INL/EXT-19-55799

Light Water Reactor Sustainability Program

Addressing Nuclear I&C Modernization Through Application of Techniques Employed in Other Industries

September 2019

U.S. Department of Energy

Office of Nuclear Energy

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/EXT-19-55799

Addressing Nuclear I&C Modernization Through Application of Techniques Employed in Other Industries

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

September 2019

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

SUMMARY

Rapid advancements in industrial Instrumentation and Control (I&C) technology, the development of innovative deployment techniques, as well as the creation of lifecycle support strategies for sustainment have been revolutionary. They have enabled significant facility operating and maintenance (O&M) cost reductions in non-nuclear applications. Obsolescence management has also been fully incorporated within the lifecycle of these digital I&C systems by leveraging business Information Technologies (IT) and techniques to sustain it within an industrial I&C, Operational Technology (OT), environment. This has allowed non-nuclear industries to leverage the features of digital technology, while bounding obsolescence risks and costs in order to provide cost reliability and predictability.

I&C systems in commercial nuclear power plants in the United States have historically been developed, implemented, and sustained by traditional nuclear industry supply chain vendors. When performing sustaining activities (repair and replacement), operating units follow the same project management, engineering management, and design processes used to sustain I&C systems as those used by other systems in the plant (i.e., fluid, mechanical, electrical). This has created an institutional inertia within the nuclear industry I&C community that has constrained efficient application of non-nuclear OT in a way that hinders nuclear from realizing the benefits of these technologies as demonstrated in non-nuclear applications. Additionally, this has created an obsolescence issue as plants have avoided wholesale changeouts of legacy systems in favor of like-for-like repair or replacement on an as-needed basis.

This research focuses on presenting advancements that have been made by non-nuclear I&C vendors and potential savings that could be realized by their optimized nuclear industry application. To promote understanding and to bound the initial scope for this effort, a pilot vendor and an associated pilot implementation were chosen as an integrated presentation example for illustration. The pilot implementation at Duke Energy installed a non-safety, Distributed Control System (DCS) in four of its nuclear units. This utility is exploring performing a technology upgrade of these installed systems as part of a program to address digital obsolescence. This research presents techniques developed by vendors to enable such an upgrade and potential methods to employ them in a nuclear industry context. The objectives of such an effort are to minimize the utility cost both to upgrade the systems and to put the systems into a repeatable upgrade cycle for future obsolescence management. This will enable the utility to maximize the benefits of expanded use of their DCS as part of a larger plant strategy to eliminate obsolete I&C systems, reduce O&M costs, and improve operational performance through digitalization. This document does not provide an endorsement of any vendor or their specific technology. INL appreciates the participation of Duke Energy and Honeywell Process Solutions (HPS) in this research effort.

CONTENTS

FIGURES

TABLES

ACRONYMS

CCF	Common Cause Failure
CDA	Critical Digital Asset
DCS	Distributed Control System
EC	Engineering Change
EPKS	Experion® Process Knowledge System
EPRI	Electric Power Research Institute
FAT	Factory Acceptance Test
FMEA	Failure Modes and Effects Analysis
HFE	Human Factors Engineering
HMI	Human Machine Interface
HPS	Honeywell Process Solutions
I&C	Instrumentation and Control
IT	Information Technology
LAR	License Amendment Request
LCM	Lifecycle Management (Honeywell)
LWRS	Light Water Reactor Sustainability (Program)
MCR	Main Control Room
NEI	Nuclear Energy Institute
NRC	Nuclear Regulatory Commission (United States)
O&M	Operating and Maintenance
OT	Operations Technology
QA	Quality Assurance
QC	Quality Control
QMS	Quality Management System
SDOE	Secure Development and Operating Environment
SHA	Software Hazard Analysis
SME	Subject Matter Expert
TCS	Turbine Control System
UFSAR	Updated Final Safety Analysis Report
VDU	Video Display Unit
VM	Virtual Machine

ADDRESSING NUCLEAR I&C MODERNIZATION THROUGH APPLICATION OF TECHNIQUES EMPLOYED IN OTHER INDUSTRIES

1. Introduction

1.1 Research Overview and Objectives

This research focuses on presenting advancements that have been made by non-nuclear Instrumentation and Control (I&C) Operations Technology (OT) vendors and savings that could be realized by their optimized application in the nuclear industry. Using this technology for non-safety applications within nuclear is consistent with 10 CFR 50, Appendix A, General Design Criterion 1. Application of these advancements in nuclear with minimal adaptation promotes modernization of a significant portion of the target plants. Application of these techniques to nuclear plant Distributed Control System (DCS) implementations represents a target that would provide the maximum aggregate impact to improve plant operational and cost performance. This directly aligns with the objectives of the Department of Energy Light Water Reactor Sustainability (LWRS) Program.

Research objectives are to identify techniques to leverage established vendor processes and experience to the maximum extent practicable to minimize utility cost to deploy and periodically upgrade I&C systems via a repeatable obsolescence management cycle. This will enable the utility to maximize the benefits of expanded use of DCSs as part of a larger plant strategy to eliminate obsolete I&C systems, reduce Operating and Maintenance (O&M) costs, improve operational performance, and maximize personnel utilization through digitalization.

1.2 Research Premise

Rapid advancements in digital I&C technology, development of innovative deployment techniques, and implementation of lifecycle support strategies to sustain it have been revolutionary. Significant facility operating and I&C maintenance cost reductions in non-nuclear applications have been achieved worldwide. Obsolescence management has been fully incorporated into the digital I&C system lifecycle by leveraging Information Technology (IT) methodologies to sustain these systems within an industrial I&C environment. This has allowed non-nuclear industries to improve process performance, reduce manpower, bound digital technology obsolescence costs and risks, as well as to provide cost reliability and predictability.

1.3 Problem Definition

Current non-safety light water reactor I&C systems in the United States vary widely in age, complexity, and technology used (analog/digital). These systems have historically been developed, implemented, and sustained by traditional nuclear industry supply chain vendors. When performing I&C system sustaining activities (repair and replacement [including upgrades to digital technology]), operating units follow the same project management, engineering management, and design processes used for similar activities for other systems in the plant (i.e., fluid, mechanical, electrical).

The traditional, linear, nuclear Engineering Change (EC) process has evolved over time to address issues associated with digital I&C modernization. The rate of evolution, however, has not addressed the revolutionary nature of digital I&C technology changes. I&C system vendor processes to specify, design, implement, factory test, deploy, and validate digital system functionality are now more robust and application/industry specific. When deploying a digital I&C platform (e.g., a DCS), applying traditional utility EC processes tends to repeat, at significant cost, the exhaustive vendor platform design/implementation program.

Once installed, sustaining activities for nuclear plant digital I&C systems have largely been limited to maintaining the existing system equipment for as long as possible. When this can no longer be sustained by activities such as parts hoarding and reverse engineering, the technology in use is so obsolete that harvesting its initial intellectual property investment is difficult. In many cases, the obsolete digital system must be completely re-engineered at high cost. Again, modern digital I&C system vendors have created extended lifecycle support mechanisms that have eclipsed traditional nuclear change processes in obsolescence management. Application of these mechanisms, which retain legacy system performance, provide new functionality, and increase system robustness and reliability, does not fit the traditional EC process.

The result of these disparities is an institutional inertia within the nuclear industry I&C community that constrains efficient application of non-nuclear OT. Reliance on legacy processes has contributed to high initial costs for digital I&C modernization. Obsolescence issues that drive cost are twofold: First, plants have avoided digital modernization, due to the perceived high cost/risk in initial deployment. Second, when digital modernization has occurred in the past, these systems have been run well beyond end-of useful-life, due to the lack of a repeatable lifecycle sustaining process that bounds risk and provides cost reliability and predictability. This, combined with efforts required to recover intellectual property from legacy obsolete systems, has significantly increased the cost of digital I&C replacements.

2. Scope

To promote understanding and to bound the initial research scope for this effort, a pilot DCS vendor and an associated pilot implementation were chosen as an integrated presentation example for illustration. This integrated example is unique in that the pilot utility (Duke Energy) engaged a traditional non-nuclear I&C pilot vendor (Honeywell Process Solutions [HPS]) to install a non-safety DCS in four of its nuclear units. The pilot utility is currently exploring a technology migration from the version offered by the pilot vendor when selected in 2012, to the latest version as part of a program to address digital obsolescence. This research generically presents techniques developed by the pilot vendor to enable such an upgrade and potential methods to employ those techniques in a nuclear industry context. The objectives of such an effort are to minimize the utility cost, both to perform the technology migration and to put the DCSs into a repeatable upgrade cycle for future obsolescence management. This will enable the utility to maximize the benefits of expanded use of their DCS as part of a larger plant strategy to eliminate obsolete I&C systems, reduce O&M costs, and improve operational performance through digitalization.

This research first summarizes the pilot utility's experience in deploying the pilot vendor's Honeywell Experion® DCS. This establishes the basis for the modernization effort as well as providing lessons learned and areas of improvement that are applicable to this research. Vendor-developed methods to address obsolescence management are then generically presented to demonstrate potential methods to bound digital technology obsolescence risks and costs, as well as to provide cost reliability and predictability.

This document does not provide an endorsement of any vendor or their specific technology. This research leverages the pilot utility's experience and the vendor product selected by them to provide a specific example of how any established non-nuclear I&C vendor's technology and processes can be leveraged to enable and sustain nuclear I&C modernization. INL appreciates the participation of Duke Energy and HPS in this research effort.

3. Pilot Distributed Process Control System Initial Development and Installation

This section draws from the content of the American Nuclear Society paper 26064, "Fleet Digital Upgrade Program and Control Room Modernization." [1]

3.1 Production DCS Development and Installation

3.1.1 End State Vision and Strategy

Duke Energy launched a strategic fleet initiative to upgrade digital I&C systems at four of its nuclear units. The initial scope of this initiative was limited to non-safety I&C systems. To achieve initiative objectives, Duke established an "idealized end state" of a full plant I&C digital modernization with a fully upgraded control room. Properties of that end state vision include:

a) A standard, overarching technical solution. Attributes of this solution include:
   1. Selection and use of a fully developed, vendor-supported DCS solution with a fully developed strategy for future technology upgrades.
   2. Willingness of the vendor to support knowledge transfer to the utility.
   3. Migration of functions of legacy I&C systems to the new DCS and retirement of the legacy equipment.
   4. An enhanced performance profile through the application of advanced features such as system diagnostics, fault tolerance, graceful degradation, improved Human Machine Interfaces (HMI), etc.
   5. Full integration of the technical solution within the simulators of the impacted nuclear units. This is a technology multiplier that allows for many new capabilities.

b) A standard DCS cyber security strategy and defensive architecture.

c) Utility standard procedures and processes to develop standard design products. By designing once and building many, both initial costs and lifecycle costs are minimized.

d) A defined strategy to address concerns with digital systems, particularly Common Cause Failure (CCF). This strategy needs to address U. S. Nuclear Regulatory Commission (NRC) licensing requirements for making plant changes per 10 CFR 50.59, "Changes, Tests, and Experiments." [2]

e) A standard Human Factors Engineering (HFE) strategy that applies a graded approach to address elements identified in NUREG-0711, "Human Factors Engineering Program Review Model." [3] Authorization and implementation of the projects at the utility level.

3.1.2 Vendor Selection and Audit

Duke Energy selected Honeywell Process Control Solutions as the vendor to provide non-safety related DCS equipment, software, and engineering services. Key reasons for making this selection included:

a) The technical properties of the Honeywell Experion® Process Knowledge System (EPKS)

b) The large installed base of Experion® in industry

c) The ability of the utility to directly interact with the vendor without an intermediary

d) The backward compatibility of Experion® to incorporate legacy devices as far back as the 1970s/1980s without modification

e) The well-established technology migration process developed by the vendor and its use of virtual machines (VM) to protect/leverage initial intellectual property investments

f) The vendor's ability to engage with separate simulator vendors to integrate the DCS into the plant simulators.

g) The willingness of the vendor to team with Duke Energy to define, configure, test, and deploy the DCS, including making adaptations to support satisfying cybersecurity requirements (10 CFR 73.54 [4]).

Vendor quality assurance (QA) and quality control (QC) practices ensure base vendor platform properties are reliably provided. These products are tested individually and as part of holistic system operation. These practices were audited at a vendor site by the utility as captured in the Honeywell Quality Assurance/Quality Control (QA/QC) Assessment Report, [5]. Further explanation of how the vendor DCS product met the intent of industry codes and standards as identified by contract was provided as part of the Software Hazard Analysis (SHA) [6] described in Section 3.1.5. These activities demonstrated the selected platform addressed 10 CFR 50, Appendix A, General Design Criterion 1.

3.1.3 Configuration and Implementation of the DCS

Instead of following a traditional waterfall development process, Duke Energy chose to employ the Agile process for development of the standard DCS design. A pictorial comparison of the two processes is shown in Figure 1 below.

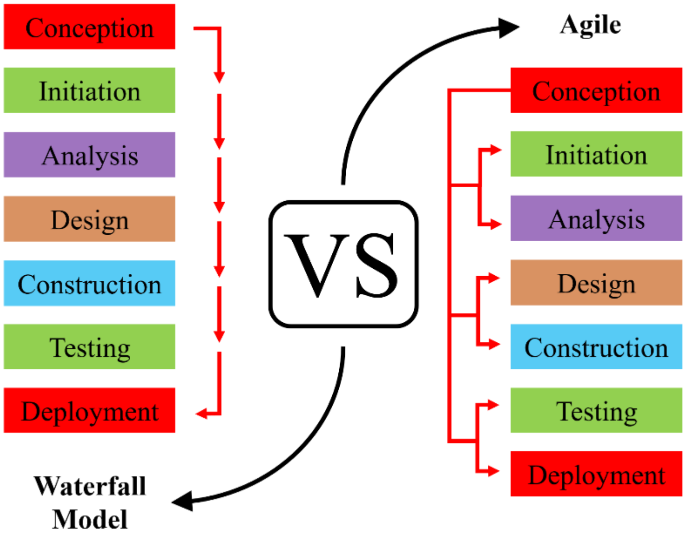


Figure 1. Agile Development Process Compared to a Traditional Waterfall Process.

While both processes share the same major steps, disadvantages of the waterfall process are that it is linear and that it assumes that system engineers fully understand the system requirements from the start. Another disadvantage is that such system requirements are envisioned as “free standing,” and that systems built to satisfy them are created from scratch or modified to conform to them. The Agile process is more iterative and flexible than the waterfall process. It is also more adept in accepting attributes of a mature product as a design input to meet the need.

A key feature of the Agile process as employed was that a full fleet laboratory system was purchased early in the design, based upon preliminary requirements and an understanding of the attributes of the selected vendor platform. The purpose of this was to understand and adapt the selected vendor’s platform properties, in order to be able to conform them to meet identified plant needs. This understanding is necessary because platform properties 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.

Duke Energy and vendor engineers performed an initial system configuration and test on this fleet laboratory system in a Secure Development and Operating Environment (SDOE). The process was then iterated multiple times and employed the SCRUM methodology of the Agile process (including multiple "sprints"). These sprints addressed the entire breadth of the DCS architecture as well as integrated DCS configuration and operation all at once. Lessons learned through each sprint were fed back into the appropriate design areas/design documentation identified in Figure 1. Not only did this facilitate development of final DCS design specifications, this activity was the primary vehicle for knowledge transfer from the DCS vendor to the utility.

Standard base system configuration work instructions, software templates, and application work instructions were developed and applied to produce the final production system architecture. The resultant DCS Architecture was then verified to satisfy the requirements through a combination of activities shown in Figure 2. Relationships to the Honeywell QA/QC Assessment Report [5], the SHA [6], and the Hardware Failure Modes and Effects Analysis (FMEA) [7] as described in Section 3.1.5 are also conceptually shown in Figure 2 to depict how they integrate into DCS design and implementation activities.

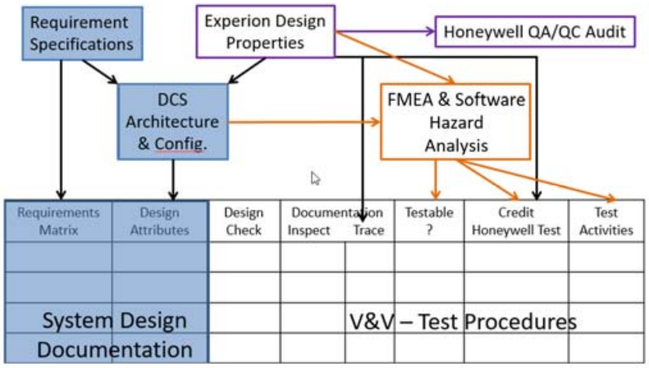


Figure 2. DCS Design, Implementation, and Test Activities.

Standardization of the design and test process provided a "design once, build many" path for production system purchase, configuration, testing, and deployment.

3.1.4 Cyber Security

NRC endorsed the methodology contained in Nuclear Energy Institute (NEI) 08-09 Revision 6, "Cyber Security Plan for Nuclear Reactors," [8] as acceptable for use in meeting the requirements set forth in 10 CFR 73.54, "Protection of Digital Computer and Communications Systems and Networks." [4] The standard DCS design used the technical controls (Appendix D) and administrative controls (Appendix E) of NEI 08-09 as a design input. Each technical control, as well as each administrative control that presupposed a technical capability (e.g., device log recording is an administrative control but requires a technical solution to perform it) was evaluated and addressed as part of the design.

The Experion® PKS system possesses certain attributes that could be leveraged to address NEI 08-09 controls. It was lacking in others. Duke Energy collaborated with the vendor to develop and deploy a suite of cybersecurity tools on the standard DCS that filled these gaps without negatively impacting DCS performance. Duke Energy personnel worked hand-in-hand with Honeywell to configure these tools and to become the subject matter experts (SMEs) on installing, configuring, and maintaining them.

Standard cybersecurity assessments were also produced for the standard DCS, in accordance with fleet procedures. The entire system was decomposed into only five "types" of critical digital assets (CDAs) that share a substantially similar security posture. Each type was then assessed as permitted by NEI 13-10 Revision 4, "Cyber Security Control Assessments." [9] This extended the concept of "design once, build many" into the realm of cybersecurity to minimize initial development and lifecycle support costs.

3.1.5 Addressing System Failure Concerns

When implementing any nuclear plant control system change, particularly one with such far-reaching potential impacts as one that migrates multiple separate plant control functions onto a DCS, attention needs to be focused on addressing system failure concerns. Two comprehensive system analyses were performed to address these concerns. These included (1) a hardware FMEA and single-failure analysis for the DCS hardware, and (2) a DCS SHA.

The hardware FMEA evaluates the DCS's vulnerability to postulated single-component failures, to determine if such failures could cause the loss of the DCS during normal plant operating conditions. The FMEA does not consider multiple independent failures as being credible conditions.

The DCS SHA documents that Experion® PKS (EPKS) was developed in accordance with industry recognized codes and standards appropriate for non-safety-related monitoring and control system applications. EPKS software development (as well as integration of commercially available products into it) occurred using industry-recognized codes, standards, and lifecycle management (LCM) methods. When properly configured in accordance with extensively tested and documented Honeywell best practices, EPKS will perform in a manner where there is reasonable assurance that the likelihood of failure due to software is sufficiently low. These best practices have been incorporated into the DCS requirements documents and design. Software delivered as part of the DCS can be expected to perform dependably.

Topics addressed in the SHA include:

a) DCS SHA Analysis Criteria and Initial Conditions
b) DCS Development, Lifecycle Support and Quality
c) A generic presentation of DCS control hierarchy and communications priority. This forms a basis for the understanding of how the DCS performs process control and supports the more detailed discussions provided later in the document.
d) Multiple sections and an appendix present how postulated CCFs are addressed in the DCS design, using the system architecture and the Purdue Model as framework

Plant I&C applications moved from obsolete I&C equipment to the DCS are constrained to operate in an environment bounded by the target plant's design and licensing basis (unless a License Amendment Request [LAR] is to be pursued). To address this, the SHA also describes techniques needed to accomplish application migrations as part of a holistic strategy. This is further developed in Section 3.1.6 below.

3.1.6 Leveraging Vendor DCS Design Properties and Application Implementation Strategy (Licensing Strategy)

In order to properly apply vendor DCS technology for a non-safety implementation in a nuclear plant, several interrelated topics were required to be addressed. These are show pictorially in Figure 3 and include:

a) The intrinsic properties of the particular vendor's technology
b) Utility DCS requirements and how these are combined with the vendor's technology into DCS architecture attributes
c) Establishing rules for how legacy I&C functionality is moved to the DCS to address the particular plant's licensing basis
d) Application of those rules when moving functions described in the impacted units Updated Final Safety Analysis Report (UFSAR).

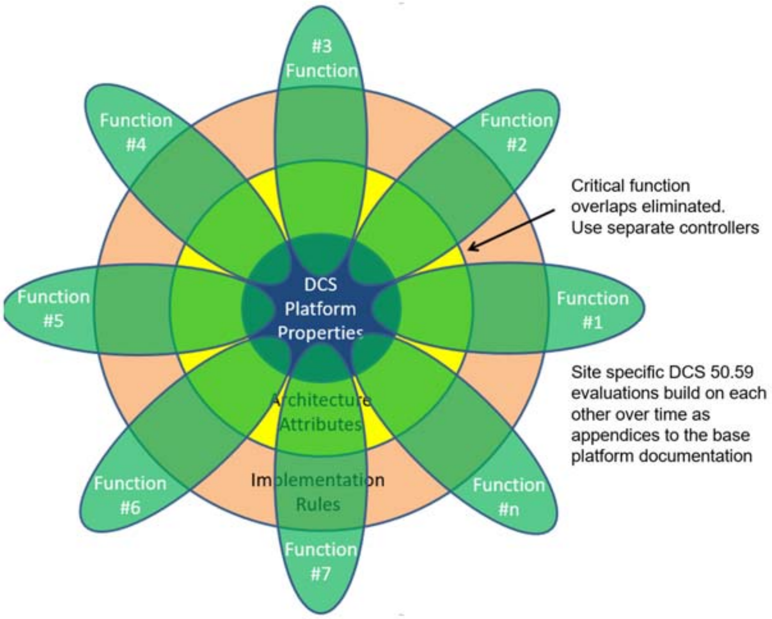


Figure 3. DCS Design Property Utilization and Application Implementation Strategy.

EPKS platform properties provide the core upon which the Duke Energy DCS is built. EPKS platform properties exist through product development by Honeywell independent of the particular use envisioned by a customer. Section 3.1.3 above outlines how Duke Energy collaborated with Honeywell to ensure necessary architecture attributes (e.g., redundancy and configurations to support failover, etc.) were identified, documented, and implemented as part of the design through system configuration.

The SHA also established implementation rules for applications hosted by the DCS. Duke Energy chose as a foundational tenet to conform application implementation on the DCS to maintain the functional segmentation as captured in a nuclear unit's UFSAR. These are depicted as green "petals" in Figure 3. This prevents a failure impacting one separate function described in the UFSAR from impacting another separate function. This approach leveraged concepts captured in the Watts Bar Unit 2 DCS Segmentation Analysis [10] as accepted by the NRC in the associated Safety Evaluation Report [11].

Plant application software development implemented on the DCS is beyond the scope of the SHA. Application software errors are a result of human error. Many are detected in the development phase of particular application's implementation project. DCS application software is subject to testing to ensure validity and conformance to specifications. Application software is also subjected to validation during the application Factory Acceptance Test (FAT). Site Acceptance Testing and Post-Modification Testing then follow, occurring after installation onsite. These multiple testing levels are designed to detect application software problems and provide opportunities to correct them.

DCS design tools and processes cannot eliminate the possibility of an application software defect in a controller. If a defect is triggered and the integrity of the software is compromised, this will fault the affected software module. This will fail the associated controller, and the backup controller takes over. If the same software error is present in the backup, it may also fail. Proper system design of the I/O output modules will then place their outputs in a pre-programmed safe state. This potential outcome is addressed by DCS function segmentation rules.

3.1.7 Lessons Learned / Potential Areas of Improvement

The effort described in the subsections above required innovative thinking and adaptation of processes (e.g., Agile and SCRUM) to traditional methods to implement an EC in a nuclear plant. Many other decisions had to be made to advance the project. Reflection on this activity after its completion identified several lessons learned and potential areas of improvement. Several of these are presented below and are indented and *italicized*.

3.1.7.1 Systems Procured and Knowledge Transfer

A number of separate systems were purchased in support of DCS production system efforts at Duke Energy. These included:

1. The production systems installed in each unit (4 total)
2. A fleet laboratory system (1 total). This system was used for requirements refinement, and development of standard configuration work instructions for the DCS. It was also procured to be an off-process, full replica of the production systems to be used for lifecycle support of the production systems, as described in Section 3.3.1.2.

The systems described in (1.) and (2.) above accomplished their intended purpose.

Lesson Learned #1: Utility/Vendor Teaming

> Non-nuclear I&C vendors possess a wealth of knowledge in both the operation of their technology and in its application to solve customer process control challenges. Utilities can be challenged to provide requirements that are complete and that avoid specifying not only what the control solution is to provide, but how the utility expects it to operate. Many times, utility specified "hows" in initial versions of requirement documents used for vendor proposals are not actual requirements and can preclude leveraging vendor products. Utility/vendor teaming to iterate to a mutually understood set of final, detailed requirements can result in an optimized design that converges more rapidly.

Lesson Learned #2: Early Fleet Laboratory System Procurement and use of Agile/SCRUM processes

> Procuring a system as part of the Agile/SCRUM enabled requirements development, specification development, configuration instruction development, and FAT processes was instrumental in accelerating the design and implementation effort, producing a better final product, and facilitating vendor teaming & knowledge transfer. Maintaining this system as off-process system lifecycle support tool in an SDOE environment not only supports lifecycle activities, but is instrumental in retaining system knowledge, training personnel, and enabling the utility to maintain and modify the system in-house.

Lesson Learned #3: Use of the Fleet Laboratory System to Configure Instances of the Production System Software

> Use of the fleet laboratory system in the SDOE allowed for site specific software configurations to be developed independent of the individual site production system purchase. Software configurations for all four production systems were developed in the same secure location by the same individuals, following the same procedures. This promoted standardization and the utilization of lessons learned. The software and hardware for each production system were married together at each individual site and tested, reducing plant resources needed and outage impact during system installation.

Potential Improvement Area #1: Optimization of the Initial Development System

> The footprint of the initial procurement fleet laboratory system could be reduced. For utilities that have not yet embarked on a major DCS implementation, a clearer understanding of vendor quality processes and platform testing, improved initial utility training on the DCS platform, and a clearer understanding of the envisioned end state utility lifecycle support model could be used to reduce the initial footprint of the fleet laboratory development system to that of a single site-specific development system as described in Section 3.3.1.2 (c). The benefits obtained by Lesson Learned #2 could still be realized, but at a significantly reduced cost. Since a full-scale system would not be

available for a FAT of the standard DCS configuration, a utility would be required to perform the due diligence necessary to establish that the vendor solution would still meet the DCS implementation requirements. This would be a similar effort to that described for a system upgrade as described in Section 6.3 below.

Potential Improvement Area #2: Leveraging Vendor Testing Results Instead of Performing Limited Scope Testing on Production Systems

The culture of the nuclear industry is to independently verify the performance of a procured system to ensure specified requirements are met. This is particularly informative and warranted when a system is purpose-built to meet those requirements.

When deploying a fully developed DCS produced by a process control system vendor with 40 years of experience with fielding systems and servicing them on an industrial scale, the value of performing additional tests to validate basic core performance features guaranteed by the manufacturer is of questionable value. For example, in this case the fleet laboratory system was configured for a capacity performance test of less than one-tenth of the capacity guaranteed by the vendor and validated by them in their EPKS Platform test laboratory. The fleet laboratory system configuration had to be altered from its standard configuration as deployed in each unit to enable this test. Developing configuration instructions for the DCS, connecting it to a separately configured dynamic network simulator to stimulate "representative" network traffic, developing test procedures, executing the test, and documenting the results was a labor-intensive activity that impacted the project schedule. The expected result was realized. The system configured as specified by the vendor did perform as designed and previously tested by the vendor.

Alternatively, a due diligence audit by a utility on the vendor DCS platform design and testing process to ensure adequacy should be pursued. This is consistent with industry practice and in keeping with 10 CFR 50, Appendix A, Design Criteria 1, as applied to non-safety systems.

3.1.7.2 Cyber Security

Lesson Learned #4: Standard Cyber Security Design & Assessments

Implementing a standard cyber security design extended the concept of "design once, build many" into the realm of cyber security. The intent of this was to minimize initial development and lifecycle support costs. Application of a standard cyber security design and assessment process was also intended to simplify regulatory review across the multiple units at multiple sites.

Potential Improvement Area #3: Improved Coordination Between Sites for Cyber Assessments

While the utility produced standard cyber security procedures for performing assessments across its fleet, individual site interpretation of these procedures limited the use of the standard cyber security assessments. This resulted in more work and divergence of the level of detail included in the final cyber security assessments as completed at each of the three sites for the standard design. Lifecycle maintenance of these assessments was also complicated as a result. Organizational authority with regard to standardization in this area could be improved to minimize future occurrence of this issue.

Potential Improvement Area #4: Tailoring the Cyber Security Defensive Architecture to Reflect Current Industry Direction

Because of the newness of NRC regulation and industry guidance in this area in the 2012-2014 timeframe and the use of the vendor's DCS virtualized design (which was novel in the same time period), a conservative approach was used to address NEI 08-09 [8] controls in the design. The result was a comprehensive and intricate hardware and software cyber security defensive architecture. While this provides enhanced cyber security protections, it is difficult to configure and maintain. Furthermore, current industry understanding with regard addressing cyber security reveals that the defensive architecture could be simplified to provide necessary protections but at lower cost.

3.2 Integration of DCS into the Simulator

3.2.1 Activity Description

Plant training and qualification simulators are required to be high-fidelity representations of the associated operating unit. In the past, plant I&C upgrades with associated HMIs in the control room were implemented in the simulators through custom modifications to replicate the look, feel, and operational characteristics observed in the plant control room. The associated items depicted in red in Figure 4 were modified in the simulator to accomplish this end.

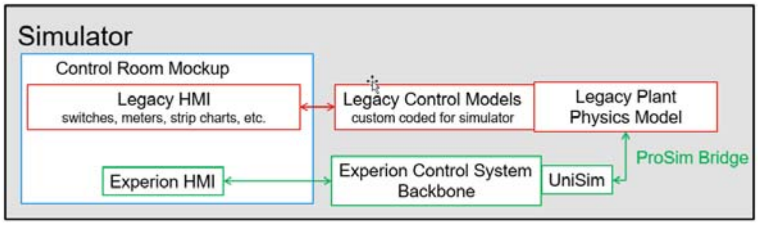

Simulator
Control Room Mockup
Legacy HMI
switches, meters, strip charts, etc.
Legacy Control Models
custom coded for simulator
Legacy Plant Physics Model
ProSim Bridge
Experion HMI
Experion Control System Backbone
UniSim

Figure 4. DCS Integration into Simulator.

These custom modifications to the legacy structure typically required significant additional effort, because there was no way to directly incorporate the plant I&C changes into the simulator. Incorporating each of them into the simulator was a unique engineering activity that followed a basic template. For the production DCS implementation to be successful, a mechanism to seamlessly incorporate plant control system and requisite control room modifications into the simulator was necessary.

Honeywell offers a process modeling solution (UniSim). This tool is used by non-nuclear industries (e.g., petrochemical) to enable the creation of simulators for uses including operations training. This is depicted in green in Figure 4. UniSim process models could not be easily applied to nuclear plant simulator use. UniSim does offer a tool (the ProSim Bridge) that allows for the use of third-party simulation models. Honeywell leveraged the ProSim Bridge to link Experion to the products provided by Duke Energy's three different simulator model vendors.

The certified plant simulators at three Duke Energy nuclear sites can now directly accept DCS control system modifications and HMI display pages. Legacy control models for functions migrated to the DCS are deleted and replaced with new EPKS controller code that is created for the plant (without modification). This new code is run in simulated Experion controllers. The controller code is linked to the legacy plant simulator model via memory mapping across the ProSim Bridge. Simulator physical changes are limited to removing legacy HMIs for the migrated function and incorporating the same DCS thin client workstations used in the plant control room.

In addition to the certified plant simulators, new glasstop simulators were implemented at each of the three sites. Two are shown in Figure 5 and Figure 6 below. These simulators operate in a manner logically identical to the simulators certified for training and qualification as depicted in Figure 4. The difference is that the operating panels in the glasstop simulator control room mockups were implemented with electronic touch screens that fully emulate actual plant control room panels.

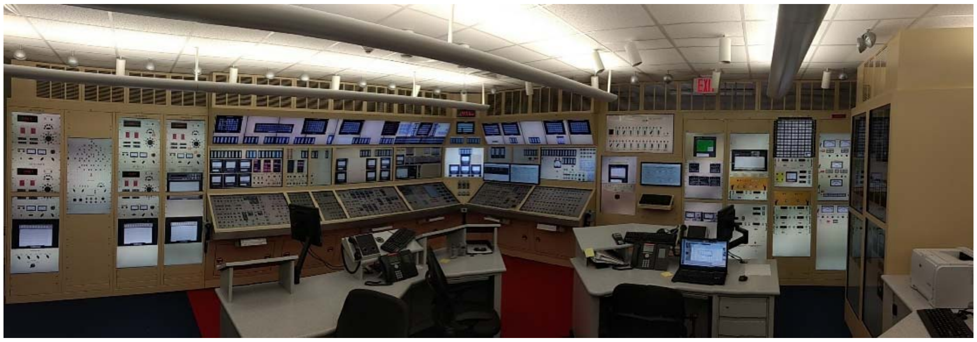


Figure 5. Robinson Nuclear Plant Glasstop Simulator Control Room.

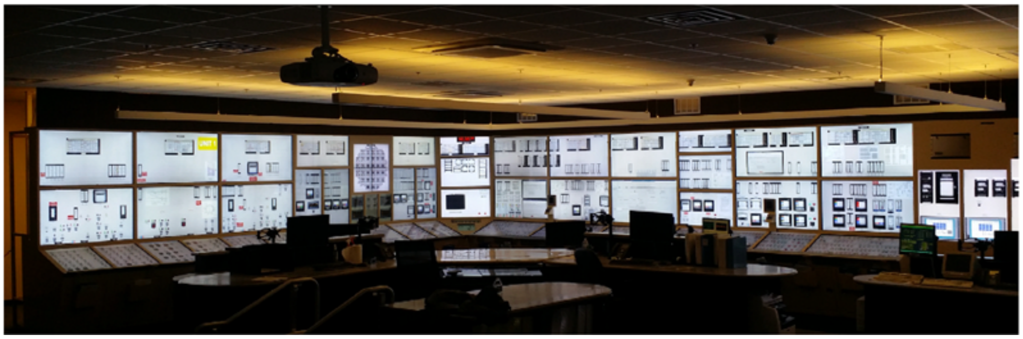


Figure 6. Brunswick Nuclear Plant Glasstop Simulator Control Room.

Indications and controls functionality are provided for legacy equipment through (1) the use of functional images that replicate indications and (2) touchscreen controls that closely replicate push button and switch functionality. Picture-in-picture functionality is also supported for HMI displays produced for presentation on the DCS in the plant on separate Video Display Units (VDUs).

These simulators were found by the Idaho National Laboratory and the Institute for Energy Technology (Norway) to be capable of supporting the Turbine Control System (TCS) Upgrade Integrated System Validation effort [12] as part of the DCS Human Factors Engineering Program as applied to that project [13].

The infrastructure investments made in the glasstop simulators and their ability to directly run HMI displays and control logic as implemented on the DCS provide a vehicle to assist future function migrations to the DCS. The glasstops can support design activities such as (but not limited to):

a) Rapid prototyping to assess control room console changes electronically early in the design
b) For indication and alarm functions to be migrated to the DCS in the control room, these console/display changes could be fully developed for the plant function, directly loaded on the glasstops, and assessed for proper human factors.
c) Provide early functional assessments of control logic as a risk mitigation.

In nearly all cases, no additional hardware or software purchases are required to support these capabilities beyond periodic system hardware and software upgrade. Simulator DCS hardware and software upgrade is planned to be synchronized with the upgrade of the production DCSs installed in the operating units at each site.

3.2.2 Lessons Learned / Potential Areas of Improvement

These glasstop simulators are less than two years old. They have already been fully embraced by plant operations and have demonstrated their value in multiple ways beyond their initial purpose of supporting the Turbine Control Upgrade Project Integrated System Validations described in Section 3.2.1 above.

Lesson Learned #5: The Importance of Incorporating the Simulator as part of an I&C Modernization Program.

Updating the simulators with DCS technology was initially envisioned as an activity that lagged production DCS development and deployment. The purpose of this activity was solely to mimic plant DCS function migrations in the simulator, including leveraging the intellectual property created for the production systems. They have performed this admirably. What was unanticipated was the degree to which Plant Operations embraced the simulator (particularly the glasstop). The deployment of this technology helped Operations grasp the features and functionality that I&C modernization can offer. The result of this is that incorporation of the DCS into the simulator created a tool that is used to visualize and drive I&C Modernization.

Lesson Learned #6: Alternative Uses for Simulators Beyond Operator Training

While they are not currently certified for formal operator qualification training and certification, the glasstop simulators provide a vehicle to perform activities such as (but not limited to):

a) Creating and validating procedures

b) Familiarizing and training operators on control system performance and procedures (particular for legacy I&C functions migrated to the DCS).

c) Identifying operational issues with the new designs provided on or linked to the DCS prior to installation in the plant (within the limits of simulation)

d) Testing plant DCS software changes identified through simulator use or by other means (within the limits of simulation)

e) Performing feasibility studies for DCS functional improvements and proposed legacy I&C function migrations to the DCS. Control software and associated HMI can be created, linked to the physics-based plant model, and demonstrated without any further hardware or software investment.

Potential Improvement Area #5: Using Appropriate Hardware for Integration of the DCS with the Simulator

In pursuit of the goal of standardization, the same DCS hardware used for the production systems was also used in the simulators as part of the integration effort. Hardware standardization to this degree was costly. Furthermore, it actually introduced performance issues, because processor speeds and data throughput to support proper simulator operation are beyond that needed for control system operation and challenged the capabilities of the equipment. Since the vendor DCS platform is fully virtualized, 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. A tradeoff analysis should be performed when upgrading the simulators as part of I&C plant modernization to determine the optimal hardware solution.

3.3 Lifecycle Support Strategy

3.3.1 Activity Description

3.3.1.1 Incorporation of Lifecycle Strategy into System Design from the Start

The need to have a fully developed lifecycle support strategy for the pilot DCS was recognized in the concept phase of the program that implemented it in each of the four target units. As stated in Section 3.1.2 (d) and (e), the vendor and their associated platform was chosen in large part because of the vendor's commitment to maintain backwards compatibility of their current DCS with legacy systems to protect legacy intellectual property investments, and because their platform was designed to protect intellectual property investments going forward from future hardware and software obsolescence.

Key pilot DCS design attributes were also selected not only to improve system reliability/availability, but also to enable subsequent lifecycle support. These include:

a) Redundancy – The entire DCS is designed as redundant system from the distributed processors employed in the field through the process control network that aggregates data and supports user HMI. Failure of any one component above the I/O module in the control architecture causes no loss of process view or control. In addition to the obvious operational benefit, this architecture enables an on-process migration of system software and hardware while the DCS is still servicing plant functions. Migration is performed by executing a "controlled failover" as one side of the system is taken off-process, migrated, and then control transferred to it. The other side is then similarly migrated. It must be understood that a unit that fully leverages an installed DCS will be using it on-process continuously, whether the unit is at 100% power or in an outage. This on-process migration capability is leveraged outside of nuclear to enable software and hardware technology upgrades without interrupting facility operation. Sections 4.2 and 5.2 outline this process in more detail.

b) Virtualization – Software implemented in a virtual environment is portable. So long as a new hardware host and the VM software host residing on it provide the requisite processing capability for VMs loaded on them, initial software intellectual property investments can be fully leveraged on new hardware.

c) Use of standard vendor tools and configurations – Vendors design their DCSs with a suite of software tools to configure their system for customer use. This includes items such as software control application tools (e.g., a "control builder") and an HMI graphics development tool. Since these vendors also leverage business IT equipment within an industrial DCS OT environment, they establish strict configuration boundaries to ensure these systems provide bounded performance characteristics required for process control. Implementation of a vendor's DCS should be bounded within the environment established by vendor directions for both tool use and DCS configuration. This again has obvious design and operation benefits by constraining the particular DCS implementation within an envelope fully bounded by the vendor test regimen. It also ensures that the DCS is in a vendor-bounded state for migration to new software and hardware. Vendor tools to facilitate such migrations can be fully leveraged to harvest intellectual property investments (e.g., software applications and HMI displays). Implementing custom solutions created outside of the envelope of the vendor standard design not only complicates the initial implementation of these solutions, but most cannot be migrated using standard vendor tools. This increases both initial implementation costs and creates intellectual property orphans that in most cases must be re-engineered when a technology migration occurs.

d) Backwards compatibility – The vendor's previous commitments to this along with their forward-looking obsolescence management plan gave additional assurance that initial intellectual property investments would be protected. Section 5 and Appendix B detail, respectively, detail how migration planning and backward compatibility are leveraged going forward.

3.3.1.2 Organizational Lifecycle Support Model

Duke implemented a three-tiered lifecycle support organizational model for their DCSs that includes:

a) Top Tier (Vendor) – The vendor provides full range lifecycle support from system patches through complete technology upgrades. Any emergent operational issues identified through the global use of their DCS product that could significantly impact operation of Duke's implementation are communicated. Any DCS issues experienced by Duke that cannot be resolved by Duke are forwarded to the vendor for analysis and resolution.

b) Middle Tier (Fleet Level) – Fleet organizations (lifecycle support and engineering) were established to address regular upkeep and emergent operations issues that could not be resolved at an individual site level, or if they impacted multiple sites. Fleet engineering was also set up to lead common DCS design modifications and major upgrades. The fleet laboratory system described in Section 3.1.7.1 is located in an SDOE facility in a centralized location to support these functions. Common design/support activities driven from the top tier or driven by fleet are tested on the fleet laboratory system prior to site deployment).

c) Bottom Tier: (Site level) – Each of the three sites implementing the DCS was provided with a site-specific development system in an SDOE (three total). These are approximately one-quarter of the hardware size of the Fleet Laboratory System. They include an instance of every hardware device and VM provided in the centralized fleet laboratory system (and their installed plant DCSs). This were procured as a vehicle for site engineering and craft personnel to maintain knowledge and proficiency in lifecycle support activities for this equipment. Site personnel could apply system changes provided from (b) above on an off-process system prior to in-plant deployment, develop site specific software applications on these systems, and perform lower level system support.

3.3.2 Lessons Learned / Potential Areas of Improvement

Potential Improvement Area #5: Optimization of Systems Used for Production System Lifecycle Support

The number of systems procured for lifecycle support should be optimized and more closely coupled with the utility's organizational structure and lifecycle support philosophy.

While the multi-tiered nature of the support model implemented by Duke is a workable solution, it is resource-intensive in terms of hardware and software, facilities, and personnel. Four off-process systems in four separate SDOEs were procured and need to be maintained. To enable sites to individually train, troubleshoot, and modify the DCS requires a larger number of people, more training, and more activities to maintain proficiency. If this model is maintained, the cost to maintain this larger support footprint will be ongoing. Furthermore, when system technical upgrades occur, all four off-process systems will need to be upgraded as well.

A potential minimum solution for technology upgrades would be to collapse the multi-tiered model described above. With the knowledge transfer of the initial system development accomplished, the fleet development laboratory system described above could be reduced in size to mimic the site-specific development systems and thus the individual site development systems could be eliminated. Lifecycle support facilities and resources could also be more centralized.

4. Modernization Overview of an Installed DCS Leveraging Vendor Developed Techniques

4.1 Key Factors that Drive DCS Modernization

4.1.1 Obsolescence Issues

4.1.1.1 Hardware Obsolescence

Due to the nature and progression of technology, it has been recognized in industry that an Operations Technology (OT)-based digital I&C hardware platform will not be supported after 7 to 10 years from its original release date. Improved processor, memory, and storage capabilities drive this obsolescence. Older OT product lines are discontinued and replaced with more capable ones to continuously improve the vendor's DCS product capabilities. This creates a cyclic condition requiring technology to be upgraded to avoid additional costs to maintain the obsolete hardware set.

4.1.1.2 Software Obsolescence

OT-based software also becomes obsolete over time; Just like hardware, operating system software, virtualization software, and application software are regularly updated to improve performance, to add new capability, to address cyber security vulnerabilities, and to address bug fixes. Older versions are replaced with newer ones. Support for obsolete software is also discontinued.

Software obsolescence can also be driven by hardware obsolescence. For example, virtualization host software is typically tested for proper performance on hardware available at the time of the software release. In the pilot DCS example described in Section 3, the server hardware equipment was discontinued in 2016 by its manufacturer. VMware virtual hosts installed on the pilot DCS are already past the "end of general support" and "end of technical guidance" dates established by VMware. No more software patches or bug fixes are provided for the installed VMware virtual host software. If an issue arises with the installed VMware virtual host software, the vendor-provided resolution is to update the software to the latest release. The latest releases of this software are not certified by the installed server vendor or by VMware to properly operate on the installed DCS server hardware. Because of this, the pilot DCS vendor will not certify proper operation of their product if the VMware virtual host software is updated to the latest release. The only way to update the VMware software to the latest release is through a synchronized update of the DCS server hardware.

4.1.2 Synchronized Hardware and Software Upgrades for Technology Migrations

Because of the interdependent nature of hardware and software obsolescence, DCS vendors tend to link product platform upgrades (both hardware and software) to major software upgrades, such as third-party provided operating system upgrades (e.g., Windows Server). This allows them to develop long-range obsolescence management plans for their products.

Vendors typically perform Supervisory Network hardware platform upgrades every 6-8 years with synchronized major software upgrades (e.g. upgrading the DCS Supervisory Network Operating System from Windows Server 2008 to 2016). This maximizes the use of both hardware and software to minimize total cost of ownership and has the least potential impact on nuclear plant operation. For the vendor utilized for the pilot DCS as discussed in Section 3, all their major platform releases have been synchronized with operating system upgrades since 2003. More detail on this subject is found in Appendix B, Table 1. Performing synchronized hardware and software DCS migrations is desirable for the nuclear industry to maximize the lifecycles of the installed DCS and to minimize cost.

4.2 Vendor Validated On-Process System Migration Activity

4.2.1 Introduction

Before presenting information that supports leveraging the vendor validated method to address obsolescence, it is best to first understand the basics of the method itself. In this context, a migration is defined as the transition of a DCS from a legacy technology (either software alone or both software and hardware) to a newer technology. Its objective is to address obsolescence of the legacy technology with a minimum aggregate cost.

4.2.2 Migration Types (Off-Process & On-Process)

An off-process migration is executed with the DCS in a state where it is not performing it design function. The "process" which the DCS is controlling is secured. An on-process migration is performed while the DCS continues to perform its design function. In an expansive nuclear plant DCS implementation, the DCS controls the majority of plant systems (e.g. nearly all plant systems that are not safety-related). Consequently, the DCS is on-process whether the plant is producing power (online) or not. Completely securing such a DCS is typically not feasible in a nuclear plant unless mitigating actions (e.g. temporary systems) are employed.

An on-process migration is the most efficient. In fact, in a nuclear context, the plant can continue to produce power during the controlled steps of the migration provided the DCS design is configured as a redundant system as further explained below.

4.2.3 DCS Architecture Overview and Migration Enablers

A basic DCS architecture consists of a Supervisory Network and a Control Network as shown in Figure 7.

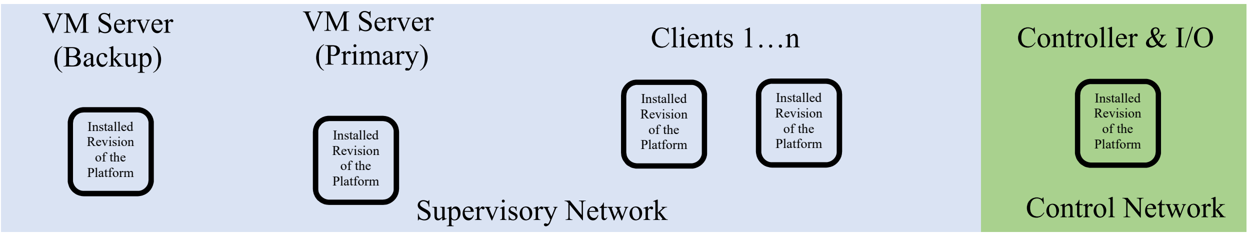

VM Server (Backup)
VM Server (Primary)
Clients 1…n
Controller & I/O
Installed Revision of the Platform
Installed Revision of the Platform
Installed Revision of the Platform
Installed Revision of the Platform
Installed Revision of the Platform
Supervisory Network
Control Network

Figure 7. Basic DCS System Architecture.

The bottom level is the Control Network (Purdue Model Level 1). The Control Network is where individual plant control and monitoring processes are distributed to numerous controllers and their associated I/O interfaces to plant systems. These controllers are then connected to the Supervisory Network (Purdue Model Level 2). This is where data across the entire DCS is aggregated. This aggregated data is presented to the operator via HMIs (primarily those in the main control room [MCR]). Operators input commands via the same HMI, which is then passed to the appropriate controllers at Level 1 to affect the operation of plant process control devices (e.g., pumps, valves, etc.).

The demarcation between the Supervisory Network and the Control Network is an important migration enabler. So long as direct plant monitoring and control processes are allocated to the Control Network, the Supervisory Network software (and hardware) can be migrated to current technology without interrupting Control Network operation. Supervisory Network software and hardware are more sensitive to obsolescence since they rely primarily on IT products adapted to an OT environment. Their lifecycles (when synchronized as discussed in Section 4.1.2) are typically 6-8 years. Control Network hardware and software lifecycles are typically much longer (20+ years) as discussed in Appendix B. This is because hardware and software at this level are typically purpose designed and built by the vendor for control purposes.

Vendors employ various methods to minimize total cost of ownership and to enable migration to current technology. Several are listed below:

- Backwards compatibility: Because of the desire to retain intellectual property and to minimize total cost of ownership, some vendors work ensure their current Supervisory Network supports backwards compatibility to legacy Control Network equipment. For the vendor studied in this research, this backward compatibility has been supported for Control Network equipment back to 1974. Details on this are provided in Appendix B.
- Intellectual property protection: Another attribute of Control Network LCM supported by DCS vendors is providing a path to harvest intellectual property from legacy systems. When it becomes necessary to retire obsolete hardware (e.g. replacement parts cannot be obtained), vendors work to provide migration paths for control algorithms running on that hardware to current systems. Details on this are provided in Appendix B.
- Decoupling of Control Network upgrades from Supervisory Network upgrades: While it may be desirable to upgrade controller and I/O firmware in the Control Network to enable new features available in current DCS releases, this is no longer a requirement for some vendors. The Supervisory Network can be upgraded without updating controller and I/O firmware. Controller and I/O update independence from Control Network upgrades retains current controller and I/O functionality. Controller firmware migration can be performed at a later time and by individual controller pairs that service different, segmented plant functions when plant operational conditions allow, or as needs dictate. The same is true for redundant I/O modules. Non-redundant I/O module firmware updates are required to be performed off-process.

4.2.4 Supervisory Network On-Process Software Migration

Figure 8 provides a simplified view of the DCS Supervisory Network hardware and software. Since the Supervisory Network of the example vendor DCS platform described in Section 3 is fully virtualized and fully redundant, this type of implementation is assumed here.

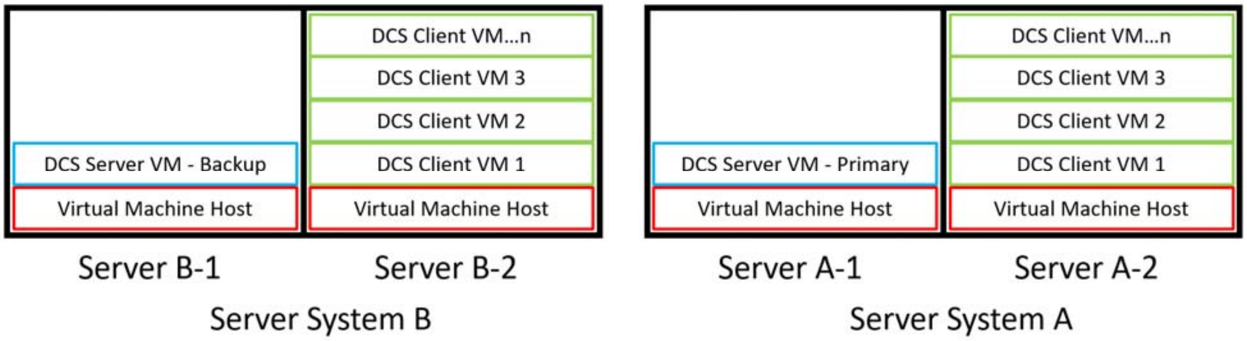


Figure 8. Simplified DCS Supervisory Network Architecture.

In this architecture, there are redundant physical server systems (A and B), each of which is made up of multiple physical servers (A-1, A-2 and B-1, B-2). Each physical server has a VM host that allocates physical server resources to individual VMs as shown. This physical design and VM allocation are done for several reasons. Loss of a single physical server (e.g. A-1) or a single physical server system (e.g. A) when the DCS is on-process results in no loss of function. The plant can continue to operate. This redundancy is also a required enabler that permits an on-process migration.

To simplify the initial presentation of an on-process Supervisory Network migration, the following discussion outlines a software migration only. Such a migration is executed as follows:

A. Copying the DCS Server VM configuration files from the DCS Server VM – Backup. Also copy the associated DCS Client VMs.

B. Shutting down the DCS Server VM – Backup,
C. Migrating the DCS Server VM – Backup and the associated DCS Client VM's to the latest software
D. Putting the migrated DCS Server VM – Backup and DCS Client VMs back on service in a "dual primary" mode where both the DCS Server VMs (original version – Primary and migrated version – Backup) run in parallel.
E. Validating the migration was successful, including migration of both the DCS Server VM – Backup and DCS Client VMs. If issues are discovered, the DCS Server VM – Backup can be secured with no loss of DCS function. If desired, the migration can even be completely reversed.
F. After validating successful migration of the DCS Server VM – Backup and Client VMs, repeating steps A through E for the DCS Server VM – Primary.

Appendix A provides a more detailed presentation of the steps associated with the software migration of Supervisory Network VMs in a redundant DCS configuration.

An on-process Supervisory Network software only migration can be performed only if the new software is compatible with the current hardware. When a synchronized hardware and software Supervisory Network migration is performed, a hybrid approach is used to further reduce risk. This approach is outlined in Section 5.2.

4.2.5 Control Network On-Process Migration

On-process migration of the Control Network can begin once the Supervisory Network migration is complete. Since the Control Network is segmented by the nature of the DCS installation, each redundant control segment is migrated individually. A single, redundant Control Network segment is shown in Figure 9.

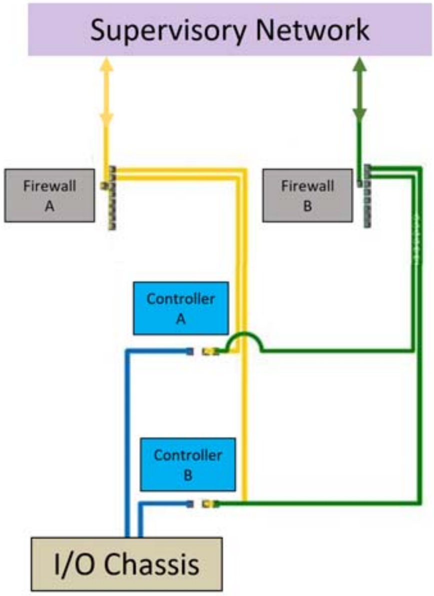


Figure 9. Single Redundant Control Network Segment.

To migrate this control segment, the firewalls are first migrated one at a time to the latest firmware release. This enables migration of controller firmware which is done one controller at a time (backup controller first followed by the primary controller). Process control for this segment is maintained through this process.

The pilot DCS implementation of such a segment also includes redundant I/O modules in the I/O chassis with redundant communication pathways from the I/O chassis to the controllers. An example is shown in Figure 10.

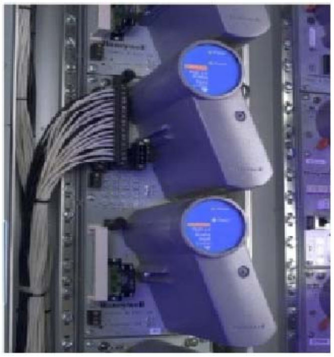


Figure 10. Redundant I/O Modules with Terminations to Non-Redundant I/O Devices.

The only non-redundant portion of the design shown in Figure 10 is the physical backplane and termination strip that connects the redundant I/O modules to the non-redundant I/O devices in the field. The physical backplane has no active components. This allows on-process updates of I/O module firmware (one at a time).

Controller and I/O module firmware update is not required when performing a Supervisory Network on-process migration as explained in Section 4.2.3 above. Controller and I/O module firmware updates are deployed to enable new features provided by the latest DCS release and/or to address any firmware issues (e.g. bug fixes) should any be identified. Base Controller and I/O module functionality is the same before and after controller and I/O module firmware updates are complete. Controller and I/O module firmware updates can be deferred to a time when it is more convenient to perform.

5. Generic Migration Planning and Execution

Architecting a full-scope non-safety DCS implementation at a nuclear plant is a complex endeavor as outlined in Section 3. As described in Section 4, the ability to perform a DCS modernization through an on-process migration is dependent upon how the DCS is initially architected. So, technology migration planning begins at the conceptual design of the original DCS implementation (see Section 3.3.1.1).

When a technology modernization is deemed necessary for a complex DCS architecture, a commensurate degree of planning is required to ensure success. The subsections below generically present key planning and execution steps to achieve a successful DCS technology migration. Since currently available DCSs offer a high degree of flexibility in supporting technology migrations (including full, on-process migrations), optimization of a technology migration in nuclear is driven by utility customer needs and constraints. These constraints are typically driven by operations, licensing, available resources, and economic considerations. Section 6 addresses optimizing DCS technical migrations in a nuclear environment.

5.1 Develop a DCS Platform Migration Plan

Developing a control system migration plan is essential to minimize problems which may occur during migration and to ensure that the migration is successful. This plan must address both the DCS and the processes that it is controlling.

When evaluating DCS for migration, several basic entry conditions need to be identified. These include

- Identifying the software release of the DCS in its current state (the current base platform release).
- Identifying the target platform software release to be deployed in this migration.
- Identifying the portions of the system to be migrated at this time.
    - Software only,

  - Software and hardware, or
  - A hybrid, such as a Supervisory Network hardware & software migration and a Control Network firmware update only
- Identifying portions of the system that are not to be migrated at this time, but during subsequent migrations.

Once these basic questions are answered, a series of more detailed questions that directly relate to the technical aspects of migrating the DCS platform are answered. These questions are answered, to a large degree, independently from processes the DCS controls. Detailed pre-migration planning checklists are employed to fully define the current state of the DCS, the future state, and the path from one to the other. The current DCS detailed configuration state is audited to ensure it is fully bounded within pre-identified limits that facilitate a successful migration. Other technical preparations such as identifying hardware/software compatibility issues, needed migration support equipment, and addressing non-native custom configurations and third-party applications within the DCS (if present) are also made.

These activities allow initial estimates of the time required to migrate the system components and development of a timetable for the migration process. This timetable includes planning, system readiness/pre-migration tasks, migration of the Supervisory Network [servers/clients] and migration of the Control Network [controllers and I/O] to the target release, and post migration tasks. Vendor migration services can offer invaluable information and guidance in planning and executing a system migration. This is because of the experience of the vendor's migration team, and their expertise in accomplishing migrations at multiple plants as part of their continuous job function.

At the same time, the process owner needs to assess potential operational impacts and constraints (operational, procedural, risk tolerance, financial, etc.) associated with performing the upgrade in their facility in general and the mode of performing the upgrade (on-process or off-process). This requires the process owner to synthesize their understanding of the DCS, the plant processes it controls, and the full intersection of the two. If there are any non-redundant system and control components, these must be migrated off-process. If a migration is planned during a scheduled plant maintenance shutdown, a migration plan must be adapted to make sure that people and resources are available and aligned to support migration efforts during the shutdown period.

This research assumes an on-process migration of a fully virtualized Supervisory Network along with firmware updates of its associated (non-virtualized) Control Network. For reasons explained in Section 4.1.2, nuclear plant DCS migrations would be optimized by synchronizing DCS Supervisory Network platform hardware updates with major software updates (e.g. operating system updates).

5.2 Develop a DCS Platform Migration Strategy

With the DCS technology migration plan defined, a detailed project strategy can be developed that establishes the various migration tasks that need to be performed and the dependencies between such tasks.

Since a synchronized DCS Supervisory Network hardware and software update is assumed, a hybrid approach to performing an on-process migration can be utilized. This is shown in Figure 11 below.

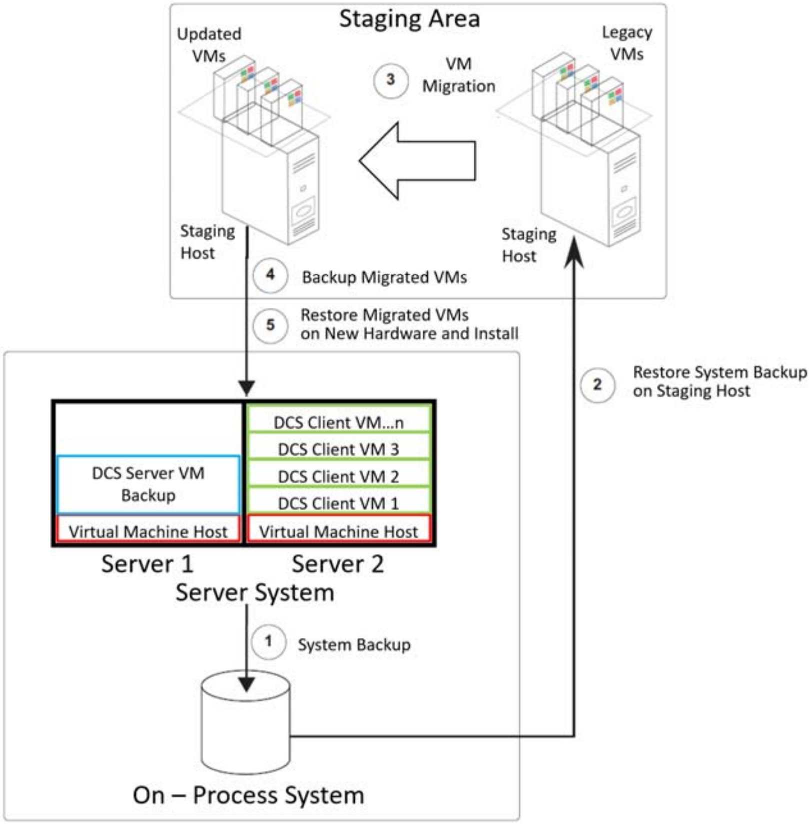


Figure 11. Hybrid Process for a Hardware and Software On-Process DCS Supervisory Network Migration.

This hybrid approach further reduces implementation risk and supports schedule compression.

Key strategy tasks are listed below. Numbered references to steps shown in Figure 11 are provided in bolded parentheses.

a) Completing tasks on the pre-migration planning checklists described in Section 5.1 to ensure the installed DCS is in a fully bounded pre-migration state to enable a successful migration.
b) Obtain copies of the current on-process DCS Server VM and the associated DCS Client VMs by performing a system backup of the on-process DCS Supervisory Network **(1)**.
c) Restore the current on-process DCS Server VM and the associated DCS Client VMs on a Staging Host **(2)** in a Secure Development and Operating Environment (SDOE).
d) Migrate the VM files obtained from the on-process DCS Network to the target release for the upgraded DCS in a virtualized staging area **(3)**. Note that this can be performed independent of the target release upgraded hardware.
e) Backup the migrated DCS Server VM and the associated DCS Client VMs **(4)**
f) Obtaining new hardware. Since standard vendor product is used, lead times for obtaining equipment once the order is placed is typically measured in weeks, not months.
g) Assemble and configure the new hardware to accept a system restore of the migrated VM's
h) Restore migrated VM's to the new DCS hardware **(5)** for the Backup Server System B
i) Perform the on-process migration of the DCS in the plant following the same general process outlined in Section 4.2.4, steps A through C. In this case, Server System A in Figure 8 assumes the role as primary for the Supervisory Network. Server System B is turned off, removed and replaced

with a new Server System B which contains all the migrated VMs created from the previous DCS release.

j) Validate the migration was successful for Server System B and then migrate Server System A as described in Section 4.2.4, steps D through F.

k) Migrate selected Control Network devices (controllers and I/O modules) as described in Section 4.2.5.

Advantages of this approach include:

- Allowing hardware procurement and software migration to run in parallel. This allows both schedule compression and delay of hardware procurement to as late as possible. Deferring hardware procurement can aid in extending the hardware lifecycle by obtaining the latest hardware version associated with the latest synchronized hardware/software DCS release.
- Performing the migration of the DCS software onto new hardware outside of the plant. This minimizes operational impact and implementation risk.
- Minimizing "cut-over" time in the plant to a minimum. By properly configuring and staging the new, fully configured Server Systems B and A, installation time for a fully upgraded Supervisory Network can be reduced to a time period measured as short as hours and no longer than a few days.
- Control Network Migration (firmware updates) can then be accomplished on one control segment at a time in the plant, and in any order that operations may dictate. This bounds the risk associated with such efforts.

5.3 Establishing Roles and Responsibilities for the Facility Owner and DCS Vendor

In order to optimize the DCS migration, the roles and responsibilities to perform it need to be clearly established. This is best accomplished by evaluating necessary skill sets and availability of resources on the part of both the vendor and the process owner as well as their intersection.

The relationship between vendor and process owner skill sets is depicted in Figure 12.

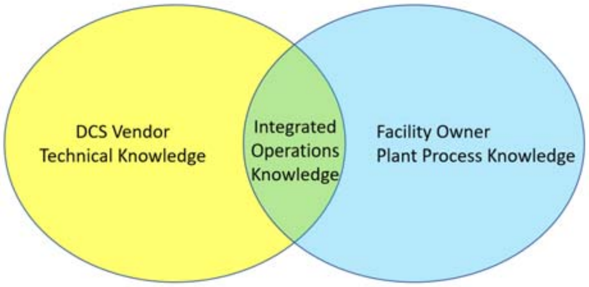


Figure 12. Vendor and Facility Owner Skill Sets as Applied to a DCS Migration.

The technical aspects associated with DCS migration to the latest hardware and software release are much more involved than the simplified presentation provided in this report. Procedures to guide the effort are complex and lengthy. Many software tools are also leveraged in concert to enable a DCS migration. Intimate technical knowledge of DCS capabilities and proper DCS platform operating characteristics are needed. Hands-on experience in performing multiple DCS technology upgrades will also help ensure a successful DCS platform migration. Vendors provide migration teams that possess these skill sets.

A DCS technology migration would occur at a particular facility owner's site approximately every 7-10 years. It is unlikely that process owner personnel would possess the necessary level of migration experience along with up-to-date technical knowledge of the latest vendor DCS platform release and migration tools to efficiently perform a technical upgrade at the identified periodicity. The most efficient path to successfully execute the technical aspects of a DCS migration is to maximize the vendor's migration team to provide the expertise colored in yellow in Figure 12.

Yet, the facility owner is still ultimately accountable for their business. The facility owner also understands the operation of their plant processes and the implications if those processes are adversely impacted during a DCS upgrade. A roving vendor DCS migration team is also unlikely possess or retain plant process knowledge when performing DCS updates at the identified periodicity. The facility owner provides the expertise colored in blue in Figure 12.

For a migration to be successfully completed, integrated knowledge of the intersection between the DCS operating characteristics and the serviced plant's operating characteristics must be established and retained. This is shown in green in Figure 12. Two ways to achieve this are:

1. Train select facility owner personnel knowledgeable in how the plant operates to become SMEs on the DCS. These individuals must not only understand how the DCS works, but how enables plant the plant to operate within all applicable constraints (e.g. the plant design basis, the plant regulatory basis including technical specification limits, regulatory concerns with software CCF, etc.)
2. Train a DCS vendor personnel to perform the same function as identified in #1 directly above. It would be expected that a minimum full-time presence of vendor personnel at the facility would be required (or be immediately deployable to the facility on an on-call basis).

The organization that possesses this integrated operations knowledge will be the one that guides the DCS technology upgrade activity and ultimately validates that it is successfully accomplished. This type of knowledgeable support is also necessary to normal plant operations. The utility is ultimately responsible to choose which of the two options will be selected and consequently which organization will guide the DCS technology upgrade.

In non-nuclear applications, many process owners contract the upkeep of their DCSs, including periodic migrations to the latest technology, to the Original Equipment Manufacturer (OEM) to minimize their facility total cost of ownership and to maximize retention of intellectual property investments. This is true even in industries where the implications of process upset are severe (e.g. the petrochemical and pharmaceutical industries). Section 6.4 discusses potential application of this concept in a nuclear.

With overall organizational responsibility identified and requisite skill sets by organization established, detailed DCS migration planning can occur. Leveraging the logical flow of activities identified in the migration strategy (Section 5.2), allocation of activities to organizations and identification of necessary resources to perform the activities can occur. Ultimately, this leads to the development of a time-phased, resource loaded, executable schedule to accomplish the DCS migration.

6. Optimizing I&C Modernization in a Nuclear Environment

6.1 Vendor Selection & Collaboration

Selecting a vendor and their product for the initial implementation of a non-safety DCS platform for a nuclear plant is a defining moment for that facility. The objective of using such a DCS is to improve plant performance while enabling lower plant total cost of ownership. This includes both the initial investment and lifecycle support costs to retain it. The more it is leveraged to address I&C obsolescence and to provide advanced features, the more intellectual property investments will be made in it. To change vendors once this investment has been made would only be considered when there was a compelling business interest to do so. Since vendor products are largely proprietary by nature, to transition all the intellectual property from one DCS platform to another would take significant time and require significant expenditures. The expectation should be that the utility will be engaged with the DCS vendor they select for an extended period, even to the point of plant decommissioning.

With the prospect of entering into such a relationship with the DCS vendor, key aspects related to vendor selection should be considered. Several of these are presented with respect to the pilot DCS implementation as presented in Section 3.1.2. Generically, such items include:

a) **Identifying key properties to be provided by the DCS to enable vendor product selection.** These properties are identified by a utility at a higher level than detailed functional requirements. The Electric Power Research Institute (EPRI) Digital Engineering Guide [14], Section 4.1, presents these in terms of identifying "stakeholder needs." At this point, the focus is on identifying "what" properties the vendor product provides rather than specifying "how" the vendor product provides them. This way of thinking needs to be informed by the fact that the vast majority of non-safety monitoring and control functions that need to be serviced in a nuclear plant are in no way unique to a nuclear plant. Necessary control system features such as determinism, fault tolerance, graceful degradation, and guarding against CCF are also not unique needs of nuclear DCS implementations. Over-specifying the "how" in initial vendor product selection will invariably result in fewer responses from DCS vendors (both traditional nuclear and non-nuclear) to requests for proposals, higher costs in the proposals received, and longer schedules for design and implementation.

b) **The ability to employ the selected DCS without customization**. By not over-specifying how the vendor solution provides required functionality and developing detailed requirements using a collaborative Agile process as described in Section 3.1.3, the need to create customized features not supported by the base vendor product and its associated design tools is minimized. The use of third-party software applications is also minimized. This simplifies initial deployment of the DCS. It also supports fully leveraging vendor activities that validated the performance characteristics of the platform as part of its design independent of any particular customer's application of it. This enables utility specific platform level testing to be minimized or in some cases eliminated.

   This approach also simplifies technology migrations because the scope of the migration is limited to the vendor's base product. Entry condition for the technology migration are fully bounded within the vendor's design envelope. Vendor mechanisms to implement technology migrations and validate the result can be fully utilized. Implementation of custom coding and operator displays outside of the vendor's standard DCS development tools are typically accomplished at additional cost, require specific testing, and are largely not migratable when performing a DCS technology upgrade. The same is generally true for the use of third-party software applications.

c) **The willingness of the vendor and utility to team to develop DCS detailed requirements and configuration instructions.** As presented in Section 3.1.3, the pilot implementation of a non-nuclear I&C DCS in a nuclear plant was enabled in a large part by the teaming relationship established between the utility and the selected vendor. There are several reasons for this. The nuclear industry has lagged other industry sectors in the implementation of digital I&C systems. This has resulted in industry personnel being unfamiliar with the capabilities of modern digital I&C systems. When utilities then attempt to write detailed requirements while suffering from this deficit, the result is much more difficult for the vendor to implement. It creates significant churn in the design and implementation phases of a DCS installation or upgrade. This is exacerbated when interactions with the vendor to resolve resulting issues are constrained within a rigid contracting structure where the vendor communicates large numbers of exceptions to requirements through contract documentation and the utility responds in kind. Also, the complexity of the configuration of a modern DCS is such that full specification of every setting is beyond the capability of the utility by itself to specify by requirement. Better detailed requirements and system configuration instructions can be realized more quickly by leveraging the vendors knowledge of their DCS's design attributes and capabilities in an Agile development process. The Agile process has demonstrated its value in other industries and in the identified DCS pilot.

   In nuclear, this teaming is especially valuable when addressing the nuclear industry need to address cyber security per 10 CFR 73.54 within the context of the vendor's DCS design. By the utility identifying cyber security requirements up front, methods and techniques can be employed to address many of them by leveraging the design properties of the vendor's standard product. For requirements that cannot be addressed in this fashion, custom solutions can be added in a way that is segregated from the vendor base product. There are multiple benefits, which include:

- Maintaining the configuration of the DCS within the bounds of vendor design and test envelope. This eliminates the need to revalidate DCS design performance to address cyber security induced deltas. For the pilot DCS cyber security efforts described in Section 3.1.4, the utility teamed with the DCS vendor to identify the optimal cyber security toolset. The core product selected to perform cyber security monitoring and data aggregation/analysis was selected over others because it could be interfaced to the DCS in a way that supported this end.
- Enabling migration of the DCS vendor product via the vendor validated process to do so. Segregation of these functions allows base DCS product technology upgrade to occur using vendor developed processes as previously discussed. It must be noted that the cyber security tools employed (both software and hardware) have obsolescence issues of their own that must be managed. While the DCS vendor can assist in selecting third party cyber tools and help ensure they do not interfere with DCS performance, it cannot be expected that the vendor will retain expertise on these tools over time. For the DCS pilot discussed in Section 3, utility personnel became the SMEs in configuring the cyber security tools including establishing the lifecycle support strategy for them.
- Coordination of cyber security expertise between OT and IT systems. OT technology deployed in the DCS leveraged cyber security tool that are widely used in business IT systems. In the DCS pilot described in Section 3, the core product selected to perform cyber security monitoring and data aggregation/analysis was also one that had been selected by the utility's IT department as a standard for the corporate business network. This coordination can be leveraged to lower acquisition and support costs as well as facilitate utility knowledge retention to support upgrading DCS cyber security hardware and software.

d) **The ability to incorporate the DCS seamlessly into the plant simulators.** This topic is fully presented in Section 3.2. Upgrading the DCS in the simulator is expected to follow the same general flow as that implemented in the plant. By leveraging concepts identified in *Potential Improvement Area #5* in Section 3.2.2, hardware costs when upgrading the simulator could be significantly reduced as enabled by virtualization.

e) **The size, market penetration, historical experience, and resource depth of the vendor.** Leveraging a vendor with global market penetration and wide acceptance of their products spreads the vendor's DCS development cost operating experience base across a myriad of different industries and applications. This economy of scale and competitive business environment drives down DCS utility costs. It also improves quality. Lessons learned from millions of runtime hours over decades are incorporated into an evolving product line to drive improved performance and reduced system operational issues. It is in the vendor's best interest to establish quality practices not only as a method to adhere to industry standards, but to demonstrate to customers the commitment to maintain and improve system performance and reliability. By selecting a vendor that is large, stable, experienced, widely used outside of nuclear, and with a reputation for producing quality product and supporting it for decades enables leveraging all of these attributes without having to have contributed to the investment to create them. It also minimizes implementation risk.

Information regarding this subject for the DCS vendor involved in pilot implementation at Duke is provided in Appendix D. It would be expected that a nuclear utility would evaluate similar information provided by any vendor they are considering when making a DCS vendor decision.

h) **The ability of the vendor to maximize the protection of utility intellectual property investments.**

In order to maintain a competitive position within the process control industry, some DCS vendors have long recognized that protecting the intellectual property investments made by their customers in the past. This improves the vendor value proposition when proposing hardware and software upgrades to address obsolescence. Many industrial DCS Control Network products released by system vendors can date their origins back to the 1970s and 1980s. With economics being a major driver when considering DCS upgrades, many industrial customers will only perform Control Network upgrades either when either obsolescence drives them to do so, or when the upgrade provides significant financial benefit. Completely re-engineering a Control Network solution on new hardware and software in such cases is often cost prohibitive. Industry demands that new DCS products be backward compatible.

Some DCS vendors has responded to this customer imperative by ensuring their new DCS products are backwards compatible with their legacy Control Network products. Backwards compatibility of Control Network enables DCS Supervisory Network on-process migrations as discussed in Section 4.2.3. All the intellectual property contained in the Control Network is retailed during such a migration.

Paths for future DCS Platform technology migrations need to continue to support backwards Control Network equipment compatibility. When obsolete equipment can no longer be replaced, some major DCS vendors have developed migration paths to harvest the intellectual property off the obsolete equipment and place it on current Control Network hardware that is supported. For the DCS vendor involved in pilot DCS implementation at Duke, Table 2 in Appendix B shows how harvesting of intellectual property is supported in some cases for a period exceeding 40 years.

Protecting Supervisory Network intellectual property investments has become increasingly important as DCS's have leveraged IT technology to improve performance and provide additional functionality. Processes akin to that described in Section 4.2.3 have been created expressly to achieve this end. The application of IT virtualization technology to OT coupled with DCS vendor efforts to use it to enable retention of intellectual property at Control Network is expected to become more prevalent moving forward.

The degree to which a vendor demonstrates an established track record of backwards compatibility going far into the past as well as a mature intellectual property protection strategy going forward should be a deciding factor when choosing a vendor and their product line for DCS implementation.

i) **The ability of the vendor to act as an I&C Systems Integrator**

If the strategic objective of deploying a non-safety DCS is to support a larger digital modernization, then the ability of the non-safety I&C System vendor to act as an overall I&C systems integrator should also be considered when making a selection. When fully leveraging a DCS as part of larger modernization, the functions of many disparate, legacy I&C systems would be transitioned to the DCS. Those legacy I&C systems would then be decommissioned. If this progression is continued until a majority of plant I&C functionality is supported by the DCS, day-to-day plant operation will largely be performed from it. Significant control room modifications would also be required. For a fully digital nuclear plant, the non-safety DCS becomes the nexus for gathering and distributing plant I&C data. This is shown in Figure 13.

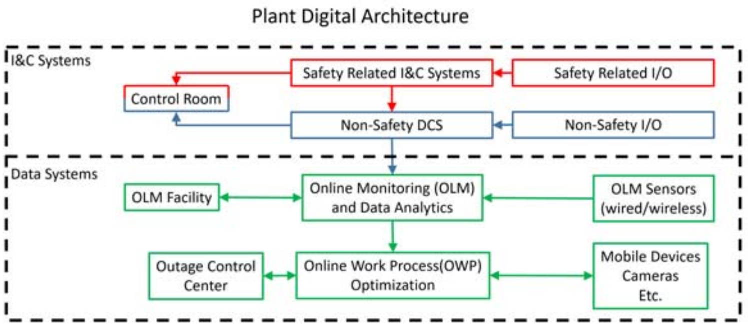

Plant Digital Architecture
I&C Systems
Safety Related I&C Systems
Safety Related I/O
Control Room
Non-Safety DCS
Non-Safety I/O
Data Systems
OLM Facility
Online Monitoring (OLM) and Data Analytics
OLM Sensors (wired/wireless)
Outage Control Center
Online Work Process(OWP) Optimization
Mobile Devices Cameras Etc.

Figure 13. Simplified Nuclear Plant Digital I&C Architecture.

> Optimally, the training simulators would also deploy the same DCS technology as described for the DCS pilot in Section 3.2. This involves integrating the DCS technology with the physical simulators owned by the utility and the physics-based plant models typically supported by a vendor (e.g. GSE Systems, Western Services Inc. etc.).
>
> While the utility is still ultimately accountable for the successful outcome of their DCS upgrades and subsequent technology migrations, leveraging the expertise of the non-safety DCS vendor's technical knowledge and system integrator capabilities can further reduce risk in strategic I&C modernization efforts.

All of these considerations help to point the utility to a vendor who is capable of and competent to provide a well-developed product with a fully functional feature set that may then be utilized to control the plant's functions and to maximize operational efficiencies. This allows the utility to then leverage the vendor's investments and expertise to apply the technology needed to solve the plant's issues and to streamline the plant's processes. Effective teaming between the utility and their selected vendor can produce a much better product in a shorter time period, at a lower cost. It is also critical for long term support to manage obsolescence.

6.2 Utility Personnel Training on the Selected Platform

In order for the utility to effectively team with the vendor, utility I&C personnel need to obtain training on the selected platform from the vendor as soon as possible. The intent of this training is not to enable the duplication of the vendors capability within the utility organization. Rather, it is to enable the utility personnel to become more educated, contributing members of the utility/vendor team.

For the pilot DCS implementation at Duke Energy, this directly contributed to:

- Collaborative requirements development and test procedure development/execution by the utility and the vendor
- Collaborative development of nuclear specific cyber security requirements by the utility and vendor for incorporation into the DCS design
- Utility development of the DCS Hardware FMEA [7] and the DCS SHA [6]
- Utility development of the strategy for leveraging the DCS to implement I&C functions migrated from obsolete I&C to the DCS while staying within the bounds of licensing commitments made to the NRC.

For performing a DCS migration from obsolete hardware and software to the latest release, similar utility training is needed to further this teaming. Training topics should address:

- The specific obsolescence issues facing their installed DCS,

- How these obsolescence issues are addressed by migrating to the latest hardware and software releases along with new features provided in the latest releases.
- Specific information with regard to how intellectual property contained on the DCS to be retained when the DCS is migrated to the latest technology
- The migration process itself, including establishing initial conditions for the migration, steps to accomplish the migration, and the level of post migration testing required to ensure it was successful.

Utility personnel armed with this information are able to leverage their knowledge of plant operation and plant processes to enable executing the technology migration most efficiently within utility administrative processes and procedures while striving to assure that the migration will occur without any plant operational upset.

Benchmarking of initial vendor DCS installations and technology migrations at similar facilities should also be undertaken by utility personnel as appropriate to enhance their understanding of the technology and their role as the facility stakeholders for these efforts.

6.3 Audit Vendor Design and Lifecycle Support Processes to Ensure Acceptability for Leveraging in Nuclear

In order to leverage vendor design processes and vendor platform testing to the maximum extent practicable for both the original installation of their DCS and subsequent migrations, the utility must perform audits of these processes. Due diligence is required to ensure that by leveraging these processes, the nuclear plant design basis is fully supported, and regulatory commitments are still satisfied when deploying or migrating the DCS.

Requirements to meet established industry standards for industrial I&C systems need to be included in vendor contracts. In the initial DCS implementation phase, the audit should focus on ensuring that the intent of these standards is being properly met by the vendor. For the DCS pilot, this audit process is described in Section 3.1.2. This was augmented by the vendor providing additional specific information with regard to how their engineering process meets the intent of contracted industry standards. This is captured in the DCS pilot SHA, Reference [6].

A similar audit activity is also necessary the vendor migration process. This builds on the foundation set created by the initial audit done to enable initial DCS implementation and extends it to cover DCS migration activities. To gain insight into what would be necessary to perform a migration process audit and to generically understand the steps required to perform such a migration to support this research report, a multi-day meeting was held at the pilot DCS vendor’s facility. A complete walkthrough of a software migration of an example Supervisory Network Virtual Machine configuration was demonstrated as part of this meeting.

The intent of these audits is to establish that vendor design and quality assurance properties for the DCS platform are sufficient and that utility retest of DCS platform performance characteristics is unnecessary. Audit performance and generation of requisite documentation demonstrates the necessary due diligence to support this claim. This requires that the utility DCS platform configuration is fully constrained with the design and test envelope established by the vendor. By establishing that vendor DCS platform design and testing activities are sufficient, all the activities associated with a nuclear utility re-evaluating these features becomes unnecessary. The resources and the time spent re-evaluating these test activities can be harvested as significant cost savings both in the initial installation and subsequent technology upgrade of the DCS platform in nuclear. This ultimately enables the utility to consider the DCS platform more as a commodity product serviced by the vendor. This matches the model for DCS platform utilization in non-nuclear industries.

This in no way diminishes the required testing of individual applications (e.g. function specific control applications and HMI displays) that are created to enable plant specific control and monitoring capabilities. The same is true for any DCS platform customizations that would place the DCS configuration outside the boundaries of the vendor established design and test envelope. In fact, this approach focuses design and testing activities precisely in these areas, which represent the predominant mode for design errors to impact control and monitoring functional performance. This also matches the model for DCS platform utilization in non-nuclear industries.

6.4 Enabling an Optimal Utility/Vendor Organizational Structure by Modifying Processes to Leverage Vendor Capabilities

6.4.1 Optimizing Utility/Vendor Organization Structures

Section 5.3, identifies that a decision is needed with regard to whether the utility or vendor possesses integrated operations knowledge of both the plant and the DCS. This ultimately determines which organization guides DCS technology upgrades. The driver for making this decision is the need to optimize resource utilization for the upgrades to achieve success.

Deciding the degree of vendor utilization is important because it impacts the cost of providing the necessary DCS supported control functionality for the duration of the functional life of the plant. If the resources of the vendor are appropriately utilized, they can drive down the costs and increase the productivity of plant staff. The vendor can provide both the technical knowledge of the DCS as it evolves over time and become knowledgeable of plant operational characteristics and utility change processes that would traditionally be maintained and kept entirely internal to the staff plant. This plant and process knowledge, while critical, is typically more static.

A very small number of vendor DCS expert personnel could be trained to become intimately knowledgeable of plant operating characteristics and utility engineering processes. These personnel could be located at the utility site (either at the plant or in a centralized engineering facility) or placed on call with pre-established response times (e.g. 2 hours) to reach the site. These vendor personnel would not only have extensive DCS knowledge, but they would have direct access to a deep bench of DCS SMEs to not only provide long term lifecycle support, but to address any emergent DCS performance issues. Vendor personnel would expand their knowledge to encompass much of the "integrated operations knowledge" area shown in Figure 12.

Such a model would reduce the expenditure of resources on training utility staff on the technical details of internal DCS operation and system troubleshooting techniques. In a utility centric support model, utility staff would have to maintain a level of DCS knowledge and proficiency for them to be capable to support ongoing operations and provide both near term (applying software patches) and long term (DCS technology migrations) lifecycle support activities without significant outside help. Due to the infrequency of DCS migration evolutions (every 7-10 years), it is difficult and costly for the plant staff to establish and maintain their knowledge and proficiency on the DCS platform. These time frames and the typical staff turnover which occurs during them would require an almost continual re-training cycle for utility staff to support migrations.

Going from a traditional internal utility I&C support model to one that is more vendor led is something that will occur over time as the utility establishes increasing confidence in the vendor. This transition is aided by utility personnel receiving initial training on the DCS platform (Section 6.2), performing audits of the vendor design and lifecycle support processes (Section 6.3), and gaining operational experience with the DCS after it is installed.

6.4.2 Optimizing Utility Processes to Enable the Optimal Organizational Structure

The traditional, linear, nuclear utility Engineering Change (EC) process has evolved over time to address issues associated with digital I&C modernization. The rate of evolution, however, has not addressed the revolutionary nature of digital I&C technology changes. Many EC procedure changes that have been identified by specific events and organizational lessons learned have been implemented in a piecewise manner. While each individual change may have merit, when viewed in the aggregate over time they tend to create an overly complicated composite set of EC procedures. This makes it difficult to efficiently deploy large I&C system modifications particularly when they provide something more than a like-for-like replacement of function. Use of the industry recognized Agile development process as described for the pilot DCS implementation in Section 3.1.3, while not prohibited by current EC procedures, is more difficult to explain and document within a traditional linear EC procedural model. Finally, utility EC processes can be challenging when trying to leverage vendor processes to specify, design, implement, factory test, deploy, and validate digital system functionality. These vendor processes are now more robust and application/industry specific than in the past. When deploying and updating a modern DCS, applying traditional utility EC processes tends to drive a utility to repeat, at significant cost, the exhaustive vendor DCS platform design and test program.

Utility procedures for digital I&C engineering modifications need to be critically evaluated with the objective of eliminating steps that are non-value added and/or not required by regulation. If steps are required by regulation, methods to address them by referencing vendor processes that meet industry standards need to be identified.

Utility procedures also need to be streamlined to permit non-nuclear I&C vendor employees to more directly perform work on plant I&C systems while meeting regulatory requirements.

7. Conclusion

This research presents advancements that have been made by non-nuclear I&C OT vendors and savings that could be realized by their optimized application in the nuclear industry. It identifies techniques for nuclear utilities to leverage vendor processes and experience to minimize utility costs for initial DCS deployment as well as for periodic technology migrations that address obsolescence. Application of these techniques will aid utilities in overcoming the institutional inertia impeding the large-scale implementation of digital technology in the nuclear industry. Key attributes required to accomplish technology migrations at minimum cost include leveraging vendor developed processes while at the same time protecting past intellectual property investments. Proper application of these techniques maximizes the benefits of expanded use of DCSs as part of a larger plant strategy to eliminate obsolete I&C systems, reduce O&M costs, improve operational performance, and maximize personnel utilization through digitalization. Modification of current industry processes and procedures to leverage vendor tools and techniques will further minimize utility costs.

Methods to accomplish technology migrations of the DCS are highly developed and employed in non-nuclear critical infrastructure. These methods are provided as part of the vendor's self-funded product lifecycle support strategy. In fact, technology migration of DCS Supervisory Network hardware, software and Control Network firmware with the nuclear plant at power (on-process) is not, in and of itself, an overly risky activity. The method to perform on-process migrations as presented herein is well defined and has been successfully implemented in non-nuclear critical infrastructure. By enabling on-process migrations in nuclear, it is possible to decouple non-safety DCS technology migrations and other system changes from outages. Significant efficiencies can be achieved by performing these upgrades in non-outage periods. Planning and execution of these upgrades outside of outage periods also reduces outage risk and enables performing other work that may require an outage that could not otherwise be supported.

The pilot utility's experience in deploying a modern non-safety DCS demonstrates that by using innovative techniques and leveraging vendor experience, modern I&C technology used outside of the nuclear industry can successfully be installed in nuclear plants and incorporated into their simulators. Efforts performed during this activity, such as utility training on the vendor system, performing vendor audits, and performing analyses such as a FMEA and a SHA helped validate deployment of this technology in nuclear. These efforts, along with effective utility and vendor teaming, built confidence and enabled the initial implementation. These efforts are foundational and must be sustained to enable subsequent technology migrations.

Increasing nuclear industry confidence in leveraging I&C vendor techniques and resources over time can drive organizational changes that further reduce overall I&C lifecycle support costs and support the long-term economic viability of nuclear power.

8. References

1. Paul Hunton, Charles Kiplin Smith, and Jason Watts, "Fleet Digital Upgrade Program and Control Room Modernization," Duke Energy, 2018, *Proceedings of the Eleventh American Nuclear Society International Topical on Nuclear Plant Instrumentation, Controls and Human-Machine Interface Technologies (NPIC & HMIT 2019).* American Nuclear Society (2019)
2. Code of Federal Regulations, Section 10, Part 50.59, "Changes, Tests, and Experiments," Nuclear Regulatory Commission.
3. NUREG-0711, Rev. 2, "Human Factors Engineering Program Review Model", Nuclear Regulatory Commission (2004).
4. Code of Federal Regulations, Section 10, Part 73.54, "Protection of Digital Computer and Communications Systems and Networks," Nuclear Regulatory Commission.
5. Paul Hunton, "Honeywell Quick Hits Assessment," Document #G-MPJ-SA-14-14, Duke Energy, November 26, 2014
6. Paul Hunton and Charles Kiplin Smith, "Software Hazard Analysis for Distributed Instrumentation and Control System Platform (DICSP) using Honeywell Experion® PKS (Release 410) and Associated Infrastructure Hardware," Document NED-I/INST-1004, Rev. 0, Duke Energy
7. Neil Archambo, "Failure Modes and Effects and Single Failure Analysis for Honeywell Experion PKS (Release 410.2) and Associated Infrastructure Hardware," Document NED-I/INST-1003, Rev. 0, Duke Energy
8. NEI 08-09 Rev. 6, "Cyber Security Plan for Nuclear Reactors," Nuclear Energy Institute, April 2010
9. NEI 13-10 Rev. 4, "Cyber Security Control Assessments," Nuclear Energy Institute, November 2015
10. 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
11. NUREG-0847, Supplement 23, "Safety Evaluation Report Related to the Operation of Watts Bar Nuclear Plant, Unit 2," July 2011
12. Per Øivind Braarud, Håkan Svengren, "A Graded Approach to the Human Factors Validation of Turbine Control System Digital Upgrade and Control Room Modernization," Institute for Energy Technology, 2018, *Proceedings of the Eleventh American Nuclear Society International Topical on Nuclear Plant Instrumentation, Controls and Human-Machine Interface Technologies (NPIC & HMIT 2019).* American Nuclear Society (2019)
13. J. Joe, R. Boring, T. Ulrich, and L. Hanes, "Development of a Fleet-Level Human Factors Engineering Program and its Use to Support the Digital Modernization of Multiple Turbine Control Systems," Idaho National Laboratory, 2018, *Proceedings of the Eleventh American Nuclear Society International Topical on Nuclear Plant Instrumentation, Controls and Human-Machine Interface Technologies (NPIC & HMIT 2019).* American Nuclear Society (2019)
14. M. Gibson, "Digital Engineering Guide, Decision Making Using Systems Engineering," Electric Power Research Institute, October 2018, document number 3002011816

Appendix A.
Detailed Virtual Migration Explained

This appendix discusses the steps for a generic, on-process software migration of a virtualized DCS Supervisory Network and related firmware updates to the Control Network. It is required that virtualized Servers as well as physical Controllers and I/O modules be in a redundant configuration for on-process migration. This description is based on using the host DCS hardware throughout the entire process. No hardware is migrated in this example. Control of the processes serviced by the DCS is not impacted during the migration described.

A stable system as shown in Figure 14 is the starting point as established by ensuring all vendor specified pre-migration activities as described in Section 5.1 are complete.

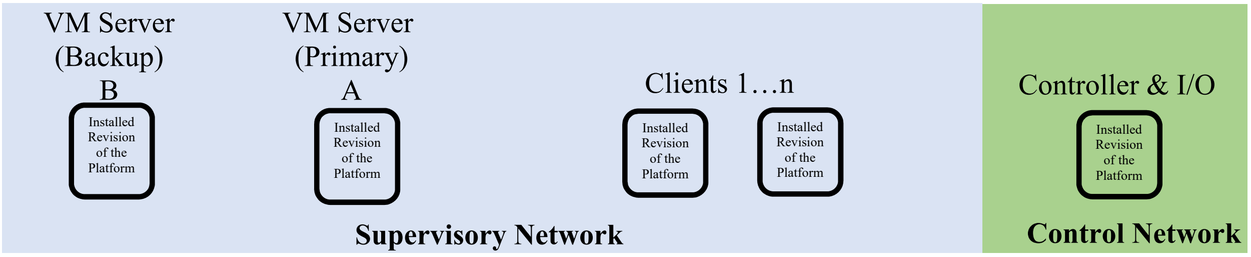

VM Server (Backup) B
Installed Revision of the Platform
VM Server (Primary) A
Installed Revision of the Platform
Clients 1…n
Installed Revision of the Platform
Installed Revision of the Platform
Controller & I/O
Installed Revision of the Platform
Supervisory Network
Control Network

Figure 14. Base System Diagram

Step 1: Server Pair Synchronization

The redundant DCS VM server pair must be synchronized to ensure that Server A reflects the same configuration as Server B, where the server migration will start. All clients will be connected to Server A for continuing production operations.

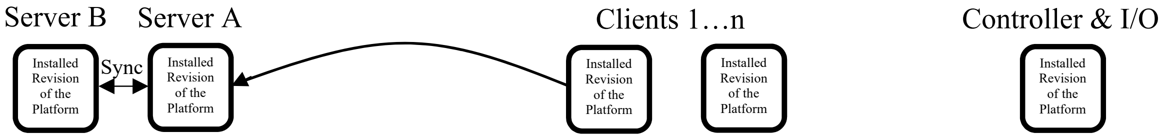

Server B
Server A
Installed Revision of the Platform
Sync
Installed Revision of the Platform
Clients 1…n
Installed Revision of the Platform
Installed Revision of the Platform
Controller & I/O
Installed Revision of the Platform

Figure 15. Step 1: Synchronization of Configurations Between Servers is Performed and All Clients are Connected to Server A.

Step 2: Copying Server Configuration to Backup Storage

Backup storage of some type must be established on the Supervisory Network. This will retain the end user configuration / database. In step 2, the customer configuration is copied from Server B and stored on the backup storage.

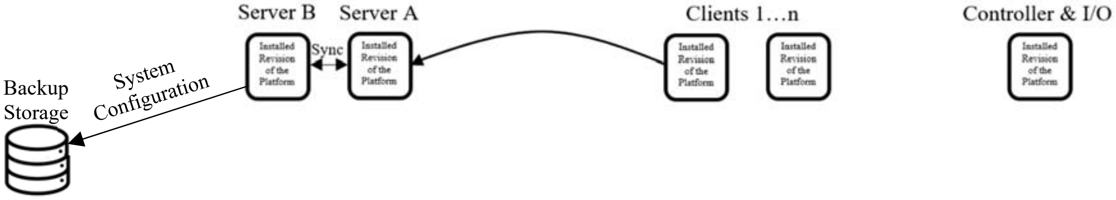

Server B
Server A
Installed Revision of the Platform
Sync
Installed Revision of the Platform
Clients 1…n
Installed Revision of the Platform
Installed Revision of the Platform
Controller & I/O
Installed Revision of the Platform
Backup Storage
System Configuration

Figure 16. Step 2: System Configuration is Backed-Up for Installation on the Updated Platform.

Step 3: Connecting the Installation Media and installation of the Updated Revision of the Platform

Installation media must be connected on the Supervisory Network. This stores the installation files and allows the installation to be faster since both USB and network are many times faster than installing from a DVD. In step 3 updated revision of the platform is installed on Server B.

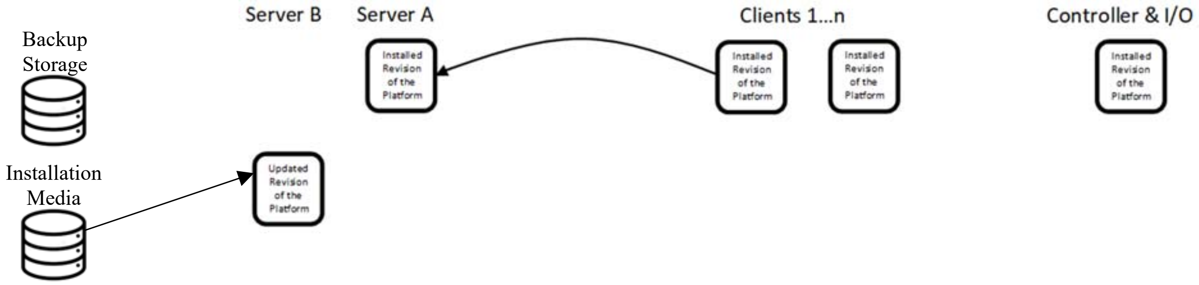

Server B
Server A
Clients 1...n
Controller & I/O
Backup Storage
Installation Media
Installed Revision of the Platform
Installed Revision of the Platform
Installed Revision of the Platform
Installed Revision of the Platform
Updated Revision of the Platform

Figure 17. Step 3: Server B is Updated to the Current Revision.

Step 4: Re-loading the End User Configurations onto the Updated Server B

Remember, that while this is happening the production system is still controlling the process, running on the installed revision of the platform on Server A. Once the updated revision of the platform software has been installed, it is time to load the end user configuration (e.g. DCS Client VMs) to the updated Server B.

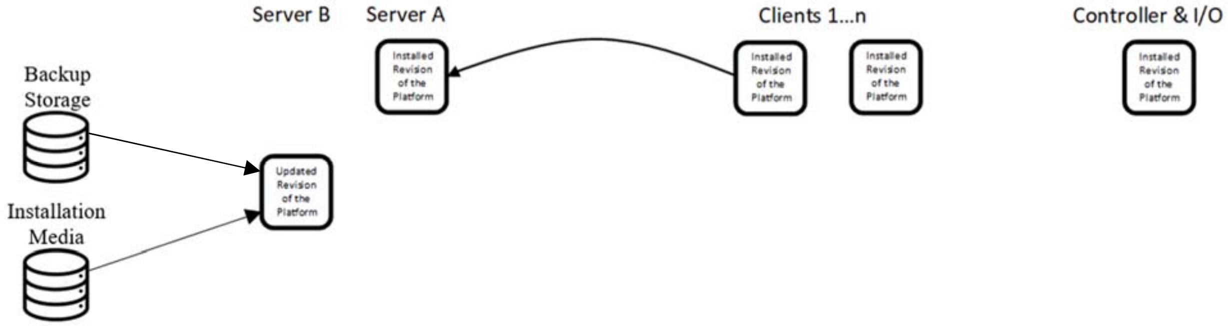

Server B
Server A
Clients 1...n
Controller & I/O
Backup Storage
Installation Media
Installed Revision of the Platform
Installed Revision of the Platform
Installed Revision of the Platform
Installed Revision of the Platform
Updated Revision of the Platform

Figure 18. Step 4: End User Configuration is Re-installed on Server B.

Step 5: Dual Primary Mode is Established; First Client is Migrated; Operational Status Verified

Now that Server B is running the updated revision of the platform and has the end user configuration, the DCS is now placed in a "dual primary" mode. This means that Server A is running on original revision of the platform that existed before migration began and Server B is running on the updated revision. These two servers are running in parallel. Both have access to all DCS processes. Control actions performed from Server B and the first related DCS Client VM that has been updated can be observed from Server A and pre-update versions of first DCS Client VM. This allows check out the upgraded software and comparison the operations of that upgraded software with the previous revision. This check out should start when the first Client VM is moved to the new release. If there is an issue with the Server B and DCS Client VM update, Server B and its Client VM can be taken off-process with no impact on DCS performance. The original configuration of Server B and its Client VMs can be restored to its pre-migration state if desired.

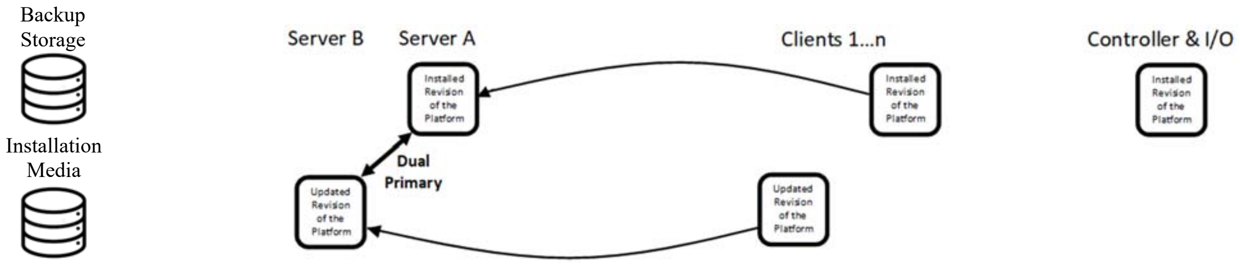

Backup Storage
Installation Media
Server B
Server A
Clients 1...n
Controller & I/O
Installed Revision of the Platform
Installed Revision of the Platform
Installed Revision of the Platform
Dual Primary
Updated Revision of the Platform
Updated Revision of the Platform

Figure 19. Step 5: First VM Client is Updated and Moved to the Updated Server for Testing.

Step 6: Remaining Clients are Migrated to Updated Server B

Once the configuration of the updated Server B and its first VM Client have been through the checkout and testing process and the control strategies and graphics have been confirmed to operate as intended, the remaining VM Clients can be updated and loaded onto Server B.

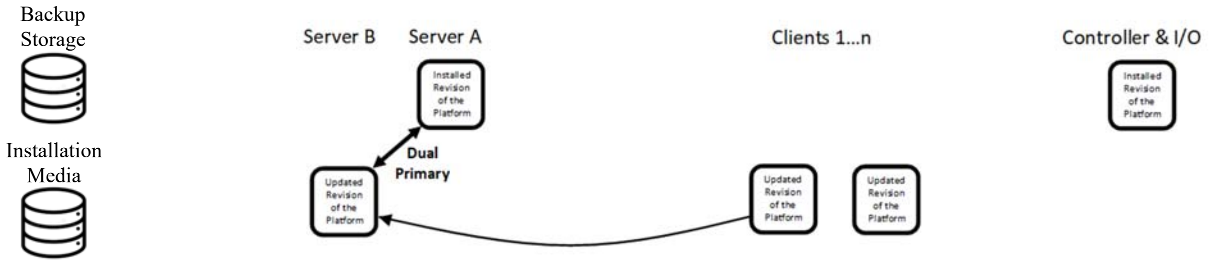

Backup Storage
Installation Media
Server B
Server A
Clients 1...n
Controller & I/O
Installed Revision of the Platform
Installed Revision of the Platform
Dual Primary
Updated Revision of the Platform
Updated Revision of the Platform
Updated Revision of the Platform

Figure 20. Step 6: Remaining Clients are Moved to the Updated Server.

Step 7: Server A is Updated to the New Revision of the Platform and End User Configurations are Restored (A State of Full Server Redundancy is Re-established)

Once all clients are upgraded to the new revision, full server redundancy is re-established by upgrading the Server A to the new revision.

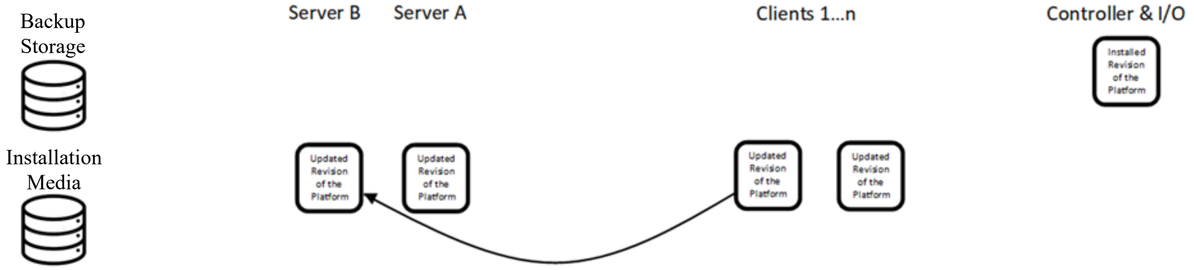

Backup Storage
Installation Media
Server B
Server A
Clients 1...n
Controller & I/O
Installed Revision of the Platform
Updated Revision of the Platform
Updated Revision of the Platform
Updated Revision of the Platform
Updated Revision of the Platform

Figure 21. Step 7: Server A is Updated to Match Server B and Redundancy is Restored.

Step 8: Controller and I/O Firmware is Updated

When the VM upgrades to Server A and Server B are completed, their operation is then synchronized. Both are now running the updated revision of the platform servers as well as all the VM Clients. It is now time to upgrade the controller and I/O firmware. This is required only if there are desired features in the new release that are enabled in the controller by the firmware upgrade.

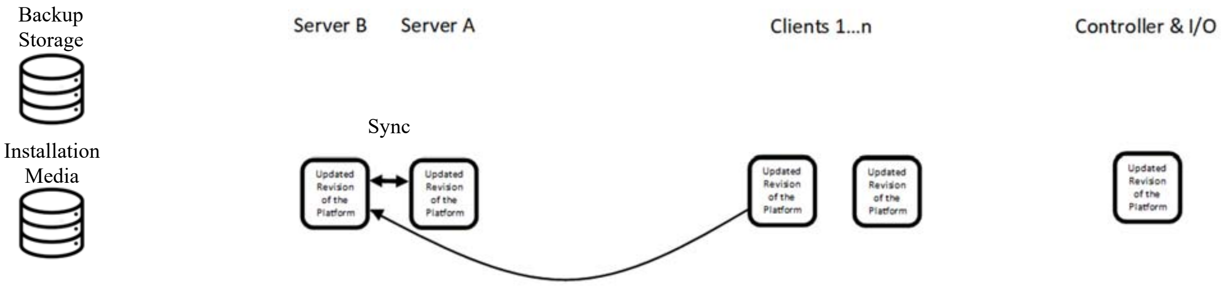

Backup Storage
Installation Media
Server B
Server A
Sync
Updated Revision of the Platform
Updated Revision of the Platform
Clients 1...n
Updated Revision of the Platform
Updated Revision of the Platform
Controller & I/O
Updated Revision of the Platform

Figure 22. Step 8: Servers are Synchronized, and Controllers are Updated (as needed).

Each of the two controllers in redundant control segment is updated one at a time by taking the backup controller offline, updating the firmware, placing it online, and updating the remaining controller. Once the controller firmware is updated, the redundant I/O module firmware is similarly updated. When all the controller and I/O firmware updates are complete, the DCS has been upgraded from a previous revision to the current revision. The DCS remained on-process during the entire upgrade evolution. Operation of process being monitored and controlled by the DCS was not impacted.

Appendix B.
Pilot Vendor Platform Lifecycle and Backwards Compatibility Management

Established control system vendors have come to recognize that the longevity of their platforms as well as its cross-generational compatibility make their products more attractive and useable for their customers. Firstly, they ensure that throughout the lifecycle of the platform there is support available to ensure the product lives up to the long-life expectations of the customers, which creates value within the platform for those customers. But as with all things, every product eventually becomes too old and outdated to actively maintain and support as a viable market product. When this point comes, it does require that every field-installed piece of outdated equipment or software needs to be replaced with a new product. This would require customers to incur great costs much more regularly than should be the case. At this point, backwards compatibility of the system becomes a vital characteristic. System backwards compatibility allows users to continue using functional products long after the technical, vendor-identified, end-of-life of the product.

This appendix discusses multiple key features of DCS platform lifecycle and backwards compatibility management:

- Supervisory Network Hardware and Software
- Control Network Hardware and Software

Information provided in this Appendix leverages the pilot DCS vendor's information for illustration. When evaluating any vendor for a DCS application, similar information to that presented below should be gathered and analyzed as part of the utility vendor select

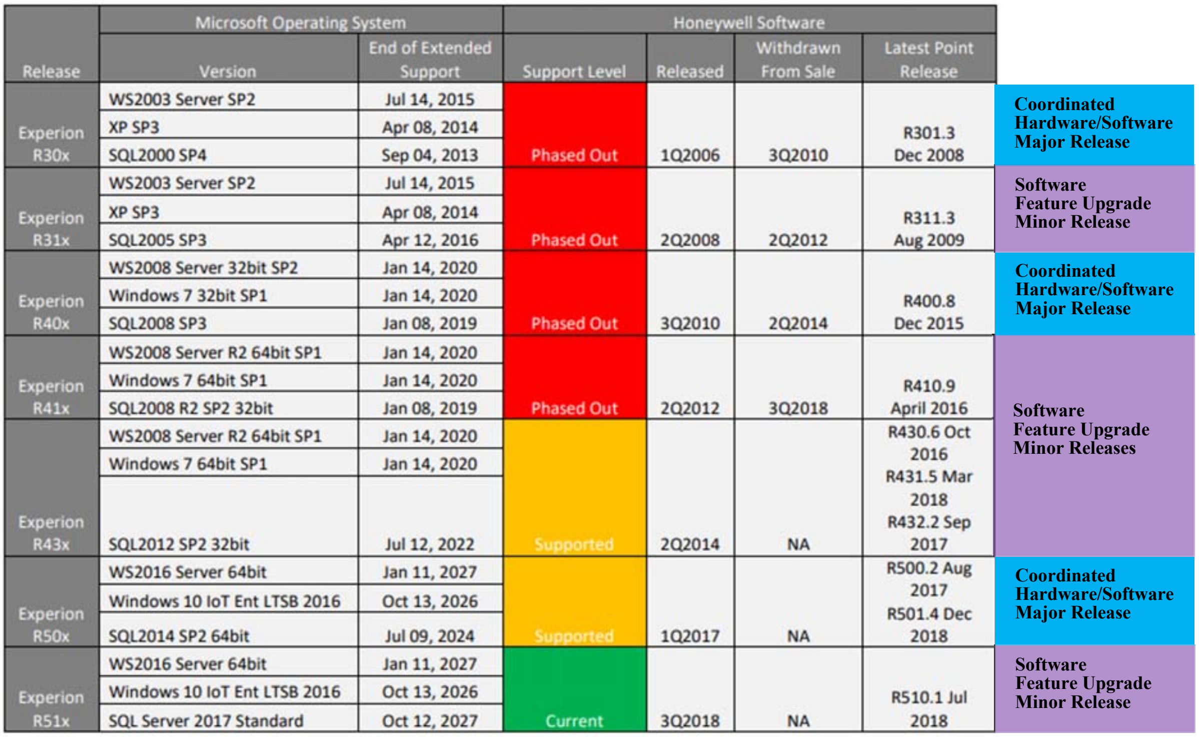
Supervisory Network Hardware & Software

Supervisory network hardware replacement is impacted by the manufacturing support of the piece parts that make up the hardware set in the DCS platform. Unexpected early discontinuance of IT platform hardware leveraged in OT environments can impact DCS major hardware/software release frequency. The predominant driver for hardware replacement, however, is software obsolescence. As hardware ages, key software running on the DCS (e.g. the Supervisory Network operating system, VM host software, etc.) is no longer supported by suppliers that provide them. Newer operating systems and other DCS software generally require newer hardware systems with more capabilities to operate most efficiently. New software such as this may not be compatible with legacy hardware. To use the latest DCS software on previous major release hardware would require testing by the DCS vendor to ensure compatibility. The investment required to perform this level of backwards compatibility at the Supervisory Network level on obsolete hardware is typically not economically justifiable from the DCS vendor perspective.

Generally, DCS vendors coordinate DCS Supervisory Network hardware upgrade to coincide with major platform software migrations to maximize the lifespan of their integrated product set. Customers can reduce the frequency of their DCS Supervisory Network upgrades (and extend the time between upgrades) by synchronizing their upgrade schedule with the DCS vendor's major hardware/software product releases.

For the pilot vendor examined for this research, the coordinated hardware/software upgrades are identified in blue at the far right of Table 1. 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 1. Honeywell Experion® Release History.



Release	Microsoft Operating System		Honeywell Software				
	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					

Note the following:

- The Honeywell-coordinated hardware/software major releases occur after Microsoft operating system releases. There is a time lag between Microsoft releases and Honeywell Experion releases. The time lag is getting shorter over time. This is due in part because of the supplier/vendor relationship Microsoft and Honeywell have established.
- The “withdraw from sale” Honeywell software dates occur approximately 5 years before the Microsoft operating system “end of extended support” dates. This gives the coordinated hardware/software major release a term of operating system extended support for a period from 8 to 9 years after initial release.
- Each new coordinated hardware/software major release occurs approximately 5 years. The period between the last two coordinated hardware/software major releases was just over 6 years

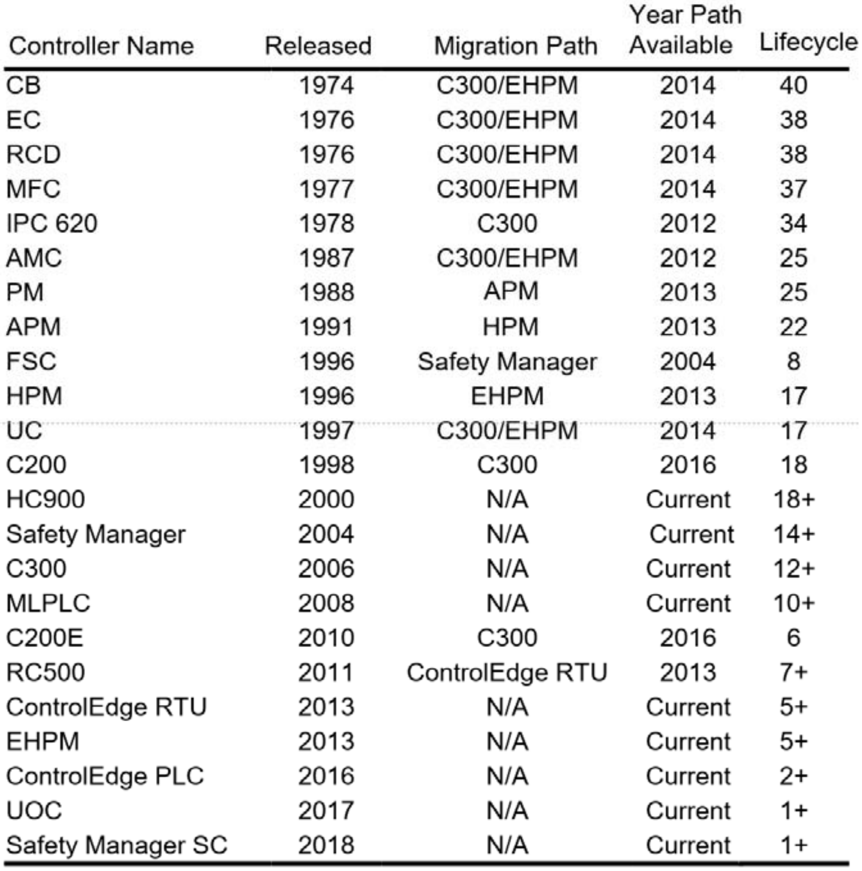
The overlap between the Microsoft operating system end of extended support dates and coordinated hardware/software major releases allows maintaining full operating system support, while establishing a regular hardware/software upgrade period of approximately 7 to 8 years.

Interim software upgrades can be more fluid and seamless. These upgrades typically provide interim functionality improvements (new features) so the vendor can stay competitive in the industry between major system upgrades. These are shown in purple at the far right of Table 1. These software updates can also be installed on-process, maintaining process operation at full functionality as discussed in Section 5. Unless these new features provide an operational/economic benefit that can justify the effort to perform an interim upgrade before the next major release (where they will be provided as a matter of course), it would be expected that a nuclear utility would not implement interim software functionality upgrades.

Control Network Hardware & Software

Table 2 below lists the controller products supplied to industry by the pilot DCS vendor from 1974 to present. The controller name acronyms presented in the table are not of particular significance. What is significant in Table 2 is the information contained in the “Lifecycle” and “Migration Path” columns.

Table 2. Pilot Vendor Support for Control Network 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+
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 40+ years ago, the pilot vendor has retained both backwards compatibility to their current DCS Control Network products and a path to harvest the intellectual property in them when replacements for obsolete hardware cannot be obtained. For example, control algorithms in the Basic Controller (CB) released as part of the world’s first DCS (TDC 2000) in 1975 can be migrated into their latest DCS using vendor-validated techniques. For all current controllers, their lifecycles are planned to be at least 20 years. For those controllers:

- The design approach is to have a migration path to next controller (as demonstrated for all legacy products shown in Table 2
- On-process migration of redundant controllers is typical
- Preservation of customer intellectual property is typical
- Preservation of I/O is typical.

For current products, such as the C300 controller and ControlEdge products (and related I/O modules for both), all future DCS product releases are planned to be backward compatible to these without requiring firmware upgrades to this Control Network hardware.

If a controller is transitioned to “legacy” status = no longer produced, Honeywell policy states:

- Customers will receive 1-year notice before going to legacy status

- 10 years of support will be provided after the controller goes to legacy status

A total of 11 years of support will be provided after initial notification. This, combined with providing a migration path for intellectual property transfer from this controller to a current product as discussed above, provides ample time to establish a plan to migrate to current controller product as obsolescence dictates.

Appendix C.
Pilot Vendor Support Capabilities to Reduce Total Cost of Ownership

In order to provide cost reliability and predictability, vendors engage in support activities. They work very hard to ensure that their products are not subject to itinerant failures and that they have proven, long-lived, and technically supported product (hardware and software). Some vendors take this a step further and offer DCS customers with lifecycle support services to enhance cost reliability and predictability as terms and conditions of their customer contracts. In this way, the control system vendor can be rewarded when performance conditions are met and held responsible if failures occur outside of the predicted frequencies or timeframes.

Information provided in this Appendix leverages the pilot DCS vendor's information on this topic for illustration. When evaluating any vendor for a DCS application, similar information to that presented below should be gathered and analyzed as part of the utility vendor selection process.

Honeywell Lifecycle Management

Honeywell Lifecycle Management (LCM) is an example of one such vendor contracting mechanism. Honeywell LCM is a multi-year service agreement based on a user site strategy that provides DCS support for Honeywell hardware and software until they are upgraded. It is flexible enough to adapt to users' schedule of automation/modernization and is ideal for long-term automation planning (>=3 years). Benefits of leveraging LCM include:

- Extending the life of assets through a cost-effective means to support the control system's physical and intellectual assets, providing incremental upgrades, as well as guaranteed hardware support on installed Honeywell products.
- Reducing the unpredictability & risk by funding migrations and upgrades over multiple years, predicting support costs for spare parts and upgrade kits and financing options that spread costs and keep cash flow predictable and positive.
- Addressing current needs and future demands flexibly with the benefit from Experion® entitlements and a planned approach to users' support and upgrade investments.

Honeywell Assurance 360

Some automation vendors have realized that total cost of ownership and creating a lasting value in the control system is important to operators of these systems. One example of an automation vendor's solution to creating this lasting value and relationship with customers is Honeywell's Assurance 360 offering. Assurance 360 builds on the foundation established by LCM. Through Assurance 360, Honeywell provides agreed service levels rather than prescribed quantities of materials and labor, takes a strategic view to minimize asset ownership costs, guarantees performance, and uses automation to improve business outcomes. The results are predictable operating expenses and capital expenditures; greater system stability, reliability and quality; and optimized total cost of ownership. Benefits of leveraging Assurance 360 include:

Integrated Automation Assessments - Industrial organizations can identify their specific migration needs and opportunities with a Honeywell supplied Integrated Automation Assessment. The assessment provides a report on the system configuration based on Honeywell best practices, a security summary on security performance, a lifecycle summary on supported hardware and software revisions, and, finally, a synopsis on overall asset performance.

System Performance Analyzer (SPA) - A powerful software tool designed for and included only in premium support programs. It continuously monitors control applications, DCS system performance and capacity functions in real time to provide early warnings and notifications of potential issues. The tool addresses factors such as central processing unit (CPU) health, controller loading, memory, and network traffic on a 24/7 basis. With this solution, users gain insights to help minimize the frequency and impact of any degraded control system performance.

Remote Preventive Maintenance - Will provide customers with proactive alerting, actionable insights and consistent quality of delivered services. This allows the onsite field service staff to focus and execute higher-value activities, increase key resource availability, and increase productivity. It also enables Honeywell to bring the best qualified SMEs to bear on a task, irrespective of where they are physically located.

Premium Support Center - Honeywell has established a global support center to deliver comprehensive assistance to customers participating in its premium support program. Honeywell SMEs are tasked with monitoring control system health and making performance improvement recommendations utilizing the advanced, cloud-based predictive analytics with the SPA solution.

Cyber Security Managed Services - With Assurance 360 services, a remotely managed security services team is available to perform control system audits to identify a wide range of cyber security vulnerabilities. This includes penetration testing and other services to help customers detect and mitigate ever-evolving cyber threats to their automation assets.

Assurance 360 Performa – Improved Automation Competency and Expertise - Honeywell Assurance 360 Performa addresses today's skills shortage, helping industrial firms maintain automation assets that are crucial to meeting production goals. With Assurance 360 Performa:

- Collaborates with internal staff to develop valuable knowhow and augment the workforce to tackle resource challenges, and helps build competencies and sustain expertise within an organization through best practices in automation support, which are tracked by outcome-based metrics
- Cultivates knowledge and skills within your organization via 24x7access to Honeywell specialists
- Manages the complete asset lifecycle by keeping control hardware and software up to date
- Delivers competent resources to complement your workforce
- Implements Performance Management to provide a Honeywell focal point, report on system performance, recommend maintenance improvements, coordinate Honeywell activities, and act as a customer advocate within Honeywell
- Provides continuous system monitoring with alerts to incidents and data diagnosis for reporting, availability, capacity and problem management
- Performs system audits to identify automation and cyber vulnerabilities and "Stable Platform" remediation requirements
- Delivers cost certainty through an outcome-based model.

Assurance 360 Optima– Guaranteed Performance and Operational Benefits - Assurance 360 Optima delivers agreed service levels in system support, maintenance, optimization and change management with guaranteed results. As a strategic partner, Honeywell is responsible for providing the resources you need to achieve defined outcomes, with payment adjusted to the results attained:

- Ensures support accountability through continuous scoring of service level attainment and a fee-adjusted schedule
- Guarantees against loss of view or control events through payment penalties, and over-and-above fee adjustments from other service level measurements
- Delivers cost certainty through an outcome-based model
- Offers preventative maintenance based on best practices
- Provides continuous system monitoring with alerts to incidents and data diagnosis for reporting, availability, capacity and problem management

- Performs system audits to identify automation and cyber vulnerabilities and “Stable Platform” remediation requirements
- Implements Performance Management to provide a Honeywell focal point, report on system performance, recommend maintenance improvements, coordinate Honeywell activities, and act as a customer advocate within Honeywell.

Appendix D.
Pilot Vendor History and Design Processes

Leveraging a vendor with global market penetration and wide acceptance of their products spreads the vendor's DCS development cost operating experience base across a myriad of different industries and applications. This economy of scale and competitive business environment drives down DCS utility costs. It also improves quality. Lessons learned from millions of runtime hours over decades are incorporated into an evolving product line to drive improved performance and reduced system operational issues. It is in the vendor's best interest to establish quality practices not only as a method to adhere to industry standards, but to demonstrate to customers the commitment to maintain and improve system performance and reliability. By selecting a vendor that is large, stable, experienced, widely used outside of nuclear, and with a reputation for producing quality product and supporting it for decades enables leveraging all of these attributes without having to have contributed to the investment to create them. It also minimizes implementation risk.

Information provided in this Appendix leverages the pilot DCS vendor's information on this topic for illustration. When evaluating any vendor for a DCS application, similar information to that presented below should be gathered and analyzed as part of the utility vendor selection process.

Honeywell Background and Experion® PKS (EPKS) development History

Honeywell is a Fortune 100 diversified technology and manufacturing leader, serving customers worldwide with aerospace products and services, control technologies for buildings, homes and industry, turbochargers, and performance materials.

Honeywell has been serving the industrial automation industry since 1934. Honeywell Process Solutions (HPS), a business unit of Honeywell International, has pioneered process automation control technology. HPS currently has over 11,000 employees in 120 countries servicing industrial customers in the oil and gas, refining, pulp and paper, industrial power generation, chemicals and petrochemicals, biofuels, life sciences, and metals, mining, and minerals industries.

HPS helps industrial customers around the world operate safe, reliable, efficient, sustainable, and more profitable facilities. HPS offers leading control system technologies and comprehensive lifecycle services that help to ensure more productive and stable operations. As one of the industry's leading automation equipment suppliers, Honeywell has an established track record in supporting its control system installed base worldwide. After its introduction of the first-generation distributed control system in the 1970s, the company has followed a consistent support strategy, which includes integration of its older-generation control system functions within the more recent ones.

In the 1990s, the industrial market demanded what was termed "open systems" for industrial control systems. The concept was to leverage open operating systems like Microsoft Windows infrastructure that would allow the use of "best-in-class" applications and deliver the supervisory level of the control system on personal computers to remove the high cost of proprietary hardware. At that time, HPS was delivering the number one control system in the industry, which had a proprietary operating system as well as hardware. HPS had already recognized the market trend and had developed an open system for the upstream oil and gas market as well as batch applications. This system was called PlantScape.

HPS launched a development program to take the learnings of the proprietary system, called TDC3000, and incorporate those into PlantScape. In parallel to this activity, HPS began integrating "open platforms" with TDC3000. This new system with the open systems integrated at the supervisory level was called TotalPlant™ Solution (TPS). TPS gave the installed base of customers the opportunity to leverage the benefits of "open systems," while protecting their intellectual investments in control strategies.

In 2003, HPS launched Experion® Process Knowledge System (EPKS). EPKS is Honeywell's flagship control system in today's market. EPKS evolved from all the experience gained from the proprietary systems applied now to an "open system," and also maintained all of the features that were present as

PlantScape. EPKS represents a natural blend of TDC, TPS and PlantScape to deliver a system that meets the requirements for most processes in open yet secure way. Because Honeywell maintains the philosophy of "Continuous Evolution," all of this work was done in a way to protect the customer's intellectual and capital investments. A customer would only have to develop a control strategy once while enjoying continuous updates and enhancements of their control system. As a differentiator in the market, these technologies were developed to be updated without having to shut down the process. This is unique in the industry.

EPKS was developed from control systems that have led the market for 40 years and has been done in a way that protects the intellectual investments of installed customers over the lifecycle of their business. EPKS is designed to control the most difficult processes in the world; it is used on some of the largest manufacturing sites in the world and continues to represent the "state of the art" for industrial control systems.

EPKS can integrate and run on top of systems that were delivered over 40 years ago, preserving the customer's investment in those control strategies while enjoying the benefits of 21st century technologies. Over 8000 Experion systems are installed in 4000 sites in 110 countries around the world in every major industry that Honeywell serves.

Honeywell has a strong commitment to protecting its customers' automation investments while they take advantage of the latest innovations. Many users today have multiple generations of Honeywell technology working seamlessly side-by-side at a single site, spanning controllers and other TDC2000 equipment dating from 1974 to the latest EPKS operator stations.

Honeywell's migration solutions are specifically designed to provide industrial organizations with access to up-to-date automation technology without having to "rip and replace" their entire legacy hardware and software system. Honeywell also provides guidance for both short- and long-term projects. HPS migration specialists work with the end user to develop a comprehensive automation vision to keep pace with future needs.

Experion PKS Technologies

EPKS uses a mixture of Honeywell-developed EPKS platform specific technologies as well as generic commercial hardware and software technologies to provide overall EPKS functionality.

EPKS platform specific technologies developed by Honeywell are focused primarily on the direct process control functions of EPKS. These technologies provide a set of building blocks for hardware, software elements, and development tools that serve as the foundation for the system's control and monitoring functions. Examples of these EPKS specific technologies include:

- The hardware modules interfacing with field devices
- The software tools used to program the customized application software
- The EPKS software providing the user interfaces to the workstations.

These technologies make up the basic functionality of a DCS platform at Network Level 1 (Control Network) and the Human System Interface portion of Network Level 2 (Supervisory Network and Operator Interface).

Because these EPKS Platform specific technologies are provided by a single vendor (Honeywell), they are a potential source of a CCF. Honeywell designed and implemented EPKS platform-specific technologies for this specific purpose, subjecting them to an extensive, customized testing program. This ensures EPKS platform-specific technologies function correctly within the DCS environment. Generic commercial technologies employed by EPKS are primarily computers and networking components/software designed for general-purpose use.

Generic commercial technologies provide more typical information technology functions such as mass data transfer, mass data storage, virtualization to minimize the need for dedicated hardware, and graphical user interfaces. Generic commercial technologies are not specifically designed for control and monitoring system use. Industry standard technologies come from major hardware and software vendors such as Intel, Microsoft, IBM, Dell, and Cisco. These industry leaders have a reputation for providing high-quality products, services, and support.

Quality Assurance Measures Employed in Experion PKS Development

In Honeywell's 80 years of experience in meeting the industrial automation needs of customers, Honeywell has led the industry in assuring their products are of the highest quality. Honeywell's practice is to design, develop, test, and maintain their products using a formal, auditable, Quality Management System (QMS) based upon internationally accepted standards. Honeywell development teams contributing to the EPKS use both ISO 9000 and Capability Maturity Model Integration (CMMI) Institute as measures of the quality of their software development practices.

The Honeywell QMS has been developed, maintained, and is certified in accordance with the requirements of ISO 9001:2008 and is defined/described in the HPS Global Quality Manual. HPS has also been appraised at the highest Maturity Level (5) by the CMMI Institute in the area of Software Development.

A Maturity Level 5 appraisal verifies Honeywell's quality and process performance objectives are established, continually revised to reflect changing business objectives and organizational performance and used as criteria in managing process improvement. The effects of deployed process improvements are measured using statistical and other quantitative techniques and compared to quality and process performance objectives. The project's defined processes, the organization's set of standard processes, and supporting technology are targets of measurable improvement activities.

An organization assessed at Maturity Level 5 is focused on managing and improving organizational performance. The organization is concerned with overall organizational performance using data collected from multiple projects. Analysis of the data identifies shortfalls or gaps in performance. These gaps are used to drive organizational process improvement that generates measurable improvement in performance. This assessment covers 22 process areas.

Software Version Control and Configuration Management

EPKS uses a mix of Honeywell-developed software products and standard commercial software products. These are integrated with commercially available hardware and Honeywell designed hardware and sold as major product releases.

Rules have been established by Honeywell regarding the types of changes allowed at each type of product release. For example, a point release is not allowed to introduce any:

- New functionality
- New operating system platform technology
- Major third-party technology/function changes (minor changes are allowed under specific circumstances)
- Initial introduction of a new product
- Changes to minimum hardware requirements from Series/Functional release
- Significant architectural/infrastructure changes
- Database structural changes
- Complex migration procedures (i.e., reformatting the system and requiring re-installing applications).

As presented above, a point release is a cumulative update of all patches and previous point releases. Necessary testing/analysis is performed by Honeywell on point releases to ensure the functional performance of systems on which the point releases will be implemented in industry will be unaffected other than to correct specific issues/anomalies as captured in the Product Anomaly Reporting System.

Consistency with the previous versions is further ensured by following a regression analysis process of each new EPKS release version received from Honeywell. This consists of reviewing the EPKS release documentation and validation analysis/testing of the modified or upgraded software release on an off-process set of equipment.

Configuration management of EPKS software releases is also closely controlled/maintained. Each EPKS software release is made up of a series of software "packages," which are bundled in a standard format. Each PKS software release package has a specific revision number, and all of the source code modules that make up the specific package version are recorded and documented as part of the software release infrastructure and process. Therefore, for any release version (such as Release 410.6), the specific source code modules making up the EPKS platform software contained in the system is established. The EPKS platform software version that is installed on EPKS can be verified.

The software release process and infrastructure tools in place at Honeywell ensure a software release at a certain major revision and patch level is unique and can be traced back into the configuration control information.

Product Anomaly Reporting System

The Honeywell Product Anomaly Reporting (PAR) System® is used for reporting problems with EPKS. The PAR System is used internally at Honeywell and is also used by EPKS users. Details regarding the PAR system are provided below.

A diagram depicting how potential anomalies with EPKS are addressed is provided in Figure 23 below. Steps to progress through the PAR process as shown in Figure 23 are numbered sequentially.

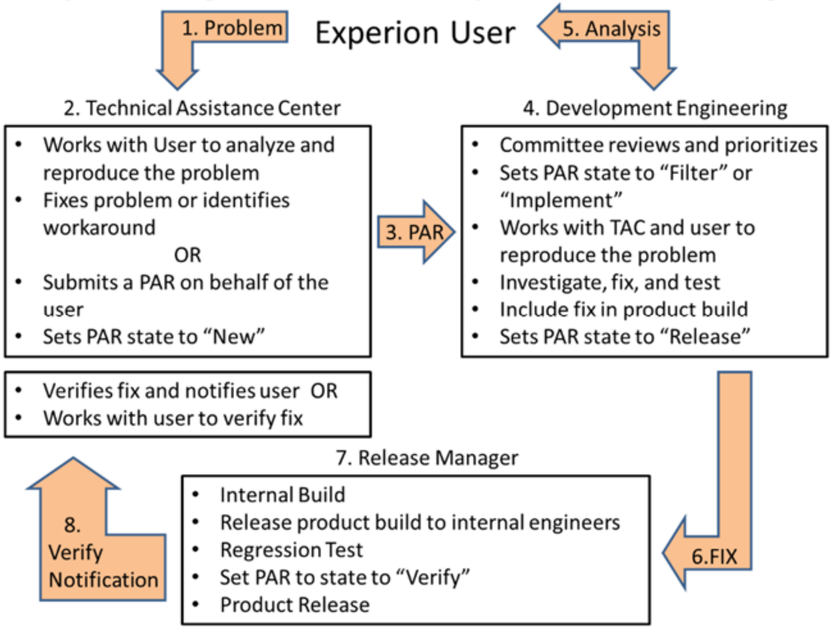

1. Problem
Experion User
5. Analysis
2. Technical Assistance Center
• Works with User to analyze and reproduce the problem
• Fixes problem or identifies workaround
OR
• Submits a PAR on behalf of the user
• Sets PAR state to "New"
3. PAR
4. Development Engineering
• Committee reviews and prioritizes
• Sets PAR state to "Filter" or "Implement"
• Works with TAC and user to reproduce the problem
• Investigate, fix, and test
• Include fix in product build
• Sets PAR state to "Release"
• Verifies fix and notifies user OR
• Works with user to verify fix
7. Release Manager
• Internal Build
• Release product build to internal engineers
• Regression Test
• Set PAR to state to "Verify"
• Product Release
8. Verify Notification
6.FIX

Figure 23. Pilot Vendor Product Anomaly Resolution Process.

In addition to the information presented above, additional activities occur during this process when it is determined a PAR is appropriate. These are depicted in Figure 24 below.

Figure 23 Step

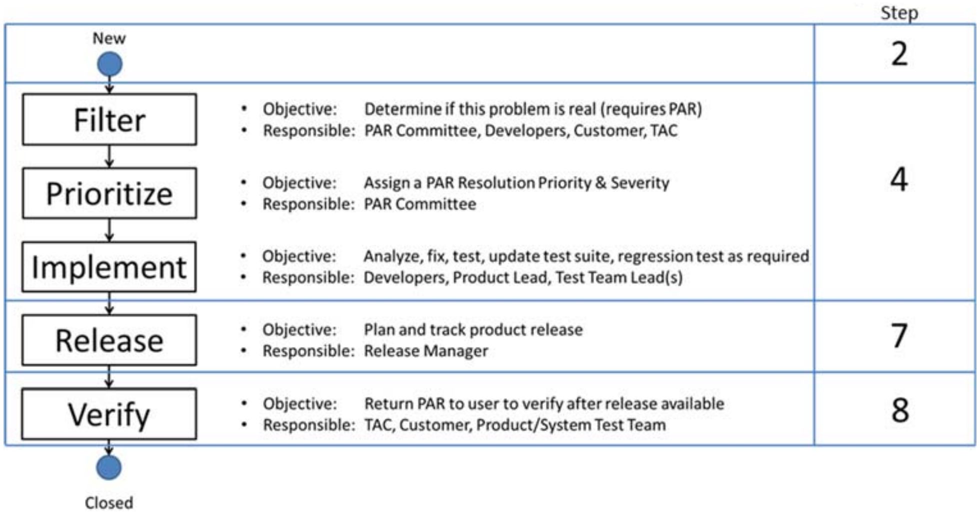

Step
New
2
Filter
• Objective: Determine if this problem is real (requires PAR)
• Responsible: PAR Committee, Developers, Customer, TAC
Prioritize
• Objective: Assign a PAR Resolution Priority & Severity
• Responsible: PAR Committee
4
Implement
• Objective: Analyze, fix, test, update test suite, regression test as required
• Responsible: Developers, Product Lead, Test Team Lead(s)
Release
• Objective: Plan and track product release
• Responsible: Release Manager
7
Verify
• Objective: Return PAR to user to verify after release available
• Responsible: TAC, Customer, Product/System Test Team
8
Closed

Figure 24. Product Anomaly Resolution Flow.

A key part of the Product Anomaly Resolution Flow shown in Figure 24 is determining the severity of the anomaly and assigning the priority to resolve the anomaly. PAR severity and resolution priority is assigned using a PAR assessment matrix. The Honeywell PAR process is configuration controlled and closely tracked.

Customers can view known product defects at a pre-established priority/severity level that have been addressed or remain open when each EPKS release occurs at the www.honeywellprocess.com support site. After registration on that website, customers can subscribe to automatically receive messages for specific products and releases. These messages include notifications of product issues (both Priority Notifications and Be Aware Notifications), software updates, and software patches (all of which are tracked as PARs). In addition to the automatic notification, customers can view all this information at the website. Customers can download patches, maintenance releases, and point releases uploaded at the support site according to their entitlements (e.g., Solutions Enhancement and Support Program –Value Plus support status) or by purchasing the service. Duke Energy in preparation for the installation of EPKS systems at multiple plants evaluated the PAR process as part of the EPKS QC/QA assessment [5].

Conclusion

The EPKS has a long and pedigreed development and operational history. Technology applied in EPKS is carefully selected based upon proven performance. EPKS has been developed leveraging control system industry recognized codes and standards to ensure quality. Software development processes used in its development have been certified by an industry recognized independent third party to be at the highest level of maturity. Software version control, configuration management, and lifecycle support has been established and maintained by the vendor. This includes a robust PAR system that is used to identify, screen, prioritize, and resolve product issues.