NBSR REACTOR CONTROL ROOM UPGRADE

Dağıstan Şahin
National Institute of Standards and Technology Center for Neutron Research
100 Bureau Dr., Gaithersburg, MD 20899 USA
dagistan.sahin@nist.gov

ABSTRACT

The maintenance and modernization of the National Institute of Standards and Technology (NIST) Center for Neutron Research (NCNR) reactor, known as the NBSR, is an ongoing process to endure until the eventual decommissioning of the reactor. As part of the renovation effort, the reactor control system is to be upgraded. Following some initial outsourcing efforts, the NBSR reactor control system upgrade has been restructured to be implemented by in-house means. The beginning stage of the upgrade involved the development of a simulator environment based on a PC system and digitization of the majority of nuclear reactor monitoring data. The NBSR reactor surveillance data consists of approximately thirteen hundred input/output points, including analog/digital sensor signals, signal conditioners, and relay logic. The aim of the current phase is to implement a new reactor data acquisition and display system (RDS) and lay out the infrastructure for the upgrade of the reactor control system (RCS). Key design criteria are to implement a reliable, redundant, diverse, modular and candid system where any complex digital manipulations are taken outside of the control room. Basically, the data analytics and custom codes are separated from reactor operation control and decision making logic. Furthermore, the new RDS is designed such that it could be maintained internally by NCNR personnel. The RDS is unique in design and modularity, minimizing custom codes and testing, making it ideal for research reactors.

Key Words: reactor display system, digital reactor control, digitalization, modular reactor console

1 INTRODUCTION

The diminishing supply of analog components for process control systems is a pressing issue for many nuclear power plants ensuing major control room modernization efforts [1]. Although many other industries already heavily rely on digital instrumentation and control hardware and software, the nuclear industry has been reluctant to a swift conversion to digital systems. The main driving mechanism for slower change from analog technology may be the lack of clear guidelines, regulations and sophisticated requirements for reliable and safe replacements.

The National Institute of Standards and Technology (NIST) Center for Neutron Research (NCNR) reactor, known as the National Bureau of Standards Reactor (NBSR) , has been in operation since 1967. The modernization of the NBSR is an ongoing process to endure until the eventual decommissioning of the reactor. The reactor control system had been through a few minor upgrades since the first installation, yet the majority of the control and display systems are still analog. The beginning stage of the upgrade involved the development of a simulator environment based on a PC system and digitization of the majority of nuclear reactor monitoring data [2]. Consequently, the reactor control system is being upgraded with a digital data acquisition and display system. The main goal of this upgrade is to maintain or increase the reliability of the NCNR control room console.

The NBSR reactor surveillance data consists of approximately 1243 input/output points including analog sensor signals, equipment states such as pump on/off conditions and relay logic. The eventual goal is to convert the reactor control system over to a distributed Supervisory Control and Data Acquisition (SCADA) system and completely replace the existing console.

2 DESIGN

The NBSR Data Acquisition and Display System (RDS) is a simple redundant system utilizing digital recorders, a mimic display monitor, and isolated digital meters. The new RDS satisfies the requirements for the safe and reliable operation of the NBSR through basic engineering and design controls. Key design criteria is to implement a robust, reliable, redundant, diverse, modular and straightforward system where any complex digital data manipulations are taken outside of the control room. Historical data trending, data analytics, storage and web services are separated from reactor control and decision making logic. Additionally, the new RDS is designed to be modular, such that it could be easily maintained internally by the NCNR personnel.

Process sensor signals are either acquired by remote I/O modules or by local I/O modules and digital meters and displayed on a trending digital recorder, a mimic screen and a digital meter in the Control Room Console. The high-level architecture of the RDS is presented in Fig. 1. Only one section is shown in Fig. 1, where the full system employs multiple sections.

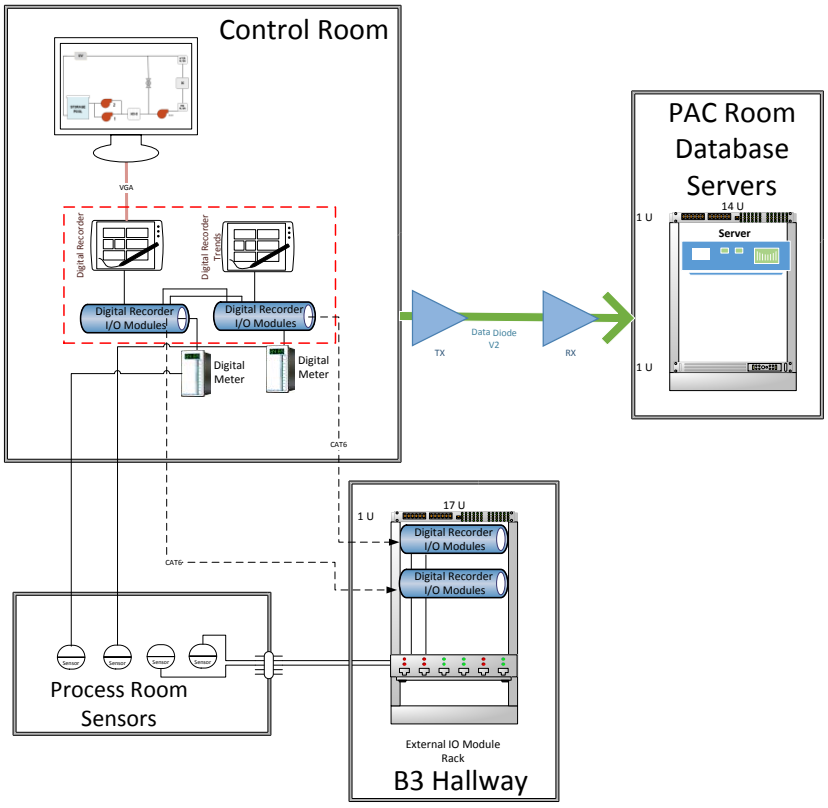

Figure 1. High-Level Architecture for the NBSR RDS

A one-way data diode transfers plant parameter information to the outside historian database servers. Details on the one-way data diode are given elsewhere [3]. A database server is then used to store historical plant condition data for later analysis. A basic data flow diagram for the RDS is shown in Fig. 2.

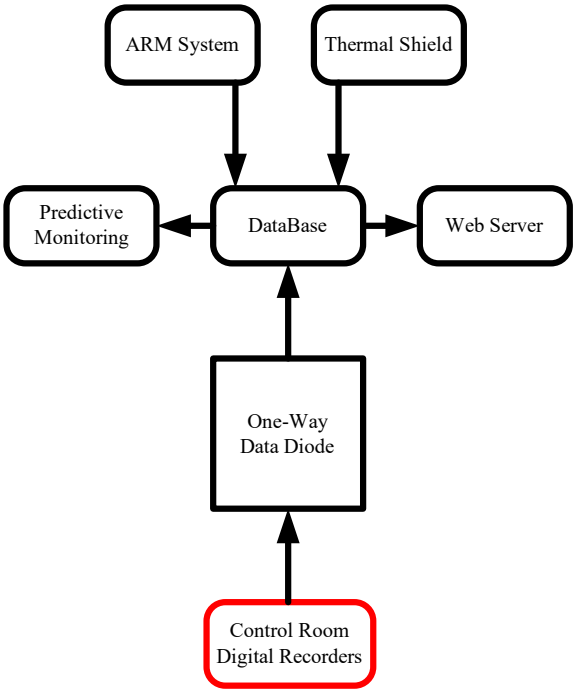

Figure 2. Data Flow Diagram

2.1 Architecture and Operating Principle

The level of importance, normal, annunciating, rundown and scram, designates which loop circuit the sensor signal follows. These parameters are based on process criticality as explained below.

Normal: An Instrument that does not have any annunciator nor action. The information is only relevant for continuous operation. The sensor value is displayed on the trend digital recorder and mimic screen.

Annunciator: The device is critical for the safety of a component or system. Notification of the operator is critical only for operational purposes. The sensor value is displayed on the trend digital recorder and mimic screen. These sensors follow a loop circuit as shown in Fig. 3 and values are displayed on the trend digital recorder and mimic screen.

Rundown: The instrument monitors a critical parameter for a system, structure or a component's safety. Notification of the operator and an automatic rundown is needed to prevent damage to a component or system. These parameters are listed in the NBSR Updated Safety Analysis Report (UFSAR). Fig. 4 shows an example circuit diagram for a rundown associated sensor. A rundown associated signal is displayed on two recorders and a class 1E digital meter. The rundown action is completed by three relays in series. The rundown circuitry is different from normal and annunciator circuitry in that a direct analog signal connects the transmitter to the class 1E digital meter and digital recorders.

Scram: The instrument monitors a critical safety parameter for the Reactor to prevent catastrophic accidents as evaluated in the UFSAR. An automatic scram signal is sent and operators are notified. Fig. 5 presents an example circuit diagram for a scram associated sensor. A scram associated signal is displayed on two recorders and a class 1E digital meter. Scram action is completed by three digital relays and an Action Pak in series. The scram circuitry also is different in that a direct analog signal connects the transmitter to the class 1E digital meter, digital recorders and an action causing Action Pak.

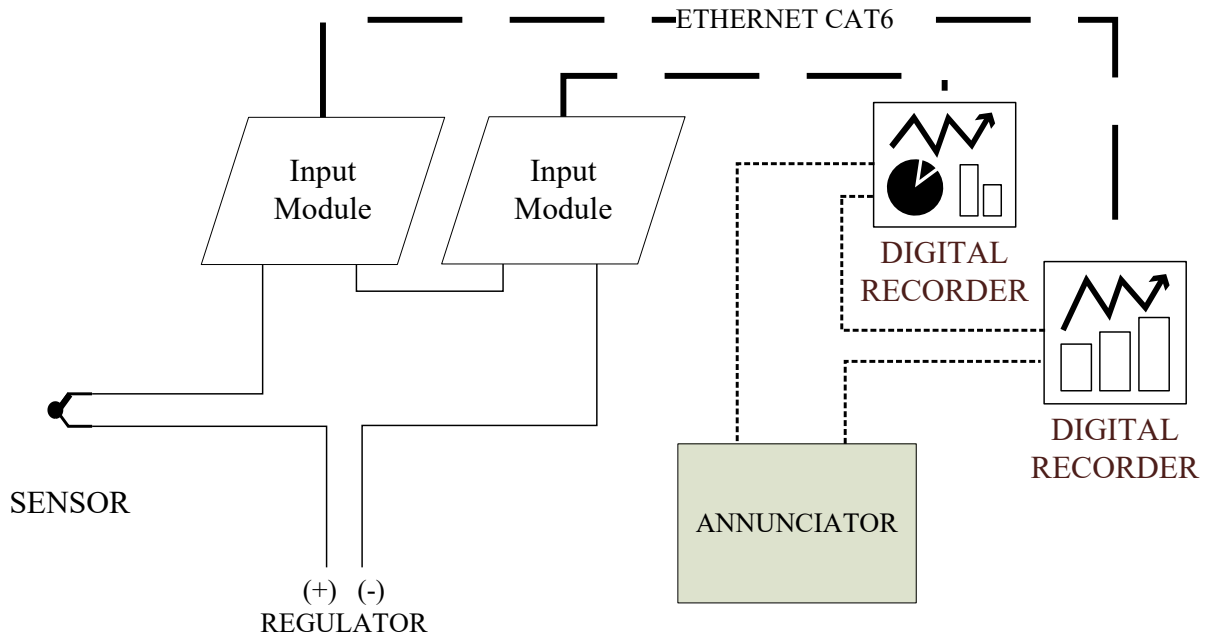

Figure 3. Annunciator Associated Sensor Parameter Sample Circuit

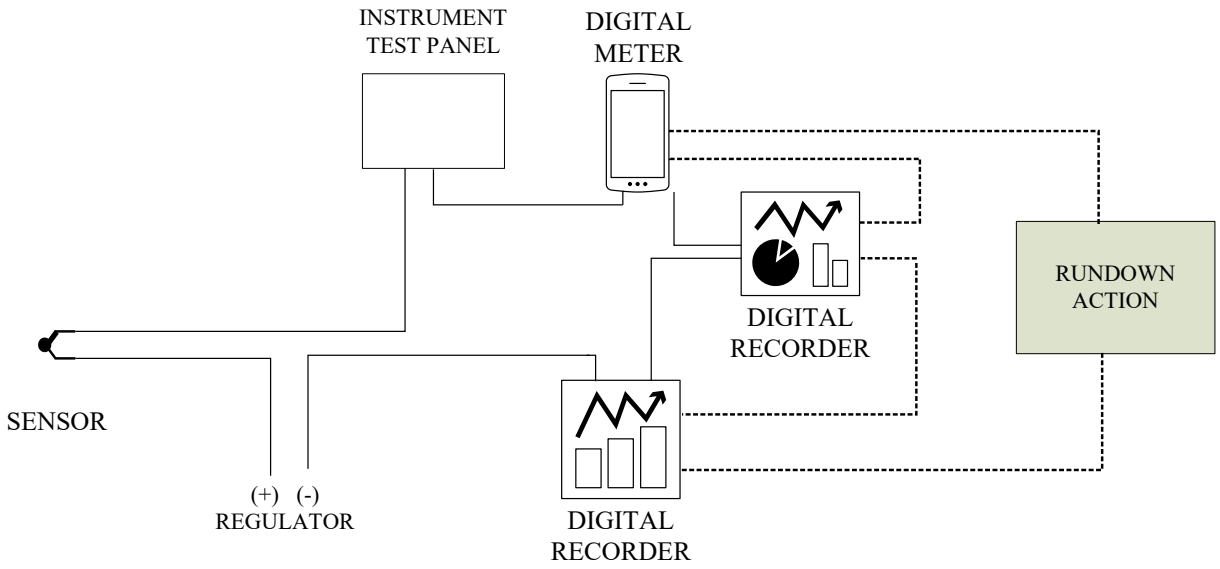

Figure 4. Rundown Associated Sensor Parameter Sample Circuit

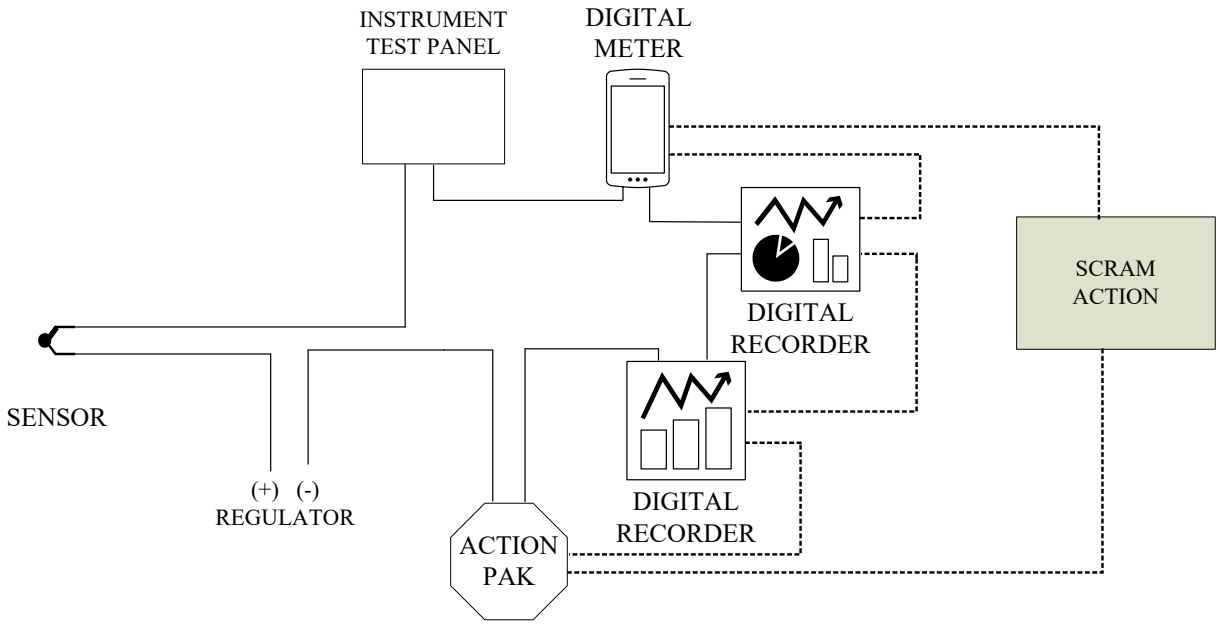

Figure 5. Scram Associated Sensor Parameter Sample Circuit

Normal and annunciating signals are acquired outside the control room, closer to the sensors, thus significantly reducing the number cable runs to the control room. Out of the 120 analog sensor signals, only 14 safety related signal cables would be routed directly to the control room and class 1E digital meter and action causing relay. Approximately 100 Action Pak devices would be removed from the control room console.

Control echelon within the data acquisition and display system are the indicators, annunciators, and alarms associated with the instruments as listed in Appendix A. Monitoring and indication echelon provides accurate and redundant sensor information for the operators to perform their tasks. The monitoring and indication echelon includes one digital recorder providing trending data, two digital meters, PID controllers (if necessary) and a separate digital recorder coupled with an industrial monitor to display a mimic screen.

3 DESIGN ANALYSIS AND COMMON CAUSE FAILURE CONSIDERATIONS

The new RDS satisfies the aforementioned key design criteria by implementing a robust, reliable, diverse, modular system with inherent defense-in-depth.

A Common Cause Failure (CCF) Susceptibility Analysis provides necessary information and conclusions to determine which outcomes exist for the software and hardware portions of the digital modification. A thorough review of the development and available operating history of the hardware and software was performed and documented to assess the dependability of the new digital control system. The hardware and software failure modes for each component within the new RDS has been evaluated.

3.1 System Reliability

The hardware used for data acquisition and display do have excellent Meantime Between Failure (MTBF). Digital recorders have an MTBF of 30.7 years. The IO modules and extensions for the recorders have more than 50 years MTBF. The digital meters are built as military grade and use the same firmware as the 10CFR50 APP. B & 10CFR21 qualified nuclear versions and have a lifetime warranty.

3.2 System Redundancy

Process information is displayed on a mimic screen using a digital recorder. Another recorder displays trending data. Additional digital meters (different brand and model) display section critical parameter information, such as primary flow and temperature indications, as shown in Fig. 4 and Fig. 5. The loop signal is provided in series to each piece of equipment, where only rundown and scram related circuitry completes a signal cable run to the control room. The Trending recorder and mimic recorder employ separate, isolated I/O units to acquire readings. Digital meters use internal I/O circuitry to gather readings.

Digital components with different firmware/make are interchangeably used in the system, digital recorders and digital meters are manufactured by different providers. Hardware used in the RDS provides functional, software and equipment diversity for displaying sensor information and in actuating associated alarms and actions.

3.3 Defense-In-Depth

Process parameters are displayed on a mimic screen and trend screen both provided by two independent digital recorders. Important system parameters, sensors providing rundown or scram signals, are additionally displayed on digital meters. Digital recorders and digital meters are based on different technologies developed by distinct companies. Both digital recorders and digital meters employ relays. A process parameter that has annunciator action is completed by two recorder relays. A rundown actuating parameter action is completed by the recorder relays and digital meter relays. Scram parameters employ an Action Pak in addition to the digital recorders and a digital meter. Digital meters employ 10A relays, while the digital recorder relays are 3A SPDT. The digital meters and digital recorders are isolated from each other preventing single point common cause failures. In other words, any of them failing does not affect others for signal, power, or relay actuation. The relays will be set to Normally Closed (NC) de-energize. This means that the relay will be in the same state when an alarm occurs as when the unit is shut down. This ensures that the relay fails in a safe mode, causing an alarm, if there is ever a problem with the unit or the unit loses power. Furthermore, the digital recorders do have a separate relay for fail output, actuated whenever a CPU failure has happened. “The relay is energized when the CPU is normal and is de-energized when a CPU error occurs. Therefore, relay output is carried out also when the power is off (including a power failure).” [4].

3.4 System Diversity

Digital components with different firmware/make are interchangeably used in the system. Hardware used in RDS provides functional, software and equipment diversity for displaying sensor information and actuating associated alarms.

3.5 Modularity

Configuration files for the simple digital components, recorders and meters are saved on a subversion system. The components can be easily replaced in place with minimal impact and testing. Connections to the process are made by plug-and-play type terminals, similar to DB9 or RS485 connections.

3.6 Human System Interaction Considerations

The operators interact with the RDS through digital recorder trend, mimic and digital meter interfaces. The RDS does not directly provide any control action of pumps, valves or other controls. The NBSR reactor operators are familiar with the interface of the digital recorders. There will be additional one-to-one training for the operators before the final system installation.

3.7 Physical Interaction

The RDS does not provide any control action. Therefore, there are no scenarios of an adverse impact resulting from physcial interaction with the digital system. Human errors are not likely. The UFSAR does not evaluate human error induced accidents. No different type of accident possibility is introduced.

3.8 Information Presentation

The information presented on the new digital recorders, mimic screen, trending screens and digital meters are different from existing analog meters. The NBSR console is divided into function based sections representing auxiliary or primary systems, such as primary mechanical system, primary nuclear system, secondary system, area radiation monitoring system, etc. All of the current analog meters for each system will be combined into digital systems maintaining these sections as shown in Fig. 6. Although the combination of functions into digital displays reduces separation of individual meters, the combination does not affect the variety and/or layers of the design described in the UFSAR. The new system employs multiple diverse digital units to display information. The NBSR console already employs digitals recorders for information display. The new recorders are similar regarding presentation.

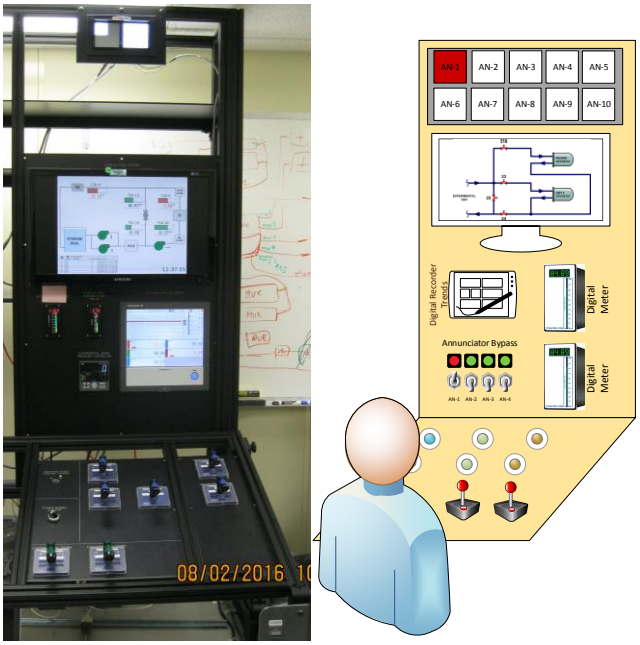

Figure 6. Mock-up System (left) and Schematic Diagram of the new NBSR Control Room Section (right)

No portion of the proposed activity involves how individuals interact with the new digital devices or the information presented by the new devices. The same information will be available with the new devices, and the information will be used in the same manner. Since no unreceptive Human System Interface (HIS) aspects are implemented with this change, no adverse impacts are possible.

3.9 CCF Considerations Hardware

The RDS utilizes commercial off-the-shelf digital meters and digital recorders to perform data display, acquisition, and alarming functionality. These units come with firmware installed, tested and verified by the manufacturer. All power to the hardware is supplied by the NBSR critical power system. The RDS utilizes a redundant power supply for the transmitter and expansion I/O racks located close to the sensory equipment. An example expansion box is shown in Fig. 7.

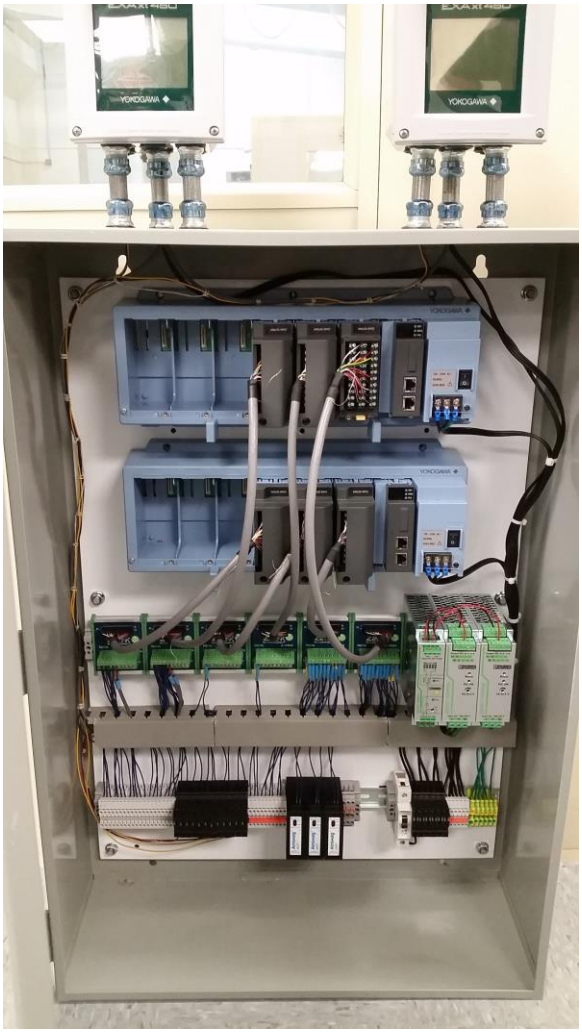

Figure 7. Mock-up Expansion I/O box for the new NBSR RDS

The mimic and trending recorders employ isolated I/O modules and expansion and communication modules fully redundant to each other. Isolated digital meters display important system parameters and provide extra redundancy for display and alarm actuation as well as safety actions, such as rundown and scram if needed for that section. No single failure can cause a loss of overall system function. Any recorder, I/O module or digital meter failure does not affect the others. A redundant power supply is used to power transmitters and expansion I/O modules. The failure of the redundancy module would fail the expansion I/O modules and transmitters. However, when the expansion modules fail the digital recorders and digital meters would not fail and still execute safe alarm action.

3.10 CCF Considerations Software

Since the digital meters and digital recorders employ completely different firmware and hardware and are produced by different companies, a common cause software failure is not anticipated. The digital recorders are connected to the expansion modules with direct cabling, without any intermediate hardware. The failure in communication within digital recorders or digital recorder I/O modules does not affect digital meters. All such failures are detectable by the operators or, when applicable, recorded in the recorder alarm lists.

The firmware in the digital recorders and digital meters were developed and tested using a software requirements specification, factory acceptance testing, a site acceptance testing plan, and verification and validation plan. The manufacturer provided QA documentation and certifications for specific units are on file and analyzed thoroughly. The configuration changes will be controlled by the appropriate site configuration management procedures and equipment operating instructions. Therefore, since the dependability of the digital control system has been established, the dependability of the associated design functions has been confirmed.

A critical digital review of the RDS digital units' firmware was performed. Although some additional testing was employed for each unit, there is no evidence of extensive testing of all internal and external state combinations and there is no analysis that demonstrates untested state combinations are irrelevant. Unprecedented failures may still be possible, but unlikely to happen simultaneously for both devices: digital recorders and digital meters.

4 SECURITY

The system connects some control console devices that were previously un-networked. If one device on that network is compromised, the concern is that device would then have the capability to compromise other devices on the network.

To prevent an outside malicious programmer from having any means to directly access the new RDS, the Reactor Network is a private network with no connection to the internet. Also, there are no means to accidentally connect the reactor network to the internet as all of the devices on the network are configured to static private network IP addresses.

Assuming that malicious software was to infect one of the devices on the reactor network, that malicious software could not affect any of the reactor safety systems, any of the devices that control reactor processes, or any of the displays that the Reactor Operators rely upon to make decisions in the control of the reactor. The digital recorders are not prone to any viruses [4]. Digital meters used in the data acquisition system are isolated and cannot be reached by any network. To enforce further protection, the reactor network is configured such that all traffic must pass through a Modbus Read-only firewall. This firewall only allows properly formatted Modbus read requests and Network Time messages to pass through it. All other network traffic is stopped by the firewall. A one-way data diode collects measurement data from the digital recorders and transfers to the research network over RS-232 cables [3].

5 CONCLUSIONS

The proposed changes will not impact the frequency of occurrence of the accidents evaluated in the UFSAR. Since an increase in the likelihood of a malfunction of the new RDS is not discernible, there is not more than a minimal increase in the likelihood of a malfunction of a system, structure or componentimportant to safety previously evaluated in the UFSAR due to a software/hardware-related CCF.

A new reactor display system which lays out the infrastructure for the upgrade of the NBSR reactor control system is described. The new RDS satisfies the design criteria by implementing a robust, reliable, diverse, modular system with inherent defense-in-depth. The new design allows a significant reduction in cables and Action Pak's, thus enabling easy maintenance and troubleshooting. Furthermore, the new RDS is designed such that it could be sustained internally by NCNR personnel. The RDS is unique in design and modularity, minimizing custom codes and testing, making it ideal for research reactors.

6 ACKNOWLEDGMENTS

Special thanks to the NBSR Reactor Operation and Engineering personnel for their support and valuable feedback provided during the development of this project. Thanks to Samuel MacDavid, Daniel

Keyser, Scott Arneson, Anthony Norbedo and Susan Deeb providing technical input during the design phases.

7 DISCLAIMER

Certain commercial equipment, instruments, or materials are identified in this study in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

8 REFERENCES

1. INTERNATIONAL ATOMIC ENERGY AGENCY, *Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants*. IAEA Nuclear Energy Series No. NP-T-1.4, IAEA, 2009.
2. G. J. Reyenga, "NCNR Control Room Modernization Phase I," in *Trans Am Nucl Soc*, Washington, DC (USA), 2011.
3. S. Arneson and D. Şahin, "Cyber Security using Multi-Threaded Architecture Data Diode at the NBSR," in *Trans Am Nucl Soc*, San Francisco, CA, TBP.
4. Yokogawa, "Model GX10/GX20/GP10/GP20 Paperless Recorder User's Manual." Yokogawa Electric Corporation, May-2014.