains of redundant instrumentation.
- Due to the increased complexity of computer system tasks, it is difficult to verify freedom from programming error and assure correct task performance under all possible circumstances.
- Computers normally take advantage of standard tools such as their operating systems or compilers, both during on-line operation and during development; it is virtually impossible to get such tools error free.
- Sensitivity of digital based systems to plant environments: EMI/RFI, temperature, power quality, grounding
- Affect on safety margins by processing time
- Affect on reliability through input considerations;
- Loss of a processor can affect multiple channels

Because of the lack of Appendix B suppliers for advanced sensors and actuators, the commercial dedication of hardware and software will be required which is required for the use of hardware and software that has not received prior approval by the NRC staff for use in safety-related nuclear power plant applications.

Qualification testing for these sensors and actuators is another area of concern due to the potential harsh environment exposure for these technologies, although the normal practice is to locate any digital equipment in a mild and protected environment. This regulatory uncertainty is one of the causes for preventing the application of smart, digital based sensors and actuators in both operating and new plants.

In 1995, the NRC Advisory Committee on Reactor Safeguards (ACRS) requested the National Academy of Science (NAS) to perform an evaluation of the licensing and implementation of digital systems in nuclear plants in the U.S. The resultant report is *Digital Instrumentation and Control Systems in Nuclear Power Plants*, issued 1997 (Reference 9.3).

In this report, the following key technical issues were identified with recommendations for improvements in the regulatory process to provide more guidance on the process for approving digital upgrades in each of the technical areas:

- Systems aspects of digital technology
- Software quality assurance
- Common-mode software failure potential

- Safety and reliability assessment methods
- Human factors and human machine interface
- Dedication of off-the-shelf hardware and software

In 1997 and again in 2007, the NRC updated the Standard Review Plan – NUREG 0800 (Reference 9.5) Chapter 7 and associated Branch Technical Positions (BTP's) and Regulatory Guides to provide more guidance to NRC reviewers and licensees on regulatory requirements for digital safety systems. Recently, cyber security concerns have entered the licensing arena. The use of smart sensors and actuators will be required to follow and adhere to all relevant cyber security requirements.

In a related licensing issue, plant designers have opted not to pursue some potential Technical Specification improvements enabled by the use of digital systems including the potential use smart sensors and actuators. Rather, they have left it to the plant owners to apply for these after the plants are licensed and operating. There is some merit to the approach here in that the plants need to establish an operating reliability record on which to base the relaxation in Technical Specifications. However, it is clear that the primary motivation is to avoid undertaking additional licensing or design risks caused by implementing new sensor and actuator technologies.

3.2 Familiarity

Overall, there is a high degree of familiarity and comfort factor with the existing systems and actuators in operating plants due to the long history of performing both periodic surveillance testing and corrective maintenance. With digital upgrades, depending on the level of support provided by the I&C supplier, there may be a lack of on-site experience in troubleshooting, problem recognition, and assimilation of systems into the plant. There is a concern that technicians might introduce adverse effects during maintenance due to lack of training and experience. There is a need to acquaint plant operators with the performance and maintenance advantages of the advanced sensor and actuator technologies to achieve a full appreciation of how these new devices can improve overall plant performance.

Complexity is another issue for digital systems. While interfacing digital control systems with digital sensors and actuators presents many new opportunities due to the greatly expanded amount of available information, this in itself creates design complexity. In addition, these advanced sensors and actuators also have microprocessors, albeit fairly simple ones. However, a "simple" microprocessor-based system may have software with 100,000 or more lines of code. A microprocessor chip may have more than 5 million gates. Microprocessor support chips are equally complex.

3.3 Diversity

Diversity is a major concern for utilities installing digital systems for operating plants and new plants. While this is a licensing concern as previously discussed, it is foremost a nuclear safety issue for the plant operators. There must be a reasonable assurance that safety-related plant systems and components will perform their design basis functions. Having a diverse set of components contributes to this assurance by avoiding a common origin of component defects and performance problems.

Although diversity is mostly concerned with software common cause failure concern, it addresses other critical safety and operational issues, such as the operability of redundant components when problems are found or when a Part 21 notification (component qualification issue) is received from a supplier. This can result in an immediate regulatory shutdown due to both safety trains being inoperable. Other issues include impairment of redundant or backup safety functions due to design misapplications and errors, hardware common cause failures, and maintenance-induced equipment faults.

4. Overview of I&C Design for New Plants

The new plant designs utilize fully integrated DCS architecture as advances over the designs implemented in the first generation of U.S. nuclear power plants. Table 1 provides an overview of the platforms selected by the vendor for the major designs being licensed and built in the U.S. and, in some cases, around the world. The ABWR is being built in Taiwan (Lungmen). The EPR is being built in Finland (Okiluoto), France (Flammaville), and China. The AP1000 is being built in China (Sanman) and the US (Vogtle and V.C. Summer).

Interviews were conducted with knowledgeable representatives of the following new plant designers to gain insights into how they are incorporating digital technologies into the information, control, and protection systems; and where they are continuing to use analog technologies to minimize the concerns and risks discussed in Section 3.

4.1 Westinghouse AP1000

As an overview, there is a large effort underway to provide digital systems in the part of the loop between the sensors and the actuators. Also, such items as power distributions are now being installed with digital properties. The Common Q and Ovation were discussed as the Westinghouse digital devices to be installed in safety systems and non-safety systems respectively.

Also, the Applied Logic System (ALS) Field Programmable Gate Arrays (FPGAs) are being installed in the Diverse Actuation System (DAS) and Component Interface Module (CIM) for the AP1000. Currently there are two operating plants with the ALS either installed (Wolf Creek) and to be installed (Diablo Canyon). All of these digital platforms have their own communication networks which are up-to-date and meet the USNRC regulations.

To a large degree, sensors and actuators will remain based on analog technology, especially in safety-related applications.

4.2 General Electric ABWR and ESBWR

For the Toshiba ABWR, the Reactor Trip and Isolation System (RTIS) and the Neutron Monitoring Systems are non-rewritable FPGA based systems. These FPGA devices are configurable logic devices that process digital signals in a deterministic manner. These FPGAs provide the logic and control functions for the Reactor Trip System. The RTIS contains four redundant divisions of digital trip functions. The trip decision from each division is used as an input to the trip logic function module. These trip decisions are passed to other divisions through isolated communication links. The logic format is fail safe. The neutron monitoring system has input directly to the trip logic functions. The trip coincident logic is input to the output logic units which are devices that provide a diverse interface for several manual functions.

The Engineered Safety Features Platform is implemented with a microprocessor based platform. This digital platform provides the control and interface function for automatic actuation, control and display for the Engineered Safety Features System. This system contains four redundant divisions with one division of sensors being capable of a manual bypass. A CIM module provides priority logic to override control when an ESF actuation occurs.

Likewise, the control system is also microprocessor based but diverse from the Engineered Safety System digital platform. The diverse actuation system provided by Toshiba should meet the NRC diversity guidance and requirements. There appears to be no use of digital-based sensors in the safety systems for the ABWR at South Texas Plant (STP) 3&4. In addition, no examples of advanced actuation devices were provided.

In discussions with General Electric Hitachi (GEH) representatives, outside of the conventional digital DCS implementation, very little use of "smart" technologies are anticipated due to licensing concerns, including the ever growing evaluations for cyber security. The one exception is in the use of digital breaker controls for switchgear which are being used in the design now. This use of analog applies both to the sensor and actuator ends of the loops.

4.3 AREVA EPR

The EPR is being built in Finland, France and China with different regulatory regimes and, as a result, different DCS designs in the fully integrated digital control rooms that are state-of-the-art. The regulatory burden, including increasing scrutiny on cyber-sensitive elements, was given as the reason why smart sensors and the associated networks are not utilized in the new EPR designs. Because of the similarity to earlier LWR designs, no new sensor technologies are required to support the safety and non-safety system design.

Similarly, the actuators are not being changed from earlier plant designs based on proven and available technology. New plants are still employing the older type radiation monitoring systems that require vacuum pumps, blowers, or movable filter media for gaining radiation information. New sensors and wireless networks are being designed for the environmental monitoring systems, including the Chemical and Radiological Data System for the EPR.

4.4 MPower SMR

MPower is designing their Small Modular Reactor(SMR) to meet utility and NRC requirements for new deployment in the US in the coming years. Their design process is in the development of the Design Certification Document (DCD) at the time of this report. No smart transmitters or communication networks are included in the sensor string for safety systems due to the licensing risk, including increasing scrutiny of the cyber security of these installations. On the balance-of-plant side, consideration of communication networks for actuator technology, including ROTORK smart actuators, are being considered for implementation based on reducing operation and maintenance expense over the lifetime of the plant. These smart actuators can implement specific valve curves in software and through advanced diagnostics, correct for valve wear.

For SMR implementation, MPower recommended consideration of advanced research and development for in-vessel sensors for flow and level that could be implemented in the future in a fully integrated enclosed design such as MPower (all primary pumps and components within the reactor vessel).

5. Analog Sensor Technologies for New Plants

Each of the new plant designers indicated that there remains widespread usage of analog technology in the new designs, especially in safety-related applications where there are more stringent requirements in licensing, environmental qualification, and component performance history for reliability considerations.

5.1 General Discussion of Analog Sensors and Circuit Devices

The following is a discussion of the most common analog technologies that will be employed in new designs, with a brief discussion of their drawbacks. To avoid unintended implications for the companies supplying information to the project, these analog technologies that will be discussed in general and not directly associated with a specific new plant design.

It should be noted that due to the proprietary nature of detailed control schemes in the new plant designs, it is not possible to confirm every type of analog device that is to be deployed. In many cases, it is not yet known what specific devices will be used in the various plant control functions in that the detailed designs have not been completed. Therefore, the discussion below is based on both confirmed and likely implementations of analog components as indicated by either the lack of fully-qualified digital options or the general reluctance to use digital technology in high-risk or regulatory-sensitive applications (as discussed in Section 3). Use of any specific analog technology will be confirmed in later phases of this project work prior to becoming part of the scope to investigate digital alternatives.

Analog Instruments

Any process input is first captured as an analog value, representing some sensed parameter such as a pressure, temperature, position, etc. For measurements involving fluids and gases, there is typically an impulse line that runs from the process to the instrument. This is a source of inaccuracy depending on the length of the run (energy losses) and changes in the parameter along the run, such as temperature or density. These changes require some form of compensation. The instruments themselves have mechanical set points that are difficult to establish an exact setting and can drift over time. The sensed parameter must be converted to some form of energy that can be transmitted, typically an electrical signal.

The closer an instrument is to the sensed parameter source, the fewer inaccuracies are introduced. Sometimes significant distances are necessary, for instance, in the case of locating the instrument outside a high radiation field to comply with its environment qualification requirements. Sometimes the sensed parameter must be isolated from the instrument, as in the case of a contaminated (radioactive) fluid. These situations often use oil-filled capillary systems that transmit pressure signals through an isolated medium. Again, these interposing devices introduce inaccuracies.

Some instruments are indirect measures of the desired parameter. For example, fluid flow is often measured as the differential pressure (dP) across an orifice that is in the flow path (pipe). The flow is proportional to the square root of the dP and so a square root extractor is used in series with the pressure transducer, introducing yet another inaccuracy. Neutron flux is another such indirect measure, measuring not the neutron count, but measuring a proportional current from the interaction of neutrons with gas molecules in a fission chamber. There is appreciable loss of accuracy in indirect measures. In these cases, it would be desirable to find a direct measure of the process parameter and convert it directly to a digital value.

Position sensors, such as linear voltage differential transformers (LVDTs), can be highly accurate as analog measurement devices, but are subject to the same inaccuracy factors in transmitting the position information back to control devices and control rooms.

Analog Transmitters

These devices are sometimes packaged with an instrument or can be separate devices. Transmitters are typically based on current and voltage loops. Current loops are usually 4-20 mA signals that are scaled to represent the lowest to highest range of the sensed parameter. At a minimum, they contain a transmitter, a power supply, and a receiving device that either displays the instrument value or uses it in a control or protection function. They are relatively accurate in that the current is forced to the desired value by a varying voltage source and therefore remains the same value over the entire loop regardless of the distance to the receiving device or the number of devices that are placed in the loop. However, they are hard to maintain within the specified accuracy band and require frequent maintenance.

Voltage loops are used in some short-distance applications, typically using a 0 – 10 VDC range that is scaled to the process values. Voltage loops are susceptible to voltage losses along the conductors and typically do not employ the use of a non-zero lowest value, to distinguish the range's lowest value from a circuit failure.

Electromechanical Relays

Electromechanical relays have long been a staple of hard-wired control logic based on analog components. This includes such logic functions as permissives, interlocks, seal-in circuits, contact multiplication, and voters (e.g. two-out-of-four logic). These devices typically consist of a solenoid coil that when energized, moves a plunger that either closes or opens contacts. There are electronic counterparts to the electromechanical relays that use electronic switches to accomplish similar logic functions.

While the use of PLCs and even the newer field programmable gate arrays (FPGAs) are overtaking the use of electromechanical relays in new plant designs, there is still some use of the legacy analog devices, especially in safety-related applications.

Other Circuit Devices

There is a large class of analog circuit devices that are still employed in control circuits and operator interfaces, including switches, gauges, chart recorders, status lights, potentiometers, timers, counters, filters, and isolators. These devices have both electromechanical and electronic equivalents. The problem is that, as discrete analog devices, they each represent a potential failure point, a loop accuracy factor, a circuit time-response delay, and a maintenance burden.

While many of these devices are being replaced with the digital control systems in the new plant designs, there are still pockets of usage for local plant control and indication functions outside the main control room and, in some cases, for diverse actuation systems.

5.2 Survey of Sensor Technologies for New Plant Designs

As a goal of this research effort, data on the deployment of advanced sensors and actuators is being evaluated. To obtain data on the current status in sensor technology in the new plant design process, interviews were conducted for a number of the reactor and instrument vendors as documented in the following sections.

The following table provides the results of interviews with Nuclear Steam System Suppliers (NSSS) and vendors of both safety and non-safety equipment for the sensor systems and components. The reference to analog related to sensing of the parameter and also to the output from the sensor which becomes the input to the DCS.

Design	Pressure	Level	Temp	Speed	Vibration	Voltage	Current
AP1000	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*
ESBWR	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Digital*	*Digital*
ABWR	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*
EPR	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*
MPower	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*
NuScale	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*

With just a couple of exceptions, analog technologies overwhelmingly dominate the deployment of sensor technologies in the new plant designs. It has also been confirmed that analog transmitters with 4 – 20 ma current loops are the most common means of communicating field inputs to the digital control systems, especially in safety-related applications. There is some use of digital transmitters in non-safety applications.

The obvious conclusion is that there is significant opportunity for performance improvement in control functions for the new plant designs, as well as reduced maintenance costs.

6. Analog Controller and Actuator Technologies for New Plants

From information supplied by new plant designers and I&C system suppliers, certain controllers and virtually all actuator applications will continue to relay on analog technologies in new plant designs. In the case of controllers, many of the traditional applications are now incorporated into the digital control systems, typically known as the distributed control system (DCS). However, discrete electrical controllers continue to be used in single loop applications for local control panels and diverse actuation systems. Also, pneumatic controllers are a necessary component for air-operated actuators.

For actuators, analog technologies remain in widespread usage. The most common types of analog actuators use instrument air or hydraulic oil as the motive force. Electromagnetic coils are also commonly used as analog positioners as found in solenoid operators. There are fewer qualified digital options for actuators and so the continued reliance on analog technologies is to be expected.

6.1 General Discussion of Analog Controllers and Actuators

Similar to the discussion of analog sensor technologies in Section 5, a general discussion of the most common analog controller and actuator technologies is presented along with a brief discussion of their drawbacks. Again, to avoid unintended implications for the companies supplying information to the project, these analog technologies that will be discussed in general and not directly associated with a specific new plant design.

PID Controllers

These are stand-alone feedback controllers that are commonly found in single loop applications. Using an analog electronic circuit, a feedback signal from the controlled process is compared to the setpoint to generate an error signal that is then subjected to three types of control actions – proportional, integral, and derivative – that are then summed to correct the process deviation in an optimum manner. Specifically, these control actions are tuned to find the optimum controller response that balances timely correction with control system overshoot and settling time as a function of damped oscillation.

PID controllers are difficult to tune in an optimum manner and employ a variety of compensation mechanisms to counteract certain inherent effects of the physical circuit effects (e.g. using a deadband to reduce component wear due to excessive signal correction, using setpoint ramping to avoid integral windup). These devices require frequent maintenance to stay properly tuned and are subject to component failure.

Pneumatic Controllers

Pneumatic controllers are used to supply the necessary air pressure to correctly position air operated components. For this reason, they are sometimes referred to as positioners. They are analog devices that create a demand signal (typically in the range of 3 – 15 psi) to a component operator, such as an air-operated valve or an air-operated damper. This air demand signal is proportional to an electrical control signal (typically a 4-20 mA current loop signal) that is supplied from the control system through an electro-pneumatic (E/P) converter.

Pneumatic controllers require highly-pure compressed air as a source. Filters and regulators are inserted in the air supply upstream of the controllers for this purpose. Also, for safety-related applications, three-way air solenoid valves (one each for both safety trains) are placed between the output of the controller and the air-operated device, so that the air supply can be quickly dumped such that the component will fail to its safe position. All of these devices together make for a complex and troublesome configuration to provide control to a single plant component.

Pneumatic controllers require frequent calibration and are subject to a variety of failure mechanisms, including internal parts wear, air leakage, and internal binding due to the build-up of contaminants (e.g. moisture, oil) in the air supply. Due to the failure rates of these devices, redundant controllers are sometimes used in critical valve applications, such as feedwater regulation valves.

Air-Operated Valves and Dampers

These types of operators for components use a controlled air pressure acting against a diaphragm to counteract a calibrated spring pressure to correctly position a component, moving either a valve stem or damper piston/arm assembly.

Control is difficult because air is a compressible fluid affecting the precision in the air pressure. These operators tend to overshoot because they must build up enough force to overcome the friction in the stem or piston, which must be sufficiently stiff to keep the process fluid from moving it. In addition, there is a delay time depending on the length of tubing from the controller to the operator. PID controllers are typically needed to provide precise control and are they difficult to tune in these applications. When tuning is not correct, air-operated valve have a tendency to "hunt", meaning they constantly moving which affects the flow feedback and keeps the control circuit in constant change.

Air-Operated Valves and Dampers are high maintenance components to keep all of these parts working and in calibration. They are very prone to air leaks, particularly around the fittings and the valve diaphragm, which tends to become brittle over time.

Hydraulic Oil Actuators

These types of actuators are used in high-force and high-precision applications, using oil as the force medium because it is non-compressible. A typical application is a steam turbine governor valve. Like their air-operated counterparts, they require a variety of associated components such as oil reservoirs, filters, high pressure pumps, relief valves, pipes/hoses, and fittings.

These actuators also require frequent maintenance involving oil leaks, pump seals and bearings, and oil contaminants (such as water). Maintenance and calibration of these actuators is complex and labor intensive, particularly with regard to the internal parts of the actuator.

Solenoid Valves

Solenoid valves are electromechanical devices that use a solenoid (electromagnetic coil) to act against a spring to open or shut valves. They are often used to control fluids in pneumatic or hydraulic systems. They control the valve to a full open or closed state, and cannot be used to throttle the process.

These devices are not complex from a maintenance standpoint, but they are prone to failures. They are often used in applications requiring frequent cycling and so internal parts, such as O-rings, tend to wear and leak.

Motor-Operated Valves

Motor-operated actuators are used in high-force applications typically where there will be full valve travel to the open and close position. One such application is isolation valves where it is critical that there be no leakage through the valve. In these cases, the valve travel is controlled by a torque switch that ensures a sufficient amount of operator torque has been applied to valve leakage across the valve seat. In other cases, valve travel is controlled by limit switches ensuring that a set amount of valve stem travel has occurred.

The most frequent maintenance problem with these types of operators is the set up of the analog limit switches and torque switches, including torque by-pass and overloads. These settings have a tendency to drift and impair valve performance. The performance of safety-critical valves is monitored from a regulatory standpoint under the NRC's Generic Letter 89-10.

6.2 Survey of Controller and Actuator Technologies for New Plant Designs

The following table provides the results of interviews with NSSS and vendors of both safety and non-safety equipment for the actuator (output of DCS) systems and components. The term analog refers to the output of the DCS communication to the actuator, motor, etc.

Design	Trip	Pressure	Speed	Valve Position	Start/Stop	Flow	Voltage/ Frequency
AP1000	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*
ESBWR	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Digital*
ABWR	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*
EPR	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*
MPower	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*
NuScale	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*	*Analog*

Again, it is evident that there are many opportunities to improve performance of these components where the use of analog devices contributes to inaccuracies, frequent failures, time-consuming trouble shooting, and excessive maintenance and testing requirements.

6.3 Maintenance and Reliability Issues for Actuator Support Systems

The reliability of analog sensors and actuators is dependent on complex, expensive, and hard-to-maintain support systems that present their own challenges in making these control functions reliable. A considerable amount of plant resource is dedicated to keeping these systems functional and available.

All of the air- operated devices depend on a clean, well-regulated source of instrument air to supply pneumatic logic and motive force requirements. A nuclear plant's instrument air system is a very complex set of components spread through all plant areas where air-operated components are located. This system consists of air intakes, compressors, filters, dryers, piping receiver tanks, and local accumulators. The multiple compressors operate in a piggy-back and stand-by arrangement to ensure that air pressure does not decrease below a minimum value upon loss of anyone compressor.

There is constant maintenance and testing on these components to keep them reliable. Filters and desiccant material for dryers have to be periodically replaced. The control systems for the compressors are complex and troublesome. The piping systems have to be periodically blown-down to remove moisture and other contaminants.

Loss of instrument air is one of the most difficult operational transients that can occur because all safety-related air-operated components fail to their safe position. This results in a reactor trip and a plant recovery with limited equipment availability. Because instrument air is not safety-related (and therefore is not supplied with emergency power), a loss-of-offsite power (LOOP) also causes a loss of instrument air.

In all, significant expense and reliability problems could be avoided if the nuclear plant by eliminating dependence on instrument air for the control of safety-critical components. Safety margins would also be improved due to the availability of these components during LOOP and loss-of-instrument-air transients. This is a promising area to move from analog to digital technology.

Likewise, hydraulic oil presents its own set of problems. It must be clean and free of contaminants. This usually means that oil purification systems have to be maintained that consist of pumps, filters, cyclone moisture separators, etc. These components are maintenance intensive. For example, moisture separators have to be disassembled and cleaned on a frequent basis to keep sludge from building up in their parts. Again, this is an expensive, maintenance intensive set of components that have to be maintained solely for the purpose that certain analog actuators are enabled to operate correctly.

Hydraulic oil is both a fire and environmental hazard. Fire suppression systems have to be installed around significant oil sources, further adding to the array of plant components that support these analog control systems. The oil also has to be accounted for in the combustible loading for the plants Fire Hazard Analysis, which complicates the fire response plan and affects the fire zones that are used to segregate redundant plant functions.

In summary, the support systems contribute significantly to the cost and staffing workload of a nuclear plant to maintain high reliability and availability for these analog actuators. They negatively affect nuclear safety margin, fire protection, and environmental compliance. The necessity and requirements of these support systems should be a major factor in the consideration of whether to use modern digital technology in lieu of these legacy analog components.

7. Digital vs. Analog I&C – What Are the Advantages?

At the highest level, plant owners and operators have established high level goals for availability and reliability of the overall plant and operator interface to maintain cost-effective and safe operation. In order to accomplish these, improvements in the human machine interface as well as the reliability and availability of both human decision making and hardware/software need to be made. These include:

- Maximize plant capacity/output levels – per Nuclear Energy Institute (NEI) and Institute of Nuclear Power Operation (INPO) reports, in the range of 90% plant capacity for most of the U.S. plants. Reliability of equipment and risk of forced outages is a major factor
- Achieve and maintain high reliability --- both due to online monitoring and built in redundancy of equipment in newer systems – unlike their older counterparts
- Achieve and maintain high availability --- similarly benefit from internal redundancy that digital systems can provide – higher fault tolerance
- Maintain high levels of safety –primary goal of the nuclear safety culture --- with increased levels of scrutiny toward Probabilistic Risk Assessment (PRA) and requirement failure based decisions on replacement and upgrade philosophy. Newer systems also have automatic adjustment for drift or drift free for higher confidence in the accuracy over the operating cycle
- Maintain high levels of operator awareness of plant and equipment states --- more information on both operations and diagnostics and prognostics are available with more intelligent automation
- Minimize the likelihood of human errors thru higher level of input to the decision making in the man-machine interface
- Integrate fault tolerance and fault recovery into systems(from both human and equipment errors/failures) – latest systems are much better than analog in the ability to ride thru or recover from faults
- Use commercially available products--- thru the Electric Power Research Institute (EPRI) programs we have benefited greatly from the overall qualification and supply chain improvements coming into nuclear

- Reduce O&M Costs – Challenge is in the transition and the training of the workforce to match the new systems. Some like Hart, PROFIBUS – are more complex – but also handle faults better when properly configured.

7.1 Inherent Disadvantages of Analog Sensors

Analog sensor degradation is more difficult to determine when compared to the degradation of advanced sensors. Currently, sensor degradation is detected by performing channel checks or removal of the sensor for calibration. Channel checks are only a comparison of the four sensor channels sensing the parameter and do not directly indicate the sensor is problematic unless a significant change has occurred in the sensor output. The technician would have to perform an analysis of the readings to make a determination of sensor degradation. Advanced sensors have the capability to provided intelligent output of information regarding its operational capability.

Calibrating analog sensor is a labor intensive process that can become quite complex for certain types of sensors and can require extensive testing equipment. Often plant shutdowns are required to carry out this process. However, with analog sensors this is the only means for validating a sensor's output and based on analog sensor reliability information, it should be checked and calibrated on a frequent basis. On the other hand, advanced sensors can often be calibrated in-situ by taking advantage of the on-board digital technologies offered by these advanced sensors. By calibrating in-place and on-line, the disadvantages cited above can be eliminated.

Obsolescence is an issue that for the moment is more of a concern for the sensor manufacturers than the utilities. The manufacturers continually upgrade their workforce including the sensor designers. They will use the latest techniques to design sensors including digital technology. The direct effect of this is to freeze the development for the analog sensors such that no improvement will be gained for these designs. In other words, the analog sensors manufactured today and in the future will be of the same design as manufactured in the past. Plant maintenance personnel are also changing over time and eventually will consist of personnel that are not familiar with analog sensor design and performance techniques. This will lead to longer lead times for calibrations and repairs. Reliability will become more of an issue due to the skill levels for both manufacturers and utility personnel. This will have a negative impact on maintenance cost, training cost, and obsolescence.

Setpoint issues such as accuracy and repeatability have not changed since the early implementation of the analog sensors. The analog sensor technology has remained the same over a large number of years. Because of this, setpoint derivations have largely remained the same without any improvement. It is believed that the sensor accuracy is a major portion of the conservatism within the setpoints. By implementing advanced sensors, setpoints could be brought closer to the process safety limits by using the advanced sensor accuracy and reliability numbers. A major result of this is that the setpoint will be further from the process and movement towards it will cause less frequent channel trips. This creates less maintenance concerns and better plant economics.

Analog sensors require the transmission of their signals through analog means such as copper cabling. The signals are normally 4 to 20 mA and are converted to a voltage level or digital reading at the channel processor. By replacing these analog sensors with smart sensors, communication networking becomes readily available since the advanced sensor signals are digital at the output of the sensor process and can be transmitted over fiber optic cabling rather than copper.

Fault tolerance is a beneficial characteristic gained by using advanced sensor technology. Personnel are able to determine the fault approach and the advanced sensor has the ability to make a digital decision on alleviating the fault. The benefits of fault tolerance technology become quite apparent and consist of less maintenance requirements, anticipation of failures well in advance of the actual failure, and corrections by changing to an alternate in-situ advanced sensor that is on standby.

7.2 Inherent Disadvantages of Analog Actuators

Analog (legacy) actuators were designed decades ago and the design has not evolved significantly since their inception. There are a number of reasons for this as discussed in other sections of this report. Their evolution into smart or digital actuators has not been nearly as rapid or complete as the modernization of the remaining portions of the instrument loop. Some disadvantages associated with the implementation and use of legacy actuators are as follows:

- Obsolete technology- availability of new analog actuators and spare parts limited
- Documentation inadequacies
- No diagnostic capabilities-wear monitoring and fatigue monitoring is not available
- Increased O&M costs due to aging
- Decreased reliability due to aging
- Stand alone maintenance concerns
- Ability of maintenance personnel to maintain legacy actuators
- Network use is limited-analog data transmission with cables and connectors
- Power Sources-large both in capacity and size.

7.3 Improved Performance with Digital

Most existing instrumentation and control systems in nuclear power plants are based on discrete component analog electronics and relay technologies (See Figure 3). These systems were developed in the 1960's and 1970's and have become difficult and costly to maintain. In many cases, the original manufacturers are no longer in business or have dropped their 10 Code of Federal Regulations (CFR) 50 Appendix B Quality Assurance (QA) programs due to lack of business and the high cost of maintaining the programs. The challenges applicable to analog systems include:

- Analog systems are experiencing excessive drift because of aging
- Vendors are discontinuing analog product lines
- Difficulty in obtaining product support for existing analog systems

Digital technology has been widely used in commercial and industrial applications for several decades, with decreasing use of traditional analog systems. The commercial applications require high reliability with requirements similar to the nuclear industry.

It is increasingly true that the only practical replacements for much of the older analog equipment, and for installations in new plants (See Figure 4), are based on digital technology, typically microprocessors. This is true for large, complex systems such as feedwater control or reactor protection systems and smaller stand alone devices such as meters and recorders.

As discussed in EPRI TR-102348, Rev. 1 (Reference 9.4), nuclear utilities are upgrading existing analog instrumentation and control (I&C) systems due to increasing problems with obsolescence, difficulty in obtaining replacement parts and increased maintenance costs. Obsolescence in itself does not drive the upgrade process. It can still be maintained through good maintenance and spare parts support. However, vendors will not support obsolete systems forever. As the supply of replacement parts decreases, maintenance costs increase and the older systems become more difficult to support. This support difficulty, combined with digital technology that offers performance and reliability improvements, creates a significant incentive to upgrade. Some of the improvements made possible with digital technology include:

- More reliable with the use of fault tolerance capabilities and the use of active spares.
- More stable, accurate without drift (improved operating margins)
- Better diagnostics and self-testing can lower maintenance and repair costs.
- Automated testing can reduce the burdens and risks during surveillance testing. Technical Specifications can be employed that are relaxed for testing intervals.
- Better performance
- Easier and more economical to change. Repairs usually consist of only replacing a module board or card from the spare parts supply.
- Improved Human Machine interface (HMI)
- Available and supported. Operating history for smart sensors and actuators are extensive and should be available from other industries such as chemical and oil.
- Some plants want to take advantage of digital system flexibility
- Monitoring and Diagnostics
- Reliability/Availability
- Fault Tolerance
- Greater accuracy-reduced margins-increased power output
- Reduced O&M costs.

In addition, in comparison with analog systems, digital systems provide expanded capabilities for:

- Process large data volumes
- Data validation techniques
- Extensive diagnostic capabilities
- Integrated diagnostic and predictive algorithms
- System based early fault detection
- Intelligent displays, e.g. alarm filtering
- Operations/maintenance/engineering advisory systems
- Automated processes
- Electronic procedures with information and control
- Multi-media capabilities.

By providing these benefits, and facilitating maintenance, modern digital systems offer the potential to provide greater system availability through the use of reliable digital components and features such as automatic self-testing, diagnostics and automatic calibration capability. New reactors are using digital I&C systems for the decision making process (logic solver) to the virtual exclusion of analog systems.

At the time of review and issue of NUREG-6842 (Reference 9.1), the review of sensor and actuator technologies documented the following:

> "For light water reactor technology, the evolutionary digital I&C designs have not revealed any new regulatory issues about safety class 1E sensor technology. However, significant research has been conducted toward improving sensor technology that will probably have application and be cost-effective in commercial nuclear power plants. In addition, new sensing systems, unique measurement parameters, and environmentally compatibility under more extreme conditions may be required to support other advanced reactor designs. As a result, a research program to support licensing of future plants should consider maintaining an ongoing awareness of such developments and determining the viability of such improvements to nuclear power plant applications."

7.4 Nuclear Industry Experience with All Digital Designs

7.4.1 Early Digital Upgrades

In the late 1980's, the US NRC recognized that digital systems were being installed in existing nuclear plants, and also recognized they were not well prepared to regulate digital systems with software. Regulatory guidance up to that time focused on earlier analog technology. By the early 1990's, utilities began to make changes under 10CFR50.59. In an early attempt to replace the Reactor Protection System (RPS), the DC Cook Digital RPS ran into trouble when the Factory Acceptance Test (FAT) failed due to requirement specification issues.

Later, the Zion plant attempted a Process Protection System (PPS) upgrade under 10CFR50.59, without prior NRC approval. During this review, the SWCCF issue was raised. Even though the replacement system "performed the identical function of the original system," Technical Specification changes were determined to be required due to the different manner in which the operations were performed. The Channel Operational Test (COT) was defined. The Tennessee Valley Authority (TVA) Sequoyah Plant upgraded the PPS process protection using the same platform as Zion. During this review, verification and validation became serious issues for NRC review.

In the mid 90's, the Pacific Gas and Electric (PG&E) Diablo Canyon plant upgraded the PPS with the same equipment as Sequoyah and Zion. Diablo Canyon had an Anticipated Transient Without Scram (ATWS) Mitigation System Actuation Circuitry (AMSAC) system built by the same manufacturer as the PPS. This raised the issue of diversity and defense in depth, which became "How diverse is diverse enough?" and eventually resulted in issue of NRC NUREG 0800, "Standard Review Plan," (SRP) (Reference 9.5) Branch Technical Position (BTP) HICB-19.

7.4.2 Fully Digital Designs

The advances made in the development of many current generation operating reactors in other parts of the world provided the basis for the next generation of instrumentation and control including fully integrated digital control rooms, like the N4 reactors in France and the Advanced Boiling Water Reactors (ABWR) in Japan. The national and international research community has been involved with research and development of advanced control and monitoring systems for nuclear power plants for many years. The international community, particularly in Europe, Japan and Korea, have developed and built integrated advanced control rooms. Now more recently, China and the U.S. have followed with new builds with advanced control rooms and fully integrated DCS designs as well. This move forward has been supported by research and development in automation of plant operations and advanced plant monitoring and diagnosis in the international community. The following summaries are provided for the

N4 and ABWR digital designs, as examples of fully digital designs within the overall plant architecture. Additionally, Reference 9.1 provides details on many other partial or full digital system implementations around the world.

N4 Series

In the late 1970's, the French nuclear power industry undertook the design of a very large (1,500 Mega Watts electric (MWe)) PWR with the N4 design. The N4 was the first to use the numerical integrated protection system (SPIN) technology, which was the most modern computer technology used in French safety systems at the time. The French also included a radical new design for the I&C and human-system interface. The main control room operator stations are compact cockpit-style, sit-down workstations that are entirely driven by digital computers. Graphical visual display units (VDUs) display process data, plant graphics, procedures, and alarms; touch screens provide the means of executing manual controls. The entire I&C architecture was, for the first time, based upon the use of digital computers, rather than analog hardware.

ABWRs

In 1978, General Electric (GE) began the conceptual design of a family of advanced light-water reactor plants that share a common technology base. They are the 1,300 MWe ABWR and 600 MWe Simplified Boiling Water Reactor (SBWR). The world's first ABWR, Kashiwazaki-Kariwa Unit 6, was completed in Japan by a consortium of Toshiba Corp., Hitachi Ltd., and GE. This was followed by Kashiwazaki-Kariwa Unit 7. The design of these two units is similar to ABWR designs certified by the NRC. Kashiwazaki-Kariwa Unit 6 began generating electricity in December, 1996 and Kashiwazaki-Kariwa Unit 7 began commercial operation in July, 1997.

The Kashiwazaki-Kariwa plant I&C systems use state-of-the-art digital and fiber optic technologies. The ABWR has four separate divisions of safety system logic and control (SSLC) including four redundant multiplexing networks to ensure plant safety. Separate control rooms and other panels house the SSLC equipment for controlling the various safety function actuation devices. The diverse I&C features are designed to provide protection against common-mode failures of the protection systems.

7.5 Experience of Other Industries

Digital technology has been widely used in commercial and industrial applications for several decades, with decreasing use of traditional analog systems. The commercial applications require high reliability with requirements similar to the nuclear industry. It is believed that the nuclear industry has shied away from advanced sensor and actuator applications because the licensing risk is viewed to be a greater negative than the advantages offered by their application in new plants. Training sessions for System designers would be beneficial to aid the plant and vendor personnel in making educated decisions regarding advanced technologies for sensors and actuators. These training sessions would include licensing and technical aspects for advanced sensors and actuators.

Unlike the nuclear industry, smart sensors and the associated communications protocols, have been widely used in the refinery, petrochemical and pharmaceutical industries, in new builds and plant upgrades that have been implemented in recent years. In at least one case, a non-nuclear power plant has installed Foundation Field Bus (FFB) technology with intelligent digital sensors. There are a number of communications protocols that support intelligent sensors including:

- Foundation Fieldbus (FFB) - the most complex architecture

- Highway Addressable Remote Transducer (HART) - which is the most stable and has been around the longest
- Process Field Bus (PROFIBUS)
- Device Net

For example, the FFB is a bi-directional, all digital communication bus designed for the integration of process measurement and control devices. The FFB provides all of the benefits of the traditional 4 to 20ma standard, while providing greater data access to both control and system health information. An example FFB network is shown in Figure 4.

The HART communications protocol and current design can support any mix of standard 4- 20 ma devices and HART devices. A pair of modules combines to provide redundancy at the Fieldbus module level.

The redundant PROFIBUS communications interface module provides an interface between the DCS and PROFIBUS slave devices including motor drives, I/O modules, and field I/O devices. A standard module, which can be used in a single or redundant configuration, supports two PROFIBUS links with a maximum of 125 slave devices per port when repeaters are utilized.

DeviceNet is a digital, multi-drop network linking scanners and I/O devices. Each device and scanner is a node on the network. DeviceNet systems can be configured to operate in a master-slave architecture. DeviceNet has power on the network, enabling devices with limited power requirements to be powered directly from the bus and simplifying building of the network.

The reasons these advanced architectures have been selected and deployed in these new installations include:

- Reduction in required cable runs and reduced wiring costs
- Improvements in accuracy through self-calibrating intelligent devices
- Asset management improvement through access to a wider selection of suppliers
- Easy access to device maintenance information

The reasons given for disadvantages for deployment of these new systems include increased design complexity and varied licensing issues.

7.5.1 Fisher-Rosemount Sensor Division

Fisher-Rosemount is a major supplier of qualified and commercial sensor products to the nuclear industry and has been involved in the NRC and industry working groups for codes and standards and digital system upgrades to nuclear plants. Rosemount has developed and deployed a smart sensor, the 3051 series, which is qualified for nuclear safety applications in a mild environment, with a HART communication protocol input to the DCS. Similarly, a division of Fisher-Rosemount (Topworx), has qualified a proximity switch for use in nuclear safety applications. The majority of applications Fisher-Rosemount is called to support for new reactor deployments, however, are in the 4-20 mA sensor lines, which have been offered for many years. Several years ago, the representative from Fisher-Rosemount stated that they did a survey of customer needs for Foundation Field Bus (FFB), HART, and other communication technologies that support smart sensors, and made a conscious business decision to continue focus on the supply of the existing 4-20 mA sensor designs, as what the majority of the customers wanted. Also, the number of inquiries into cyber security features and considerations for Fisher-Rosemount devices has increased according to the representative.

7.5.2 Invensys MESH Network and Communications Architecture

A representative of Invensys was interviewed who has worked in the Invensys Switched Ethernet Network (MESH) network and communications protocol design and development role for a long time, and provided significant information resources, which provides the basis for the input for communication networks. His experience also confirmed the customer preference for analog sensor networks for power plants, as a whole, while more advanced networks are commonly considered for the refinery, petrochemical and other advanced controls industries, which are served by Invensys.

8. Conclusions

The purpose of this report is to identify legacy sensors and actuators that are being used in new plant designs, and evaluate these legacy sensors and actuators. The next generation reactors in the U.S. are an opportunity for vendors to build new reactor technology with advanced Instrumentation and Control Systems (control rooms, DCS, etc.). The advances made in the development of many current generation operating reactors in other parts of the world are being used in the design and construction of new plants. These new plants are expected to have fully integrated digital control rooms, computerized procedures, integrated surveillance testing with on-line monitoring and a major effort toward improving the O&M and fault survivability of the overall systems.

However, to date, the new reactor designs have not taken advantage of implementing advanced sensors and actuators including advanced communication techniques for the transmission of data to and from these devices. There are a number of significant concerns with the use of the legacy analog and actuators that have been discussed and presented to the reader. Technology is available or emerging that could eliminate dependence on such legacy devices, with their obsolescence issues, attendant inaccuracies, limited reliability, and maintenance burdens. However, the nuclear industry has been slow to adopt these improved technologies due to concerns about the suitability, licensing complexity, or technical readiness for safety significant applications. Without a resolution of this deficiency in the qualification basis for advanced sensors and actuators, new plants and advanced design may be constrained to continue reliance on legacy technologies for sensors and actuators rather than employ fully digital I&C systems.

Obviously there are advantages (and disadvantages) to replacing these legacy devices with smart devices.

The question becomes one of “why has the implementation of smart sensors and actuators lagged the implementation of microprocessors and field programmable gate arrays for signal conditioning, bistables, and logic devices.

There are a number of reasons for this reluctance as discussed above. The major ones are non-familiarity with the smart sensor and actuator availability and another is the licensing concerns caused by the use of smart technology for the sensors and actuators as they are based on digital technology. However, it is believed that both of these concerns can be overcome by applying the proper training techniques and using the licensing approach taken for the application of digital based platforms in the I&C architecture.

Further research on this topic will explore in more depth the problems associated with the use of the legacy sensors and actuators in both operating and new plants. It will address the need to identify digital alternatives to analog sensors, local control loops, and actuators that meet the availability, reliability, and qualification requirements of safety-significant NPP I&C systems. In addition, it will identify candidate alternative digital sensors and actuators and evaluate their suitability in meeting the applicable qualification requirements.

9. References

9.1 US NRC NUREG/CR-6842, Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants, 2004

9.2 DOE-INL Technology Roadmap, "Instrumentation, Control, and Human-Machine Interface to Support DOE Advanced Nuclear Energy Program," March, 2007

9.3 National Academy of Sciences, "Digital Instrumentation and Control Systems in Nuclear Power Plants," issued 1997, at the request of NRC ACRS.

9.4 NEI-01-01, Guideline on Licensing Digital Upgrades, A Revision of EPRI TR-102348 to Reflect Changes In the 10 CFR 50.59Rule, July, 2001.

9.5 U.S. NRC NUREG-0800, Standard Review Plan, 1997 and 2007

9.6. IAEA TECDOC-952, Advanced Control Systems to improve Power Plant Reliability and Efficiency, July 1997

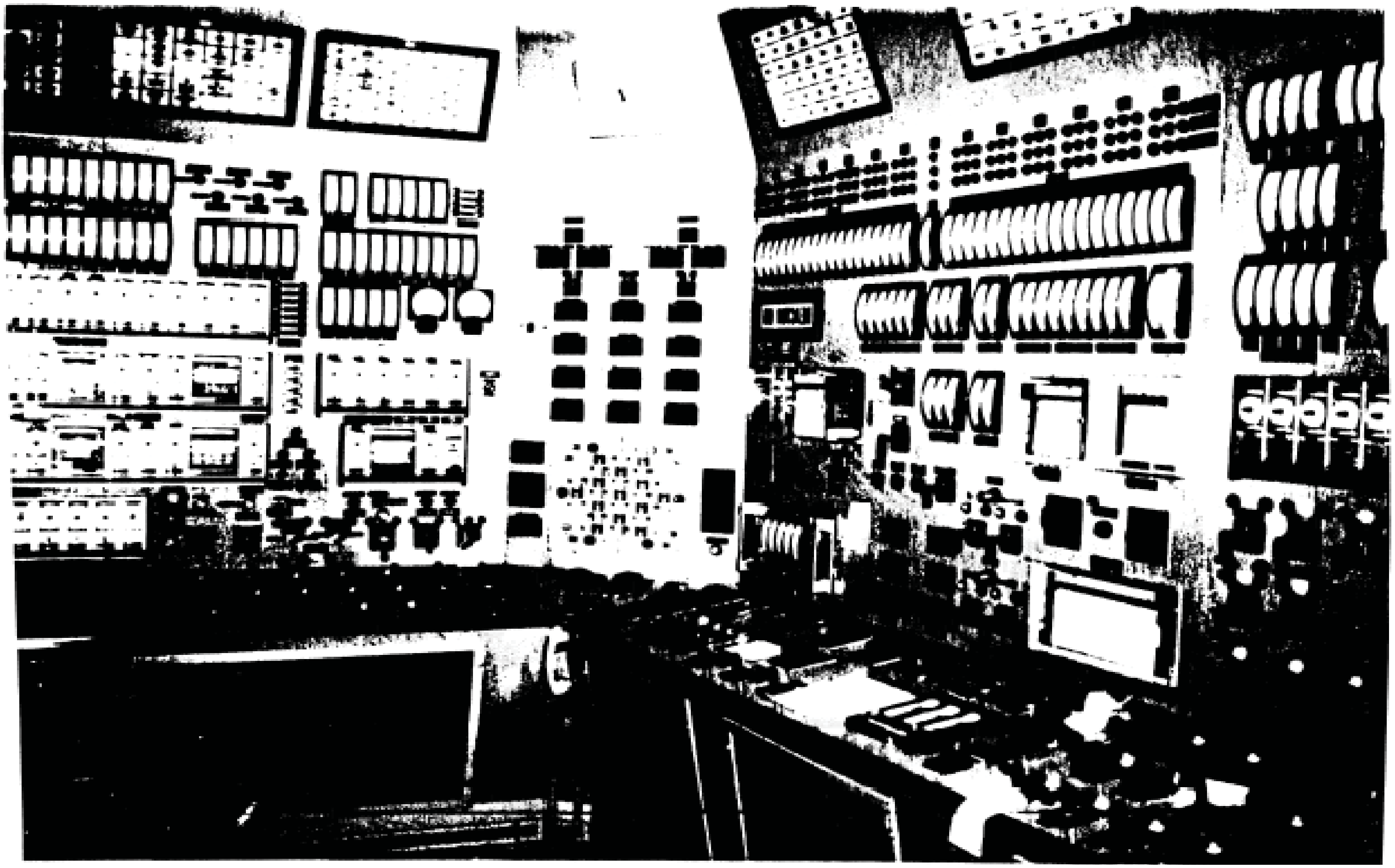

Figure 3 Fort St. Vrain Point-to-Point Control Room

Figure 4 ABWR Control Room Layout

Table 1 New Plant I&C DCS Design

Type	RPS	ESF	DAS	PCS
AP1000	Common Q	Common Q	FPGA	Ovation
ESBWR	NUMAC	Triconex	Mark VIe	Mark VIe
ABWR	FPGA	Common Q	Ovation	Ovation TOSMAP
APWR	MELTAC	MELTAC	Analog	MELTAC
EPR	Teleperm XS	Teleperm XS	Digital	Digital

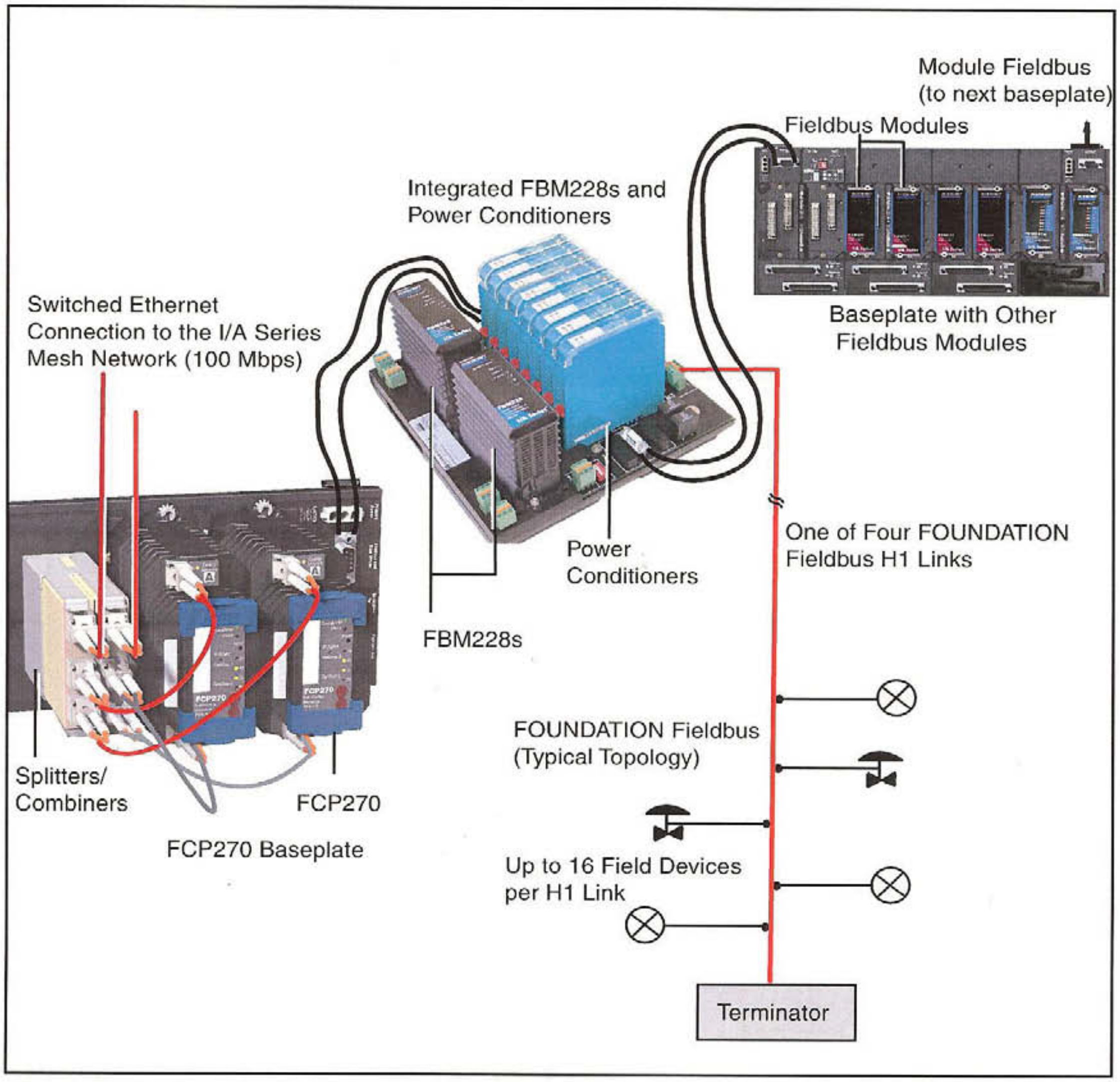

Figure 5 Example Foundation Fieldbus (FFB) Network (Typical Topology)