INL/RPT-24-80256
Revision 0

Light Water Reactor Sustainability Program

Integrated Operations for Nuclear: Work Reduction Opportunity Demonstration

August 2024

U.S. Department of Energy

Office of Nuclear Energy

INL/RPT 24-80256
Revision 0

Integrated Operations for Nuclear: Work Reduction Opportunity Demonstration

Paul J. Hunton
Senior Research Scientist, Principal Investigator – Idaho National Laboratory

Sean Lawrie
Chief Strategy Officer – Lumerra Corporation

August 2024

Idaho National Laboratory
Light Water Reactor Sustainability Program
Idaho Falls, Idaho 83415

http://lwrs.inl.gov

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

Page intentionally left blank

EXECUTIVE SUMMARY

The Idaho National Laboratory Light Water Reactor Sustainability Program (LWRS) Plant Modernization (PM) Pathway has been working with industry to leverage digital technology to extend the life and improve the operational and economic performance of the existing U.S. nuclear fleet. Two parallel and complementary efforts have been pursued by the PM Pathway to achieve these ends. Digital Infrastructure (DI) research has focused on leveraging available modern digital technology across a nuclear plant and integrating those technologies across a utility fleet consisting of both nuclear and non-nuclear generating units. Integrated Operations for Nuclear (ION) research has focused on optimizing the overall concept of operations for nuclear plants while holistically addressing people, technology, process, and governance (PTPG) issues to enable workload reduction opportunities (WROs).

INL/RPT-23-74393, “Pilot Business Case Analysis for Digital Infrastructure,” (DI BCA) captures initial efforts to synergize DI and ION at a target nuclear plant. In this case, a plant Owner (Vistra) of a two-unit Reference Plant (Comanche Peak) is looking to perform digital instrumentation and control (I&C) upgrades to address obsolescence, maintain or improve reliability, and reduce operating and maintenance costs. The Owner is also looking to implement other digital technologies to realize WROs to further reduce operating and maintenance costs and address labor shortages. The positive business case captured in the DI BCA assisted the Owner to obtain initial project approvals to upgrade 22 current safety and non-safety related I&C subsystems. This will be accomplished by migrating the function these I&C subsystems to or interfacing these subsystems with either a digital safety-related digital platform or a digital non-safety distributed control system (DCS) platform. This two-platform solution is being pursued to consolidate respective safety-related and non-safety related functions as presented in LWRS research report INL/EXT-21-64580, “Digital Infrastructure Migration Framework.”

The DI BCA document also identifies specific, digitally enabled WRO categories for further study. These were selected as most relevant by Reference Plant personnel from a larger list of WRO areas identified across the nuclear industry as captured INL/RPT-21-64134, “Process for Significant Nuclear Work Function Innovation Based on Integrated Operations Concepts.”

This ION WRO demonstration report was developed to provide illustrative, specific, and actionable direction for intertwined PTPG changes associated with digital modernization efforts. The coordinated changes in these areas are intended to maximize safe plant operational and economic performance. This includes enabling WROs associated with detailed configuration, implementation, and use of digital systems and how they are supported over their lifecycle. Illustrating this direction through a minimum set of advanced technology examples establishes a model PTPG framework that can be leveraged across the spectrum of nuclear plant digital modernization efforts going forward.

This document addresses many related concepts. To promote an integrated understanding of the topics that make up this work, this document contains an extensive set of internal hyperlinks. This set includes hyperlinks to page numbers in the table of contents, section numbers, items in lists, figures, tables, and references to other documents within the report. When hovering the cursor above hyperlinked text in Adobe, the cursor will change from “I” to “☝.” When the “☝” appears, a left mouse click will take the reader to the referenced location in the document. To return to the original location in the document, the reader need only press and hold the “alt” button on the keyboard and then simultaneously press the “<” directional key on the keyboard.

Section 1 provides a primer on general LWRS PM Pathway goals and describes the bases behind the collaboration between INL and the Owner to advance digital modernization efforts at the Reference Plant. It also provides brief summaries of ION and DI concepts which form the foundation for a new state PTPG construct proposed by this report. This new PTPG construct enables a digitally enhanced future state concept of operations which drives WRO realization. These concepts are presented in the context of using digital technology to “run the plant” safely and reliability while at the same time “running the business" of a nuclear site or fleet as efficiently as possible to maximize revenue. Included in this primer is an expanded version of a previous nuclear-unit-specific DI simplified architecture diagram to one that envelopes all digital systems within a utility corporate enterprise. It ends with a summary of lessons learned reports from recent nuclear plant digital I&C upgrades either performed or in progress that are leveraged in this current work as well as the need for culture change to fully realize the capabilities of digital modernization and associated PTPG changes to enable WROs.

Section 2 summarizes the DI BCA research report that was the impetus for this current work. It also summarizes why the scope of this current work was limited to two specific technical areas being pursued by the Reference Plant. These two areas are the implementation of a non-safety related DCS platform in the context of the DI and evaluation of an artificial intelligence (AI) software tool to realize software application assisted business process automation WROs.

Section 3 provides an overview of current state Reference Plant non-safety related analog I&C systems. It also discusses how the existing Plant Process Computer is being used to enable capabilities such as remote monitoring and diagnostics and emergency preparedness functions. Section 3 then summarizes a proposed future state where a non-safety related DCS is used to modernize current state Reference Plant I&C systems. DCS operations technology is then integrated with information technology, which together makes up the larger DI migration framework. This provides improved I&C capabilities and performance while expanding existing remote monitoring, diagnostics, and emergency preparedness capabilities to support WRO realization.

Section 4 provides more specific information with regards to capabilities associated with a modern DCS to provide the technical foundation for improved I&C system performance as well as lifecycle cost and workload reductions. A discussion of the DCS operations technology architecture is provided to aid in understanding how DCS capabilities enable changing the concept of operations for both "running the plant" and "running the business" of a nuclear utility. Additional capabilities supported by connectivity of the DCS with higher levels of the DI are then discussed. These include providing operators with digital tools associated with running the plant, keeping the DCS cybersecure, and expanded and more efficient support of nuclear site and fleet emergency preparedness capabilities. It also includes providing DCS collected data to IT systems for utility and vendor centralized DCS support to enable expanded remote plant diagnostic, prognostic, and logistics capabilities to deliver WROs.

Section 5 proposes transitioning the current site-centric I&C system governance model used at many nuclear utilities to a fleet model. A fleet model better aligns utility people, processes, and governance to capabilities enabled by DCS technology installation within the larger DI to deliver WROs. The fleet governance model standardizes DCS configuration and lifecycle support processes and procedures that are then accomplished more efficiently through a tiered fleet resource model. Enabling technical facilities including a single DCS fleet laboratory system and the deployment and use of new, site-specific glasstop simulators are also proposed. Glasstop simulators support the use of iterative modern techniques (e.g., the Agile development process) to more quickly converge DCS configuration and testing activities and to affect technology knowledge transfer from the DCS vendor to the utility. Glasstops also enable human factors engineering activities to develop and validate human-system interfaces developed as part of I&C digital modernization. Section 5 concludes with a presentation of a proposed organizational structure and associated responsibilities for the fleet governance model. Execution of organizational responsibilities in context is also presented through four process flowcharts that provide a structure for major activities associated with coordinated fleet DCS deployments and associated lifecycle support activities.

Section 6 describes efforts to apply an AI software tool at the Reference Plant as an Owner fleet pilot. This involves leveraging the AI tool in existing report creation by engineers, enabling WROs without significantly altering existing procedures and workflows. This is a novel nuclear industry application. The AI tool assists experienced report authors in quickly accessing, retrieving, and editing the data determined by the AI tool to be relevant based upon the context provided by author input, which enables authors to draft reports more efficiently. This approach leverages the AI's ability to provide relevant draft results based on input data on demand from a large knowledge base, allowing authors to focus on validating the content rather than manually searching through extensive historical documents, gathering pertinent information, and assembling the report. Lessons learned associated with this activity are presented. Some of these are technical and tool-specific, while others deal with organizational, intellectual property protection, and other business process challenges associated with such a first-of-a-kind effort. A comparative example of AI use is provided is provided in Appendices A and B.

The LWRS Program appreciates the research support provided by the Owner. This document makes no Owner commitments.

Page intentionally left blank

CONTENTS

FIGURES

TABLES

ACRONYMS AND DEFINITIONS

AI	Artificial Intelligence
ANI	Artificial Narrow Intelligence
ANS	American Nuclear Society
ANSI	American National Standards Institute
BAC	Boric Acid Corrosion
BCA	Business Case Analysis
CAP	Corrective Action Program
CFR	Code of Federal Regulations
CIP	Cybersecurity Critical Infrastructure Protection (standards)
CR	Corrective Action (an item identified for tracking in a utility Corrective Action Program)
DA&A	Data Architecture & Analytics
DCS	Distributed Control System
DI	Digital Infrastructure
Display	A software generated image which is presented on a video display unit (hardware screen) to present information to a user (e.g., a plant operator, an office worker, etc.)
DMZ	Demilitarized Zone (established to provide cybersecurity protection)
EC	Engineering Change
EOF	Emergency Operations Facility
EP	Emergency Preparedness
EP-Net	Emergency Preparedness Network
EPRI	Electric Power Research Institute
ERDS	Emergency Response Data System
FAT	Factory Acceptance Test
HA	High Availability (as it relates to functionality of paired, redundant DCS blades)
HFE	Human Factors Engineering
HSI	Human-System Interface
HSSL	Human-Systems Simulation Laboratory (located at the Idaho National Laboratory
HTI	Human & Technology Integration
I&C	Instrumentation and Control
INL	Idaho National Laboratory
ION	Integrated Operations for Nuclear
ISV	Integrated System Validation
IT	Information Technology

LLM	Large Language Model
LWRS	Light Water Reactor Sustainability (Program)
MCR	Main Control Room
ML	Machine Learning
NEI	Nuclear Energy Institute
NERC	North American Electric Reliability Corporation
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission\
O&M	Operations and Maintenance
OSC	Operations Support Center
OT	Operations Technology
Network Level	Purdue Industrial Control System Model Network Level (as depicted in Figure 4, Figure 7, and Figure 8)
PKS	(Experion) Process Knowledge System (a Honeywell DCS product)
PM	Plant Modernization
POC	Power Optimization Center (operated by Vistra Corporation)
PPC	Plant Process Computer
PRB	Project Review Board
PTPG	People, Technology, Processes and Governance
PV	Preliminary Validation
PVS	Passive Vulnerability Scanner
PWR	Pressurized Water Reactor
RG	Regulatory Guide
SAT	Site Acceptance Test
SDOE	Secure Development and Operating Environment
SIL	Software Integrity Level
SME	Subject Matter Expert
T&Q	Training and Qualification
TSC	Technical Support Center
V&V	Verification and Validation
VDU	Video Display Unit (computer physical screen)
VM	Virtual Machine
WRO	Work Reduction Opportunity

Page intentionally left blank

Integrated Operations for Nuclear: Work Reduction Opportunity Demonstration

1. INTRODUCTION

1.1 Plant Modernization Pathway Overview

The Plant Modernization (PM) Pathway of Light Water Reactor Sustainability (LWRS) Program at Idaho National Laboratory (INL) is focused on applying digital technology to enhance the ability of existing nuclear plants in the United States to operate for a total lifetime of 80-100 years. These nuclear plants are currently managed using a labor-centric operations model that is increasingly inefficient and costly to operate and sustain compared to modern generation plant operations, such as a natural gas combined cycle plant, or other comparable heavy industry applications, such as petrochemical facilities. Nuclear plants have been slower in applying modern digital technology, which can improve efficiency as well as attract and retain personnel to choose a career in nuclear.

An overview of the LWRS PM Pathway research objectives and goals are shown in Figure 1.

Plant Modernization Research Objectives and Goals				
Objectives	Extend the life and improve the performance of the existing fleet through modernized technologies and improved processes for plant operation and power generation. Develop modernization solutions that improve reliability and economic performance while addressing US nuclear industry's aging and obsolescence challenges. Deliver a sustainable business model that enables US nuclear industry to remain competitive.			
Research Areas	Digital Infrastructure	Data Architecture & Analytics	Human & Technology Integration	Integrated Operations for Nuclear
Outcomes	A multi-layered, sustainable digital foundation to enable plant modernization	Advanced monitoring and data processing to replace labor-intensive support tasks	Tools and methodologies that maximize efficiency while ensuring safety and reliability are maintained	Light water reactor fleet electric market competitiveness

Figure 1. LWRS PM pathway objectives and goals.

The Digital Infrastructure (DI) hosts Data Architecture & Analytics (DA&A) software applications as well as Human & Technology Integration (HTI) capabilities. Efforts in these areas are coordinated to enable Integrated Operations for Nuclear (ION) outcomes that enable the long-term, competitive operation of existing nuclear units in the United States.

1.2 Collaboration with Vistra Corporation

Vistra Corporation (referred to as the "Owner" in the remainder of this document) is a leading Fortune 500 integrated retail electricity and power generation company based in Irving, Texas, that provides essential power resources to customers, businesses, and communities from California to Maine.

The Owner is the largest competitive power generator in the United States, with a capacity of approximately 41,000 megawatts, or enough to power 20 million homes, operating in all of the major competitive wholesale markets in the country. The Owner is a leader in energy transformation and expansion with an unyielding focus on reliability, affordability, and sustainability, powered by a diverse portfolio that includes natural gas, nuclear, coal, solar, and battery energy storage facilities. The company continues to grow its zero-carbon resources, operating a fleet of nuclear power plants (NPPs), a substantial battery energy storage capacity, and a growing number of solar facilities.

Included in the Owner's generation portfolio are four nuclear plants with a total of six operating units. These units have a combined generating capacity of 6,365 megawatts. LWRS PM Pathway researchers have been working with the Comanche Peak Power Company, a subsidiary of the Owner, in their efforts to modernize the two-unit Comanche Peak NPP (referred to as the "Reference Plant" in the remainder of this document). The Owner intends to leverage the digital modernization efforts at the Reference Plant and at other nuclear plants in their portfolio. This activity is intended to directly support license renewal activities for these nuclear units. This document makes no commitments either for the Reference Plant or the Owner.

1.3 ION: Work Reduction Opportunity Demonstration

This report builds upon previous work performed by INL researchers, particularly in the areas of DI and ION. These previous efforts are capture in detail in the following reports:

- INL/EXT-19-55799, "Addressing Nuclear I&C Modernization Through Application of Techniques Employed in Other Industries" [1]
- INL/EXT-21-64580, "Digital Infrastructure Migration Framework" [2]
- INL/RPT-23-74393, "Pilot Business Case Analysis for Digital Infrastructure" [3]
- INL/RPT-23-74671, "Integrated Operations for Nuclear: Work Reduction Opportunity Demonstration Strategy" [4]
- INL/RPT-22-68671, Revision 1, "Integrated Operations for Nuclear Business Operation Model Analysis and Industry Validation" [5].

The remainder of Section 1 provides an overview of the concepts contained in the above documents and relates them to this current work to demonstrate the application of ION for a selected set of modernization enabled work reduction opportunities (WROs) by advancing their incorporation into approved projects. If the reader has previously reviewed and is conversant in topics covered by [1] through [5], the reader may choose to proceed directly to Section 2.

1.3.1 ION Concept

The ION concept, developed by the LWRS PM Pathway, provides a comprehensive, business case-driven strategy to support plant modernization for the U.S. nuclear fleet. Its primary objective is to transition the existing labor-centric nuclear plant operating model into one that is increasingly more technology-centric. An ION business transformation aims to maintain or improve plant safety and operating capacity factors while reducing total ownership cost and enabling extended plant operational lifetimes.

Applying digital technology by itself to the existing plant concept of operations can provide some opportunities to reduce operations and maintenance (O&M) costs. A more impactful result requires a technology-enabled transformational change to the plant concept of operations.

The following subsections provide a brief discussion of the current state concept of operations. They then describe a transition to an envisioned new state concept of operations to provide context for ION WRO demonstration. A more detailed presentation of this information is provided in [3].

1.3.2 Current Concept of Operations

A simplified depiction of a generic current state concept of operations for existing nuclear plants is provided in Figure 2. This presentation was developed around a single plant view. For a utility with a fleet of nuclear units, variations of the same model would apply to them all individually as well as to the whole fleet.

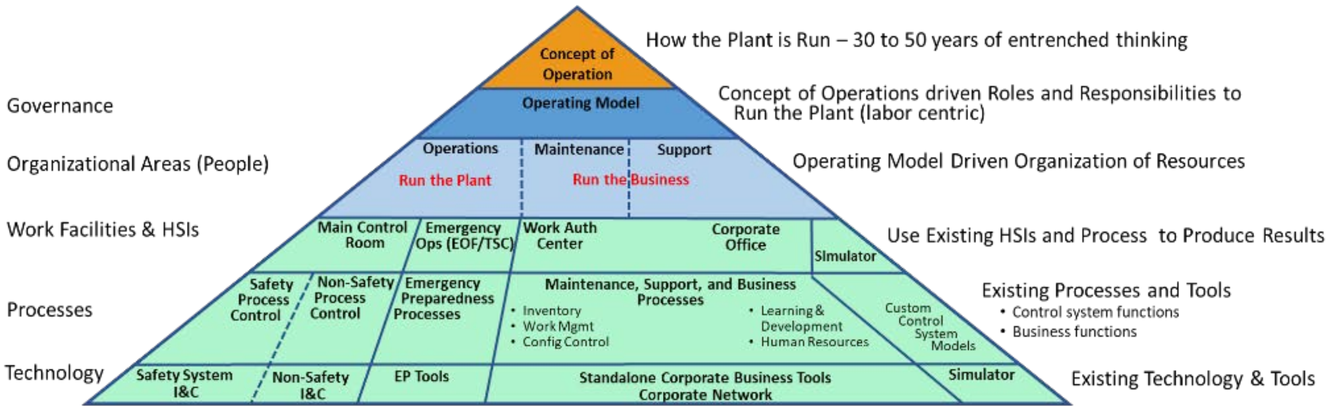


Figure 2. Current state concept of operations diagram.

The top two layers of the pyramid shown in Figure 2 depict the existing overall concept of operations and the governing operating model associated with it. The current concept of operations is focused on maintaining safety margins and maintaining or improving plant capacity factors. This has resulted in high levels of operational performance and capacity factors of over 92% for the U.S. commercial nuclear fleet (What is Generation Capacity? | Department of Energy). Efforts to establish and maintain this continued level of safety and operational performance, however, have largely been focused on maintaining the status quo by maintaining existing systems using existing labor-centric processes.

The third layer from the top of Figure 2 identifies the three fundamental organizational areas needed to implement the concept of operation. To further simplify the discussion and relate it to the technology-enabled layers shown in the three lowest layers in Figure 2, these organization areas are grouped under the following categories:

A. **Run the Plant** (Operations)—Activities directly related to personnel who:
   - Operate the plant through instrumentation and control (I&C) systems in all operating modes
   - Providing capabilities to enable emergency response personnel to directly assist operations personnel in the event of a nuclear plant emergency.

B. **Run the Business** (Maintenance and Support)—Activities that do not directly relate to the operation of or providing emergency response capabilities to "run the plant" but without which sustained plant operation cannot continue. If the "run the business" function is not performed, the plant will soon be unable to operate because of equipment failures, failure to meet regulatory commitments, inability to train personnel, economic obstacles, etc.

1.3.3 DI-Enabled ION New State Concept of Operations

Figure 3 provides a depiction of a digitally enabled new state concept of operations that is intended to replace the current labor-centric model with one that is more technology-centric.

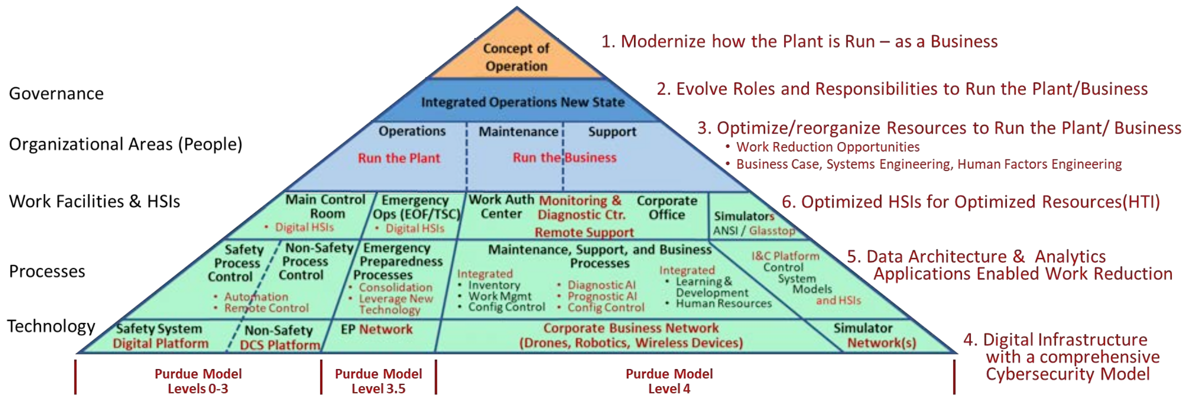


Figure 3. ION-enabled new state concept of operations diagram.

ION documentation [5] refers to people, technology, processes, and governance (PTPG) that support any concept of operation construct. These items are shown on the left in Figure 2 and Figure 3 to align with the rest of the diagrams. Specific steps, numbered as aligned on the right of Figure 3, to transition from the existing concept of operations shown in Figure 2 to that shown in Figure 3 are:

1. **Modernize how the plant is run as a business**

   The plant concept of operation is modernized through the holistic deployment of digital technology as justified by business case analyses to provide maximum operational and financial benefit.

2. **Evolve roles and responsibilities to run the plant and business**

   General digital technology application and the process improvements they enable can fundamentally alter existing roles and responsibilities of organizations that "run the plant" and "run the business." The target of this effort is to be more revolutionary than evolutionary (as has occurred in nearly all sectors that have embraced digital capabilities). For example, I&C and non-I&C digital technologies are capable of capturing and indefinitely retaining configuration-controlled data records. Digital systems can now make these records available anywhere in the world for retrieval and analysis. These capabilities can have a significant impact on the roles, responsibilities, numbers, and locations of utility staff currently charged with capturing, managing, and leveraging this data.

3. **Optimize and reorganize resources to run the plant and business**

   The results of Steps 1 and 2 for WROs are aggregated and evaluated. Roles and responsibilities of the remaining staff are reallocated to maximize harvestable labor savings through staff attrition. Work may be centralized at remote locations or outsourced as enabled by technology to achieve cost efficiencies. The number of auxiliary operators in the plant may also be reduced through remote control and automation capabilities provided by modern digital I&C systems. This optimization and reorganization effort realizes aggregate O&M cost savings.

4. **Deploy a DI with a comprehensive cybersecurity model**

   The DI is the foundational technology that enables Steps 1–3. This is accomplished through the bottom technology layer of Figure 3 in red. The Purdue Industrial Control System Model Network Levels shown at the bottom of Figure 3 are aligned with the Purdue Network Model Levels shown on the left of the simplified single NPP DI diagram provided in Figure 4 from [2]. For simplicity, the term "Network Level" is used to signify "Purdue Industrial Control System Model Network Level" in the remainder of this document. A key concept associated with the DI diagram is to consider the entire construct as a whole, made of separate but integrated "domains" shown in different color boxes (e.g., red, green, etc.) within Figure 4.

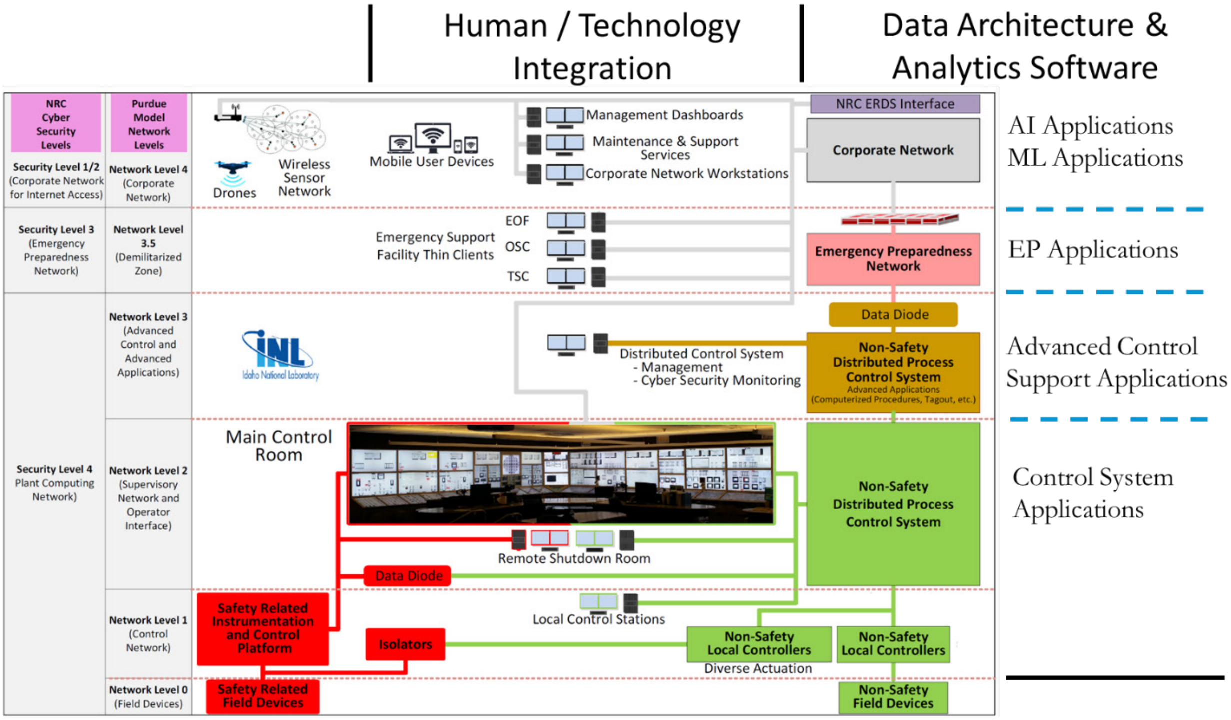


Figure 4. Simplified DI diagram for a single nuclear unit.

"Run the plant" activities are accomplished by Operations personnel monitoring plant status and directing control actions using I&C and operations technology (OT) equipment at Network Levels 0–3 as depicted in Figure 4. Because of their function, these capabilities fall within the purview of 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," [6] as shown at the far left of Figure 4 under the Nuclear Regulatory Commission (NRC) Cyber Security Level 4—Plant Computing Network. Personnel performing emergency preparedness (EP) activities leverage the Emergency Preparedness Network (EP-Net) equipment shown at Network Level 3.5 in Figure 4. Digital systems used for EP also fall within the purview of [6] and are associated with NRC Cyber Security Level 3—EP-Net as shown in on the left of Figure 4.

"Run the business" activities are accomplished by Maintenance and Support staff using equipment at information technology (IT) equipment at Network Level 4. The capabilities to "run the business" do not fall within the purview of [6].

Details with regard to how cybersecurity infrastructure capabilities fit into the DI as architected are provided in Section 2.3 of [2].

It is expected that, for utilities that have already been pursuing significant DI upgrades, these as well as new efforts will be aggregated and integrated over time to more fully enable the DI construct as depicted in Figure 4. Enveloping these efforts in one overarching DI provides for an economy of scale, standardization of design, and development of a standard, overarching cybersecurity defensive architecture.

The DI by itself is just that, an infrastructure. It provides the physical electronic equipment (input/output [I/O] modules, controllers, servers, networking equipment [switches and routers] and user workstation human-system interfaces [HSIs]) to present results to people. It also includes firmware, operating software, and cybersecurity capabilities to host and protect application software and databases. Specific capabilities to "run the plant" and "run the business" are enabled by deploying specific DA&A applications at the proper levels of the DI based upon the capability to be provided.

5. **Data architecture and data analytics applications enable work reductions**

   "Run the plant" applications are loaded onto either the safety-related or non-safety related I&C systems shown in Network Levels 0–3 in Figure 4. These directly enable operating the nuclear plant by providing indications and manual controls as well as increased capabilities for automation. This software is typically purpose-developed to directly support the plant control function and system diagnostics. While EP-Net applications at Network Level 3.5 are not directly used in plant operation, they are necessary to support plant operation in emergency situations. As the I&C systems become increasingly digitized, data and HSIs created for the control system can be directly replicated in EP facilities at very little additional cost. Additional purpose-built HSI software displays to support the EP function can also be developed using the expanded I&C digital dataset.

   Network Level 4 hosts all "run the business" software applications generally captured in the areas of Maintenance and Support. This includes all logistics, human resources, and other administrative tools. Data from across the DI can also be gathered and correlated here and analyzed by increasingly capable artificial intelligence (AI) diagnostic and prognostic software tools. These tools will over time produce results that may be significantly impactful in supporting plant Operations. The use of "run the business" applications information by Operations personnel to inform plant operation decision-making must be properly controlled (through revised processes).

   "Run the business" applications can be used to inform plant operators of conditions or events that may be identified by applications hosted at Network Level 4. The use of Network Level 4 applications (such as the output of AI and prognostic applications analyzing plant operational information) to inform plant operation must be properly controlled (through governance and process) to provide the necessary functionality at the proper level of the DI to optimally provide the functions needed to realize WROs. Example DA&A application capabilities are shown in red in the process layer of Figure 3 and similarly on the right of Figure 4.

6. **Optimize HSIs for the optimized workforce that remains through human-technology integration**

   For the people who will be using the DA&A applications hosted on the DI to accomplish their tasks as efficiently and error-free as possible, a properly developed set of HSIs needs to be developed. HTI research is leveraged to ensure the safe and reliable use of advanced technologies by personnel. This effort is reflected in updates to the work facilities and HSI layer as shown in Figure 3 and the HSIs shown at multiple layers of the DI as shown in the center of Figure 4.

Coupling the ION concept with the application of DI, DA&A applications, and HTI provides a mechanism to reallocate current labor and rely on technology and automation to streamline selected work activities. Utilities may also centralize or outsource source certain tasks (e.g., engineering, fuels) to vendors to more efficiently accomplish those tasks.

1.3.4 Integration of Modern I&C Systems into Plant Simulators

Each nuclear plant site also leverages a high-fidelity main control room (MCR) simulator for operator training and qualification (T&Q). The simulator fully replicates the plant MCR HSIs represented by the imbedded picture near the center of Figure 4. A simplified representation of the capabilities in an existing simulator, such as at the Reference Plant, is provided in Figure 5.

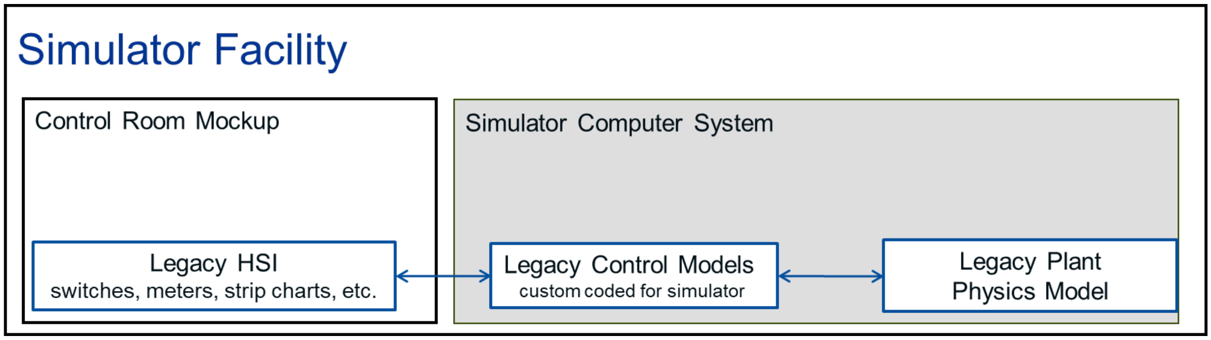


Figure 5. Simplified MCR T&Q simulator facility (existing capability).

Existing simulators were developed to mimic the performance of legacy analog instrumentation and discrete controls based upon 1970s technology. Legacy physics-based plant model fidelity has improved significantly over the years due to improved modeling software coupled to vastly improved computing power and speed. Simulator vendors have developed custom algorithms to mimic legacy analog control system performance, to present information using legacy analog indications that mimic those in the plant, and to accept control inputs from legacy control devices (switches). Where limited digital upgrades have been installed in the plant, simulator vendors have developed upgrade-specific custom control models and HSI capabilities to mimic those in the plant MCR.

The Owner is pursing digital I&C systems upgrades, leveraging a two-platform solution as depicted in Figure 4, and evaluating the degree to which these platforms can be integrated into their Reference Plant simulator facility and how the digitally upgraded simulator will connect to their larger DI. A method to realize and leverage this connectivity is provided in Figure 6.

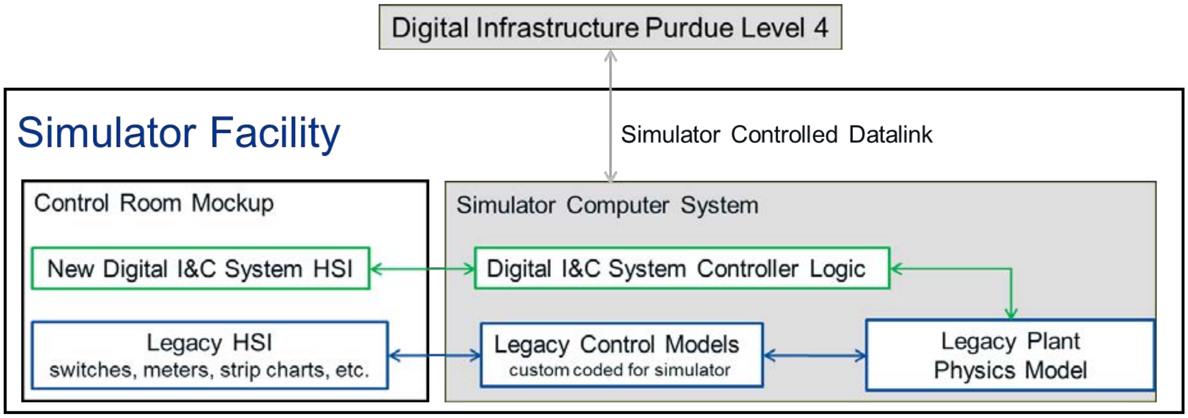


Figure 6. Simplified MCR T&Q simulator facility (expanded capability).

The method and level capability shown in Figure 6 within the simulator facility is highly interdependent with design decisions made with respect to the upgraded I&C system design envisioned for the plant. The degree to which the simulator facility can be leveraged beyond the facility itself is dependent upon the degree of connectivity between the simulator computer system and the rest of the DI. This project assumes the Owner will endeavor to maximize capabilities both within the simulator facility itself and as part of the larger DI. This summary of simulator integration discussion is provided here to aid in the discussion of fleet DI integration described in Section 1.4. The creation and use of a glasstop simulator using the same technology leveraged in the MCR T&Q facility is further presented in Section 5.3.

1.4 Fleet DI Integration for Expanded ION Implementation

As stated in Section 1.2, previous LWRS PM Pathway research work with the Owner has been focused on modernizing the Reference Plant. The Owner now intends to leverage the digital modernization efforts at the Reference Plant to other nuclear plants in their portfolio and to integrate these efforts with similar ones across their entire electric generation portfolio. This expanded effort needs a larger, utility-wide DI construct. Figure 7 proposes such a construct as an outgrowth or the simplified DI for a single nuclear unit provided in Figure 4.

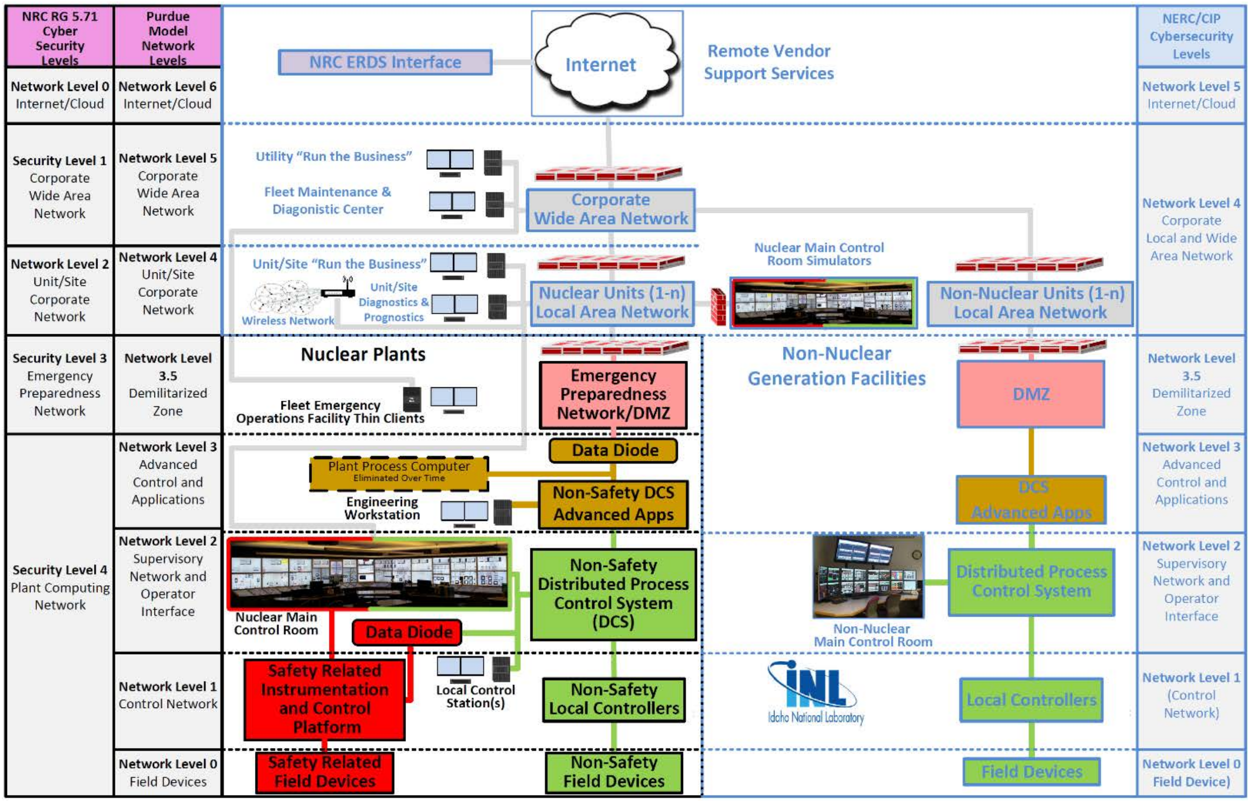


Figure 7. Fully integrated fleet DI for a diverse utility (nuclear and non-nuclear).

There are several key additions made to the fleet DI construct in Figure 7 compared to Figure 4, including:

- A more complete instantiation of NRC-defined Cybersecurity Levels 2, 1, and 0 from Figure 6 in NRC Regulatory Guide (RG) 5.71, "Cybersecurity Programs for Nuclear Power Reactors" [7] as shown on the left of Figure 7.
- Integration of the qualification and training nuclear plant simulator (as well as glasstop simulators discussed in Section 5.3) into the DI. Such an integration can leverage and integrate MCR operator training simulators with digital systems already required to be present at nuclear sites to support performing more realistic EP drills. Through fleet digital connectivity shown in Figure 7, the functionality of multiple existing, standalone, site-specific Emergency Operating Facilities (EOFs) for a fleet can be replaced by one centralized location that consolidates the functions of all. Such consolidation can significantly reduce the physical infrastructure costs to maintain multiple EOFs. It can also enable significant WROs by reducing the number of qualified individuals necessary to support multiple EOFs to those needed to support the one consolidated facility.

- Incorporation of a non-nuclear DI construct and corresponding North American Electric Reliability Corporation (NERC) cybersecurity critical infrastructure protection (CIP) levels that apply to utilities with non-nuclear generation sources, which is shown to the right of Figure 7.
- Integration of the nuclear and non-nuclear DIs into a single construct that:
    - Connects the two into one comprehensive construct to enable a more coordinated capability to "run the business" of a utility with a diverse nuclear and non-nuclear generating fleet
    - Identifies that the construct is expandable to include multiple nuclear and non-nuclear generating units (1-n)
    - Clearly delineates within the comprehensive construct where cybersecurity requirements are different:
        - Areas that fall under NRC purview (shown in black outlined boxes with black text)
        - Areas that fall under the North American Electric Reliability Corporation or the utility (shown in blue outlined boxes with blue text).

This broader view of DI provides additional perspective with regards to the architecting nuclear digital technology upgrades (hardware, dataflows, and software applications) to support ION within a utility-wide integrated operations framework.

1.5 Similar Project Lessons Learned and Culture Change to Enable a New State

1.5.1 Lessons Learned

INL researchers have either been directly involved with or provided support for several large-scale digital modernizations at multiple NPPs. In collaboration with participating utilities, several reports have been generated. The most notable of these include:

- For a multiunit and multisite non-safety related digital I&C modernization at Duke Energy (Robinson, Harris, and Brunswick NPPs)
    - INL/EXT-19-55799, "Addressing Nuclear I&C Modernization Through Application of Techniques Employed in Other Industries" [1]
- For a multiunit safety-related and non-safety related digital I&C modernization at Constellation (Limerick Generating Station)
    - INL/EXT-20-59809, "Safety-Related Instrumentation and Control Pilot Upgrade: Initial Scoping Phase Implementation Report and Lessons Learned" [8]
    - INL/RPT-23-72105, "Safety-Related Instrumentation and Control Upgrade: Conceptual – Detailed Design Phase Report and Lessons Learned" [9]

These documents describe technical, licensing, and programmatic details with regards to activities performed for these upgrades as well as associated lessons learned.

1.5.2 Embracing Disruptive Culture Change to Enable Digital Technology Benefits While Addressing Related Challenges.

Attachment B to the Electric Power Research Institute (EPRI) Digital Engineering Guide [10] discusses optimizing a digital engineering organization. This section summarizes, modifies, and adapts the information in Attachment B of [10] as well as INL experience and industry lessons learned (e.g., [1], [2], and [9]) for applicability to the Owner's planned fleet digital modernization effort.

Digital technology has been disruptive in every industry into which it has been introduced. When embraced, properly managed, and leveraged, this disruption can result in revolutionary operational improvements and efficiencies while retaining or improving upon current levels of safety and reliability. To achieve this end, the U.S. nuclear fleet must address characteristics that impact the optimal application of digital technology, including:

A. Establishing new, faster, and cheaper ways to digitize standalone legacy functions, to improve their functionality (by adding control system automation or advanced data processing), and to enable digital communications to aggregate previously separated legacy functions. This drives higher levels of functionality between people, between digitized functions, and between people and digitized functions, which is necessary to optimize overall facility performance.

B. Updating or replacing existing compartmentalized, overly formalized, and linear design change processes used in nuclear power to identify, prioritize, design, factory test, install, post-modification test, and provide lifecycle support for existing systems. Legacy processes for modifications or upgrades predate holistic and iterative (Agile) digital technology modernization efforts. New processes and organizational structures need to be established that are more compatible with delivering, commissioning, and maintaining modern, digital systems in a timely, repeatable, and sustainable manner.

C. Improving and revamping the qualification of current "system engineers" and "design engineers." Their current training is biased toward maintaining current systems. A pipeline needs to be developed for qualifying digital "system**s** engineers" who understand how the plant is to operate and how modern digital systems can be best applied and sustained to optimize plant operation considering the plant design and licensing bases. This needs to occur in concert with procedure and organization structure changes identified in item B) directly above. The attraction and retention of digital workers is dependent upon providing them with an understanding that they will be working on state-of-the-industry technology with a defined career path that maintains and improves their skills so they remain current with technology advancements.

D. Leveraging rapid progress in digital equipment hardware technology and software features that has been driven by relentless commoditization. At the same time, it must be recognized that such progress results in short commercial digital system lifecycles by nuclear industry standards. The time to implement current nuclear processes to conceive, design, install, and commission nuclear digital upgrades can take longer than entire lifecycle of the selected hardware and software versions of vendor technology selected as part of this effort. Techniques need to be identified to improve the timeliness of performing digital upgrades. Digital systems upgrade designs can also be developed in a manner to permit implementation during plant power operations as opposed to during refueling outages.

E. Adopting streamlined techniques for applying regular software and firmware update patches, cybersecurity definition updates, and vendor-warranted form, fit, and function hardware replacements outside of the burdensome design change process while maintaining digital system performance and configuration control. Treating such function sustaining activities as "design changes" using legacy processes can significantly add to the cost associated with digital upgrades.

F. Adopting a "fleet-centric" over the existing a "unit-centric" or "site-centric" digital system support model. The rapidly evolution of digital technology coupled with its high reliability tends to result in a bursts of activity surrounding initial installations or system-level modification and updates followed by extended periods of very low activity to support the system at a particular unit and site. Consequently, maintaining a fully qualified and proficient staff at each particular unit and site can be difficult, inefficient, and costly. Alternate support models need to be developed to better optimize utility labor resources to match this digital technology induced environment.

1) Utilities that operate a fleet of nuclear units may be best served by establishing a multitiered support model that includes:
    a. A minimal support staff to perform periodic and routine system checks as well as tightly bounded repair activities (e.g., swapping out self-configuring line replaceable units).
    b. A utility-staffed fleet digital systems support group shared by all of its units, which would be the utility design authority of the digital I&C systems across the fleet and provide the level of support typically needed between major system expansions or updates.
    c. Contracted vendor(s) to provide support for major system expansions or updates along with troubleshooting support for complex and challenging system issues.
2) Smaller or single site nuclear utilities could maintain a more capable local support group while still outsourcing digital system support to larger utilities or to vendors to optimize system support staff and cost as much as practicable.

G. Standardizing design and related processes. The degree to which the industry in general and vendors and utilities in particular can standardize digital upgrade designs and associated evergreen lifecycle support capabilities will directly aid in lowering implementation and lifecycle costs through economies of scale.

H. Establishing closer collaboration between those who are responsible for OT systems shown as Network Levels 0–3 of Figure 7 and the IT organizations responsible for Network Levels 3.5–5 both within its nuclear facilities and across the utility's larger nuclear fleet.

I. Providing sustained commitment for a 6–10 year process to accomplish the first full set of digital upgrades and to establish lifecycle support strategy that will likely extend another 30 years or longer after that (to the end of plant life).

Section 2 of this paper identifies how the characteristics listed in this section influenced the selection of the specific WROs from the initial business case analysis (BCA) [3] for further analysis. The rest of the paper details more specific and coordinated PTPG capabilities and attributes to enable WROs realization.

2. PILOT BUSINESS CASE WRO IDENTIFICATION AND FOCUS FOR FURTHER ANALYSIS

2.1 Digital I&C Upgrade Original Business Case

INL/RPT-23-74393, "Pilot Business Case for Digital Infrastructure" [3], captures the BCA performed for the digital modernization project being proposed at the Reference Plant. This project includes upgrades of 22 safety-related and non-safety related I&C subsystems, which is intended to be accomplished by leveraging a two-platform solution where safety-related I&C functions are migrated to or interfaced with a safety-related digital I&C platform and non-safety related I&C functions are migrated to a non-safety related digital distributed control system (DCS). This BCA analysis also leverages WROs identified by ION researchers to provide a more holistic presentation of integrated cost savings enabled by digitalization.

Reference [3] provides additional research to address concerns associated with the potential high implementation costs of plant I&C upgrades. It also captures the application of the BCA methodology from [11] on an expanded set of safety-related and non-safety related I&C digital upgrades envisioned for implementation at the research target Reference Plant for this research. The Reference Plant is a Pressurized Water Reactor. Reference [3] identifies upgrades of 22 current safety-related and non-safety related I&C subsystems by migrating their function or interfacing equipment that performs their function into either a safety-related digital platform or a non-safety related DCS platform. This two-platform solution is being pursued to consolidate respective safety-related and non-safety related functions as presented in LWRS research report INL/EXT-21-64580, "Digital Infrastructure Migration Framework" [2].

The resultant BCA provides a Net Present Value for the upgrade project and an Internal Rate of Return. The detailed BCA for applying the two-platform I&C solution from [2] provides a compelling case for these digital I&C upgrades. Table 1 from [3] summarizes the order of magnitude and nonproprietary results of this BCA for the baseline case for 30 and 50 years of continued operations.

Table 1. Net present value of I&C digital modernizations for 30 and 50 years.

Scenario Title	Payback Period	Net Present Value	Internal Rate of Return
Baseline (30 Years of Continued Operation)	17.8 years	$74M	8.1%
Baseline (50 Years of Continued Operations)	17.8 years	$685M	11.8%

The BCA [3] also estimated the opportunity cost of lost generation revenue from equipment reliability events due to the failure of current I&C components for long-term operations. It determined that avoiding a single I&C obsolescence-induced 7 day forced outage during the summer (at $300/MWh) during the next 30 years would result in an immediate breakeven business case for the digital I&C upgrade.

The BCA [3] was presented to Owner senior leadership demonstrating the upgrade's economic viability. This directly contributed to the Owner including the full scope of this project in their long-range plan for long-term plant operations.

2.2 Identification of WROs for Further Analysis

INL researchers who developed this current work determined that examining the expansive scope of digital I&C upgrades and ION WRO areas as identified in the Reference Plant BCA [3] would provide only a generalized result. To provide the most illustrative, specific, and actionable direction for WRO enabling digital modernization PTPG changes, researchers selected two specific technical areas being pursued by the Reference Plant to focus their efforts. These are described in the subsections 2.2.1 and 2.2.2.

Such a down selection focused INL research efforts to provide intertwined PTPG changes that will enable future detailed design, implementation, and lifecycle support strategies for the selected areas to realize WROs for these digital modernization efforts. It is also intended to provide a roadmap for additional digital modernization efforts to enable similar WRO associated with them to go forward. This is particularly important to the Owner as it plans to leverage this research to guide digital modernization efforts not only at their Reference Plant but also across their larger nuclear fleet. It also benefits the larger industry by providing recommended PTPG changes that are generally applicable for similar digital modernization efforts at other nuclear utilities.

2.2.1 Detailed Study of Non-Safety Related Digital I&C System Benefits and Design and Lifecycle Support Strategies

The Owner is currently in the conceptual design phase for the planned digital I&C upgrade described in Section 2.1. A key enabler for the long-term technical and economic viability of the Reference Plant is to provide architecture guidance for the non-safety related DCS within the Owner's fleetwide DI in a way that integrates with and enables proposed ION PTPG changes to deliver on identified WRO savings.

Enabling non-safety related DCS platform technology capabilities provided by the non-safety related DCS platform are identified in Section 4.

Related enabling process and governance capabilities to leverage DCS platform technologies to empower a more efficient use of people are identified in Section 5.

2.2.2 Practical Application of AI for Plant Support Activities

Digitizing activities through software, as enabled by the integrated build out of the DI as depicted in Figure 7, allows for applying AI across the utility enterprise to improve efficiency in support processes used to “run the business.” For example, current maintenance scheduling is performed manually and requires a unique skill set. The collection and analysis of additional equipment condition data over time enables the schedulers to make informed decisions and estimations about the best time to take equipment out of service and repair it. These activities are labor intensive and require a high degree of knowledge and iteration. A utility that operates several nuclear units is working to enable work reductions in maintenance scheduling by leveraging and integrating this data into an AI model capable of inference to optimize the scheduling process while reducing workload. These AI tools are intended to enable schedulers to more quickly identify optimal methods to schedule maintenance or order new components for installation. Through use, the model is continuously provided with more schedule input data that improves its future predictions.

AI-assisted maintenance scheduling as described above can be easily simulated to test the performance of different AI models to optimize the process. Using AI in this case is benefited by the fact that the set of input information provided to the AI tool can be focused and bounded. This better enables the AI model’s ability to continuously learn and provide schedulers with improved recommendations that they can validate. Instead of waiting until a component breaks or is about to break, schedulers can calculate and predict component lifecycles based on historical and current data and assist in scheduling work in a way where maintenance contractors are hired to support focused periodic maintenance sessions that minimize failures. AI models can synthesize all the information they have access to into data-supported decisions for the scheduler to validate, while consistently improving over time as they ingest statistically significant amounts of data. This not only enables maintenance scheduling WRO costs but also enables the plant to operate more smoothly and reliably during longer operating periods to maximize revenue.

While some utilities have been applying AI to improve efficiency for processes like maintenance scheduling, AI is also being researched for additional applications in the nuclear power industry. In Section 6, one expansive use is being pursued by the Reference Plant to apply AI technology to draft engineering evaluations and reports. This pilot project at the Reference Plant demonstrates how recent AI advancements have automated traditionally manual tasks, providing valuable insights relating to the implementation process, challenges, and lessons learned that come with integrating AI solutions into current support processes.

Digitizing safety and non-safety related control systems at NPPs provides many opportunities to collect significant data on plant equipment for additional monitoring purposes and maintenance decision support.

3. DIGITAL NON-SAFETY I&C CURRENT STATE AND TARGETED NEW STATE

3.1.1 Current State Technology

3.1.1.1 Existing I&C Systems Scoped for Replacement

The research scope of the non-safety related digital I&C upgrade strategy for the Pressurized Water Reactor Reference Plant includes the digital modernizations of the subsystems below:

- Westinghouse 7300 non-safety related analog control system platform. This platform is still supported by Westinghouse, but it is implemented using 1970s technology and design concepts.

These design concepts, while proven, do not provide any advanced control, redundancy, diagnostic, lifecycle support, and remote support capabilities provided by modern digital systems. Analog systems require significant and increasing amounts of maintenance, manual component calibrations, and periodic surveillances. As they age, analog systems become less reliable and require more frequent repair. Obtaining replacement parts on platforms such as the 7300 is also increasingly challenging over time. This translates to cost for the plant as shown in the BCA provided by [3]. Establishing and maintaining personnel qualifications on antiquated analog platforms is increasingly costly to utilities and unattractive to the utility workforce who expect to work on modern systems to maintain and grow their skills.

The 7300 non-safety related control system platforms supports a myriad of nuclear steam supply system non-safety related reactor plant control functions as well as balance of plant control functions that directly support the operation of systems and equipment that support operation of the nuclear plant steam cycle.

- Existing electronic (analog or obsolete digital), pneumatic, hydraulic, and mechanical control systems or direct manual controls that are either standalone or interface with other control systems. These are similarly increasingly obsolete and difficult and costly to operate and maintain. These control systems also introduce many single-point vulnerabilities that can challenge power production. Finally, these systems all suffer from a lack of ability to find, train, and retain personnel with the qualifications and interest to support such systems.
- Sensing devices, contained within the sensing circuits of both the non-safety related 7300 system and the safety-related 7300 system, used to provide indications to the non-safety related plant process computer (PPC). Safety-related signals obtained by the PPC are provided through safety-related isolation devices.

3.1.1.2 Existing I&C Data Capture Systems, Diagnostics, and Remote Support Capabilities

Where certain standalone digital I&C systems are in place (such as the upgraded turbine control system and feed pump control system in the Reference Plant), these can possess limited local capabilities to capture and trend related process values, record alarms, and capture and present diagnostic information. This data is not typically transmitted outside of these systems and is obtained locally by leveraging maintenance and test equipment.

The majority of live digital plant data that the Reference Plant collects, captures, and presents is primarily accomplished through the PPC. Functionality of the PPC is largely provided to meet utility commitments to implement NUREG-0696, “Functional Criteria for Emergency Response Facilities” [12]. The PPC also provides data to meet commitments to support Emergency Response Data System functionality as described in NUREG-0654, “Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants” [13]. The PPC is a standalone, non-safety related data system that performs no control function. The PPC at the Reference Plant has been recently updated with newer technology. It collects digital data from the field by directly connecting to sensing circuits also used by the current I&C systems in the plant. It makes this plant data available in the Reference Plant MCR, the Technical Support Center (TSC) and the EOF. To achieve these ends, the PPC connects to the existing, partial Reference Plant DI at Network Level 3 as shown in Figure 7. The location of the connection of the PPC to the DI can vary somewhat from plant to plant depending on its classification and use with regard to cybersecurity levels defined in each plant’s cybersecurity plan and how that plan relates to the levels in RG 5.71 [7]. PPC plant information is also forwarded to IT systems to make it available to the local Reference Plant IT network (Network Level 4).

Additional Reference Plant sensor data collection has been added to gain additional visibility into the operation of selected plant systems and components. This information is collected by sensors and digital systems directly connected to local Reference Plant IT systems. This function is encompassed within the “wireless sensor network” depicted at Network Level 4 at the top-left of Figure 7 since this is, in most cases, the most economical way to add devices to collect such data. This information can be used by itself or aggregated with other data from the PPC to enable diagnostic and prognostic analyses. Data collected directly in this manner as well as the results of any software program that analyzes this data cannot be directly used by operators to affect plant control.

The Reference Plant is a “standalone” nuclear entity within the Owner’s portfolio of nuclear plants with remote support provided by Vistra from the Vistra Power Optimization Center (POC) located Dallas, Texas. The POC provides advanced monitoring and diagnostics services to its own generation and production facilities as well as to others as a commercial enterprise. Industry-seasoned engineers and experienced process control operators identify incipient and long-term equipment issues around the clock, providing actionable intelligence directly to those responsible for real-time operations. The success of the POC is driven by the competitive market advantage its clients achieve through realizing maximum asset performance. The POC capability is encompassed in the “fleet maintenance & diagnostic center” shown at the top-left of the fully integrated fleet DI provided in Figure 7.

3.1.2 Future State: Application of Digital I&C Technology

3.1.2.1 DCS Overview

The Reference Plant plans to use a commercially available non-safety related DCS and a commercially available safety-related digital platform for the I&C upgrades. A simplified architecture diagram of this aggregate solution is depicted in Figure 8. This is an adaptation of the DI diagram provided in Appendix A of the DI Migration Framework document [2].

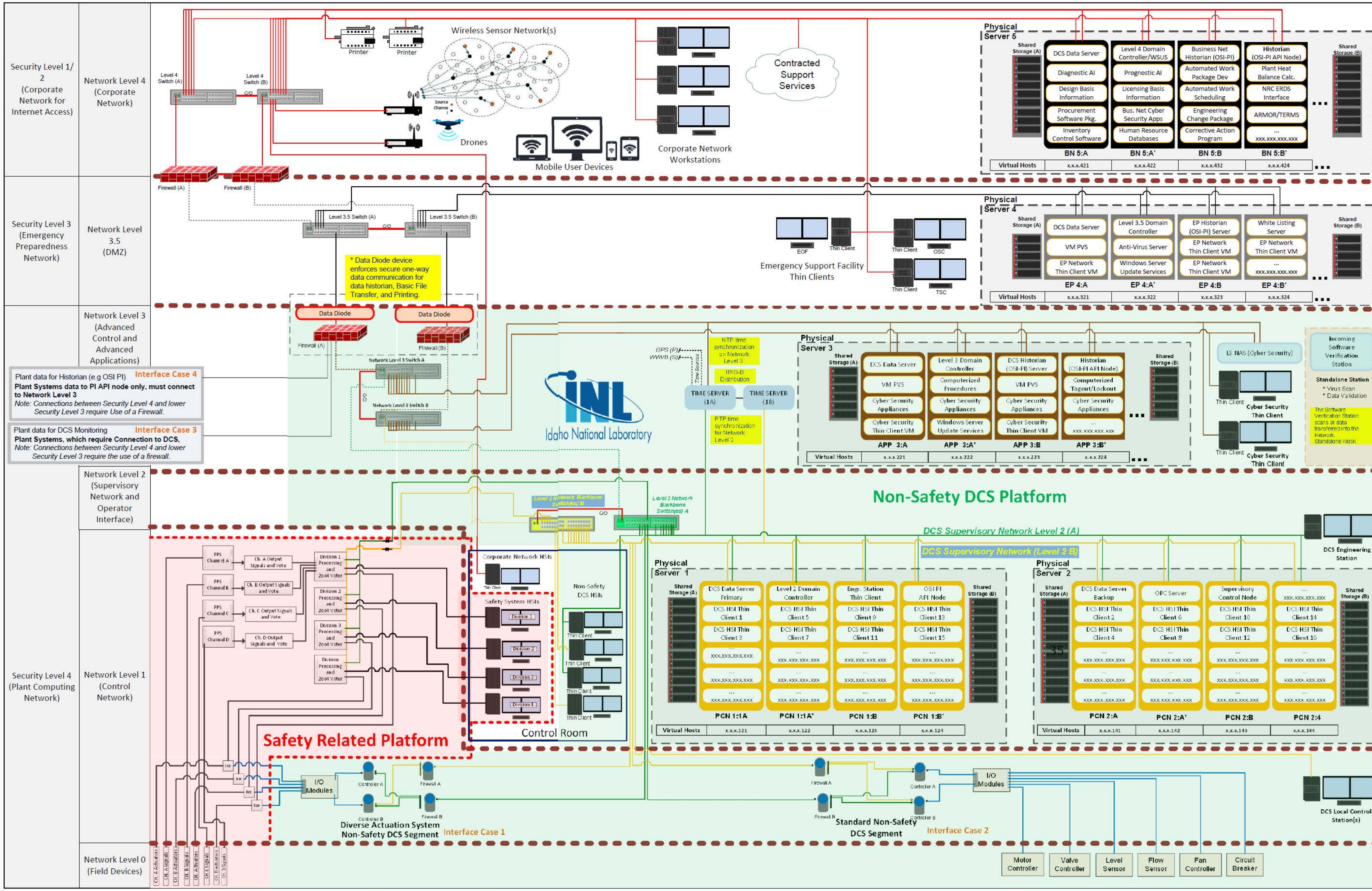


Figure 8. Generalized digital I&C architecture highlighted within the DI framework.

Figure 8 genericizes the design features of several commercially available non-safety related DCS systems (e.g., the Honeywell Experion Process Knowledge System [PKS], the Emerson Ovation Platform). It also generalizes design features associated with safety-related digital I&C systems and presents a simplified four-channel, four-division digital safety platform interfaced to the non-safety related DCS through optical isolators to prevent any faults in the non-safety related DCS from promulgating to the safety platform. Bulk digital data transfer from the safety-related platform to the non-safety related DCS (and beyond) is accomplished through data diodes.

The non-safety related I&C DCS platform highlighted in green at the bottom right of Figure 8 is proposed to host a phased migration of the functions provided by existing non-safety related I&C equipment, including:

- Nuclear Steam Supply System Process Control
  - Steam Generator Level and Feedwater Control
  - Pressurizer Pressure and Level Control
  - Steam Dump Control
  - Reactor Temperature and Rod Speed Control, Rod Insertion Limit
  - Chemical Volume Control
  - Low Pressure Letdown Control
  - Boron Recovery
- Balance of Plant Controls
  - Auxiliary Steam
  - Circulating Water
  - Component Cooling Water
  - Compressed Air
  - Condensate
  - Demineralized and Reactor Makeup Water
  - Feedwater Heater Control
    - Extraction Steam
    - Heater Drains
    - Necessary Sensors and Replacement Digitally Controlled Valve Positioners
  - Main Steam Reheat and Steam Dump
  - Plant Gas Supply
  - Potable and Sanitary Water
  - SG Blowdown Cleanup
  - SG Feedwater
  - Spent Fuel Pool Cooing and Cleanup
  - Station Service Water
  - Turbine Oil
  - Turbine Plant Cooling Water
  - Miscellaneous Ventilation Area Functions
  - Annunciator System
- Anticipated Transient Without Scram Mitigation System Actuation Circuity using Non-Safety Related DCS.

Digital systems expected to be interfaced to the DCS include:

- Upgraded safety-related digital platform (highlighted in red in Figure 8). It is expected that all process data (e.g., sensor inputs, operator inputs, and processed outputs such as alarms, calculated results outputs, and operator inputs) will be transmitted to the non-safety related DCS.
- PPC interface. The current PPC is intended to be phased out over time as signals from current plant I&C systems are migrated to the non-safety related DCS directly or provided from the safety-related digital platform being installed at the Reference Plant to the non-safety related DCS. Until that occurs, it is expected that the PPC will be interfaced to the non-safety related DCS as shown by Interface Case 3 on the left side of Figure 8.
- Other assorted systems as listed below:
    - Interface to recently upgraded, separate Turbine Control System provided by others
    - Interface to recently upgraded, separate Feed Pump Control System provided by others
    - Rod Position Indication (updated to a separate digital system)
    - Rod Control Systems
    - Flux Mapping System
    - Containment Atmospheric Monitoring.

These non-safety related subsystem functions are expected to either be directly hosted on the new non-safety related DCS platform as illustrated by Interface Case 2 in green on the bottom right of Figure 8 or performed by standalone subsystems digitally interfaced to the DCS. If direct digital interfaces to the DCS are used, DCS functionality may be limited to only receiving data for indication on the DCS with control functions being accomplished by using subsystem capabilities and associated HSIs. Alternatively, the DCS may be used to provide supervisory monitoring and select supervisory control capabilities to connected subsystems (e.g., turbine supervisory control accomplished through DCS HSIs).

3.1.2.2 Introduction of the Owner's New State Non-Safety Related I&C System Capabilities and DI Integration

3.1.2.2.1 The Reference Plant as a Pilot for the Owner's Nuclear Fleet

The installation of a modern non-safety related digital DCS in the non-safety domain into the Reference Plant in a deliberate and forward-looking manner enables coordination with other DI investments in other domains and the possibility of a more revolutionary future state advanced concept of operations as discussed in Section 1.3.3. As existing plant non-safety related I&C functions are migrated to the non-safety related DCS, not only is the availability of plant data in a digital format increased but the availability of DCS self-diagnostics is introduced. The diversity of non-safety related I&C systems is also reduced over time, reducing the number and diversity of spare parts and reducing associated training on diverse systems.

Leveraging DCS vendor technical support capabilities can provide near real-time diagnostic capabilities to address emergent system issues. Day-to-day configuration support, configuration management, and necessary system patching can be accomplished by systematically leveraging vendor experience across their entire customer base. Addressing lifecycle support challenges, particularly the obsolescence of DCS hardware and software, can be similarly supported by the vendor.

To best enable these capabilities requires:

1. Awareness of vendor capabilities (technologies) in these areas.
2. Knowledge of how to architect the DCS to optimize the utilization of these capabilities and to fit it within the larger DI.

3. A change in the concept of operations of the plant in terms of organization (governance) and processes to realize savings that can be enabled by the two capabilities described directly above. While the outcomes to "run the plant" safely and reliably and to "run the business" economically remain the same in the macro, **how it is done** must be conformed to the capabilities technology of the present to have the largest impact.
4. Negotiating lifecycle support services as an integral part of the original detailed design contract for the DCS. It is at this point that the utility has the most leverage/buying power to negotiate with the DCS supplier to obtain the most advantageous terms in this area. It is possible that vendors will provide discounts on hardware, software, and engineering services. The larger potential contract or contracts which are expected to be let by a utility with multiple units increases this buying power.

Section 4 identifies more specific technical capabilities that can be enabled by DCS technology as it is envisioned to be architected within the DI for nuclear plant use. This lays the foundation for Section 5, which presents governance and associated process changes to enable an optimal concept of operations that leverages the proposed DCS for a single station.

3.1.2.2.2 Enabling Synergy Across the Owner's Nuclear Fleet and Non-Nuclear Electrical Generation.

Sections 4 and 5 also discuss expanded leveraging of the pilot upgrade effort beyond the Reference Plant to the rest of the Owner's nuclear fleet and across the Owner's entire generation enterprise. The possibility that the Owner may leverage a single DCS vendor across both its nuclear and non-nuclear assets opens additional opportunities to harmonize how the Owner "runs the fleet" and "runs the business" of the utility supported by the fully integrated fleet DI technology foundation pictured in Figure 7.

3.1.2.3 Strategic Planning with the New State in Mind

Current plans for I&C digital upgrades at the Reference Plant are outlined to occur as a staggered set of four separate installation phases at each of the two units. The entire effort is forecasted to occur over an 8 year period.

4. NEW STATE I&C TECHNOLOGY, ARCHITECTURE, AND LIFECYCLE SUPPORT CAPABILITIES THAT CAN ENABLE COSTS AND WORKLOAD REDUCTIONS

Section 2.4 of the Pilot BCA for DI [3] provides an overview of expected benefits of proposed I&C digital upgrades (both safety-related and non-safety related). These benefits are subdivided into three categories: labor savings (internal and external), material savings, and avoidance of lost generation revenue. The focus of this section is to provide more detailed information as to specific technology features the non-safety related I&C digital platform is expected to provide to enable these benefits.

The following subsections are focused on presenting **how** using capabilities associated with a modern DCS can provide the technical foundation for system lifecycle cost and workload reductions. These capabilities are described in relation to the first three Network Levels as shown in Figure 4, Figure 7, and Figure 8. It is suggested that the reader have a separate copy of Figure 4 and Figure 8 in hand when reading this section to promote understanding. The capabilities described are generalized based upon the capabilities of DCS products produced by different vendors. There may be specific instances where a feature generally described below may only be available from a particular vendors.

Sections 4.1–4.3 provide a condensed summary of a virtualized DCS OT architecture. A basic understanding of this technology is necessary to understand how its capabilities can enable changes to the concept of operations to both "running the plant" and "running the business" of a nuclear plant and utility.

Section 4.4 provides a condensed summary of an intermediary network between the DCS OT systems and a utility's IT systems above it in the DI. This intermediary network supports nuclear plant EP capabilities within the constraints of NRC cybersecurity directives and also presents aggregated OT data from the DCS for integration and analysis by software hosted on IT systems above it in the DI. This section also discusses how EP capabilities can be enhanced to deliver WROs through capabilities made available by the non-safety related DCS.

Section 4.5 briefly presents how a virtualized DCS architecture can enable enterprise-wide IT capabilities for a utility with diverse generation sources as depicted in Figure 7.

4.1 Network Level 1: Local Control

4.1.1 Input and Output Devices

4.1.1.1 Basic Function

DCS I/O devices accept three different types of field input signals:

1. Discrete digital I/O devices (typically fixed voltage): Digital inputs represent direct field device status inputs (pump on/off or valve open/shut) that are simply converted into a logic 1 or a logic 0. This value is assigned an address in the DCS to permit its capture and use. Alarm and warning values for inputs can also be set for digital inputs. Discrete digital outputs are addressable DCS points that place a discrete digital value to a field device to command an actuation.
2. Discrete analog I/O (varying voltage or current): Analog inputs representing variable sensed values in the field are converted directly into calibrated digital values that represent the sensed parameter in engineering units. An initial configuration is performed to establish the proper signal resolution level and initial alignment so that each analog input is converted to a digital value accurately representing the measured parameter in the field (pressure, variable actuator position, etc.). This digital value is also assigned an address in the DCS to permit its capture and use. Alarm and warning values for inputs can also be set for analog inputs. Analog output devices convert an addressable engineering value representing a variable command state to a variable output value that is used to control a device in the field.
3. Direct digital I/O information from smart field devices: When modernizing existing nuclear plants, the bias is to leverage installed sensors and devices described by Types 1 and 2 to reduce costs. When new sensors and actuators are being installed to replace failing ones or to enable new functions, such as improved feedwater heater control as proposed for the Reference Plant digital upgrade, data input to the DCS can be enhanced by leveraging smart devices. There are a plethora of different device networks using different technologies and configurations that can be leveraged. As a whole, device network technologies provide capabilities in diagnostics, configuration, and device level control. Nearly all DCSs have I/O devices capable of leveraging smart field device protocols include HART (which uses a digital carrier on a 4–20 ma analog signal loop) and digital protocols such Foundation Fieldbus, Profibus, DeviceNet, etc.

4.1.1.2 Properties of DCS I/O Modules to Reduce Lifecycle Costs and Workload

Unlike analog I/O, digital I/O circuits by their very nature are not subject to drift over time. As a result, this eliminates workload currently expended on surveillances and calibrations to combat drift.

Typical DCS I/O devices are architected to include multiple modules, including:

- Electronic module(s) that perform signal processing and digital communications
- A passive backplane that provides:
  - Less susceptibility to failure (no active components)

- Connectivity for power for the electronics module(s)
- Termination blocks for wiring coming from sensors and going to controlled field devices that then connect to the module(s). These termination blocks are typically detachable from the backplane to facilitate replacing the backplane if necessary without having to de-terminate and re-terminate individual wires coming from the field.

Dependent on customer needs, DCS vendors can provide nonredundant or redundant I/O modules. This work assumes that redundant configurations are the default for nuclear plant DCS implementations. Representative example I/O Modules are shown in Figure 9 and Figure 10. As shown, both designs are architected to be fully redundant above the individual field device termination strip and passive backplane.

Figure 9. Honeywell universal I/O module redundant configuration.

Figure 10. Emerson Ovation R-Line I/O module redundant configuration.

I/O signal processing at the I/O module level often uses separate electronics modules mounted in the same chassis as the I/O signal processing modules. Digital communications between the I/O modules and Network Level 1 local controllers is accomplished via redundant, dedicated I/O links to redundant local controllers (discussed in Section 4.1.2) for both data acquisition and control functions. These redundant links connect the I/O modules with I/O processors in the local controllers.

I/O module configuration and diagnostics are performed using purpose-built software tools developed for the DCS. Failure and diagnostic information is typically communicated by I/O modules to higher levels of the DCS (the data server at Network Level 2). Fail-state outputs to controlled field devices can also be established. This provides for placing controlled devices at Network Level 0 in a preprogrammed fail state should communication between Network Level 1 I/O modules and the controllers be interrupted.

Should an individual I/O module fail in a redundant configuration as shown in Figure 9 and Figure 10, a replacement can typically be “hot swapped” by simply removing and replacing the failed component without deenergizing the I/O chassis or the redundant I/O module. This replacement can be accomplished with no loss of I/O function to the system. 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.

There is typically no capability for the insertion of a separate data analysis and analytics software features 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-warranted performance characteristics.

4.1.1.3 Other Considerations

When selecting I/O modules to be used for specific implementations, there are several other attributes that need to be considered, which include but are not limited to:

- **I/O signal ranges.** DCS I/O modules are typically designed to support standard signal ranges of inputs and outputs (e.g., 4–20 mA, 0–5 V, 0–24 V). In some cases, the values for process variables in legacy monitoring and control systems do not fall within this range. For digital outputs, interposing relays may need to be added. When dropping resistors have been used in sensing current loops in legacy circuits, the resistance values selected to stay within the loop current budget may have resulted in non-standard voltage ranges. Changing the resistance value to generate a standard voltage range may not be an option. If it is an option, the labor to make the modification and modify the loop calculation documentation will add to modification labor costs.
- **Sequence of events (SOE) enabled I/O and I/O scan rates.** To track the proper execution of specific control system events to verify system performance and troubleshoot issues, DCS vendors offer SOE I/O modules. These I/O modules capture discrete, time-stamped events at a much higher scan rate (as high as 1 ms) than used for process control (typically 100 ms—also configurable). SOE values are typically stored locally for transmission during the next I/O module scan. Overuse of the SOE capability and setting faster scan rates than necessary for I/O in general consumes network bandwidth and can negatively impact system performance.
- **Room for expansion.** When installing a DCS to be the target for migrating legacy I&C functions from obsolete systems, the DCS I/O design needs to account for the state when all envisioned legacy functions are to be migrated. Ideally, an additional margin for adding new functionality would also be included. The overall physical and power footprint of the new DCS is typically significantly less than the legacy systems they replace, enabling such a build out. Planning ahead in this area can significantly reduce cycle time when adding new I/O.
- **Use of "universal I/O."** Some DCS vendors offer an I/O module intended to provide a maximum degree of flexibility within a set of bounding parameters. For example, the Honeywell CC-PUIO31 universal I/O module can eliminate process I/O and control cabinets from a channel-type hardware dependency (Series C I/O Modules | Honeywell). It also supports SOE capabilities. This eliminates the need for custom hardware alignment with different I/O configurations, allows for last-minute design changes without having to swap I/O module hardware, supports a smaller system footprint, and enables standard cabinet designs, which can significantly reduce engineering costs and improve schedule performance. While these modules can come at a higher initial cost, overall spare parts savings may be realized through the reduction of I/O module diversity. Supported signal ranges for these modules may be more restrictive than that supported by the full range of signal-specific I/O modules (e.g., specific digital I/O and analog I/O modules) that the DCS vendor offers.

4.1.2 Controllers

Network Level 1 local controllers make up the heart of the functionality of a DCS. To properly apply vendor DCS technology for a non-safety related implementation in a nuclear plant at Network Level 1, several interrelated topics must be addressed, which are described in the subsections below.

4.1.2.1 Basic Function

DCSs vendors over the years have developed an ever-expanding set of DCS controller capabilities to allow them to penetrate the process control marketplace. These capabilities are highly configurable to satisfy the particular use envisioned by a customer. Utility DCS platform selection is largely influenced by these platform properties at Network Level 1. The basic properties enabling a DCS controller include:

- Controller operating system properties, controller process separation features, integration with prevalidated application software development tools (e.g., function block programming) to create specific control algorithms for execution, 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, which are set at different time intervals based upon process need, thus optimizing overall use of controller processor resources.

These key properties, when properly applied during a systems engineering process ensure that, given proper inputs, the controller will produce required outputs to affect process control.

4.1.2.2 Properties of DCS Controllers to Reduce Lifecycle Costs and Workload

Beyond just providing the basic control function, DCS vendors include a host of other system attributes and capabilities that are intended to improve reliability, availability, and support:

- Online diagnostics, including (but not limited to)
    - Analog input health monitoring
    - 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 fault and diagnostic information, firmware versions, and configuration information are collected by the DCS data server
- Structured, prevalidated configuration and application programming tools that also detect errors associated with these two activities during system configuration or when performing programming using separate off-process systems for this purpose.

4.1.2.3 Network Level 1 Architecture and Associated Attributes

Application of modern digital technology at Network Level 1 can enhance plant and I&C system performance while enabling alternate operations model and organizational structure. Methods and techniques to achieve this include:

- **Combining vendor technologies with utility DCS requirements to provide a robust DCS architecture.**

  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 they can operate completely independent of each other and independently of the DCS system clock. If isolated from the DCS, they will continue to function following its normal programming or place the isolated segment in a known, preprogrammed condition. This supports maintaining the existing control system segmentation as described in station licensing and design documentation.

- **The ability to support equipment redundancy to mitigate single failures and provide for the graceful degradation of system performance in the event of multiple failures.**

  Typical DCS controllers are also architected to include multiple modules. These typically include:

  - Electronic module(s) that perform signal processing and digital communications
  - A passive backplane that provides:
    - Less susceptibility to failure (no active components)
    - Connectivity to power for the electronics module(s).

  Representative example DCS controllers are shown in Figure 11 and Figure 12.

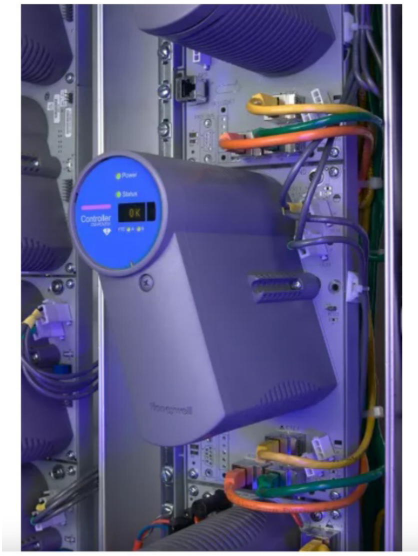


Figure 11. Honeywell C-300 redundant controller.

Figure 12. Emerson Ovation OCR1100 redundant controller.

Again, DCS vendors can provide nonredundant or redundant I/O controllers. This work assumes that redundant configurations are the default for nuclear plant DCS implementations. Both designs are architected to be fully redundant and provide bumpless transfer should an on-service controller fail. Honeywell controller redundancy is provided by provisioning a second controller and backplane assembly (partially shown at the top of Figure 11). The Ovation control backplane provides electrical isolation between the two redundant controllers shown in Figure 12 internally. Both controller configurations support separate power supplies as well as redundant local and remote I/O module connectivity. Redundant communications with the Network Level 2: Supervisory Control (Section 4.2) are also provided. Communications devices that connect Network Level 1 controllers to Network Level 2 devices can also be configured to bound the time to accomplish communication failover and to protect the controllers should there be improper Network Level 2 function. The net result of these capabilities, if fully implemented, is to protect against any single electronics module or communication failure with Network Levels 1 or 2 and to provide protection against a number of (but not all) multiple failures. Such redundancy at the controller level can also support performing software updates or hot swappable controller replacement online without interrupting controlled system operation.

Each controller also provides health and diagnostic information, firmware revision, and other configuration information to Network Level 2.

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 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 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 the specified DCS performance is assured.

- **Establishing a menu of "use cases" for controllers and associated I/O interfacing.**

  Modern DCSs are nearly infinitely configurable. While this is generally beneficial, it can support an unnecessary level of diversity of implementation that can drive costs. Each "new" method of interface configuration must be individually developed, validated, and maintained. Working to limit the diversity through the identification, validation, and implementation of a minimum set of standard I/O use cases (associated with standard controller configurations) supports a "design once, use many" mindset where the next migration leverages the last. This tends to drive implementation and lifecycle costs down.

4.1.2.4 Level 1 Obsolescence Management and Intellectual Property Migration

DCS I/O modules are typically custom designed by each manufacturer as part of vendor-specific OT product lines. Being custom designed, their lifecycle is typically longer than that IT equipment. They are often manufactured over long periods of time (10–20 years) and technical support is typically provided for extended period of time even after manufacturing has transitioned to new product lines. When parts are no longer available, a migration path to newer hardware will be needed. As described in Section 4.1.1, field termination blocks from current I/O module backplanes can be disconnected and reconnected to updated I/O module backplanes, which eliminated the need to re-terminate individual field connections. Vendors typically endeavor to design new equipment to fit within the same envelope as older equipment to minimize infrastructure impacts (stay within existing cabinets with minimum impact to cabinet wiring, cooling, etc.). Backward compatibility to connect newer I/O modules to legacy controllers may also be offered.

Similar obsolescence attributes as described above for I/O modules are also provided for DCS controller modules. These also are typically custom designed by each control system manufacturer as part of a product line. They are designed to function, are produced, and are supported for extended periods of time (typically ~20+ years) to protect against obsolescence. For supported, state-of-the-industry DCS systems, newer controllers are typically backwards compatible with legacy I/O modules to allow for controller upgrades without having to replace the facility I/O infrastructure. For example, the newer Emerson Ovation OCR3000 controller as pictured in Figure 12 is a functional replacement for the OCR1100 controller with improved orientation and vent designs in the base assembly for heat dissipation. The backplane has the same footprint, connectors for powering, I/O bus, and status indicator as the OCR1100 to facilitate easier upgrades. Servicing the upgrade market tends to drive new controllers to maintain backwards I/O compatibility.

Companies that have been in the digital control system market for a significant period of time also tend to support harvesting intellectual property in the form of in-service control code in their legacy controllers. Existing control code in legacy controllers has been factory acceptance tested, site acceptance tested, post-modification tested, and field proven for years. When choosing to implement a digital modernization at facilities running analog I&C systems or unsupported digital I&C systems at end of life, it is of paramount importance to select a vendor and its technology based upon the vendor's demonstration of and commitment to a comprehensive approach to harvest and migrate controller software applications. Leveraging this capability in nuclear is a key enabler to minimizing the cost of controller equipment obsolescence when existing plants are looking to extend their total plant lifetimes to 80–100 years. Controller software does not get old or wear out. The vendor's ability to migrate software applications using prevalidated techniques eliminates the cost of recoding existing applications and can either eliminate or vastly reduce the scope for significant subsequent post migration software regression testing.

Table 2, taken from [1], illustrates this point using representative data from a DCS vendor (Honeywell) from 1974 to 2018. The controller name acronyms presented in Table 2 are not of particular significance. What is significant in Table 2 is the information contained in the "Lifecycle" and "Migration Path" columns.

Table 2. Representative vendor support for controller hardware & software (Honeywell).

Controller Name	Released	Migration Path	Year Path Available	Lifecycle	
CB	1974	C300/EHPM	2014	40	
EC	1976	C300/EHPM	2014	38	
RCD	1976	C300/EHPM	2014	38	
MFC	1977	C300/EHPM	2014	37	
IPC 620	1978	C300	2012	34	
AMC	1987	C300/EHPM	2012	25	
PM	1988	APM	2013	25	
APM	1991	HPM	2013	22	
FSC	1996	Safety Manager	2004	8	
HPM	1996	EHPM	2013	17	
UC	1997	C300/EHPM	2014	17	
C200	1998	C300	2016	18	
HC900	2000	N/A	Current	18+	
Safety Manager	2004	N/A	Current	14+	
C300	2006	N/A	Current	12+	Still Current in 2024
MLPLC	2008	N/A	Current	10+	
C200E	2010	C300	2016	6	
RC500	2011	ControlEdge RTU	2013	7+	
ControlEdge RTU	2013	N/A	Current	5+	
EHPM	2013	N/A	Current	5+	
ControlEdge PLC	2016	N/A	Current	2+	
UOC	2017	N/A	Current	1+	
Safety Manager SC	2018	N/A	Current	1+	

These two columns together show that, for products released up to 50 years ago, the representative vendor has established backwards compatibility to their current control system products and a migration path to harvest the intellectual property in them when replacements for obsolete hardware cannot be obtained. This migration path has been developed and validated at the expense of the DCS vendor. This provides an added benefit of eliminating or minimizing the need for extensive post-modification testing. Non-safety related DCS vendor technologies being considered non-safety related DCS nuclear plant modernizations (Emerson Ovation or other) should demonstrate a similar capability to the same level of detail as shown above as part of the lifecycle support section of proposals made to nuclear utilities. INL makes no recommendation as to the use of any supplier by the industry in this area.

4.2 Network Level 2: Supervisory Control

4.2.1 Functional Overview

Network Level 2 provides two primary functions:

1. To capture and make available all data collected by Network Level 1 and 2 (both plant process data as well as DCS performance data) and make it available to other Network Levels within the DI. These capabilities are further described in Section 4.2.1.1.
2. To allow the operator to view and control Network Level 1 processes through HSI physical devices and software. These capabilities are further described in Section 4.2.1.2.

4.2.1.1 DCS Data Server

The DCS data server collects and distributes data between DCS Network Level 1 controllers (and their associated I/O) and presents it to operators on HSI workstations to enable monitoring and control (by providing operator inputs) from those workstations. The server application is a complex software construct that fully instantiates every data point in the DCS. This includes both process control data as well as DCS configuration and diagnostic information. The data servers are also capable of accepting data from other digital systems and software applications. For example, properly formatted safety-related digital I&C system process control data can be transmitted through the data diode installed between the two systems for this purpose. This safety system data becomes additional data points on the DCS data server. The DCS data server can similarly capture data transmitted to it from other digital networks (within Cybersecurity Level 4). The DCS data server facilitates the flow of this data within the DCS.

Other examples of vendor-provided features supported and enabled by the DCS data server include:

- **DCS system health and diagnostic monitoring**: DCSs continuously monitor control applications and DCS system performance and capacity functions in real time to provide early warnings and notifications of potential issues. Factors such as central processing unit health, controller loading, memory, and network communications can be continuously monitored. This provides users with insights to help minimize the frequency and impact due to degraded control system performance and to identify specific methods to address specific system issues causing such conditions.

- **Remote vendor support:** Remote vendor support is enabled by the DI, which provides a one-way data pathway to communicate DCS data server information from Network Level 2 through higher levels of the DI and ultimately to the vendor, as shown at the top of Figure 4 and Figure 7. A summary of such services is provided in Section 4.5.3.

4.2.1.2 HSI Capabilities

As legacy I&C functionality is transitioned to non-safety related DCSs, Network Level video display unit (VDU) hardware will become the primary means for operators to supervise and control these functions in the plant. HSI workstation VDUs at this level provide the capability for an operator to access and navigate through software-generated display pages created with DCS software graphics packages. The DCS HSI VDUs can also be used to monitor safety-related equipment as long as safety-related I&C systems provide the requisite digital information to the non-safety related DCS for this purpose. To enable this functionality, requisite DCS HSI display pages to present safety-related system information need to developed using the non-safety related software graphics packages.

In order to harmonize the VDU-based HSI's, the safety-related and non-safety related 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 utility MCR digital modernizations will occur as a multiphase effort as I&C upgrades are implemented over several years. These interim state HSIs must be fully functional on their own. They also should be designed in such a way as to be guided by the envisioned new state. Ideally, interim state HSI software graphics will be incrementally modified. As additional I&C functionality migrated to the DCS over time, the objective is that HSI modifications be preplanned and additive to minimize HSI rework and promote a logical progression of operator understanding where additional needed training is minimized. Development and use of a consistent HSI style guide established at the outset of a digital modernization program is key to achieving this objective.

4.2.2 Virtualized Design and Use of Properly Configured IT for OT Use

When DCS designs began to leverage IT technology until the early 2010s, Network Level 2 DCS architectures were more hardware intensive due to computing power and associated physical memory limitations. Hosting of a specific software functionality was primarily accomplished with specific hardware in a more one-to-one relationship. For example the DCS data server function was provided by on a single physical server computer with enough computing power and memory to host the DCS data server software and the operating system that permitted the server software to utilize the hardware. Large computer systems could require an array of these types of physical computer servers (the ubiquitous “server room”). HSI workstations were similarly constrained and were provided as full, standalone computer workstations running operating systems and application software located in the MCR. These separate physical devices were each connected to physical network routers and switches. While fully functional, this required a larger physical footprint, many physical network cable connections, and significant amounts of power to run all the computers and networking equipment. Software updates also had to be performed on individual hardware devices. This particularly impacted MCR operations as technicians were required to perform software updates at the device in the MCR. Systems configured as described above are still supported by DCS vendors to meet customer specific needs.

The industry trend since the early 2010s is to use more modern commercially available IT equipment and software tools to construct Network Level 2. DCS vendors have increasingly turned to virtualizing computing functions and networking capabilities. Virtualization provides a software layer that abstracts operating systems, applications, and much of networking from the I&C DI as described in the paragraph above. While this has many benefits, it presents a potential hazard to system performance. Most IT hardware is procured by DCS vendors from third parties (e.g., IBM, Dell, Cisco) and is highly configurable. Associated utility software (virtualization software, operating systems, etc.) comes in many different versions. The idea that a utility can follow its IT processes (applicable to Network Levels 3.5 and higher) to buy, configure, and maintain DCS IT based equipment and software directly from the manufacturer when deploying a DCS is not realistic. DCS vendors go to great lengths to establish tight configuration control measures on their DCS-leveraged IT equipment, software, and firmware. This is done for hardware down to the make, model, version, and even the specific chipsets used. The same is true for utility software (e.g., operating systems) and vendor-specific DCS configuration and HSI software. They do the same with regard to bounding the specific configuration settings for this equipment and software. Exhaustive testing of these specific, bounded configurations are then performed to establish the bounding capabilities of the DCS. This allows the vendor to warrant system performance capabilities appropriate for a control system so long as a particular system configuration is constrained within the established bounds. Any configuration outside those tested by the DCS vendor, including such seemingly mundane software updates, such as applying Microsoft Windows operating system patches provided by Microsoft to the general public, can void warranted DCS performance (e.g., determinism, fault tolerance capabilities). For this same reason, the addition of non-native software applications or clients not specifically tested by the vendor on a utility’s DCS should be prohibited.

The capacity of modern, high-capability physical computing devices provides the benefit of enabling the hosting of Network Level 2 computing and networking services on a much more compact physical footprint. This capability for the DCS is shown as Physical Server 1 and 2 in Figure 8. These are excerpted from Figure 8 and shown in Figure 13 to aid in understanding.

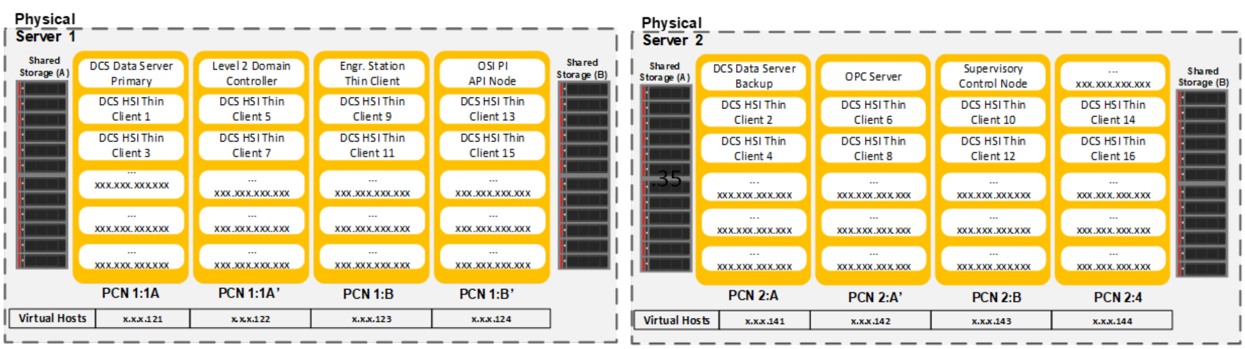


Figure 13. Generic DCS Level 2 physical server diagram (Populated Blade Chassis).

The physical servers as shown in Figure 13 include:

1. **Virtual machines** (VMs). These are shown in white ovals. VMs are software representations of physical computers. These include an operating system and the software applications used to perform the function assigned to it. Each VM can run a different operating system. A fault on one VM (e.g., a Windows operating system crash [blue screen]) will not propagate to other VMs.
2. **Individual computing devices** ("blades"). These are shown in yellow. Each of the four blades shown is a high-performance computing device typically containing multiple processor cores and extensive memory resources. Each blade possesses the processing power of a server room using 1990s–2000s technology. Included with the blade is a software application (a hypervisor) that allocates blade computing resources to each VM hosted on the blade. The hypervisor also provides communication resources between VMs. Each VM on a blade is connected to a virtual network, which allows the VMs on a blade to communicate with each other as if they were on their own physical network.
3. **The physical server chassis** (which physically hosts the blades). This shown in gray. The physical server chassis provides shared storage (solid-state drives and hard drives shown in black) or connectivity to network addressable external storage. The physical server also provides power (redundantly sourced if desired), cooling, physical resource management, and physical networking between the blades and with the rest of the DCS. Manufacturers offer networking between blades in a physical server chassis either internally within a chassis or through separate network switches.

   Blades within a physical server can also be configured as "high availability (HA) pairs." This capability provides redundancy in the event of a single blade failure. VMs hosted on a failed blade configured in an HA pair will automatically transfer to and restart on the other blade in the pair. Restarting VMs on the paired blade can take up to several minutes.

   Allocation of the DCS data server VMs and HSI VMs on blades hosted within the DCS physical server chassis is particularly important to enable both operations and lifecycle support capabilities. To understand the significance of properly architecting this capability needs to be more fully explained. This is provided in Section 4.2.3.

The DCS installations at Duke Energy as presented in [1] demonstrated the degree to which the physical footprint for Network Level 2 can be reduced. All DCS Network Level 2 equipment (physical server chassis, networking equipment [physical switches and routers]) along with other necessary support equipment (e.g., power supplies and cabinet tamper monitoring equipment) are contained in a total of four standard 19 inch equipment racks.

4.2.3 Architecting DCS Data Server and Related HSI Capabilities

4.2.3.1 DCS Data Server Redundancy, Fault Tolerance, and Other Capabilities

While it is technically possible to use a nonredundant DCS data server implementation, the function of the DCS data server is so critical to DCS operation that it is recommended to be configured in a redundant, virtualized configuration in Network Level 2. There are several ways to provide this redundancy. A primary and backup configuration is presented in this document. Again, the detailed configuration of the DCS data server VMs is shown within Physical Server 1 and 2 in Figure 8. These two physical servers are excerpted from Figure 8 and shown more clearly Figure 13 to aid in understanding.

The primary DCS data server VM is shown at the top-left VM in Physical Server 1 in Figure 8 with its backup in the same location of Physical Server 2. To minimize the possibility of a single hardware or software fault affecting DCS data server performance:

- Physical Server 1 and Physical Server 2 are powered from separate sources or two separate auctioneered sources
- The primary DCS data server VM is hosted on one blade of a high-availability pair within Physical Server 1 while its backup VM is similarly hosted in Physical Server 2.

Loss of a blade hosting the primary DCS data server will cause:

- Immediate failover to the backup DCS data server on the blade in Physical Server 2. The backup DCS data server becomes the primary.
- Reboot of the original DCS data server function on the HA blade paired with the one that failed in Physical Server 1. This reboot may take up to approximately 2 minutes. This results in the functionality of the original DCS data server being restored (which now becomes the backup DCS data server).

If the blade hosting the backup DCS data server fails, it will be restored on its paired HA blade as described above. No failover will occur.

As a result of this configuration, the loss of one blade, one HA blade pair hosting one of the redundant DCS data servers, or one entire physical server chassis due to either a hardware or software fault in these devices will not cause the loss of DCS data server VM functionality.

Other physical server and redundancy schemas can also be implemented that achieve similar DCS data server fault tolerance.

4.2.3.2 HSI Redundancy

In a virtualized design, operator HSIs are enabled through the use of HSI thin client workstations. Thin client workstations are nothing more than a small, low-power, low-cost, solid-state computing device that relies on a connection to a DCS physical server that performs computational tasks historically performed by a fully provisioned HSI desktop workstation. The computing tasks for HSIs are now provided by dedicated thin client VMs hosted on blades in the DCS physical servers. The thin client device provides the operator with all the necessary interfaces (a keyboard, pointing device, and one or more VDUs as a typical computer workstation). Each thin client VM has access to the DCS data server VM, which also hosts the HSI software displays files used to affect monitoring and control. In the MCR, any DCS thin client operator workstation can access all DCS display pages to affect monitoring and control. This arrangement allows for reduced power usage to drive DCS HSIs in the MCR and allows for any HSI VM software updates to be performed outside the MCR.

A notional configuration of thin client devices and associated physical server hosted VMs that provide the computing function for them is also presented in Figure 8 and Figure 13 in an enlarged form. Physical Servers 1 and 2 are shown as hosting odd and even numbers of HSI VMs hosted on HA blade pairs. A loss of any single blade in a HA pair will cause a temporary interruption of function (up to approximately 2 minutes) for associated thin client workstations that are driven from that failed blade until the affected VMs restart on the other blade in the pair. The loss of both blades in a high-availability pair will cause a loss of function to those HSI thin clients associated with the failed blades. The loss of an entire physical server will result in a loss of function for those HSIs hosted by that physical server. The consideration of the number and location of HSI thin clients in the MCR needs to account for the failure modes discussed above. Each unaffected thin clint HSI has the capability to affect the full range of monitoring and control functions provided by the non-safety related DCS.

The DCS data server can also be replicated in a read-only format on higher DI levels as depicted in Figure 8. The availability of the replicated DCS data server at higher DI levels is a key technology that promotes concept of operations and governance changes and WROs, which are further discussed in Section 4.4.3.

4.2.4 DCS Network Properties

DCS vendors can provide a nonredundant DCS network configuration if requested by customers. For nuclear non-safety related applications that affect electric power production, a redundant DCS configuration is assumed leveraging the current, typically nonredundant field I/O. Properties associated with the DCS network are generally described in this section. Not all features described are necessarily available on every commercially available DCS network.

DCS networks connect Level 1 devices (controllers) to the Level 2 and connect Level 2 devices with each other. Redundant Network Level 2 connectivity is shown in yellow and green devices and associated network connections in Figure 8. As depicted, vendors provide Network Level 2 configurations that support multiple communication paths. Such configurations enable the network to tolerate all single communication faults and many multiple faults. While IT technologies are typically used, they are specifically configured to support the control mission. This is to provide not only fault tolerance but also the performance, determinism, and security required for industrial control applications. A well-designed Network Level 2 DCS network configuration prevents communication faults and events such as broadcast storms from adversely affecting the performance of monitoring control functions.

For DCS Network Level 2 connections to controllers, vendors provide configurations to ensure only properly formatted, valid network signals are passed through to DCS controllers at Network Level 1. Signals that do not meet these criteria are ignored by the controller. If a primary communication path is lost, controllers will switch over to its redundant connection. If a primary controller loses all connection, it will transfer control to the backup controller. If a controller and its backup both lose all communication with Network Level 2, the controllers can be programmed to continue to provide automatic control, maintain the current static state, or put the controlled process in a predefined safe state. Controllers can also be configured to not communicate with each other to maintain existing functional segmentation incorporated into the design and credited in the plant licensing basis. This prevents having a controller fault from creating the possibility of a new malfunction or a malfunction with a different result not analyzed in the plant safety analysis.

4.2.5 DCS Cybersecurity Design

When initiating projects to install a non-safety related DCS in nuclear plants as described in [1] starting in 2012, most of documents that established the regulatory and industry framework to address cybersecurity were new or being developed. These included:

- The cybersecurity rule 10 CFR 73.54 [6]
- The initial revision of RG 5.71 [7] provided by the NRC in 2010 to aid industry in meeting the rule [6]
- The NRC-endorsed version of Nuclear Energy Institute (NEI) 08-09, "Cyber Security Plan for Nuclear Reactors" [14]
- The NRC-endorsed version of NEI 13-10, "Cyber Security Control Assessments" [15].

Incorporating general cybersecurity protections into the design of commercially available DCSs was also relatively new at that time. To address these facts without requiring expensive and unique design changes to the latest version of the commercially available DCS platform selected for implementation in 2012 was a challenge. This challenge was tackled through coordination between the implementing utility and their DI&C platform vendor. The selected DCS platform possessed certain attributes that could be leveraged to address NEI 08-09 [14] controls. It was lacking in others. NEI 08-09 administrative and technical controls were provided to the DCS vendor as a design input to fill identified cyber attribute gaps and meet regulatory expectations. Utility personnel then worked hand in hand with the DCS vendor to leverage DCS attributes and to configure additional cybersecurity tools to disposition the NEI 08-09 controls. These additional cybersecurity tools were deployed within the defined DCS vendor-validated design and configuration envelope, ensuring that deterministic DCS performance characteristics were maintained. To achieve this result, non-native cybersecurity applications that require significant amounts of memory and computing capability to collect and analyze broadcasted raw log data from Network Level 1 and 2 DCS devices and to passively collect and analyze network monitoring information are provided on Network Level 3.This is further described in Section 4.3.1.5. Through these efforts, utility personnel also became subject matter experts (SMEs) on installing, configuring, and maintaining the Network Level 1, 2, and 3 cybersecurity defensive architecture.

Standard cybersecurity assessments were also produced for the standard DCS as described above, in accordance with fleet engineering developed procedures. The entire DCS was decomposed into only five "types" of critical digital assets that share a substantially similar security posture. Each type was then assessed as permitted by NEI 13-10 [15]. This extended the concept of "design once, build many" into the realm of cybersecurity to minimize initial development and lifecycle support costs for the DCS selected platform.

Current state-of-the-industry non-safety related DCS I&C platforms have significantly increased their capabilities in cybersecurity as driven by the marketplace without compromising performance. DCS communication networks have been encrypted. DCS cybersecurity-related system update processes (e.g., operating software and cybersecurity patch management) have been institutionalized through highly controlled processes, including rigorous predeployment testing, to prevent events such as the 2024 CrowdStrike incident where a flawed software update on IT systems inflicted billions of dollars of economic damage worldwide.

4.2.6 Level 2 Obsolescence Management

Digital I&C DCS systems, which leverage commercially available IT equipment, software, and communications technology, continue to expand their footprint in the process control marketplace based upon the capabilities they provide. Using IT equipment and software in this manner, however, exposes DCS vendors and their customers to the obsolescence lifecycle issues associated with it.

IT equipment manufacturers and software companies are continuingly updating their products in tandem to offer more capabilities and features (faster communication speeds, faster data processing, improved data storage techniques, etc.) demanded by the marketplace. As this occurs, two processes occur in parallel:

1. New DI foundational software tools (operating systems such as Windows Server 2016 and Windows 10, VM host software, etc.) are developed to leverage the capabilities of the latest digital hardware to provide maximum performance.
2. Support for existing DI foundational software tools running on DCS Network Level 2 (e.g., the operating system, VM host software) wains as IT users continuously migrate to the latest generation of hardware and enabling DI foundational software tools. Eventually, legacy DI foundational software tools are no longer supported by suppliers that provide them (e.g., Microsoft for operating systems and VMware for VM hosts). Key (and required) support activities to maintain these legacy software tools (e.g., software patches, cybersecurity updates) are no longer provided by the software vendor.

New DI foundational software tools developed for new hardware are in many cases incompatible with legacy hardware. To attempt to use the latest DCS software on a previous major hardware release (if compatible with legacy equipment) would require significant testing by the DCS vendor to ensure compatibility. The investment required to perform this level of backwards compatibility at Network Level 2 on 8–10-year-old obsolete hardware is typically not economically justifiable from the DCS vendor perspective.

To combat IT system and software obsolescence, DCS vendors coordinate Network Level 2 hardware upgrades to coincide with major platform software upgrades to maximize the lifespan of their integrated product set. Customers can reduce the frequency of their DCS Network Level 2 upgrades (and extend the time between upgrades) by synchronizing their upgrade schedule with the DCS vendor's major hardware and software product releases.

For the collaborating research vendor (Honeywell) examined in [1], the coordinated hardware and software upgrades for their Experion PKS DCS are identified in blue at the far right of Table 3. The key items to note are the Microsoft Operating System versions, the associated Honeywell DCS version release dates, and the associated Microsoft Operating System end of support dates.

Table 3. Representative vendor Network Level 2 platform hardware and software release history.

	Microsoft Operating System		Honeywell Software				
Release	Version	End of Extended Support	Support Level	Released	Withdrawn From Sale	Latest Point Release	
Experion R30x	WS2003 Server SP2	Jul 14, 2015	Phased Out	1Q2006	3Q2010	R301.3 Dec 2008	Coordinated Hardware/Software Major Release
	XP SP3	Apr 08, 2014					
	SQL2000 SP4	Sep 04, 2013					
Experion R31x	WS2003 Server SP2	Jul 14, 2015	Phased Out	2Q2008	2Q2012	R311.3 Aug 2009	Software Feature Upgrade Minor Release
	XP SP3	Apr 08, 2014					
	SQL2005 SP3	Apr 12, 2016					
Experion R40x	WS2008 Server 32bit SP2	Jan 14, 2020	Phased Out	3Q2010	2Q2014	R400.8 Dec 2015	Coordinated Hardware/Software Major Release
	Windows 7 32bit SP1	Jan 14, 2020					
	SQL2008 SP3	Jan 08, 2019					
Experion R41x	WS2008 Server R2 64bit SP1	Jan 14, 2020	Phased Out	2Q2012	3Q2018	R410.9 April 2016	Software Feature Upgrade Minor Releases
	Windows 7 64bit SP1	Jan 14, 2020					
	SQL2008 R2 SP2 32bit	Jan 08, 2019					
Experion R43x	WS2008 Server R2 64bit SP1	Jan 14, 2020	Supported	2Q2014	NA	R430.6 Oct 2016 R431.5 Mar 2018 R432.2 Sep 2017	
	Windows 7 64bit SP1	Jan 14, 2020					
	SQL2012 SP2 32bit	Jul 12, 2022					
Experion R50x	WS2016 Server 64bit	Jan 11, 2027	Supported	1Q2017	NA	R500.2 Aug 2017 R501.4 Dec 2018	Coordinated Hardware/Software Major Release
	Windows 10 IoT Ent LTSB 2016	Oct 13, 2026					
	SQL2014 SP2 64bit	Jul 09, 2024					
Experion R51x	WS2016 Server 64bit	Jan 11, 2027	Current	3Q2018	NA	R510.1 Jul 2018	Software Feature Upgrade Minor Release
	Windows 10 IoT Ent LTSB 2016	Oct 13, 2026					
	SQL Server 2017 Standard	Oct 12, 2027					

Since the issuance of [1], there have been two more feature upgrade minor releases of the Experion PKS Platform:

- Experion PKS R520 launched on August 31, 2021
- Experion PKS R530 launched on February 5, 2024.

The representative vendor also offers prevalidated migration strategies to harvest Network Level 2 intellectual property (e.g., the DCS data server VM configuration including HSI displays, thin client VM configuration) from the utility's installed configuration. Such tools (developed and validated by the vendor at their cost) translate this intellectual property into a form compatible with their latest Network Level 2 DI hardware, operating system software, and VM host software. This is critical to minimizing the effort and cost when performing such a migration. Vendor-validated migrations minimize the need for separate utility validation testing.

As can be seen in Table 3, a repeatable cadence has been established of initial coordinated hardware and software major releases followed by one or more minor software feature releases. Extrapolating this cadence along with the two latest minor feature releases, it would be expected that the next coordinated hardware or software release for the representative vendor is coming, based upon the fact that the current product Windows Server operating system will reach end of support from Microsoft on January 11, 2027. Windows Server 2025 is expected to become generally available in the fall of 2024. This will provide for sufficient runtime in the public domain (essentially “beta testing”) of Windows Server 2025 to identify and address any significant issues prior to it being incorporated and fully tested and validated by the representative vendor prior to the release of their related updated products.

Such forward-looking information can be critical in vendor and platform selection and lifecycle planning. To illustrate this concept, consider the following scenario. The Owner is planning a multiphase installation of their new DCS at the Reference Plant over a period of several years. The first phase implementation may be installed in 2026. If the Owner were to choose the representative vendor’s current product (R530 from above), they would be using a base DI Network Level 2 platform released in 2017, which will no longer be updated by Microsoft after January 11, 2027. The Owner would likely be installing 9-year-old technology in 2026 while new equipment (presumably R600) would be available for purchase. But, informed by the lifecycle support information above, the Owner would be best served, from a long-term lifecycle strategy point of view, by targeting the installation of R600 in 2026 but developing all the Reference Plant intellectual property using R530 tools. This arrangement provides a “best of both worlds” solution. Because the representative vendor does not release newer versions (e.g., R600) without a validated migration strategy from legacy systems (e.g., R530) to the newest release, DCS Data Server and HSI development could begin as soon as practicable with the result being validated and then migrated using the vendor-validated migration process and installed in the plant on R600 hardware and DI software and firmware). Subsequent phases would be developed by directly using R600 tools and configurations. This would permit the full scope of the multiphase non-safety related DCS upgrade to occur while R6XX is the current vendor product and enable maximum use of R6XX before it may need a “tech refresh” when Windows 2025 is replaced by the next operating system 8–10 years from now.

Other DCS vendors such as Emerson Ovation also offer lifecycle planning services. General information on their offerings is publicly available on the internet. It is critical that, prior to selecting any non-safety related DCS vendor (or a third-party supplier that provides and configures DCS vendor equipment and software), the vendor provide a full roadmap of their historical technology migration strategy for their platform for evaluation to be evaluated by the Owner. This historical background is needed to demonstrate they understand and have a mature process to address DCS Network Level 2 hardware and software obsolescence management. The vendor or supplier should describe their plans in detail going forward based on their currently offered products. Their migration strategies for harvesting and migrating DCS Network Level 2 utility intellectual property (e.g., conversion of the DCS data server VM configuration, thin client VM configuration) from legacy to next generation versions of their systems also must be fully understood. Any restrictions to leveraging the original equipment vendor capabilities by potential third-party suppliers needs to be fully understood and challenged if project needs require. INL makes no recommendation as to the use of any supplier by the industry in this area.

4.2.7 Network Level 1 and 2 Architecture Recommendations

The non-safety related DCS hardware and software properties described in Sections 4.1 and 4.2 support a highly diverse set of configurations. When deploying such a system as a target platform to support digital I&C modernization of legacy I&C functions at a nuclear plant, the DCS platform should be configured to achieve several key objectives, including:

1. Provide the highest levels of reliability and availability. The non-safety related DCS should be able to support power production unimpeded by any single fault above an I/O module passive backplane, as described in Section 4.1.1.2, and multiple faults of other individual modules. No loss of a single source of power to the DCS should disable the ability of operators to view and control plant processes.
2. Enable ease of repair with no or minimum impact on operations when failures occur.
3. Promote digital obsolescence lifecycle management with a minimum aggregate impact to plant operations and utility resources (dollars and people).

4. Minimize licensing risk by design. This is significantly enabled by designing and deploying the non-safety related DCS in a manner that maintains the as-built plant control segmentation either explicitly described in licensing documentation or implicitly established through the updated final safety analysis report for a particular nuclear unit. By maintaining the existing segmentation of non-safety related I&C control when migrating legacy control functions to the non-safety related DCS, such upgrades can be performed without prior approval from the NRC as allowed under 10 CFR 50.59, "Changes, Tests, and Experiments." [16]. The precedent for this is captured in the Watts Bar Unit 2 DCS Segmentation Analysis [17] as accepted by the NRC in the associated safety analysis report [18].
5. Develop and maintain the DCS using standard hardware and software building blocks, configurations of those building blocks, processes, and procedures. Needed diversity to support specific I&C functions should be supported as much as practicable through a diverse configuration using these standard tools.

The architecture shown in Figure 8 for DCS Network Levels 1 and 2 and described in this section and Section 4.1 provides for most of the objectives listed above. A brief summary of specific DCS related architecture recommendations and associated process changes to meet all five of the objectives from above are:

A. Each separate Network Level 1 control segment migrated to the DCS as described in Item 4 above provides:
   - Redundant, hot swappable I/O electronics modules above the backplane that interfaces to field I/O devices.
   - Redundant, hot swappable controllers with:
     - Redundant communication down to the each of the redundant I/O electronics modules described above
     - Redundant communication up to Network Level 2.
   - Redundant power supplies to each Network Level 1 control segment so that the loss of any one power source will not interrupt operation for any segment.

B. A fully redundant DCS Network Level 2 is provided that:
   - Connects all Network Level 1 segments in such a way that no single failure of any network device (e.g., router or switch) will cause any loss of connectivity to Network Level 1 controllers or Network Level 2 physical servers.
   - Connects Network Level 1 controllers to Network Level 2 in such a way as to not compromise functional segmentation at Network Level 1 as described in Item 4 above.
   - Is made up of redundant physical servers that are:
     - Virtualized to:
       - Optimize Network Level 2 resource utilization.
       - Leverage a high-availability blade pair configuration within a physical server such that any failure of a single blade at most causes a momentary interruption of a predefined set of Network Level 2 services until affected VMs automatically reboot and restore function utilizing the other blade in the pair. This momentary loss of VM functions will not deny operators the ability to view and control processes on the DCS.

        - Host the DCS data server in such a way that the loss of one blade hosting it in a physical server or a loss of function of an entire physical server causes an immediate transfer of the DCS data server to its backup on the redundant physical server with no loss or interruption of DCS data server function.
    - Configured such that a complete loss of function of one Network Level 2 physical server will not result in a complete loss of operator view and control through DCS HSIs or any other necessary Network Level 2 capabilities needed to operate the plant. Certain DCS vendors only host single homed virtualized HSIs. If such a system is utilized, HSI thin client and virtual host pairs need to be allocated to redundant physical servers such that sufficient operable HSIs are available to operators with sufficient capabilities to view and control processes through unaffected thin client HSIs on the DCS.
  - Is provided with redundant power supplies for all routers, switches, and physical servers so that the loss of any one power source will not impact Network Level 2 functionality.

C. A fully redundant DCS architecture as described in Items A and B above provides the capability to support lifecycle "technology refreshes" when deployed versions of the DCS (or portions thereof) reach the end of their useful life as an added benefit. In the nuclear industry, utilities have been reluctant to perform corrective maintenance or technology refresh activities on I&C systems, including a non-safety related DCS, during generation periods between refueling outages. This reluctance is based on concerns that such activities pose risks to generation. Such work is typically deferred to plant outage periods to minimize such perceived risks.

Such deferrals create risks of their own. Deferring the repair of a failed component whose function is being performed by an installed redundant device leaves a plant susceptible to a loss of plant control function (and loss of generation) should that redundant device fail. Deferring system-level DCS upgrades to outage periods can also extend outage durations. As more legacy I&C functions are transitioned to the DCS at a nuclear plant, the more the plant will also rely on the DCS to perform control and monitoring functions during the outage. A DCS failure during an outage or taking a DCS capability out of service to perform a DCS upgrade during the outage may negatively impact controlling path work during an outage. Resource constraints impacting DCS work during an outage period can exacerbate this challenge.

Outside of the nuclear industry, other production facilities with high safety and financial consequences associated with system failures and extended downtime (e.g., petrochemical facilities) perform DCS repairs and technology refresh activities while the facility is online producing its product. This process highly leverages vendor-validated tools to migrate existing DCS intellectual property to the refreshed platform in a way to minimize rework and post-modification testing. Using vendor-supported standard hardware and software building blocks, standard configurations of those building blocks, standard processes, and standard configuration procedures greatly enables this activity. A detailed presentation on how a technology refresh on a fully redundant DCS can be executed for a particular DCS vendor is presented in Section 4.2 of [1]. Other DCS vendors provide similar capabilities.

Doing repairs and lifecycle support modifications to the DCS online reduces the scope of work performed during outages and levels the workload across non-outage periods. Planning and executing such activities online allows for use of more simplified and flexible policies and procedures for controlling online work. The net result of applying these concepts to the nuclear industry enables substantial WRO realization while enhancing sustained operational performance years into the future.

4.3 Network Level 3

4.3.1 Functional Overview

Network Level 3 hosts software applications that provide advanced features (operator aids) accessed by operators that use DCS thin clients at Network Level 2 to view and control the plant. It also provides for the collection, aggregation, and storage of digital I&C data from all such systems within Cybersecurity Level 4 as shown in Figure 4 and Figure 7. Cybersecurity functions for the DCS are also provided here. The collected digital I&C and cybersecurity data is then transmitted through a one-way data diode to Network Level 3.5 and above. The subsections below provide brief summaries of these features based on the more comprehensive presentation of this information in Section 4.4 of [2] to promote understanding in the context of this document. A partial or complete loss of function of Network Level 3 resources cannot negatively impact DCS operation by design.

4.3.1.1 Computerized Procedures

DCS vendors and third-party system integrators can provide software applications that can integrate plant operating procedures with DCS data in an electronic environment. For example, the logic of procedure steps can be dynamically linked to the Network Level 2 DCS data server or the Network Level 3 data historian (again through an application programming interface [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 DCS HSI Network Level 2 displays from which a control action described in the procedure can be taken for DCS-connected final control elements.

4.3.1.2 Advanced Alarm Management and Presentation

The HSI presentation of the alarm status of each DCS I&C system point configured with an alarm is typically provided at Network Level 2 in a native DCS application. The non-safety related DCS will now capture this information for both the safety I&C system and the DCS. This combined 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.

4.3.1.3 Computerized Tagout

Vendor-offered software applications can provide a means to electronically identify and inhibit the operation of plant equipment from the DCS as required by tagout-lockout processes. This is necessary because legacy methods of placing paper tags on MCR control switches does not translate when those controls are migrated to a digital VDU HSI interface.

4.3.1.4 Configuration Backup of DCS Network Level

Network Level 3 provides storage to capture DCS configuration backup files for Network Level 1 and 2. These configuration backup files enable prompt configuration of individual DCS component replacements. Exported backup files to removable media support configuration control and disaster recovery capabilities.

4.3.1.5 Cybersecurity Data Aggregation and Analysis

Multiple software tools can be hosted by Network Level 3 to manage DCS cybersecurity. Functions performed by these tools include managing network access, collecting and automating the analysis of logs from devices to monitor for cybersecurity events, 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 and beyond to automatically notify utility cybersecurity personnel of issues in near real time. Such information can also be provided directly to centralized utility personnel and vendor resources to identify, isolate, and remediate any cybersecurity events on the DCS should any occur. DCS vendors also offer cybersecurity remote monitoring and support as a fee for service to support cyber protection. This can support a reduced need for local and fleet qualified cybersecurity experts for a utility and promote WROs for those that remain.

4.3.1.6 Digital Data Historian

A digital data historian captures and aggregates I&C data from the non-safety related DCS, the safety I&C platform at Network Level 2 and other interfaced systems. Such a historian already leveraged by industry (e.g., OSI/PI®) can provide this functionality along with others. Several DCS vendors offer an API that allows this digital data historian data to be dynamically linked to their DCS data server. This API makes all this data available on the DCS data server for presentation on Network Level 2 DCS VDUs (e.g., DCS process view displays for other interfaced systems and trend displays for all process information collected by the digital data historian). All digital data historian information is expected to be transmitted to the upper Network Levels (4 or higher) of the DI in Figure 7 for analysis (e.g., AI and machine learning [ML] applications for diagnostic, prognostic, and process optimization). This analysis will enhance both "running the plant" by enabling capabilities such as condition-based maintenance and enable "running the business" by enabling streamlined, remote troubleshooting and logistics support (e.g., automatic order and shipment of replacement DCS parts by a vendor when a failure is detected by the DCS and communicated to them).

4.3.2 Network Level 3 Architecture

Network Level 3 provides a location to accommodate non-safety related DCS control system functionality that is not native to the vendor DCS. Attempting to load such applications at Network Level 2 can put the Network Level 2 DCS in a state that has not been analyzed by the DCS vendor and may negatively impact DCS performance (e.g., determinism). Providing such functionality at Network Level 3 is also intended to ensure that any hardware or software fault at Network Level 3 will impact the performance of the direct DCS view and control provided to plant operators through Network Level 2 or 1.

Network Level 3 also provides positive isolation of access to it from high levels of the DI. This is accomplished by installing data diodes at the boundary between Network Level 3 and Network Level 3.5. These diodes allow Network Level 1–3 information to be broadcast to higher levels of the DI while at the same time making it physically impossible to receive information from higher levels of the DI.

Architecting in redundancy at Network Level 3 is recommended because:

- Of the nature of its use by plant operators as part of the DCS to better enable "running the plant"
- It is the conduit by which Network Level 1–3 data can be broadcast to higher levels of the DI, which enables the proposed governance model to "run the business" proposed in Section 5.1 and the associated reorganization of people leveraging new technology in a tiered support model as proposed in Section 5.2 to optimize "running the business."

4.4 Network Level 3.5

4.4.1 Level 3.5 Functional Overview

Network Level 3.5 as shown in Figure 7 is not part of the non-safety related DCS. Yet, the DI design of the Network Level 3.5 and the connectivity it provides to higher DI levels is critical to maximizing the full range of efficiencies to optimize "running the plants" and "running the business" of a utility. This section identifies technical attributes and associated functional capabilities of how DCS data transmitted to and utilized by higher levels of the DI enable the fleet-centric governance model described in Section 5.1.2 and the reorganization of people to align with the fleet-centric governance model described in Section 5.2. Network Level 3.5 falls with the purview of the NRC cybersecurity rule [7] because it supports the EP function described in Section 4.4.3. To provide this function and allow access to Network

Level 1–3 data to higher levels of the DI, a particular architecture-enabled functionality is outlined in Section 4.4.2.

4.4.2 Cybersecurity Demilitarized Zone

Network Level 3.5 acts as a cybersecurity demilitarized zone (DMZ). This is accomplished by establishing a protected and monitored Network Level 3.5 node as part of the Network Level 3.5 configuration. This protected node faces Network Level 4. This 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 providing mass data transfer broadcast through the Network Level 3 data diode from Network Level 1–3.5 data to DA&A applications at Network Level 4 and beyond.

4.4.3 EP Support

To support emergency response operations facilities required by regulations, particularly those that are geographically separated from an NPP site (such as the EOF), Network Level 3.5 as shown must be configured to host a copy of the DCS data server 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 EP thin client VM workstations and the DCS data server copy depicted in Physical Server 4 shown in Figure 8. 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 4 and Figure 8 are logically connected to Network Level 3.5 even though they are physically connected to Network Level 4. The configuration of the emergency support facility thin clients and the communication means established as described above fall within the auspices of [7].

DCS vendors also offer software that enables the capability present HSI displays developed for presentation at Network Level 2 (including navigation) in read-only versions on IT networks so long as those networks are provided with the requisite DCS information. This can greatly aid individuals in an EOF (either local or remote) in providing timely and accurate support to a plant as needed. Some of these same software packages can be used to develop new HSIs using the same tools and techniques used to develop DCS MCR HSIs to specifically support the EOF function.

4.5 Network Levels 4–6 Corporate IT Networks and the Cloud

Network Levels 4–5 provide corporate IT capabilities and interfaces to the internet at Level 6. These systems do not directly fall within the auspices of the cybersecurity rule [6]. These systems are nevertheless critical for a utility to “run the business” at a particular nuclear site (Network Level 4) or at the larger utility enterprise level (Network Level 5). Utilities can enable WROs by coordinating their cybersecurity activities for both their IT and OT networks through the use of standard tools and techniques to the maximum extent practicable. Care must also be exercised with communicating cybersecurity information from Network Levels 1–3.5 to Level 4 and above so as not to provide information that could reveal cybersecurity vulnerabilities to adversaries that may gain access to the utility corporate IT networks.

Through the connectivity of the DI shown in Figure 4 and Figure 7, and explained in the subsections above, it is expected that all following digital data will be passed from Network Levels 0–3, through the data diode at the top of Network Level 3, to the DMZ for presentation to Network Level 4 and above. That data includes:

- Digital I&C data collected by the non-safety related DCS, including digital data provided to the DCS through interfaced systems from Network Levels 0–2
- DCS system configuration, system health, and diagnostic information
- Cybersecurity monitoring data and analysis information performed either mostly or completely at Network Level 3.

It is beyond the scope of this document to discuss the myriad of capabilities that can be enabled by utility IT networks. Items discussed in the following subsections relate to uses for collected digital I&C system information to support WROs.

4.5.1 EP Support

In addition to enabling a utility fleet EOF facility through virtual private network tunneling as described in Section 4.4.3, the same HSIs available for viewing in the EOF can be made available on the Network Level 4 by hosting another read-only copy of the DCS data server in Physical Server 5 as shown in Figure 8. Additionally, transmission of plant data required to be digitally provided to the NRC via the Emergency Response Data System as required by 10 CFR 50, Appendix E, "Emergency Planning and Preparedness for Production and Utilization Facilities" [19] can be accomplished over the internet.

4.5.2 Utility Remote Plant Status Monitoring and Optimization

As more legacy I&C system functions are migrated to the non-safety related DCS and as digital safety systems are deployed that transfer their data up to higher levels of the DI (likely through the non-safety related DCS), the amount of live digital process data associated with connected plant systems will grow substantially. To augment I&C system data, digital plant monitoring devices can also be connected to the Corporate Network. As shown on the left side of Network Level 4 of both Figure 4 and Figure 7, this will likely 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. Having this wealth of data on a system with the computing power to analyze it with AI and ML applications, will enable significant diagnostic and prognostic capabilities to enable WROs and to tune the nuclear plant optimize efficiency. This will also significantly enable the Owner to maximize its use of the Vistra POC as described in Section 3.1.1.2 for the Reference Plant and other nuclear units in its fleet that pursue similar upgrades. Depending upon the Owner's business plan, it could become either a provider of diagnostic and prognostic analyses or leverage third parties to perform these analyses.

Any results intended to influence the operation of the nuclear plant must be properly vetted and assessed by operators and other station personnel as necessary in accordance plant operating procedures and within the constraints of the plant's licensing and design bases. Developing proper policies and procedures to do this can enable significant improvements. As a simple example, as more plant data is collected for analysis by the DCS and wireless sensor information at Network Level 4, it will become possible to perform more sophisticated heat balance calculations. Software could then identify proposed operational adjustments to plant equipment (e.g., recommend valve positions) to enhance thermal efficiency to produce more megawatts. By writing procedures that direct operators to validate that those recommended valve positions are bounded within the envelope of normal plant operations and can be supported by current plant conditions, operators could set the valve positions as proposed by heat balance application even though the calculation results were produced by non-I&C systems on IT networks not under the auspices of the cybersecurity rule [6].

4.5.3 Tier 3 Fleet Engineering Organization and Vendor DCS Remote Support

Several examples of DCS platform remote support capabilities by organization are described in the subsections below. A key enabling capability that maximizes the impact of such support is the standardization of DCS implementations across a fleet within the bounding configuration constraints established by the vendor for DCS configuration. Customized utility design solutions developed by vendors specifically for individual utilities or nuclear units are typically not provided vendor support via the means described below. DCS vendors typically do not provide any support for custom solutions they provide that are configured outside of vendor bounding configuration constraints after they have been factory acceptance tested. Such custom designs are also not typically migratable when upgrading a DCS to leverage newer hardware and software.

4.5.3.1 DCS Status and Troubleshooting

DCS vendors offer customers a wide variety of read-only data capabilities that can be made accessible via the corporate networks and the internet. These can provide up to full view-only capabilities to access DCS status information via a computer or smartphone. These capabilities can allow the Tier 3 utility DCS fleet support engineering team described in Section 5.2.1, as well as vendors, to provide a range of remote DCS support services. Such services include (but are not limited to) proactive alerting of either or both Tier 3 utility and vendor personnel via IT or internet systems when DCS system issues are detected providing actionable insights to promote consistent (or improving) quality of delivered services over time. They can also identify specific failed components to enable leveraging utility and vendor logistic support capabilities to address such failures, etc. This allows utility personnel (assisted by vendor field service staff if found by utilities to be more efficient) to focus and execute higher-value activities, increase key resource availability, and increase productivity. It also enables utilities and DCS vendors to bring the best qualified SMEs to bear on a task, irrespective of where they are physically located.

Again, attention to detail is required when pursuing such remote access to DCS system information. Aspects of vendor support services may not be fully supported without a means of establishing a bidirectional communication between IT systems above Network Level 4 and the DCS Platform at Level 2. Also, DCS information made available even through a one-way communication path out of the DCS could potentially expose information that could negatively impact the security posture of the DCS.

4.5.3.2 Cybersecurity Services

DCS vendors also offer customers increasingly robust capabilities to enable remote cybersecurity monitoring and support. Capabilities vary between DCS vendors. These capabilities can similarly be leveraged by the Tier 3 utility DCS fleet support engineering team as described in Section 5.2.1 as well as DCS vendors. The same concerns with regard to attention to detail as discussed in Section 4.5.3.1 need to be addressed. Having a centralized utility fleet wide cybersecurity support capability can significantly enable cybersecurity WROs.

5. MODIFICATION OF THE GOVERNANCE MODEL AND REORGANIZATION OF RESOURCES TO ACHIEVE MAXIMUM TECHNOLOGY-ENABLED BENEFIT

Section 4 is focused on presenting **how** the capabilities associated with a modern DCS can provide the technical foundation for system lifecycle cost and workload reductions.

To achieve the maximum benefit of deploying non-safety related DCS technology, there must be a commensurate change in the governance, alignment of resources (people and facilities), and procedures used to implement and maintain the DCS. Lessons learned as described in Section 1.5.1 and the need to embrace culture change as described in Section 1.5.2 provide direction as to **what** needs to be done. This section endeavors to propose more specific information with regard to **how** this can be done for consideration and refinement by the nuclear industry.

5.1 Transition from a Site-Centric to a Fleet Governance Model

5.1.1 Current Site-Centric Model and Structural Inertia when Performing Upgrades

For a utility that operates several nuclear stations, such as the Owner, many have a semi-independent management strategy for plant support where each station identifies, prioritizes, and implements sustaining engineering activities to keep unit(s) operating. In many cases, this is an outgrowth of mergers and acquisitions of plants and utilities over time. Each of these sites tends to independently follow standard industry practices and processes to achieve this end, including using plant health processes that leverage the Institute of Nuclear Plant Operations AP-913, “Equipment Reliability Process Description,” [20] and use of the mitigating system performance index concept.

Following these processes, I&C system engineers at a nuclear site are primarily responsible for maintaining current systems. These system engineers are assigned to support existing, specific I&C systems in the plant. They track system performance, identify any deficiencies in a corrective action (CR) system, and identify methods to address those deficiencies. Activities to address those deficiencies as directed by station procedures, and processes that do not require a design change to accomplish are typically addressed by system engineers.

I&C design engineers at that same site are engaged when a design change is identified as needed to address I&C system CR(s). Examples of design changes directed by these design engineers include reverse engineering replacement parts that provide the same form, fit, and function as failed legacy parts, enabling new capabilities through software program changes to existing digital systems, designing new systems that provide like-for-like functionality of existing obsolete systems, or designing new systems that provide enhanced functionality when compared to functions such as eliminating single-point vulnerabilities and automating existing manual functions. When an engineering change (EC) is identified as needed, it is processed, reviewed, and ultimately prioritized for implementation.

The net result of single nuclear site organizations following the processes above has been to improve and sustain the safe, reliable operation of nuclear plants in the United States for years. The trajectory with regards to operational and business risk to continue following this path, however, is not favorable. This is demonstrated by the fact that:

- Most existing I&C systems have been operated well beyond their original design lifetime.
- Costs to maintain existing I&C systems are rising rapidly as shown in INL business case analyses [3] and [11]. The exponential trajectory of these costs increases demonstrates that the lifetime of existing I&C systems is finite. Existing I&C systems will not support planned plant life extensions being proposed through initial or subsequent license renewal applications.
- Further investment in antiquated and fragmented I&C systems also provides no opportunities for leveraging the capabilities of new technologies to improve or maintain plant safety and reliability while minimizing total cost of plant ownership.
- Individuals who are qualified and motivated to maintain existing antiquated I&C are exiting the workforce. It is difficult to attract, train, and retain new employees when their job would be to:
    - Become a SME on unfamiliar, outdated technology, which stunts their professional careers compared to those who work on or support “state-of-the-industry” digital systems.
    - Perform mundane and labor-intensive tasks, such as surveillances, calibration, and troubleshooting legacy equipment (mostly analog) that are no longer required when modern digital systems are employed.

These concepts are developed in more detail in Section 3.1.1.1.1 of the Constellation Limerick design phase lessons learned report [8]. Together they represent a “structural inertial” in the industry that drives repair or like-for-like replacement-oriented thinking, following engrained plant health processes, and running the business of nuclear primarily at an autonomous site-specific level.

5.1.2 Fleet-Centric Governance Model Applied to Non-Safety Digital I&C Modernization

This section presents a specific fleet governance model to implement non-safety related digital I&C modernizations as a foundation for the remainder of DI modernization. This governance model enables and relies upon fully integrated DI technology for a nuclear unit as depicted in Figure 4. It is envisioned that the two units at the Reference Plant act as the lead units for the Owner’s modernization efforts for its other stations (Beaver Valley [two units], Perry [one unit], and Davis-Besse [one unit]) following in suit.

Affecting the level of change identified above by commissioning non-safety related DCS platforms for six Owner units will require significant and sustained investments and time. Current plans for the Reference Plant show the initial two-unit non-safety related DCS upgrades occurring over an 8 year period tied to multiple outage periods. Waterfalling completion of similar upgrades at the other Owner nuclear units may extend the implementation period for the entire fleet to a period of 10 years or longer and cost up to several hundred million dollars. This necessarily requires a clear (but not perfect) view of the new state target, a map to get there, and a sustained commitment through senior management ownership (by name or position title) and responsibility while leaving room for flexibility based on emergent needs and lessons learned.

To accomplish this, the governance model:

- Drives fleet non-safety related I&C digital modernization, starting at the Reference Plant, as a single corporate objective instead of a large set of individual, fragmented projects. The exposition of new non-safety related DCS technology in Section 4 within the larger DI outlines in advance what success looks like when driving to a defined new state.
- Assesses and prioritizes non-safety related I&C modernization activities. This is presented in more detail in Section 5.4.2.2.
- Endeavors to find innovative ways to minimize aggregate work and operational downtime. For example, designing a fully redundant DCS allows for the ability to perform significant DCS repairs or upgrades while the plant is operating. Decoupling such activities from outages can improve overall operating performance and spread work historically done during outages (potentially controlling path) to other time periods.
- Establishes and maintains a schedule for each site coordinated with the larger integrated fleet master schedule. Major modifications to the site and fleet schedule meeting utility identified thresholds must be approved by utility senior management. These thresholds are expected to include items such as:
    - Moving an approved and scheduled project out of a slotted outage
    - Impacting approved projects across multiple sites (e.g., delay of a major upgrade at one site that impacts the ability of another site to complete an approved upgrade per the integrated master schedule)
    - Significantly alters (>$10 million) the budget of the current year work.
- Standardizes a minimum set of foundational investments and processes and enforces common implementation to maximize efficiency. This implementation also must be designed to minimize regulatory risk and overall cost.
- Establishes a culture and associated lifecycle apparatus for digital systems so that technology investments are planned, designed, installed, maintained, and refreshed in a continuous and deliberate manner.

This governance model is not intended to establish another bureaucracy on top of the current organizational model. It transforms that model by consolidating and developing in-house utility digital systems expertise and focusing their efforts for maximum corporate benefit. This is best enabled by:

- Realigning corporate resources to maximize their collective impact to meet corporate objectives
- Adopting an organizational structure that owns and champions the transformation.

5.2 Reorganization of People to Align with Governance

The following subsections propose a tiered technical organization (supported with physical facilities) to enable the governance model described in Section 5.1.

5.2.1 Tier 3: Fleet Design, Technical Support, and Lifecycle Management Engineering Team

This team represents the core team who possesses the highest level of technical acumen to establish, support, and maintain the standardization of methods and techniques used to design, implement, support, and maintain the backbone non-safety related DCS and safety-related I&C platform selected by the Owner to be deployed at the Reference Plant and other units in their larger fleet. It is expected that this team would be centrally located in a corporate facility to provide support to all fleet units. To promote quality of life and retention, the expectation is that this team would work in a professional office environment (e.g., a corporate headquarters in a city rather than at a remote nuclear unit site).

Responsibilities of this team are:

- Design authority for coordinated digital I&C upgrades across the fleet. This includes the non-safety related DCS and other deployments of standard I&C systems. Some of the points listed below are DCS specific.
  - The standard implementation, support, and technology refresh strategy for standard digital I&C upgrades
  - The standard human factors engineering (HFE) program plan for digital I&C upgrades
  - The standard HSI style guide for digital I&C upgrades
  - Defining and directing the application of use cases leveraged to enable the migration of legacy I&C system functions to the DCS
    - At Network Level 1
      - Directly controlled by DCS equipment (controllers and I/O modules)
      - Supervisory control of third-party devices through DCS controllers (e.g., interface to a third-party turbine control and protection system).
    - At Network Level 2 and 3 (e.g., interfacing third-party systems to enable DCS supervisory functions).
- Developing integrated scopes and schedules and budgets for senior management approval for implementing DCS I&C upgrades across the fleet as well as the identification and coordination of "major" legacy I&C functions migrations to the DCS. In this context, "major" migrations would include large groupings of individual legacy I&C function migrations and migration of significant capabilities (e.g., elimination of the plant process computers across the fleet, turbine control migrations).
- Developing standard design content for the activities above for capture in site-specific implementation EC packages created by Tier 1 personnel.
- Providing oversight to Tier 2 personnel as identified in Section 5.2.2 and individual site (Tier 1) personnel as identified in Section 5.2.3.
- Coordinator for and conduit to access vendor-provided DCS support services.
- Owner of standard methods for:

    - Achieving and maintaining a standard cybersecurity defensive strategy across DCS deployments fleetwide, including (but not limited to):
        - Standard cybersecurity defensive architecture design
        - Standard cybersecurity assessment methods and documentation (e.g., identifying a standard minimum number of critical digital asset "types" and methods to ensure they are cyber secure)
        - Standard cybersecurity auditing processes
    - Providing monitoring with a DCS data server and connection to DCS historian software to support fleet integration
    - Maintaining configuration control
    - Providing for disaster recovery.
- SME level of knowledge on the selected DCS and safety-related digital platforms. This is best obtained through implementing a development process where Tier 3 utility personnel collaboratively develop the DCS and safety platform initial standard configurations with the selected vendors.
- Sized to support an implementation of the coordinated fleet schedule for digital upgrades.
- Made up of existing resources across the fleet (grow and maintain internal qualified resources vs. outsourcing and contractors).
- Responsibility to develop and maintain an optimized I&C modernization process
    - Shared vision across the portfolio (one target vs. multiple separate targets)
    - Standard procedure interpretation and use by the team
    - Standard design and associated documentation reusable between sites for common projects
    - Standardize designs
        - Maximize standard platform implementations (as much as practicable and supported by BCAs) to minimize design diversity (and related costs).
- Solve complex non-safety related DCS platform issues where Tier 2 (Section 5.2.2) and Tier 1 (Section 5.2.3) need assistance. Engage vendors when necessary.
- Evaluate significant functional and cybersecurity patches, updates, and design modifications released by I&C platform vendors that impact core platform functionality.
- Engage platform vendors in identifying, evaluating, and selecting prudent major lifecycle events for implementation.
- Production platform support for troubleshooting and small modifications.
- Interface with IT departments (Site and Corporate) to maximize availability of I&C platform information, including (but not limited to):
    - Direct transmission of DCS data server information to higher levels of the DI. This allows for other uses of DCS information and HSI displays to support "run the plant" activities such as EP and "run the business" activities such as DCS vendor remote support services.
    - Transfer to and long-term storage of time-stamped plant historian information (e.g., process monitoring and control information synchronized to a sitewide time source). This enables the synchronization of this data with other process data gathered and time stamped from other sources (e.g., data from wireless sensors installed in the plant for non-control purposes such as pump vibration monitoring). This information can be analyzed in detail by advanced algorithms such as AI and ML tools at higher, non-control levels of the DI. Results from these analyses can enable cost savings through improved diagnostics supporting equipment condition-based maintenance and reduction in surveillance frequencies. Analyses of plant parameters can also support operational recommendations to improve plant performance thermal performance to produce more power and reduce wear on critical plant components.

This team would be expected to be SMEs with a thorough understanding of all aspects of the DCS design. The initial group of qualified SMEs would gain experience and knowledge through involvement in the project from its inception, through the selection process of the DCS and vendor, and through iterative design refinement in collaboration with the DCS vendor (ideally following an Agile development process similar to that described in Section 3.1.3 of [1]). A more general primer on the Agile process along with associated tenets can be found online at https://www.agilealliance.org/agile101/. The use of the Agile process for a Duke Energy non-safety related DCS upgrade along with lessons learned are captured in Sections 3.1.3 and 3.1.7.1 of [1]. Challenges encountered when working to implement Agile development process thinking for the Limerick safety-related digital upgrade effort are captured in Section 3.1.1.2.1 of [9].

The initial Tier 1 team at Duke Energy, which developed and deployed a standard configuration non-safety related DCS at four nuclear units at three sites as described in [1], was made up of five individuals.

5.2.2 Tier 2: DCS Fleet Laboratory and Operational and Upgrade Support Team

5.2.2.1 DCS Fleet Laboratory

The fleet DCS laboratory hosts an "off-process" version of the standard DCS platform used to develop a standard configuration for and provide lifecycle support to the unit-specific DCS configurations. Ideally, a utility would identify preliminary DCS functional requirements early in the project lifecycle that identify specific platform capabilities (**what the platform must do**) that are needed while at same time **not specifying exactly how the envisioned DCS platform does it**. Early evaluation not only of a vendor's technical capability but also its track record and future planning for lifecycle management should be considered. The intent of this effort is to identify the "best fit" vendor that can provide solutions not only to solve current I&C obsolescence issues but also to support necessary lifecycle DCS updates to efficiently enable long-term operations through digital obsolescence management.

Once a vendor and platform are selected in this manner, a full DCS fleet laboratory system can be purchased. The cost to procure the hardware and software for such a fleet laboratory is minimal when compared to the total cost of implementing standard DCSs across several units. Equipment purchased at this early in the project is leveraged for the remainder of the design effort and for future lifecycle support. It doesn't "go to waste."

The initial purpose for a fleet DCS laboratory system is to understand and adapt the selected vendor's platform properties and configuration procedures to be able to conform them to meet identified plant needs. This understanding is necessary because platform properties and configuration instructions are a result of product development by the vendor independent of the particular implementation envisioned by a customer for its use. It is necessary to tailor the enveloping vendor solution to meet bounding plant requirements.

Procurement of the equipment and operating system software should include all Network Level 3 and Network Level 2 servers shown in Figure 8. Associated network equipment (switches and routers) would also be provided along with representative HSI thin clients. Configuration capabilities (e.g., a virtualization configuration network) as well as installed cybersecurity capabilities and features also need to be provided. It should also include connected use cases of Network Level 1 at a minimum. These use cases are intended to bound and standardize Network Level 1 interfaces to physical plant processes for monitoring and control either directly or through interfaces to third-party digital equipment that affect supervisory monitoring and control of those systems. It should also host other standard plant I&C digital equipment (e.g., portions of the safety-related I&C platform as needs require and budgets allow). Since this system is ultimately used to develop software that will be deployed in an operating nuclear plant, the DCS fleet laboratory must be assembled and configuration controlled within a secure development and operating environment (SDOE).

Early procurement and configuration of the DCS fleet laboratory system provides a key enabling capability for utilities. Tier 3 and Tier 2 personnel working with the vendor can now have the capability to exercise the Agile development process, including multiple "sprints." These sprints address the entire breadth of the DCS architecture as well as integrated DCS configuration and operation all at once.

Lessons learned through each sprint are fed back into the appropriate design and associated deign documentation. This results in much higher quality and better understood design specifications. This activity also directly enables detailed and specific technical knowledge transfer from the vendor to the utility while at the same time developing the design.

The DCS fleet laboratory, configured to represent the final fleet standard design, can be used for factory acceptance testing (FAT) and for lifecycle support efforts going forward. The DCS fleet laboratory can host multiple, site-specific instances of each the DCS configuration. Migrations of deployed DCS platforms in nuclear units to address obsolescence would first be performed and validated on the DCS fleet laboratory system.

5.2.2.2 Operational and Upgrade Support Team

Supporting the DCS fleet laboratory system in an office environment identified for Tier 3 personnel may be challenging for a utility. The laboratory facility to support the systems identified above must provide sufficient power and other features (raised flooring, cooling, fire suppression, etc.) as appropriate. It also must possess the necessary attributes to function as a SDOE for the digital I&C systems it is to support. This section is written assuming it is not practical to colocate Tier 3 personnel in the same geographic location as the DCS fleet laboratory. As a result, the Tier 2 operational and upgrade support team would be necessary. Responsibilities of this team include:

- Owning and maintaining configuration control of the digital laboratory I&C equipment within the SDOE facility.
- Developing standard procedures for and perform testing of all vendor-provided DCS software patches and updates to keep the DCS current. This exercises the procedures to install this software and validates that DCS system performance is not negatively impacted. Once testing is complete, procedures and associated patches are provided to Tier 1 personnel as described in Section 5.2.3 to implement.
- Developing standard procedures for and testing of all cybersecurity patches and updates provided by vendors leveraged to support this service in a similar fashion to that described for the DCS directly above.
- Providing troubleshooting activities associated with difficult and multisite non-safety related DCS problems in collaboration with Tier 3 and Tier 1 personnel.
- Evaluating, screening, prioritizing, and roll out fleet DCS implementation and modification instructions.
- Developing and evaluating plans, policies, and procedures and testing for major lifecycle events (e.g., a DCS system hardware and software refresh as part of the larger DI).

Qualifications of Tier 2 team members are necessarily the same as those for Tier 1 team members. Duke used a standalone Tier 2 team because the digital laboratory facility was in a different location than the Tier 1 team. Individuals in the Tier 2 team were brought in later in the process (closer to the first unit DCS configuration FAT). The initial Tier 2 team at Duke Energy for the effort described in [1] was made up of two individuals.

Responsibilities of this team would ideally be combined with Tier 3 in as described in Section 5.2.1 to promote maximum efficiency in the use of qualified personnel. Combining Tier 3 and Tier 2 responsibilities is enabled by colocating his combined team with the DCS fleet laboratory.

5.2.3 Tier 1: Site Digital Instrumentation & Control Systems Team

This group consists of a limited number of site staff personnel (craft and site design engineering). Site digital process system team would be qualified and responsible to perform:

- Routine activities such as:
  - Own and maintain configuration control of site digital I&C systems.

- Direct and oversee the processes to perform hot-swap replacements of failed DCS components as the design allows. Ideally, site procedures would be modified so the DCS vendor could perform such actions directly under the supervision of site personnel.
    - Direct minor, design-bounded adjustments to configuration items (e.g., control system setpoints) following approved processes.
    - Apply DCS platform and related cybersecurity patches as directed by Tier 2.

  The level of qualifications of personnel performing routine support activities is expected to be significantly lower than the DCS SMEs in Tier 3 or Tier 2. Based on the fact that the DCS is fully redundant, the expected day-to-day level of effort to support this function would be expected to be minimal. Activities performed by Tier 1 individuals would be highly structured using policies and procedures. During normal plant operation, it would be expected that one person would be available on site during the day shift to perform routine activities and be on call during other shifts to provide as needed support.
- Bounded engineering efforts such as:
    - Developing EC packages to design and implement small-scale, site-specific application function migrations to the DCS following fleet standard procedures and with Tier 1 support.
    - Directing the DCS vendor to perform site-specific application software changes through the EC process.
    - Supporting the development of EC packages to implement Tier 1 and Tier 2 led efforts as necessary based upon the scope of those efforts.

The level of qualifications to oversee and direct bounded engineering efforts would require a level of DCS technical knowledge above that possessed by personnel performing only routine activities. The expectation would be that site engineers performing this work would have general knowledge of the overarching DCS design and be qualified to a sufficient level of knowledge to direct, manage, and perform activities to implement specific instances of predefined “use cases” to migrate legacy non-safety related I&C functions following approved procedures that have been developed by Tier 1 personnel. These individual would also be trained to access DCS HSI capabilities used to identify specific failures in the DCS to aid in troubleshooting.

Since configuration control is retained at the site level, individuals who fill the Tier 1 engineering role need to have enough general knowledge of the DCS to own the EC packages that implement either a Tier 3 directed or Tier 1 directed EC package. Again, Tier 3 support of Tier 1 is expected in either case.

The size of the Tier 1 team is dependent upon the number of bounded design engineering activities identified for performance at the site level. At a minimum, two personnel at the site need to be qualified for this role with additional personnel added based upon the number of bounded site DCS engineering activities being pursued.

5.3 Coordination of Control System Design and HFE Efforts Using a Glasstop Simulator

Section 1.3.4 introduced the development and use of a modernized MCR T&Q simulator facility in the context of using digital technologies to enable the larger ION new state concept of operations. Connecting this T&Q MCR simulator to the utility DI can enable improved EP drill performance quality. By employing the DI connectivity proposed in this document, EP drills can fully integrate and leverage near-real-time data and digital display HSIs created for the non-safety related DCSs, not only from the plants but also from the MCR T&Q simulators across the fleet. Such connectivity also enables the consolidation of the function of multiple, site-specific EOFs into one centralized facility to reduce facility costs and enable WROs. The EOF supporting multiple sites can be qualified and used to support concurrent emergencies at multiple sites.

The MCR T&Q simulator facility is designed to address the relevant version of American National Standards Institute and American Nuclear Society (ANSI/ANS) 3.5, “Nuclear Power Plant Simulators for Use in Operator Training and Examination,” [21] as committed to by a utility for a particular unit or site. It provides a high degree of fidelity when compared to the actual plant MCR both in its HSIs and in its ability to faithfully represent real-time plant performance to establish and maintain operator qualifications. This facility is in near-constant use by site personnel for this purpose.

When implementing the two-platform I&C digital modernization described in Section 3.1.2 as a holistic approach, a method must be established to develop and validate both HSI modifications and associated procedure modifications to be implemented through digital I&C upgrades. This is necessary to ensure operators maintain their ability to operate the plant in accordance with the plant licensing and design bases. Modifying the ANSI/ANS-3.5 T&Q simulator for this purpose prior to completing I&C upgrades in the plant is problematic as it would by necessity impact the primary use of this facility for training in its as-built condition.

To address this challenge and to enable additional capabilities to facilitate digital modernization, INL has worked with several utilities to demonstrate the value of employing glasstop simulators. Initial HSI studies to support non-safety related digital DCS I&C installations at multiple Duke Energy units and safety-related and non-safety related I&C upgrades at Constellation’s Limerick Generating Station leveraged INL’s human-system simulation laboratory (HSSL) in Idaho Falls as shown in Figure 14.

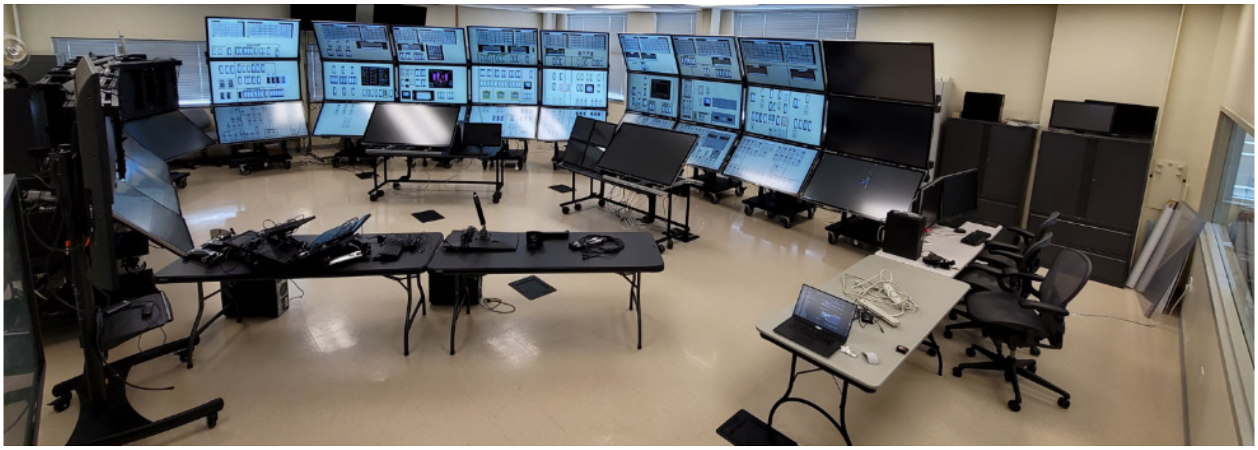


Figure 14. Human-System Simulation Laboratory.

The HSSL, as utilized for both Duke Energy and Constellation, was configured to host the same software loads hosted on their respective ANSI/ANS-3.5 [21] qualified simulators for the plants where digital I&C upgrades are being pursued, which is shown in Figure 6. This software was then dynamically linked to digital renditions of legacy physical indications and controls (provided by the utilities) as well as to new prototypical digital HSI displays developed for the HSI upgrades to provide increasing levels of interactive dynamic performance. For Constellation’s Limerick digital upgrade effort, the HSSL was used to perform a HFE conceptual verification [22] and a preliminary validation (PV) [23] of the HSI and associated procedure modifications.

The successful use of the HSSL for HFE purposes also demonstrated other capabilities that lead both utilities to procure separate glasstop simulators for their respective sites. Several of these glasstops are presented in Figure 15, Figure 16, and Figure 17.

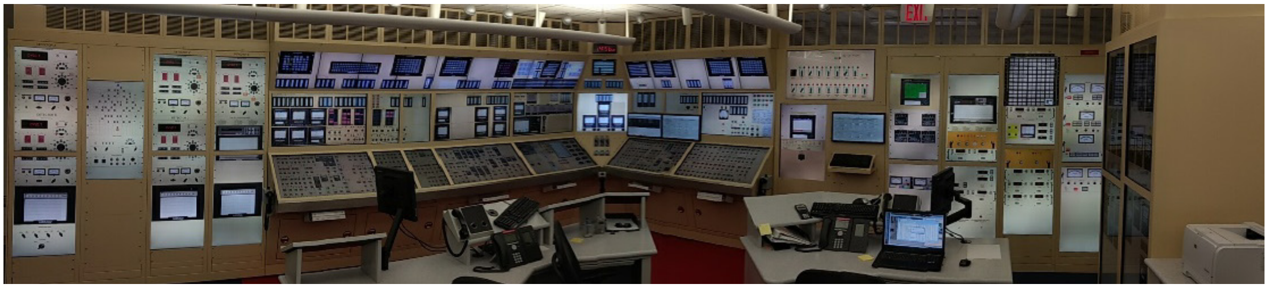


Figure 15. Robinson nuclear plant glasstop simulator control room.

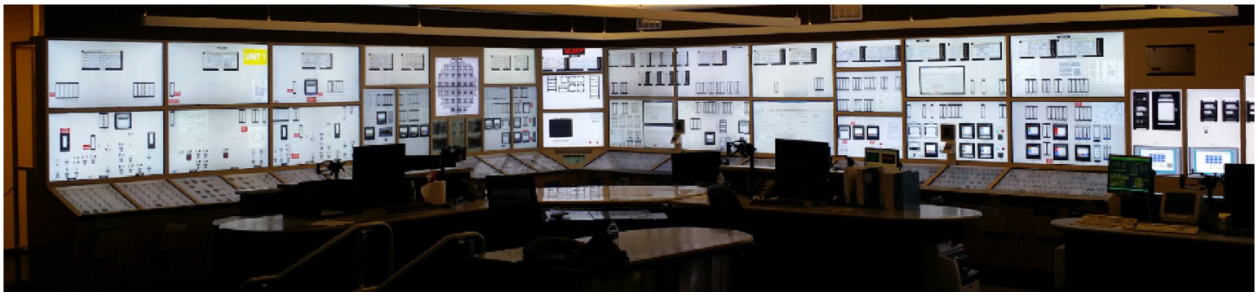


Figure 16. Brunswick nuclear plant glasstop simulator control room.

Figure 17. Limerick nuclear plant glasstop simulator control room (panoramic view).

These facilities, while not qualified to the ANSI/ANS-3.5 standard [21] at this time, can provide a high level of performance that will increasingly converge toward the level of fidelity provided by the MCR T&Q simulator facility. This convergence may allow for ANSI/ANS-3.5 certification for glasstop simulators in the future. For the Limerick safety-related I&C upgrade as captured in the PV report, the HSSL was determined by Constellation to provide sufficient fidelity to support the HFE portion of their license amendment request as submitted to the NRC as captured in [23].

Glasstop simulators can also be logically partitioned to host multiple instances of a simulator software load. When hosting a copy of the software that reflects the actual plant configuration as captured in the MCR T&Q simulator, it can be used for functions such as non-credited operator training, classroom training, procedure development, and EP drill execution. Having these capabilities in an alternate facility enables and augments the ANSI/ANS-3.5 qualified simulator to support its primary mission.

A separate logical partition on a glasstop simulator can also be configured to host a baseline instance of the ANSI/ANS-3.5 simulator software to support I&C modification activities. A glasstop configured in such a manner can support design activities such as (but not limited to):

A. Rapid prototyping of HSIs to assess control room console changes and associated DCS logic implementation early in the design.

B. Assessing indication and alarm functions to be migrated to the DCS in the control room, these console and display changes could be fully developed for the plant function, directly loaded on the glasstops, and evaluated for proper human factors.

C. Enabling assessments of DCS I&C upgrade HSIs and control logic as a risk mitigation. Glasstops have found errors in HSIs and control logic for digital upgrades when both were loaded on them and evaluated. These errors were found after FAT of the associated upgrade HSIs and control logic.

D. Comprehensive HSI development, verifications, and validations, up to and including integrated system validations (ISV) for I&C function migrations performed as part of the overall digital I&C upgrade strategy leveraging NRC NUREG-0711, “Human Factors Engineering Program Review Model” [24] guidance.

By partitioning the function of glasstop in this way, is possible to quickly switch its configuration between these two different use cases. All the attributes of the glasstop simulators discussed above are oriented toward enabling associated WROs as described above.

Costs to build out the glasstop simulators as pictured in Figure 15 (Robinson), Figure 16 (Brunswick), and Figure 17 (Limerick) are driven primarily by either constructing or modifying and provisioning an existing facility to support the plant MCR space envelope, a computer room, and an observation room for simulator instructors and HFE observers. The actual costs to obtain and assemble the replicated internals of the MCR in the glasstop facility are low when compared to the overall project cost. The electronics included in the MCR space can be supported with a fully virtualized architecture. As a result, the electronic equipment in the MCR mockup portion of the facility are largely limited to thin clients that support the VDUs, keyboards, and pointing devices. The physical buildout of the facility needs to provide an arrangement that is as close as practicable to the actual MCR arrangement in the plant using commercially available devices. This can be done in different ways as illustrated by the three figures listed above. For the Robinson glasstop, a variety of commercially available VDUs of different sizes were chosen to more closely replicate the size and relative arrangements of new HSIs and the depiction of legacy HSIs. For Brunswick, the overall MCR arrangement was developed using standard size large screen VDUs and electronically depicting both new digital HSIs and legacy HSIs in a proper relative arrangement using picture-in-picture methods.

The computer host for the virtualized HSIs as well as for the I&C software and the plant models need not physically replicate the hardware that hosts virtualization in the plant. The software is agnostic to the hardware it is run on in the simulator, so long as that hardware enables running it in a manner that provides realistic and repeatable simulator performance to the ANSI/ANS-3.5 standard.

To enable the capabilities described above, it is imperative that the non-safety related I&C vendor be capable of developing and deploying the production non-safety DCS system in parallel with developing and deploying ANSI/ANS-3.5 MCR T&Q facility modifications and the glasstop simulator. The I&C vendor’s capability to do so should be assessed prior to vendor section. It is critical to maintain coordinated configuration control between the upgraded digital I&C systems in the plant and those represented in the simulators to enable the identified WROs. This is best accomplished by directly leveraging vendor tools that allow for direct importation and faithful execution of DCS I&C code developed for the plant into the simulators (both the T&Q and the glasstop). Using tools already developed and validated by the vendor to ensure proper simulator performance can lower deployment costs, and better ensure long-term vendor supportability. Using a validated emulation of I&C code developed for the plant by tools provided by an I&C system third-party integrator is also acceptable.

There are strengths and weaknesses associated with these two different paths. For the first path, the I&C vendor may have challenges implementing specific functions required in the nuclear industry for simulators (e.g., repeatability of performance from established initial conditions and providing “freeze” and "backtrack" capabilities to support training). For the second path, creating an emulation of I&C control code for simulator use may solve many of the issues just listed in the previous sentence. The emulation tool however may be a custom-built construct, which may have long-term lifecycle support issues including tying the utility to a the third-party integrator as a single source for simulator support. Whichever path is chosen by the utility, the DCS I&C vendor or third-party integrator needs to be able to closely coordinate with those organizations that support the existing simulator models (e.g., Western Services Inc. [recently acquired by Curtis-Wright], GSE Solutions) to deploy and provide lifecycle support for the simulators as described above.

5.4 Processes for Maximizing Non-Safety DCS Utilization

This section utilizes four flowcharts to outline key processes to deploy, maintain, and refresh non-safety related DCS investments as a utility fleet program. These flowcharts are informed by and intended to be largely congruent with utility and industry processes to enable the deployment and lifecycle support of non-safety related DCS upgrades. To promote flowchart understanding, the organizations involved and their roles and responsibilities are first described in Section 5.4.1. An overview discussion of each flowchart is then provided in Section 5.4.2.

5.4.1 Organizational Structure and Responsibilities to Enable Fleet Digital Modernization

In the flowcharts presented in Section 5.4.2, color coding delineates organizational responsibilities. Actions along with text describing activities to accomplish each action are color coded based upon the roles of three organizations as shown in Figure 18.

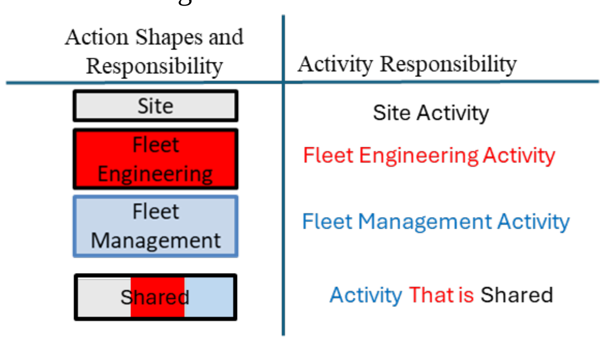


Figure 18. Organizational responsibility key for flowcharts presented in Section 5.4.2.

- **Site:** Site management and site engineering personnel supporting a particular unit or units at that site. Site engineering includes Tier 1 site digital process systems personnel as discussed in Section 5.2.3.
- **Fleet Engineering:** The utility centralized organization that coordinates and standardizes digital I&C modernization efforts across the utility fleet. Fleet engineering maximizes efficiency through standard design, development and use of standard processes and procedures, and standard lifecycle support strategies. Fleet engineering includes the Tier 3 fleet design, technical support, and lifecycle management engineering team personnel as discussed in Section 5.2.1 and the Tier 2 fleet operational and upgrade support team discussed in Section 5.2.2.
- **Fleet Management:** The centralized utility management organization that owns and directs the implementation of a comprehensive digital modernization strategy for their nuclear operating fleet. Key attributes of this strategy include:
    - o Driving fleet digital modernization as a single corporate objective instead of independently pursing a myriad set of fragmented projects across multiple sites

- Standardizing on a minimum set of foundational investments and processes and enforcing a common implementation to maximize efficiency
    - Developing and maintaining a coordinated schedule for initial modernization implementations across units included in the fleet
    - Establishing a lifecycle apparatus for digital systems so that technology investments are planned, executed, maintained, and refreshed in a continuous and deliberate manner.
- **Shared:** Activities that are collaboratively accomplished by two or more organizations.

5.4.2 Process Flowcharts to Enable Fleet Digital Modernization

The process flowcharts presented in the subsections below are intended to be leveraged by the three organizations described in Section 5.4.1 to:

1. Implement the fleet-centric governance model described in Section 5.1.2
2. Leverage the proposed tiered I&C organizational structure as described in Section 5.2 to enable the governance model from (1) directly above
3. Utilize the facilities described in Sections 5.2.2.1 and 5.3, which provide the necessary tools to implement and support (1) and (2) directly above
4. Deploy, maximize the use of, and maintain the digital non-safety related DCS systems to be implemented at the Reference Plant and across other nuclear units across the Owner's fleet.

With an understanding of the information provided to this point in Section 5, the following subsections provide summary discussions of each flowchart provided. This information is intended to be an input to utilities to promote the modification of industry procedures to facilitate adopting these concepts. Incorporating this information into industrywide guidance and processes as described in Section 5.1.1 may also support developing common methods that could be used industrywide.

5.4.2.1 Small-Scale, Site-Specific I&C Function Migration Process

To best illustrate the processes used to implement a comprehensive fleet strategy for utilizing a non-safety related DCS, it best to start with a simple and specific migration of an obsolete I&C function to the DCS and expand the explanation from that point. A process flow chart for identifying, screening, and migrating I&C functions currently operating on obsolete equipment to the non-safety related DCS follows the process depicted in Figure 19. To illustrate this case requires the reader to presuppose that the DCS has already been installed and that the tiered organizational model presented in Section 5.2 has already been implemented.

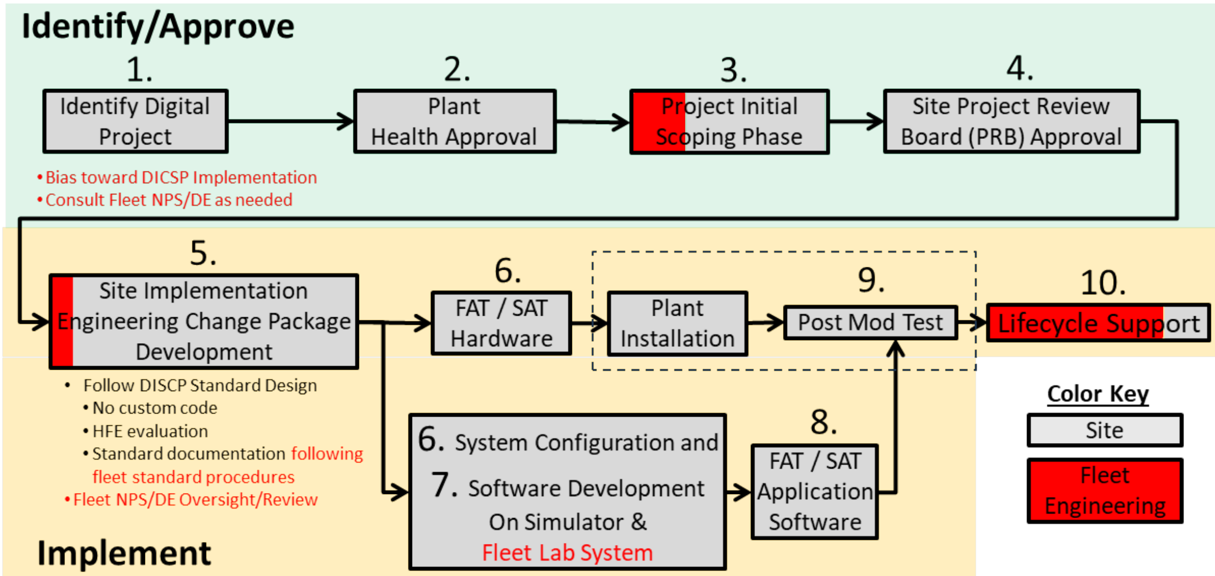


Figure 19. Process for site-specific I&C function migration to a non-safety related DCS.

A brief, simplified description of the effort that occurs for each action shape as numbered in Figure 19 is:

1. **Identify potential digital projects:** When any individual plant system is identified as being challenged at a plant or site due to a component failure, a system failure, obsolescence, or other anomaly impacting operations, it is captured through a CR per the corrective action program (CAP) for that plant.

   CRs that are related to I&C at a site are typically identified by and assigned to Tier 1 personnel described in Section 5.2.3. These individuals propose resolution paths (e.g., replace parts in inventory, a bridging strategy to obtain replacement parts, reverse engineer form, fit, and function replacement parts, or engineer a new solution) to be pursued. If the resolution path identifies replacement of the existing I&C system impacted by the CR, the activity is proposed as an EC. Since the utility has begun to pursue a non-safety related DCS platform as their modernization strategy, it is at this point where such upgrades should be biased toward implementation on the DCS (unless there is an overriding issue, for example cost or immediate threat to operation necessitating immediate repair).

2. **Plant or site health committee approval to commence project development:** The proposed EC is presented to the plant or site health committee and evaluated. If the plant health committed determines it would be advantageous to pursue the EC, efforts are authorized to perform the initial scoping phase of the project.

3. **Perform the digital project initial scoping phase:** The Tier 1 site system engineer collaborates with Tier 3 personnel to develop the initial scope, budget, and schedule for the legacy function migration to the DCS platform leveraging standard rules established by Tier 3 personnel described in Section 5.2.1 to standardize and optimize DCS utilization. Tier 3 personnel verify standardization rules have been followed and works with Tier 1 personnel to make necessary accommodations. A preliminary project prioritization scoring is also developed to assist management in ranking the priority of proposed ECs. At this point, Tier 3 fleet personnel may work to incorporate this single function migration upgrade with others already planned as a set to be developed and installed together to leverage synergies and minimize overall plant impacts to lower aggregate costs.

4. **Site project review board (PRB) approval of EC to proceed with design**: A Tier 1 site system engineer presents the initial scoping document for the EC to the site PRB for review approval and confirmation of project prioritization scoring. At this point, the project to perform the EC is “funded.” Authorization and scheduling to execute the project does not occur until the budget is allocated by site management.

5. **Site implementation and EC package development:** With authorization to proceed, qualified Tier 1 personnel with support from Tier 3 fleet engineering and the DCS vendor perform the design and document the efforts in the EC package. The EC package development process governs the project from conceptual design through final testing and project closeout. The remaining steps are completed as governed by the EC package.

6. **Hardware configuration including FAT and site acceptance test (SAT):** Equipment selection, DI-related hardware configuration, and software tools to implement the migrated function are fully defined. Necessary documentation to complete the upgrade is also fully defined. Hardware configuration to accept project software can occur largely independent of and in parallel with software application development. Basic hardware FAT and SAT can be accomplished without associated application software.

7. **Develop application software:** Since the DCS is being utilized, the expectation is that the DCS native software package will be used to produce monitoring and control applications to load into physical controllers. Additional native DCS native software packages will be used to develop HSI software displays. These HSI displays will be developed and integrated with the rest of the HSI hosted on the DCS and presented to operators on standard DCS VDUs. HSI display development will follow the fleet HSI HFE program plan developed by Tier 3 personnel.

   Depending upon the qualifications of Tier 1 site personnel, the complexity of the specific upgrade, and associated costs, Tier 1 personnel, the vendor, or Tier 3 personnel could develop the necessary software. The DCS fleet laboratory (described in Section 5.2.2.1) and the MCR glasstop simulator (described in Section 5.3) can be leveraged to develop both the project control software and HSI software. This directly supports the Agile development discussed in Sections 5.2.1 and 5.2.2.1 for individual I&C function migrations to the DCS.

8. **FAT and SAT application software:** Both the DCS fleet laboratory and the discussed in Item 7 can support completing the software FAT and SAT prior to integration with associated production DCS hardware to be installed in the plant. Tier 3 guidance and support would be provided here. Two types of testing are necessary. First, the control software to operate in Network Level 1 controllers needs to be tested to ensure proper operation. Procedures to load the software on hardware and verify proper installation can be developed and validated in the DCS fleet laboratory. Methods to set the proper configuration settings for control software applications can also be evaluated.

   Testing can also be performed in the MCR glasstop simulator and the associated physics-based plant model representing plant operation. There may be limits of simulation constraints associated with using the MCR simulator, and final Network Level 1 control system software application tuning will likely be required during post-modification testing (Item 9).

   HSI display software testing follows two tracks. HSI software-based displays need to provide the necessary indications and controls to provide the operators with a sufficient capability to monitor and control the supported plant functionality. This can be tested in the DCS fleet laboratory. Additionally, HFE evaluation is necessary to ensure that the HSIs properly integrate with the totality of the concept of operations of the plant and are congruent with the conventions of the surrounding HSIs in the plant. This is particularly important when there is a significant impact to HSIs in the MCR. The scope and complexity of these HFE evaluations is governed by the scope of impact on the HSIs. Leveraging a glasstop simulator as discussed Section 5.3 to perform HSI evaluations can benefit even simple HSI modifications for small-scale I&C function migrations to the DCS. The HSI effort can be “right sized” based on the project scope while leveraging portions of the standard HFE program plan also discussed in Section 5.3 for the utility fleet.

9. **Plant installation and post-modification testing:** When plant conditions can be established (either during plant operation [preferred] or during a plant outage if required), hardware and software that have both been evaluated through FAT and SAT are brought together and installed in the unit. Post-modification testing is performed to validate proper performance of Network Level 1 control algorithms and Network Level 2 HSI, and the modification is placed in service.

10. **Lifecycle support:** With the modification complete leveraging standard processes and a standard implementation “use case,” lifecycle support for this application migration falls predominantly within the overall DCS platform lifecycle support strategy managed by Tier 3 personnel. Any site-specific efforts such as applying procedurally direct changing of application setpoints within pre-established ranges identified in the implementing EC could be performed by Tier 3 personnel.

It needs to be noted that groups of individual function migrations to the DCS that would likely follow the flowchart for implementation presented in this section are not intended to simply be functional like-for-like replacements. Hosting multiple legacy I&C functions on the DCS provides an opportunity to improve operator interfaces to enhance human performance. There is also an opportunity to provide properly vetted design improvements such better control schemes and automation capabilities. These need to be evaluated as part of the current design and licensing bases. Another basic objective for function migrations is to minimize or eliminate any design changes when deploying the DCS such that a license amendment is required. This minimizes licensing costs and associated schedule risks.

5.4.2.2 Standard Process for Non-Safety DCS Migration and Utilization

With an understanding of the process outlined in Section 5.4.2.1, for a single site-specific migration of an I&C function to the DCS, Figure 20 provides a more generic and expansive standard process for deploying a DCS along with identifying, screening, and migrating multiple I&C functions currently operating on obsolete equipment to the non-safety related DCS.

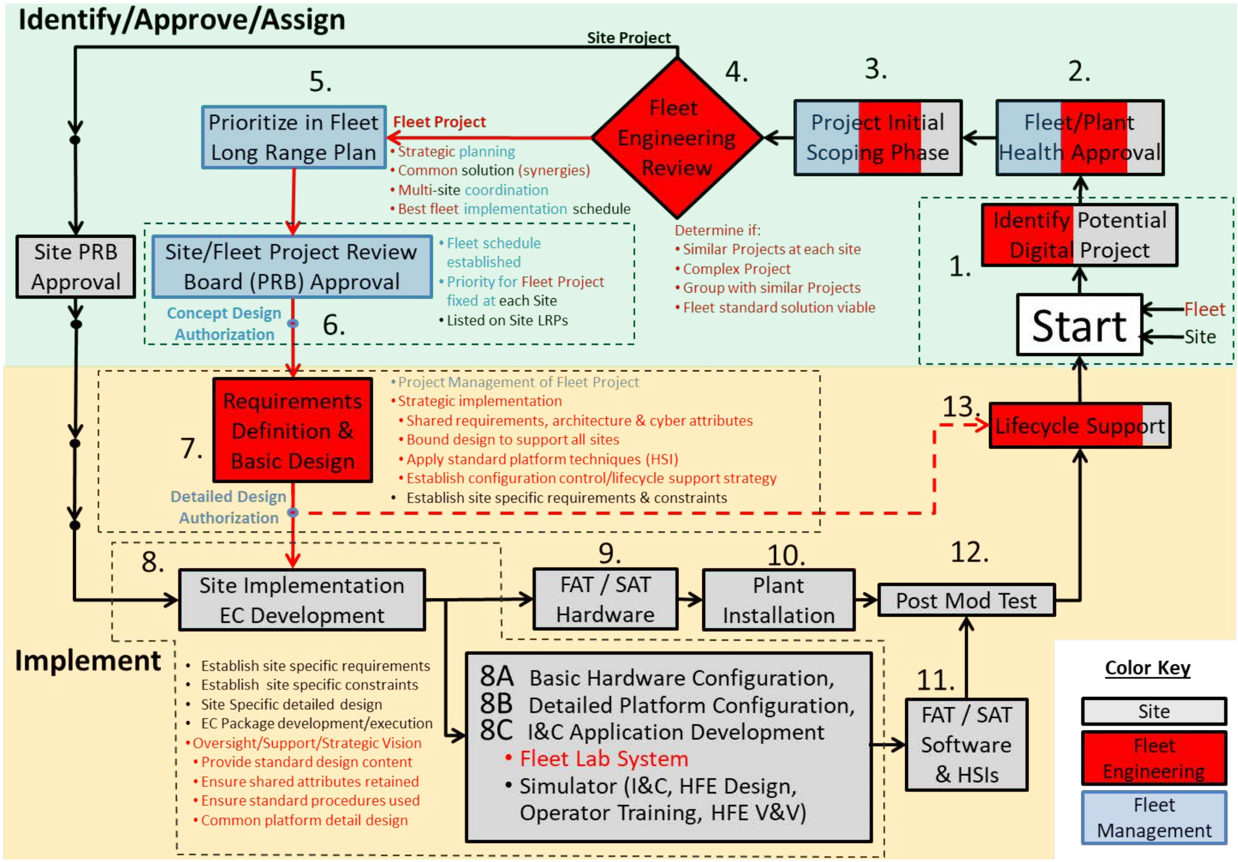


Figure 20. Standard process for installation of and I&C function migration to a non-safety related DCS.

Figure 20 addresses all I&C function migrations to the DCS at individual sites as well as fleetwide DCS implementation and lifecycle support activities. The single, site-specific function migration discussed in Section 5.4.2.1 and shown in Figure 19 is represented as the "outside track" of Figure 20. A site-specific CR initiates the activity at the "start" activity shape in Figure 20.

Large-scale, DCS implementations as well as fleet coordination of the same across multiple units and sites are executed through accomplishing activities represented by the "inside track" of Figure 20. Site-specific steps on the outside track, which are led and approved by the site, are shown as black dots to the left of their "inside track" action shape counterparts.

Figure 20 is intended to be a working tool for those familiar with the process. Key activities associated with select action shapes are provided in Figure 20 for the intended audience. Additional general discussion of the inside track action shapes for fleet activities is provided below to provide additional insights, following the numbering in Figure 20:

1. **Start and identify potential digital projects:**

   For small-scale, site-specific I&C function migration projects, guidance for these activities are covered in Item 1 of Section 5.4.2.1. These items should be considered for grouping with other by Tier 3 fleet engineering personnel.

   Many existing non-safety I&C functions that may be candidates for migration to a non-safety related DCS have likely already been identified through normal processes at a utility. This is demonstrated at the Reference Plant in Sections 3.1.1.1 and 3.1.2.1. In such cases, proposals for consolidating and standardizing I&C modernization efforts for a unit, site, or fleet of utility units to address common I&C challenges can be put forth by the site Tier 1 or the fleet Tier 3 organization charged with coordinating digital I&C modernization efforts. Several individual I&C function migrations identified by this process may be grouped together at an individual site to permit phasing the work over time. For the Reference Plant, the installation of the DCS and migration of existing I&C functions to it as identified in Section 3.1.2.1 is planned to occur in four phases for each of the two units in a staggered schedule over a period of approximately 8 years.

The expansive scope and level of coordination necessary to accomplish a fleet non-safety related DCS implementation necessitates the appointment of a project manager early in the initial scoping phase. Specific lessons learned in this regard in industry have shown that, for large digital projects, early investments in project management coupled with DCS platform requirements definition, basic design, and test planning is critical as captured in INL/EXT-20-59809, "Safety-Related I&C Pilot Upgrade Initial Scoping Phase Implementation Report and Lessons Learned," [25] Section 3.3.1. Appointing a project manager and developing a project plan in the project initiation phase applies additional rigor not typically applied until the conceptual design phase. Early project management engagement enables production of more detailed initiation phase engineering, licensing, and project management deliverables. These enhanced deliverables are intended to address risks as early as possible and to establish implementing utility confidence to authorize proceeding into conceptual design.

2. **Fleet and plant health committee approval to commence project development:** The holistic addressing of non-safety related I&C obsolescence through deploying a DCS at a facility like the Reference Plant and extending it across the Owner's nuclear fleet as a strategic plan is a significant organizational decision. Pursuing such a strategy at one unit or site will take several years and cost many tens of millions of dollars to achieve initial implementation. Expanding this concept across a fleet will likely take over 10 years and cost hundreds of millions of dollars to accomplish implementation. Lifecycle management for the fleet of DCSs that are installed will occur over a period likely to extend 30–40 years into the future or more. For this reason, both the unit and site plant health committee and utility executive management must be made aware of, authorize, and coordinate such activities at a fleet level to obtain maximum efficiency and minimize risk. It is proposed that a fleet organization (a fleet health committee or equivalent) be established to be aware of and authorize the development of proposals to pursue, implement, and maintain such efforts.

3. **Perform the digital project initial scoping phase:** For an enveloping DCS implementation, initial scoping actually begins at Step 1 directly above while identifying potential digital projects. For a single sitewide DCS implementation, this is where the total scope of the effort is more tightly bounded and where initial schedules and resource estimates to implement are established. Surveys to evaluate vendor DCS properties and technical capabilities to support not only initial installation but also the willingness to transfer knowledge to utility Tier 3 and Tier 2 personnel should be determined. Vendor lifecycle support capabilities also need to be established here.

   In this step, outreach to other sites within the fleet should be undertaken to determine the applicability of the planned DCS fleet modernization. For a fleetwide migration of a similar major function or set of functions at multiple sites and units to the DCS (e.g., a common turbine control upgrade or migration of MCR annunciator capability to the DCS) similar coordination as described for DCS implementation should also occur.

4. **Fleet engineering (Tier 3) review:** For small-scale I&C function migrations proposed by a particular site as described in Section 5.4.2.1, fleet engineering evaluates whether that particular upgrade could be grouped within a larger set of I&C function migrations planned at that site to improve efficiencies and minimize schedule impacts. Fleet engineering can also inquire of other sites whether they are having similar issues with the same or similar function at their locations.

Such evaluations may determine that the particular site issue is actually applicable fleetwide and propose a fleetwide solution. Fleet engineering may also determine that the scope of the site-specific function migration is beyond the capability of site Tier 1 personnel without assistance. If none of these considerations are applicable, the particular site-specific function migration follows the outside track as described in Section 5.4.2.1. Otherwise, the proposed effort moves to the next step in the inside track.

5. **Prioritize utility DCS efforts in the Fleet Long-Range Plan:** When considering significant digital upgrades using a standard methodology across a fleet of nuclear units, there are many variables to consider in prioritizing fleet DCS implementation and utilization efforts. Many of these items listed below are actually considered during the initial scoping phase and fleet engineering review to enable prioritization. Significant items include (but are not limited to):

   - Individual unit outage schedules
   - Individual unit safety and reliability status as impacted by the degree of I&C obsolescence, available qualified personnel to service these systems, parts availability, and other "bridging strategies" to deal with operating systems at or beyond their useful life
   - Facility setup and availability (e.g., development of a DCS fleet laboratory) (Section 5.2.2.1) and a glasstop simulator (Section 5.3)
   - Availability of qualified resources (or an ability to qualify sufficient resources at all three utility resource tiers) (Section 5.2)
   - Identifying and selecting vendors (at least two) with:
     - The technical capability, quality control capability, and logistics support apparatus to provide equipment to meet schedules.
     - A robust DCS operational support capability (ideally including live remote technical support leveraging available electronic DCS data transmitted to the vendor by the DCS using the DI as pictured in Figure 7.
     - A robust and demonstrated DCS lifecycle support capability as summarized in Sections 4.1.2.4 and 4.2.6 and willingness to enter into long-term service and support agreements. It is during the vendor selection process that the utility has the most purchaser buying power to negotiate discounts for long-term support in term of reduced labor rates and discounts on hardware and software purchases for lifecycle support.
     - An ability to leverage "out of the box" cybersecurity protections built into their native platforms as much as practical to address the NRC cybersecurity rule [6] while leveraging the NRC cybersecurity guidance provided by RG 5.71 [7]. The objective here is to introduce as few non-native nuclear-specific deviations to the vendor-provided DCS platform as possible. Such specific non-native deviations may present challenges when performing DCS platform technology refreshes.

   Vendors being considered should be able to provide objective quality evidence that they possess these capabilities independent of whether or not they earn the utility's business. Utilities have the most negotiating power to obtain the highest levels of service for the best value in all these areas when initially selecting and contracting a vendor or vendors. DCS vendor selection ideally establishes "covenant" relationship between the utility and the selected DCS vendor that will last for 30–50 years.

   Selecting two vendors to move forward into conceptual design may incur higher costs in the short term but promotes competition and innovation that can enable further cost efficiencies.

Consideration of items such as those listed above is critical to enable the development of a realistic, prioritized, resource loaded, executable schedule for phased implementation of the standard DCS backbone and migrations of groups of legacy I&C functions to the DCS across multiple nuclear units using standard techniques. It is critical to establish and remain faithful to such a schedule across the fleet as much as possible to optimize utility and vendor resource use and to avoid churn introduced by individual site delays causing cascading fleet schedule re-racks.

6. **Site and fleet PRB approvals and conceptual design authorization:** After iterative collaboration between engineering and management at both the fleet and impacted sites, the fleet program scope, schedule, and resource plan for DCS deployment and utilization is presented to the fleet PRB for review. In this context, it is best to describe this effort as an overarching fleet program that coordinates many interrelated projects.

   Within this context:

   - The overall program budget for a phased fleet DCS deployment and associated function migrations will likely reach a cost threshold that requires senior leadership team (e.g., board of directors) approval at the utility. The fleet PRB, after reviewing and accepting the program proposal, will coordinate with the senior leadership team to obtain such authorization. It would be expected that such authorization may be based on the concept of "rolling wave scheduling." DCS platform implementations and identified "first phase" functional migrations at a minimum should be developed to a sufficient cost threshold to meet utility procedural requirements to authorize conceptual design (e.g., an estimated cost with an uncertainty of +X% / -Y%).
   - The time frame to accomplish such a program deployment for a fleet will likely be exceed 10 years). Lifecycle management planning for such a program if properly established should extend to the end of operation for each included site. Such a long-range commitment can only be sustained through the fleet PRB under the direction of the utility senior leadership team.
   - Prioritization of program implementation at each site is best determined by fleet PRB under the direction of the senior leadership team as driven by corporate objectives to maximize "run the business" returns while minimizing "run the plant" risks. The fleet PRB fixes the prioritization of program-related projects in each site's long-range project planning tool.
   - Cost accounting for DCS implementation program work in most utilities must still be accounted against physical assets (e.g., a nuclear station). Therefore, site PRB personnel and site management must be fully engaged and accept the budget for program-related projects and directly contribute to the successful implementation of those projects at their site.

   When the fleet PRB obtains senior leadership team approval for the DCS implementation program, the DCS conceptual design is authorized. Associated "first phase" legacy function migrations to the DCS may also be authorized for specific sites and units. At this time, a project manager for the pilot implementing site should be identified and appointed. Others should be appointed as identified in the fleet DCS implementation schedule.

   After fleet PRB approval, significant changes to program-related projects need to reviewed and approved by the fleet PRB and approved by the senior leadership team if associated thresholds are reached. Such changes include changing the project priority, scope, budget, and schedule beyond specific thresholds.

7. **Requirements definition, basic design, and detailed design authorization:** Early DCS platform requirement definition, establishment of basic design concepts, and early test planning is critical. The object of this effort is to coordinate activities to maximize and maintain standard elements of DCS platform deployments across the fleet and to establish standard processes and procedures to leverage

the standard design for site-specific function migrations. It must be understood at this early stage of the program that, while each DCS implementations will be “standard,” they will never be the same. Standardizing methods and techniques to leverage the DCS within the design envelope of the selected platform as bounded and tested by the vendor minimizes diversity while supporting unique aspects of each individual unit. During this step, Tier 3 fleet design engineering endeavors to:

- Identify the key characteristics of available DCSs in industry and determine which provide the best overall fit to meet the current and future needs of the implementing utility.
- Evaluate specific platform vendor offerings against the key characteristics referenced above and their associated lifecycle support capabilities.
- Establish and capturing requirements for utilitywide, shared attributes such as deterministic performance, redundancy, supply of power, allowed communication paths and failover characteristics, etc. For example, the core DCS Network Level 2 architecture can be assembled and configured in an identical manner for each unit. So long as this configuration envelopes the needs of all units, this provides a “design-once-build-many” approach.
- If multiple vendors have been carried into this point in the project, a detailed evaluation of information provided by the competing vendors should be evaluated against shared DCS attributes. If there is a single vendor that distinguishes itself at this time in terms of capability, cost, and lifecycle support, it can be very advantageous to procure a DCS fleet laboratory system from that vendor at this early stage. Compared to the total cost of the fleet effort, the purchase cost of such a system would be minimal.

  Such a purchase should represent a “best approximation” of the DCS configuration that would meet initial bounding requirements for the fleet as they are understood. During conceptual design, the application of the Agile process could then be used to perform initial configuration and testing iterations of the fleet laboratory (directed toward development the first unit configuration and test program). This can help to rapidly converge on a more refined set of design requirements for the DCS based on first-hand knowledge of its capabilities. This includes all shared aspects of the design including the cybersecurity capabilities. This Agile process also promotes knowledge transfer from the DCS vendor to the utility. These benefits can fully justify the purchase cost of the DCS fleet laboratory, which will then continue to be available for additional project support. If the purchased vendor system does not meet utility needs and expectations, no long-term commitment has been established with that vendor. Other vendors who have remained involved can then similarly be engaged.

Tier 3 fleet engineering personnel also directly develop or work with others to develop a standard HFE program plan for the fleet DCS program. This plan establishes a fleet method for developing, verifying, and validating HSIs to be created to enable plant operators to use the DCS to monitor and control the plant. Existing HFE licensing commitments for each unit need to be understood because they may be different. It is suggested that utilities leverage NUREG-0711, “Human Factors Engineering Program Review Model,” [24] as a basis for development of the standard HFE program plan since the NRC’s review of HFE products will be informed by this reference. The utility should not commit to implementing NUREG-0711 if their current licensing basis does not include it. Such a commitment is not required and can add an additional engineering and administrative burden.

Any site-specific enveloping requirements and constraints that are necessary to implement the standard DCS design at a particular plant need to be identified by Tier 1 personnel at that plant.

Based upon requirements definition and basic design efforts, the DCS fleet program project manager develops updated scope, schedule, and resource estimates.

8. **Site implementation engineering change package development:** Because system configuration control is maintained at the individual unit level, EC packages and all related documentation that support it need to be captured and maintained at the unit level by Tier 1 personnel. Tier 3 fleet design personnel provide EC technical content associated with the design and deployment of the standard design for Network Level 2 and 3 and collaborate with Tier 1 site personnel to ensure it can be properly interfaced to the plant.

   When developing digital systems for nuclear plant implementation following an iterative development process, EC development and DCS system configuration software development are best performed in parallel. How this is accomplished is presented below.

   A and B: For DCS Network Level 2 activities:

   Efforts in these areas focus on continued iterations that develop the standard Network Level 2 platform configuration for fleet implementation. This is best performed led by Tier 3 and Tier 2 personnel using the DCS fleet laboratory system (Section 5.2.2.1), which includes production of:

   - Increasingly detailed configuration instructions that are enveloped by vendor established constraints ensure vendor-validated performance characteristic are maintained. If this is not done, the utility cannot expect that DCS will provide the performance characteristics warranted by the vendor. Novel configurations or first-of-a-kind designs demanded by the utility for implementation on DCS will be custom to the utility and require unique testing and qualification. This will all be performed at the utility's expense. Furthermore, DCS vendors will not provide lifecycle support to maintain this functionality. Such functionality will not likely be migratable to upgraded platforms when current equipment and software become obsolete.

     These configuration instructions also must address the particular requirements imposed by the utility to provide more specific capabilities within the vendor established configuration envelope. An example of such a specific utility capability at Network Level 2 would be to statically configure all Network Level 2 communication ports and communication paths. Such configurations contribute to locking down the Level 2 network. Doing this enables the detection of any modification made to this configuration (e.g., plugging a device into an unused port or unplugging a cable from a used port) as a cybersecurity protection feature.

   - Increasingly detailed configuration verification instructions and Network Level 2 test procedures are also developed in a similar manner. As configuration instructions become more detailed, so do the instructions to verify proper configuration has been performed. As captured in [1], configuration verification represents a very significant portion of the scope of verification and validation (V&V) of the Network Level 2 design. Developing procedures for and performing operational checks of system characteristics to verify vendor-warranted levels of DCS performance (e.g., throughput, determinism, and latency) can also be developed. As documented in Section 3.1.7.1 of [1], however, performing such Network Level 2 operational V&V activities tends to be contrived and of limited value.

   Iterative efforts to develop configuration instructions and associated configuration verification instructions leveraging the DCS fleet laboratory system described in Section 5.2.2.1 and the Agile development process as previously discussed both tend to accelerate Network Level 2 detailed design efforts and enables successful accomplishment of DCS Network FAT and SAT.

   When developing the standard DCS platform configuration, it is necessary to plan for the possibility that there could be a catastrophic failure of the platform that could require a complete system rebuild. To perform such a disaster recovery requires that configuration procedures be differentiated into two types. These include:

- A disaster recovery software backup of all system-level configurations. Once the DCS platform configuration has been developed on the DCS fleet laboratory system and successfully completed configuration verification and system validation tests, a disaster recovery software backup is created. All system software files capable of being backed up and restored to a new system are captured in this backup.
- Basic hardware configuration instructions. These are the procedures to perform basic hardware configurations necessary to permit loading a “bare metal” disaster recovery system out of the box with the software backup as described in previous point. The objective is to create a fully functional replacement DCS platform. The restored configuration is then subjected to the same configuration verification and system validation tests as the original system FAT.

DCS Network Level 2 physical design efforts include internal cabinet design for processing and networking equipment. For the DCS application performed at Duke Energy using a fully redundant virtualized architecture as documented in [1], two 19 inch cabinets were used to host the DCS data servers and two additional 19 inch cabinets were used to host networking equipment. The equipment in these four cabinets provide sufficient Network Level 2 capability to support the migration of all envisioned legacy I&C function migrations for the unit in which the DCS installed. Designs, drawings, and associated instructions to remove legacy I&C equipment and install the new DCS Network Level 2 equipment are also developed. These address redundant power needs, cooling needs, floor loading and fire loading issues, electromagnetic and seismic analyses, etc.

C. DCS Network Level 1 activities:

Efforts in this area are directed toward two parallel and complementary areas:

- Requirements for hardware development focus on the generic development and specific application of Network Level 1 use cases as described throughout this document. For each individual function migration to the DCS, the number and type of specific Network Level 0 I/O field interfaces needs to be defined for each application while leveraging a predefined use case. Any unique I/O features for the particular function migration (if any) will need to be addressed. This information will be used to determine the number and type of I/O modules to be used. Typical use cases will leverage redundant I/O modules and controllers as described in Section 4.1. Designs, drawings, and associated instructions to remove legacy I&C equipment and install the new DCS Network Level 1 equipment need to be developed in a similar fashion to that described for Network Level 2 equipment above.

  When performing multiple legacy I&C function migrations to the DCS, physical segmentation of both I/O and controllers as discussed in Section 4.2.7 must be considered and maintained as necessary to support the objective of performing such migrations under 10 CFR 50.59. This minimizes licensing costs and associated schedule risks.

  Additional Network Level 1 specific hardware development details revolve mostly around Network Level 0 I/O interfacing techniques and the location of Network Level 1 equipment. To minimize wiring to connect the field I/O, it may be desirable to use local I/O modules to connect as close to the field signals as possible and to leverage a digital communication capability to connect these remote I/O modules to controllers located in centralized locations that are either colocated with Network Level 2 hardware or close to it. Alternatively, if Network Level 0 device field wiring is already routed to centralized location(s) such as a cable spreading room, it would likely be advantageous to connect to Network Level 1 I/O modules there. If existing I/O field wiring is connected to legacy analog or digital control equipment using an existing physical connector, it may be advantageous to leverage that physical connector. A new connector designed to mate to the existing connector coming from the field could be installed on one end of a premanufactured interface cable. The other end of the same cable could be prewired to a connector compatible with the I/O module backplanes such as those shown in Figure 9 and Figure 10. The use of such premanufactured I/O physical interfaces provides for significant WROs. Ease of installation and testing are significantly enhanced. The number of required changes to configuration-controlled unit design drawings would also be minimized.

- Requirements for software development focus on configuring I/O modules and developing software applications. These requirements support collecting field data, manipulating it as necessary to present the information to software algorithms and operators, and accepting and translating outputs from either to send necessary control signals to field devices. As with Network Level 2, Network Level 1 software development uses prevalidated tools and configuration techniques provided by the DCS vendor. At Network Level 1, it is also necessary to constrain the use of these tools within the boundaries defined by the DCS vendor for the same reasons given for Network Level 2 above.

  Having accurate information that fully instantiates the characteristics of field I/O interface signals is critical in configuring the I/O modules. Correct I/O module processing requires that field inputs in whatever form are converted to properly calibrated digital values with a resolution commensurate with its use for monitoring and control. Outputs calculated as digital values in the controllers that are sent to the field must also be similarly calibrated so that signals received by Network Level 0 devices produce the correct response. Attention to detail is also required to ensure the proper physical connection of field sensors and actuators. Improperly connecting one signal on a connector can “phase shift” all the remaining connections, resulting in significant rework. The use of universal I/O as described in Section 4.1.1.3 can mitigate this error should it occur, but this still can result in significant rework.

  Software development for control algorithms hosted in Network Level 1 controllers accept properly digitized field and operator inputs and compute outputs to perform either automatic functions or operator initiated manual actions. HSI software application development generates digital images on VDU devices to provide plant operators with the capability to monitor and control the plant. Both of these can be accomplished much more efficiently through the coordinated development of the DCS fleet laboratory system described in Section 5.2.2.1 and through the incorporation of the new Network Level 1 digital design into training simulators, as described in Sections 1.3.4 and 5.3. The use of glasstop simulators in developing properly human-factored HSI display features and capabilities while leveraging NUREG-0711 HFE guidance as described in [24] has demonstrated itself to be critical. Glasstop simulators provide a digital MCR HSI capability to iteratively produce increasingly refined and specific design inputs for the development of DCS HSIs using available DCS software graphics generation tools and associated vendor and utility software development processes. As an example, INL glasstop simulators were used by the Limerick Generating Station to develop and demonstrate the use of HSIs for a fully digital safety-related I&C protection system upgrade. The resultant PV report [23] was submitted by Constellation to the NRC as supporting information for its license amendment request to implement the upgrade. HSI display depictions and associated HFE items identified during both the conceptual verification [22] and PV [23] were provided by Limerick to their safety-related I&C

vendor as input to allow the vendor to develop actual digital I&C system displays using platform graphics design tools. It is expected that a similar HFE process using glasstop simulators would be used for large-scale DCS projects.

It again needs to be noted that groups of individual function migrations to the DCS that would likely follow the flowchart for implementation presented in this section are not intended to simply be functional like-for-like replacements. Hosting multiple legacy I&C functions on the DCS provides an opportunity to improve operator interfaces to enhance human performance. There is also an opportunity to provide properly vetted design improvements such better control schemes and automation capabilities. These need to be evaluated within the context of the current design and licensing bases. Following standard implementation techniques for application software and HSI development again tends to support a "design-once-build-many" strategy. It is also important that HSI design development be forward-looking. As more legacy I&C function migrations to the DCS occur, consideration needs to be given to how best to integrate these into the DCS HSI graphics incrementally over time, as described in Section 4.2.1.2.

For Network Level 3 activities: Efforts in this area are directed toward applying non-native capabilities to support cybersecurity functionality to protect the DCS at Network Levels 2 and 1 and to assist operators in their use of Network Level 2 systems to enhance operator performance, as presented in Section 4.3. For the DCS implementation, the key capability that can most significantly impact DCS performance is addressing DCS platform cybersecurity needs. Cybersecurity design efforts for DCS implementation are described in Sections 4.2.5 and 4.3.1.5. Cybersecurity design, V&V, and commissioning activities performed during EC development and execution follow the same process as the DCS itself, as described above, as it is integrated into the DCS design. The use of the DCS fleet laboratory leveraging an Agile development process directly supports the definition and application of cybersecurity technologies to support this end. It also supports the development and implementation of necessary policies and procedures to manage, maintain, and enhance those cybersecurity technologies to support initial implementation and the DCS lifecycle.

Configuration and use of other third-party applications hosted on Network Level 3 such as computerized procedures, alarm management, and use of a digital data historian can also be supported by the DCS fleet laboratory and glasstop simulator. Such efforts are directed toward configuring interfaces between them and the DCS to enable their particular function. From a DCS platform point of view, the failure of any or all Network Level 3 functions cannot negatively impact DCS Network Level 2–0 functions.

9. **Hardware configuration including FAT and SAT.** For a fleet implementation, orchestration of FAT and SAT activities can occur that can support significant WRO opportunities. A method to perform this orchestration is illustrated below:

   - **DCS FAT and SAT for the Network Level 2 standard DCS platform design.** FAT and SAT testing is best performed first using DCS fleet laboratory described in Section 5.2.2.1. These activities represent the final iteration of the Agile development process for the DCS platform and are outlined below:

     - The DCS fleet laboratory hardware (identical with that to be installed in each utility unit) is first restored to a "bare metal" condition.

     - It is then fully configured and tested using the standard, approved documentation developed as described in Item 8a and 8b above. This standard documentation is developed by Tier 3 and Tier 2 personnel captured in each unit-specific EC package. Tier 1 personnel should be included as as much as possible in this effort to gain both familiarity and to establish site ownership of the DCS platform.

  - After successful completion of testing, a disaster recovery software backup of all system-level configurations is captured using standard procedures and the DCS fleet laboratory is again restored to a "bare metal" condition. Again, this standard documentation is captured in each unit-specific EC package.
  - The DCS fleet laboratory hardware is configured using approved procedures to accept loading the disaster recovery software backup and then the backup is restored to the system.
  - The restored system is again tested following the same testing documents as before. This establishes validity of the disaster recovery process.

- **Unit-specific Network Level 2 standard DCS platform design and FAT.** The DCS fleet laboratory system in an SDOE enables unit-specific DCS Network Level 2 software configurations to be developed. This is because the virtualized nature of the DCS allows for the segmentation of the DCS fleet laboratory system. Segmentation enables the development and hosting of multiple, unit-specific DCS Network Level 2 software configurations. This allows for each production DCS Network Level 2 configuration to be developed in the same secure location by the same individuals, following the same procedures. This promotes standardization, the continuous utilization of lessons learned for each iteration, and WROs.

  FAT for each unit-specific configuration can thus be performed on the DCS fleet laboratory system. This process can allow for truncating the FAT of each site-specific DCS Network Level 2 platform configuration. As the same processes and procedures are used for each standard, site-specific configuration as used for the successfully factory acceptance tested fleet laboratory partition, continued performance of the site-specific performance-based FAT activities to repeatedly test the same configuration are of diminished value. This is a lesson learned captured from the Duke DCS implementation as described in Section 3.1.7 of [1] and represents another WRO.

  With each successful unit-specific FAT, a unit-specific disaster recovery software backup of all system-level configurations is captured using standard procedures and the DCS fleet laboratory.

- **Unit-specific Network Level 2 DCS platform SAT.** With a unit-specific factory acceptance tested disaster recovery software backup and a validated disaster recovery procedure in hand, methods to perform SAT can be optimized. Each standard set of site-specific equipment that makes up DCS Network Level 2 can be separately ordered and shipped directly to the site when the site is ready to receive it to perform the SAT. It can then be assembled and configured following validated fleet standard disaster recovery procedures to accept the loading of the factory acceptance tested disaster recovery backup. Since this disaster recovery process has been completely validated in the DCS fleet laboratory, it is possible to reduce the scope of the SAT significantly, enabling another significant WROs.

10. **Unit-specific DCS Network Level 2 installation.** With completion of SAT, site-specific installation will occur as described in the unit-specific EC package as developed primarily by Tier 1 personnel. The system will be powered down in a controlled manner, disassembled to the degree necessary to relocate and land the equipment in its final location. Power and communications cables will be connected and the system power restored.

11. **FAT and SAT of Network Level 1 application software and HSIs.** Unit-specific I&C software applications as developed as described in Item 8(C) are tested by several means. I&C I/O system configurations are verified by performing end-to-end continuity checks from the field inputs through controllers to the DCS server. I&C software algorithms in controllers are reviewed against system requirements to validate that, for provided inputs, expected, predetermined outputs are obtained.

Controller application performance validation can be assisted (within the limits of simulation) by incorporating those applications either directly or through emulation into the glasstop simulator as described in Sections 1.3.4 and 5.3.

HSI FAT and SAT activities focus on two separate aspects. First, each digital DCS HSI display as provided for in Item 8(C) above has not been coded as part of that step. The vendor uses the inputs as described in that step to enter into the quality-controlled software process appropriate for non-safety systems to produce the HSI displays. Each item that appears on each display needs to be validated for proper mapping to data resident in the DCS server to enable all required aspects of display functionality. HSI FAT and SAT also validate that every procedure executed using DCS HSIs has the information and control capabilities as specified by the procedures to allow operators to perform the procedures to operate the plant. This is typically called task support verification.

Secondly, DCS HSIs need to be evaluated against HFE project guidance. This includes ensuring that the DCS HSI style guide was faithfully used to produce a coherent set of indications and controls for the operators that will use them. For MCR digital HSIs, the more digital HSIs are leveraged, the more those new digital upgrades need to be harmonized with existing HSIs that either will be upgraded later or not at all. For complex I&C upgrades, such as those being proposed in Section 3 for the Reference Plant, any significant impact to MCR HSIs (either done in phases or in a "one-shot" upgrade) will likely need to be validated through additional HFE testing and evaluation. NUREG-0711 [24] guidance identifies this activity as ISV.

ISV is intended to validate, using performance-based tests, that the integrated system design (i.e., HSI hardware, software, procedures, and personnel elements) supports the safe operation of the plant. Performing an ISV may not be a licensing requirement for safety-related I&C upgrades (e.g., as addressed by PV for Limerick) or for any particular non-safety related I&C function migration to a DCS platform under 10 CFR 50.59 [16]. It is, however, good engineering practice for all digital upgrades with a significant MCR HSI component. Performing wholesale digital upgrades without accounting for, designing in, or evaluating the net impact to the nuclear unit concept of operations through ISV could have negative impacts on plant reliability, availability, and ultimately plant safety. Conversely, including ISV as part of the digital upgrade program has improved performance in these same three areas across the process control industry.

ISV for DCS enabled I&C upgrades is optimally performed using the final HSIs coded by the DCS vendor along with associated DCS I&C functional application code software in a high-fidelity MCR simulator. Validated emulations of both can also be used. Glasstop simulators, while not qualified under ANSI/ANS 3.5 [21] have been successfully used for HSI evaluations to non-safety related DCS upgrades associated with supervisory control of the main turbine at three nuclear sites [1] and for PV for the safety-related I&C upgrades at Limerick [23]. Using a glasstop for this purpose allows for ISV without impacting the use of the ANSI/ANS-3.5 T&Q simulator for its function to support the plant prior to digital upgrade installation in the plant. Training and simulator operating personnel need to work with engineering and unit operations to develop the training and evaluation program to properly accomplish ISV, which also directly supports developing the training program for all operators that will use the new digital systems.

Modifying the T&Q simulator will be directly supported through the coordinated development of the digital I&C upgrades and glasstop simulator. Utilities can also use the glasstop simulator as a training bridge when updating the T&Q simulator after digital upgrades are implemented in the unit.

12. **Post-Modification Testing.** For both the Network Level 2 DCS platform upgrades (through Item 10) and Network Level 1 upgrades (through Item 11), operational checks and control algorithm tuning occur. These activities are performed using existing methods and techniques currently used for I&C upgrades.

13. **Lifecycle Support.** Lifecyle support is shown as the last item in Figure 20 because that is when any completed project enters into the traditional operational and support phase. For traditional fluid and mechanical system upgrades, waiting until this time to identify methods, techniques, and contracting models for lifecycle support is not necessarily wrong or risky because, in most cases, the lifecycle support for such systems is well known and predictable. Waiting until this time to establish an overall lifecycle support strategy for the DCS platform and all the legacy I&C migrated to it would be a major mistake. It is for that reason that Item 5 identifies the importance of fully considering DCS platform lifecycle support in the fleet long range planning phase, even before project approval and conceptual design authorization. Vendor selection and authorization to purchase of the DCS fleet laboratory are depicted as occurring no later than detailed design authorization, which occurs after Item 7. The dotted line on from detailed design authorization to this item in Figure 20 shows that the DCS platform lifecycle support strategy is cast at this point and will govern the iterative DCS lifecycle of technology refreshes.

5.4.2.3 DCS Platform Software Patching Process

With the DCS fleet laboratory (Section 5.2.2.1) and a glasstop simulator (Section 5.3) in place to support the production non-safety related DCS systems deployed at one or more units, all can be leveraged together in an integrated manner to deploy DCS software and cybersecurity patches. Figure 21 provides a coordinated process for evaluating and deploying these patches.

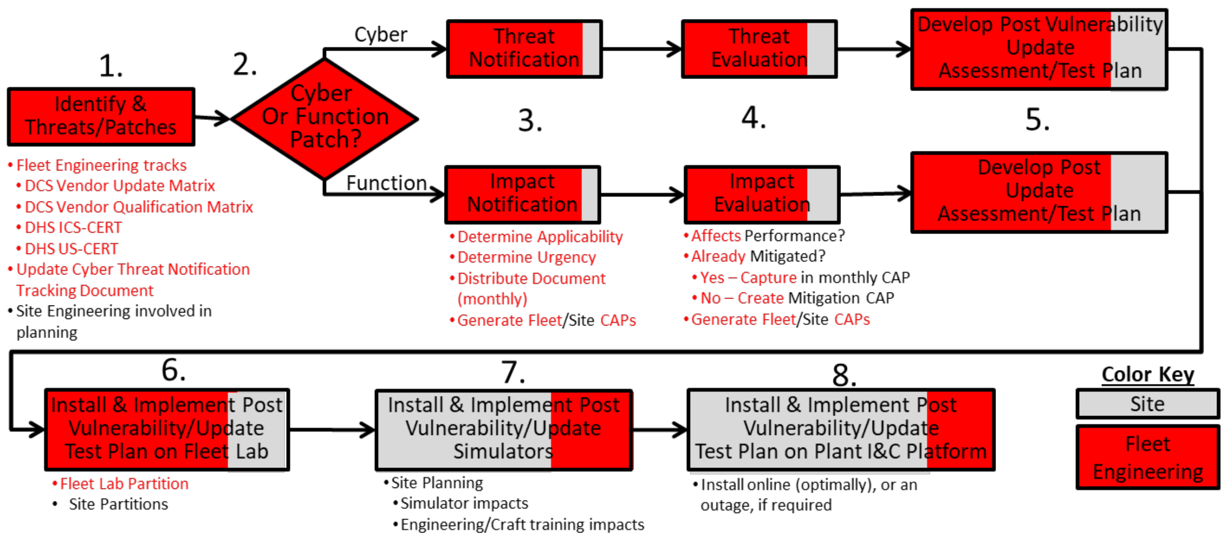


Figure 21. Process for non-safety related DCS software patching.

A brief, simplified description of the effort that occurs for each action shape depicted in Figure 19 is provided here, following the numbering of steps in Figure 21.

1. **Identify cybersecurity threats and functional issues and patches to address them.** The DCS vendor tracks both the worldwide performance of their product and potential cybersecurity threats that may be applicable to it. This includes threats for products in their supply chain (e.g., operating systems such as Microsoft Windows®, VM host software). Tier 2 (Section 5.2.2) and Tier 3 (Section 5.2.1) personnel also coordinate to evaluate other sources of cybersecurity threat information as listed in the figure to identify threats that could impact the non-safety related DCS. These are communicated to the DCS vendor.

   The DCS vendor has the primary responsibility to determine the applicability and nature of the issues (whether they are cybersecurity threats or DCS operational issues) and determine the path forward to remediate them. The vendor validates patches provided by their suppliers or developed by themselves to address them. The vendor only provides prevalidated cybersecurity or DCS functional patches to their customers because of the potential safety and economic risks to themselves and their customers associated with an unintended DCS function upset induced by applying an unvalidated patch. As identification, creation, and vendor validation of cybersecurity and DCS functional patches takes time, OT DCS patching tends to lag similar patching activities in IT systems. This is accounted for in the remaining items from Figure 21 as described below.

2. **Identify whether the identified patch is related to cybersecurity or DCS functionality.** As can be seen in Figure 21, the path for each type of patch is very similar as far as execution is concerned. They are different when it comes to how they are tracked and documented. While all patches are evaluated by Tier 2 and Tier 3 engineering personnel for operational impact to the DCS, cybersecurity evaluations at nuclear utilities tend to follow additional processes and produce separate documentation to demonstrate compliance with the cybersecurity rule (10 CFR 73.54) [6] and other NRC and industry guidance (e.g., [7], [14], and [15]). For ease of understanding, the rest of the items below are described at a level of abstraction to envelope both types of patches.

3. **Threat and impact notifications.** Utility organizations that own DCS systems (e.g., the DCS fleet laboratory [Tier 2], the glasstop simulators [training organization personnel], and the installed DCS systems across the fleet [Tier 1]) are notified of the issue, determine its applicability and urgency to address it, and start the process of implementing the patch through the CAP process.

4. **Threat and impact evaluations.** These are performed to determine the nature of the issue requiring the patch. These evaluations identify potential cyber and operational performance impacts that could result from the cyber threat being exploited or likelihood and severity functional impacts that may occur if the issue associated with the functional patch is manifested before the patch is developed, vendor-validated, and installed.

5. **Develop post cyber and operational impact vulnerability update assessment and test plan.** Based upon the threat and impact evaluation results from Item 4, a plan is developed to obtain the necessary vendor prevalidated patch, test it, and ultimately install it in the plant production DCS platforms in the nuclear units. The expected typical path for testing and deploying such updates to build confidence that the patch will not negatively impact the function of the production DCSs is outlined in items 6-8 below.

6. **Install and implement post vulnerability update using the test plan on the DCS fleet laboratory system.** The identified patch is first loaded on the DCS fleet laboratory system by Tier 2 personnel following vendor installation procedures and its impact on system operation is evaluated. Any issues that are discovered are reviewed and rectified. Any additional utility specific procedural controls or installation instructions are developed to permit patch installation on site-specific simulators (glasstop and T&Q) and on plant production DCS platforms.

7. **Install and implement post vulnerability update using the test plan on the glasstop and ANSI-ANS 3.5 T&Q simulators.** After successful patch installation and testing on the DCS fleet laboratory, the patch is installed on both of the identified simulators. If any issues are discovered, these are also evaluated and rectified as necessary.

8. **Install and implement post vulnerability update using the test plan on the plant production DCS platforms.** Only after the patch has been successfully performed on the DCS fleet laboratory system and site-specific simulators, the patch is then installed on the unit-specific DCS platforms.

Following this process updates all the separate instances of the DCS at each unit and across the utility fleet. The order of installation ensures each patch has been validated by the vendor and tested on at least three nonproduction systems prior to installing it on the first production DCS platform in a nuclear unit.

Procedures to implement the patching process described above are best developed during the detailed design process for the standard non-safety related DCS platform implementation. EC design documentation should be written in such a way that performing cybersecurity or functionality related patching is an O&M support activity, not a design change that must follow the EC process. This represents a significant WRO. This is enabled by the fact that the vendor validates that such patches, when properly installed, maintain the DCS within its bounded configuration so that its performance characteristics are maintained. Standard fleetwide procedures used to accomplish such patch installations need to update system documentation such that configuration control is maintained for all the platforms upgraded in this manner across the utility fleet.

5.4.2.4 Fleet DCS Platform Upgrade Process

There will be a time when DCS platform initial installations reach a level of obsolescence where it is more advantageous to perform a system technology refresh rather than sustain legacy DCS equipment and operating system software. The process to perform this evolution is represented by the "inside track" of Figure 20. Since the Network Level 2 portion of the DCS is reliant on DCS vendor utilization of IT technology, its refresh cycle will be shorter than that for Network Level 1 DCS equipment. To illustrate the Network Level 2 system refresh, a simplified version of the process presented in Figure 20 is provided in Figure 22 to highlight several key differences. It is best to discuss these differences by leveraging the two shaded areas in Figure 22.

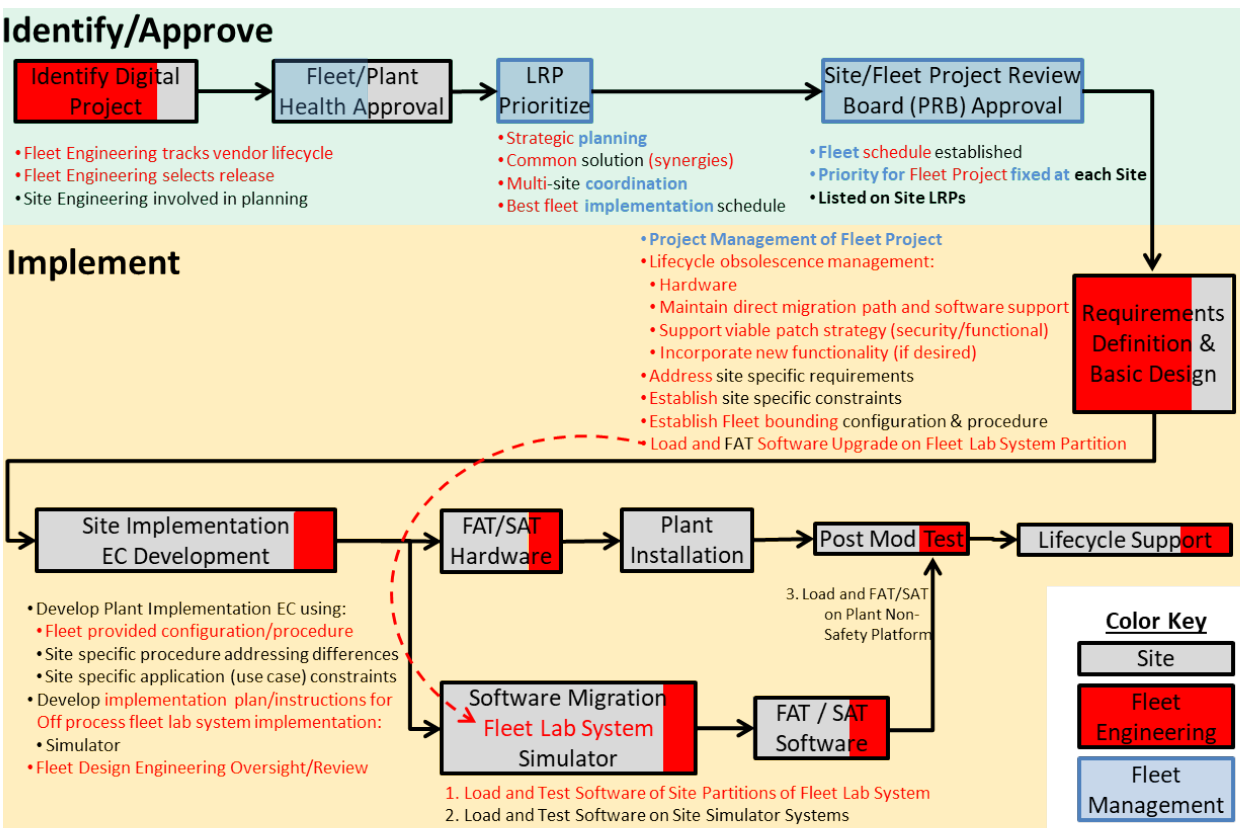


Figure 22. Process for fleet distributed process control system platform upgrade (Network Level 2).

- **Identify and Approve.** In this portion of Figure 22, decisions are made at a utility fleet level regarding the selection of the most advantageous target version of the DCS that will enable the maximum useful life for the DCS systems when refreshed. Discussion on how to select the target refresh version is captured in Section 4.2.6. With the DCS vendor version selected and an overview of the expected sequence of refresh implementations across the fleet, individual site and fleet plant health committee approval is obtained. Detailed strategic planning then occurs through collaboration between all three engineering organizational tiers as described in Section 5.2. The result is a detailed fleet coordinated schedule prioritized to enable Network Level 2 technology upgrades at minimum cost with the lowest operational impact across the fleet. Again, this activity would be best implemented while plants remain online during the technology refresh process. This would provide maximum flexibility for fleet DCS technology refreshes and reduce workload during plant outages. Also, non-safety related DCS system functionality would be available during outage periods to support outage controlling path work.

Once the fleet DCS platform technology refresh schedule is prioritized and approved by the individual site and fleet senior leadership, significant schedule changes should be minimized and require approval of the utility fleet leadership team to contain fleetwide impacts that could result from such a change.

- **Implement.** So long as the fully redundant Network Level 2 configurations at each site have remained within the validated configuration envelope established by the DCS vendor, a technology refresh of Network Level 2 can be performed using predeveloped and prevalidated vendor techniques. A detailed discussion of how this is enabled by virtualization for a representative DCS vendor is provided in Section 4 and Appendix A of [1]. All of the Network Level 2 hosted software applications and the DCS server can be exported and migrated to new hardware hosting new operating systems in a separate vendor facility. V&V of the migration typically occurs in the same vendor location. On-process installation and post-modification testing in non-nuclear process control applications can be accomplished in a matter of days. Adapting this process to achieve such levels of performance to nuclear may be challenging, but it offers significant opportunities for WRO realization.

  It is expected that a technology refresh of DCS platforms will follow the same order of operation for applying cybersecurity and functional patches (DCS fleet laboratory, site simulator, and then production DCSs in operating units). This further mitigates risks associated with technology refresh activities as much practical experience will be gained by first upgrading nonproduction DCS systems.

Representative methods enabling a similar technology refresh of redundant DCS Network Level 1 implementations is outlined in Section 4.2.5 of [1].

6. PRACTICAL APPLICATION OF AI FOR PLANT SUPPORT ACTIVITIES

6.1 Industry AI Landscape

AI has become a major focus for technology giants, as companies like Apple, Microsoft, and Google scramble to integrate AI tools into their products. These Large Language Models (LLMs) are now capable of quickly answering a wide range of complex questions in context. Once integrated into commonly used applications, these models will provide users with powerful AI-enabled efficiencies to improve their existing workflows. Given these recent advancements, there are many options for businesses to integrate AI tools into their workflows. There are also many questions that must be considered before implementing such tools. Businesses will need to choose if they want to query a public LLM, buy subscriptions for their employees to use these public LLMs, hire an AI vendor to help them choose and create a custom solution, develop an AI solution themselves using open-source software, or purchase a subscription for developing guided AI suites. There are many different problems that can be solved with AI technology, but successful cost-benefit analyses are important to choose the right solutions for use cases desired by the business. Consideration of data security requirements also needs to be a significant factor in these decisions because different AI options allow varying levels of data security.

The current industry landscape for AI is one where the top performing LLMs use cloud storage and require subscription fees. There are also AI development suites, such as IBM's watsonx.ai, that require subscriptions but help developers create custom solutions. These AI development suites can help guide AI developers in creating and using AI models that meet their performance and data security requirements.

Free open-source models offer powerful and flexible solutions for AI developers. Leveraging open-source models, however, requires significant training data and customization to make them useful for business applications. Training data first provide the information AI models ingest to learn how to mimic human processes or solve problems. Secondly, training data provide a set of example expected outputs based upon the input training data so the AI can learn the relationships between input information and the desired outputs. Through pattern recognition, the AI learns to use the training data, enabling it to predict and produce the desired outputs from similar input information. This effectively mimics the functional process currently performed by people at a high level of performance. For example, to train an AI model to create a report template based on information from a chart, the appropriate training data would be a sufficient set of past reports that humans wrote that include the charts that will form the basis for the new AI template within them. These past reports and included charts allow the AI model to learn how to create the report from the chart inputs just like the humans already do. While this learning is challenging to implement, open-source LLMs enable engineers to create customized AI models to automate tasks efficiently without paid subscriptions.

For practical tasks where businesses desire to leverage AI-enabled efficiencies, a more compartmentalized AI model is sometimes preferable compared to an LLM. This may be especially true when the task requires predictive monitoring or complex physical movements and is not intended for general tasks. Artificial Narrow Intelligence (ANI) dominates current practical applications in this area, particularly in industries like robotics, where specialized, reliable solutions are preferred to AI tools intended for more general applications. Such ANI models are designed for specific applications and continuously improve through reinforcement learning. For instance, ANI has been used to streamline work order scheduling in some NPPs, which is a very specific use case but when optimized prevents delays and their associated costs.

Whether a utility chooses to use subscription or open-source AI tools, data security is a concern. Most subscription and open-source AI models can be configured to employ cloud, private cloud, or onsite storage options. Cloud storage provides scalable access from almost any location, but public cloud models should not be used with sensitive data. Private cloud storage can mitigate these data security concerns and provide scalable access at multiple locations, but this storage option requires subscriptions and customized AI tools to be configured. Private cloud storage also requires security to be managed, and the private AI will not have access to the large amount of training data that the public models do by default. Finally onsite storage is an attractive option for handling sensitive data but is not usually scalable for large amounts of data that need to be accessed from multiple locations. A utility employing AI models will need to decide on the optimal data security model based on their needs and concerns.

Consultants who specialize in nuclear power and AI technology can offer tailored solutions for automating complex tasks at nuclear plants while ensuring data security, reliability, and operational efficiency. This approach allows NPPs to continue operations with minimal disruption. Experts in integrating customized AI solutions will be valuable in industries with stable regulatory environments, mature protocols, and secure operations. The need for customized solutions and secure operation tend to make public models and general AI solutions infeasible for nuclear industry application in the long-term.

6.2 Defining Generative AI

Generative AI involves deep learning models that create multimedia content based on patterns learned from data. These models can respond to user prompts by generating new content. Deep learning, a subset of ML that predictively monitors systems, uses multilayered neural networks to mimic human decision-making. It requires substantial data and computing power for the algorithms to learn the arbitrary relationships within datasets and predict patterns accurately.

In a generative AI model that can interpret, describe, summarize, and answer questions about a given text or data in human language, the process starts with training the model with many texts like what it will receive as input when used. Generative AI is particularly useful for finding patterns in unstructured data such as text, which allows the model to predictively answer questions about the text based on its complex knowledge of the contextual relationships between words.

Through iterative reinforcement learning, the model learns from its successes and failures by adjusting the weight or value of importance for the data relationship that informed its right or wrong decision. For models intended to answer a wide variety of questions like Chat GPT, a diverse set of training data is required. For more specific applications, however, it is best to use training data analogous to the data it will be expected to process once finished.

Generative AI models are easily implemented to assist humans by speeding up their tasks, instead of replacing humans in tasks that require near perfection. For instance, if an NPP implements an AI model to learn report creation, it would be infeasible and against current protocol to direct an operator to perform a field task (e.g., manipulating a valve) based solely on the output of the AI tool. This is because the operator needs to validate the contents of the report against conditions in the field. It would be most helpful to have the AI model learn to draft the report template, allowing the operator to complete the important and complicated sections. This would assist the operator in completing the task as usual without wasting time on the administrative sections the AI model is capable of drafting. Review and approval by qualified SMEs for reports written with the assistance of AI tool would still be required.

6.3 Current Uses for AI in the Nuclear Industry

AI technology advancements are increasingly making AI tools viable and cost effective to enhance the efficiency of various tasks in nuclear power, such as business processes, documentation creation, task automation, and other activities not directly involved in direct physical operation of the plant. For instance, AI has been employed at a limited number of nuclear facilities operated by one utility to assist in specific activities associated with creating schedules for corrective work orders and capturing related items and information associated with performing those scheduled work orders. This includes scheduling the work orders following predetermined rules and documents bundled tasks based on crew availability and qualifications, parts availability, and plant conditions required to perform the work.

6.4 Pilot Application of AI Tool at the Reference Plant

AI chatbots that help with creative document writing tasks are different from AI tools presented in Section 6.3. They are also different from those used in ML algorithms used to predictively monitor systems. Regardless of this, the power of these technologies is in their extremely accurate and reliable prediction capabilities when given an adequate training set. In fact, these technologies also incorporate user feedback into their results, as well as collecting continued data for their training to increase their predictive power.

AI chatbots used to support document drafting tools work by predicting and returning information relevant to the user prompt leveraging a natural language understanding engine. They do that using the context from their training information. ML monitoring systems and ANI technology however take historical data to perfect the decisions and predict the responses of plant factors in components to prevent errors, especially repeat errors that happened in the past, which they can analyze using causal patterns to prevent similar negative outcomes.

6.4.1 Overview

The integration of AI as a tool for creating reports represents a novel application in the nuclear power industry. This project, as being pursued at the Reference Plant, aims to incorporate an AI chatbot tool into the existing workflow of report creation by engineers, enhancing efficiency without significantly altering established procedures and workflows. The AI tool assists experienced report authors in quickly accessing, retrieving, and rearranging the data determined by the chatbot to be relevant based upon the context provided by author input. This enables authors to draft reports more efficiently. This approach leverages the AI's ability to provide relevant draft results based on input data on demand from a large knowledge base, allowing authors to focus on validating the content rather than manually searching through extensive historical documents, gathering pertinent information, and assembling the report.

6.4.2 Objective

The primary objective of this project is to explore WROs through the integration of an AI chatbot tool into the existing workflows for report creation by engineers at NPPs. The AI tool helps engineers write reports faster with high quality while retaining the benefits of human verification for maintaining accurate reports. This AI tool, trained on relevant historical nuclear reports and documentation, aims to modernize the report creation process without requiring changes to current procedures or protocols. Additionally, the preparation of historical data for AI training creates a centralized and easily searchable knowledge base, by converting previously scanned paper documents into a word-searchable digital format and combining those with other digitally stored word-searchable documents as well.

6.4.3 Approach

The project began with a conversation at the ANS Utility Working Conference, leading to a pilot project at the Reference Plant. After obtaining Owner approval and funding, the approach involved pre-processing of over 20 years of human-verified historical data in collaboration with the Reference Plant's selected AI vendor (NuclearN). This included removing irrelevant information from the training data to retain only essential text, allowing the AI to be implemented without procedural changes. The AI vendor's experience in nuclear engineering processes and modern AI technology was crucial to this effort. Human-verified training data is essential to prevent the AI from learning and incorporating erroneous information in the text of a report generated by the tool. Leadership buy-in was secured, and contracts for support were established, including a private, secure, DOE Part 810 compliant host data environment and a single deployment of the Owner model. The protected transmission of documents and development with vendors were integral steps in the approach.

NPPs are fortunate to have a significant amount of validated documentation and operational data on past equipment failures. Additionally, there are very few novel failures at an NPP. These two factors help provide a firm foundation for the application of generative AI to assist with work order development and problem identification when new equipment challenges or failures occur. Documents included into the generative AI tool training scope include:

- Completed work orders
- Procedures
- Design basis documents
- Vendor technical manuals
- Final safety evaluation reports
- Vendor correspondence
- Previous corrective action evaluation reports.

The abundance of this data makes training an AI to assist with these tasks an efficient solution for drafting documents given the available resources.

The steps being followed as part of this effort are:

1. Engagement with the industry
2. Engagement with engineers to determine use cases and necessary enabling input information to enable them
3. Engagement with corporate, legal, and other stakeholders to obtain buy-in and funding
4. Contracting the vendor for proof-of-concept activities
5. Establishing broader applicability of tool usage based on initial learnings
6. Developing plans and applicable guidance to use the tool and produce outputs
7. Rolling out the tool to one site (current state as of the writing of this report) to obtain initial user feedback and incorporate changes to improve the user experience and output product quality prior to exposing the tool to a larger audience.
8. Adding more data for more sites
9. Rolling it out to the fleet. This rollout will include guidance that specifies that the AI tool will be used as a tool to assist authors in developing initial draft products. Existing procedures to review and approve products to ensure accuracy and completeness prior to use will still be followed.

Relevant information about the use of the AI product is also being documented and will be reported in future research.

6.4.4 Preliminary Results and Benefits

The AI tool has been used to demonstrate several direct use cases. Engineers have interacted with the AI by typing prompts with the applicable input information. The AI responds within seconds, integrating its knowledge of protocols, procedures, and site components. This interaction allows engineers to quickly retrieve relevant information from site documentation and historical documents, making this data available on demand instead of requiring a lengthy search process. The AI tool also has the capability to output grammatically correct results in the context established by the input information provided. This capability significantly reduces the time required to author and review reports. This allows engineers to focus on output product validation rather than the mechanics of product creation.

At the time of authoring this document, engineers are in the process of integrating this tool into their normal workflows for creating reports. While the general capabilities are known through the generation of "directionally correct" draft results, estimating the near- and long-term benefits realized will be quantified and discussed in future research.

Use cases include drafting documents and evaluations in:

- Boric acid corrosion (BAC) evaluations
- Procedure drafting
- Maintenance rule evaluations
- Simple failures
- Work orders

The Reference Plant project team focused on BAC evaluations as an illustrative first use case for AI tool usage for two key reasons:

1. The significant number of historical evaluations that have been developed and validated by Reference Plant experts.
2. The broad applicability to the industry. Nearly all nuclear plants produce many of these evaluations (~50 per year).

Appendix A provides an example of an existing BAC evaluation report to orient the reader of this document as to the content and format of a current report written by an engineer.

Appendix B provides examples to demonstrate the capability of the chatbot-enabled AI report generating tool. For each example,

1. Inputs provided to the AI tool by an engineer tasked to perform a boric acid evaluation and author a report are listed.
2. Representative outputs from the AI tool produced as a result of Item 1 directly above are provided
3. Commentary for each example is then given that:
    a. Describes the value added by representative AI tool outputs provided by Item 2.
    b. Applies a questioning attitude to AI tool outputs to generate outputs intended to:
        i. Identify how document authors should best leverage the outputs in to assist in generating BAC evaluation reports
        ii. Enable continued AI tool improvements to enable production of increasingly specific and valuable output information to tool users.

6.4.5 Lessons Learned

Several lessons were learned during the project, including the importance of vendor selection, data management, and cybersecurity and are discussed in this section.

An important lesson learned in this project was understanding the data requirements for training the AI chatbot and what needed to be done to identify, capture, organize, and reformat historical site data and NRC documentation for that purpose. To make the historical documents useful as training data, removing irrelevant information such as signatures, names, handwritten information, etc. was necessary.

The need to perform this pre-processing was identified after the tool was loaded with raw data. Tool performance and the quality of the tool output were both negatively impacted if the tool was loaded in with unprocessed or unscrubbed training data. Finishing the data pre-processing was time consuming because many of the historical documents had been digitally scanned as images. These images needed to be converted to digital text documents using optical character recognition so they could be used to train the AI tool. Once this was accomplished, the vendor was able to train the AI with digital tabular data and digital text information. Significant improvement to AI tool performance and the quality of text outputs has been observed.

Another time-consuming project challenge was obtaining assent to move the project forward from the Owner legal and cybersecurity teams. This process took almost 3 months. Significant education on AI technology and project education on how it was to be used was necessary. Agreement that the project needed to be import and export control compliant had to be established. Siloed behavior with regard to the contract approval process had to be addressed. Finally, cybersecurity concerns associated with setup, use, and data storage mechanisms for the AI tool had to be addressed. This required agreement that cybersecurity risks must be understood and that mitigation strategies be identified to address them. These conversations also led to the idea that this project should be expanded beyond the Reference Plant to an Owner fleetwide approach. To accomplish this, it is planned to conglomerate historical data from the other nuclear sites in the Owner fleet to create the most efficient and effective AI product for the Owner's "run the business" enterprise.

A fleet approach for leveraging AI products across several NPPs requires a consistent level of security and standardized processes to enforce security practices related to the use of the AI tool across the fleet. It also allows enterprisewide historical training data to be utilized, making the AI tool a comprehensive solution for any site in the fleet.

Also, a centralized approach helps ensure that innovative projects like these do not have their approval stifled due to site-specific managerial disagreements between departments or teams and creates a standard procedure for the safe implementation of these projects.

Given the high frequency of AI technology and myths surrounding it in the media, additional important lessons learned are to:

- Address and mitigate any real risks that the technology might have
- Dispel any misconceptions that might hinder the adoption of the AI tool
- Dispel any misconceptions that might cause misuse of the AI tool.

The AI tool created in this project is a document creation tool to help engineers write reports faster due to its encoded knowledge of the historical data and documentation from the site. This tool is only to be used by personnel (primarily engineers) to draft documents efficiently. The significant amount of time previously spent by these personnel to retrieve and apply reference information, format their documents, and write the prose for the reports is greatly reduced. There are not any use cases at this time for this AI product other than aiding the engineers in drafting the reports more efficiently. Qualified engineers will still validate the reports through reviews before they are used to inform or direct worker activities. There will be no changes in existing review procedures and protocols. Cybersecurity has been effectively managed for this project to date. A potential risk or concern in using the AI tool in this manner relates to negatively impacting the level of knowledge and experience of engineers who draft reports using the AI tool over time. The manual activity of searching for relevant information to produce reports, analyzing that information, determining its relevance, and manually incorporating it into a coherent report is labor intensive. It does, however, have significant training value. Such activities tend to enhance the qualification and experience of engineers as such efforts broaden and increases the depth of knowledge with regard to the work being performed. Still requiring SME reviews and manual correction of items that are identified by such reviews may help mitigate this concern.

When the data was being conglomerated for the Reference Plant, there were additional lessons learned related to cybersecurity and data storage. The dataset grew to the point that it consists of 450 gigabytes of information. This dataset needed to be securely shared with the AI vendor for AI tool development and training. The only secure options to share such a large dataset was to either fly a physical hard drive out and deliver it to the vendor or use a secure server to store and transfer the data. The second option was chosen, but the server was not designed for transferring that much data. To address this challenge, the vendors created a macro on their end to effectively download the information from the server. The AI model itself is securely stored on a private government regulatory compliance server.

Taking the time to identify and select a qualified AI vendor was another lesson learned in this project. There are multiple AI vendors who have the general technical acumen to support a project such as the one undertaken by the Reference Plant and now being pursued across the Owner fleet. However, there are not many vendors for this type of project that also have extensive experience with nuclear engineering. The vendor selected for this project has this experience. As a result, they were able to validate the success of the model as they trained it to support a nuclear customer. While this vendor chose not to use the most advanced and well-trained models available, their experience in nuclear engineering was most helpful as the goal of the project was to solve a very specific problem. The most advanced commercially available models also are intended for a wider variety of use cases than currently envisioned by the utility. Much of the success of this project is due to the vendor’s ability to apply the selected AI technology to this specific use case, and their experience in nuclear engineering was vital to enable this opportunity in a timely manner.

Another lesson learned and benefit of this project was the centralization of data into an organized and searchable database. This has been a side effect of conglomerating the data to share it with the vendor. This centralization created a virtual and searchable knowledge base that contains significant sets of documents that were previously stored in disparate locations. This feature helps the process of report creation by making this expansive dataset accessible and in a standard digital format and significantly increases the speed at which included documents can be retrieved for any purpose. Before the data was conglomerated, it was stored separately in multiple locations and was in a variety of formats, causing a lengthy process for anyone collecting data from the different locations.

In terms of the scope of work for this project, it has been necessary for the AI vendor to be flexible and help in formulating different ideas as possible solutions in collaboration with the Reference Plant project team. The vendor helped hone down the different possible applications of the technology and was open to the team's suggestions of what functionality they wanted. The lesson learned in this stage of the project was that it is important to choose an AI vendor with nuclear experience that will at the same time listen and work with the Owner project team to address concerns and find the most efficient and secure solutions for the implementation of the AI tool.

Lastly, there were lessons learned about the guidance to be given to engineers acting as authors on how to use the AI tool in their normal workflows. Authors were first provided instructions on how to use the AI tool interface. They were then instructed to prompt the AI tool with sufficient input information to enable the AI tool LLM to produce context-appropriate output text to be used in authoring a report on a particular topic. Once the author provided enough information to the AI tool for it to produce an output that the author believed to be sufficient to address the topic at hand, a small team of experienced engineers reviewed that output. Based upon the quality of the outputs produced following this method, it was determined that the AI tool should be treated by engineers acting as authors as a virtual intern capable of writing initial drafts for their reports. The qualified engineer using the tool output is expected to make necessary changes and corrections to complete the work product for its particular use. By feeding the result back into the AI tool input dataset, the AI tool will continue to learn over time with the expectation that it will produce increasing more contextually correct results over time.

An expanded set of individuals using the AI tool as discussed above will continue to test its applications in the production of reports. This will continue until such time as it is deemed appropriate to leverage the AI tool more widely across the fleet. Clearly defining specific use cases and limitations of the AI tool to the engineers has been and will continue to be an important step in driving the adoption of the tool and making sure it is used correctly and only when appropriate. This AI tool also includes a sophisticated English language tool that is intended to help engineers avoid grammatical mistakes and run-on sentences that can occur as part of the writing process.

As shown in the list of activities being accomplished for this initial pilot effort in Section 6.4.3, development work in this area continues. Future lessons learned will continue to be documented as the project progresses and will be applied to this effort going forward. These early efforts demonstrate the potential benefits of applying this AI tool technology to deliver WROs in the area of administrative processes. It is expected that, as AI and ML technology continues to mature, it will also be able to leverage live digital I&C data provided by OT digital I&C systems as well as low-cost IT monitoring systems across the DI for analysis to improve plant operational efficiency and more fully enable WROs such as condition-based maintenance and system and component diagnostic and prognostic monitoring.

6.5 Potential Future Research

Future research will continue to explore the capabilities and applications of AI in nuclear power, with specific areas to be determined as the technology and its integration into workflows evolve. Potential research directions include further enhancements in AI-assisted documentation, such as the tool discussed above, improved data management strategies, and expanded use of AI for other non-plant operations functions. The ongoing evaluation of this AI tool's impact on work reduction and efficiency will also guide future developments and refinements. It is expected that this future research will help to expand WRO realization in a way that can be fully integrated into future ION activities.

7. CONCLUSIONS

This document provides a comprehensive foundation to demonstrate digital technology enabled ION WROs. This foundation includes a holistic approach that integrates nuclear utility people, process, and governance changes with modern digital technology applications implemented within the DI framework to deliver WROs. Relying on or overemphasizing the importance of one of these areas (e.g., focusing primarily on what digital technology can do as opposed to how it will be used and maintained for its lifecycle by people following processes) will likely produce suboptimal results in the long run.

This document focuses on the two areas where digital technology within the ION PTPG construct can be most highly leveraged: non-safety related I&C OT technology at Purdue Network Levels 0–3 and labor-saving vendor support capabilities and software applications such as AI tools running on IT systems at Network Levels 4–6. Safety-related I&C systems can feed information to non-safety related OT systems and utility IT systems for presentation and analysis. This capability can enhance both "running the plant" and "running the business" activities and enable a more limited set of WROs on safety-related I&C systems.

Current regulations on safety-related OT, while providing for the highest levels of plant safety, tend to slow the ability of these systems to keep up with digital technology capabilities offered outside of this arena to provide additional WROs. The time and costs associated with performing the engineering and licensing efforts to develop a topical report for and obtain a favorable NRC safety evaluation of a state-of-the-industry safety-related digital I&C platform is daunting. Efforts to keep such systems technically current following the same processes are similarly challenging. Leveraging NRC RG 1.250, "Dedication of Commercial-Grade Digital Instrumentation and Control Items for Nuclear Plants" [26], which endorses NEI-17-06, "Guidance for Using IEC 61508 SIL Certification to Support Commercial Grade Equipment for Nuclear Safety" [27], provides a potential avenue for the nuclear industry to deploy and support safety-related digital platform upgrades with more modern platforms. Following this guidance to commercially dedicate a software integrity level three (SIL-3) digital platform and its lifecycle support strategy from one or more commercial control system vendors could significantly reduce costs to modernize and maintain safety-related I&C systems going forward. This path would likely also provide the nuclear industry with the capability to realize additional WROs by leveraging a more comprehensive set of features that vendors offer to enable WROs for their non-nuclear customers.

8. REFERENCES

1. Hunton, P., R. England. 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.

2. Hunton, P., and R. England. 2021. "Digital Infrastructure Migration Framework." INL/EXT-21-64580. Idaho National Laboratory. https://doi.org/10.2172/1822876.

3. Hunton, P., R. England, and S. Lawrie, et. al. 2023. "Pilot Business Case Analysis for Digital Infrastructure." INL/RPT-23-74393. Idaho National Laboratory, https://www.osti.gov/biblio/1999195.

4. Hunton, P., R. England, and S. Lawrie, et. al. 2023. "Integrated Operations for Nuclear: Work Reduction Opportunity Demonstration Strategy," INL/RPT-23-74671. Idaho National Laboratory. https://www.osti.gov/biblio/2000859.
5. Remer, J., J. Hansen, and S. Lawrie, et. al. 2023. "Integrated Operations for Nuclear Business Operation Model Analysis and Industry Validation." INL/RPT-22-68671 Revision 1, Idaho National Laboratory. https://lwrs.inl.gov/Advanced%20IIC%20System%20Technologies/ION_Operation_Model_Analysis.pdf.
6. Code of Federal Regulations, Section 10, Part 73.54. 2015. "Protection of Digital Computer and Communication Systems and Networks." https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html.
7. Nuclear Regulatory Commission. 2023. "Cyber Security Programs for Nuclear Power Reactors," Regulatory Guide 5.71. https://www.nrc.gov/docs/ML0903/ML090340159.pdf.
8. Hunton, P., R. England, et. al. 2020. "Safety-Related Instrumentation and Control Pilot Upgrade: Initial Scoping Phase Implementation Report and Lessons Learned." INL/EXT-20-59809. Idaho National Laboratory. https://www.osti.gov/biblio/1668846.
9. Hunton, P., R. England, et. al. 2023. "Safety-Related Instrumentation and Control Upgrade: Conceptual – Detailed Design Phase Report and Lessons Learned." INL/RPT-23-72105. Idaho National Laboratory. https://www.osti.gov/biblio/1983868.
10. Electric Power Research Institute. 2023. "Digital Engineering Guide." Report number 300202011916.
11. Hunton, P., S. Lawrie, et. al. 2020. "Business Case Analysis for Digital Safety-Related Instrumentation & Control System Modernizations – as Applied to the Limerick Generating Station." INL/EXT-20-59371. Idaho National Laboratory. https://www.osti.gov/biblio/1660976.
12. Nuclear Regulatory Commission. 1981. "Functional Criteria for Emergency Response Facilities," NUREG-0696
13. Nuclear Regulatory Commission. 2023. "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants," NUREG-0654, Revision 2
14. NEI 08-09 Rev. 6, "Cyber Security Plan for Nuclear Reactors," Nuclear Energy Institute, April 2010
15. NEI 13-10 Rev. 4, "Cyber Security Control Assessments," Nuclear Energy Institute, November 2015
16. Code of Federal Regulations, Section 10, Part 50.59, "Changes, Tests, and Experiments," Nuclear Regulatory Commission,
17. Nuclear Power Group Calculation Titled "Segmentation Analysis for Watts Bar Unit 2 Distributed Control System," Tennessee Valley Authority, August 2, 2010 – Nuclear Regulatory Commission ADAMS #ML102240384
18. NUREG-0847, Supplement 23, "Safety Evaluation Report Related to the Operation of Watts Bar Nuclear Plant, Unit 2," July 2011
19. "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
20. Institute of Nuclear Plant Operations. 2021. "Equipment Reliability Process Description," AP-913, Rev. 1.

21. American Nuclear Society. "Nuclear Power Plant Simulators for Use in Operator Training and Examination." ANSI/ANS-3.5 (version invoked in NRC plant license is plant specific)

22. Constellation Energy Generation, LLC. April 5, 2023. "Limerick Generation Station, Units 1 and 2 Renewed Facility Operating License Nos. NPF-39 and NPF-85 NRC Docket Nos. 50-352 and 50-353. Subject: Supplemental to License Amendment Request to Revise the Licensing and Design Basis to Incorporate the Replacement of Existing Safety-Related Analog Control Systems with a Single Digital Plant Protection System – Human Factors Engineering Conceptual Verification Results Summary Report Human Factors Engineering Preliminary Validation Results Summary Report." https://www.nrc.gov/docs/ML2309/ML23095A223.pdf.

23. Constellation Energy Generation, LLC. June 26, 2023. "Limerick Generation Station, Units 1 and 2 Renewed Facility Operating License Nos. NPF-39 and NPF-85 NRC Docket Nos. 50-352 and 50-353. Subject: Supplemental to License Amendment Request to Revise the Licensing and Design Basis to Incorporate the Replacement of Existing Safety-Related Analog Control Systems with a Single Digital Plant Protection System (PPS) – Human Factors Engineering Preliminary Validation Results Summary Report." https://www.nrc.gov/docs/ML2317/ML23177A224.pdf.

24. U.S. Nuclear Regulatory Commission. 2012. "Human Factors Engineering Program Review Model." NUREG-0711, Rev. 3, Washington, DC. https://www.nrc.gov/docs/ML1232/ML12324A013.pdf.

25. Hunton, P. J., et al. 2020. "Safety-Related I&C Pilot Upgrade Initial Scoping Phase Implementation Report and Lessons Learned." INL/EXT-20-59809, Idaho National Laboratory. https://www.osti.gov/servlets/purl/1668846, https://www.osti.gov/biblio/1668846.

26. Nuclear Regulatory Commission. October 2022. "Dedication of Commercial-Grade Digital Instrumentation and Control Items for Nuclear Plants," RG-1.250, Revision 0.

27. NEI 17-06, Rev. 1, "Guidance on Using IEC 61508 SIL Certification to support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications," Nuclear Energy Institute, December 2021

Appendix A: Boric Acid Corrosion Evaluation Baseline Example

Introduction

This appendix provides a completed example of content generated for an existing BAC evaluation produced by the Reference Plant. The purpose of providing this example is to provide a basis of comparison between manually generated engineer authored content for such an evaluation with content generated by the AI tool under study as provided in Appendix B.

It is not intended that the reader objectively evaluate the information provided in this appendix for its technical validity as that would require a more comprehensive understanding of the Reference Plant's BAC prevention program.

Reference Plant specific information (e.g. work order numbers, CR numbers, device numbers, etc.) has been redacted from this example as it does not pertain to the comparison between the content presented here against AI produced outputs as provided in Appendix B. Redacted information is identified using random capital letters (e.g. X, Y, Z, etc.)

Example Report Content

A Purpose

Perform a BAC evaluation IAW STI for the following locations:

1. X-LWPS RCDT PMP Y-0Z SUCT VLV
2. X-PRZR AUX SPR VLV
3. INJ VLV X1
4. INJ VLV X2
5. X-Y TST LN ISOL VLV
6. Y-FT-X: REACTOR COOLANT LOOP Z FLOW TRANSMITTER X PROT CHAN II

B Summary

WO-X will clean all boric acid from locations noted in CR-X Various WOs to rework components as needed. No components structural integrity has been affected.

C Evaluation

1. LWPS RCDT PMP Y-Z SUCT VLV

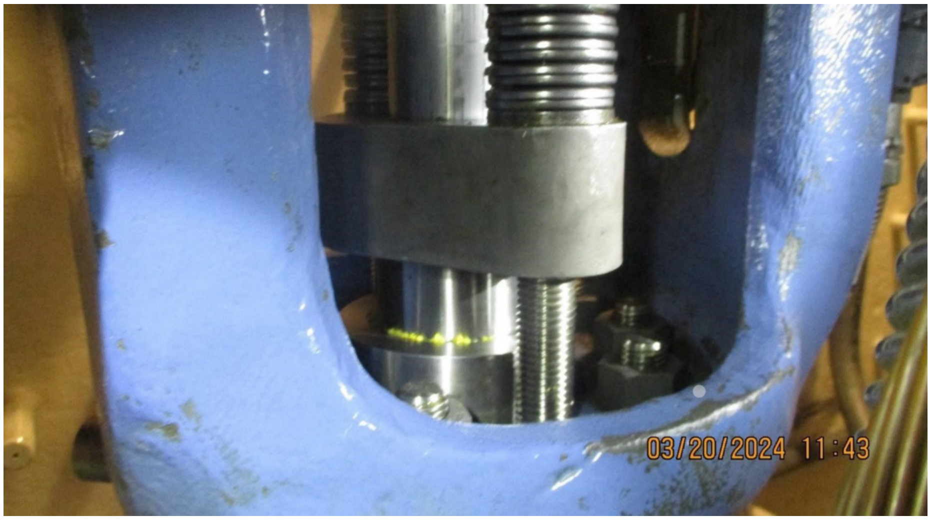
Part number X is the Y-Z RCDT Pump Suction Valve. Approximately 1 tablespoon of discolored, dry boric acid accumulation was identified at the diaphragm. The accumulation is present on the bonnet, bonnet studs and nuts, diaphragm, and finger plate. The boric acid accumulation has migrated to the floor and pump stand base but is touching concrete only. The boric acid has come into contact with the fingerplate which is constructed of carbon steel. All the other affected components are constructed of stainless steel which is resistant to BAC. The remaining carbon steel components of the valve are located near the handwheel and are not targets of boric acid. The EPRI BAC Guidebook indicates that tests conducted (for carbon steel, low alloy steels and martensitic stainless steels) when exposed to boric acid crystals exhibited very low corrosion rates. The highest rate observed on any of the alloys was 0.0005 inches per year. Though the fingerplate has a low thickness, there is low risk of significant corrosion occurring due to the low corrosion rate. There is no evidence of degradation or wastage, and the structural integrity of the component has not been affected. The component will continue to be monitored by the leak tracking list until repairs are completed. Work order X was created to rework the valve as needed. Work order Y was created to clean the boric acid.

2. PRZR AUX SPR VLV

X is the Unit Y Pressurizer Aux Spray Valve. A dry boric acid accumulation was identified at the packing. The boric acid accumulation is present on the packing gland, gland follower, stem, and the bonnet. The boric acid accumulation is < 1 tablespoon and contains some discoloration. The boric acid accumulation is localized at the packing and has not migrated to any other components. There was no evidence of degradation or wastage to the valve bonnet, packing gland, gland follower, or the stem. These components are constructed of stainless steel which is resistant to BAC. Because the boric acid has not contacted any carbon steel material, the discoloration in the accumulation is the result of the boric acid contacting grease/oil on the valve bonnet and stem. The structural integrity of the components has not been affected. Work order X was created to clean the boric acid.

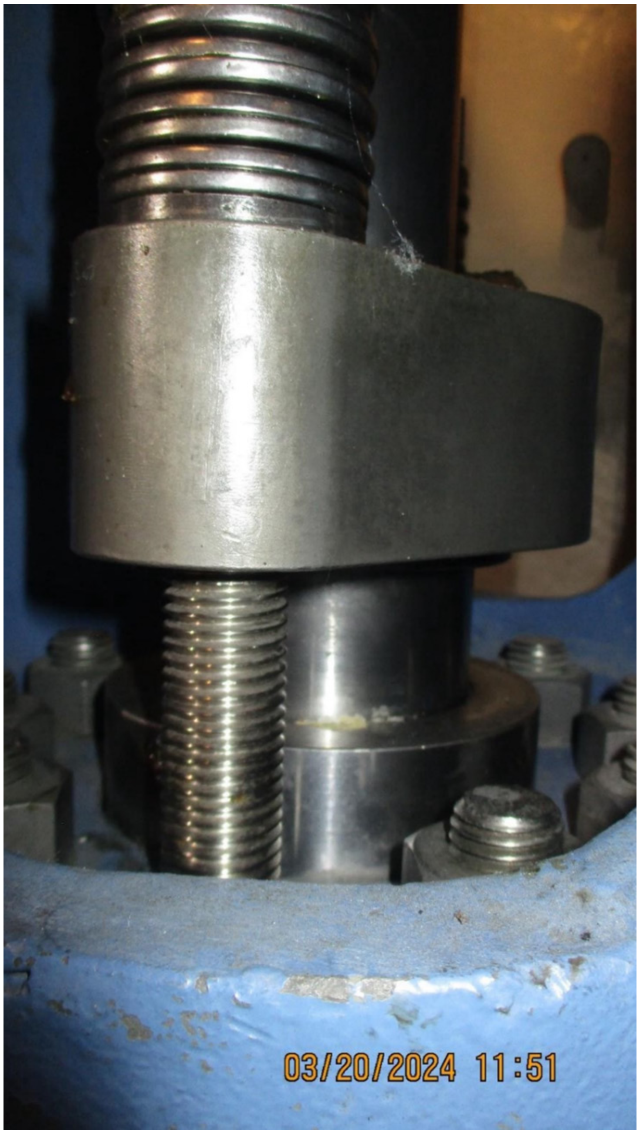
3. **INJ VLV X1**

Y is the Safety Injection Accumulator X1 Injection Valve. A dry boric acid accumulation was identified at the valve packing. The boric acid accumulation is present on the valve bonnet and the packing gland. The boric acid accumulation is < 1 tablespoon and contains some light discoloration. The boric acid accumulation is localized at the packing and has not migrated to any other components or structures. There was no evidence of degradation or wastage to the valve bonnet or the packing gland. These components are constructed of stainless steel which is resistant to BAC. Because the boric acid has not contacted any carbon steel material, the discoloration in the accumulation is the result of the boric acid contacting grease on the packing gland. The structural integrity of the component has not been affected. Work order X was created to clean the boric acid.



4. **INJ VLV X2**

Z is the Safety Injection Accumulator X 02 Injection Valve. A dry boric acid accumulation was identified at the valve packing. The boric acid accumulation is present on the valve bonnet and the packing gland. The boric acid accumulation is < 1 tablespoon and contains some light discoloration. The boric acid accumulation is localized at the packing and has not migrated to any other components or structures. There was no evidence of degradation or wastage to the valve bonnet or the packing gland. These components are constructed of stainless steel which is resistant to BAC. Because the boric acid has not contacted any carbon steel material, the discoloration in the accumulation is the result of the boric acid contacting grease on the packing gland. The structural integrity of the component has not been affected. Work order X was created to clean the boric acid.



5. X-Y TST LN ISOL VLV

X is the Safety Injection Accumulator Y Test Line Isolation Valve. A dry boric acid accumulation was identified at the packing. The boric acid accumulation is present on the valve bonnet, hold-down plates, packing gland, gland follower, and the follower studs. The boric acid accumulation is approximately 2 tablespoons and contains some light discoloration. The boric acid accumulation is localized at the packing and has not migrated to any other components. There was no evidence of degradation or wastage to the valve bonnet, hold-down plates, packing gland, gland follower, or the follower studs. These components are constructed of stainless steel which is resistant to BAC. Because the boric acid has not contacted any carbon steel material, the discoloration at the gland follower is the result of the boric acid contacting the delta ferrite which is present for forged components. The delta ferrite is usually present at the surface of cast components. The discoloration at the valve bonnet is the result of the boric acid contacting dirt/dust. The structural integrity of the component has not been affected. Work order X was created to clean the boric acid. Work Order Y was created to adjust the packing.

6. **Y-FT-X: REACTOR COOLANT LOOP Z FLOW TRANSMITTER X PROT CHAN II**

Y-FT-X is the Reactor Coolant Loop Z Flow Transmitter X Protection Channel II. Dry boric acid accumulations were identified at two locations associated with this flow transmitter. Both accumulations are located on the test fittings on the 3-way manifold. Both accumulations are dry and contain some discoloration. The boric acid accumulation is 3 tablespoons in total split between the two test fittings. The boric acid accumulation has migrated to the lower tubing support associated with Y-FT-X and finally on the floor below. The 3-way manifold, tubing and fittings are constructed of stainless steel which is resistant to BAC. The tubing supports and associated bolting are constructed of carbon steel and are susceptible to BAC. Based on EPRI's BAC Guidebook, the corrosion rate for dry boric acid crystals is 0.0005 in/year. The low corrosion rates and no evidence of wastage to tubing supports indicate that there is little risk of significant corrosion occurring due to the leakage. There was no evidence of degradation or wastage to any of the components. The structural integrity of the component has not been affected. Work order Z was generated to clean the boric acid accumulation and rework fittings.

Appendix B: Representative AI Tool Generated Boric Acid Corrosion Evaluation Content

Introduction

This appendix highlights the capabilities of the AI tool being piloted at the Reference Plant to aid in the development of document content generated by engineering authors as described in Section 6.4.4 in the body of this report. To provide a comparison between previously produced BAC evaluation content generated manually as captured in Appendix A, Section C, the AI tool was used to develop draft Boric Acid Corrosion (BAC) evaluation content of similar scope. The Reference Plant selected this content for two key reasons:

1. The significant number of historical evaluations that have been developed and validated by Reference Plant experts.
2. The broad applicability to the industry. Nearly all nuclear plants produce many of these evaluations (~50 per year).

As shown in the examples below, the AI tool is able to develop output content at a similar level of detail as presented in the examples in Appendix A, Section C, with the exception of adding the pictures and the corrective actions section at the bottom of those examples. This demonstrates how the AI tool can be used to save significant engineering time when authoring draft BAC report evaluation content by inputting relevant inputs as compared to manually performing all the research, analysis, and compilation necessary to create draft BAC evaluations from scratch.

As with Appendix A It is not intended that the reader objectively evaluate the information provided in this appendix for its specific technical validity as that would require a more comprehensive understanding of the Reference Plant's BAC prevention program.

Commentary is also provided with regard to the usability of the AI tool, accuracy of results, and suggestions to further advance AI tool deployment to enable WROs.

At the time of authoring this document, engineers are in the process of integrating this tool into their normal workflows for creating reports. While the general capabilities are known through the generation of "directionally correct" draft results, estimating the near- and long-term benefits realized will be quantified and discussed in future research. Additionally, there are no planned changes in existing review procedures and protocols by the Reference Plant. The intention of the AI tool is instructed to be used as a tool to support existing processes and protocols.

Example Report Content

Individual BAC evaluations for valves similar to those in Appendix A, Section C were selected to be examples for use of the AI Tool discussed in Section 6.4. For each valve, the inputs provided to the tool and the resulting outputs are provided below.

C Evaluation

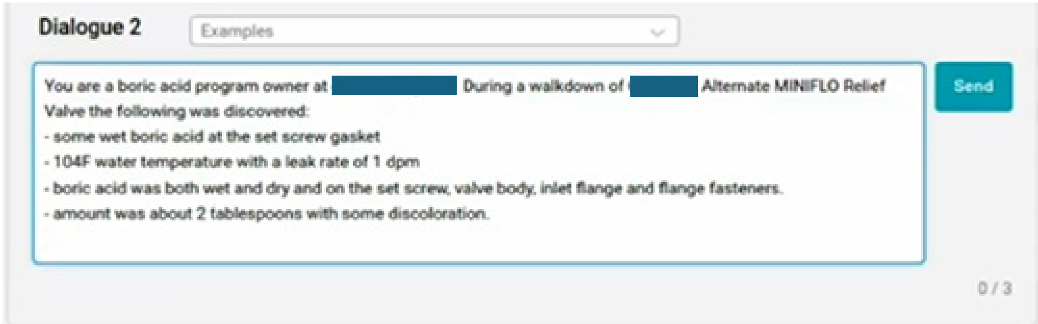
1. CCP 1-02 Alternate MINIFLO Relief Valve

Input provided to AI tool

The author entered the following content into the AI tool:

> You are a boric acid program owner at the reference plant. During a walkdown of CCP-X-## alternative MINFLO Relief valve the following was discovered:
>
> - Some wet boric acid at the set screw gasket
> - 104F water temperature with a leak rate of 1 dpm
> - Boric acid was both wet and dry and on the set screw, valve body, inlet flange and flange fasteners
> - Amount was about 2 tablespoons with some discoloration

For ease of use, below is an example picture of AI Tool input:



Output provided by AI tool

The following is a recommendation for the disposition of the boric acid leakage.

The boric acid accumulation is present on the set screw gasket, valve body, inlet flange and flange fasteners. The boric acid accumulation is approximately 2 tablespoons and contains discoloration. The boric acid accumulation is localized at the set screw gasket and has not migrated to any other components.

The discoloration in the accumulation is the result of the boric acid contacting the carbon steel valve body and flange fasteners. There was no evidence of degradation or wastage to the set screw gasket, valve body, or the inlet flange. These components are constructed of stainless steel which is resistant to boric acid corrosion. The structural integrity of the components has not been affected.

The flange fasteners are constructed of carbon steel which is susceptible to boric acid corrosion. However, there was no evidence of degradation or wastage to the flange fasteners. The flange fasteners are coated to protect against contact with boric acid. The discoloration in the accumulation is the result of the boric acid contacting the carbon steel flange fasteners.

The source of the leakage can positively be identified, the leak site is not obstructed, and the leaking component and/or surrounding components and surfaces are not affected. The EPRI Boric Acid Corrosion guidebook indicates that tests conducted (for carbon steel, low alloy steels and martensitic stainless steels) when exposed to boric acid crystals exhibited very low corrosion rates. The highest rate observed on any of the alloys was 0.00005 inches per year. Because there was no evidence of degradation or wastage to the flange fasteners, their structural integrity has not been affected.

Work order XXXX was generated to clean the boric acid accumulation and adjust the set screw gasket.

For ease of use, below is an example picture of AI Tool output:

The following is a recommendation for the disposition of the boric acid leakage.

The boric acid accumulation is present on the set screw gasket, valve body, inlet flange, and flange fasteners. The boric acid accumulation is approximately 2 tablespoons and contains discoloration. The boric acid accumulation is localized at the set screw gasket and has not migrated to any other components.

The discoloration in the accumulation is the result of the boric acid contacting the carbon steel valve body and flange fasteners. There was no evidence of degradation or wastage to the set screw gasket, valve body, or the inlet flange. These components are constructed of stainless steel which is resistant to boric acid corrosion. The structural integrity of the components has not been affected.

The flange fasteners are constructed of carbon steel which is susceptible to boric acid corrosion. However, there was no evidence of degradation or wastage to the flange fasteners. The flange fasteners are coated to protect against contact with boric acid. The discoloration in the accumulation is the result of the boric acid contacting the carbon steel flange fasteners.

The source of the leakage can positively be identified, the leak site is not obstructed, and the leaking component and/or surrounding components and surfaces are not affected. The EPRI Boric Acid Corrosion Guidebook indicates that tests conducted (for carbon steel, low alloy steels and martensitic stainless steels) when exposed to boric acid crystals, exhibited very low corrosion rates. The highest rate observed on any of the alloys was 0.0005 inches per year. Because there was no evidence of degradation or wastage to the flange fasteners, their structural integrity has not been affected.

Work order [redacted] was generated to clean the boric acid accumulation and adjust the set screw gasket.

Commentary with regard to the AI output:

The AI tool was helpful to identify the reference to the EPRI Boric Acid Corrosion guidebook. Additionally, the suggestion that the flange fasteners may be coated to protect against contact with boric acid was helpful.

There are several items identified by AI tool output that provide directionally correct information which would be expected to prompt the evaluation author to consider specific conditions associated with boric acid corrosion for the particular subject valve. These include:

1. The specific locations and amount of boron that is present at the leak site
2. The color of the boron present (which can indicate corrosion has occurred).
3. The presence of dissimilar metals on the valve, where only some of which are susceptible to this corrosion.
4. The possibility that the valve flange bolts may be coated to protect them against boric acid corrosion.
5. The need to inspect for gasket condition and leakage (not only for the set screw gasket, but also other gaskets (e.g. valve flange gaskets)
6. The need to ensure that all surfaces of the subject valve are inspected, particularly if the direct view of some surfaces is obstructed.
7. Reference to a work order to for a similar leak on what appears to be the subject valve or one similar to it.

These would be expected to prompt the evaluation author to perform more research to determine the specific materials that make up the subject valve and to include inspections to address these items in the evaluation text.

The AI result also references validation of the highest concentration rate, which appears to come from the EPRI guidebook. This would be expected to prompt the evaluation author to establish the highest boron concentration rate experienced during the leakage event which could impact corrosion rates.

The AI output also provides specific outputs which cannot be directly related to the inputs. For example, the AI output states, "The discoloration in the accumulation is the result of the boric acid contacting the carbon steel valve body and flange fasteners." This output is likely inferred from past evaluations through the AI tool database. The input does not state that the valve has a carbon steel valve body or carbon steel flange fasteners. Inferences such as these need to be validated by the BAC evaluation report author.

Assuming the input information provided to the AI tool was collected by a person knowledgeable of the data that needs to be collected for a boric acid leak, the author of the evaluation should question why the fluid temperature provided did not result in any AI output that references it. If this data point should impact the AI output, the report author and/or reviewer needs to identify this issue, capture it in the final BAC evaluation report. Feeding this finished report into the AI tool database will increase the likelihood that the AI tool will identify leak temperature considerations going forward.

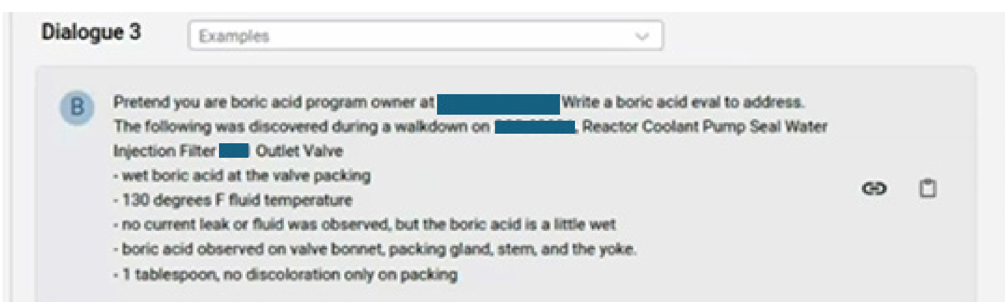
2. Reactor Coolant Pump Seal Water Injection Filter XX Outlet Valve YY

Input provided to AI tool

The engineer entered the following content into the AI tool:

> Pretend you are boric acid program owner at reference plant. Write a boric acid eval to address. The following was discovered during a walkdown on YY, Reactor Coolant Pump Seal Water Injection Filter XX Outlet Valve
>
> - Wet boric acid at the valve packing
> - 130 degrees F fluid temperature
> - No current leak or fluid was observed but the boric acid is a little wet
> - Boric acid observed on valve bonnet, packing gland stem, and the yoke.
> - 1 tablespoon, no discoloration only on packing
> - For ease of use, below is an example picture of AI Tool input:

For ease of use, below is an example picture of AI Tool input:



Output provided by the AI Tool

The following was discovered during a walkdown on XXXX Reactor Coolant Pump Seal Water Injection Filter YY Outlet Valve

- Wet boric acid at the valve packing

- 130 degrees F fluid temperature
- No current leak or fluid was observed but the boric acid is a little wet
- Boric acid observed on valve bonnet, packing gland stem, and the yoke.
- 1 tablespoon, no discoloration only on packing

Boric Acid Evaluation

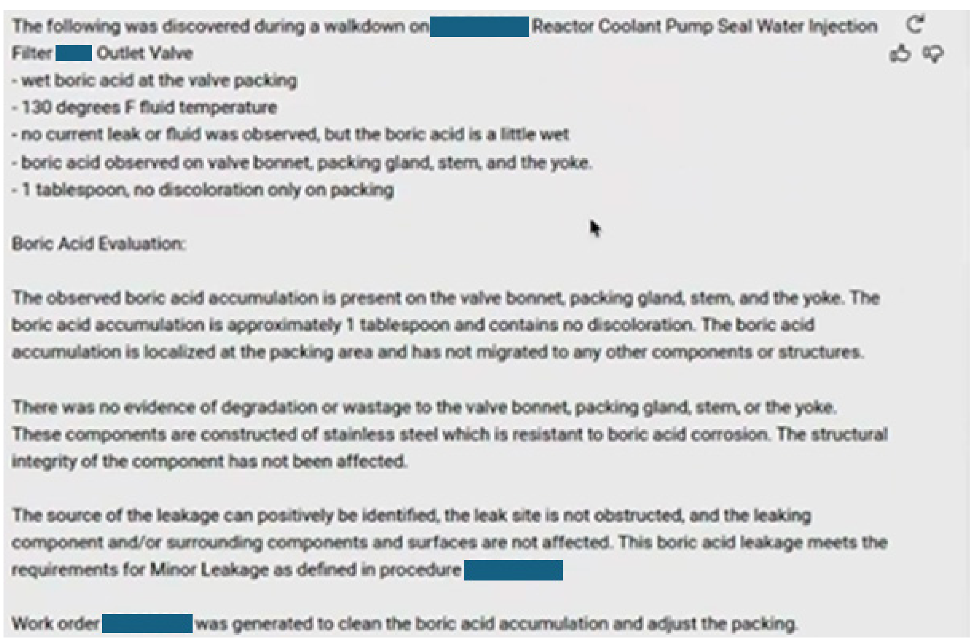
The observed boric acid accumulation is present on the valve bonnet, packing gland stem, and the yoke. The boric acid accumulation is approximately 1 table spoon and contains no discoloration. The boric acid accumulation is localized at the packing area and has not migrated to any other components or structures.

There was no evidence of degradation or wastage to the valve bonnet, packing gland stem, or the yoke. These components are constructed of stainless steel which is resistant to boric acid corrosion. The structural integrity of the component has not been affected.

The source of the leakage can positively be identified, the leak site is not obstructed, and the leaking component and/or surrounding components and surfaces are not affected. The boric acid leakage meets the requirements for Minor Leakage as identified in procedure STI-ZZZ

Work order ZZZZ was generated to clean the boric acid accumulation and adjust the packing.

For ease of use, below is an example picture of AI Tool output:



The following was discovered during a walkdown on [redacted] Reactor Coolant Pump Seal Water Injection Filter [redacted] Outlet Valve
- wet boric acid at the valve packing
- 130 degrees F fluid temperature
- no current leak or fluid was observed, but the boric acid is a little wet
- boric acid observed on valve bonnet, packing gland, stem, and the yoke.
- 1 tablespoon, no discoloration only on packing

Boric Acid Evaluation:

The observed boric acid accumulation is present on the valve bonnet, packing gland, stem, and the yoke. The boric acid accumulation is approximately 1 tablespoon and contains no discoloration. The boric acid accumulation is localized at the packing area and has not migrated to any other components or structures.

There was no evidence of degradation or wastage to the valve bonnet, packing gland, stem, or the yoke. These components are constructed of stainless steel which is resistant to boric acid corrosion. The structural integrity of the component has not been affected.

The source of the leakage can positively be identified, the leak site is not obstructed, and the leaking component and/or surrounding components and surfaces are not affected. This boric acid leakage meets the requirements for Minor Leakage as defined in procedure [redacted]

Work order [redacted] was generated to clean the boric acid accumulation and adjust the packing.

Commentary with regard to the AI output:

Again, there are several areas identified by AI tool output that provide directionally correct information which would be expected to prompt the evaluation author to consider specific conditions associated with boric acid corrosion for the particular subject valve. These include:

1. Similar topics to those previously identified in the first example above.
2. Identification of reference plant approved guidance associated with an active boron leak (which is unique to this example).
3. The need to not only inspect the component leaking boric acid for deposits and related corrosion, but also to inspect the wider vicinity for the same.

These would be expected to prompt the evaluation author to do more research to similarly address issues this example shares the previous one. The author would also be expected to take actions to address the procedural requirements for an active boric acid leak.

As with the first example, there was also no output information provided for the input temperature at the leak location. Expected action to address this is the same as for the first example.

Another operational feature observation when using the tool was observed. The AI tool relates keywords and phrases within the context they are used to identify patterns that are then leveraged to produce outputs that relate to the inputs. While the AI tool user should endeavor to be diligent in providing error free, quality inputs (e.g. grammatically correct sentences with proper spelling), notice the AI tool still produced useful results in spite of the following:

1. A grammatical error of missing "a" in the statement "Pretend you are **a** boric…"
2. Using the shorthand ("eval") instead of correct word (evaluation)
3. Use of poor syntax, such as: "Pretend you are boric acid program owner at reference plant. Write a boric acid eval to address.").
    a. "Pretend" is irrelevant.
    b. "Write a boric acid eval to address" is an incomplete thought which does not identify that a boric acid leak needs to be addressed.

The degree to which such input errors impact the output quality have not yet been evaluated.

General commentary and conclusions.

Overall, a general questioning attitude is necessary when reviewing AI tool outputs based upon the specific inputs it is provided. This questioning attitude must be informed by AI tool users possessing a clear understanding of the initial content and accuracy of the AI tool training dataset and its evolution over time. This evolution will likely include be driven by adding additional baseline plant information along with feeding completed reports which have been validated to be accurate and complete.

As it relates to the examples provided above, application of a questioning attitude identified several areas that warrant further examination as provided below:

1. The outputs provided by the AI in several cases are not by themselves directly relatable to the inputs. One example is that the inputs to example 1 above say nothing about the protective coatings being applied to the flange fasteners. The particular valve fasteners may have this coating based upon other general input data used to train the AI tool. When occasions where "unsolicited information" is provided, the expectation is that the BAC evaluation author will validate that such outputs are correct and relevant for the particular component or components within the scope of the BAC evaluation. There are other instances of this in the examples above.

2. The outputs are also written in a way that appear to state “facts” which could be misinterpreted by the author using the AI tool. For example, the outputs of both examples state, “The source of the leakage can positively be identified, the leak site **is not obstructed** (emphasis added), and the leaking component and/or surrounding components and surfaces **are not affected** (emphasis added).” Again, this may be true based upon specific information within the AI tool database for the particular valves, but it must be validated by the BAC evaluation report author. This could be addressed by the AI tool identifying the source document for such statements as identified above.
3. The inputs for both the first and second example identified active boric acid leaks and provided the temperature measured at the leak location. Only the output of the second example identified applicability of the reference plant approved guidance associated with an active boron leak. Neither output provided any information associated with the temperature that was noted as part of the input information as relevant. It is expected that temperature is measured because this can affect the corrosion rate at the leak location. Questions should be asked when input information produces no related output information. Personnel with previous experience in manually authoring BAC evaluations are likely to catch such discrepancies and omissions between reports as suggested here. Individuals with less experience will be more reliant on training to identify such issues.
4. It has already been recognized that specific guidance and training needs to be developed and provided to individuals who generate input information for the AI tool. Based upon review of the examples provided here, several suggestions for consideration are offered. Inputs need to focus on importance, relevance, and technical accuracy. Identification of such key input data for different report types to be supported by the AI tool and use of a controlled set of standard words, structured phrases, and acronyms to capture inputs will enable AI tool to produce higher quality outputs. Having an enveloping list of typical inputs and expected related output characteristics for AI generated report content may also help authors and reviewers to best assess the validity of AI generated results.

   The LLM being used for this pilot has demonstrated its ability to produce relevant output based upon administratively challenged inputs. While this is helpful, personnel using the AI tool need to be trained to provide administrative error free input information to produce consistent and higher quality outputs. Methods to minimize such input errors (e.g. use of English language tools provided in software programs such as Microsoft Word) should also be employed.