INL/EXT-21-64580

Light Water Reactor Sustainability Program

Digital Infrastructure Migration Framework

September 2021

U.S. Department of Energy

Office of Nuclear Energy

INL/EXT-21-64580

Digital Infrastructure Migration Framework

Light Water Reactor Sustainability Program

Paul J. Hunton, Sr, Research Scientist, Principal Investigator
Robert T. England, Research Engineer

September 2021

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy

Executive Summary

Commercial nuclear power in the U.S. has been an unqualified success by any measure, having provided safe, low-cost, carbon-free baseload electricity for decades. Today, the industry is at the peak of its historical performance in terms of generation output, reliable operations, and demonstrated nuclear safety. However, nuclear power generation faces financial challenges. Operating costs, driven by antiquated and labor-centric operating models using analog technology, have forced the early closure of multiple nuclear stations and placed the larger population of stations at-risk. The effects of economic headwinds and diminishing returns in innovating within the current business model point to the need for a transformed nuclear generation business model. This model must maintain or enhance plant safety and reliability while reducing total ownership cost.

The U.S. Department of Energy's Light Water Reactor Sustainability Program Plant Modernization Pathway has produced a framework for transforming the current nuclear power plant operating model. This framework is termed "Integrated Operations for Nuclear" and is more fully presented in INL/EXT-20-59537, "Analysis and Planning Framework for Nuclear Plant Transformation" (Reference 1). It is recommended that Reference 1 be reviewed by readers of this document to provide proper context. Reference 1 content has been briefly summarized in this work in Section 1.2 to aid in readability.

Section 4.3.5.6 of Reference 1 identifies the need for strategic activities and associated documents to plan the orderly implementation of technology used to transform work functions in order to lower nuclear plant operating costs. This set of documents and their interrelationships are briefly presented below:

1. **Digital Infrastructure (DI)** (described in this document)**:** Establishes the comprehensive physical/logical foundation to host Data Architecture and Analytics capabilities (below).
2. **Data Architecture and Analytics:** Researches, develops, leverages, and integrates DI technologies with software applications/capabilities (control system automation, modern human-system interfaces, machine learning, and artificial intelligence) across the full range of a nuclear power generating facility as well as a utility's corporate enterprise.
3. **Human and Technology Integration:** Research and development efforts that evaluate and apply technology solutions within a human-centric framework that optimizes the effectiveness of humans and technology to significantly reduce risks of modernization and improve performance.
4. **Integrated Operations for Nuclear:** The transformational operating model for the nuclear industry that guides the efforts/activities associated with activities 1—3 above to establish, augment, and sustain the safe, reliable, and economic operation of a nuclear power plant in a way that enables continued operation for 80+ years.

This document provides a generic technology strategy and is presented from a technology platform point of view. This platform is ultimately the union of activities1 and 2 above. Specific technologies and software applications are researched, developed, implemented, and then integrated in such a way as to optimize both the performance of the technology and the capabilities of users who leverage it (activity 3 above). The ultimate objective is to enhance safety, reliability, and economic performance such that the result provides much more than the sum of its constituent parts. The selection of these technologies is driven by an Integrated Operations for Nuclear driven Advanced Concept of Operations and associated business case analyses which are unit, station, and utility specific (activity 4 above).

This document presents a full-scope DI implementation and lifecycle support recommendations that enable a plant life of 80+ years. Depending upon a unit's operational lifetime, concepts presented in this report can be applied either individually or as partial implementations. For example, governance and administrative processes can be streamlined by Data Architecture and Analytics software applications hosted at the Corporate Network Level of the DI. While additional benefits could be obtained by coupling these software applications with digital data from new DI instrumentation and control platforms, a limited operational lifetime (e.g., <10 additional years) may not provide a sufficient return on investment to justify the new instrumentation and control platforms.

CONTENTS

FIGURES

Appendices

Acronyms and Definitions of Key Terms

10 CFR 50	Title 10 of the Code of Federal Regulations, Part 50, Energy
10 CFR 73	Title 10 of the Code of Federal Regulations, Part 73, Physical Protection of Plants and Materials
API	Application Programming Interface
ATWS	Anticipated Transient Without Scram
BOP	Balance of Plant
BTP	Branch Technical Position
CAP	Corrective Action Program
CDA	Critical Digital Asset
CIM	Westinghouse Component Interface Module®
CFR	Code of Federal Regulations
CWS	Circulating Water System
DA&A	Digital Architecture and Analytics
DI	Digital Infrastructure
DI&C-ISG-04	Digital Instrumentation and Controls Interim Staff Guidance #04
DI&C-ISG-06	Digital Instrumentation and Controls Interim Staff Guidance #06
DAS	Diverse Actuation System (function in a Distributed Control System)
DCS	Distributed Control System
Display	A software generated image presented on a Video Display Unit
DKT	Display, Keyboard, and Trackball (a Human Machine Interface device type)
DMZ	Demilitarized Zone
EOF	Emergency Operations Facility
EPOCH	Efficient Plant Operations Concept using Human-system-integration
ERO	Emergency Response Organization
ERDS	Emergency Response Data System
ESFAS	Emergency Safety Feature Actuation Systems
FPGA	Field-Programmable Gate Array
FSAR	Final Safety Analysis Report
GDC	General Design Criteria
HFE	Human Factors Engineering
HSI	Human-System Interface
HTI	Human-Technology Integration
I&C	Instrumentation and Control
I/O	Input/Output
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
ION	Integrated Operations for Nuclear
ISG	Interim Staff Guidance

IT	Information Technology
LLC	Limited Liability Company
LWR	Light Water Reactor
LWRS	Light Water Reactor Sustainability (Program)
MCR	Main Control Room
ML	Machine Learning
NAS	Network Addressable Storage
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission (United States)
O&M	Operating and Maintenance
OCC	Outage Control Center
OSC	Operations Support Center
PM	Plant Modernization
PPC	Plant Process Computer
RPS	Reactor Protection System
SLR	Subsequent License Renewal
SPDS	Safety Parameter Display System
TOC	Total Ownership Cost
TSC	Technical Support Center
VDU	Video Display Unit – a physical device on which software generated displays are presented

DIGITAL INFRASTRUCTURE MIGRATION FRAMEWORK

1. Industry Need

1.1 Problem Statement

Commercial nuclear power in the U.S. has been an unqualified success by any measure, having provided safe, low-cost, carbon-free baseload electricity for decades. Today, the industry is at the peak of its historical performance in terms of generation output, reliable operations, and demonstrated nuclear safety.

The commercial nuclear sector, however, faces unprecedented financial challenges. Operating costs, driven by increasingly antiquated labor-centric operating models and analog technology, have forced the early closure of multiple nuclear stations and placed a much larger population of nuclear stations at-risk. The combined effects of economic headwinds, diminishing returns in innovating the current business model, and the onset of a strategic inflection point for nuclear generation all point to the need for a transformed business model for nuclear generation. This transformed business model must maintain or enhance plant safety and reliability while reducing total ownership cost (TOC).

The U.S. Department of Energy's Light Water Reactor Sustainability (LWRS) Program Plant Modernization (PM) Pathway has produced a framework for transforming the current nuclear power plant (NPP) operating model. This framework is termed "Integrated Operations for Nuclear" (ION) and is more fully presented in INL/EXT-20-59537, "Analysis and Planning Framework for Nuclear Plant Transformation" (Reference 1). It is suggested that Reference 1 be reviewed by readers of this document to provide proper context. Reference 1 content has been summarized in Section 1.2.1 to aid in readability.

This transformed operating model relies upon the use of digital technology as a foundational enabler to achieve its objective of extending the operating lifetime of existing LWRs to 80+ years from an economic and technical perspective. This document proposes that a single, enveloping Digital Infrastructure (DI) consisting of tightly integrated subsystems hosting software applications provides the most efficient and sustainable method to provide this foundation.

1.2 Integrated Operations for Nuclear – A Model for Transformative Change

1.2.1 Integrated Operations for Nuclear Overview

Section 4.3.1 of Reference 1 discusses setting the operational context for the application of the ION methodology. All capabilities that must be addressed to achieve a future New State as enabled by ION must be identified and managed. This is difficult because of the complex interrelationships among various capabilities. To aid in addressing this complexity, a capability stack model was developed as described in Section 4.3.2.2 of Reference 1. A capability stack model is defined as:

> *…a layered representation of a complex system. The stack model seeks to decouple the complexity of the system by introducing distinct layered activities connected by standard interfaces.*

The layers of the stack model assume that the capabilities of a lower level are needed to execute the capabilities of a higher level. It is further assumed that information can be exchanged across the layers via standard interfaces. The following are characteristics that describe the layers:

1. Each layer must have a dominant or compelling value proposition.
2. Each layer must have clearly defined and shared interfaces with adjacent layers.
3. Each layer must reflect an active market for products or services.

4. Each layer much have a well-defined business-oriented set of metrics that reflect the core value proposition.

Figure 1 below depicts the generic nuclear capability stack model for ION as adapted from Reference 1:

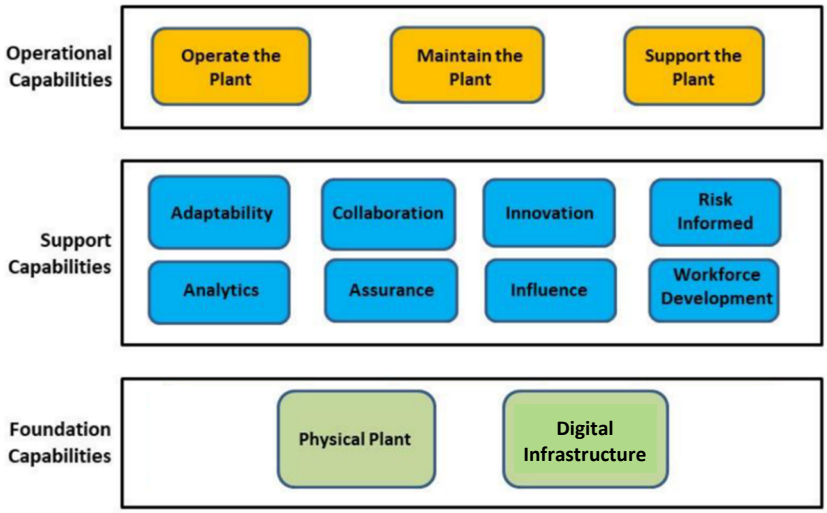


Figure 1 – Generic Nuclear Capability Stack Model

The stack model provides a holistic basis for LWRS PM Pathway research. The DI provides foundational capabilities at the bottom of Figure 1 to host Data Architecture and Analytics (DA&A) software applications developed to enable support capabilities shown in the middle of Figure 1. Human and Technology Integration (HTI) activities ensure that the DI human-system interface (HSI) hardware, along with the DA&A application functionality accessed through these HSIs, optimizes the execution of operational capabilities shown at the top of Figure 1. The net result is to reduce nuclear plant TOC. Specific objectives and outcomes for these research areas are shown in the left three columns at the bottom of Figure 2 below.

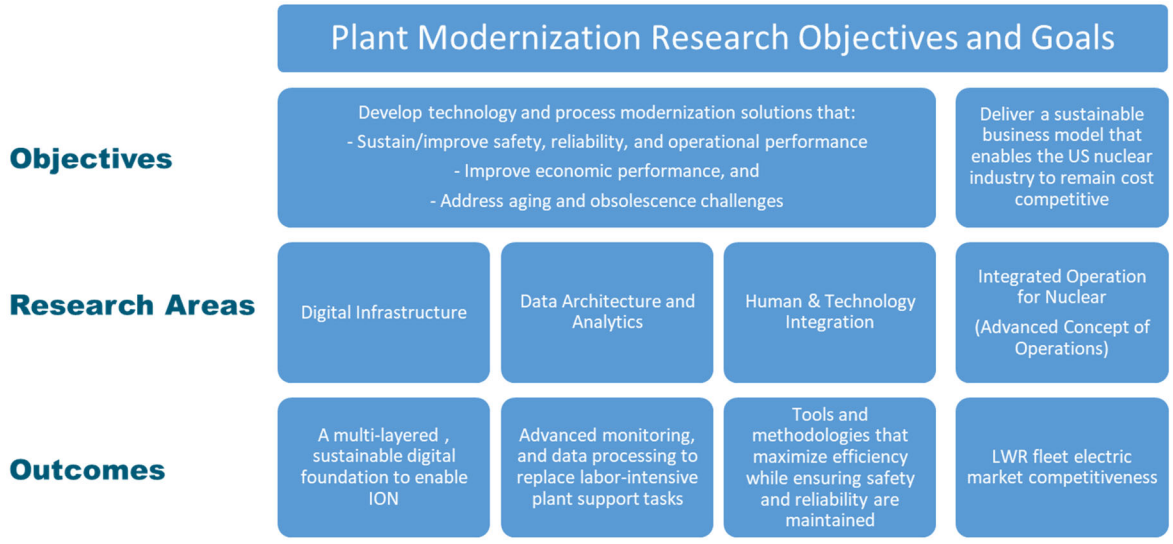


Figure 2 – LWRS-PM Pathway Objectives and Goals

The ION Model and associated Advanced Concept of Operations research makes up the far-right column of Figure 2. ION provides strategic direction for all LWRS PM Pathway efforts that are performed for

utility benefit. Research outcomes in the three left columns of Figure 2 are not performed for their own sake but are focused to enable operational capability process improvements identified by ION to enhance LWR fleet electric market competitiveness. Note that the left-to-right flow of the bottom two columns of Figure 2 mimics the bottom-to-top flow of the stack model shown in Figure 1.

Utilities create budgets and schedules for implementing improvements that leverage technologies enabled by LWRS research as well as those available in industry. The objective of such improvements is to realize an ION identified market-based electricity price point for a nuclear unit. LWRS PM top-down strategic objectives shown in Figure 2 are achieved by assisting utilities through research and focused support in the successful execution of these projects. Work is also analyzed by utilities from the bottom-up for opportunities to optimally address existing operational and obsolescence issues within the strategic ION framework while aggressively focusing on essential modernization activities that can be resourced within available budgets.

It must be understood that the ION Model is not intended to replicate existing processes and accomplish them in more efficient ways through the utilization of technology. ION emphasizes a holistic evaluation of activities and applications of technology to improve nuclear unit market competitiveness as opposed to piecewise activities that address individual problems in isolation. Following this approach, the ION-driven result can be much more than the sum of piecewise efforts.

ION also includes the exercise of challenging whether existing processes are still necessary and whether they provide the intended value add for the cost of performing them. As an illustration, execution of the nuclear industry corrective action program (CAP) many times results in the implementation of procedural changes to address identified deficiencies. When a small number of simple changes to procedures are made following this approach, these often result in more accurate and timely procedure execution. This is an intended result of the CAP. Following the same practice for twenty years can result in a complex procedure set created by piecewise change, which is very difficult to follow. Replicating the execution of paper copies of such procedures with new technology may reap some marginal benefit and perhaps some cost savings. ION, however, would evaluate such procedures with a new set of eyes with the intent of simplifying them to support their original intended purpose while making their execution far more efficient and accurate. Combining the result of such an effort with advanced technology would then further amplify their efficient and accurate execution.

1.2.2 Integrated Operations for Nuclear – Technology Focus Areas

The fundamental technology focus areas of LWRS PM Pathway research, as shown in the left three columns of Figure 2 above, are being simultaneously aligned and pursued to enable the ION Model on the far right of the same figure. Each of these three technology research areas is described in more detail below:

- **Digital Infrastructure.** This effort establishes the comprehensive physical and logical foundation to support DA&A capabilities. The DI consists of multiple levels. Each level is established based upon the functions performed on it and associated requirements based on those functions. Each level consists of hardware and configuration/utility software (e.g., firmware, hardware resource management tools, operating systems, programming tools, self, diagnostic tools, cybersecurity monitoring tools).

  Efforts to migrate to and sustain this DI are the primary focus of this research report. It is presented in the context of a full-plant digital transformation for units expected to receive subsequent license renewals (SLRs) to operate for a total of 80–100 years. Concepts to address obsolescence concerns with digital equipment and associated configuration/utility software are also presented.

- **Data Architecture and Analytics.** This develops, leverages, and integrates technologies and software applications/capabilities (e.g., control system automation, modern HSIs, digital data

management, machine learning, artificial intelligence) across the full range of a nuclear plant/utility enterprise to enable the "support capabilities" shown at the center of the Generic Nuclear Capability Stack Model shown in Figure 1. The full set of software applications are created/purchased and integrated together to achieve the lowest TOC for the facility/enterprise that employs it.

These technologies and software applications/capabilities are myriad and occupy specific locations within the DI presented above based upon their function and other requirements. Taken individually, they can provide like-for-like capabilities to digitize current labor-centric processes and provide a degree of improvement in any particular area. When integrated as a cohesive set, they are optimized to provide an aggregate benefit to lower TOC that goes far beyond that achieved through a "sum-of-its-parts" approach.

This document illustrates how DA&A software applications/capabilities are optimally populated in the levels of the DI based on the functions they perform and associated requirements based on those functions (e.g., cybersecurity requirements).

These software applications/capabilities are deployed in such a way as to be as independent as possible from any particular instance of the DI technology on which they run. This insulates DA&A intellectual property investments (both the base software and the digital data populated therein) from obsolescence issues associated with digital equipment. DA&A software applications and databases implemented in this manner do not "wear out."

Details with regard to DA&A research, capabilities, and features are to be the subject of a separate, subsequent research report.

- **Human and Technology Integration.** The HTI research area conducts research and development to evaluate and apply solutions within a human-centric framework that jointly optimizes the effectiveness of humans and technology to significantly reduce risks of modernization. Within the overall conceptual framework of the LWRS PM Pathway, HTI is downstream of the DI and DA&A research areas, as seen in Figure 2, and as such receives the outputs of those research efforts. Those outputs can be viewed as technologies that HTI uses as inputs to be integrated with the efforts of humans that must use them.

  A key HTI research activity that is working in a cohesive and structured manner with the upstream DI and DA&A research areas (and ION) is the Efficient Plant Operations Concept using Human-system-integration (EPOCH) project (Reference 28). EPOCH's research focus is on developing HTI guidance to enable the effective adoption of advanced automation and other digital capabilities. A more detailed summary of EPOCH is provided in Section 5 below. The Section 5 summary follows the presentation of the DI and DA&A software applications to provide the HTI discussion with the proper context.

2. Digital Infrastructure Generic Framework

The simplified DI generic framework diagram proposed for nuclear, as shown in Figure 3 on the following page, is adapted from the Purdue Enterprise Reference Architecture that has been in generic industry use since the 1990s.

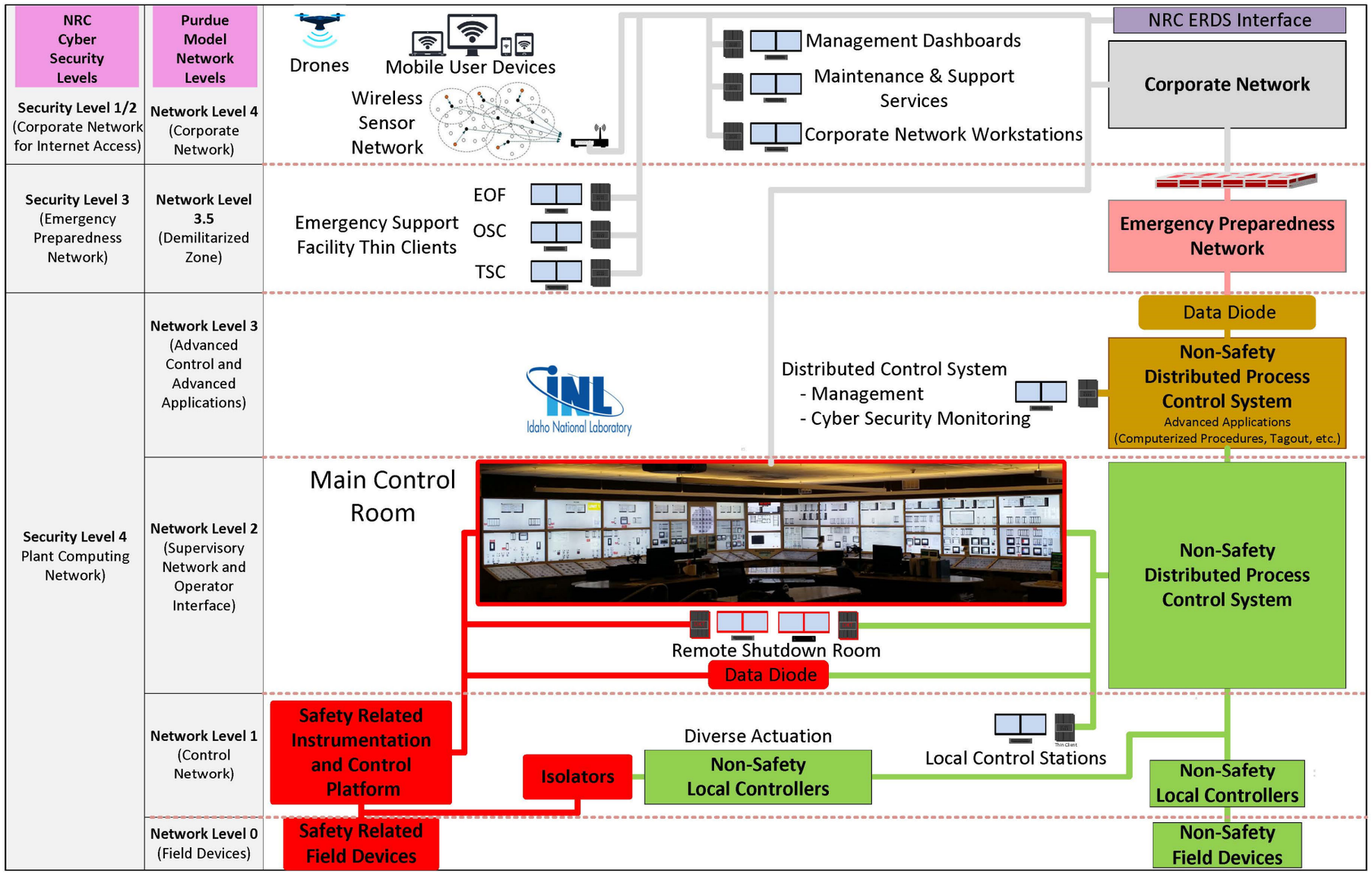


Figure 3 – Simplified DI Generic Framework for Nuclear

A more detailed depiction of representative technology and connectivity used in implementing DI is provided in Appendix A at the end of this report. When reading through the balance of this document, it is strongly recommended that the reader have separate copies of both of these depictions available for direct reference to aid in understanding.

The subsections below provide:

- A brief description of the generic architecture with regard to industry standard Purdue Enterprise Reference Architecture Digital Network Levels shown in Figure 3 (Section 2.1)
- A description of the quality requirements for digital subsystems shown in Figure 3 based upon their function (Section 2.2)
- United States Nuclear Regulatory Commission (NRC) Cybersecurity Levels shown at the far right in Figure 3 (Section 2.3).

2.1 Purdue Enterprise Reference Architecture Levels

A brief, simplified description of each Purdue Network Level (denoted by "Network Level" in the remainder of this document) as shown in Figure 3 above is provided below for orientation purposes. More details with regard to each Network Level in a nuclear plant implementation are provided in Section 4. Some of the detailed descriptions in Section 4 necessarily deviate from the summary description provided here.

- **Network Level 0: Field Devices**

  Devices that connect to, measure or control plant physical processes are included in Level 0. Devices are grouped into two areas:
  - Safety-related field devices
    - Field sensors (pressure, flow, temperature, neutron flux, etc.) that detect plant conditions and feed that data to a safety-related Reactor Protection System (RPS)
    - Field device final control elements to operate safety-related plant equipment (pumps, valves, fans, circuit breakers, heaters, etc.)
  - Non-safety field devices
    - Field sensors that detect plant conditions and feed that data to non-safety distributed control system (DCS)
    - Field device final control elements to operate non-safety plant equipment.

- **Network Level 1: Control Network** (Local Control)

  This is where the control field hardware resides and where control algorithms are executed. This is accomplished using:

  - Input and Output (I/O) blocks that receive data from the field and send control signals to Network Level 0 final control elements.
  - Control logic modules (controllers) process the data from the input blocks and make logic-based decisions based on automation and control elements within controllers and transmit control signals to the output blocks. Controllers also present information to Network Level 2 and receive control commands from Network Level 2.
  - Local HSIs used for direct local control are encountered at this level when installed.

- **Network Level 2: Supervisory Control**

  The primary functions supported at this level permit the operator to view Network Level 1 monitored processes and provide control signals to those processes. Coordinated supervisory

control of Network Level 1 controllers is possible at Network Level 2, but for reasons explained in Section 4.3.2, their use should be controlled in nuclear applications.

This is the first level that resembles a more traditional information technology (IT) system as leveraged in a DCS. It includes:

- Networking capability executed on switches (which can be installed in a redundant network configuration in order to mitigate the consequence of failure of any given switch or network connection).
- Traditional servers as depicted in Appendix A, which are used to virtualize the supervisory control environment. Functions performed at this level are not required to be virtualized, but such an implementation will require more physical hardware and all the necessary services associated with that hardware.
- HSIs at this level are the primary means for operators to supervise and control plant equipment from the Main Control Room (MCR). For a non-safety DCS, an additional engineering station typically located outside the MCR have lower-level access to control function logic programming and system configuration within the DCS at both Network Level 2 and Network Level 1.

- **Network Level 3: Advanced Control and Advanced Applications**

This is the level at which there is additional DCS server capacity with sufficient separation from essential control functions to leverage higher level functions such as:

- Hosting applications that are non-native to the DCS but provide for improved capabilities to affect overall plant control. This includes operator aid applications such as computerized procedures and computerized lockout/tagout. It also includes a data historian for the entire safety and non-safety I&C systems. These can be accessed as separate applications and presented on Network Level 2 HSIs.
- Hosting utility software applications such as patching servers as well as cyber security application tools to enable cybersecurity monitoring, logging and policy management for the DCS control system infrastructure. These applications are maintained at this level through the dedicated thin clients.

This level also provides necessary hardware time servers for the DI.

This level is considered the top of the control network. It is protected from the higher levels of the network by firewalls and isolated by data diodes. This ensures that intrusion attempts are detected and that no information originating from higher Network Levels can reach the control network and affect controlled processes or modify attributes within the control system.

- **Network Level 3.5: Emergency Preparedness Network and Demilitarized Zone (DMZ)**

Network Level 3 supports two fundamental functions:

- It hosts emergency preparedness digital capabilities (providing necessary data, DA&A applications, and supporting HSIs) to enable the Technical Support Center (TSC), Operations Support Center (OSC) and the Emergency Operation Facility (EOF) for a nuclear unit. The functions of each of these three facilities and how they are supported are described in Section 4.5 below.
- It provides controlled Network Level 4 access to select data stored within the Network Level 3.5 historian through a data buffer (DMZ). This function is also described in Section 4.5 below.

- **Network Level 4: Corporate Network**

  For the purposes of this report, no comprehensive elaboration is provided on all the possible Corporate Network interfaces and services. This report only presents those relevant to the higher functions implemented at this level that relate to the operation of a nuclear plant and methods to increase plant efficiency, including:

  - Connectivity that promotes mass data collection from all digital data sources in the DI. This includes the collection of all data from Network Levels 1–3.5. It also includes data collected by wired sources and wireless devices, such as sensors, drones, tablets and laptops connected at Network Level 4.
  - Advanced applications hosted at this level that:
    - Collect and integrate data sources within a common data model with an optimized framework for data capture, storage, and retrieval.
    - Analyze the data contained therein to optimize the business of running a NPP. In addition to applications available to industry, the LWRS PM Pathway at the Idaho National Laboratory (INL) has been and is continuing to pursue multiple data analysis research activities to more fully realize the potential to maintain or improve plant safety and reliability while reducing operational costs.

    These applications are presented in Section 4.6.2.
  - Presenting the results of this data analysis to utility personnel in support facilities to enable efficient and accurate planning and decision-making across the enterprise.
  - Enabling capabilities such as the centralization of support staff in locations remote from a nuclear plant site or the outsourcing of support activities to third parties through either the utility Corporate Network or the internet to improve efficiency and lower plant TOC.
  - Providing continued support of the NRC Emergency Response Data System (ERDS) interface.

2.2 Digital Systems: Differentiation of Quality Requirements

2.2.1 Instrumentation and Control Systems

The basic quality objectives for I&C systems resident in Network Levels 0–3 and the methods to achieve them are generic. Simply stated, I&C systems are designed to achieve high reliability and availability so that the systems they monitor and control can be safely operated and produce desired results or products. This is true for automobiles, aircraft, manufacturing facilities, or NPPs. Quality assurance requirements and associated levels of documentation required to demonstrate quality requirements are satisfied are tailored to risks associated with the potential consequences of I&C system maloperation.

2.2.1.1 Safety-Related Systems

The consequences associated with the maloperation of safety-related I&C systems, particularly those associated with reactor protection systems (RPS) and emergency safety feature actuation systems (ESFAS), include damage to a reactor core and the uncontrolled release of radioactive fission products to the environment. Such consequences necessarily drive RPS/ESFAS I&C quality requirements. Codes and standards that establish requirements for these systems are specified by 10 CFR 50.55a (h), “Protection and Safety Systems” (Reference 2). These are augmented by multiple, specific, general design criteria (GDCs) in 10 CFR 50 Appendix A, “General Design Criteria for Nuclear Power Plants” (Reference 3) that apply to these systems, along with specific quality assurance criteria as captured in 10 CFR 50 Appendix B, “ Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants” (Reference 4). Compliance with the requirements for these systems is inspected as directed by the

"Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (Reference 5), Section 7, "Instrumentation and Control Systems" as amplified by several related NRC Branch Technical Positions (BTPs) and Interim Staff Guidance (ISGs) documents.

Application of such nuclear industry specific requirements has achieved the necessary high degree of reliability, and availability for safety-related nuclear plant I&C systems. These successes come at a cost. Nuclear I&C requirements compliance has had the tendency to drive up the cost of developing, implementing, and maintaining these systems (whether they are custom designed to meet the requirements or commercially dedicated to do the same). Reliance on proven technology, along with the difficulty in demonstrating requirements compliance for capabilities enabled by new technologies (particularly digital), has tended to slow the application of digital technology to RPS and ESFAS I&C systems. This challenge to update RPS and ESFAS is exacerbated by the fact that existing analog RPS and ESFAS I&C systems are becoming increasingly obsolete and that the industrial knowledge and spare parts base to support them is waning.

2.2.1.2 Non-Safety Systems

Non-safety I&C systems in a NPP, while not tasked performing RPS and ESFAS functions, are no less important when it comes to achieving the objective of a commercial nuclear plant. This objective is a safe, reliable, and economical source of heat to generate electricity (typical use) or to enable other industrial processes (e.g., emerging commercial production of hydrogen). If non-safety I&C systems cannot provide highly reliable and available control of balance-of-plant (BOP) systems in a way that enables safe, efficient and economical plant operation, existing nuclear plants will be shut down and new ones will not be built.

Consequently, existing or potential future plant commercial nuclear operators are particularly concerned with ensuring that BOP I&C systems are highly reliable, available, economically obtainable, and sustainable. This is achieved through the development of such I&C systems in accordance with quality practices established in the commercial industrial control industry. The NRC has accepted the application of standard industry practices in Generic Letter 84-01 (GL 84-01), "NRC Use of the Terms, 'Important to Safety' and 'Safety-Related,'" (Reference 6).

In GL 84-01, the NRC states that NPP permittees or licensees are responsible for developing and implementing quality assurance programs for plant design and construction or for plant equipment that follows the more prescriptive requirements from Appendix B to 10 CFR Part 50 (Reference 4) for safety-related plant equipment and 10 CFR 50, GDC-1 (Reference 3) for other plant equipment. GDC-1 states the following:

> **Quality standards and records.** Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

In GL 84-01, "important to safety" as used above is defined as a category of equipment for which the "more prescriptive requirements for of Appendix B to 10 CFR Part 50 for safety-related plant equipment" do not apply.

Consequently, nuclear utilities have developed, and the NRC has approved quality assurance programs for their nuclear plants, which apply appropriate quality control for non-safety related systems, including

the use of appropriate industry standards for non-safety related I&C systems. The NRC affirms this practice in GL 84-01 by stating, "… [it is] the staff view that normal industry practice is generally acceptable for most equipment not covered by [10 CFR 50] Appendix B."

This does not make non-safety, BOP I&C systems "lower quality" or result in them being less reliable or available than safety-related I&C systems. It means that it is the utility's responsibility to ensure that quality, reliability, and availability are assured following generally recognized industry standards and their NRC-approved quality program for non-safety equipment. This affords a utility much more flexibility to adopt well-proven, more modern I&C system and software application techniques with requisite quality at a lower cost. Such efforts are focused on sustaining or improving nuclear plant safety, reliability, and availability while at the same time leveraging the capabilities of these modern systems to enable a more economic and sustainable operation of their facilities both in the near and long term. These capabilities are then magnified by the proper connectivity of digital I&C systems to other levels of the DI.

There has sometimes been a tendency by industry and the regulator to blur the clear demarcation of quality requirements for I&C systems. In order maximize the aggregate benefit of the DI concept, the boundaries and associated quality requirements between safety-related and non-safety I&C and between I&C and non-I&C related Network Levels must be unambiguously differentiated.

2.2.2 Support Networks

Support networks at Network Levels 3.5 (Emergency Preparedness/DMZ) and 4.0 (Corporate Network) are outside the realm of I&C systems since these provide no direct means of controlling plant equipment and do not provide indications that are directly used by operators to perform control functions. As such, industry and NRC standards for I&C system quality, reliability, and availability do not apply to support networks. Again, this does not mean that these systems are unimportant and that their quality, reliability, and availability are similarly unimportant. On the contrary, while the nuclear plant can physically operate without the support networks, a station cannot legally operate without these networks for long. The station or utility enterprise which the support networks service cannot effectively operate as a business without them.

Support networks must be available both from a regulatory and an economic perspective. The functionality of emergency preparedness functions supported by Network Level 3.5 are driven by NUREG-0696, "Functional Criteria for Emergency Response Facilities" (Reference 7). A loss of this functionality will result in an affected unit entering a limiting condition of operation as specified in their technical specifications. Such an occurrence requires compensating actions to be taken. Plant configuration management and other required regulatory records are increasingly hosted on Network Level 4. The ERDS as required by 10 CFR 50, Appendix E, "Emergency Planning and Preparedness for Production and Utilization Facilities" (Reference 8) is supported here. Plant maintenance and engineering modifications records and scheduling are accomplished using these tools. Inventory control for spare parts and consumables are also hosted here as are plant configuration control software tools. A loss of such capabilities can also violate nuclear plant technical specification limits and other NRC requirements. Necessary business financial software applications and human resources software tools, such as time accounting and payroll, are also hosted here.

It is the responsibility of the utility to establish quality control requirements for support networks at Network Levels 3.5 and higher. This includes the submittal of a specific Emergency Response Plan in accordance with "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans Prepared in Support of Nuclear Power Plants," NUREG-0654 (Reference 9). A specific ERDS implementation program plan, which must include, but is not be limited to, information on the licensee's computer system configuration (i.e., hardware and software), interface, and procedures per Reference 8, Section VI must also be submitted. Furthermore, any hardware and software changes that affect the transmitted digital data points identified in the ERDS Data Point Library (site-specific data base residing on the ERDS computer) must be submitted to the NRC within 30 days after the changes are completed.

As presented in more detail in Sections 4.5 and 4.6, these support networks, when fully integrated within the DI, provide a degree of current and potential future digital data gathering, correlation, and analytics capabilities that could not have been imagined when many of the existing commercial NPPs in the United States were built. The application of such capabilities is foundational to achieving facility and utility efficiency goals to enable sustained economic performance.

2.3 U.S. Nuclear Regulatory Commission Defined Cybersecurity Levels

The capabilities of the DI and the associated DA&A software suites at each Network Level as one, fully integrated set are myriad. Other industries have leveraged such a construct to revolutionize the operations and business models of their entire enterprise. While this has enabled the optimization of their activities to minimize cost and maximize economic competitiveness, it has also created a new threat. Cybersecurity attacks by malicious actors have damaged large corporations and hobbled government entities. To address this issue within the sphere of nuclear plant operations and emergency preparedness, 10 CFR 73.54, "Protection of digital computer and communication systems and networks" (Reference10) was established as a regulatory requirement for nuclear facilities. This is typically called the "Cybersecurity Rule." Reference 10 states in Section (a)(1) that each nuclear plant licensee shall provide high assurance that digital computer and communications systems and networks are adequately protected against cyberattacks. Licensees shall protect digital computer and communication systems and networks associated with:

i. Safety-related and important-to-safety systems

ii. Security functions

iii. Emergency preparedness functions, including offsite communications

iv. Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities" (Reference 11) establishes Cybersecurity Levels and further identifies the digital equipment that falls under the Cybersecurity Rule. The numbering of these Cybersecurity Levels is shown in the first column of Figure 3 and Appendix A and is generally the reverse of that used for the Purdue Network Level Model. A brief discussion of the different Cybersecurity Levels presented in Reference 11 is provided in the subsections below.

2.3.1 Cybersecurity Level 4: Plant Control and Monitoring Systems

Cybersecurity Level 4 includes Critical Digital Assets (CDAs) associated with safety, important to safety, and security functions, as well as support systems and equipment which, if compromised, would adversely impact safety, important to safety, and security functions.

Security functions and voice communication systems are not addressed in this document. While these systems are important, their function is fundamentally different than those used to directly monitor and control the plant. Quality requirements for these systems are also fundamentally different. This does not mean that such systems cannot share isolatable portions of the physical DI (e.g., use of separate optical fibers in a shared fiber-optic cable plant) so long as the appropriate physical controls are implemented to protect the shared resources).

Data communications between different systems at Cybersecurity Level 4 are not restricted from a cybersecurity point of view. Data Communications between safety-related and non-safety I&C systems at Cybersecurity Level 4, however, are further strictly controlled as defined in DI&C-ISG-04, Revision 1 "Highly-Integrated Control Room - Communications Issues (HICRc)" (Reference 17) to prevent any adverse impact on a safety-related system originating from a non-safety system. One-way transfers of plant status and I&C safety-related system status data to non-safety I&C systems are permitted so long as

this control is satisfied. This provides access to safety-related I&C data by the non-safety digital I&C system

Both safety-related and non-safety Cybersecurity Level 4 I&C CDAs are protected from other equipment in the DI at Cybersecurity Levels (3, 2, 1, and 0) by prohibiting any inward communications link from any of these lower Cybersecurity Levels to Cybersecurity Level 4. Processes to upload software and to connect portable maintenance and test gear to Cybersecurity Level 4 equipment are similarly strictly controlled to eliminate inward threat vectors.

Only one-way digital communications links (e.g. a data diode) outward from Cybersecurity Level 4 to Cybersecurity Level 3 are allowed.

2.3.2 Cybersecurity Level 3: Emergency Preparedness Network

Computer systems and networks that provide emergency preparedness functions are allocated to Cybersecurity Level 3. Plant data gathered from plant I&C systems at Cybersecurity Level 4 are passed through a one-way data diode to the Emergency Preparedness Network for it to be able to perform its function to support Emergency Preparedness Facilities (e.g. the TSC, OSC, and EOF).

Cybersecurity Level 3 also acts as a DMZ network. A DMZ network is used to connect hosts that provide an interface to an untrusted network. It passes Emergency Preparedness Network information (including plant I&C information it has received unidirectionally from Cybersecurity Level 4) to the Corporate Network Level 4 at Cybersecurity Level 2/1 as described in Section 2.1.

Offsite voice communications for emergency preparedness functions are not addressed in this document. While these systems are important, their function is fundamentally different than those used to directly monitor and control the plant. Quality requirements for these systems are also fundamentally different. This does not mean that such systems cannot share isolable portions of the physical DI (e.g., use of separate optical fibers in a shared fiber-optic cable plant) so long as the appropriate physical controls are implemented to protect the shared resources.

2.3.3 Cybersecurity Level 2/1: Corporate Network

The Cybersecurity Rule (Reference 10) does not apply to the higher levels of the DI (Corporate Network Level 4). Yet, this does not mean that the protection of Network Level 4 from cyberattack is unimportant.

Utility computer systems and networks are used to perform support, maintenance, and other functions (administrative, human resources, etc.). While these systems do not fall under the Cybersecurity Rule, these networks must be protected for corporate data confidentiality, integrity, and availability for the reasons presented in Section 2.2.2 above. As with quality, it is the responsibility of the utility to establish cybersecurity requirements for support networks at Network Level 4.

2.3.4 Cybersecurity Level 0: Internet

Utility computer systems and networks are typically provided internet access to support business functions. Nuclear utilities also use the internet to transmit plant data sourced from digital I&C systems at Cybersecurity Level 4, through the intervening Cybersecurity Levels (3, 2, 1) to the NRC ERDS. While the utility cannot control the cybersecurity features of the internet, tools can be employed to ensure secure communications on the internet (e.g. VPN tunneling, encryption, etc.). Mechanisms can be employed to protect the Corporate Network at its interfaces to the internet using industry available tools (firewalls, DMZs, communication scanning, etc.).

3. Design Tenets as Applied to the Digital Infrastructure Migration Framework

To establish a consistent direction in the development of a nuclear DI, a set of Design Tenets are proposed below for the DI Migration Framework. These Tenets support the technical development and

sustainability of the DI as well as the ION objective to enable the long-term economic viability of the industry.

1. To best visualize the breadth and depth of capabilities to be hosted by the DI, it is best defined in the context of a "New State." The New State DI addresses the full range of the physical and logical infrastructure to support New State DA&A capabilities that envelope all technical activities that make up ION. By directing the development and implementation of both the DI and DA&A capabilities toward this defined New State, metrics for expected TOC improvements can be established, evaluated using business case analyses, and used to direct achieving the "New State."
2. Ensuring the "New State" is not an "End State." This DI Migration Framework is formulated to support a full-scope, enterprise-wide DI modernization to enable SLRs to operate existing nuclear plants for a total of 80–100 years. The initial "New State" DI created to support SLRs needs to possess two fundamental properties:
    a) When initially achieved, the initial New State DI must be expandable to support DA&A innovations as capabilities in this area continue to be enabled by research and the availability of new products in the marketplace.
    b) The DI must be designed to be periodically "refreshed" with updated technology to address obsolescence in a systematic way:
        i) With no or very limited plant DA&A capability functional impact to direct plant production or business-related processes during a refresh.
        ii) So that intellectual property associated with DA&A capabilities is maintained by direct migration to the refreshed DI as much as possible. This must be done to eliminate or minimize additional creation, testing, and implementation costs associated with having to re-create that intellectual property because it is incompatible with the "refreshed" DI technology.

    The DI is maintained as "evergreen" and enhanced with new features by transitioning from the initial New State (e.g., a Version 1.0) to subsequent New States (e.g., Version 2.0 and beyond) as obsolescence is addressed during SLR periods. To achieve this end, the traditional linear thinking of performing upgrades (inception to retirement) needs to be replaced by a circular model that emphasizes continuous DI lifecycle planning. Without having such a digital obsolescence management strategy from the start, the DI will become increasingly more difficult and costly to maintain, and its reliability will degrade. DA&A intellectual property investments will increasingly run the risk of being lost. Expensive complete hardware and software system redesigns may then be required.
3. Vendor and technology selections associated with DI as well as DA&A capabilities are critical to enabling this evergreen capability. The use of stable vendors with deep and worldwide market penetration provides assurance that their technology and the expertise to support it will remain available well into the future. Technology selections should highly favor systems with a proven track record of backward compatibility and a well-developed and demonstrated lifecycle management strategy. This strategy should include leveraging vendor-developed and validated capabilities to efficiently harvest intellectual property associated with DA&A capabilities from legacy DI versions and validate the correctness of the migration of this when performing a refresh. As an example, for non-safety DCSs, vendors design their new equipment, software, and design tools in such a way as to support migrating of the intellectual property (software applications) from obsolete to new equipment and software operating systems. This is further described in INL/EXT-19-55799, "Addressing Nuclear I&C Modernization Through Application of Techniques Employed in Other Industries" (Reference 12). This significantly reduces the installation and testing costs of performing a "technology refresh" of the platform when compared to the legacy practice of performing complete

system replacements, including re-design, re-implementation, re-coding, re-verifying, and re-validating the application software. Safety I&C platform vendors have similarly identified techniques to manage digital obsolescence to reduce lifecycle costs.

4. Creating a multi-Network Level DI that allows for:
    a) Optimal DA&A software application functionality allocation based upon use (e.g., control system software applications are allocated to the proper Network Level [0–3] while non-control DA&A software applications are allocated to other Network Levels [3.5 and higher]).
    b) Controlled data flows between Network Levels that permit the efficient mass collection, aggregation, storage, trending, correlation, and analysis of all digitized data across the enterprise to maximize DA&A capabilities and associated operational/economic efficiency.
    c) Tailored application of regulatory and other requirements (e.g., quality, reliability, and cybersecurity requirements) based upon functions performed and placement of those functions within each DI Network Level to minimize implementation and lifecycle support costs.
5. Leveraging the capability of new digital systems to capture and correlate data from throughout the DI. Augmenting the existing functionality provides data and control capability previously unavailable to operators in the MCR. This can aid in eliminating remote stations and reducing workload. Trending, diagnostic, and prognostic features enabled by the availability of this data can be used to improve plant performance (produce more power) and reduce time-based maintenance activities and associated costs.
6. Supports an integrated human factors engineering (HFE) strategy. Application of HFE in the development of HSIs to directly monitor and control the plant in the MCR and other plant operating stations is required. The industry guidance most used to guide these activities is NUREG-0711, Revision 3, "Human Factors Engineering Program Review Model" (Reference 13). The fundamental object of HFE is to optimize human performance in the monitoring and operation of the plant and minimize human performance errors. Reference 13 is proscriptive with regard to the steps to be performed when performing I&C upgrades at Network Level 2 as shown in Figure 3. These steps include:
    a) HFE Program Management
    b) Operating Experience Review
    c) Functional Requirements Analysis and Function Allocation
    d) Task Analysis
    e) Staffing and Qualifications
    f) Treatment of Important Human Actions
    g) HSI Design, Including the Development of HSI Style Guides
    h) Procedure Development
    i) Training Program Development
    j) Human Factors Verification and Validation
    k) Design Implementation
    l) Human Performance Monitoring

    A graded approach as allowed by Reference 13 is performed to achieve this end. This approach must provide for a flexible solution for the MCR that supports both the interim DI upgrade states and the

envisioned New State for the MCR. This is because MCR upgrades associated with DI and DA&A implementations will likely occur over several plant outages over a period of years. Each interim state must be able to stand alone when it comes to demonstrating its capability to safely operate the nuclear plant per Reference 13. At the same time, the objective is to fully leverage interim state modifications without further alteration when working toward the New State to minimize rework and associated costs.

When implementing a more comprehensive DI and associated DA&A capabilities, HFE concepts need to be extended as good engineering practice beyond the realm of traditional I&C to include HSIs at Network Levels 3.5 and above. As shown in Figure 3, capabilities provided by DA&A software applications on the Corporate Network Level 4 will be accessible in the MCR. Examples of this include work-management software applications, results of plant health monitoring software applications, and weather information. Non-control capable facsimiles of MCR displays (software generated images presented on hardware video display units [VDUs]) will be available on the Corporate Network along with additional displays populated with data either directly from the Emergency Preparedness Network (Network Level 3.5) or created from the analysis/synthesis of Network Level 2 data in the form of Management Dashboards. How HSIs for these capabilities are developed and integrated as part of the DA&A capabilities hosted on the DI must be accomplished in a way that enhances safety, reliability, while enabling continuous improvement in the area of efficient plant operations through:

- Standardization of physical devices (VDUs) that provide the HSIs
- Standardization of how DA&A software applications are hosted on the DI HSIs (e.g., thin clients, fat clients, workstations, etc.)
- Standardization of the DA&A software applications that graphically present information on the VDUs
- Standardization of the graphical images themselves using HSI style guides, including mechanisms to clearly differentiate displays of different types (e.g., Network Level 2 I&C control displays from Corporate Network Level 4 information displays)
- Establishment of policies and procedures with regard to HSI use in an environment where displays from multiple Network Levels (e.g., Levels 2 and 4) are necessarily available simultaneously (e.g., the MCR)

7. Leveraging the enhanced reliability and availability of digital technology. Using proven Network Level 1 and 2 technology significantly reduces the potential for I&C platform induced maloperation (e.g., operating system errors). Use of vendor validated DA&A structured programming tools such as function block programming of I&C control algorithms along with validated software testing tools and processes greatly reduces the potential for application software to contain design errors (software does not “fail”). System redundancy and graceful degradation capabilities designed into modern systems address system failure modes. Self-diagnostics capabilities perform active monitoring to detect system I&C system issues. These features, coupled with increased component reliability and component count reduction when transitioning from analog to digital (particularly in I&C where component counts can be reduced by up to 75%), will significantly improve plant reliability and availability.
8. Standardizing designs to the maximum extent practical across the entire DI provides the following benefits:
   a) Standard building blocks (hardware and operating system software) support supply chain consolidation.

b) Standard development tools as well as standard design processes reduce costs to implement, maintain, and configuration control of the DI and DA&A software applications.

c) One, overarching cybersecurity defensive strategy for the DI and associated DA&A can be developed and maintained with controls tailored toward specific requirements for each Network Level. For example, all system functions of obsolete digital systems migrated to the non-safety DCS will be enveloped by one cybersecurity defensive strategy built into that platform as opposed to maintaining the disparate cybersecurity efforts currently applied to each individual legacy I&C system.

9. Minimizing I&C system acquisition and lifecycle costs for modernization by driving I&C modernization efforts toward using only two digital platforms This is accomplished by:

   a) Consolidating the functions of existing safety-related I&C system functions onto one safety-related I&C platform. The safety platform is expected to be expandable to be capable of hosting most of the safety-related functions in the unit, within the hardware capabilities of the utility selected vendor product.

      By using software application code to perform logic functions and through the elimination of redundant equipment in the disparate systems to be combined into the safety I&C platform, component count can be reduced dramatically. This will also reduce surveillance and calibration costs for maintaining the equipment as well as acquisition, installation, and lifecycle support costs (including supply chain costs) for obtaining replacement parts and keeping them in inventory.

   b) Consolidating existing non-safety I&C system functions onto one non-safety DCS. Additionally, any necessary RPS diverse actuation system (DAS) functionality should be implemented on a non-safety DCS segment (as explained in Section 4.2.2.1 (c) below). It is presupposed that a diversity and defense-in-depth analysis of a digital RPS based on NUREG/CR 6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems" (Reference 14) and "Branch Technical Position Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," BTP-7-19 Revision 8 (Reference 15) will determine that DAS functionality is required to address the potential for a common cause failure of a digital safety I&C platform. Even if additional DAS functions are not required for the RPS functionality, anticipatory transient without scram (ATWS) functionality is required by 10 CFR 50.62 (Reference 27). By consolidating ATWS and necessary DAS functionality as separate segments on the single envisioned non-safety DCS, there is no need for an additional, separate I&C system to host DAS/ATWs functionality.

      Consolidating non-safety I&C functionality, including DAS/ATWS functionality, on a DCS reduces unique equipment types to reduce costs while providing necessary equipment diversity. This is the approach that is further developed INL/EXT-20-61079, "Vendor-Independent Design Requirements for a Boiling Water Reactor Safety System Upgrade" (Reference 16).

   By maximizing the use of these two platforms, standard design methods can be employed to reduce implementation costs. Maintenance and operator training, inventory control, obsolescence management, and other lifecycle support efforts are vastly simplified by consolidating I&C functions onto one safety I&C platform and one non-safety DCS.

10. Providing a standard, shared, safety qualified HSI architecture that provides for a flexible solution for the MCR that supports both the interim states and the envisioned hybrid New State for the MCR. A minimal number of manual switches and hardwired indications for the RPS remain in the MCR. The remaining manual hardwired RPS switches and indications are retained as diverse backups for the RPS itself. The remaining hardwired switches act directly to execute such functions as a reactor scram by deenergizing the primary scram solenoid pilot valves and energizing the backup scram valves. All other operator interactions use soft controls on the video displays. The HSI architecture design concept developed as described in Section 3.6.3 of Reference 16 leverages a commercially

available design example that is expected to meet the cybersecurity requirements of 10 CFR 73.54, (Reference 10) and the communications precepts of DI&C-ISG-04 (Reference 17). This is further discussed in Section 4.3.3 below.

By driving I&C modernization efforts to the use of two standard I&C platforms, HFE activities can also be standardized, with resultant HSIs being more easily harmonized and presented on the shared HSI architecture to provide a more consistent and universal operator experience.

11. Reducing direct operating and maintenance (O&M) costs associated with sustaining the replacement I&C systems for up to an 80-year plant life. Several digital platforms approved for safety I&C use by the NRC include advanced fault detection and self-diagnostics features to minimize O&M costs when compared to current analog systems. The NRC has approved the use of such features to eliminate Technical Specification surveillance requirements (Reference 18) for safety-related digital equipment in new plant designs (i.e., Westinghouse AP1000®). These features, coupled with proper system design, identify failures down to the affected field replaceable unit, which can then be replaced while the plant remains online, again improving system and plant reliability and availability. All modern digital non-safety DCS platforms have such capabilities. By design, both digital platforms eliminate analog equipment calibrations for the equipment they replace.
12. Enabling a "design once, build many" approach. Methods and techniques described in this report for the development of the DI and DA&A applications along with HTI efforts, are directly transportable to all nuclear sites within a utility enterprise. By leveraging them in this way, the maximum benefits afforded by ION can be achieved, particularly for a utility that operates a fleet of NPPs. An example of potential value of employing concepts similar to ION in the North Sea oil and gas industry is provided in Section 3.1.1 of Reference 1. Forecasted benefits for this oil and gas industry example are in the tens of billions of dollars with a 10× return on investment

4. Purdue Model Digital Infrastructure Levels and Capabilities

The following subsections describe generic features and capabilities of each level of the DI following the Purdue Network Model as depicted in the simplified Figure 3 diagram above and in the more detailed diagram provide in Appendix A below. It is suggested that the reader have a copy of these two diagrams separately available for cross-reference when reading this section.

To promote a comprehensive understanding of the DI, the layers and their associated functionality are presented below from the bottom-up with discussion of the connectivity between each successive layer. It should be noted that significant benefits can be realized through a top-down and/or partial implementation of the DI. For example, capabilities at Level 4 Corporate Network, as described in Section 4.6 below, can be implemented independent of the lower levels of the infrastructure to provide organizational and related financial benefits.

The purpose of this section is to augment the summary information concerning functionality at each Purdue Model Level given in Section 2.1 by:

- Providing a general overview of DI technology at each Network Level for a nuclear plant
- Describing the configuration of each Network Level to support its function and hosted DA&A software applications
- Generically describing the capabilities of envisioned DA&A software applications at each Network Level to maximize the use of digital technology to support ION
- Describing the intended portability of software-based DI configuration and hosted software applications to support DI obsolescence management at each Network Level
- Discussing HSI resources at each Network Level.

A more detailed development of the suite of envisioned DA&A software applications at each level to support ION will be the subject of a companion research report to be developed in the future.

When reading the subsections below, it needs to be understood that digital I&C systems used in safety-related applications are typically either purpose-built or adapted in such a way as to meet NRC requirements for safety and reliability. To accomplish this end, well-understood, proven technology and simplified designs are leveraged as much as possible. While this is necessary and appropriate, one of the outcomes of such an approach is that digital technology used and capabilities supported by digital safety-related systems and applications typically lag behind those supported in the non-nuclear process control industry worldwide. The discussions of DI layers and capabilities provided in this section are generically based on the non-nuclear process control industry. Safety-related I&C systems possess similar features in some cases and not in others. For example, safety-related I&C systems may use commercial/industrial computer operating systems and multi-function capable software, but such use is implemented leveraging nuclear industry specific guidance, such as Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," (Reference 19). Other safety-related I&C systems use digital technology, such as Field-Programmable Gate Arrays (FPGAs). While the concepts presented in this section are also generically applicable to safety-related digital I&C systems, they may not directly align with safety-related I&C system capabilities.

Also, when reading the subsections below, it needs to be understood Digital Systems at Network Level 2 and above typically apply available IT used in larger business applications. Configuration of such equipment and the software that runs on it is controlled based upon its function within the architecture.

The information provided in the presentation of Network Level 0–2 is informed by the technology studied by LWRS researchers as described in INL/EXT-19-55799, "Addressing Nuclear I&C Modernization Through Application of Techniques Employed in Other Industries" (Reference 12).

4.1 Network Level 0: Field Devices

This section primarily focuses on the attributes of non-safety DCS field device digital technology implementations. For safety system I&C protection and ESFAS functions, the vast majority of field devices are analog or simple digital (logic 1 or 0) with little or no capability to host DA&A features.

4.1.1 Interface to I&C Systems - Configuration

Network Level 0 electrical field devices are directly connected to plant process. They are the intersecting point between I&C systems and the processes they monitor and control. These include items such as level, flow, temperature, and position detectors as well as motor controllers, valve controllers, and circuit breakers). Field devices communicate status information to and receive control signals from Network Level 1 in either an analog, simple digital (logic 1 or 0) or via a digital protocol format.

Digital field devices can be configurable. Some are only configurable when manufactured. Others can be configuration capabilities that can be leveraged by a technician or system administrator. Configuration may be accomplished by directly using a separate, portable device developed for this purpose, or though Network Level 1 or 2 interfaces to device level networks (e.g., Fieldbus, Modbus, PROFIBUS).

4.1.2 Human-System Interfaces

Many field devices provide direct HSIs. Motor and valve controllers typically provide the capability for the direct control and indication of device status (motor running, valve position). Digital sensors often provide direct indication of the monitored parameter and some can even provide indication of status context with regard to setpoints. Device fault conditions may also be displayed. Such interfaces are typically very simple and offer very limited capability for configuration change (such as conforming the device HSI to a HSI style guide).

4.1.3 Data Architecture and Analytics Features Hosted at this Network Level and Associated Portability

Some digital field devices can be programmable and can even perform simple control functions when connected directly to other field devices. This can be accomplished with FPGA technology or with software. Manufacturers of devices that support end user configuration/programming of devices typically support the retention of this configuration/programming so that if a device fails or is replaced due for other reasons (obsolescence), the functionality of the new device can be established by restoring the programming of the original device using the same or similar tools used for programming the original device. This is similar to the programming of controllers at Network Level 2 as discussed in Section 4.2 below. This portability should be validated by the vendor when going from an existing to a replacement device. By design, DA&A capabilities are limited and directed solely to support I&C functions.

4.2 Network Level 1: Control Network (Local Control)

4.2.1 Input/Output Modules (I/O Modules)

This section primarily focuses on the attributes of non-safety DCS I/O module digital technology implementations. For safety system I&C protection and ESFAS, the vast majority of I/O capabilities are analog or simple digital (logic 1 or 0) with limited capability to host advanced DA&A features.

4.2.1.1 Input and Output Signal Processing Modules - Configuration

Network Level 1 is the foundation of digital I&C systems. It is where signals are received from the field for the purpose of monitoring and controlling connected devices. At this level, field signals are received either in a digital or analog format. Input modules process this data and translate it into the native digital format for the I&C system developed by the vendor selected by the utility user.

Output modules process control signals they receive and provide either analog or digital outputs as necessary to field devices to affect control.

4.2.1.2 Input/Output Communication Modules - Configuration

Input/output signal processing at the I/O module level often uses separate, input/output communications modules mounted in the same chassis as the input/output signal processing modules. Digital communications between the I/O modules at Network Level 1 and Network Level 1 local controllers is typically accomplished via redundant, dedicated I/O links to redundant local controllers for both data acquisition and control functions. These redundant links connect the I/O modules with I/O processors in the local controllers that are independent of controller processors that execute control algorithms.

4.2.1.3 Data Architecture and Analytics Features of Input/Output Modules and Associated Portability

For DCS's, I/O module configuration and diagnostics are performed using purpose-built software tools developed for the DCS. I/O modules are configured to calibrate analog inputs and outputs. Alarm and warning values for inputs can also be set for analog and digital inputs. Fail-state outputs to controlled field devices can also be established. This provides for placing controlled devices at Network Level 0 in a pre-programmed fail-state should communication between Level 1 controllers and the I/O modules be interrupted.

Should an individual I/O module fail, a replacement can typically be "hot swapped" by simply removing and replacing the failed component. The new I/O module can be reconfigured using the same utility software tools used to configure the original module. Most industrial control systems also store the configuration of each module in the system. This can be manually pushed by a system administrator to the replacement I/O module. If desired, most industrial control systems can also be configured to automatically restore the configuration of a replacement I/O module simply by inserting the new module into the system. I/O modules are typically not redundant. Loss of an I/O module or an I/O chassis results

in the loss of control system function and operator view and control of connected Network Level 0 devices.

There is typically no capability for the insertion of separate data analysis and analytics software feature at the Network Level 1 I/O module level beyond that provided by the manufacturer and summarized in this section. To add non-native software to a DCS at this level will violate the manufacture standard configuration and void vendor guaranteed performance characteristics.

DCS I/O modules are typically custom designed by each control system manufacturer as part of a product line. They are designed to function, are produced, and supported for extended periods of time (typically ~20+ years) to protect against obsolescence. If replacement I/O modules are unavailable, newer models typically must be configured using the purpose-built software tools associated with the newer product line.

4.2.1.4 Input/Output Module Human-System Interfaces

Limited HSI capability is directly provided at this level. Typically, Network Level 1 devices display simple status information with regard to controller operation (either normal or fault indications to facilitate troubleshooting). Fault conditions in Network Level 1 I/O modules are typically communicated to local controllers which then forward them for presentation on control system VDU HSIs higher in the control system architecture. Portable HSIs can also be used to access this information if the I&C platform design supports this function.

In certain special cases, HSIs are provided at purpose-built output modules. For example, the safety-related Westinghouse Component Interface Module® (CIM) has the capability for an operator to provide a direct input at the module to actuate a connected device. This bypasses all software-initiated commands provides as inputs to a CIM.

4.2.2 Local Controllers

4.2.2.1 Non-Safety Control System - Configuration

For DCS's, Network Level 1 local controllers make up the heart of the functionality of the control system. In order to properly apply vendor DCS technology for a non-safety implementation in a nuclear plant at Network Level 1, several interrelated topics are required to be addressed. These are shown pictorially in Figure 4 and described below:

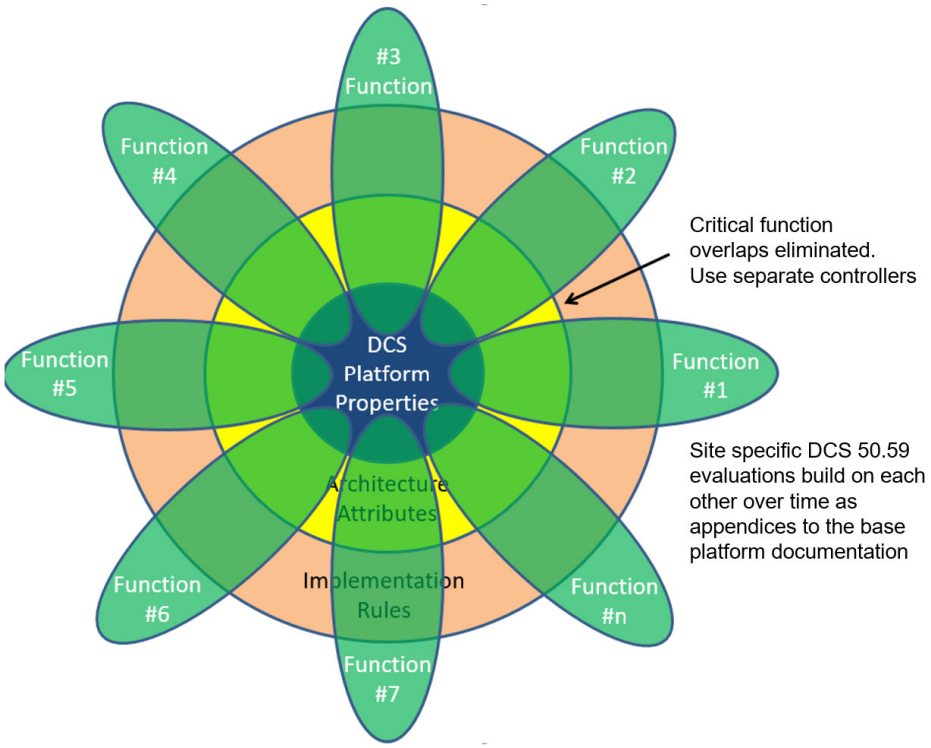


Figure 4 – DCS Design Property Utilization and Control System Application Strategy

a) The intrinsic properties of the particular vendor's technology

Vendor-developed DCSs include platform properties (shown in blue in Figure 4) that are independent of the particular use envisioned by a customer. Utility DCS platform selection is largely influenced by these platform properties at Network Level 1. Some generic key properties as identified in a utility Software Hazard Analysis (Reference 20) performed on a DCS include (but are not limited to):

- Technical Properties
  - Controller operating system properties (demonstrated use in industry, robustness, controller process separation features, integration with application software development tools, management of controller resources, process time management, processor task priority, and deterministic execution of control algorithms)
  - Controller I/O scan rates and processor execution rates. These can be set at different time intervals based upon process need, thus optimizing overall use of processor resources
  - Online diagnostics including (but not limited to)
    - Analog input health monitoring (signal quality)
    - Controller time synchronization monitoring (compared to system time)
    - Hardware watchdog timers that detect failures that disrupt controller instruction execution
    - Control algorithm execution task monitoring
    - Monitoring of tasks critical to enabling the operator to properly supervise processes

        - Divide by zero error detection
        - Program execution infinite loop monitoring
        - Communication monitoring and failover to alternate communications paths
        - Detection and correction of single-bit memory errors not induced by hardware failures
        - Detection and report of uncorrectable hardware single-bit memory errors
        - Controller failure on multi-bit hardware memory errors
      - Controller redundancy capability and failover characteristics (e.g., bumpless transfer)
      - Structured, pre-validated configuration and application programming tools that also detect errors associated with these two activities.
  - Lifecycle support properties as identified in Reference 12, including:
      - Demonstrated ability to support backward compatibility to incorporate legacy devices without modification
      - Demonstrated and validated capability to migrate controller programs from legacy devices to current products without impacting the original function of that program when performed on the current product
      - Well established technology migration strategies to address hardware and software obsolescence that have been demonstrated through past experience and provide a defined roadmap for future migrations.

b) A utility's DCS requirements and how these are combined with the vendor's technology into DCS architecture attributes

Control system vendor provided DCSs are essentially infinitely configurable. Specific DCS capabilities often depend upon how components are configured. Key DCS platform attributes for nuclear control system implementation at Network Level 1 include:

- The ability to allocate particular plant functions to individual controllers. Functions can be segmented on separate controllers. Functions so segmented can be configured such that that they can operate completely independent of each other and the independently of the DCS system clock. If isolated from the DCS, they will continue to function in automatic or place the isolated segment in a known, pre-programmed condition.
- The ability to support equipment redundancy to mitigate single failures and provide for graceful degradation of system performance in the event of multiple failures. Such redundancy at the controller level can also support performing software updates or controller replacement online without interrupting controlled system operation.
- Communications devices that connect Network Level 1 controllers to Network Level 2 devices can be configured to establish communications redundancy, minimize and bound the time to accomplish communication failover, and also to protect the controllers should there be improper Network Level 2 function.

Such specific architecture configuration attributes are established for Network Level 1 by the utility through collaboration with their DCS vendor. These attributes as depicted in yellow in Figure 4 are tailored based upon the particular DCS implementation by establishing configuration work instructions developed and applied to produce the final Network Level 1 architecture. These configuration instructions must be enveloped within the vendor specified bounding configuration so that specified DCS performance is assured.

c) Establishing rules for how legacy I&C functionality is moved to the DCS to address the particular plant's licensing basis

Specific configuration of architecture attributes is necessary to satisfy particular plant control system needs. For example, the selected DCS platform may include features (e.g., time sequenced batch process control) that, if utilized, could violate a design tenet (e.g., process control shall not rely on a single system clock). Certain processes may be significant enough to require redundant controllers. One way to ensure such configuration decisions are properly implemented is through the creation and imposition of design rules. These are shown in Figure 4 above in orange. As a specific example of rule implementation, legacy control system functional segmentation, as mentioned in (b) above, is either directly described or inferred in a nuclear plant's licensing basis as captured in its Final Safety Analysis Report (FSAR). To maintain such functional segmentation, rules are established to ensure that separate functions so described in the plant FSAR are not combined on a single controller segment such that a software or other failure affecting that segment creates a new malfunction or a malfunction with a different result than that previously analyzed in the FSAR. This segmentation is consistent with the functional segmentation developed for Watts Bar Unit 2 (Reference 21) and the related Watts Bar FSAR addressing it (Reference 22). This segmentation is shown for multiple segmented functions in the green portions of Figure 4 above. Such individual non-safety DCS segments are represented by Interface Case 2 on the bottom-right of Appendix A as well as on Figure 3.

In order to satisfy the need to provide a diverse means of establishing and maintaining safe shutdown in the unlikely event of a common cause failure of the safety-related I&C platform, a separate non-safety DCS segment (or segments) can also be used through safety-grade interface devices such as a Westinghouse CIM that permit component-level control of safety-related field devices from the non-safety DCS. Such a segment is represented by Interface Case 2 on the bottom-right of Appendix A as well as on Figure 3.

Documentation of architecture configuration must be retained and maintained so that when components at this level are replaced, their replacements maintain or enhance the configuration attributes established when the original equipment was installed. Vendors typically continue to provide existing configuration enabled capabilities when the next generation of this equipment is offered along with enhancements, which customers may choose whether or not to implement. Vendors also often offer tools that capture the existing platform configuration directly from the DCS. This information can be used to pre-configure replacement components to ensure configuration-enabled capabilities are retained by the new hardware.

DCS's also offer advanced self-monitoring and diagnostic tools as part of their standard offering. These tools are closely coupled with system configuration tools. In most cases, failed components are identified down to the line-replaceable unit to facilitate ease of repair.

With all these configuration decisions made, software application code can be developed to enable monitoring and control functions enabled by Network Level 1 controllers. This is discussed in Section 4.2.2.3 below.

4.2.2.2 Safety-Related Control System - Configuration

Safety-related digital control systems used for the purposes of RPS and ESFAS can also be configured using software tools that satisfy NRC inspection guidance for software development (i.e. NUREG 0800 [Reference 5], Chapter 7 "Instrumentation and Controls," including BTP 7-14, "Guidance on Software Reviews for Digital, Computer-Based Instrumentation and Control Systems," [Reference 19]). Similarly, FPGA systems can also be configured by use of software tools. NRC guidance for using software to perform this configuration is provided in NUREG/CR-7006, "Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems" (Reference 23) and NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems" (Reference 24).

To minimize implementation costs and licensing risk, utilities considering safety-related I&C control system upgrades are looking to leverage existing digital platforms that have received a favorable Safety Evaluation Report from the NRC. Examples of such pre-qualified and available digital, safety-related I&C platforms include:

a) Schneider Electric: Tricon V10

b) Westinghouse: Common Qualified Platform (Common Q)

c) Rolls-Royce: Spinline 3

d) Mitsubishi Electric: Total Advanced Control (MELTAC)

e) General Electric: NUMAC

f) Doosan: HFC-6000

g) Lockheed Martin: NuPAC (FPGA technology)

h) RADICS LLC and Curtis-Wright: RadICS (FPGA technology)

i) Westinghouse: Advanced Logic System (FPGA technology)

Documentation of the safety-related architecture configuration must also be retained and maintained so that when components at this level are replaced, their replacements maintain or enhance the configuration attributes established when the original equipment was installed.

Digital safety-related I&C systems also offer advanced self-monitoring and diagnostic tools as part of their standard offering. An example of where such tools can be leveraged to lower costs associated with performing legacy surveillance activities is provided by Reference 18. These tools are closely coupled with system configuration tools. In most cases, failed components are identified down to the line-replaceable unit to facilitate ease of repair.

With safety-related configuration decisions made, software application code can be developed to enable monitoring and control functions enabled by Network Level 1. This is discussed in Section 4.2.2.3 below.

4.2.2.3 Data Architecture and Analytics Features of Local Controllers and Associated Portability

Each control system vendor has developed a suite of software programming tools to implement monitoring and control functions for serviced system processes. These validated tools can provide functional control across the full range from manual to fully automated as supported by connected field devices. These tools are either directly applied to produce software applications that will run on digital controllers (non-safety and safety-related software programmable systems) or they are used to create programming that can then be implemented on FPGAs.

DCS vendors typically provide a fully developed, extensively tested, function block library that provides a host of pre-programmed control functions that covers the breadth of control functionality to support customers worldwide. These function blocks are arranged to create monitoring and control applications that are thoroughly tested prior to installation. These systems are essentially infinitely configurable within the DI bounds established by the vendor. These bounds include capacity limits (e.g., number of unique data points monitored, network throughput, memory, processing capabilities) and control of the system configuration within the vendor-defined envelope where performance has been tested and guaranteed. Custom programming outside of the capabilities supported by the vendor provided toolset is not recommended, as there is no vendor guarantee that such applications will perform properly without custom testing or that such application s will migrate from one controller type to another as provided by the same vendor. The addition of non-native software at this level of a DCS will also typically void DCS vendor guaranteed performance characteristics.

Safety-related control system vendors provide software tools with similar programming tools. When compared to the tools and associated application capabilities as provided for a non-safety DCS, safety-related tools and features are limited. This is largely driven by the exhaustive and unique documentation and testing requirements for safety-related configuration and application software tools as well as applications developed with those tools. As an example, in Item (f) of Section D.4.2.1.6, "Software Design" of "Digital Instrumentation and Controls Interim Staff Guidance #06, Licensing Process," Revision 2 (Reference 25) it states:

> *The software design should describe how adequate coverage of software requirements is achieved. There should be no unnecessary functions. Predeveloped digital platforms and preexisting software (e.g., operating system software) may contain features that are not used (or not configured for use) in a specific DI&C system. In those cases, the NRC staff should verify that, unless otherwise demonstrated as part of a platform topical report approval, the licensee has identified those unused capabilities. The staff should evaluate whether those functions may affect the performance of the safety function and identify any compensatory measures taken.*

The net effect of this is that only necessary and sufficient capabilities of software directly used for safety-related I&C configuration and application development are provided. In nearly all cases, legacy safety-related I&C application functionality at the channel and division level of the architecture (as shown in the block diagram at the bottom left of Appendix A) is retained along with limited improvements.

For both non-safety DCS and safety-related I&C implementations, the effort to develop requirements for Network Level 1 software applications, to code them, and to then verify and validate their functionality represents a significant initial economic investment. For this reason, utilities need to be deliberate in their lifecycle planning efforts, ensuring vendors they select have a defined strategy to harvest Network Level 1 software application intellectual property investments. A specific non-safety DCS vendor's Level 1 Control Network hardware and related software lifecycle support strategy is summarized as a representative industry example in Appendix B, "Pilot Vendor Platform Lifecycle and Backwards Compatibility Management" of Reference 12. While lifecycle support strategies for safety-related Network Level 1 control hardware and software may be different in execution based upon system design and regulatory constraints, they need to achieve the same end with regard to application software harvestability.

4.2.2.4 Human-System Interfaces

Direct inputs (e.g., switches or pushbuttons) by the operator to initiate specific system-level actions (e.g., isolate containment that requires more than one valve actuator to operate) are Network Level 1 HSI input devices.

For non-safety DCS's, very limited HSIs display capability is directly provided at this level. Typically, Network Level 1 devices display status simple information with regard to controller operation (either normal or fault indications to facilitate troubleshooting). DCS fault conditions in Network 1 modules are typically communicated to higher levels of the DCS architecture.

Local DCS HSI operator display screens can be distributed within a nuclear plant to be in close proximity to particular plant systems to facilitate local operation. These are shown at the bottom-right of Figure 3 and Appendix A. While these support Network Level 1 functions, it is accomplished using VDUs connected to Network Level 2 as described in Section 4.3.3 below. Configuration of DCS Network Level 1 devices is normally also accomplished at the DCS engineering workstation shown at the right at Network Level 2. This is also described in Section 4.3.3 below.

Safety-related software to support operator HSIs is allocated to Network Level 1 in this report. This is because for safety-related systems, these functions are supported within the individual Network 1 channels and divisions. The concept of larger supervisory control functions does not readily conform to the supervisory control schema as ascribed to Network Level 2 for a DCS. The VDUs in the MCR used

to perform HSI functions for safety-related platforms are depicted at Network Level 2 because the MCR is the station that provides supervisory control. Safety-related diagnostic HSI software can also depict safety system equipment status either on the MCR VDUs or on other VDUs dedicated for that purpose. Portable HSIs may also be connected to safety-related I&C equipment to retrieve diagnostic information, perform troubleshooting, and make configuration changes.

4.3 Network Level 2: Supervisory Control

Network Level 2 provides two primary supervisory control functions. These include:

1. The capability of the operator to view Network Level 1 processes connected to the non-safety DCS and the safety-related I&C platform, respectively
2. The capability of the operator to control Network Level 1 processes.

Subsections 4.3.1 and 4.3.2 focus on non-safety DCS capabilities and HSI used for supervisory control.

As explained in Section 4.2.2.4 directly above, supervisory control at Network Level 2 for safety-related I&C systems at Level 1 is focused on supporting HSIs in the MCR only. This safety-related HSI support is explained in more detail in Section 4.3.3 below.

4.3.1 Configuration

As shown in Appendix A, the DCS supervisory network is conceptualized as a multi-redundant and virtualized system made up of two Physical Server Blocks (1 and 2) with a redundant network capability (Network Level 2[A] and 2[B]). While similar functionality can be achieved without using virtualization, the resulting footprint of the equipment (number of separate physical devices, the space they take up, the power they consume, the heat they produce, and the effort to configure and maintain them) will be higher.

Redundancy is provided for two fundamental purposes. The first is to ensure continued operation should failures occur. All single DCS hardware failures and many failures of more than one physical component or communications path can be tolerated without any loss of supervisory control function. The second is to leverage this failover capability in a controlled manner to promote periodic "technology refresh" up to and including the complete replacement of Network Level 2 DI equipment and associated utility software. This is further explained in Section 4.3.2 below.

As shown Appendix A, the safety-related I&C platform can forward digital process control data to the DCS supervisory network. This allows for the correlation of both safety-related and non-safety-related digital data to be time-stamped and aggregated in the DCS in redundant DCS data servers.

Configuration of DCS Network Level 2 and Level 1 devices is typically accomplished from a DCS engineering station. This is shown as being provided by a thin client HSI shown on the right edge of Appendix A directly above Physical Server Block #2 along with a corresponding virtual machine in at the top of PCN1:1A' in Physical Server Block #1. The DCS engineering station is loaded with specific software that provides capabilities to create and load graphics displays, upload and download device programs and configurations, and DCS data server database management. The engineering station is typically inactive during normal DCS operation. Access to it is strictly controlled.

The configuration settings of non-safety DCS equipment is backed up in shared storage shown in Physical Server Block 3 at Network Level 3 in the DI. This is discussed more in Section 4.4.2.

Most DCS vendors use commercially available IT equipment and software tools to construct Network Level 2. While this helps control cost and helps provide for equipment supplier supported lifecycle support strategies, it presents a potential hazard to system performance. Most IT hardware is procured from third parties (e.g., IBM, Dell, Cisco) and are highly configurable. Associated utility software (virtualization software, operating systems, etc.) comes in many different versions. DCS vendors go to great lengths to establish tight configuration control measures on the IT equipment used, down to the make, model, version, and even the specific chipsets used. The same is true for utility software and

vendor specific configuration software. They do the same with regard to bounding the specific configuration settings for this equipment. Exhaustive testing of these specific configurations to establish bounding capabilities are then performed. This allows the vendor to guarantee system performance so long as a particular system configuration is constrained within these bounds. Any configuration outside those tested by the vendor, including such seemingly mundane tasks as applying Microsoft Windows operating system patches provided by Microsoft to the general public, can void guaranteed system performance. These bounding configurations are also considered to be part of establishing and maintaining architecture attributes as depicted in yellow in Figure 4. For this same reason, the addition of non-native applications or clients not specifically tested by the vendor should be prohibited by rule as depicted in orange in Figure 4.

4.3.2 Data Architecture and Analytics Features and Associated Portability

The key applications hosted at Network Level 2 are the DCS data servers and the HSI workstations. The DCS data servers collect and distribute data between DCS Network Level 1 controllers (and their associated I/O) and HSI workstations to affect monitoring and control from those workstations. The server application is a complex software construct that fully instantiates every data point in the DCS. This includes controlling data flow. The data servers are also capable of being fed data from other digital systems and software applications. For example, safety system data points can be captured and correlated in the servers as transmitted through the data diode installed between the two systems for this purpose. This safety system data becomes additional data points on the server. It can do the same for data transmitted to it from other digital networks (within Cybersecurity Level 4). This data is typically captured within a Cybersecurity Level 4 data historian such as OSI/PI® as used by the nuclear industry hosted at Network Level 3 (see Section 4.4.2 below). While it is technically possible for non-native server data points to be used for control by the non-safety controllers, this is not recommended and should be controlled by rule (shown in orange in Figure 4). This is because such use may violate FSAR segmentation as discussed in Section 4.2.2.1(c). Also, the latency of the data being provided from non-native data points to the Network Level 1 DCS controllers may be such that it is not suitable for affecting control.

DCS HSI workstations are enabled by software generated graphic displays. These graphic display files are also hosted on the DCS server and accessed by the HSI workstations associated with the DCS server. Associations between data points used within graphics displays and the data points on the DCS data server are managed by the DCS server.

Due to the dependence of Network Level 2 functionality on the DCS server, the server is fully redundant. In the virtualized architecture shown in Appendix A, a virtualized Primary DCS server is hosted on one physical device in Physical Server Block #1 with its backup hosted on Physical Server Block #2. Failover to the backup DCS server occurs automatically should the primary fail.

When migrating the DCS to new hardware and/or updated versions of the DCS software suite, it is imperative that the DCS server migration be accomplished in an error free manner. For this reason, DCS vendors develop error checking migration programs to validate that server migrations are successfully executed.

DCS vendors also provide for coordinated Network Level 2 supervisory control functions across multiple Network Level 1 controller segments. This is particularly useful outside of the nuclear industry when performing coordinated batch control where one process control segment produces a product that is then supplied to a separate process control segment in a production line or when separate related process segments are geographically separated. Such coordinated control can be implemented in the nuclear industry so long as a failure of the supervisory control algorithm does not create a new malfunction or a malfunction with a different result as captured in the plant's FSAR. Such use of supervisory control functions should be controlled by rule (shown in orange in Figure 4).

Virtualization of all software Network Level 2 DA&A applications as shown in Server Block #1 and #2 along with the redundancy offered by this configuration supports complete migration of this intellectual property from one physical and associated utility software instantiation on the DI to another. Such migrations are performed outside the nuclear industry while the process under control still operates. All of the virtual machines at Network Level 2, along with the associated DCS configuration can be exported, migrated, loaded on new hardware, validated in a staging area, and then installed by sequentially replacing Server Block #1 followed by Server Block #2. This process is explained in detail in Appendix A of Reference 12.

4.3.3 Human-System Interfaces

As legacy I&C functionality is transitioned to the digital safety platform and non-safety DCS, Network Level 2 VDUs will become the primary means for operators to supervise and control the plant. HSI workstation VDUs at this level provide the capability for an operator to access and navigate through display pages created with software graphics packages that are developed in concert with either the non-safety DCS or the digital safety platform.

In order to harmonize the VDU-based HSI's, the safety and non-safety software graphics packages need to be able to present similar functional information to operators in similar ways so as to be consistent with each other and with remaining non-VDU-based controls and indications. This is necessary because it is expected that MCR modernization will occur as a multi-phase effort as I&C upgrades are implemented over several years. These interim states must be fully functional and be designed in such a way as to be properly used by operators. Ideally, these interim state HSI software graphics will be designed such that they can be fully leveraged to support the New State MCR with no or little modification. Development and use of a consistent HSI style guide established at the outset of a digital modernization program is key to achieving this objective.

To achieve what is euphemistically described as a "glass" New State MCR primarily made of VDUs, an Advanced Concept of Operations for the New State MCR needs to be defined early in a digital upgrade program. This must be defined with enough specificity as to guide the digital transformation of the MCR while also having some degrees of freedom to adapt as lessons are learned along the way. An example to illustrate this concept relates to how the DI will ultimately support Network Level 2 VDUs. As more and more VDUs are installed in the MCR, a certain point will likely be reached where the MCR becomes "saturated" with VDUs. At that point, as additional legacy I&C functions are migrated to either the safety I&C platform or the non-safety DCS, their monitoring and control functionality will be represented as software display pages on existing VDUs along with associated navigation capabilities to reach those display pages.

For digital point-solutions, such HSIs would be provided as a standalone workstation VDU associated with the particular I&C platform. That VDU would host the graphics package software to present the necessary display pages to the operators. As more and more display pages are hosted on that workstation, either the limits of the workstation capability or the need for the operator to be able to see more than one display page at the same time necessitates the need for additional DCS VDU workstations. Safety system VDU workstations are typically provided for each separate division. Maintaining the separation between safety systems and non-safety systems has also historically driven the need for separate VDUs for each of these two platforms. This is a solution that can be made to work when performing a digital transformation of the MCR. But this constrains both the MCR layout and the DI design to support these VDUs.

Having full-capability standalone workstations hosting HSI software packages as described above requires the installation of computers in the MCR that need to be supported. This can increase the power draw and associated heat load in the MCR. If these workstations need software updates or hardware maintenance to be performed on them, this will likely require direct access to them by maintenance personnel in the MCR. This disrupts MCR operation. By using thin client HSIs instead of standalone

workstations, the hardware physical and power envelope to support MCR VDUs drops considerably. Since these thin clients are typically solid-state devices with no loaded application software, any updates performed on the HSI software they access occurs on the server hosting a virtual machine running the HSI software application. This server is located outside of the MCR. Hardware issues with thin client are typically very rare. These thin clients act simply as VDU operator interfaces. The non-safety DCS Level 2 infrastructure depicted in Appendix A fully supports this concept with the Network Level 1 and Level 2 operator VDU software hosted as virtual machines on Server Block 1 and Server Block 2. Safety I&C platforms that support standard VDU interfaces (video connections and serial data links) at Network Level 1 (as described in Section 4.2.2.4) can also adopt a similar concept to remove all VDU algorithm processing from the MCR.

While the above helps with alleviating some issues associated with VDUs by providing them as thin client interfaces, a modernized MCR that only leverages this concept maintains the traditional separation of safety and non-safety I&C system VDU functionality. This constrains what appears on the VDUs. Safety system information and control is provided from safety system VDUs. Non-safety indication and control are provided on non-safety VDUs. While non-safety VDUs can also display safety system I&C information as enabled through the data diode shown in Network Level 2 both in Figure 3 and in Appendix A, no safety system control actions can be initiated from non-safety system VDUs. While this can be made to work, it significantly constrains the use of VDUs in a saturated "glass" MCR environment.

Research as described in Reference 16, Section 3.6.3 (Shared, Safety-Related Human-System Interface Architecture) describes a design approach that alleviates this constraint. This is shown as the safety HSI network switches A&B and the representative MCR VDUs below them in the bottom left of Appendix A. They are also pictorially represented in the MCR graphic in shown in Figure 3. These VDUs are described as display, keyboard, and trackball (DKT) devices in Reference 16 to differentiate them from other similar devices not connected to the shared MCR HSI architecture. In this architecture, any safety system or non-safety DCS HSI display can be configured to be accessed from any DKT in the MCR. It is expected that only DKTs at the reactor operator's watchstanding locations would be configured to issue commands to the application logic in the safety I&C platform or the non-safety DCS. All other DKTs would have access to view displays from either platform.

In existing MCRs during accidents or infrequent/transient conditions (e.g., a reactor startup), additional non-licensed personnel are stationed at various locations in the MCR to verbally relay plant status data to the licensed operators manning the MCR. Using the DKT architecture, operators in the MCR will have much more flexible and direct access to properly human-factored displays. It is expected that this will reduce workload and improve operator performance to the point that the additional personnel are no longer required in these situations.

In some currently licensed nuclear plant MCRs, fixed location safety-related VDUs provide data from one channel and division. This requires four, side-by-side, fixed location VDUs to present all data. Additional redundant VDUs are also required to meet the single failure criterion. In those MCRs, the failure of any one of the four fixed location safety-related VDUs requires MCR operators to use a VDU in another, often inconvenient location until the primary VDU can be replaced. This situation will be addressed by the flexibility of the DKT architecture. Also, the real estate used in the MCR for these separate, dedicated, and redundant safety platform VDUs is reclaimed for other use, since any DKT in the "glass" MCR can be configured as a backup should one normally used for safety system access by configuration, procedure, or convention fail.

There is no potential for the postulated failures that drove DI&C-ISG-04 (Reference 17) to place restrictions on multidivisional displays, since this architecture proposes using safety-related equipment and each DKT can only interface with one operator-selected safety channel/division HSI host or one DCS HSI virtual machine at any time. An evaluation of a specific, available vendor technology as captured in Reference 16 indicates that that such a DKT switch architecture can be shown to comply with the DI&C-

ISG-04 concerns identified for multidivisional displays. Such a capability would also allow for safety-related DKTs in the MCR to access any computer network (e.g., Corporate Network Level 4). Such access and operator use would be controlled by configuration (which MCR DKTs could access Network Level 4 and how the information is presented) and procedure (how that information is allowed to be used in the MCR).

This flexible DKT architecture also more generally supports MCR HSI interim states. While the number and location of DKT interfaces may change when proceeding from the current state to the envisioned "glass" New State, DI and the associated DA&A applications (graphics development packages) remain the same and follow the same HSI style guide. By designing HSI displays with the New State in mind, the ability to directly harvest and incorporate displays and navigation strategies produced for interim I&C/MCR upgrade states is enhanced when progressing to the New State. The objective is to directly leverage interim state products with either no or minimal rework to achieve the New State while minimizing the total cost.

Configuration of DCS Network Level 2 and Level 1 devices is normally accomplished at the DCS engineering workstation shown at the right at Network Level 2. This separate workstation would likely be placed in the equipment room where non-safety DCS equipment cabinets are located. Physical and logical access to the DCS engineering station is strictly controlled. This workstation could be a dedicated, non-safety HSI thin client or it could be a safety-related DKT configured for this purpose.

A limited number of physical buttons/switches will likely remain in the New State MCR. These will likely be limited to:

- Those that provide direct input to a final control element within a system with no interposing logic (e.g., a scram button or switch), which would be considered Level 0 devices as described Section 4.1.2
- Those that provide a direct input to the safety platform controllers for initiation of system-level functions (e.g., operation of multiple valves to isolate containment), which would be considered Level 1 devices as described in Section 4.2.2.4.

Any remaining direct indications from the field provided in the MCR are Network Level 0 devices as described in Section 4.1.2.

4.4 Network Level 3: Advanced Control and Advanced Applications

Network Level 3 provides a location to accommodate non-safety DCS control system functionality that is not native to the vendor DCS. It also provides for the collection, aggregation, and storage of digital I&C data from all such systems within Cybersecurity Level 4. The collected digital I&C data is then transmitted to Network Level 3.5 and Network Level 4.

4.4.1 Configuration

The computing capability of Network Level 3 is conceptualized as a Physical Server Block 3 at the middle-right of Appendix A. As with other Network Levels, Level 3 must:

- Possess the processing capability, data throughput capability, and storage necessary to host applications loaded on it.
- Be configuration controlled with corresponding documentation being maintained per Section 2.2.1.2 above.
- Be protected against cybersecurity threats. This Network Level is subject to the 10 CFR 73.54 Cybersecurity Rule (Reference 10) as explained in Section 2.3.1 above.
- Be designed and configured along with hosted DA&A software applications and databases to support migration of software applications and databases to new equipment when existing

equipment becomes obsolete. To emphasize this necessary capability, hosted software applications are depicted as separate virtual machines within Physical Server Block 3.

All of the servers within Network Level 3 are part of the non-safety DCS. Because of this, and the fact that all of the non-safety DCS is within Cybersecurity Level 4, there is no need for firewalls between Network Level 2 and Network Level 3 as shown Figure 3 and Appendix A. To support where other digital systems exist within Cybersecurity Level 4, a provision is made to bring their information into the DCS to facilitate the creation of common HSIs and a shared database for all I&C data within Cybersecurity Level 4. This provision includes a firewall that services the following Interface Cases shown in the middle-left of Appendix A:

- Interface Case 3: This provides a means to collect I&C information from legacy, standalone, digital I&C systems for purpose of providing HSI displays on the DCS for those legacy systems. This data will be collected by the I&C historian and presented to the DCS server (as described in Section 4.4.2 below). This interface can be configured to provide both indication of and control command functionality to those legacy I&C systems connected through it. Because of potential latency issues across this interface, control algorithms that compute results are not allowed on the DCS by rule (See section 4.2.2.1 (c) above).
- Interface Case 4: This provides a means to collect:
    - I&C data from a digital Plant Process Computer (PPC) or similar system used to satisfy the requirements for a Safety Parameter Display System (SPDS) in the MCR. This allows for the integration and harmonization of SPDS displays with the DCS while meeting the SPDS requirements of Reference 7. This also supports the migration of PPC/SPDS functionality to the DCS at Network Level 1 and elimination of the PPC/SPDS as a separate system in a nuclear plant. This data will also be collected by the I&C historian (described in Section 4.4.2 below).
    - Field data that can be used to support emergency preparedness functionality when forwarded to Network Level 3.5. An example of such data includes meteorological data collected for use by the emergency response organization (ERO) as discussed in Section 4.5.2 below.

For both of the above Interface Cases, data provided as an input to the DCS should not be used for input into either DCS Network Level 1 control algorithms or Network Level 2 supervisory control algorithms. This should also be controlled by rule (see Section 4.2.2.1 (c) above).

A data diode to permit only one-way mass data transfer out of the Network Level 3 I&C historian must also be provided to enable Network Level 3.5 and Network Level 4 DA&A application functionality as described in Sections 4.5.2 and 4.6.2. This is shown at the top of Network Level 3 (top-right of Figure 3 and at the top-left of Appendix A).

System time for the DI is also provided at Network Level 3 through time servers depicted in the center of Appendix A. System time is primarily used for time correlation of data across the DI. It can also be used to detect network and connected device issues that manifest themselves through device internal clock deviations from system time (particularly Network Level 1 controllers [Section 4.2.2.1]). So long as batch processing is not performed across multiple controllers (which relies on system time), individual DCS controllers will continue to operate on “local time” within the controller if there is a deviation between local time and system time.

4.4.2 Data Architecture and Analytics Features and Associated Portability

The Network Level 3 Physical Server Block 3 as depicted in Appendix A hosts non-native applications (shown as separate virtual machines). These applications provide advanced features that are accessed by

operators that use DCS thin clients at Network Level 2 to view and control the plant. This includes applications such as:

1. An I&C data historian. This historian could either directly leverage the current OSI/PI® software application used across the nuclear industry for this purpose or a similar product. The historian captures and aggregates I&C data from the non-safety DCS and the safety I&C platform at Network Level 2 as well as from Interface Case 3 and 4 as described in Section 4.4.1 above. Several DCS vendors offer an application programming interface (API) that allows this data to be dynamically linked to their DCS server. This API makes all this data available for presentation on Network Level 2 DCS VDUs (e.g., trend displays).

2. Computerized procedures. This software application can provide capabilities far beyond that of electronically presenting the text of current procedures. For example, the logic of procedure steps can be dynamically linked to the Network Level 2 DCS server or the Network Level 3 data historian (again through an API). This enables coding and depicting the logic of procedure steps to automatically determine and present if the steps are satisfied based on plant status as detected by Network Levels 1, 2, or 3. Live values used by operators to make decisions as to which path to follow in procedures can also be presented. Hyperlinks can also be provided within the computerized procedure to provide direct access to system mimic displays from which a control action described in the procedure can be taken for DCS connected final control elements.

3. Advanced alarm management and presentation. Basic HSI presentation of alarm status of each I&C system point configured with an alarm in an I&C system is typically provided as a native application with the DCS at Network Level 2. As described above, the non-safety-DCS will now capture this information for both the safety I&C system and the DCS. This alarm status data can also be monitored by additional software applications at Network Level 3. Advanced alarm management tools can analyze this alarm data to prioritize and filter alarms based upon plant conditions. As an example, such tools can suppress alarm floods that can occur during plant operating scenarios. Such floods can impede operators efforts to identify the underlying cause of the alarm flood and impede operator response. Advanced alarm management software analyzes these alarms, prioritizing and filtering them to aid the operator in identifying the underlying cause of the alarms more quickly and accurately so that appropriate actions can be taken. Alarms can also be grouped and presented on HSIs in in such a way as to similarly help operators identify the underlying cause more quickly and to speed operator actions to address that cause. This can include hyperlinks on alarm tiles on an HSI display so that when they are selected in the alarm management software, the system mimic HSI display on which the alarm is sourced is directly presented to the operator (without need to perform any navigation).

4. Tagout/lockout applications. These software applications provide a means to electronically identify and inhibit operation of plant equipment as required by tagout/lockout processes for maintenance or other reasons. This is important because legacy methods of physically placing paper tags on switches in the MCR for this purpose do not translate to a “glass” MCR HSI interface. Such software applications can be dynamically linked to the DCS HSIs to provide indications (e.g. representations of danger and other tags) on those displays from which plant Level 0 devices (e.g. pumps, valves, etc.) are operated. This linking can also inhibit the operation of devices from the non-safety DCS HSIs while an “electronic tag” is “hanging” on the control for the particular device on the HSI display.

5. Cybersecurity monitoring. Multiple software tools can be hosted Network Level 3 to manage cybersecurity of the DCS. Functions performed by these tools include managing network access, collection of logs from devices to monitor for cybersecurity events, virus scanning, whitelisting of applications, passive vulnerability scanning, etc. Detected cybersecurity issues can be captured in the Network Level 3 data historian and forwarded up to Network Level 4 to automatically notify utility cybersecurity personnel.

Cybersecurity applications need to be selected carefully and their interactions with Network Level 2 need to be clearly identified and controlled. Improperly configuring of log collection from Network Level 2, for example, can potentially cause operational situations that were not analyzed by the DCS vendor and void performance guarantees for Network Level 2. Virus scanning of Network Level 2 devices by software on Network Level 3 can similarly disrupt Network Level 2 performance, impacting DCS view and control performance as described in Section 4.3.

Required storage of cybersecurity related data (e.g. equipment logs, etc.) is provided by Network Level 3. Due to the expansive nature of this data, this storage is depicted as being provide a separate network accessible storage (NAS) device at the right of Network Level 3 as depicted in Appendix A.

6. DCS Network Level 2 and Network Level 3 system configuration backup. Network Level 3 provides a location within the shared storage of Physical Server Block 3 to place backup files. These backup files fully capture the DCS configuration of these two levels of the DI. These configuration backup files can be used to configure individual DCS component replacements if one should fail. The backup files can also be exported to removable media to support configuration control and disaster recovery capabilities.

4.4.3 Human-System Interfaces

For the purposes of operating the plant, Network Level 2 DCS HSIs (either DCS VDUs or DKTs accessing the DCS) are used to access Network Level 3 DA&A applications. HSI thin clients associated with Network Level 3 cybersecurity configuration monitoring and Network Level 3 configuration management are shown to the right of Figure 3 and Appendix A.

4.5 Network Level 3.5: Emergency Preparedness Network and Demilitarized Zone

The functionality provided by Network Level 3.5 supports two purposes.

1. Support for emergency preparedness functions by:
    a) Capturing I&C system data provided by the Network Level 3 historian in a Network Level 3.5 historian. The Network Level 3.5 historian also captures any data/information created within Network Level 3.5 when performing its emergency preparedness functions.
    b) Hosting DA&A applications and providing necessary HSI access to enable ERO facilities as described in NUREG-0654 (Reference 9), including those listed below:
        - The Technical Support Center (TSC) is an onsite facility that provides plant management and technical support to the reactor operating personnel located in the MCR during emergency conditions.
        - The Operations Support Center (OSC) is an onsite emergency response facility that provides for maintenance and other support personnel to gather as a ready resource to support emergency response actions
        - The Emergency Operations Facility (EOF) functions as the primary base of emergency operations for the licensee during a radiological incident. The EOF facilitates the management and coordination of the overall emergency response, including the sharing of information with federal, state, local, and tribal government authorities.

2. Providing Network Level 4 access to select digital data stored within the Network Level 3.5 as described in 1(a) directly above. This data buffer capability enables the DA&A application functionality provided by Network Level 4 (Section 4.6.2 below).

4.5.1 Configuration

Network Level 3.5 receives I&C system data from Network Level 3 through the data diode described in Section 4.4.1.

The computing capability of Network Level 3.5 is conceptualized as a Physical Server Block 4 at the top-right of Appendix A. As with other Network Levels, Level 3.5 must:

- Possess the processing, data throughput capability, and storage necessary to host applications loaded on it.
- Be configuration controlled with corresponding documentation being maintained (Section 2.2.2 above).
- Be protected against cybersecurity threats. This Network Level is subject to the 10 CFR 73.54 Cybersecurity Rule (Reference 10) as it provides Emergency Preparedness functionality as explained in Section 2.3.2 above.
- Be designed and configured along with hosted software applications and databases to support migration of software applications and databases to new equipment when existing equipment becomes obsolete. To emphasize this necessary capability, hosted software applications are depicted as being hosted on separate virtual machines within Physical Server Block 4.

In order to act as a DMZ, a protected and monitored Network Level 3.5 node must be established as part of the Network Level 3.5 configuration. This protected node faces Network Level 4. That node is only provided Network Level 3.5 information exposed to it, while the rest of Network Level 3.5 is safe behind a firewall. This DMZ capability supports DA&A applications at Network Level 4.

To support the ERO facilities, particularly those that are geographically separated from a NPP site (such as the EOF), Network Level 3.5 as shown must be configured in such a way as to allow emergency support thin clients physically connected to Network Level 4 to have network connectivity through the DMZ to access the emergency preparedness thin client virtual machines workstations depicted in Physical Server Block 4 shown in Appendix A. This is accomplished through a secure logical means (e.g. virtual private network tunneling). Through this method, the emergency support facility thin client HSIs shown in Figure 3 and Appendix A are logically connected to Network Level 3.5 even though they are physically connected to Network Level 4. Configuration of the emergency support facility thin clients and the communication means established as described above fall within the auspices of the Cybersecurity Rule (Reference 11).

It is possible to interface field devices to Network Level 3 for the purposes of supporting ERO functions. Such data sources also fall within the auspices of Reference 11. To address this issue, this report assumes all such data is provided through Interface Case 4 as presented in Section 4.4.1.

4.5.2 Data Architecture and Analytics Features and Associated Portability

As Network 3.5 only supports the two functions of supporting ERO facility HSIs and the passing of I&C data from Network Level 3 historian to the Network Level 4 DI enterprise historian, the DA&A applications running at this level are few in number.

Software applications at Network Level 3.5 are limited to those that enable the ERO function. These include:

- The Network Level 3 historian.

- Any software applications that can be used to process I&C data from Network Level 3 in order to support the ERO function. The results produced by such applications are also be stored in the Network Level 3 historian.
- HSI graphics packages that are used to provide ERO personnel with capability to view data in the Network Level 3 historian to accomplish the ERO function and input information that can then be shared between the individuals working in the ERO facilities. Such graphics packages should include a means to:
    - Create purpose-built HSI displays to support unique ERO functions
    - Provide facsimiles of every safety I&C system and non-safety I&C DCS display to facilitate efficient communication and coordination between the MCR and the ERO facilities. Many I&C DCS vendors provide such software packages to replicate DCS displays on IT networks.
- Computerized procedures similar to those described in Section 4.4.2 above developed for the purpose of supporting the ERO. Note that computerized procedures at this level have no linkage to control functions. Network Level 3.5 provides no capability to pass information to or control the actions of any equipment in Network 3 and below.
- Cybersecurity monitoring applications necessary to satisfy Reference 10 as Network Level 3.5 falls within the auspices of the Cybersecurity Rule.

4.5.3 Human-System Interfaces

The only HSIs supported by Network Level 3.5 are those that enable the ERO facilities and the features described in Sections 4.5.1 and 4.5.2 above and an administrative workstation (not shown) to configure/maintain Network Level 3.5. It should be noted that the ERO facilities will most likely also possess Network Level 4 workstations that can potentially support ERO functions as an alternate/diverse source (e.g. National Weather Service information from the internet) not under the auspices of the Cybersecurity Rule (Reference 11). Use of such information would need to be clearly defined by procedure.

4.6 Network Level 4: Station Corporate Network

4.6.1 Configuration

As more functions of legacy I&C systems are migrated to the safety-related and non-safety digital I&C target platforms, as identified in Section 3, Item 9 above, the amount of live digital process data associated with connected plant systems will grow substantially. While this data will be directly used by control systems and plant operations personnel using control system displays at Network Level 2 to run the plant, it will also be made available to Level 4 through a one-way data diode at Level 3 and the Level 3.5 DMZ. This data flow path is shown on the top-right of Figure 3. Digital data with regard to the digital I&C systems themselves (configuration, operational status, self-diagnostics information, etc.) will also be made to Network Level 4.

To augment I&C system data, digital plant monitoring devices can also be connected to the Corporate Network. As shown at the top-left of Figure 3 and Appendix A, this will include automatic input from wireless sensors and drones as well as manual plant-related input from personnel in the field using mobile electronic devices or computer workstations. Note that as I&C systems are digitized, there is no need to use separate wireless sensors to collect data from physical plant processes monitored by these I&C systems.

The net result of this is the digitization of plant data at the source across the DI, eliminating the need to use manual means (paper) to collect and manage the data. This makes a wealth of direct digital data available for plant optimization uses on the Corporate Level 4 Network.

The computing capability of Network Level 4 is conceptualized as a Physical Server Block 5 at the top-right of Appendix A. Actual configuration of Network Level 4 resources is the responsibility of the utility IT department. As with other Network Levels, Level 4 must:

- Possess the processing, data throughput capability, and storage necessary to host applications loaded on it.
- Be configuration controlled with corresponding documentation being maintained (Section 2.2.2 above).
- Be protected against cybersecurity threats. This is necessary even though this Network Level is not subject to the 10 CFR 73.54 Cybersecurity Rule (Reference 10) as explained in Section 2.3.3 above.
- Be designed and configured along with hosted software applications and databases to support migration of software applications and databases to new equipment when existing equipment becomes obsolete. To emphasize this necessary capability, hosted software applications are depicted as being hosted on separate virtual machines within Physical Server Block 5.

At Network Level 4, data aggregation and data analysis capabilities enable optimization of utility enterprise practices that are not related to direct plant monitoring and control by operators (Levels 0–3) and Emergency Preparedness functions (Level 3.5). Each of these capabilities at Network Level 4 are summarized in Section 4.6.2 below.

4.6.2 Data Architecture and Analytics Features and Associated Portability

The LWRS FY2021 PM Pathway Technical Program Plan (Reference 26) provides descriptions of many research activities being performed in the areas of DA&A features at INL. These are summarized in the subsections below to provide an overview of specific functionality envisioned to be supported at Network Level 4. This functionality researched by INL and developed/applied by INL and industry will significantly contribute to reductions in plant TOC when applied as guided by the ION Model and its associated Advanced Concept of Operations, as described in Section 1.2.1 above.

All of the features summarized below need to be developed and deployed in such a way that they can be migrated as a set from different instantiations of the Network Level 4 DI as equipment obsolescence needs dictate. This ensures that intellectual property investments at this level are protected and leveraged for the remainder of plant operating life.

4.6.2.1 Data Aggregation - Digital Architecture for an Automated Plant

The act of obtaining data by itself does not mean that the data is necessarily useful. In existing nuclear plants, data are collected at Network Level 4 from plant I&C systems, work-management systems, scheduling programs, configuration management tools, operator logs, plant equipment condition monitoring programs, etc. Much of this data is manually collected and then digitized. Remaining data are collected directly by digital means. These different digital databases have different structures and tools and are typically used independently. The integration of digital data from these databases is performed manually. For example, an LWRS pilot study previously attempted to integrate scheduling activities from one tool with work-order steps from another for the purpose of tracking work progress in an outage. Because a scheduled activity can represent one or more steps in a work order, the mapping process had to be performed manually and required tens of hours to map one work order to one schedule. The problem is much broader than this example.

Such problems are addressed by creating a data warehouse at Network Level 4. The data warehouse is the Network Level 4 enterprise historian that enables the collection and integration of digital data sources within a common data model. The framework of this model is optimized for data capture, storage, and retrieval by Network Level 4 DA&A applications. Direct benefits and cost saving are achieved through enabling the automation of manual data searches and enabling the sharing and comparison of data from

various software application tools for a single plant or multiple plants. It also reduces the need for training plant staff on various tools used to support legacy, disparate databases. Such a data warehouse supports a standard visualization approach for all the data within it associated with operations and maintenance, enabling a holistic staff perception of plant activities.

The digitization of data at the source as enabled by the DI also vastly increases the amount of digital data that can be directly collected (number of points) and the time frequencies of digital data collected from those points within the data warehouse. It also allows for automatic correlation of this data in time. Such a structured and expansive digital data warehouse fully empowers the use the of software applications for data analysis as discussed in Section 4.6.2.2 below.

4.6.2.2 Data Analysis

Enabled by the data warehouse hosted on the DI as described in Section 4.6.2.1, other software applications can analyze the data contained therein to optimize the business of running a NPP. In addition to applications available to the industry, the LWRS PM Pathway at INL has been and is continuing to pursue multiple data analysis research activities to more fully realize the potential to maintain or improve plant safety and reliability while reducing operational costs. Several of these research initiatives are described in Reference 26 and summarized below by area. Note that in this context of this section, the term "automation" is applied to work processes at Network Level 4, not to control system automation which is performed at Network Levels 1 and 2.

a) Online Monitoring and Plant Automation

- Advanced Remote Monitoring for Operational Readiness

  With current technology advancements in sensors and digital data analytics, it is possible to replace a significant portion of operations activities with sensors and centralized and automated analysis process. This enables appropriate organizations to address anomalies before their severity escalates. The New State requires developing methods to autonomously analyze plant process and support systems digital data on a holistic level. It will also require identifying plant monitoring gaps and introducing new technologies or sensors to improve the operator's decision-making process.

  Ongoing research activities in this area are developing an advanced operations approach that automatically ensures plant readiness and identifies plant anomalies along with what caused them as issues progress. This will reduce the number of plant workers gathering data, allowing the operations team to focus on ensuring optimal plant performance. This is achieved by researching and developing methods to automate the methods of data-collection (i.e., transform the way surveillances are performed) to reduce the cost of manual operations processes. The project will also develop machine intelligence technologies that integrate data from various plant equipment sensors with plant process data for a holistic and continuous approach to operations monitoring, revealing anomalous conditions that cannot be inferred based on a single method of monitoring and developing a library-based monitoring platform to enable rapid, flexible, and expandable integration of monitoring methods used by plants and vendors. The research will target high-cost processes in order to ensure maximum return on investment. Existing technology capabilities, data, and expertise will be leveraged to achieve reduction in O&M costs on identified plant assets.

- Technology Enabled Risk-Informed Maintenance Strategy

  This research focuses on transitioning from a labor-centric to a technology-centric maintenance strategy based upon real-time condition and risk of failure assessments of plant assets to lower maintenance costs. The prototype assessments described below provide a basis for expansion of demonstrated monitoring and risk assessment

techniques to all plant structures, systems, and components that currently require time-based maintenance:

- Present the utilization of circulating water system (CWS) heterogeneous data and fault modes from both the Public Service Enterprise Group Nuclear, LLC plant sites in order to develop salient fault signatures associated with each fault mode. The machine learning (ML) diagnostic/prognostic models utilize these fault signatures to automatically determine the condition (healthy vs. unhealthy) of the CWS; a determination otherwise performed by subject matter experts at plant sites and/or monitoring and diagnostic centers. The developed approach automatically categorizes a specific fault mode with a high degree of confidence, thereby offsetting the time-consuming, labor-intensive practices of the preventive maintenance program.
- Achieve integration of component-level predictive models into a robust system-level model enabled by federated-transfer learning. Federated learning is a decentralized approach to ML: collecting data from CWS components across different units to develop robust models that are combined for representation in the ML algorithm (i.e., "model"). Transfer learning is an approach that allows the application of a developed "model" to different but related systems within the same plant site or to the same system (i.e., CWS) at different plant sites. This advancement is a first-of-a-kind application of federated-transfer learning in the nuclear industry.
- Develop a detailed, physics-informed model of a CWS motor and pump set to capture the dynamics of CWS operation. This modeling approach provides the ability to simulate data associated with fault modes for which minimal or no evidence is available in historical plant process data, enabling the generation of comprehensive fault signatures to achieve robust predictive models.
- Achieve the coupling of a three-state Markov chain risk model and a prognostic model, using a proportional hazards model to derive probabilities reflecting NPP states (i.e., full-load operation, derate, and trip). These state probabilities are used to understand the economics of automation achieved by transitioning from a time-consuming, labor-intensive, cost-prohibitive preventive maintenance program to a risk-informed, predictive maintenance strategy.
- Outline the development of a user-centric visualization that provides the right level of information, in the right format, to the right person. The HSI design, based on user-centric visualization guided principles, uses the design inputs provided by users from the Public Service Enterprise Group Nuclear, LLC owned Salem and Hope Creek plants. This approach also focused heavily on ensuring that the ML models were transparent and explainable to skeptical users by implementing human-centered artificial intelligence concepts. The inputs were collected via a series of structured virtual interviews, and an initial prototype was evaluated in a second round of similar interviews. A representative user-centric HSI was developed using the Microsoft PowerBI platform.

- Online Monitoring of Active Components, Concrete Structures, and Secondary Piping Systems

- Online active component monitoring pilot activities to develop a diagnostic and prognostic online monitoring analysis framework have been performed on emergency diesel generators, large power transformers, and induction motors. This research leveraged the Electric Power Research Institute FW-PHM suite software to identify specific component degradation and fault conditions. Analytical model development efforts were focused on diagnostic and remaining useful life advisors.
- Online monitoring and data analytics of plant concrete structures including embedding and retrofitting sensors, correlating the data with non-destructive examination techniques, model predictions, laboratory experiment results, and expert opinion using Bayesian networks for effective inference. Also included in this research are visualization techniques to enhance data interpretation.
- Online monitoring of secondary system piping research focuses on monitoring structural health to reduce the cost of preventive maintenance. Again, this leverages the state-of-the-art sensor modalities, data fusion, and advanced data analytics for the purpose of moving from labor-intensive inspection-based maintenance to condition-based maintenance.

- Advanced Online Monitoring Facility

  Planned future research in this area will address adapting the new monitoring, diagnostic, and prognostic capabilities enabled by the DI and provided by DA&A applications as summarized in this report into a nuclear utility fleet online monitoring facility. A prototype online monitoring facility will enable piloting online monitoring technology developed by the LWRS Program and other research organizations and evaluation of them in an operational environment in collaboration with utilities. This will utilize the Monitoring, Diagnosis, and Automation Laboratory and the Human-Systems Simulation Laboratory at INL. Lessons learned from this effort are planned to be captured in a technical report to support industry-wide implementation of these new capabilities in utility maintenance and diagnostic centers.

- Management Decision Support Centers

  Planned future research in this area will address enabling improved nuclear plant and enterprise management decision-making by leveraging the DI and DA&A application capabilities at Network Level 4. There are three types of decision support centers that will be enabled as listed below. All three facility types will leverage the wealth of DI data collected and information produced by DA&A applications to improve the quality of operational decision-making while reducing workload. To ensure this end is achieved, HTI efforts will need to be performed to optimize facility operation both individually and as a set as discussed in Section 5 below. Each of their interactions with the MCR will also need to be taken into account. This will ensure that information is properly synthesized and presented to managers in all these facilities, who will in turn use that information into direct proper actions.

  - The first type are purpose-built facilities at a NPP and at a utility headquarters location for a fleet of nuclear plants. Enterprise management decision-making associated with plant operations, maintenance, and business-related functions will be enhanced in these facilities by properly organized and presented live data feeds and information that are the result of automated analysis of that data.

- Another type of decision support center is used for coordination of plant outage work. The outage control center (OCC) manages nuclear outages in a safe and efficient manner. This is a complex task that led utilities to develop formal outage organizations dedicated to planning and executing refueling and forced outages. OCCs were built that collocate the activity managers for all the major site organizations so that they can closely coordinate their activities. In addition, they maintain a number of other work execution centers that control critical elements of the work, such as safety tagging for system and component isolation, nuclear risk management coordinators, and similar functions needed to address other constraints on how the outage is conducted. Research performed in this area leverages the information availability and DA&A application capabilities hosted at Network Level 4 to better optimize and coordinate outage planning and execution activities outside and within the OCC to reduce outage cost and risk. Direct digital connectivity to field workers and the OCC will provide those workers information to perform their tasks more efficiently and with less errors. This connectivity will also automatically report back on outage work tracking. This will improve performance and reduce workload.
- The third type of management decision support center are those used by the utility emergency response organization (ERO). The ERO makes decisions regarding how to classify, mitigate, and provide protective actions for nuclear emergency events. These deliberations occur in the dedicated emergency response facilities, namely the TSC, the OSC, and the EOF; the latter of which is offsite and sometimes serves the entire fleet. These facilities will leverage Network Level 4 resources to physically connect EOF, TSC, and OSC thin client workstations to Network Level 3.5. These thin clients will be logically connected to Network Level 3.5 and controlled in accordance with 10 CFR 73.54 (Reference 10). ERO capabilities will be enhanced by DI and DA&A capabilities, enabling workload reductions in the areas of data gathering, analysis and communication. Efforts to further the consolidation of EOFs for nuclear fleets will also be supported.

- Virtual Plant Support Organization

  Due to the complexity of plant systems and the large number of components in NPPs, utilities maintain a large staff of highly trained operators, engineers, technicians, and other types of specialists at each site to ensure safe and successful operations. Considerable ongoing investment in the form of training and development is made in this workforce to enable them to maintain the unique and aging technologies in the plants.

  This approach to staffing is becoming increasingly unsustainable because, like the aging I&C systems that plants must be replaced, the aging workforce is on the brink of a substantial retirement wave in which a significant portion of the workforce will have to be replaced in a relatively short amount of time. Going forward, there are concerns whether the commercial nuclear industry will be able to attract and retain the needed engineers and technicians, given the looming shortage of technically trained workers in this country coupled with a new generation of workers who are more prone to change jobs multiple times in their careers. It is also inefficient for utilities with a fleet of NPPs to sustain separate, standalone organizations at each site. Centralization of such a workforce can provide significant efficiencies to reduce NPP TOC across such a fleet.

An alternative model to address these challenges and to centralize expertise for more efficient work execution is to build a virtual plant organization that is seamlessly connected through the DI. A virtual support organization is a combination of a nuclear site's or nuclear utility's own organization, plus external organizations that have been delegated direct support roles in operating and maintaining the plant. The term "virtual" indicates that the organization is interconnected through the DI for data exchange, communications, and collaboration, as opposed to being constrained to being located onsite. This allows the NPP to tap into far greater resources and expertise than can be practically maintained at the NPP site or facility.

This capability is depicted as a cloud of "contracted support services" in the top-center of Attachment A. Additional, vendor proprietary DA&A applications could potentially be leveraged using a "fee-for-service" model as is used in other industries, such as live remote monitoring and diagnostics for aircraft jet engines in flight. Use of such capabilities would need to be folded into an enterprise Concept of Operations, as described in Section 1.2.1 above.

b) Advanced Applications and Work Process Automation for Field Workers

Three specific technologies are being researched by the LWRS PM Pathway to improve field worker performance and efficiencies. These include:

- Mobile technologies. Use of mobile technologies (e.g., wireless tablets/laptops, wireless headsets, etc.) to improve human performance is increasingly pervasive outside the nuclear industry, revolutionizing how humans conduct their routine personal and work-related activities. The nuclear industry is working diligently to integrate the functionality enabled by these devices into plant work processes. To achieve this end, these devices must have access to real-time plant information, support real-time collaboration with workers in other locations, particularly those who are coordinating overall plant operations and maintenance activities in MCR, maintenance shops, or in management decision support centers.

  These mobile technologies are hosted at Network Level 4, where their use is permissible. They are shown on the top-left of Figure 3 and Appendix A. Policies to use these devices along need to be defined consistent with the enterprise Concept of Operations. Controls also need to be established with regard to user access along with configuration controls to ensure they provide valid and timely information to plant personnel commensurate with the duties of the field workers.

- Augmented reality. This is a specific application of mobile technologies for field workers. Wireless digital devices are used to provide these workers with plant information critical to safely and successfully complete activities when this information may not be directly visible. These technologies allow the worker to "see" otherwise unavailable information that will enable them to make informed decisions about their activities and personal proximity to hazards. For instance, this might include smart safety glasses that can superimpose a transparent color-shaded representation of a radiation field directly into a worker's field of view. Similarly, plant data could be superimposed directly onto the components in the field of view, allowing the worker to "read" the data by merely looking at the components. A host of other capabilities, such as remote radiation and location monitoring of field workers, can be supported by this technology.

- Computer-based procedures. These procedures are a specific application (or application set) that would be accessed by those workers using mobile technologies described earlier. Computer-based procedures can enforce adherence expectations

and perform data manipulations in a correct manner to minimize errors in execution. Furthermore, in an integrated computer-based procedure environment using wireless technology, it is possible to track the timing of real-time actions of procedure steps to detect unintended interactions among procedures or with the desired plant configuration.

These applications would be hosted at Network Level 4 either as applications loaded on the mobile devices themselves or hosted by servers for which the mobile devices act as an HSI. Digital information from the entire DI would be available to enable "intelligent procedures" that can us this data to automatically validate the completion of procedure steps.

4.6.2.3 Other Network Level 4 Software Applications

Network Level 4 also requires a myriad of additional software applications to perform its functions beyond those described in Section 4.6.2 above. No effort is made to provide a complete list of such applications here. Notable applications that provide capabilities pertinent to the scope of this report include (but are not limited to):

- HSI packages to present Network Level 2 and 3.5 displays as information on Network Level 4.
- HSI applications (or HSI capabilities within data DA&A applications described in Section 4.6.2.2) are needed to present analysis results to users on Network Level 4, particularly those in the management decision support centers also described in Section 4.6.2.2.
- Cybersecurity software tools are necessarily hosted on Network Level 4. As previously described in Section 2.3.1 above, Network Level 4 does not fall under the auspices of the Cybersecurity Rule (Reference 10).

4.6.3 Human-System Interfaces

HSIs at Network Level 4 cover the spectrum of capabilities offered by digital technology. This includes wired corporate workstations and or thin clients that provide the same functionality through virtual machines hosting HSI functions on Physical Server Block 5 as shown in Appendix A. The concept of a "glass MCR" can be extended to the management decision support centers described in Section 4.6.2.2 where large video screens can be used to promote improved, shared situational awareness with multiple individuals. Mobile devices including wireless laptops/tablets and augmented reality headsets and associated input devices can be used by field workers to access information, perform work, and document work performance electronically.

As shown in Figure 3 and Appendix A, it is possible to present Network Level 4 information in the MCR either using separate Corporate Network workstations, separate thin clients, or using DKTs connected through the safety HSI network switches A&B as described in Section 4.3.3 to access Corporate Network thin client hosts.

Use of these HSI must be carefully and deliberately considered and accounted for by design and by procedure. For example, using Network Level 4 as the direct source of information to operate plant equipment (whether through an MCR DKT, a wireless tablet, or an augmented reality headset) may actually result in correct and improved capabilities to do work. It also violates the current understanding of the Cybersecurity Rule (Reference 10). HSIs need to be designed (as directed by a global HSI style guide) to make the source of data being presented by a digital HSI intuitively obvious by DI Network Level. Procedures must establish exactly how data from each DI Network Level can be properly used within the context of the Advanced Concept of Operations to optimize work performance within the nuclear utility enterprise.

5. Human and Technology Integration

A pictorial representation of how DI, DA&A, and HTI relate is provided by Figure 5 below.

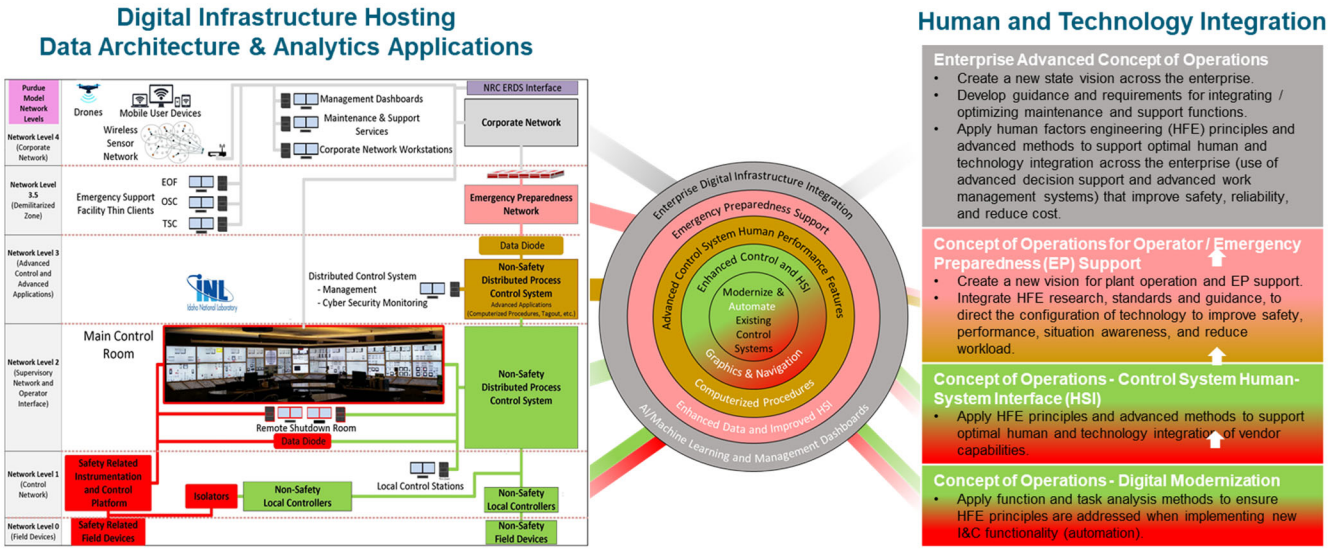


Figure 5 – Relationships between DI, DA&A, and HTI

The union of the DI with DA&A software applications provides powerful capabilities as presented in Section 4. This union is represented on the left side of Figure 5 as the colored digital platforms at the different Network Levels that make up the DI. Proper utilization of these capabilities must consider their usability by personnel at all levels of the DI. This is accomplished through digital HSIs depicted at Network Levels 1 through 4 at left in Figure 5.

Efficient Plant Operations Concept using Human-system-integration (EPOCH) LWRS researchers are working in a cohesive and structured manner with the DI and DA&A researchers as well ION researchers to achieve this end. The initial premise behind EPOCH is that the operating model (i.e., Concept of Operations) for commercial NPPs must be transformed. Furthermore, the transformation of the NPP operating model requires going beyond like-for-like replacements and entails a technology-centric approach that fundamentally changes the way the plant is operated, maintained, and supported—from a low automation, high manual action Concept of Operations to one with high automation (with high transparency) and operators in a more supervisory role. Procedure impacts associated with this transformed operating model are also addressed by EPOCH.

The color coding of the individual subsystems that make up each of these Network Levels shown in the DI flow from left to right across Figure 5 to support this transformational Advanced Concept of Operations in a holistic manner. As shown in the target in the center of Figure 5, DI and DA&A capabilities (shown in black text) correspond with automation and HSI capabilities (shown in white text in the target) that are then implemented at each level of the Purdue Model shown in the HTI column on the right side of Figure 5 (with white text headings). The result is a single, comprehensive, DI and DA&A enabled, EPOCH-driven enterprise Advanced Concept of Operations.

Based on prior research experience, EPOCH has recognized three key barriers that need to be overcome to adopt this technology-centric operating model. The three barriers are:

1. Business Case: developing a clear business case regarding the actual cost reductions seen with advanced technology. This is driven primarily by the ION-identified market-based electricity price point for a nuclear unit as described in Section 1.2.1

2. Perceived Risk: the perceived regulatory, licensing, and cybersecurity risk affecting technology acceptance and its HTI aspects.
3. Incomplete Guidance: insufficient guidance in performing significant digital modifications to the power generation side of the plant.

As such, EPOCH has been developing an implementation strategy that addresses these barriers to enable the adoption of advanced automation that transforms an NPP's Concept of Operation.

Additionally, EPOCH researchers have developed a methodology to enable the adoption of advanced automation and digital capabilities to extend the life and improve performance for the LWR fleet. Building on existing standards and guidelines from the NRC, the Electric Power Research Institute, the Institute of Electrical and Electronics Engineers (IEEE), and others, this methodology recommends the early involvement (i.e., during the planning and conceptual design phases) of HFE experts to support the evaluation of the safety and reliability of advanced automation technologies. The five primary phases of the methodology that represent the lifecycle of the project are shown in Figure 6 below.

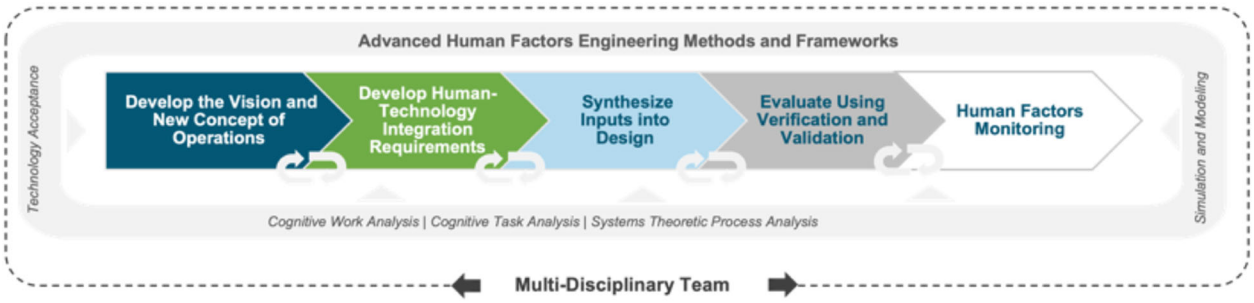


Figure 6 – Process Model for the EPOCH Methodology

It is beyond the scope of this report to describe the EPOCH methodology further. Full details are available in "Development of an Assessment Methodology that Enables the Nuclear Industry to Evaluate Adoption of Advanced Automation," INL/EXT-21-64320 (Reference 28 which will be published in September 2021).

6. Tailored Implementations of the Digital Migration Framework

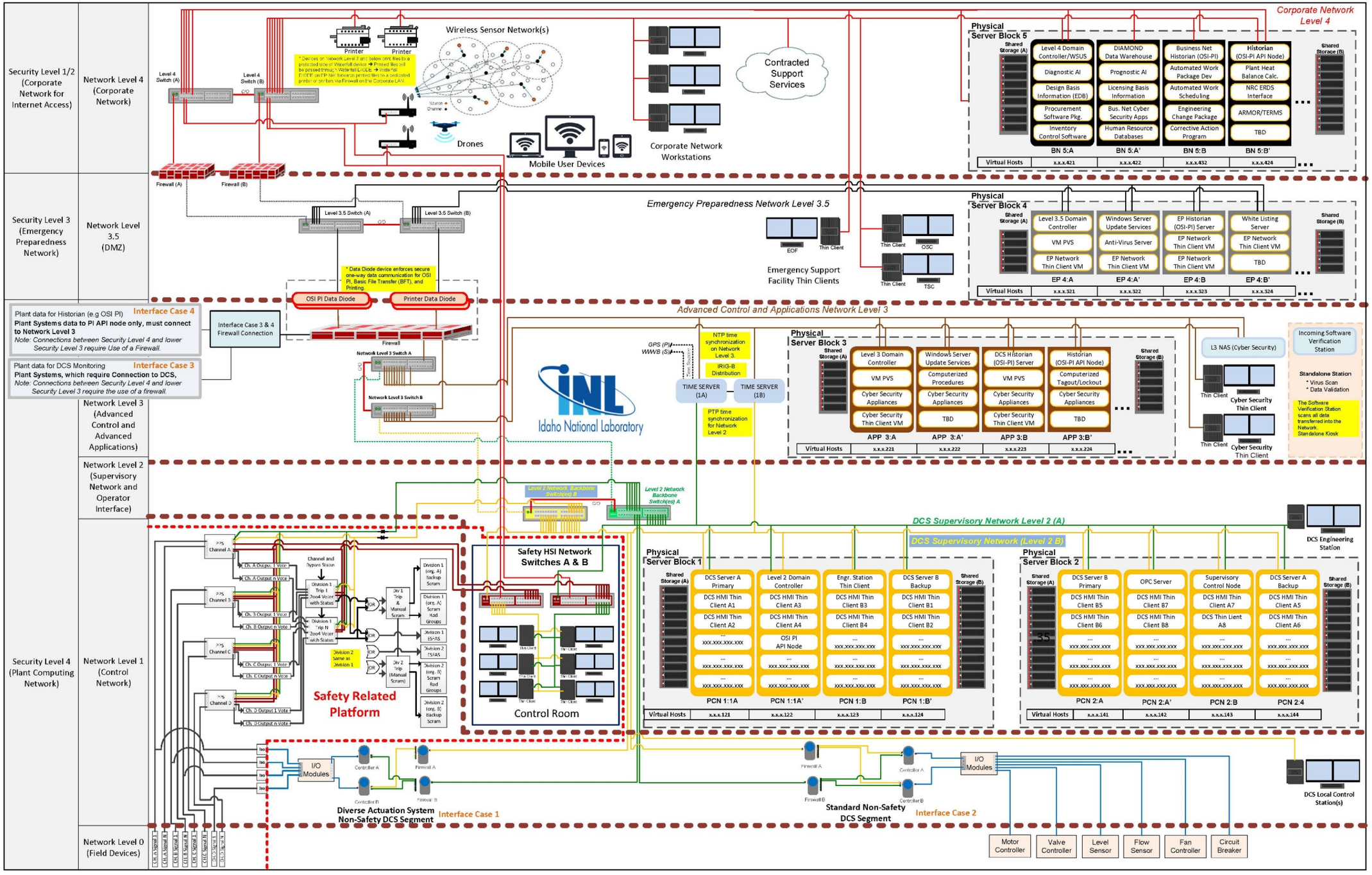
This document has presented a full-scope DI implementation and lifecycle support recommendations that will enable a plant life of 80+ years. For logical purposes associated with data flows, the DI and associated DA&A applications were presented from the bottom-up. Depending upon a unit's operational lifetime, concepts presented in this report can be applied either individually or as partial implementations. These may also be considered from the top-down perspective. For example, governance and administrative processes can be streamlined by DA&A software applications hosted at the Corporate Network Level 4 of the DI. While additional benefits could be obtained by coupling these software applications with digital data from new DI instrumentation and control (I&C) platforms at Network Levels 1, 2, and 3, a limited operational lifetime (e.g., <10 additional years) may not provide a sufficient return on investment to justify the new I&C platforms.

7. References

1. Thomas, Kenneth; Remer, Jason; Primer, Craig; et. al. 2020, "Analysis and Planning Framework for Nuclear Plant Transformation." INL/EXT-20-59537, Idaho National Laboratory https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_26540.pdf
2. "Codes and Standards," *Code of Federal Regulations*, Section 10, Part 55 (a), Section (h), "Protection and safety systems" (2021) https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0055a.html

3. “General Design Criteria for Nuclear Power Plants,” *Code of Federal Regulations*, Section 10, Part 50, Appendix A (2021) https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appa.html
4. “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants,” *Code of Federal Regulations*, Section 10, Part 50, Appendix B (2021) https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appb.html
5. “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition,” NUREG-0800, Nuclear Regulatory Commission. https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/index.html
6. NRC. “NRC Use of the Terms, ‘Important to Safety’ and ‘Safety-Related,’” Generic Letter 84-01 https://www.nrc.gov/docs/ML0311/ML031150515.pdf
7. “Functional Criteria for Emergency Response Facilities, Final Report” NUREG-0696, Nuclear Regulatory Commission. https://www.nrc.gov/docs/ML0513/ML051390358.pdf
8. “Emergency Planning and Preparedness for Production and Utilization Facilities” *Code of Federal Regulations*, Section 10, Part 50, Appendix E (2021) https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appe.html
9. “Criteria for Preparation and Evaluation of Radiological Emergency Response Plans in Support of Nuclear Power Plants,” NUREG-0654, Revision 2. Nuclear Regulatory Commission. https://www.nrc.gov/docs/ML1934/ML19347D139.pdf
10. “Protection of digital computer and communication systems and networks.” *Code of Federal Regulations*, Section 10, Part 73.54 (2015). https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html
11. “Cyber Security Programs for Nuclear Facilities,” Regulatory Guide 5.71, Nuclear Regulatory Commission, March 2009. https://www.nrc.gov/docs/ML0903/ML090340159.pdf
12. Hunton, Paul and England, Robert. 2019. “Addressing Nuclear I&C Modernization Through Application of Techniques Employed in Other Industries.” INL/EXT-19-55799, Idaho National Laboratory. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_20014.pdf
13. O’Hara, J.M., et.al. 2012. “Human Factors Engineering Program Review Model.” NUREG-0711, Revision 3, Nuclear Regulatory Commission. https://www.nrc.gov/docs/ML1232/ML12324A013.pdf
14. Preckshot, G. G. 1994. “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems.” NUREG/CR-6303, Nuclear Regulatory Commission. https://www.nrc.gov/docs/ML0717/ML071790509.pdf
15. “Branch Technical Position Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,” BTP-7-19, Revision 8 (January 2021). https://www.nrc.gov/docs/ML1601/ML16019A344.pdf
16. Hunton, Paul, et. al. 2020. “Vendor-Independent Design Requirements for a Boiling Water Reactor Safety System Upgrade.” INL/LTD-20-58490, Idaho National Laboratory. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_27502.pdf
17. NRC. “Digital Instrumentation and Controls Interim Staff Guidance #04, ‘Highly- Integrated Control Rooms – Communications Issues (HICRc),’” Revision 1, March 2009. https://www.nrc.gov/docs/ML0833/ML083310185.pdf

18. Merkiel, Steven L. 2020. “Common Q Platform and Component Interface Module System Elimination of Technical Specification, Surveillance Requirements.” WCAP-18461-NP, Revision 0, Westinghouse. https://www.nrc.gov/docs/ML2002/ML20020A009.pdf
19. “Branch Technical Position Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” BTP 7-14, Revision 6 (August 2016)
20. Paul Hunton and Charles Kiplin Smith, “Software Hazard Analysis for Distributed Instrumentation and Control System Platform (DICSP) using Honeywell Experion® PKS (Release 410) and Associated Infrastructure Hardware,” Document NED-I/INST-1004, Rev. 0, Duke Energy
21. “Segmentation Analysis for Watts Bar Unit 2 Distributed Control System” (August 2010) https://www.nrc.gov/docs/ML1022/ML102240384.pdf
22. “Safety Evaluation Report Related to the Operation of Watts Bar Nuclear Plant, Unit 2, Docket number 50-391,” NUREG-0947, Supplement 23 (July 2011) https://www.nrc.gov/docs/ML1120/ML11206A499.pdf
23. “Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems,” NUREG/CR-7006 (February 2010) https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr7006/index.html
24. “Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems,” NUREG/CR-6463 (June 1996) https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6463/index.html
25. NRC. “Digital Instrumentation and Controls Interim Staff Guidance #06, Revision 2, ‘Licensing Process.’” Revision 2 (March 2018) https://www.nrc.gov/docs/ML1826/ML18269A259.pdf.
26. Lybeck, Nancy; Thomas, Kenneth; Primer, Craig. 2020. “Plant Modernization Technical Program Plan for FY-2021,” INL/EXT-13-28055, Revision 10, Idaho National Laboratory. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_26801.pdf
27. “Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants,” *Code of Federal Regulations*, Section 10, Part 62 (2021) https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0062.html
28. Kovesdi, Casey, et. al. 2021, “Development of an Assessment Methodology that Enables the Nuclear Industry to Evaluate Adoption of Advanced Automation,” INL/EXT-21-64320, Idaho National Laboratory.


Security Level 1/2 (Corporate Network for Internet Access)
Network Level 4 (Corporate Network)
Security Level 3 (Emergency Preparedness Network)
Network Level 3.5 (DMZ)
Network Level 3 (Advanced Control and Advanced Applications)
Network Level 2 (Supervisory Network and Operator Interface)
Security Level 4 (Plant Computing Network)
Network Level 1 (Control Network)
Network Level 0 (Field Devices)
Corporate Network Level 4
Wireless Sensor Network(s)
Printer
Printer
Drones
Mobile User Devices
Contracted Support Services
Corporate Network Workstations
Physical Server Block 5
Shared Storage (A)
Level 4 Domain Controller/WSUS
Diagnostic AI
Design Basis Information (EDB)
Procurement Software Pkg.
Inventory Control Software
DIAMOND Data Warehouse
Prognostic AI
Licensing Basis Information
Bus. Net Cyber Security Apps
Human Resource Databases
Business Net Historian (OSI-PI)
Automated Work Package Dev
Automated Work Scheduling
Engineering Change Package
Corrective Action Program
Historian (OSI-PI API Node)
Plant Heat Balance Calc.
NRC ERDS Interface
ARMOR/TERMS
TBD
Shared Storage (B)
BN 5:A
BN 5:A'
BN 5:B
BN 5:B'
Virtual Hosts
x.x.x.421
x.x.x.422
x.x.x.432
x.x.x.424
Level 4 Switch (A)
Level 4 Switch (B)
Firewall (A)
Firewall (B)
Emergency Preparedness Network Level 3.5
Level 3.5 Switch (A)
Level 3.5 Switch (B)
EOF
Thin Client
Emergency Support Facility Thin Clients
OSC
TSC
Physical Server Block 4
Level 3.5 Domain Controller
VM PVS
EP Network Thin Client VM
Windows Server Update Services
Anti-Virus Server
EP Historian (OSI-PI) Server
EP Network Thin Client VM
White Listing Server
EP Network Thin Client VM
TBD
EP 4:A
EP 4:A'
EP 4:B
EP 4:B'
x.x.x.321
x.x.x.322
x.x.x.323
x.x.x.324
* Data Diode device enforces secure one-way data communication for OSI PI, Basic File Transfer (BFT), and Printing.
OSI PI Data Diode
Printer Data Diode
Firewall
Plant data for Historian (e.g OSI PI) Interface Case 4
Plant Systems data to PI API node only, must connect to Network Level 3
Note: Connections between Security Level 4 and lower Security Level 3 require Use of a Firewall.
Plant data for DCS Monitoring Interface Case 3
Plant Systems, which require Connection to DCS,
Note: Connections between Security Level 4 and lower Security Level 3 require the use of a firewall.
Interface Case 3 & 4 Firewall Connection
Advanced Control and Applications Network Level 3
Network Level 3 Switch A
Network Level 3 Switch B
Idaho National Laboratory
GPS (PI)
WWB (SI)
NTP time synchronization on Network Level 3.
IRIG-B Distribution
TIME SERVER (1A)
TIME SERVER (1B)
PTP time synchronization for Network Level 2
Physical Server Block 3
Level 3 Domain Controller
VM PVS
Cyber Security Appliances
Cyber Security Thin Client VM
Windows Server Update Services
Computerized Procedures
Cyber Security Appliances
TBD
DCS Historian (OSI-PI) Server
VM PVS
Cyber Security Appliances
Cyber Security Thin Client VM
Historian (OSI-PI API Node)
Computerized Tagout/Lockout
Cyber Security Appliances
TBD
APP 3:A
APP 3:A'
APP 3:B
APP 3:B'
x.x.x.221
x.x.x.222
x.x.x.223
x.x.x.224
L3 NAS (Cyber Security)
Cyber Security Thin Client
Incoming Software Verification Station
Standalone Station
* Virus Scan
* Data Validation
The Software Verification Station scans all data transferred into the Network Standalone Kiosk
Level 2 Network Backbone Switch(es) B
Level 2 Network Backbone Switch(es) A
DCS Supervisory Network Level 2 (A)
DCS Supervisory Network (Level 2 B)
DCS Engineering Station
Safety HSI Network Switches A & B
Physical Server Block 1
DCS Server A Primary
DCS HMI Thin Client A1
DCS HMI Thin Client A2
Level 2 Domain Controller
DCS HMI Thin Client A3
DCS HMI Thin Client A4
OSI PI API Node
Engr. Station Thin Client
DCS HMI Thin Client B3
DCS HMI Thin Client B4
DCS Server B Backup
DCS HMI Thin Client B1
DCS HMI Thin Client B2
PCN 1:1A
PCN 1:1A'
PCN 1:B
PCN 1:B'
x.x.x.121
x.x.x.122
x.x.x.123
x.x.x.124
Physical Server Block 2
DCS Server B Primary
DCS HMI Thin Client B5
DCS HMI Thin Client B6
OPC Server
DCS HMI Thin Client B7
DCS HMI Thin Client B8
Supervisory Control Node
DCS Thin Lient A8
DCS Server A Backup
DCS HMI Thin Client A5
DCS HMI Thin Client A6
35
PCN 2:A
PCN 2:A'
PCN 2:B
PCN 2:4
x.x.x.141
x.x.x.142
x.x.x.143
x.x.x.144
Safety Related Platform
Division 2 Same as Division 1
Control Room
Diverse Actuation System Non-Safety DCS Segment
Interface Case 1
I/O Modules
Controller A
Controller B
Firewall A
Firewall B
Standard Non-Safety DCS Segment
Interface Case 2
DCS Local Control Station(s)
Motor Controller
Valve Controller
Level Sensor
Flow Sensor
Fan Controller
Circuit Breaker