INL/EXT-17-43390

Operator-in-the-Loop Study for a Computerized Operator Support System (COSS) – Cross-System and System-Independent Evaluations

Thomas A. Ulrich, Roger Lew, Ronald L. Boring,
Kenneth D. Thomas, Brandon C. Rice,
Chris M. Poresky

September 2017

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

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, trade mark, 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-17-43390

Operator-in-the-Loop Study for a Computerized Operator Support System (COSS) – Cross-System and System-Independent Evaluations

Thomas A. Ulrich, Roger Lew, Ronald L. Boring,
Kenneth D. Thomas, Brandon C. Rice, Chris M. Poresky

September 2017

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

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

(This page intentionally left blank)

ABSTRACT

A Computerized Operator Support System (COSS) is an operator assistive technology that aids operators in monitoring processes to detect off-normal conditions, diagnose plant faults, predict future plant states, recommend mitigation alternatives, and select appropriate mitigation actions. The project was funded by the U.S. Department of Energy Office of Nuclear Energy and developed at Idaho National Laboratory. The COSS works in collaboration with an advanced prognostics system called PROAID developed at Argonne National Laboratory. The COSS provides a human-machine interface to help operators maintain situation awareness and detect faults earlier than would be possible using conventional control room technologies at nuclear power plants. This report represents a status update outlining third-year efforts to develop and validate the COSS. The COSS has now been implemented as a prototype system, with multiple interaction design concepts on multiple plant systems in the simulator from a commercial nuclear power plant. Two studies involving three licensed reactor crews were conducted to evaluate the COSS. This report captures insights into the development of COSS as well as operator feedback and future development guidance derived from the operator-in-the-loop simulator studies.

(This page intentionally left blank)

ACKNOWLEDGMENTS

Authors Roger Lew and Chris Poresky worked with Idaho National Laboratory courtesy of their home organizations of University of Idaho and University of California, Berkeley, respectively. The authors thank Suibel Schuppner, Program Mangager for the U.S. Department of Energy, and Bruce Hallbert, Idaho National Laboratory, for their support of this research through the Nuclear Energy Enabling Technology (NEET) Program. While this report centers on work completed primarily at Idaho National Laboratory, the overall research project would not have been possible without the close collaboration of Rick Vilim, Yu Tang, and Austin Grelle of Argonne National Laboratory. We acknowledge Casey Kovesdi and Kateryna Savchenko at Idaho National Laboratory, who helped run the operator studies documented in this report.

(This page intentionally left blank)

CONTENTS

FIGURES

TABLE

ACRONYMS

ANIME	Advanced Nuclear Interface Modeling Environment
ANL	Argonne National Laboratory
API	Advanced Programming Interface
CBP	Computer Based Procedure
COSS	Computerized Operator Support System
CRADA	Cooperative Research and Development Agreement
CRS	Control Room Supervisor
CVCS	Chemical and Volume Control System
DCS	Distributed Control System
DOE	Department of Energy
FDI	Fault Detection and Isolation
GONUKE	Guideline for Operational Nuclear Usability and Knowledge Elicitation
gPWR	Generic Pressurized Water Reactor
HSI	Human-System Interface
HSSL	Human Systems Simulation Laboratory
HUNTER	Human Unimodel for Nuclear Technology to Enhance Reliability
I&C	Instrumentation and Control
INL	Idaho National Laboratory
LWRS	Light Water Reactor Sustainability
NEET	Nuclear Energy Enabling Technology
NPP	Nuclear Power Plant
PBP	Paper Based Procedure
P&ID	Process and Instrumentation Diagram
PFD	Primary Flight Display
PLC	Programmable Logic Controller
PWR	Pressurized Water Reactor
RCS	Reactor Cooling System
RO	Reactor Operator
SCADA	Supervisory Control and Data Acquisition
SRO	Senior Reactor Operator
TCAS	Traffic Collision Avoidance System
TCS	Turbine Control System
TH	Thermo-Hydraulic
U.S.	United States
WPF	Microsoft’s Windows Presentation Foundation

(This page intentionally left blank)

1. INTRODUCTION

1.1 Computerized Operator Support System Research Project

This report represents the culmination of efforts from the third and final year of a project supported by the Nuclear Energy Enabling Technologies (NEET) Program focused on the design for fault tolerance and resilience. Specifically, the work described in this report aimed to develop a fully integrated operator-support system for demonstration including fault detection, fault diagnosis, and control actions to mitigate fault(s). The work here primarily concerns the design and evaluation of a functional implementation of an operator support system termed the Computerized Operator Support System (COSS). This project successfully developed, demonstrated, and evaluated various COSS iterations in two full-scale nuclear control room simulator studies with a total of three licensed operating crews from a collaborative nuclear power plant (NPP). The work in this report was carried out at Idaho National Laboratory (INL), which was focused on developing the human-system interface (HSI) for the COSS. COSS used underlying fault detection provided by Argonne National Laboratory and documented separately from this report.

The remaining sections of this chapter provide background on control rooms in NPPs, which give context for the development of the COSS. These sections are adapted from a paper first published by Boring, Ulrich, and Lew (2016).

1.2 Generational Differences in Control Rooms

Industries like chemical, manufacturing, oil and gas, and energy involve multiple simultaneous processes. When multiple systems converge on a large scale, the process control facility may be said to be a plant, with designations as diverse as a chemical plant or a power plant. Typically each plant requires a control room as a central place to coordinate and control processes. While a control room may feature significant automation, operators still oversee the process from the control room, ensuring normal production and monitoring for anomalies, including threats to safety. Safety considerations become paramount, as a system malfunction can lead not only to equipment damage but also to harm to the environment or people at or near the plant.

Control room technology requires remote sensors and actuators, which rely primarily on electrical-mechanical components. While plants were possible without these technologies, the centralized control room was enabled with the advent of electrical gauges and switches in the 1920s (Bennett, 1993). Large ships are good examples of the emergence of control rooms. Steamboats brought the separation of engine room below deck and the bridge above deck. The captain or pilot set the speed and direction of the engine using the engine order telegraph, in which the captain's setting was mirrored in the engine room. Changes to the dialed position were accompanied by audible bells in the engine room to alert the engineers that they needed to change the engine speed or direction. Status indications between the engine room and bridge were also possible through telegraph, telephone, or intercom. As remote sensors and remote-controlled switches became available, the bridge was equipped with gauges to allow direct monitoring and provide direct control over the engine or other facets of the ship. The role of the ship's engineer shifted from that of control and maintenance of the engine to primarily maintenance of the engine. The control room eliminated the need for redundant personnel to relay status or control information.

1.3 Analog Control Rooms

Beginning in the 1940s, analog control rooms began to take root. The term analog is used to describe the human-system interaction used by the operators and may not necessarily apply to the technologies behind the board. Several standard characteristics of the centralized control room emerged. These included:

- *One-for-one arrangement.* In traditional analog control rooms, each instrument or indicator is directly wired to an equivalent sensor, and each control is directly wired to an actuator in the plant. There are no shared conduits or channels of information, and there is no aggregation of information or controls.

- *Simple indicators.* These indicators provide information about a single parameter like pressure level, flow rate, or temperature. Alternately, they may represent simple on-off logic like the status of charging pump or an alarm setpoint. The defining characteristic of these indicators is that they do not combine information from multiple sensors that would require computational logic or mathematical functions. Operators must integrate multiple indicators to assess the state of the plant.

- *Stand-at-the-boards operation.* While simple control boards were possible from a seated position, as additional instrumentation and controls (I&C) became available, it became necessary to expand the real estate of the boards vertically upward and horizontally outward. This arrangement eventually necessitated standing for some operations. The placement of some instrumentation higher vertically allowed monitoring supervision from across the control room.

- *Triple-layer design.* As noted, the control boards grew from operation from a seated to a standing position. A standard control layout evolved from this practice in which controls tended to be mounted low on the boards, often in a desk-like horizontal benchboard configuration. Above the desktop, a vertical panel comprises the second layer containing key instrumentation required for monitoring and control decisions. Finally, higher up the boards were found alarm lights. In this manner, immediately required information was close to eye level of the standing operator, and controls were within arm’s reach. Information such as alarms, needed only at the level of catching the operator’s attention, was placed high on the boards.

- *Setpoint alarms.* With remote sensors came the technology for setpoint alarms. These alarms were triggered when a particular measured entity reached a particular threshold, e.g., when a pipe exceeded the maximum recommended operating pressure. The threshold setpoint activated a light in the control room, which either contained a label near it or was placed in a lightbox with illuminated text upon activation. Additional features like audible alarms, flashing alarms, and silence buttons were added to the configuration, but the alarms continued to be based on the simple threshold setpoints.

- *Simple controls.* These controls are tied to a single function, usually equivalent to an on-off switch to activate a motor that in turn opens or closes a valve or pumps fluids. Typically, a control does not activate a series of sequential controls nor perform simultaneous parallel control actions. These simple controls may feature electrical or mechanical lockouts to prevent erroneous activation (e.g., turning on a pump to remove fluid when another pump is injecting fluid), and they may feature auto-stop for when a particular state (e.g., full valve open) is achieved. The controls may also feature two-factor confirmation such as when two buttons are required to be pressed simultaneously to close the circuit for emergency shutdown. In the latter case, because the consequences are high (e.g., cost of lost production or potential loss of equipment by sudden shutdown), the lockout serves to safeguard against inadvertent activation.

- *Manual operation.* Mechanical safety actuations like pressure relief valves, shear points, and electrical fuses were possible, but the control room did not feature automation. The plant was controlled entirely by the operator. A characteristic of much of process control is the achievement of steady state operations, which require minimal adjustment by the operator. However, plant transients might require extensive adjustments in prescribed sequences.

- *Procedures.* While procedures may not be part of the physical characteristics of the control room, they were increasingly required to support operations and maintain the plant within a known safety envelope, especially during transient conditions where the sequence or prioritization of particular actions was important. Eventually, e.g., in nuclear power plant control rooms, procedures became such an integrated part of the control room that special places were set aside to house the procedures within or around the control panels.

- *Command-and-control crew operation.* As the complexity of the plant process grows, the need for multiple operators likewise increases. As such, complex plants often required more than one operator. When there are multiple operators, there may be a supervisor to orchestrate actions and maintain process overview while operators monitor and control subsystems. Thus, while an individual operator may be involved in the minutia of controlling one particular system, the supervisor maintains situation awareness for the overall process. In some arrangements, the supervisor may also be in charge of issuing directives to the operators, establishing a command-and-control arrangement. Many plants have adopted a threeway communication protocol in which the supervisor issues a command or request, the operator repeats it back, and the supervisor confirms the operator has correctly understood the communication.

These features are not mutually exclusive, nor are they a template that is found in all analog control rooms. They simply serve as a reference set of features commonly observed in analog control rooms.

1.4 Digital Control Rooms

The introduction of digital technologies to the human-system interfaces within control rooms has fundamentally changed the features and functions of control rooms. Digital control rooms may feature (Furet, 1985):

- *Multipurpose displays and soft controls.* A distributed control system (DCS) features one or more displays with input capability such as a mouse, trackpad, or touchscreen (Ulrich et al., 2015). These displays may, in the architecture of the DCS, be toggled between different system function screens. As such, it is not necessary to have all information displayed simultaneously across the boards, as a single display can present distal information at one physical location. The input device likewise features remote control from a single location by providing virtual or soft controls tied to the particular screen on the display.

- *Information integrative indicators.* Automation may take the form of information automation and control automation. Information automation combines disparate information that operators would otherwise have to gather and assemble to draw a conclusion or maintain overview. With the highly distributed nature of information in analog control rooms, operators often needed to ping-pong back and forth to maintain situation awareness of processes. Digital displays can consolidate information that would otherwise be widely dispersed across the boards. Moreover, digital displays can provide aggregate views that support the operators, e.g., custom trend displays of key parameters or calculations of composite measures (e.g., overall loss of cooling rate given a failed cooling water pump) that would normally be performed manually by operators or technical support staff in the control room.

- *Complex or automated controls.* As noted, digital controls no longer require a physical switch on the control boards, as they can be controlled remotely through the DCS using soft controls available on the screens dedicated to each system in the plant. The control functions do not need to be linked to a single action, and it is possible to combine a chain of actions for each soft control. In some plants, for example, it is possible to have single-button startup or shutdown sequences without the need for ongoing human intervention. These features are a form of automation; it is also possible to have full automation for large facets of plant operations.

- *Console or workstation operation.* Digital control rooms often forgo panels because of the space efficiency and convenience of consolidating I&C on the DCS displays. With the advent of DCS workstations, the need to stand at the boards is diminished, and the workstations are often designed for seated operators. Some backup panels may be retained for safety in the event of DCS failure, but most DCS architectures feature redundant hardware and the ability to pull up any screens from any display. Thus, in the event of failure of one operator workstation, the operator could simply go to a backup workstation and resume the full range of process control for the plant.

- *Overview displays.* The triple-layer design of analog control boards is no longer required when most monitoring and control take place from a desk. However, because digital monitoring information is localized to the individual operator, it is desirable to have a shared frame of reference in the control room. Overview displays, in particular large overview displays (Jokstad & Boring, 2015), provide a way to monitor overall plant status that may not be possible with system-specific screens. The overview displays also enable troubleshooting between operators and supervisors in the control room by ensuring all parties have the same visual information during group discussions. Overview displays do not generally allow control actions and therefore serve only the function of providing visual indicators to aid operators.

- *Advanced alarm systems.* By adding control logic beyond the simple alarm thresholds found in analog alarms, it is possible to add significant functionality to alarms. For example, it is possible to exercise state dependence, by which only alarms relevant to a particular mode of operation are enabled. This feature overcomes the problem of alarms for steady state operations activating during startup or shutdown. Further, it is possible to implement alarm grouping, such that only a single alarm activates when a whole group of interrelated alarms might activate otherwise. Because process control often involves a sequence of activities, failure in one part causes a cascade of failures and corresponding alarms, which can result in an alarm flood that obscures the root fault. Other advanced alarm features include prioritized alarms that indicate severity to allow operators to take quick action in the event of multiple faults, prognostic and predictive alarms that anticipate faults, and advanced visual alarms that depict the fault in such a manner that the operator is able unambiguously to see the fault in context.

- *Single operator control.* Whereas analog control rooms often require multiple operators performing actions under direction of a supervisor, DCS technology provides the operator with the ability to perform actions independently. Features such as computer-based procedures eliminate the need for a supervisor to coordinate procedures. Additional features like automation reduce the need for constant operator vigilance and may reduce the need for multiple operators. Thus, advanced digital control rooms often yield a greatly reduced crew complement, sometimes resulting in only a single operator to oversee a large plant.

As with analog control rooms, it must be noted there is no prototypical digital control room, and different features will likely be present for each particular implementation. An important consideration for digital control rooms is that they chronologically are newer and have benefitted from the nascence of human factors engineering applications in control rooms (Strobhar, 2013). Human factors has resulted in improved design to the flow of activities in the control room, presentation of information to operators, and workflow of the operators. The marriage of automation technology, advanced visualization capabilities, and human factors optimization have resulted in significantly improved control rooms compared to their predecessors.

1.5 Control Rooms in U.S. Nuclear Power Plants

INL is engaged in human factors research in support of control rooms for the U.S. energy sector. Much of this work centers on nuclear power plant applications, where there is a twofold mission to modernize the control rooms of existing plants (Boring, 2014) and to develop new control room concepts for advanced reactor designs like small modular reactors (Hugo & Gertman, 2016).

The existing U.S. fleet of commercial nuclear power reactors is aging, and many plants are drawing to the end of their original 40-year operating license. While some utilities have chosen not to extend the license of a plant and commence decommissioning, in the vast majority of cases, the utilities that operate the plants are choosing to apply to the U.S. Nuclear Regulatory Commission to extend the operating license by another twenty years. The initial operating period was fully anticipated, and utilities stockpiled replacement parts to ensure safe and reliable operation. Replacing worn or broken components with equivalent components also ensured that the plants successfully operated within their original licensing basis without potentially requiring license amendments to accommodate the introduction of new technology. With license extensions, the plant may find itself nearing the end of useful life for existing equipment or at the point where the cost of refurbishment or like-for-like replacement parts exceeds the cost of new equipment. At this point, the utility is confronted with the unique problem of finding new equipment that serves the same function as existing equipment and determining if the new equipment fundamentally changes the conduct of plant operations such that a license amendment might be required.

INL supports efforts to modernize nuclear power plant main control rooms, featuring a stepwise, system-by-system upgrade path (Boring & Joe, 2015). This path results in a hybrid control room consisting of a mix of analog-mechanical and digital I&C. Although the term *digital island* is sometimes used pejoratively to describe the introduction of limited digital systems into existing analog control rooms, the first DCSs introduced to the control boards are an important stepping stone toward fully digital control rooms. The feasibility of performing a large-scale control room replacement is explored by the Electric Power Research Institute (EPRI; 2004), and nuclear utilities indicate that they are unlikely to be able to replace the entire control room at one time due to loss of revenue during the extended outage required for such a control room replacement (Joe et al., 2012). Instead, the utility undertakes a gradual upgrade process, typically consisting of one system or board per refueling outage. INL has designed the Guideline for Operational Nuclear Usability and Knowledge Elicitation (GONUKE; Boring et al., 2015a) to provide a process suitable for design and evaluation of new digital systems that are introduced to the control boards.

An analogous design transformation can be seen in commercial airplane cockpits, which have seen the significant introduction of new digital controls. Initial efforts resulted in the insertion of retrofitted multifunction displays into the cockpit to replace existing analog I&C. In most cases, the multifunction displays added avionics functionality to aid the pilot, from digital pitch and roll data, to navigation functions, to weather and airspace, to autopilot, to collision avoidance systems. Retrofitted cockpits offer different levels of digitization, from hybrid avionics to completely digital glass cockpits.

Control rooms for new nuclear power plants subscribe to many of the features indicted in Section 1.4 of this report. There exist some regulatory barriers to full adoption of all features found in other industries. For example, the heavy emphasis on safety has resulted in the requirement to maintain crew staffing levels analogous to analog control rooms. Additionally, the need for transparency in control logic has resulted in minimal intelligent or autonomous control. Examples of three generations of nuclear control rooms are depicted in Figure 1.

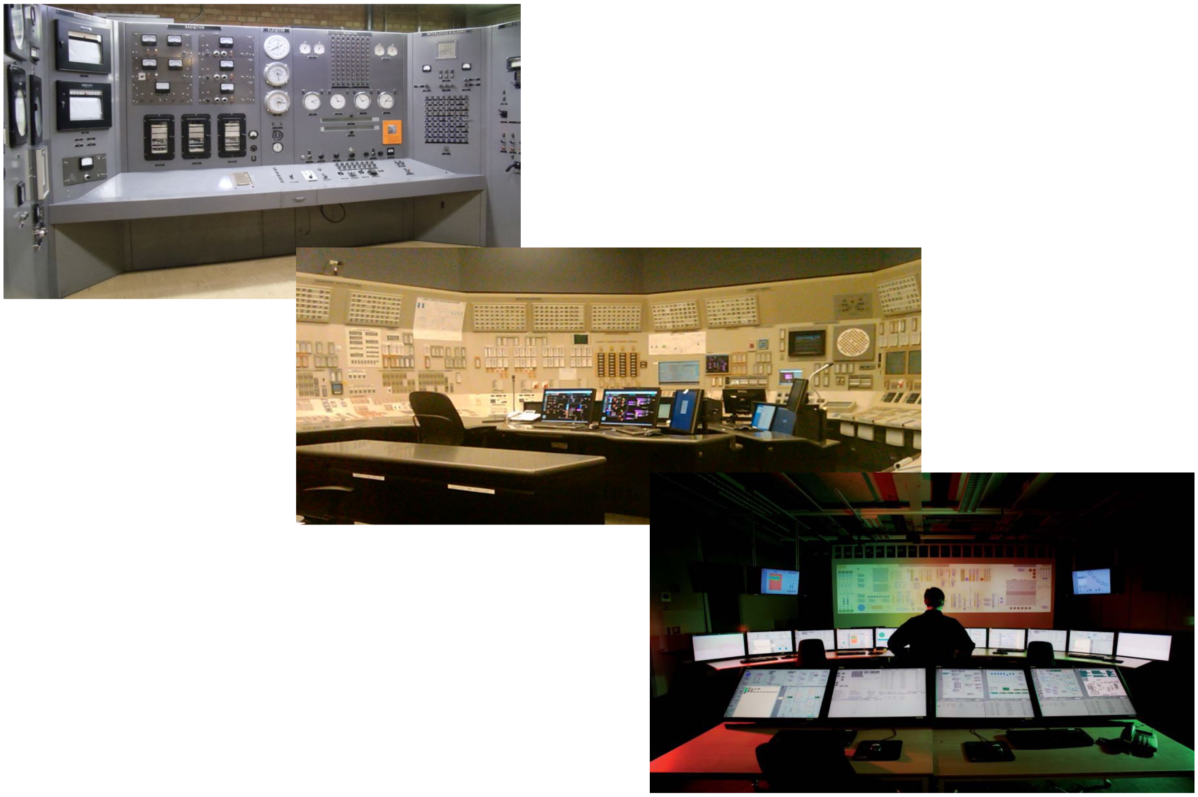


Figure 1. Three Generations of Nuclear Power Plant Control Rooms.

1.6 The Need for New Visualization in Control Rooms

The previous sections provide extensive background on the different types of control rooms. Conventional analog control rooms, such as those commonly found in nuclear power plants, represent information in a parallel fashion, typically with a one-to-one mapping of sensors to indicators. This design approach requires extensive control room real estate, especially for complex control system processes. As digital control systems, such as those found in modern control rooms for electrical grids or gas distribution networks, have begun to replace analog I&C, they have afforded the opportunity to use common displays across all systems, thereby providing a smaller footprint in the control room. The approach often uses a nested navigation scheme, whereby control operators have on-screen windows for particular subsystems.

Both approaches represent tradeoffs. For analog control rooms, operators must scan across control panels to maintain their plant overview, a complex process that demands the operators to integrate and track multiple simultaneous indicators. This disadvantage is offset by the ability to see all information at once, thereby minimizing the danger that critical indicators will be hidden in nested windows. In contrast, for digital control systems, the operators are able to avail themselves of optimized displays, including key parameter displays. However, having information consolidated on single windows may result in loss of situation awareness by these operators, as critical windows must often be toggled back and forth, thereby reducing the overview the operator may have of the larger process being controlled.

The shift to digital control rooms is inevitable, whether performed as a stepwise upgrade process or as a complete control room replacement. Successful deployment of digital technology in control rooms requires effective ways to display crucial indicator information to operators in order to allow them to monitor plant status and diagnose problems. To combat the loss of situation awareness inherent in nested displays in process control, designers of DCSs have developed overviews, often displayed as large overview displays, viewable by multiple operators across the control room. The challenge with such displays is they do not inherently reduce the problem of information overload that confronts the operator of a complex system. Design techniques for representing information in an intuitive manner help to reduce the workload in processing key information, but they do not necessarily reduce the overall amount of information the operator must monitor and process in parallel. The danger is that the operator may miss an important change in a key parameter because of the large number of visible indicators. If such is the case, eventually an alarm will indicate once the parameter moves out of acceptable bounds, but this alarm may come only at the point when remediation is necessary. Thus, the key operator role of monitoring and preventing upsets is not realized.

Several design philosophies have been created for control room visualizations, including ecological interface design (EID; Vicente & Rasmussen, 1992; Vicente, 2002), information rich design (IRD; Braseth, 2014), and high performance HSI principles (Hollifield et al., 2008).

- EID is a design approach that strives to present the operational constraints in a natural manner for key process parameters. This approach specifically capitalizes on the complex interactions inherent in process control systems by focusing on how to provide operators with sufficient context embedded within a parameter to understand what that parameter is doing and determine where the safe operating bounds are for that parameter.

- IRD aims to create high information density displays without overloading the operator. The basic design concept consists of muted or so-called dullscreen or darkscreen displays in which only important information is made salient through color. This approach is optimized for process control in that it allows a large number of process variables to be displayed concurrently.

- Finally, there is high performance HSI. Both EID and IRD produce uniquely identifiable displays. High performance HSI is not so much a single set of design principles as it is a process to infuse a systematic design across the control room. The key elements are adopting a style guide based on human factors principles and deploying that style guide consistently to design or redesign the control room.

EID, IRD, and high performance HSI are not incompatible approaches, and it is possible to use elements of all three approaches in concert. These approaches have yielded effective digital control rooms, but they represent a very small set of the possibilities for control room design.

1.7 Opportunity for Intelligent Control Systems

Nuclear power plants operate within a subspace between two types of system control philosophies, which are automatic and manual control. The combination of automatic and manual control represents a complex set of factors. Some automatic systems are used when there is insufficient time for operators to diagnose and respond to fast-moving events. The plant operates in an envelope of conditions that are supervised by the plant protection system, in the form of setpoints for protective actions that will be automatically invoked if the thresholds are exceeded. These automatic actions are configured conservatively to stay ahead of plant events, and are designed to put the plant in a safe and known condition, such as a reactor trip. Other automatic actions are part of the plant control system, and maintain important plant parameters at the desired operating points by making some adjustments to plant components such as valve positions and pump speeds. These control actions relieve the plant operators from the burden of continuous, tedious manual control of these components.

In less time-critical and more nuanced situations, operator actions are preferred because their extensive experience and unique human reasoning abilities are capable of keeping the plant online when possible. These situations occur with higher frequency and are less severe than those dealt with by the current plant protection system. In these situations human operators are superior at diagnosing the causes of the situation and performing mitigations that preserve the margin of safety without being overly conservative. Rather than trying to enhance operator response to these situations through automation, the industry has rather focused on making these events less frequent by investing in equipment reliability and redundancy. However, these types of events continue to happen in spite of the focus on equipment reliability.

A report published by INL in September of 2012, entitled *Design to Achieve Fault Tolerance and Resilience*, described the benefits of automating operator actions for transients (Quinn et al., 2012). The report identified situations where there are alternate configurations and actions that can mitigate the need for a safety actuation, such as a reactor trip, if there is time to do so. These situations are sometimes limited by the ability of the operator to accurately diagnose the cause of the upset and to take the needed actions in the available time. The ability to accurately diagnose the situation is, in turn, often limited by the available instrumentation to characterize the fault and the ability of the operator to swiftly integrate the instrument readings into a correct diagnosis. The risk of a late or inappropriate response is such that it has been judged better to invoke safety actions and accept the outcome of lost production.

Any delays in procedure-based manual control actions may possibly result in exceeding the protection setpoints and leading to an automatic reactor trip or other safety system actuation. Even when the operator is successful in arresting a plant transient and averting safety actions, the time required may negatively impact plant operations. The longer a transient is unmitigated, the larger the degree that the plant is subjected to off-normal and potentially component damaging conditions and the more of a challenge it is to arrest the plant excursion and return to within normal operating parameters. Over time, operator performance is expected to increase through better I&C, training and protocols, and increases in system reliability.

Digital control systems and computer algorithms are now capable of analyzing, diagnosing, and suggesting mitigations to even the most complex and fast-moving situations. Such systems could assist the operators in achieving a more accurate and timely response to component faults and plant transients.

Development of such technology could prove to be enormously beneficial to the currently-operating nuclear plants and new types of nuclear plants that are now being built or proposed. This would result in better management of plant upsets, improved operator performance, and ultimately make a positive impact on the industry's fundamental objectives in the areas of nuclear safety, production, and cost management. In this report we explore how operators could be assisted by a sophisticated plant monitoring and diagnosis system known as a Computerized Operator Support System (COSS).

2. COMPUTERIZED OPERATOR SUPPORT SYSTEM

2.1 Definition

The COSS is a computerized operator support system intended to aid operators in monitoring and controlling the plant. It is a valuable tool to bolster operator situation awareness, which is critical to the safe and efficient operation of nuclear power plants. Situation awareness, within the context of nuclear process control, is an accurate understanding of the plant state and current operating configuration, which includes intricacies of the control systems, the physics governing the plant processes, and the current operating safety and regulatory based envelopes. Maintaining situation awareness is a challenging task and continues to become an increasing concern as the aging experienced operator workforce must be replenished with less experienced operators who are not as inherently familiar with the existing analog plant technologies.

One solution is to ensure that technology supports the transition to a new workforce. As more and more plant information becomes available in digital form, it will be possible to provide operators with advanced information systems that aid in assessing the current plant status, safety margins, and deviations from expected operations. Further, through advanced simulation techniques, it will be possible to predict plant operations and how long the operators have to intercede in undesirable trends. Finally, the technology can recommend to an operator selected actions that can mitigate undesirable plant events and trends and return the plant to a safe operating condition with the least amount of upset possible.

A computerized operator support system (COSS) is a collection of capabilities to assist operators in monitoring overall plant performance and making timely, informed decisions on appropriate control actions for the projected plant condition. They generally have the following features (Boring et al., 2015b; Ulrich et al., 2015a):

- Monitoring a process to detect off-normal conditions
- Diagnosis of plant faults
- Prediction of future plant states
- Recommendation of mitigation alternatives
- Decision support in selecting mitigation actions

Another common term for this type of technology is “operator advisory system.” This term is generally synonymous with the concept of COSS for the purposes of this project. A number of other similar terms are sometimes used to convey the same concept, such as an “operator assistant.” Other concepts like “recommender systems” are well established in industry and research but represent only a portion of the multifaceted functionality of a COSS. However, as a class of related technologies, an important distinction to be noted is that they assist the human operator as opposed to serving as an extension of the control system. In that regard, the reasoning of the system must be transparent and familiar to the operator, and must operate on a time-scale that allows the operator to interact with the system, as opposed to the much-faster operating speed of an automatic control system.

2.2 COSS Versus Existing Advanced Control Concepts

The COSS concept embodies multiple technologies integrated to aid the operator. This integration is a crucial element in defining the COSS, because it aims to leverage the capabilities of each technology in a user-centered design framework to provide an interface that seamlessly supports operator decision making. Without this integration, the different technologies would compete with one another for the operator's attention and be either underutilized or even lead to confusion and poor operator performance. Advanced control concepts that are non-intuitive to the operator or leave the operator out-of-the-loop may yield unsatisfactory results if operator intervention is needed when operators lack situation awareness. Previous work (Ulrich et al., 2015b) has presented the various technological elements integrated into the COSS system; however, it is important to establish what the COSS can provide to the operator as an integrated system. In essence, the COSS is more than simply a sum of its parts because it brings together the diverse information and control capabilities of its sub systems. User centered design is an iterative process of refining the system to meet the needs of the user. The COSS concept still remains elusive since it has yet to be implemented in an operating plant, and therefore industry requires the necessary guidance to pursue this technology and the advantages it can provide for safer and more reliable plant operation.

2.3 COSS and Distributed Control Systems

Understanding the importance of COSS in the context of nuclear control room operators requires some historical context. Currently operating nuclear power plants were engineered and constructed before the existence of modern Distributed Control Systems (DCSs). Furthermore, because of the high safety demands, the nuclear power industry is conservative in adopting new control technologies before they have an established track record of performance. Consequentially, U.S. first generation nuclear power plants contain several independently operating analog controllers and even relay based protection systems. Commercial solid-state programmable logic controllers (PLC) began entering the market in the late 1970s and have slowly worked their way into nuclear power plant control (International Atomic Energy Agency, 1999). With current technologies the capabilities between PLCs and DCSs are becoming blurred, but historically PLCs offer higher scan rates for fast system response (10 ms) and are primarily for handling discrete input and output (Siemens, 2007). In contrast, DCSs were slower, more reliable, more expensive, and handled analog I/O. DCS architecture distributes control over several independent microprocessors, making them more scalable (Automation World, 2014). The functionality of the independent modules is integrated such that the DCS can control a series of actions constituting a process (e.g., automated generator synchronization to grid). With PLCs this would require integrating a supervisory control system. In first generation nuclear power plants the operators and procedures function as the supervisory control system. As systems are modernized, it becomes possible to use the DCS to automate some of the tasks that formally required a high degree of coordination and supervision from operators.

The extent to which existing nuclear power plants will take advantage of these capabilities for modernization is unknown. Deviating from how the plants currently operate requires modifying procedures and amending regulatory license agreements. In some instances, building in automation may be prohibitively expensive or technically unfeasible. Operators may be unfamiliar with such systems and hesitate to embrace automation. In the context of modernization, DCS systems can be implemented in a manner where they simply replace the existing control without adding in additional automation or supervisory functionality. The analog indicators and controls can be replaced with digital clones. Here we suggest that a COSS moves beyond replacement and embraces the additional automation that can be provided by modern DCS systems. A COSS can be described as an enhanced DCS.

Digital HSIs can be configured for both PLC and DCS systems. Oftentimes an HSI will be connected directly to a PLC on a Supervisor Control and Data Acquisition (SCADA) network or even integrated with a PLC. HSIs for DCSs are now typically networked to the DCS and run as an application on a thin client or PC. When it comes to HSIs for process control there are numerous approaches that can be taken to design and implement an HSI. Process control systems tend to be similar but not identical to other systems. Unlike aviation, which features a larger fleet of common systems for instance, it is difficult to design HSIs that can work well across different platforms (e.g. all pressurized water reactors, or PWRs). In aviation systems such as Traffic Collision Avoidance System (TCAS) or Primary Flight Display (PFD) systems can be installed or retrofit into several types of aircraft providing a common presentation format to pilots (Federal Aviation Administration, 2009). Predicting a collision or providing flight information relies on instrumentation, but the semantics provided by the instrumentation is abstracted from the particular avionics that are onboard the aircraft. Snow, French, and Hitzeman (2003) compared five PFDs from different vendors with U.S. Air Force pilots and found no practical differences between the slight variations between PFDs. With process control, abstraction to this degree is not possible. Plant system architectures are similar but not identical, all PWRs may have chemical and volume control systems, but the exact arrangement of the components and instrumentation will differ between PWR designs. That context is meaningful to the operator when operators must diagnose and mitigate faults.

HSIs must be designed to convey specifics of a system for the purposes of diagnostics, monitoring, and operation and must be tailored to each system. The resulting usability and consequential safety of these HSIs can be sub-par if operations and human factors engineering is not taken into consideration. This can occur if engineers design the HSI without input from operators because the engineer's understanding of the system and process is different from the operators. On the other hand, operators understand the process but may not be knowledgeable regarding interface design or human factors. Hollifield, Oliver, and Habibi (2008) note a large amount of variability in the quality of existing HSIs. Naïve designers and marketers are prone to select chrome and flash over substance. Visual features such as 3-dimensional shading and animation on components add compelling yet extraneous content to an HSI. Process and Instrumentation Diagram (P&ID) based displays provide operators with a comprehensive view of the system, but require time to build familiarity, concentration, and active scanning to maintain situational awareness. HSIs can be designed without direct feedback from operators or without taking human factors into consideration. Here we suggest that operator feedback and human factors are essential to the design of a COSS. The COSS is first and foremost an operator-centric approach. In this research effort, we start with envisioning how the operator could interact with the system and work backwards filling in control technologies that can aid operators or identifying shortcomings that will need to be invented to make the envisioned interaction paradigms a reality.

2.4 COSS and Computer-Based Procedure Systems

A computer-based procedure (CBP) system is one of the technologies the COSS integrates into its platform. Seminal human factors guidance on CBPs can be found in Chapter 8 of NUREG-0700 (O'Hara et al., 2002), among many other sources. The guidance offered by NUREG-0700 covers the procedures themselves and the HSI required to convey the procedures to the operators. In regard to the procedures themselves the most important issue to address is the organization of the procedures. NUREG-0700 provides the following guidance on organization:

> **8.1.5-1 Hierarchical, Logical Organization**
> The procedures should be organized in a hierarchical, logical, consistent manner.
> *Additional Information:* Organization will make it easier for users to see the relationships among procedures.
> **8.1.5-2 Organization of Procedure Steps**
> Each procedure should be organized into sections of related steps

Current paper-based procedures (PBPs) provide organization based on their physical print layout. This print layout requires an operator to physically move between different procedures as outlined by specific procedure step instructions. CPBs afford the technology to eliminate some of this navigation and placekeeping responsibility by aggregating the relevant procedure steps from different procedures into a single aggregated list presented digitally to the operator. The hierarchical representation of the procedure steps embodied by the print format is eliminated with the aggregated procedure steps and eliminates the context present in the physical print layout format. Reinforcing the structure and hierarchy of the procedures is crucial to providing operators with sufficient context to base their mental model of the procedure and its purposes. Maintaining this organizational structure in some form is important in CBPs to allow operators to make informed decisions with good situation awareness. Furthermore, even the most sophisticated CBP system is fallible, and the operator may be forced to forge their own path and deviate away from the prescribed aggregated procedure, which necessitates maintaining a good understanding of the overall procedure hierarchy and rationale for each procedure step. Some of these organizational issues can be addressed by how the CBPs are integrated and displayed within the COSS platform. The COSS interface serves as an organizational tool for the procedures, such that the accompanying displays provide the context based on the relevant system and components.

The integration of procedure steps within the COSS serves as a way to further delineate between standalone CBPs and the COSS system with integrated procedures. Indeed, the guidance in NUREG-0700 explicitly states that CBPs should consider the HSI they will be used within and maintain consistency with those interfaces. The approach adopted by the COSS extends this philosophy by considering the issue of integration from both perspectives. Instead of simply evaluating the CBP based on how it will interface with the COSS HSI, the COSS HSI development and the CBP development are performed in tandem.

The COSS differs from CBPs in numerous ways; however, there is one particular difference. The COSS contains a prognostic system that is capable of detecting and validating plant issues before alarms and trip setpoints are triggered. As a result of this early warning capability and embedded expert knowledge, the COSS in many instances is able to cross reference and convey a solution path before a problem requires shutting down the plant. This represents a fundamental shift from the typical operations and procedure use in modern plants. For example, during an abnormal or emergency event, the plant typically crosses some alarm indicated threshold prior to the operators taking action in which they use the procedures to diagnose the alarms and determine the root cause. From there the operators then follow the prescribed procedures to restore the plant to safe operating conditions. With the advanced diagnostic system used in the COSS, the operators may be alerted to the issue before it has evolved sufficiently to trigger a setpoint alarm. Furthermore, the procedure to correct the issue can be condensed considerably because the diagnostic actions are only required to verify the COSS diagnosis with the root problem already identified. The operators are presented with procedures that match the current configuration of the plant and have been predetermined to mitigate the issue and return the plant to steady state. In essence, the operators and the procedures have shifted in nature from reactionary to preventative. Though this shift is due to the prognostic capabilities, which is a separate module of the COSS, it fundamentally alters the CBP implementation integrated in the COSS from that of typical CBP systems under development.

2.5 COSS and Overview Displays

The COSS implementation for the chemical and volume control (Ulrich et al., 2015b) includes an overview display. Since the COSS incorporates an overview display it is important to make the distinction between an overview display and the COSS system itself. As its name implies, an overview display provides the high level system status to provide an overview of the system. In contrast, the COSS uses the overview to direct the operators' attention towards any diagnosed issues. The COSS itself is much more than an overview display, but it does assume an overview dipslay function of highlighting faulted components to direct operators' attention. The operator can then drill down to the control display level to find more specific information concerning the faulted component.

2.6 COSS and Intelligent Control Systems

An intelligent control system aspires toward an autonomous control system, having the ability to self-govern, by incorporating online artificial intelligence (machine learning) into the system (Antsaklis & Passino, 1993). In some contexts, such as deep space autonomous spacecraft, intelligent control systems have the goal of supplanting operators. The craft might travel long distances from Earth over several decades. Deep space communication latencies are on the order of several minutes, making remote guidance difficult and costly. Ideally the craft should be resilient to instrument failures or unexpected circumstances. Here it is much easier and understandable to make the case for adaptive control and autonomous self-governing. In other domains intelligent control systems with intermediate levels of autonomy and interaction with human operators are envisioned. They incorporate adaptive controllers that are capable of tuning controller parameters as the operating environment changes or measurements become degraded by noise. Intelligent control systems incorporate information assessment that attempts to validate the measurements passed to the controller. Intelligent controllers also incorporate control implementation supervisors that are capable of diagnosing faults and running fault detection and isolation (FDI) algorithms. However, overall the field of intelligent control systems is control theory centric with very little research focused on the role of humans. In contrast, the COSS is user centric, adopting a user centered design approach, were the technology is refined through an iterative process based on user feedback.

Nuclear power plants are unlikely to adopt intelligent control systems anytime in the near future. Nuclear power utilities and regulators are both committed to maintaining human supervision and decision making in the control room. Intelligent control systems with machine learning are difficult to validate and verify using traditional engineering approaches.

Although intelligent control systems and the COSS envisioned here for a modernized nuclear control room have disparate operation philosophies when it comes to the role of humans, there are similarities and lessons to be learned between the two. There are several approaches to designing intelligent control systems. One approach can be described as an expert control. Expert control systems as described by Astrom and Arzen (1993) incorporate an inference engine. The inference engine takes input from supervisory functions that are able to detect and diagnose faults. The fault data is cross referenced with heuristic knowledge based rules to change the control strategy of the system. For example, the control algorithms could re-tune their parameters or switch from a PID controller to open-loop control. Our COSS adopts a similar conceptual approach by taking the diagnostics from Argonne National Laboratory's (ANL's) diagnostic tool (PROAID) and applying predefined expert knowledge to determine whether a fault mitigation exists. If a fault mitigation exists it is available to the operators in the form of a procedure. With the intelligent expert control system the mitigation strategy is automatically applied to control a process or a variable. With the COSS the mitigation strategy is suggested to the operator, but the operator must decide whether they concur with the fault diagnosis and implement the mitigation procedure.

3. ANIME FRAMEWORK

3.1 Introduction

This chapter on ANIME is adapted from a paper first published by Boring, Lew, and Ulrich (2017). ANIME is the Advanced Nuclear Interface Modeling Environment. It is a user interface framework for building prototype HSIs for process control. The framework is built on Windows Presentation Foundation (WPF), a framework for implementing HSI prototypes that integrate with full-scope process simulators as well as microworld simulations (Chappell, 2016). WPF integrates disparate aspects of the interface, from multimedia to on-screen graphical objects. By allowing the development of user interface content as a type of skin or style sheet, it becomes possible to harmonize the interface. For example, it is possible to change common visual attributes of graphical objects, thus creating a customizable look and feel for the interface. WPF may be accessed from multiple means as part of the .NET Framework in Microsoft Windows. In the implementation of ANIME, it serves as a library of common and advanced indicators and controls featured in a HSI for a DCS. ANIME currently consists of multiple parts, including:

- Reusable libraries and C# sample code of common components that are featured in a DCS. For example, valve components come predefined with a look and feel suitable to the DCS and with functionality for interfacing with a software simulator. It is possible to change the parameters of the WPF library to change the look and feel of the HSI to meet style guide requirements or to emulate existing vendor styles. For example, it is possible to change the appearance of the user interface from a Westinghouse Ovation to a Honeywell Experion DCS with minimal parameter adjustment. The components also feature predefined behaviors, e.g., a valve may draw its status from a value in the linked simulator database, and it may feature control action behavior such as `open` and `close` that map their state back to the simulator database and effectively change the state of that component.

- Reusable libraries of advanced visualization and human factors design concepts. For example, there are advanced features for trending and alarms, including properties to highlight components in displays to represent alarm states.

- Prebuilt libraries for interfacing with full-scope simulators from GSE Systems, Western Services Corporation, and L3-MAPPS. These libraries are available as standard protocol libraries (e.g., OLE for Process Control) and as .NET compatible custom advanced programming interfaces (APIs). These libraries also allow interfacing with additional DCS platforms.

- Prebuilt libraries of simplified process modules suitable for microworld implementation. An example is the COSSplay system described in Section 3.3 below, in which ANIME is put into a standalone program without connections to a larger simulator. COSSplay is, among other applications, used for evaluating first-of-a-kind control room interfaces using student operators.

3.2 ANIME Applications

3.2.1 Background

In the four years since its conception, ANIME has been applied to a number of projects, ranging from prototypes of conventional and advanced DCSs to standalone process control systems for psychological research. The initial COSS prototype efforts formed the foundation for what would ultimately become the ANIME Framework. The COSS implementation using ANIME and other related applications are described below.

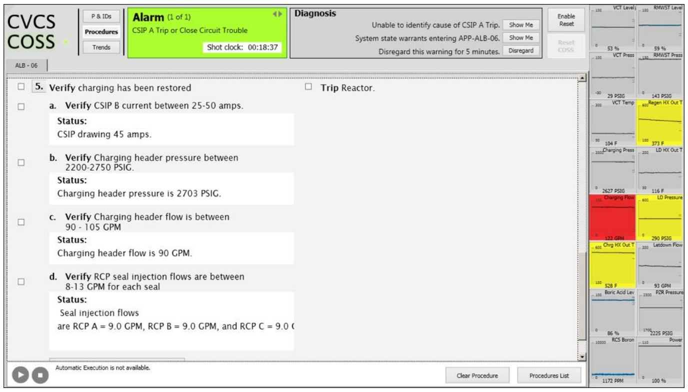
3.2.2 COSS ANIME Implementation

INL and University of Idaho researchers worked with researchers from Argonne National Laboratory to develop the COSS (Boring, Lew, Thomas, & Ulrich, 2015). The premise of COSS is twofold:

- To provide a prognostics system for fault detection to assist operators, and
- To provide a unified HSI for advanced DCS concepts.

In this configuration, COSS consists of an ANIME-based multifunction DCS (Lew, Ulrich, Boring, & Thomas, 2014) coupled with the standalone PROAID (formerly PRODIAG) intelligent fault detection system (Vilim, Park, Heifetz, Pu, Passerini, & Grelle, 2013). PROAID achieves fault detection by monitoring key parameters like pressure, flow rate, and temperature for changes that may be anomalous. The monitoring approach is generalized—not concerned with the physical type of measurement. Rather, when detected, faults are mapped on a system or component specific basis. When faults are identified, e.g., there is a descending value corresponding to a slow leak, PROAID passes that fault to COSS for operator notification. The power of PROAID is its ability to pick up a wide range of anomalies and to detect faults prior to them triggering setpoint alarms. Setpoint alarms typically occur when the fault impacts the ability of the system to function properly. In contrast, PROAID detected anomalies may serve as early warning, allowing operators to mitigate the fault without loss of critical systems or components.

In terms of the precedence of COSS in the HSI domain, while the idea of software assistants for operators is not novel, the combination of multiple assistants within a single DCS represents a unique application. COSS features an interactive piping and instrumentation diagram (P&ID) view; a computer based procedure system; a fault highlighting method; trend and prioritized alarms; a notification engine; and the PROAID prognostics fault detection engine (see Figure 2). A few of these features are worth noting, because they individually represent state-of-the-art practice in DCS development.



Alarm (1 of 1)
CSIP A Trip or Close Circuit Trouble
Shot clock: 00:18:37

Diagnosis
Unable to identify cause of CSIP A Trip.
System state warrants entering APP-ALB-06.
Disregard this warning for 5 minutes.

□ 5. **Verify** charging has been restored

□ a. **Verify** CSIP B current between 25-50 amps.
Status:
CSIP drawing 45 amps.

□ b. **Verify** Charging header pressure between 2200-2750 PSIG.
Status:
Charging header pressure is 2703 PSIG.

□ c. **Verify** Charging header flow is between 90 - 105 GPM
Status:
Charging header flow is 90 GPM.

□ d. **Verify** RCP seal injection flows are between 8-13 GPM for each seal
Status:
Seal injection flows
are RCP A = 9.0 GPM, RCP B = 9.0 GPM, and RCP C = 9.0 (

□ **Trip** Reactor.

Figure 2. COSS displaying fault highlight (green), computer based procedure system (light grey), and alarm system (red and yellow).

The computer-based procedure system, for example, might be considered a Type 4 system. IEEE-1786, *IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities* (2011), distinguishes three types of computer-based procedures: Type 1 procedures feature digital views of the text of the procedures, Type 2 procedures additionally incorporate embedded indicators, and Type 3 procedures further allow soft controls directly from the procedure. The ANIME implementation of computer-based procedures in COSS includes Type 3 functionality. In addition, it allows the automation of procedure execution, minimizing the interactions required by the operator to control that system. We propose that this functionality represents a Type 4 computer-based procedure, an additional layer of functionality beyond the three categories in IEEE-1786.

The alarm display is also worth noting. There are three alarm cues represented on the displays. The primary alarm indicator is modeled dimensionally on the annunciator tiles found in conventional control rooms. Within the same footprint, the alarm provides not just a binary status but also a trend display, the boundary conditions for alarm entry, a color-coded prioritized alarm scheme, and information on sensor parity, in case there is a drift in one or more sensor values. A secondary cue is embedded in the P&ID, in which alarmed components are imbued with a shadowed outline. This outline—colloquially known as the *green aura*—highlights affected systems. Finally, when appropriate, the PROAID notification will appear in the faceplate area within COSS. This notification will direct the operator's attention to the fault, cause, and solution, along with a shot clock to count down until the required point of action, e.g., if there's a slow leak, this might indicate the point at which the leak causes a fault.

COSS has been developed with an eye toward optimizing the HSI elements. Using feedback and performance measures obtained from operator-in-the-loop studies, the ANIME graphical front end of COSS has evolved the presentation of information. Below, we present three cases where the design of the HSI has been improved through iterative evaluation using operators:

- Initial efforts at representing the P&ID centered on simplified views, but operator feedback revealed a distinct preference for greater detail, resulting in more complex views. While a preference for more complex graphics may seem counterintuitive to the philosophy of design simplicity, the ability of experts to use complex representations to achieve situational overviews is an important finding.

- Another example of the evolution of the COSS HSI involves the number of displays used to represent the information. COSS was initially designed to fit on a single display embedded on the control boards. This design philosophy represented a dashboard view, with all functions of the system integrated into a single viewing area. More recent implementations have seen the shift to multiple displays, with a wider dispersal of information across the control boards. This allows a harmonized system replacement while also allowing greater detail for each function. For example, a dedicated alarm display ensures that a greater number of systems can be included in the COSS alarm system.
- Finally, early versions of the COSS HSI relied heavily on the dullscreen design philosophy to minimize color as much as possible (Braseth, 2014). While dullscreen is maintained in newer versions of COSS, the allowable items that are deemed important enough increase the contrast of indications. Efforts are made to reserve highly saturated colors for abnormal conditions in order to draw the operators attention. Original designs tended to use color only for alarm states. Recent iterations have also included color for a broader spectrum of meaningful information. Valve positions, e.g., open vs. closed, were previously depicted in monochrome. However, the salience of such indicators from across the control room was unfamiliar. Some operators highly preferred the use of color to indicate the valve position because it was considerably easier for operators to determine this key status at a glance, even across the control room.

3.2.3 Prototypes for Commercial Distributed Control Systems

ANIME has been used to support control room modernization efforts at existing NPPs by mimicking the functionality of commercial DCS platforms (Boring & Joe, 2015). To use a genericized example, an electric utility decided it would upgrade its NPP main control room in a piecemeal fashion, focusing first on systems where it would see improvement in electricity production or decreased maintenance costs due to aging components. The utility reviewed plant systems and created a modernization plan by which it would gradually upgrade systems and their corresponding footprint on the control boards system by system. The utility decided that it would purchase a digital turbine control system (TCS) from a DCS vendor. The DCS vendor prepared a detailed product specification and provided an HSI style guide to indicate the look and feel of the interface. The TCS specification covered all essential control functions such as latch, speed control, and load control; operational overviews like general turbine overviews, valve and trip tests, and diagnostics; required bypass functions; and system maintenance.

Using the HSI style guide, previously developed TCS DCS screenshots, and the specification, the ANIME development team created DCS screen mockups that matched the TCS. These dynamic prototypes were then embedded in revised analog control boards with the existing TCS interface removed. The net result was a mimic of an LCD touchscreen placed on the control boards (see Figure 3).

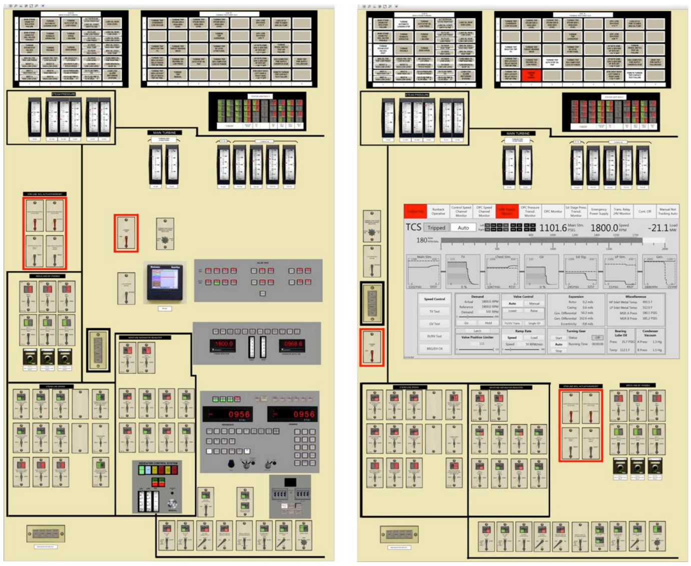


Figure 3. An example of the legacy control boards (left) and an upgraded TCS (right).

The prototype indicators and controls in ANIME were paired to their equivalent components in the simulator, thus keeping the existing TCS model intact on the simulator. Where there were deviations between the existing TCS model and the functionality in the specification, workarounds were implemented to provide users the experience of the new TCS. Workarounds included utilizing scripting functionality of the full-scope simulator, as well as embedding control logic into the ANIME framework. For testing a limited but representative set of scenarios this approach is rapid and cost effective because the alternative would require completely replacing TCS logic in the plant simulator. In this manner, the prototype TCS could be developed substantially faster than the actual DCS, because the prototype TCS did not need to create new control logic nor meet stringent quality assurance requirements that would be required of the actual DCS.

The ANIME-based prototype was tested through a series of scenarios representative of TCS use. Licensed reactor operators (ROs) were brought into the HSSL for operator-in-the-loop evaluation. The testing followed an early stage evaluation (Boring, Joe, Ulrich, & Lew, 2014), thereby allowing operators to get hands-on experience with a close approximation of the proposed TCS and provide feedback to the design and functionality of the TCS early in the design stage. Initial skepticism by the TCS vendor of the value of a third-party prototype that mimicked the TCS was replaced by appreciation that issues in the design of the TCS were identified and corrected long before deployment, thereby preventing costly reworks of the TCS.

TCS prototypes have been developed for five different plants that mimic two commercial DCS platforms. Additional systems like chemical and volume control have also been developed into DCS prototypes (Lew, Ulrich, & Boring, 2017). The same method has been used for early digital to modern digital upgrades in the form of plant process computer displays.

3.2.4 Planned ANIME Applications

Although ANIME already represents a mature product for DCS prototype development, there remain important research and deployment activities ahead. These include:

- Advanced HSI development. Currently, the features of ANIME are linked to common DCS functionality. While the transition from analog to digital control rooms is revolutionary within the nuclear industry, there remains opportunity to improve the state of the art for process control. RevealFlow (Boring, Ulrich, & Lew, 2016), a design philosophy that centers not on current status but change in status—from trend data to predictive displays—remains a promising expansion of ANIME, both in terms of novel ways of graphically representing control information and incorporation of intelligent controls.

- Advanced control system platform. Currently, ANIME is being integrated into a suite of tools that can be used for prototype development and evaluation in process control, particularly as software for experimental research. There exists a need for software between research tools like LabView and full-blown DCS applications. As national scientific user facilities such as experimental reactors increasingly become a reality at the U.S. national laboratories, it is crucial to have software that is capable of meeting experimental rigor, human factors standards, and extensive security requirements. ANIME is positioned as a tool to be made more widely available to support such user research communities.

Risk monitoring and modeling. Features in COSS hint at new directions that are possible with ANIME to support risk. In particular, the PROAID prognostics system offers a template for how a DCS may be used to monitor critical parameters and detect faults. Additionally, the computer-based procedure system affords the opportunity to model human actions in the face of a full plant model. Current efforts in computation-based human reliability analysis like the Human Unimodel for Nuclear Technology to Enhance Reliability (HUNTER) (Boring, Mandelli, Rasmussen, Herberger, Ulrich, Groth, & Smith, 2016) create a virtual plant operator that interfaces with thermo-hydraulic (TH) models. These TH models are often simplified versions of plants and may not represent the full spectrum of plant behavior, especially the interactions of redundant safety systems. To allow a more realistic risk model of emergent plant performance, it is necessary to enlist high fidelity models such as full-scope simulators. ANIME can serve as a scheduling tool for Monte Carlo simulation of possible outcomes in response to a variety of operator performance. This interface may also be represented as a look-ahead real-time monitoring system to assist operator decision-making in the face of plant upsets (Boring, Ulrich, & Lew, 2015).

Table 1 identifies current and future solutions in the ANIME toolset. This table is not exhaustive, but it positions ANIME as a tool that may be used immediately to prototype new HSI and DCS concepts for control rooms, to a point in the future when it may help realize and implement these concepts as a production DCS system. ANIME began out of necessity to prototype conventional DCS interfaces and has evolved to be a tool for advanced HSI. As ANIME continues to evolve, it is anticipated that it may very well find equally useful application outside the control room.

Table 1. Current and proposed applications of ANIME.

	Current Applications	Potential Applications
Reduced Order Simulation	Microworld	Microworld Design Mockups
Full Scope, High Fidelity Simulation	DCS HSI Prototypes	Intelligent and Advanced HSI Systems (e.g., Risk Monitors)
Deployment	Experimental Prototyping Environment	Distributed Control System for Process Control

3.3 COSSplay

The previously described implementations of ANIME consist of WPF code as a front end paired with an underlying full-scope simulator. The same HSI approach can also be applied equally well without the underlying simulator. When a simplified process control model is used instead of the full-scope simulator, the resulting environment is known as a microworld (Vicente, 1999). Because the microworld adaptation of ANIME was first used to evaluate new features of COSS, the microworlds within ANIME have broadly been called COSSplay (Ulrich, Werner, Lew, & Boring, 2016). COSSplay is word play on *cosplay*, the popular activity of dressing in costumes after popular anime, video game, and comic book characters. However, because microworlds are a form of simulation much like a video game, the idea of gamification also playfully permeates COSSplay.

A chief advantage of this microworld approach is that the process control can be simplified considerably. This approach allows testing of HSI concepts without the confounds of a highly complex and disparate control interface for multiple systems. The simplified nature of the COSSplay control system therefore allows evaluation of very specific aspects of the HSI.

Additionally, because the microworld represents a simplified interface, it is possible to train and test non-professional operators, thereby enabling studies with larger sample sizes than would be possible with actual control room operators. For many plants, for example, there are fewer than 40 total operators—a number that is unachievable in most studies and yet is a necessity in many experimental designs to achieve sufficient statistical power for significance testing. By using less experienced operators—even students—it becomes possible to draw strong inferences about study findings. Of course, there are limits to the external validity or generalizability of some studies using this approach. Reactor operators using conventional analog control systems may actually exhibit much of the functionality of the system as a mental model, since no operational model exists independent of manual control (Lew, Lau, Boring, & Anderson, 2016). Still, many facets of the HSI are generalizable even with different test participants from the target population. For example, perceptual characteristics will remain largely invariant across levels of operator expertise, such that the microworld may prove an ideal place to test the visual salience of particular interface elements. The microworld may also be used as pilot testing or screening for features that are later evaluated with actual professional operators.

A final advantage of microworlds is that no high fidelity simulation is required. Many industries do not have the full-scope simulators commonly employed in nuclear power, or many novel systems have not yet been fully modeled and deployed as simulation codes. In the absence of such robust simulators, it is quite possible to use the microworld as a low fidelity, reduced order model to drive dynamic mockups of planned systems. The microworld is an ideal early stage prototyping tool for enlisting operator-in-the-loop feedback in interfacing with an emerging DCS.

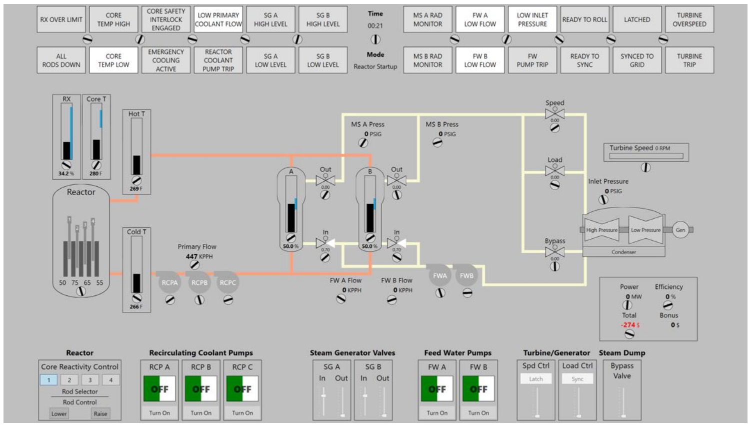


Figure 4. A simplified nuclear power plant microworld interface developed in ANIME.

A good example of the uses of COSSplay is the recent work to develop a microworld simulator (see Figure 4) to evaluate a novel method of assessing situation awareness (Ulrich, Boring, Lew, & Werner, 2017). By embedding multi-state rotating visual markers in a gamified NPP HSI, it is possible to compare visual attention to eye tracking. The disadvantage of eye tracking is that the analysis can be laborious, while some eye trackers may require frequent recalibration for accurate data collection. By testing student operators' ability to detect moving visual markers in areas of interest that feature key parameters, it is possible to duplicate functionally much of the data that are collected by eye tracking yet in a more robust and less laborious manner. ANIME libraries were used to create the simplified process control. Additionally, new basic elements including control logic models of particular systems were added to the ANIME library in the process. The graphical functions for displaying the visual markers were also built in WPF and have now become part of the ANIME library. The study illustrates that the ANIME library is extensible—adding new visual elements or underlying functions as required and thereby expanding the code library.

4. COSS DEVELOPMENT

4.1 Collaborative Effort with Argonne National Laboratory

Efforts to link PROAID (then called PRODIAG) to the COSS HSI began by configuring a virtual development workstation within the HSSL at INL (Boring et al., 2013) for ANL to use over a virtual private network. At the outset of the integration the plan was to use GSE's Generic Pressurized Water Reactor (gPWR) as the plant model for the linking ANL's PROAID to INL's COSS. ANL has a high fidelity chemical and volume control system (CVCS) model that it was used for development purposes, and a cursory analysis suggested that the gPWR's CVCS was sufficiently similar for the purposes of this work. Configuring PROAID for gPWR began by first identifying the flow path during normal letdown and charging. This path is then used to define the system at a P&ID level for PROAID. To test how PROAID would respond to CVCS faults with the available sensor set and lower fidelity model time-series data containing the component states and indicators were exported from the simulator and ran through PROAID. The available sensor set limited the accuracy of the fault detections but worked well enough to proceed with linking PROAID to gPWR in real-time by developing the PROAID Bridge described in Section 7.2.

INL's project scope of work included developing a revised COSS and conducting an evaluation workshop with licensed operators. To achieve this goal, the development efforts were aligned with a control room modernization effort at a nuclear utility in the U.S. in cooperation with the U.S. Department of Energy's Light Water Reactor Sustainability (LWRS) program (Boring et al., 2017). While the LWRS efforts focused on modernization of a turbine control system, COSS efforts focused on CVCS. Under a Cooperative Research and Development Agreement (CRADA), INL and the nuclear utility are producing an end-state vision of a modernized control room and evaluating hybrid control boards in the HSSL's full-scope, full-scale, reconfigurable glass-top control room nuclear simulator. In June of 2016 development efforts for COSS were transitioned from gPWR to the partner utility's plant for a workshop scheduled in August, 2016. The workshop provided an opportunity to allow operators to interact with the COSS prototype in real-time. Implementing the COSS for the partner plant not only meant that operators would be familiar with the system, but it also allowed comparisons to be made between hybrid digital/analog control boards and the traditional boards. The plant implementation is discussed in further detail below.

Due to the short time frame between transitioning from gPWR to the new plant model implementation, the PROAID fault diagnostics were not linked in real-time for the workshop conducted in 2016. The plant model was implemented by a different simulator vendor than gPWR and required rebuilding the bridge program to support communication. However, an offline analysis was conducted using time-series data exported from the new simulator. The fault diagnostics and temporal dynamics produced by PROAID were used to implement the COSS prototype for the workshop. For the 2017 workshop the PROAID bridge polled data in real-time from the plant and derived fault diagnoses, which were relayed to the COSS in real-time.

The goal of developing the prototype is to allow operators to see, feel, and hear how a digital HSI will respond in real-time. Real-time operation and feedback are essential to understanding and evaluating nuances in how the HSI conveys information. The development environment used for COSS provides a tremendous amount of flexibility in the plethora of interaction schemes and information presentation modes that can be presented. Here it is important to remember that prototyping effort is to evaluate COSS as a concept from a human factors perspective. The tool needs to operate in a well-defined simulation environment with plant conditions that are known in advance. The development of an actual COSS would require developing an advanced control system with architecture similar to the intelligent expert control system described in the previous chapter.

5. TEST PLANT IMPLEMENTATION

5.1 Rationale

This section on the test plant implementation and the following section on the initial operator-in-the-loop evaluation study is adapted from a paper first published by Lew, Ulrich, and Boring (2017). It is important to evaluate the COSS in a representative, real-world based simulation and scenarios to demonstrate the technology as a proof of concept. As part of collaborative work with a representative nuclear utility, INL had the opportunity to evaluate an implementation of the COSS based on the plant model provided by the collaborating utility. The collaborative plant is in the process of upgrading some non-safety critical systems as part of their control room modernization effort. Distributed control systems are being implemented in the plant to control a number of different systems including the chemical and volume control system. Distributed control systems provide a backbone for implementing advanced control concepts such as the COSS. As a result, the utility was interested in exploring futuristic advanced control concepts to inform their upgrade process. The utility needed to understand what type of control schemes and features the operators would like to see incorporated in the control room. This informed the plant in developing a style guide for the new digital HSIs as well as developing a plant endstate vision. Establishing this end-state vision is important because the upgrade process is extensive and will occur over a several-year process. In order to most effectively achieve the upgrades and ensure usable intermediary states of the control room it was important to establish the end-state concept before any upgrades are performed. This also ensures consistent upgrades of the different systems in order to maintain a consistent control scheme and HSI style throughout the upgrade process.

This upgrade process also afforded the opportunity to evaluate the COSS concept with two different operating crews. The evaluation achieved several goals for the ongoing COSS project. First, it established a starting point for implementing the COSS in an existing control room. Second, it provided the opportunity to gather invaluable feedback and performance data on the COSS concept to inform future iterations and improve the COSS design.

5.2 Existing Conventional Analog Boards

In the conventional control room layout, the controls and indications are arranged as a process mimic. The mimic depicts the major components of the CVCS and their arrangement and function in the system thus providing the organizational structure on the board. The piping of the mimic is color coded to segregate the CVCS into sub-systems (e.g., letdown path is orange, charging and seal injection is red; see Figure 5). The benefit of a mimic format allows operators to identify the function and status of the component from its placement in the mimic diagram without having to rely on memory and the component's labeling or looking back and forth between the board and documentation. The tradeoff to the mimic layout is that the spatial arrangement of the indicators and controls is not intuitive if operators are not familiar with the mimic's layout. Operators have also reported that incorrectly identifying a flow path can lead to misreading an indication or controlling the wrong component. During normal operations, most of the activity is concentrated on the right half of the board. The left half represents instrumentation and control (I&C) for boric acid recovery, boration, and dilution. The indicators and controls on the board with green and red labels are safety related.

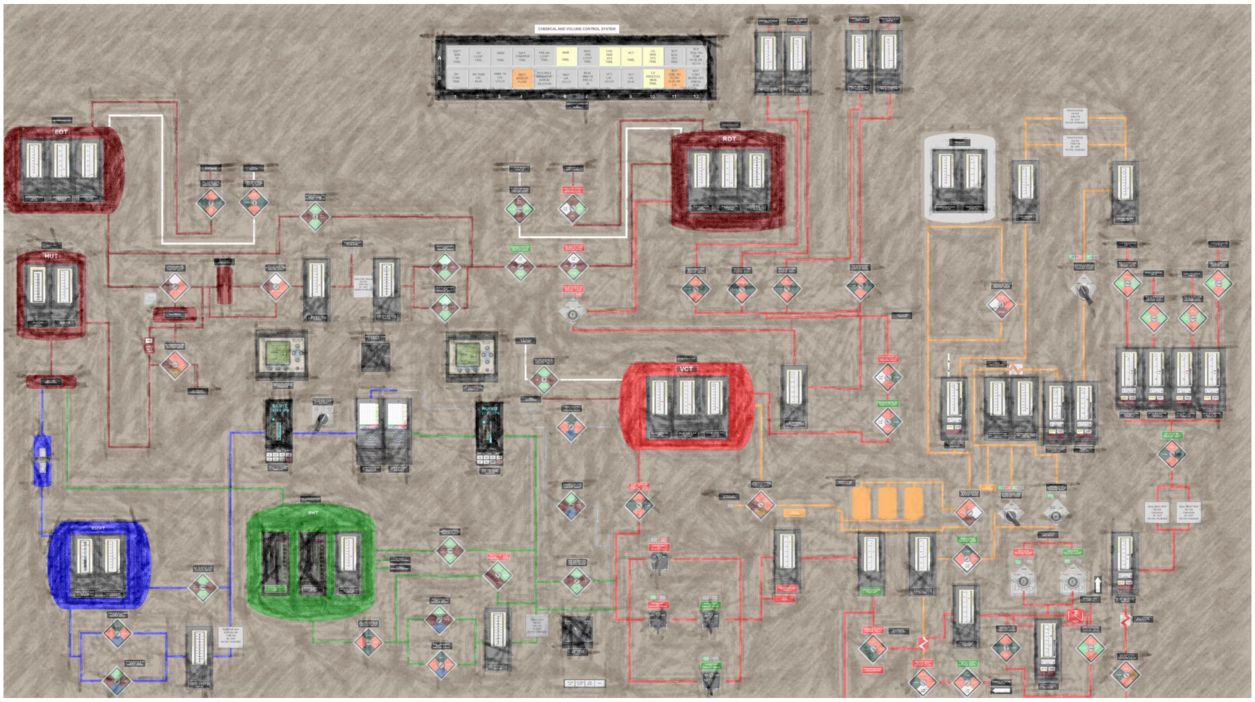


Figure 5. Sketch of the existing chemical and volume control system board.

The digital HSI implementation consists of two large overview displays placed on the vertical sections of the control boards to provide at a glance monitoring of the CVCS and RCS systems. Several indications on the large displays are intended be visible from across the control room. Below the large overview displays are four touch panel displays for monitoring CVCS subsystems and for controlling the CVCS. Several analog indicators and controls were relocated to the apron of the board. These are primarily safety related I&C along with a few additional non-safety-related I&C. The layout of the remaining analog instrumentation was organized in the form of process mimic to maintain the positive aspects of the mimic organization while capitalizing on training carry-over from operator experience with the conventional board.

The left overview is for monitoring CVCS. The overview is organized as a P&ID and is intended for monitoring during normal and abnormal operating conditions. The right overview is for monitoring Reactor Coolant System (RCS) coolant inventory. The RCS coolant inventory overview allows operators to monitor the reactor status, steam generator levels, RCS loop temperatures, and the pressurizer. The RCS and CVCS are tightly coupled. Pressurizer level is controlled through CVCS letdown, and the CVCS provides make-up for small RCS coolant losses. The RCS board resides to the right of

The four touch panel displays were implemented such that they could be operated by touch, as the end-state vision did not incorporate a keyboard, trackpad or mouse. Therefore, all control functionality was implemented such that it could be performed using a touch interface. Buttons on the display were made substantially taller compared to an interface designed for cursor input. For numeric entry an onscreen numeric keypad was presented. The touch displays allowed operators to monitor and control sub-systems and components of the CVCS such as seal-injection, boration, dilution, and automatic makeup. For the study, digital HSI screens and controls needed for the test scenario were developed. These included screens for monitoring seal injection and makeup and screens for controlling letdown flow, temperature, and back pressure as well as charging pressure.

The physical size of the displays was taken into consideration when laying out the content for the screens. Because the overview displays are roughly twice the height and width of the smaller displays, it is possible to have four times the amount of legible content on the overview screens assuming the same viewing distance.

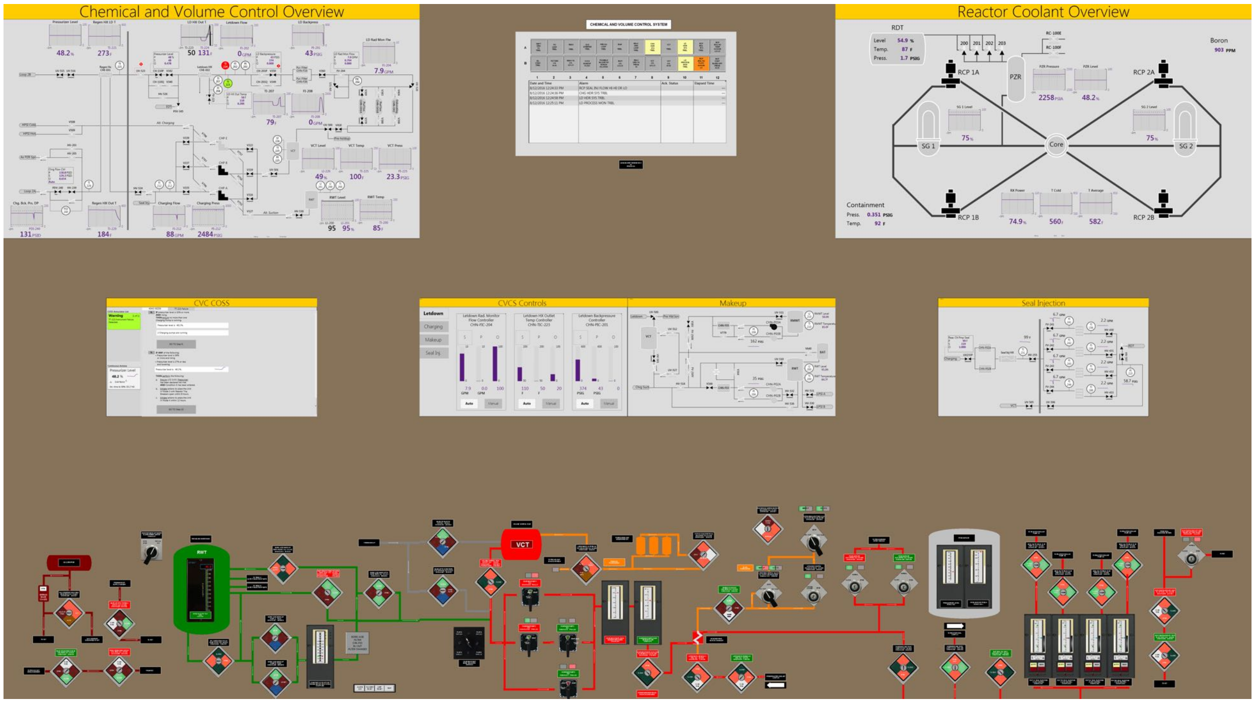


Figure 6. COSS displays embedded within the control board containing the safety related systems of the CVCS.

For the August 2016 workshop all the HSI screens were implemented in a style known as dullscreen. With the dullscreen concept the screens appear monochromatic when the annunciators and instruments are within normal operating ranges, allowing high-contrast and salient color indications to grab the operators' attention should something unexpected or noteworthy happen (see Figure 6). For the August 2017 workshop the valve indications used high contrast monochromatic styling (see Figure 7). The conventional approach to designing HSI screens identifies the minimum allowable size for text and other graphical elements and then "consistently" uses these minimum allowable sizes throughout the entire interface to maintain legibility. The downside is that everything is equally illegible. By employing graphic design and visual perception principles to the design, information can be hierarchically prioritized, and more pertinent information can be made more salient and legible to distant observers. Graphic design has long known that slight variations of font size, font weight, white-space, and typeface, and kerning can produce drastic differences in how information is perceived (Saltz, 2011). Graphic design is the art of manipulating these variations to produce a design that conveys the intended message. The science of visual perception excels at understanding the basic principles of contrast perception, text legibility, saliency, but is lacking when it comes to understanding how multiple nuanced elements to produce the gestalt, the whole perception of the features.

5.3 CVCS Displays Descriptions

The COSS is comprised of several digital HSI displays and screens hierarchically organized. The physical layout is comprised of two large overview displays and four smaller touch-enabled HSI displays. The left overview is for monitoring CVCS (see Figure 7). It is intended for monitoring during normal operations and conveys letdown and charging status information. The display is also aimed at supporting abnormal operations by providing visual annunciators and the status of safety injection systems.

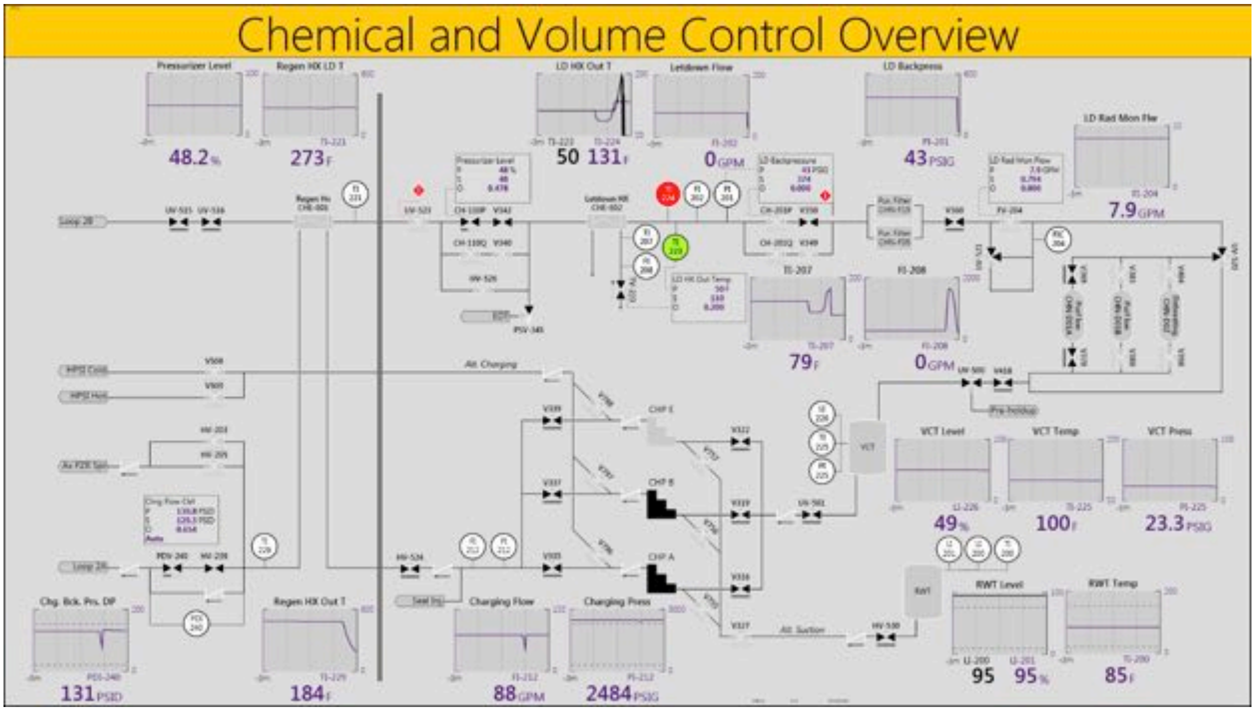


Figure 7. CVCS large overview display.

The right overview (see Figure 8) is for monitoring reactor cooling system (RCS) coolant inventory. The RCS coolant inventory overview allows operators to monitor the reactor status, steam generator levels, RCS loop temperatures, and the pressurizer. The RCS and CVCS are tightly coupled. Pressurizer level is controlled through CVCS letdown, and the CVCS provides make-up for small RCS coolant losses. The RCS board resides to the right of the CVCS, but due to the numerous safety-related controls, the board will not have room for a dedicated large overview display. Hence, the rationale for providing the RCS overview on Bay 3. For the design workshop, it was assumed that operators would not have the ability to interact with overview displays or to select the overview screen that is being presented.

Below the large overview displays are four 27-inch displays. The design concept specifies that operators would have the ability to interact with these screens via touch. Because no keyboard or mouse would be provided, it was necessary to make sure that all control functionality could be performed using only a touch interface. For instance, buttons were made substantially taller compared to an interface designed for mouse-cursor input. Secondly, an onscreen numeric keypad was presented for entering controller setpoint values.

The physical size of the displays was taken into consideration when laying out the content for the screens. Because the overview displays are roughly twice the height and width of the smaller displays, it is possible to have four times the amount of legible content on the overview screens.

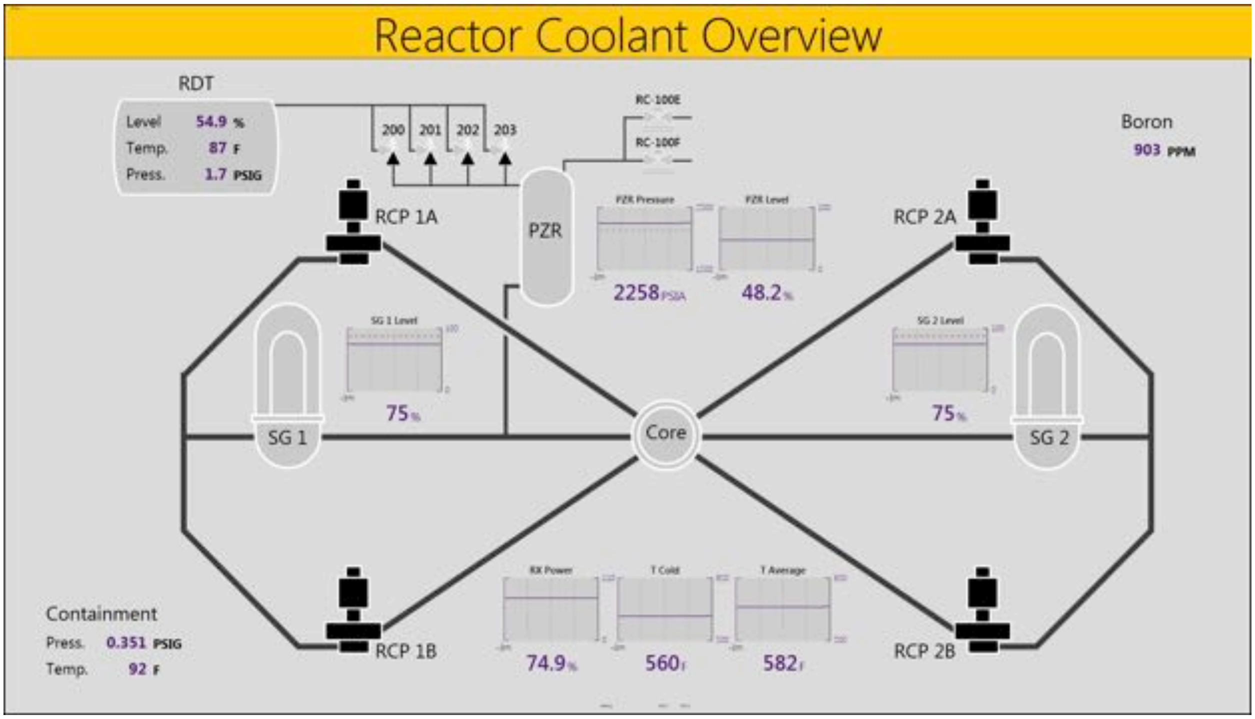


Figure 8. RCS large overview display.

In addition to Level 1 overview screens, a complete digital HSI for CVCS would include numerous Level 2 screens for monitoring sub-systems and functions of the CVCS such as seal-injection, boration, dilution, automatic makeup, etcetera, and Level 3 screens for control actions and operator guided diagnosis. For the study, digital HSI screens and controls needed for the test scenario were developed. These included Level 2 screens for monitoring seal injection (see Figure 9a) and makeup (see Figure 9b) and Level 3 screens for controlling letdown flow, temperature, and back pressure as well as charging pressure (see Figure 9c). Future work intends to expand the functionality of the CVCS HSI as additional scenarios are developed.

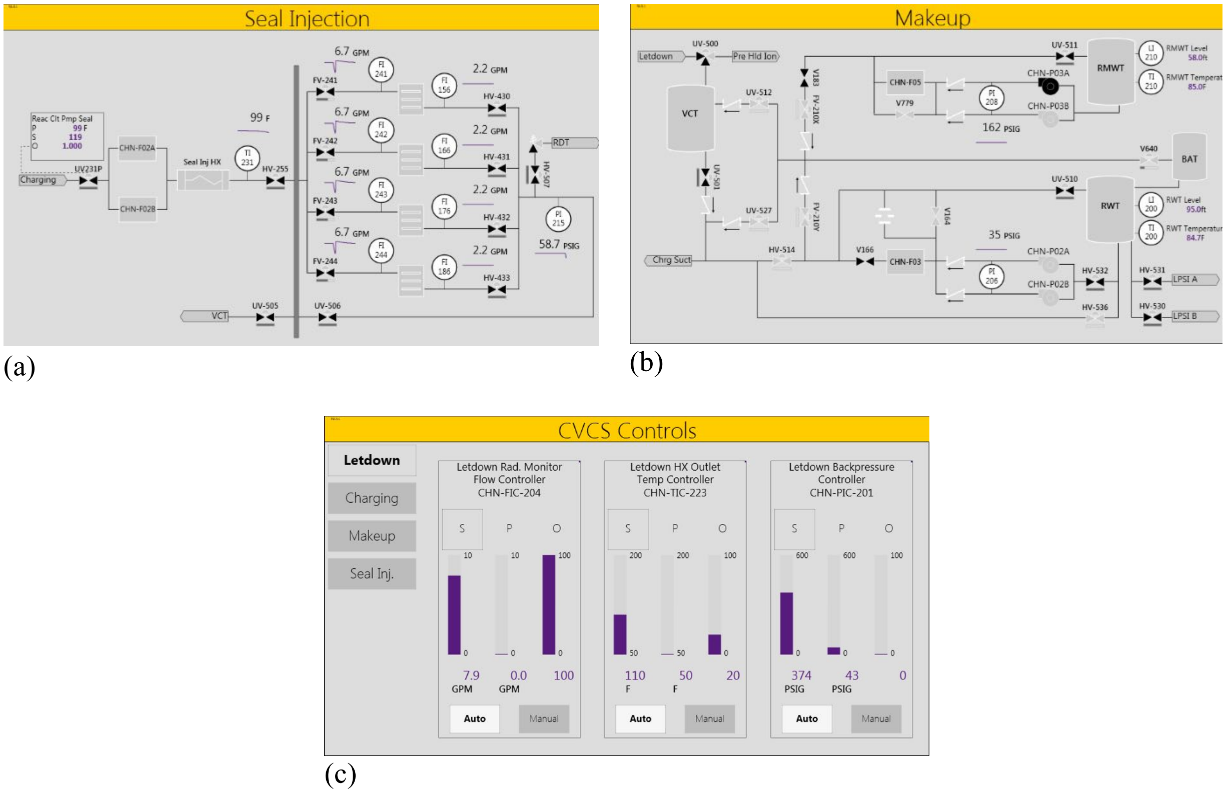
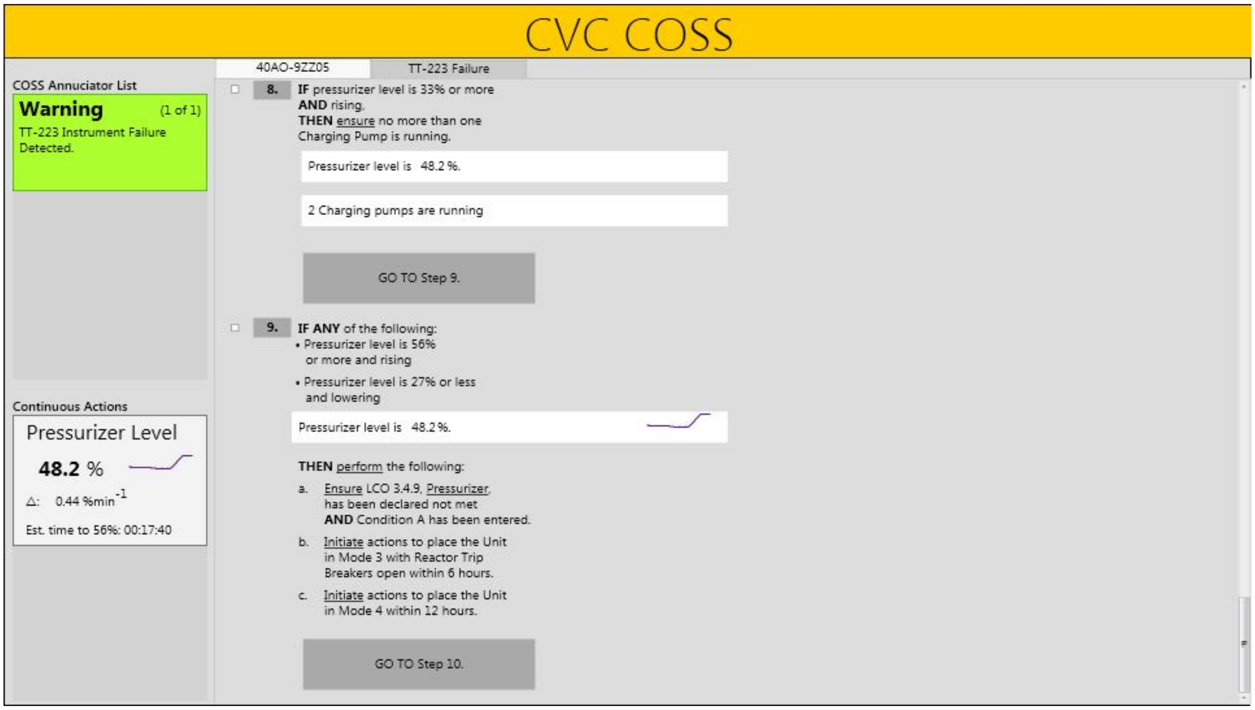


Figure 9. (a) Seal Injection level 2 display. (b) Makeup level 2 display. (c) Letdown Flow, temperature, and backpressure controls.

The COSS builds for the plant build on the digital HSI by conceiving additional features in the underlying DCS and HSI. The COSS implemented a Type 2 CBP system that provided real-time variable status embedded in the procedure and guidance for selection of the appropriate path (see Figure 10). Note that earlier versions of the COSS included additional CBP functionality such as soft controls and automation, but these features were omitted from the operator study due to concerns over the regulatory feasibility of these features.

The COSS was able to incorporate the underlying prognostic diagnosis system PROAID as described previously. PROAID is capable of determining system faults such as leaks and blockages from available sensor data. The spatial sensitivity of the diagnosis is dependent on the richness of the available instruments. One of the unique features of PROAID is that it only requires defining the system at the P&ID level. The PROAID system then trains from steady-state data to be able to recognize faults.



CVC COSS

40AO-9ZZ05 | TT-223 Failure

COSS Annuciator List

Warning (1 of 1)

TT-223 Instrument Failure Detected.

Continuous Actions

Pressurizer Level

48.2 %

△: 0.44 %min^{-1}

Est. time to 56%: 00:17:40

□ **8.** **IF** pressurizer level is 33% or more
AND rising,
THEN ensure no more than one Charging Pump is running.

Pressurizer level is 48.2 %.

2 Charging pumps are running

GO TO Step 9.

□ **9.** **IF ANY** of the following:
- Pressurizer level is 56% or more and rising
- Pressurizer level is 27% or less and lowering

Pressurizer level is 48.2 %.

THEN perform the following:

a. Ensure LCO 3.4.9, Pressurizer, has been declared not met **AND** Condition A has been entered.

b. Initiate actions to place the Unit in Mode 3 with Reactor Trip Breakers open within 6 hours.

c. Initiate actions to place the Unit in Mode 4 within 12 hours.

GO TO Step 10.

Figure 10. CVCS COSS with Type 2 computer based procedure and COSS warning from fault diagnostic system.

Fault detections from PROAID are conveyed to operators through the HSI screens using a highly salient and distinct yellow-green color. The CVCS overview is organized as a P&ID to support conveying fault diagnostics from PROAID. The fault diagnostics require highlighting sections of piping and components to show operators the location of a detected fault. The fault detections also feed a rule-based expert system that can provide fault specific guidance to the operator, allowing mitigating actions to be performed before needing to follow procedure paths that might require taking the plant offline. The workshop examined variations of COSS where: the control room supervisor (CRS) used the COSS at their desk, and the reactor operators (ROs) had a duplicated COSS at the boards (see Figure 11), and a second variation where the ROs used the COSS from the board and the CRS provided oversight from their desk.

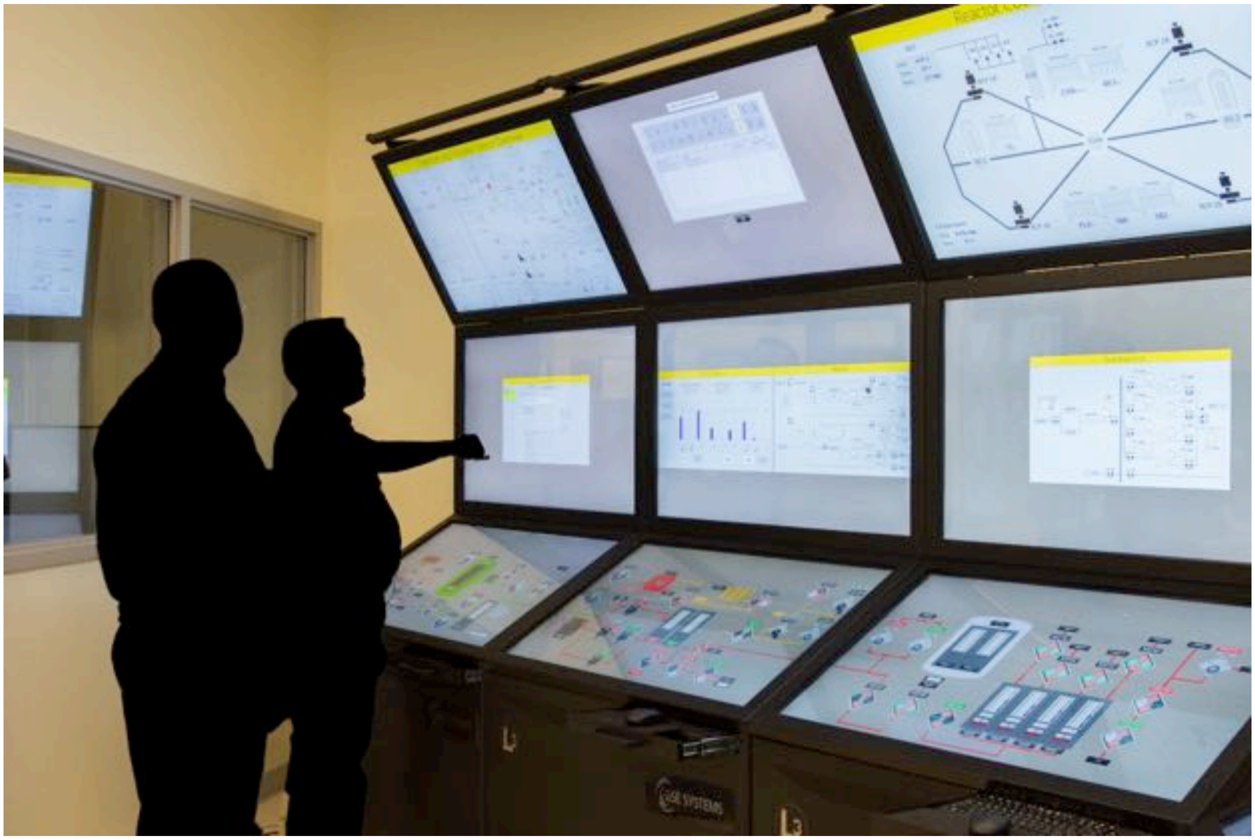


Figure 11. Operators (masked to maintain confidentiality) operating COSS from the boards.

6. INITIAL OPERATOR-IN-THE LOOP EVALUATION STUDY

6.1 Overview

In August 2016, we conducted an interface evaluation workshop with 6 licensed reactor operators. The workshop was intended to accomplish several goals. The first was to assess whether the COSS concept could aid operators during abnormal events. Secondly, we sought to capture operator impressions regarding the acceptance of COSS-like technology in the control room. The COSS prototype provided higher levels of automation compared to existing control systems. Operators may feel uncomfortable relinquishing control to technological systems. Lastly, the operators were used to identify potential shortcomings of the COSS concept and to ideate potential remediations and improvements.

6.2 Method

In August of 2016, two crews of licensed reactor operators visited INL to participate in a LWRS-COSS workshop. Each crew consisted of three individuals, and the crews participated on consecutive weeks. This allowed us to capture unbiased first impressions from each operating crew. The HSSL nuclear control room simulator was configured to represent the control room of the visiting crews. Prior to the data collection the crews conducted a small loss of coolant scenario to familiarize themselves with the glass-top controls and to validate the indicators and controls functioned as expected in the virtual control room.

6.3 Study Design

Each crew conducted a fault scenario with three variations of a CVCS control board. As a control condition the conventional analog control board was represented. In this condition the board was represented as it currently exists in the operator's plant. A second condition represented a hybrid analog/digital control board with large overview displays and a digital HSI. The second condition represented currently available technology would be commercial available for control room upgrades. The final condition incorporated advanced COSS concepts that are not yet commercially available. The following subsections describe these conditions in more detail.

6.3.1 Description of COSS Implementation

The COSS is defined here as a conglomeration of traditional and advanced control system technologies and human factors interaction concepts that are designed to function as a whole to assist operators in monitoring, controlling, and managing control processes in normal and abnormal operating conditions.

The term *designed* is of critical importance to understanding the definition. A control system and HSI could incorporate the technologies in a haphazard fashion. The resulting product could, on paper, have the same functionality, but be suboptimal to plant operations and operator interactions. The COSS concept is philosophically distinguished by incorporating design thinking into the creation of the product. Design thinking is a synthetic inductive process (solution-focused) in contrast to traditional scientifically rooted human factors that tends to be analytic and deductive (problem-focused) (Brown, 2009). The COSS concepts were conceived by thinking about what would be most ideal to the operators should a problem arise, and then fitting technology to the solution. In this manner it is a user-centered design process rather than an engineering driven design process.

This iteration of COSS was implemented for the Chemical Volume Control System (CVCS) of a pressurized water reactor (PWR). The CVCS is housed within containment and is part of the primary reactor coolant system. It serves a number of important functions necessary for running the plant for long-periods of time. It is responsible for maintaining the chemistry of the primary coolant by filtering out contaminants as well as controlling boron concentration through addition and dilution. The CVCS also provides a high-pressure water supply for the reactor coolant pump seals, and is used to manage the inventory of primary coolant. The HSI simulated a hybrid control board with both analog and digital instrumentation and control such as those anticipated to be found in modernized Generation II NPPs. The digital portion of the hybrid CVCS consisted of two large digital overviews with two smaller touch displays, while the analog portion consisted primarily of safety indicators and controls. The prototype was deployed in the INL HSSL—a full-scale, full-scope, reconfigurable glass top nuclear control room simulator (Boring, Agarwal, Fitzgerald, Hugo, & Hallbert, 2013). The HSSL simulator allowed the hybrid COSS control board configuration to be compared to a more traditional digital HSI as well as the existing analog configuration (see Figure 12).

The COSS prototype emulates several advanced technologies to help operators monitor and control the CVCS while also enhancing their ability to detect and mitigate faults. A control room can have over 10,000 analog indicators and controls in addition to indications from the plant computer and other sources. Operators must constantly monitor and integrate information across sources to assess the current state of the plant. As plants are modernized, digital infrastructure supplants existing analog systems. Digital infrastructure can be advantageous because it allows additional information to be provided to operators, but this extra information may also compete for the operator's attention. One approach to organizing and prioritizing the available information is to use large overview displays to provide operators "at a glance" system status information. More detailed system and component level information is available by “digging” down through hierarchically organized displays.

Most NPP control rooms predate the existence of modern digital alarm list displays. With existing control rooms the alarms are grouped into windows at the top of each control board. This arrangement can be beneficial to operators because they can quickly assess the state of the plant on scanning the alarm tiles. The arrangement of the alarms is static and the operators can rely on their ability to recognize familiar or unfamiliar patterns. The CVCS prototype incorporated a like-for-like digital annunciator window replacement with an alarm list. The digital replacements offer lower maintenance and replacement costs compared to their analog counterparts. The like-for-like replacement maintains the operator's ability to scan the alarm boards and to respond to incoming alarms with existing procedures. The annunciator windows also provide a means of grouping alarms and prioritizing their importance. Less critical alarms can be sent to the alarm list. While the alarm list may not facilitate rapid scanning it does have some unique advantages over the annunciator windows. The alarms in the list are time stamped and can be interactively filtered to identify critical information.

During operational scenarios, the PROAID system actively monitors plant sensors and components. When a fault occurs it can detect and inform operators to abnormal conditions before plant variables exceed alarm thresholds. Once a fault is recognized by PROAID, the HSI highlights what component(s) that may be at fault. CBPs integrated with an expert knowledge system provide operators actions to mitigate undesirable plant events and return the plant to a safe operating condition with the least amount of upset possible. This additional information could be sufficient to avoid the costly endeavor of taking the plant offline.

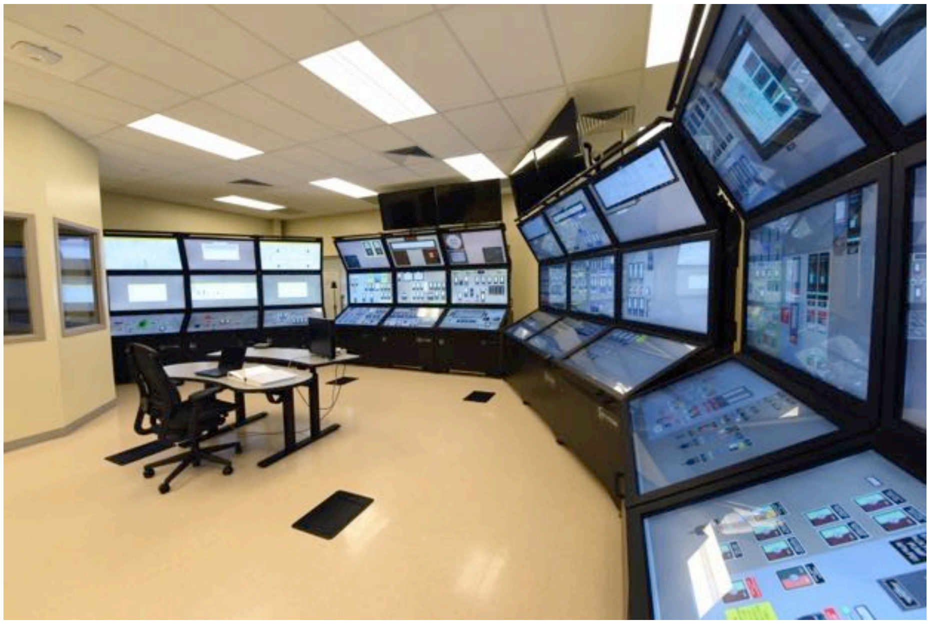


Figure 12. The Human Systems Simulation Laboratory nuclear control room simulator. The hybrid COSS-CVCS is represented on the group of 3 bays depicted on the far left.

6.3.2 Scenario Description

Operators performed the same scenario using the existing analog control boards and the modified control boards with the COSS. In the scenario, the operators were presented with a fault causing a loss of letdown. The letdown isolation event was produced by an instrumentation and control malfunction. With the conventional boards, the letdown isolation resulted from a setpoint failure of the temperature controller. The setpoint fails high with a ramp of 100 seconds, which causes the nuclear cooling flow to increase briefly before closing to its minimum value of 20%. The reduced cooling flow through the letdown heat exchanger results in the letdown flow temperature increasing. A temperature interlock linked to the temperature controller causes a first control valve to close at a temperature of 135° F and a second control valve to close at 138° F. The COSS HSI provided additional information that the operators did not have with the traditional control boards. In the COSS implementation the letdown isolation is caused by a failure of temperature controller failing high, then jumping around for a few seconds, then failing low. The cascade is the same for the scenario completed with the traditional control boards and the scenario completed with the COSS. The failure ultimately results in nuclear cooling water flow being restricted and the two control valves closing.

6.4 Results

Licensed reactor operators are a rare and expensive commodity when it comes to conducting human factors studies. As a consequence, traditional quantitative performance measures are of limited validity due to sample size constraints. Here we relied on qualitative methods to elicit and capture operator feedback. Following each scenario, an independent human factors consultant, with 30+ years of experience in nuclear human factors engineering, led a semi-structured discussion. The format presented the operators with the same set of questions for each condition. The semi-structured format allowed for additional follow-up questions and discussion. During discussion several human factors practitioners recorded operator feedback and comments. After the workshop the comments and feedback were compiled and examined, which yielded several themes pertaining to various aspects of the COSS prototype: layout and style, controls and automation, and COSS fault detection functionality. The important feedback pertaining to the CVCS implementation of the COSS is summarized in the following sections.

6.4.1 HSI Layout and Style

6.4.1.1 Hierarchical Organization

Operators expressed preference for hierarchical organization with task based displays. The displays should normally be dedicated to a single screen or set of screens belonging to a single subsystem even if it is possible to bring up a screen from any subsystem. It was recommended that the overview displays be as large as possible to permit the information on the display(s) to be readable from a distance. The overview screens should provide a holistic and rapid depiction of the system. Operators prefer use of graphical representations, mimics, colors and other coding techniques to facilitate recognition of important information. The overview screens should be intended for monitoring only and should not contain any soft controls. Task based displays should tailor the available indicators to the task. The presentation scheme needs to clearly differentiate between controls and indicators. Operators are trained to look for confirmatory indications after performing control actions. Operators would like to have feedback indicators co-located with controls. The *tags* and labels presented in the interface should be identical to the procedures.

6.4.1.2 P&ID Layouts

P&ID layouts should resemble plant engineering and training materials. For example, if charging pumps are presented C, B, A from top-to-bottom in training materials, they should be represented in that same order in the HSI.

6.4.1.3 Display Clutter

Operators are sensitive to the amount of information on a display. Detailed information should be available but should normally be hidden from view and made accessible as pop-up windows that only appear on demand. Operators preferred pop-ups to dedicating *faceplate* space for detailed panels. They felt dedicated screen space would be wasted when the faceplates are not being used. Operators expressed that the use of trends should be carefully considered. In the correct context the trend indicators provide valuable information permitting operators to better to predict future states. But, too many trends can be overwhelming and could lead to what the operators called "death by information." Operators had mixed feelings regarding auto-scaling Tufte (1983) sparkline-styled very small line charts. Some operators expressed that they wished they could set the axis limits.

6.4.1.4 Use of Color

The study found operators strongly disliked the dullscreen implementation of the HSI in which the use of color is reserved exclusively to convey only important information. Operators strongly preferred the traditional red and green valve status indicators, even when compared to high contrast monochromatic indicators within the dullscreen implementation. The interface incorporated black and purple trend lines to distinguish multiple axes. The operators thought that more contrast was needed between the two colors.

6.4.2 Controls

6.4.2.1 Maintaining Hard Controls

Operators thought it was important to keep hard controls (analog buttons, dials, switches, etc.) for critical and time sensitive actions such as tripping a turbine or scramming the reactor.

6.4.2.2 Soft Control Accidental Activation

Operators expressed anxiety about soft control buttons accidently being clicked because of user error or spurious touch panel input. Operators suggested that certain control actions need to have confirmation dialogs to prevent control actions from taking place from accidental input. Operators even suggested that buttons should remove focus to avoid being accidentally triggered and that the cursor should automatically move away from clickable button if it is left on top of a button for a set period of time.

6.4.2.3 Touchscreen Reliability / Secondary Input Device

Operators were concerned that a touchscreen failure could interfere with operations and suggested that a backup input device such as trackpad should be provided. In the event of a screen failure it should be possible to quickly and easily reconfigure what is shown on the displays. Operators also noted that they can use the mouse pointer to indicate what they are looking at on the screen to support peer checking.

Some operators are shorter, making it difficult for them to operate touchscreens. A trackpad on the apron would provide an ergonomic solution for these operators.

6.4.2.4 Ergonomic Considerations

Standing workstations present ergonomic considerations to maintain touchpanels in the reach envelope of 5th percentile females to 95th percentile males by stature. In accordance with NUREG-0700 the font on the displays need to maintain at least 16 minutes of arc across individuals (U.S. Nuclear Regulatory Commission, 2002).

6.4.3 COSS Functionality

6.4.3.1 Computer Based Procedure

They liked the capability to show plant data linked to a procedure step (decision aiding automation), which is defined as a Type 2 CBP system. They did not want the CBP system to take actions automatically to control the process (defined as a Type 3 CBP system; IEEE-1786, 2011) without their permission. They commented that the CBP system decision aiding automation was very useful, but suggested that problem diagnosis decision aiding also would be very helpful. They said that this capability should permit early identification of a developing problem and permit them to take earlier actions to mitigate the developing problem.

The CBP guided operators through procedures by highlighting the current step, as well as providing plant variable values within the procedure step itself. The COSS also provides contextual information within the procedure steps. Specifically, the COSS displays trend information within the procedure step to provide historical information about the relevant variable so that operators can assess abnormal fluctuations. Both crews noted the significant improvement with this integrated information.

Operators wanted the ability to be able to look ahead in the procedure. They also wanted the current step to be more apparent by being stylized differently.

An ad-hoc scenario variation where the reactor operators were using CBPs at the control boards versus at the SRO workstation revealed operators might respond more quickly when CBPs are available at the board, but operators reported concern with a keyhole effect where they are inclined to focus too much on the CBP to the exclusion of other information. A suggestion was that the SRO should have the ability to monitor their progression through the procedure from their workstation so that the SRO can maintain broad situational awareness of the plant and the information that the ROs are actively viewing.

6.4.3.2 PROAID Fault Detection

The existing instrumentation at the NPP may not be sufficient for increased levels of automation or for diagnostic systems like PROAID. Plants may need to consider upgrading instrumentation (i.e., sensors) to realize automation benefits.

Operators emphasized the importance of the interface to provide a transparent view of PROAID systems functioning so operators can validate the diagnostics and build trust in the system. The PROAID fault diagnosis system monitors sensors to detect faults and determines faults using logic that operators might use.

6.5 Conclusions

The operators who participated in this study lacked experience with modern DCS capabilities and digital HSI concepts and functionality. We must remember most nuclear control rooms were originally designed and implemented several decades ago. The nuclear industry has an aging workforce. Control system upgrades are being implemented with more recent technology. In comparison to decades past, there are many cases were control automation can handle tasks at least as reliably as human operators. When control automation is adopted, the role of operators shifts from continuously manipulating controls to monitoring and anticipating the automated system. In some circumstances this may be a philosophical departure from current operations. In particular, the COSS implemented higher levels of automation than operators were accustomed to, but operators expressed a desire for this automation after sufficient familiarity was attained and if sufficient reliability could be established. The information obtained from the evaluations will be incorporated into the CVCS-COSS and evaluated with licensed crews. The roadmap from prototype to actual control technology is long and arduous, but we hope our operator centric design approach influences control room modernization in the short-term and leads to next-generation advanced control systems in the long-term. The PROAID fault diagnostic system plays an important role in making COSS technologically feasible, though there is still work to be done in regard to the underlying technology that would drive an actual COSS implementation. Our work here lays the design concept groundwork for how to integrate these technological systems once they mature.

(This page intentionally left blank)

7. EXPANDED OPERATOR-IN-THE-LOOP STUDY

7.1 Overview

We conducted an additional interface evaluation workshop with 3 licensed operators (see Figure 13). The workshop was intended to address and expand on the same goals from the initial operator-in-the loop study. These goals included assessing the utility of the COSS concept as an aid for operators during abnormal events and capturing operator impressions regarding the acceptance of COSS-like technology in the control room. Since the COSS prototype provided higher levels of automation compared to existing control systems within the main control room, operators could potentially feel uncomfortable relinquishing control to these advanced technological systems. Another goal of this expanded operator-in-the loop study intended to identify potential shortcomings of the COSS concept and to generate discussion with operators on solutions to these shortcomings and general improvements to make the COSS concept more usable as an operator aid. Lastly, the goal of this expanded study was to examine a new and simplified implementation of the COSS concept on another plant system. Specifically, a distributed variant of the COSS concept was implemented as part of the turbine control system (see also Boring et al., 2017).

Figure 13. COSS operator-in-the-loop scenario run in August, 2017.

7.2 Method

In August of 2017, a single crew of licensed reactor operators visited INL to participate in a LWRS-COSS workshop. The crew consisted of three individuals that were not part of the initial operator-in-the loop study. This crew served as an additional sample of operators from the same plant. This additional sample was valuable to provide another independent sample of operator feedback and comments. Furthermore, this third crew and its unique perspective improves the collective sample of operators by making it more representative of the operator personnel at the collaborative utility. The HSSL nuclear control room simulator was configured to represent the control room of the visiting crews. Prior to the data collection the crews conducted a small loss of coolant scenario to familiarize themselves with the glass-top controls and to validate the indicators and controls functioned as expected in the virtual control room.

7.2.1 CVCS COSS Implementation

The CVCS COSS is visually identical to the implementation used in the initial operator-in-the-loop study (see section 6.3.1). This iteration of the CVCS COSS contains additional functionality necessary to support evaluating the COSS as operators interact with it on a new expanded set of scenarios. The notable difference between the current implementation and the prior CVCS COSS implementation is the live diagnostics achieved by the underlying PROAID fault detection system and the integration of two additional fault scenarios in the 2017 study.

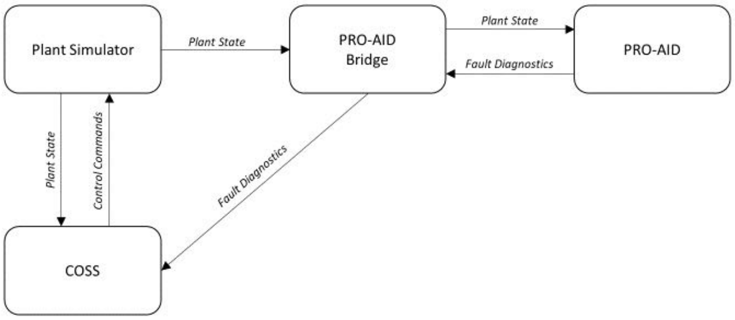


Figure 14. Communication bridge between PROAID, plant simulator, and COSS.

Communication between the simulator and PROAID was enabled by developing a *bridge program* as shown in Figure 14. Previous INL efforts have identified how to enable two-way communication between gPWR and the development environment for COSS. A common language runtime class was developed to retrieve and parse the fault diagnostic data from the PROAID bridge program to the plant-specific simulator.

7.2.2 Additional Scenarios for Real-Time PROAID Testing

7.2.2.1 Small Loss of Coolant Outside of Containment with COSS

The scenario began with the plant at 100% power. A malfunction caused a small leak in the letdown line immediately downstream of the regenerative heat exchanger. PROAID was capable of identifying the leak within 18 seconds of the fault being initiated. The plant alarms do not reach threshold conditions until 26 minutes after the fault is inserted. Because of limitations of the available indications, PROAID cannot determine the exact location of the fault and can only narrow it down to letdown line between an isolation valve and the reactor coolant filters. PROAID is also unsure whether the fault is a break or blockage. When PROAID detects the fault the fault diagnostic information is communicated to the COSS HSI. The HSI highlights the potentially faulty components in a green-yellow aura and provides description of the fault in the COSS window. Operators are advised to use the loss of letdown procedure to isolate letdown and continue running plant. The loss of letdown procedure is embedded in COSS as a CBP.

Operators found the fault diagnosis ahead of plant alarms useful. Operators suggested that having the components highlighted might provide a cue that could cause operators to focus on the wrong information. They suggested that the key piece of information that operators should be directed to in this scenario is the reduced letdown flow. Doing this is a valid suggestion and would require being able to take the fault information from PROAID and determine what the most relevant indicator or set of indications are for operators. Further analysis is needed to determine how this could be accomplished.

7.2.2.2 RCP Seal Failure with COSS

In this scenario, the #1 seal is faulted on RCP 1A. The leakage rate is below the plant alarm threshold. PROAID detects the fault within a few seconds and is able to isolate the problem to the RCP seal. The leak rate is small enough to not trigger a plant alarm. The COSS notified operators to the problem and, by examining RCP pressures, they were able to diagnose the seal leak within 2 minutes. The leak rate was small enough that normal letdown and charging can be maintained. The scenario was stopped after the diagnosis was made. In the debriefing operators discussed what the next steps at the plant would be to report and mitigate the failed seal. Operators found the COSS useful in this scenario. The green aura on the RCP seal was a salient and informative cue in conjunction with the mini trend lines (sparklines) presented on the Seal Injection Monitoring Screen.

7.2.3 Alternative Fault Detection Approach

In contrast to the PROAID approach for fault detection, the methodology supporting the TCS COSS concept does not hinge on a centralized, system-level model built from conservation equations. Rather, at the risk of sacrificing generality and flexibility PROAID provides, the TCS COSS methodology seeks to focus on identifying key phenomena of particular interest and more precisely describing their mechanisms in detail—informed by a high degree of physical understanding. This means that the TCS COSS approach incorporates engineering parameters such as heat transfer coefficients and friction factors. Consequently, building a model for fault detection in this way requires a much more specific analysis of the given system, but yields some insights that might otherwise be unavailable. Chief among the benefits is the ability to include fault parameters in the constituent equations, which may accelerate not only fault detection times, but also isolation and prognostication capabilities. By accounting for anticipated fault types, the model is able to instantaneously attribute an unexpected signal value to some pre-defined category and remove uncertainty about the root cause or nature of the fault. While the fault's effects may be apparent in multiple plant locations, this allows the system to bring the operators' focus to the originating component.

Of course, there are inherent pitfalls with this approach. What if the designer is unable to account for a fault that occurs? Will the system erroneously designate attribution or ignore the fault? To handle these cases, the model also incorporates general fault parameters, which can indicate a fault and even isolate its location but may be unable to describe its failure mechanism.

For the purpose of recent operator studies, no such detailed model was created. Instead, for the presentation of a proof-of-concept and to gather initial impressions, four specific scenarios were chosen. These scenarios were chosen both to be realistic and also to rely on feasible fault signatures for a model to detect and characterize. For example, two scenarios involve a calculated mismatch between steam valve position and steam flow. Another scenario assesses turbine bearing vibration by comparing each single bearing with vibration measurements of adjacent bearings. Finally, a different scenario raises a warning to the operators when an action is taken that does not correspond to a procedure. While these are diverse methods of fault detection for a diverse set of faults, they all represent simple mathematical or logical relationships that could be included in the mathematical models of plant components in a more general fashion. It is important to emphasize this system is intended to compliment the capabilities of the PROAID system and makes no attempt at competing with the capabilities of the PROAID system. The TCS fault detection scenarios are provided as proof of concept of the HSI for fault alerting. Implementation details of the fault detection remain the work of future research, including potential integration into PROAID.

7.2.4 TCS COSS Implementation

A generic and decentralized implementation of the COSS concept was designed for use with the TCS. The TCS provides functionality for shell and chest warming and ramping the turbine to sync speed in a controlled manner during startup. When syncing the TCS is designed to increase load and then control load by modulating the control valves. Functionality is also provided to calibrate the I&C, perform valve tests, as well as perform trip tests. The TCS also ensures the turbine is not damaged by placing it on the turning gear while offline and monitoring turbine speed and other indications; the TCS will trip the turbine if parameters fall outside of their operating envelope. The TCS was based on a design study document and existing implementations of TCS for NPPs developed by Westinghouse using the Ovation platform. A TCS emulating the look and feel of Ovation was developed to support an end-state design workshop for the utility as well as support a TCS COSS implementation.

7.2.5 Analog TCS

The TCS spans an entire section of the control board adjacent to the steam generators panel. Central to the turbine, is the analog turbine control system, which can be seen in Figure 15.

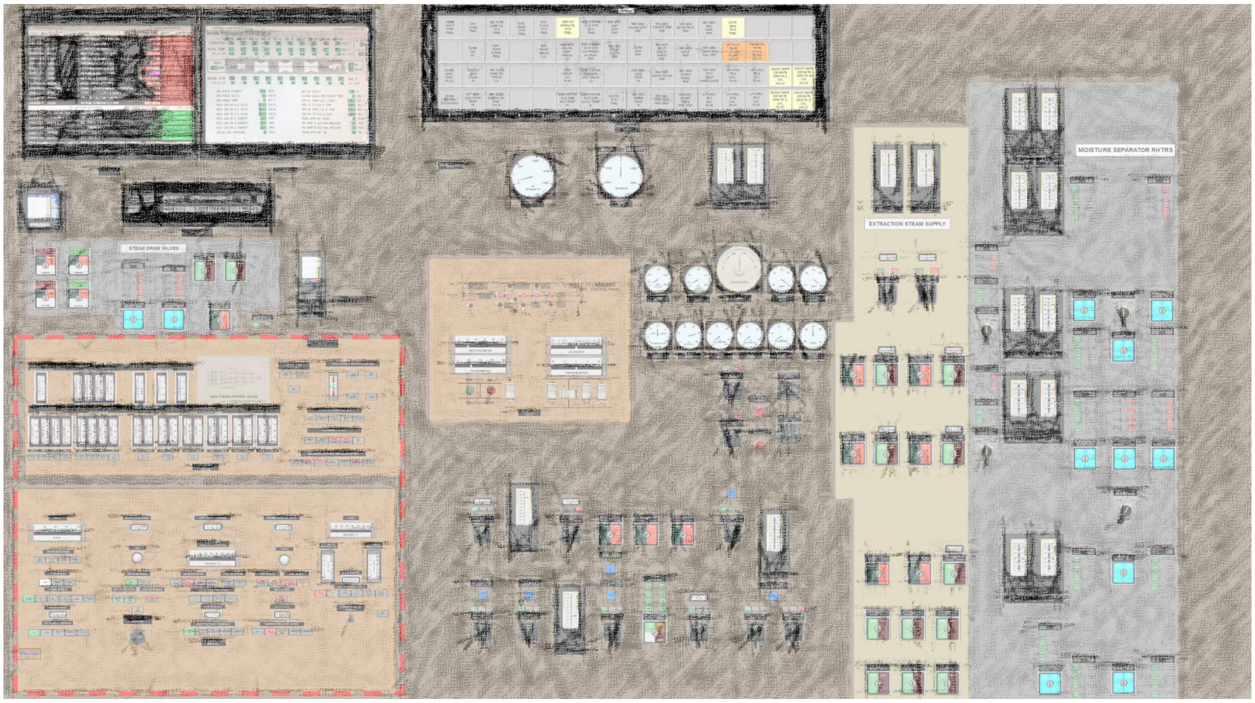


Figure 15. Sketch of the control board for containing the existing analog turbine control system.

7.2.5.1 Digital TCS with Overview Screen

As part of another project with the collaborative plant focused on the turbine control system upgrade, a digital turbine control system was prototyped and placed on the board. The digital TCS replaced all turbine controls with the exception of the steam drain valves and the generator controls and indicators. Additionally, two existing console display units were unaffected by the digital TCS upgrade. The digital TCS was comprised primarily of two thin-clients with several windowed displays that supported all relevant turbine activities. In addition to these two primary displays, an overview screen specific to the TCS was included (see Figure 16). The overview screen houses the COSS implementation for the TCS. The TCS overview provides monitoring of the TCS as well as functionality related to the turbine valves, steam drain valves, generator, moisture separation reheaters, lube oil, and bearing vibrations and temperatures.

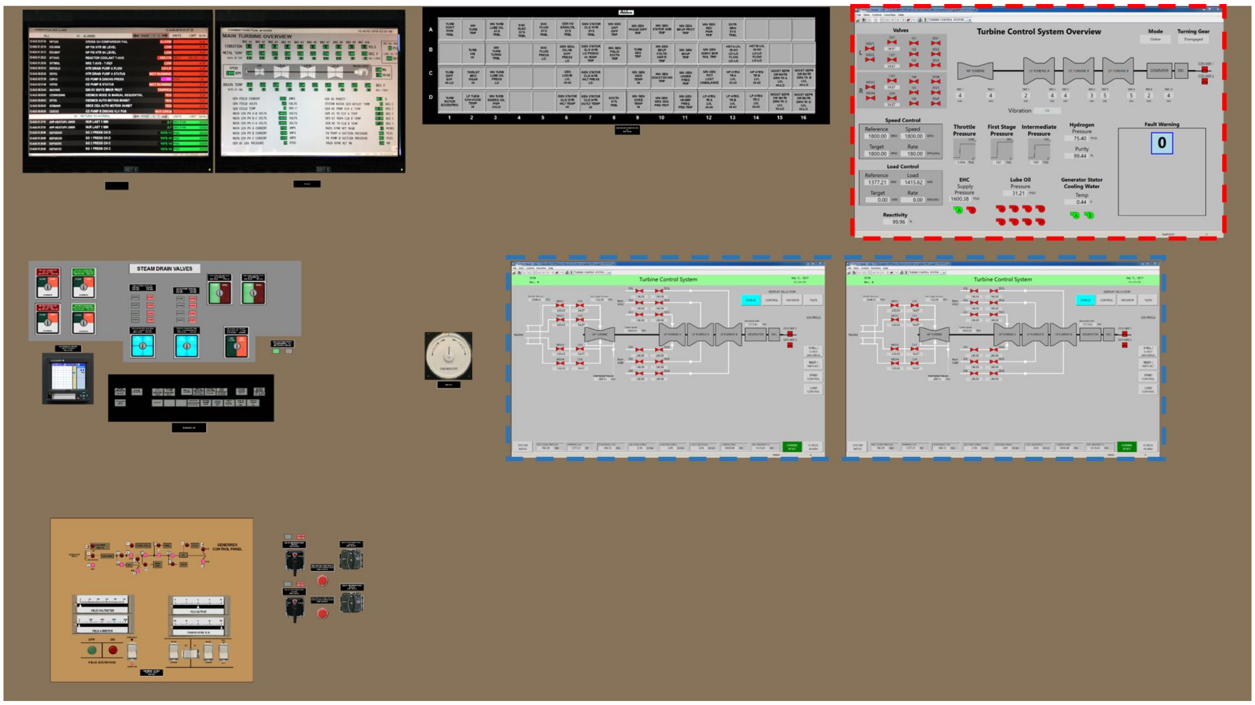


Figure 16. Digital TCS embedded within the existing control board (blue highlight). The TCS specific overview screen (red highlight) was positioned above the digital TCS interfaces.

7.2.5.2 Alternative COSS Interaction Concept

The previously described implementation of the COSS concept for the CVCS had a large footprint within the interface. The COSS also used dedicated regions of the interface to support the various technologies, such as the warning system, recommender system, and computer-based procedures. Furthermore, the COSS provided prescriptive diagnostics (prognostics) that provided the operators with clear paths to mitigate the root cause and maintain the plant within an operating envelope that would avoid a plant trip. This approach hinges upon the ability to provide a clear path based on accurate diagnoses of the root cause. This requires the diagnostic system (PROAID) to isolate the fault and an expert knowledge on how to respond to the fault encapsulated with the COSS. PROAID's ability to isolate component faults can be enhanced by incorporating additional indications. Identifying a comprehensive sensor set is a rather straightforward engineering exercise. However, developing the appropriate responses to all the possible faults could be challenging. Here we examine an alternative implementation that attempts to provide a more generic and less prescriptive interface of the COSS concept. This implementation for the TCS focused more on providing operators with basic information to aid them in diagnosing the issue, finding the root cause, and then identifying a recovery path. This reduced functionality alternative would also require a less obtrusive footprint embedded solely on the TCS overview screen. This allowed the COSS to be visible without interfering with the TCS control displays themselves and therefore was potentially less obtrusive.

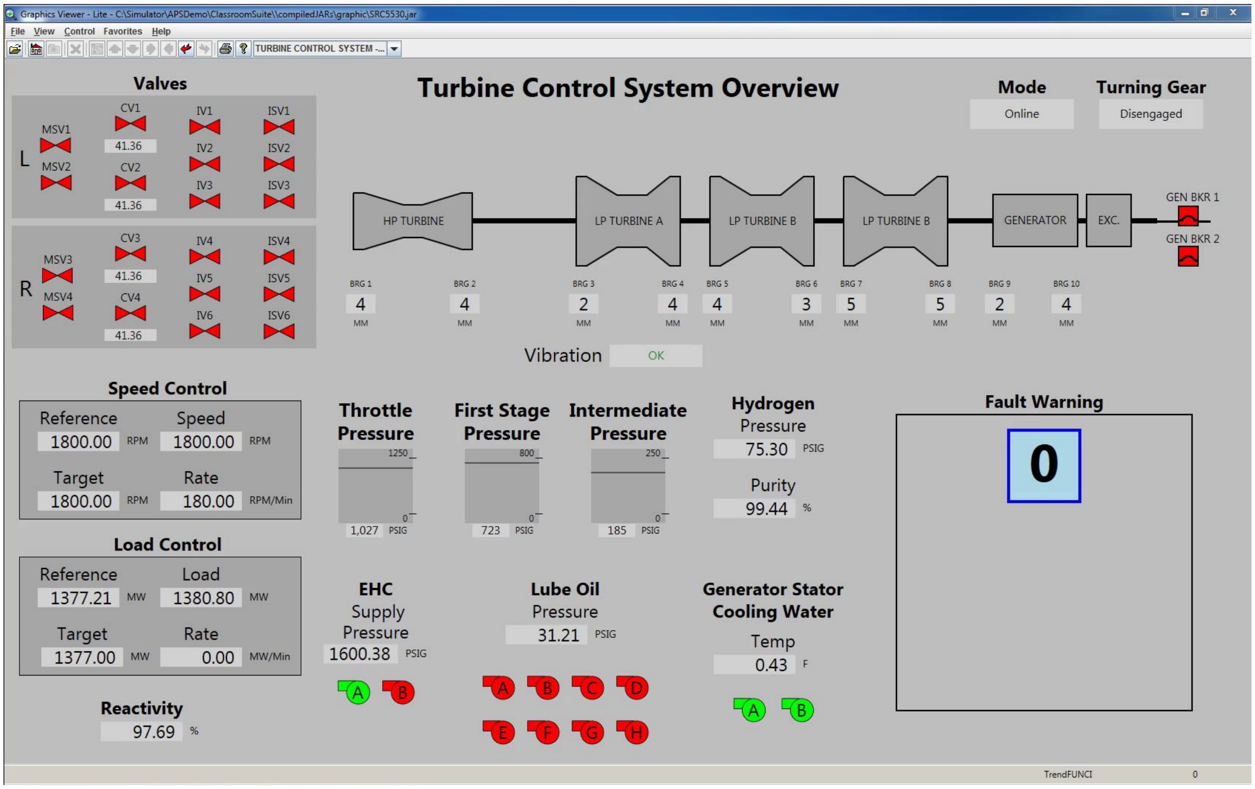
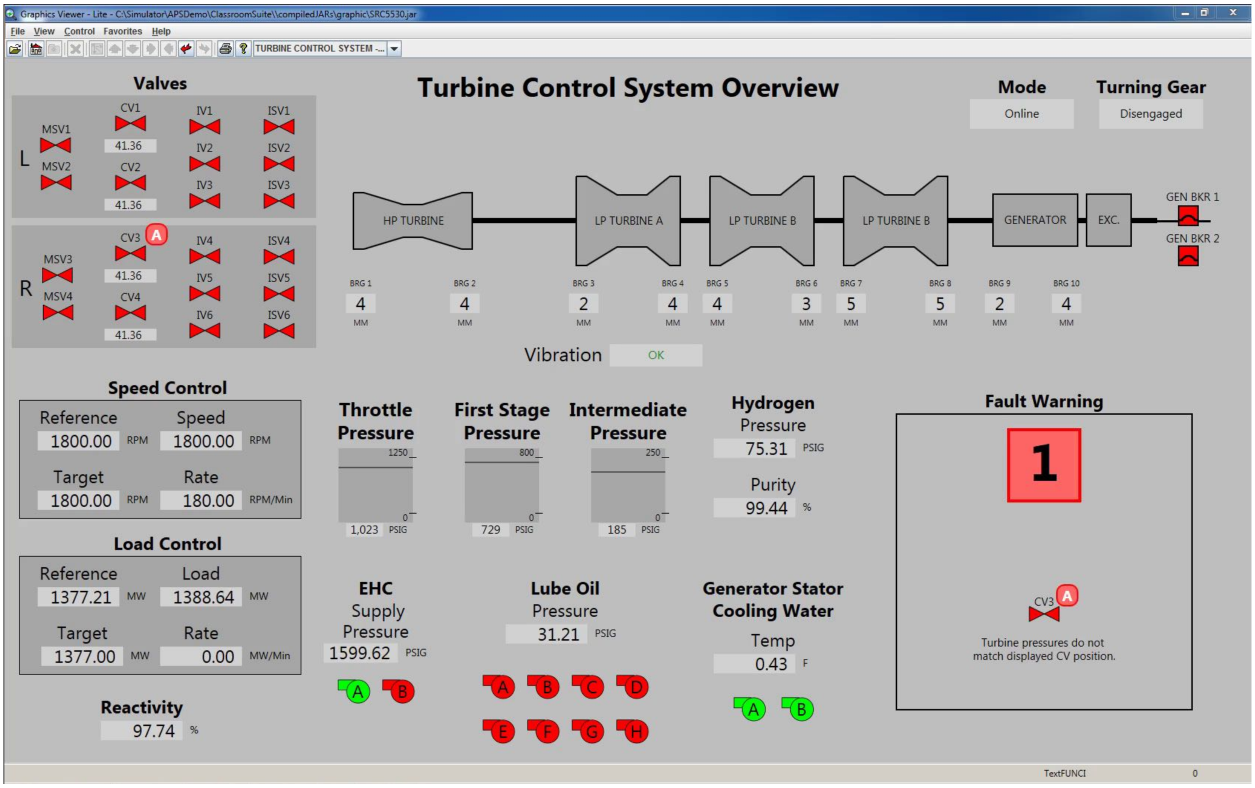


Figure 17. TCS COSS implementation depicting the fault warning region in the dormant mode in which no fault is detected indicating a normal operating state.

The TCS COSS implementation consists of a fault warning region, which provides an indication of the number of active faults and fault descriptive information. When no issue is detected the system displays a zero in a blue box to denote a system normal state as can be seen in Figure 17. Upon detecting a fault, the fault warning region changes to alert the operator of detected issues, as can be seen in Figure 18. The number of detected issues is displayed with a prominent number highlighted with a red background to draw the operators' attention. Additionally, the faulted component is displayed with both a corresponding marker and a text message describing the issue. The marker uses a letter designation, i.e. the letter A, to tag the faulted component in the overview and support multiple issues being presented simultaneously to the operator. Tagging the component is beneficial since it provides the context within the display to aid the operator in determining possible causes for the fault and how the overall system may be affected. The COSS system then processes the faulted component to determine potential mitigating actions and takes those actions if possible. The actions are much simpler then the computer-based procedure driven mitigation strategies of the CVCS COSS implementation. The mitigation strategies included with this design concept are purely information based adjustments, such as replacing an erroneous indicator value with an estimated value determined by the fault diagnosis. Several different scenarios were presented to operators to demonstrate the concept and elicit feedback on the design.

The four scenarios examined included an erroneous turbine control valve sensor, an erroneous turbine bearing vibration sensor, and a load ramp rate failure. The COSS behaved differently for each scenario, but the same general actions were performed by the COSS in which the fault is detected, the operator is visually alerted to the fault, and when possible the COSS takes mitigation actions. For example, the COSS replaces the incorrect value with an estimated correct value and provides a text message to convey this interface alteration to the operator. An additional graphical representation of the discrepancy detected by the COSS fault diagnosis was also presented to operators (see Figure 19).



Graphics Viewer - Lite - C:\Simulator\APSDemo\ClassroomSuite\\compiledJARs\graphic\SRC5530.jar

Turbine Control System Overview

Mode: Online

Turning Gear: Disengaged

Valves: CV1 41.36; CV2 41.36; CV3 41.36; CV4 41.36

Bearings: BRG 1 4 MM; BRG 2 4 MM; BRG 3 2 MM; BRG 4 4 MM; BRG 5 4 MM; BRG 6 3 MM; BRG 7 5 MM; BRG 8 5 MM; BRG 9 2 MM; BRG 10 4 MM

Vibration: OK

Speed Control
Reference 1800.00 RPM
Speed 1800.00 RPM
Target 1800.00 RPM
Rate 180.00 RPM/Min

Load Control
Reference 1377.21 MW
Load 1388.64 MW
Target 1377.00 MW
Rate 0.00 MW/Min

Reactivity 97.74 %

Throttle Pressure 1,023 PSIG

First Stage Pressure 729 PSIG

Intermediate Pressure 185 PSIG

Hydrogen Pressure 75.31 PSIG

Purity 99.44 %

EHC Supply Pressure 1599.62 PSIG

Lube Oil Pressure 31.21 PSIG

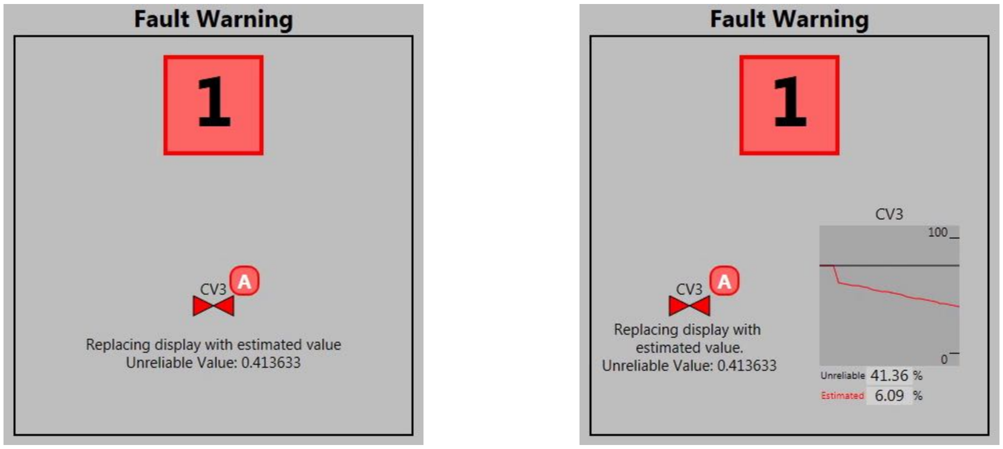
Generator Stator Cooling Water Temp 0.43 F

Fault Warning: 1

Turbine pressures do not match displayed CV position.

TextFUNCI 0

Figure 18. TCS COSS depicting a single fault detected for Control Valve 3 in which the turbine pressure does not match the valve position and steam flow.



Replacing display with estimated value
Unreliable Value: 0.413633

Replacing display with estimated value.
Unreliable Value: 0.413633

Figure 19. TCS COSS Fault Warning text only (left) and text with graphical trend representation (right) depicting the fault detection system detection of an incorrect control valve position.

Unlike the CVCS COSS implementation, this design concept did not provide computer-based procedures, but rather focused on aiding the operator in identifying potential issues associated with plant faults. This simplified approach to aiding operators with fault detection afforded the COSS capabilities to be more easily incorporated within digital interfaces since it retains a smaller footprint within the display.

7.3 Results

The evaluation of the TCS COSS was primarily qualitative in nature. Operators followed a "Think Aloud" protocol while completing the scenarios. The think aloud protocol resulted in a number of findings pertaining to the operators' impression of the TCS COSS and yielded numerous suggestions for improvements. The feedback from operators was recorded by several observers and analyzed. Several themes emerged from the analysis of the feedback. The themes include feedback concerning the prognostic system functionality, organization and layout, trend displays, feature suggestions and requests and concerns for cognitive tunneling.

7.3.1 Prognostic System Functionality

Operators' impression of the TCS COSS were largely positive. In fact numerous operators reported they found this type of system as an effective tool to mitigate some of the burden of operating the plant. The feedback was particularly positive concerning the cues that aid the operator in interpreting potential issues detected by the COSS by visually highlighting the affected component and indication within the display along with the warning message from the COSS itself.

7.3.2 Organization and Layout

This implementation of the COSS was designed to minimize the screen footprint of the COSS system. The operators approved of the implementation in regard to the use of a dedicated screen region, or faceplate, for the COSS warning system. An alternative approach would be to present the COSS as a pop-up that would occur when a fault was detected, but the operators reported a preference for always having some indication of the COSS being present to provide feedback in situations in which the no fault was detected.

7.3.3 Trend Displays

The operators reported a strong preference for trend displays over numerical values. The operators preferred the trend display configuration of the TCS COSS warning region over the text based configuration (see Figure 19). Trend displays are invaluable to the operators since it is difficult to track the thousands of parameters within the control room. The trends relinquish the mental demand of recalling prior indicator values to characterize and determine the trend of a given component or value. The operators can quickly look at the trend graph and ascertain the behavior of a component. The value of trend displays and their rich temporal context cannot be emphasized enough. Beyond just the COSS digital HSI, trend displays are a key feature that should be incorporated as appropriate in the vast majority of digital HSIs to enhance operator monitoring and control capabilities.

7.3.4 Feature Suggestions and Requests

The scenario walkthroughs using the TCS COSS elicited the operators to request a number of features to improve the COSS. The operators requested two features relevant primarily to the presentation of detected faults. First, the operators requested a time buffer for each issue detected by the COSS in order to prevent alarm flooding. Alarm flooding is a prominent issue with existing analog control boards since a single fault can result in hundreds of setpoint alarm thresholds being reached and a cascade of alarms throughout the existing control room. Fortunately, an appropriate alarm management philosophy incorporated with a fault detection system, such as the COSS, mitigates alarm flooding by performing root cause identification and filtering out the erroneous alarms present within existing analog control rooms. Therefore, a time buffer is unnecessary. This feature request made by the operators represents the concept of operations within analog control rooms and demonstrates a promising area in which an operator aid in the form of the COSS can eliminate some of the existing challenges operators are forced to contend with in existing plants.

In a related feature request pertaining to fault detection, the operators reported a scrollable fault list would be beneficial to allow them to track multiple faults over time. Easily accessible fault detection history logs are valuable, since operators can gain additional context by examining prior faults to determine the validity of an existing fault. The scrollable fault list would require operators to be able to interact with the overview display housing the COSS in a more complicated fashion than was anticipated for this implementation of the COSS. Because the COSS is embedded within the overview display, minimal control capabilities were initially envisioned, since the overview is primarily intended for information and little to no control functionality. Additional features requiring more extensive manipulation would require the COSS to be moved to another interface lower on the control with greater accessibility for the operator. Another approach would be to incorporate a dedicated control interface for the COSS, which could house the scrollable fault list in addition to its positioning in a prominent location within the overview display. This combination would afford good visibility for the operator, but also allow them to control the information presented on the COSS with more flexibility.

7.3.5 Cognitive Tunneling Issue

Cognitive tunneling, also known as the keyhole effect or tunnel vision, refers to the restriction of attention with a narrowly defined region. Individuals undergoing a cognitive tunneling state fail to attend to pertinent information and instead fixate upon a small subset of information. As a result, the individual fails to incorporate necessary information into their mental model of the situation, which leads them to make incorrect decisions and take inappropriate actions. One potential issue raised by the operators concerns cognitive tunneling and trust in the COSS fault detection accuracy. When the COSS is functioning properly, the operators' attention is correctly directed to the appropriate faulted component or indicator, but when the COSS makes an incorrect determination, the operators' attention could be inappropriately directed away from the root cause of the fault. Fortunately, this implementation of the COSS was designed with the potential for failures to occur in line with a graceful degradation philosophy. First, the COSS can quickly be dismissed by the operator and overridden in the event it has incorrectly detected a fault. Second, the COSS highlights the issue in both the warning display region and where the component or indicator is located within the overview display. Alerting the operator to examine the component within the context of the existing display supports the operator in determining the validity of the fault detection. The operator is quickly able to view the related components within the overview in order to incorporate the context of the potentially faulted component. Indeed, this alternative COSS design concept was intended to serve as a way to highlight potential issues without providing a detailed prescriptive mitigation path in order to aid the operator in diagnosing the detected fault and letting the operator ultimately make the determination for the validity of the fault. This mitigates some of the potential cognitive tunneling issues that could result from manipulating the operators' attention with the COSS.

7.4 Conclusions

This second study gathered additional impressions of the CVCS COSS prototype that was valuable to further refine the concept. The addition of the two CVCS scenarios further demonstrates the capabilities of COSS and provides a more realistic evaluation for the operators. Indeed, trust in the system to detect issues and alert the operators is paramount for this new form of automation to bring value to the operators as they monitor and control the plant. Without appropriate trust in the system, the COSS becomes another system the operators must manage and could actually prove detrimental to performance and operator workload. The TCS COSS also aided the realism for operators interacting with the COSS because another system was integrated, such that operators could see how the COSS functioned with another plant system. The alternative design concept that was evaluated was also beneficial for gathering important insights into how best to provide operators with pertinent information concerning potential faults and integrate this information with the existing plant displays, such as the TCS overview display.

8. DISCUSSION AND FUTURE DIRECTIONS

The series of operator-in-the-loop studies demonstrated the capabilities of the COSS concept to enhance operator monitoring and control capabilities. The results from the studies suggest this technology aids operators by drawing their attention to fault relevant items and providing contextual information to bolster the operator's understanding of the root cause.

8.1 Discussion

Two important outcomes resulted from this COSS project. First and foremost, the COSS developed and evaluated for this project demonstrated promise as a tool to improve operator situation awareness and aid operators in responding to fault events before they are typically detected via alarm setpoint criteria within existing analog control rooms. This current work represents the state of the COSS technology at the termination of the three-year project aimed at demonstrating the capabilities an intelligent diagnostic system can provide to allow operators to monitor and control the plant more effectively. The operator-in-the-loop evaluations represented a continued iterative design and evaluation effort that was necessary to refine the COSS capabilities and design concept and demonstrate the benefits of the technology so that the nuclear power industry can begin to embrace these technologies in both existing and new plant builds. The operator-in-the-loop studies were performed in two phases, with the first phase evaluating a COSS prototype for the CVCS on a single fault scenario. The second evaluation phase incorporated additional fault scenarios for the CVCS and also examined an alternative COSS interaction style with a prototype developed for use with the TCS. Both COSS prototypes were positively received by operators in these studies.

The other important outcome that can be attributed to the COSS project efforts is somewhat of a byproduct, but still remains quite important in it its own right. The ANIME framework emerged out of the prototyping development efforts required to build the COSS and present its various functionality to operators. The ANIME framework has since been used in a number of other applications including prototype development for usability evaluations needed for control room modernization efforts and the creation of a microworld designed for reduced scope student operator studies.

8.2 Future Directions

The COSS CVCS implementation and evaluation using this representative plant demonstrated the effectiveness of an intelligent operator support system to aid operators in monitoring and controlling the plant. Additional work is required to continue the COSS development so that it can become available for nuclear industry use. The PROAID system must undergo extensive testing based on additional systems in order to verify it can adequately detect faults given the current configuration of the sensors and components within each system. This is a large endeavor, which should be performed with additional collaborative plants.

Acquiring additional industry collaborators is important for a number of reasons. Each plant has a unique configuration that represents a different challenge in terms of the amount of sensors and information the PROAID system can make use of for its diagnostic features. Sampling multiple plants will provide a more comprehensive assessment of the PROAID systems adaptability for use in different plant configurations. Additionally, more utility collaborators will help garner industry attention and buy-in. The COSS technology represents a substantial shift from the current concept of operations at existing plants and will require some license amendments. Given the regulatory environment, it is crucial to gain industry buy-in in order to identify champions that will help shape the regulatory process so that other plants can follow suite and realize the benefits of a COSS system.

The COSS HSI also requires additional developmental work to move it toward use in the nuclear industry. The current COSS implementation uses a small subset of potential plant faults for diagnosis. The PROAID system identifies component faults; however, the language that it uses is not intended for human consumption. A diagnostic language must be developed that translates the PROAID fault detection information into something the operators can understand and use. This process involves extracting language components from existing plant procedures, such as the procedure verbiage and identifying nouns for components. These language components can then be combined in a manner to describe the content from the PROAID diagnostic information into something operators can integrate with their current conceptualization of the plant. This language would be compatible with the existing procedures, which is also important because the language found in the procedures will be carried through to the computer-based procedures during the digitization process of the overall control room modernization effort. COSS is more than a graphical HSI; to help maintain operator situation awareness, it must provide provide graphical as well as lexical information to the operators. The current implementation uses procedures to guide the operators; additional information imparted to the operators will help operators to maintain control and oversight of the system.

9. REFERENCES

Antsaklis, P. J., & Passino, K. M. (1993). Introduction to Intelligent Control Systems with High Degrees of Autonomy In P. J. Antsaklis and K. M. Passino (Eds.), An Introduction to Intelligent and Autonomous Control. Kluwer Academic Publishers.

Astrom, K. J. & Arzen, K.-E. (1993). Expert Control In P. J. Antsaklis and K. M. Passino (Eds.), An Introduction to Intelligent and Autonomous Control. Kluwer Academic Publishers.

Automation World (2014). PLC vs. DCS: Which is Right for Your Operation? https://perma.cc/JD4E-DAJH.

Bennett, S. (1993). A History of Control Engineering, 1930-1955. Peter Peregrinus Ltd., London.

Boring, R. L. (2014). Human Factors Design, Verification, and Validation for Two Types of Control Room Upgrades at a Nuclear Power Plant. Proc. of the Human Factors and Ergonomics Society 58th Annual Meeting, 2295-2299 (2014)

Boring, R., Agarwal, V., Fitzgerald, K., Hugo, J., and Hallbert, B. (2013). Digital Full-Scope Simulation of a Conventional Nuclear Power Plant Control Room, Phase 2: Installation of a Reconfigurable Simulator to Support Nuclear Plant Sustainability, INL/EXT-13-28432. Idaho Falls: Idaho National Laboratory.

Boring, R. L., & Joe, J. C. (2015). Baseline evaluations to support control room modernization at nuclear power plants. Proceedings of ANS NPIC & HMIT, 911-922.

Boring, R. L., Joe, J. C., Ulrich, T. A., & Lew, R. T. (2014, September). Early-stage design and evaluation for nuclear power plant control room upgrades. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 58, No. 1, pp. 1909-1913). Sage CA: Los Angeles, CA: SAGE Publications.

Boring, R., Mandelli, D., Rasmussen, M., Herberger, S., Ulrich, T., Groth, K., & Smith, C. (2016, October). Human unimodel for nuclear technology to enhance reliability (HUNTER): a framework for computational-based human reliability analysis. In 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13), Paper A-531 (pp. 1-7).

Boring, R. L., Thomas, K. D., Ulrich, T. A., & Lew, R. T. (2015). Computerized operator support systems to aid decision making in nuclear power plants. Procedia Manufacturing, 3, 5261-5268.

Boring, R. L., Ulrich, T. A., & Lew, R. T. (2015, August). Dynamic operations wayfinding system (DOWS) for nuclear power plants. In International Conference on Human-Computer Interaction (pp. 497-502). Springer International Publishing.

Boring, R., Ulrich, T., & Lew, R. (2016, July). RevealFlow: A Process Control Visualization Framework. In International Conference on Augmented Cognition (pp. 145-156). Lecture Notes on Artificial Intelligence, 9744, Springer International Publishing.

Boring, R. L., Ulrich, T. A., Joe, J. C., & Lew, R. T. (2015). Guideline for Operational Nuclear Usability and Knowledge Elicitations (GONUKE). Procedia Manufacturing, 3, 1327-1334.

Boring, R., Ulrich, T., Lew, R., Kovesdi, C., Rice, B., Poresky, C., Spielman, Z., & Savchenko, K. (2017). Analog, Digital, or Enhanced Human-System Interfaces? Results of an Operator-in-the-Loop Study of Main Control Room Modernization for a Nuclear Power Plant, INL/EXT-17-43188. Idaho Falls: Idaho National Laboratory.

Braseth, A. O. (2014). Information-rich design for large-screen displays. Nuclear Engineering International, 59(715), 22-24.

Brown, T. (2009). Change by design: How design thinking transforms organizations and inspires innovation. Harper Collins.

Chappell, D (September, 2016). Introducing Windows Presentation Foundation. Microsoft Developer Net-work Technical Article.

Electric Power Research Institute. (2004). Full Plant I&C Modernization in 30 Days or Less, A Feasibility Study, EPRI TR-1009611.

Federal Aviation Administration (2009) Advanced Avionics Handbook, FAA-H-8083-6.

Furet, J. (1985, Autumn). New Concepts in Control-Room Design. IAEA Bulletin.

Hollifield, B., Oliver, D., Habibi, E. (2008). The High Performance HMI Handbook. Plant Automation Services.

Hugo, J. V., & Gertman, D. I. (2016). A Method to Select Human-System Interfaces for Nuclear Power Plants. Nuclear Engineering and Technology, 48, 87-97.

IEEE-1786. (2011). IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities, IEEE-1786.

International Atomic Energy Agency (1999). Modern Instrumentation and Control for Nuclear Power Plants. Vienna: VIC Library Cataloguing in Publication Data.

Joe, J. C., Boring, R. L., & Persensky, J. J. (2012). Commercial Utility Perspectives on Nuclear Power Plant Control Room Modernization. Proc. of ANS NPIC & HMIT, 2039-2046.

Jokstad, H., & Boring, R. (2015). Bridging the Gap: Adapting Advanced Display Technologies for Use in Hybrid Control Rooms. Proc. of ANS NPIC & HMIT, 535-544.

Strobhar, D. A. (2013). Human Factors in Process Plant Operation. Momentum Press, New York City.

Lew, R., Lau, N., Boring, R. L., & Anderson, J. (2016, July). The Role of HCI in Cross-Sector Research on Grand Challenges. In International Conference on HCI in Business, Government and Organizations (pp. 519-530). Springer International Publishing.

Lew, R., Ulrich, T. A., & Boring, R. L. (2017, July). Nuclear reactor crew evaluation of a computerized operator support system HMI for chemical and volume control system. In International Conference on Augmented Cognition (pp. 501-513). Springer, Cham.

Lew, R., Ulrich, T., Boring, R., Thomas, K. (2014). A Functional Prototype for a Computerized Operator Support System. Proceedings of the International Symposium on Resilient Control Systems.

O'Hara, J., Brown, W., Lewis, P., & Persensky, J. (2002). Human-system interface design review guidelines (NUREG-0700, Rev 2). Washington, DC: US Nuclear Regulatory Commission, 12.

Saltz, I. (2011). Typography Essentials: 100 Design Principles for Working with Type (Design Essentials). Rockport Publishers.

Siemens Energy and Automation, Inc. (2007). PLC Or DCS? Seven Questions to Help You Select the Best Solution.

Snow, M. P., French, G. A., Hitzeman, T. A. (2003). Primary Flight Displays in the T-38C: When do differences among displays become inconsistencies? Defense Technical Information Center, Accession Number: ADA430679.

Thomas, L. C., & Wickens, C. D. (2001, October). Visual displays and cognitive tunneling: Frames of reference effects on spatial judgments and change detection. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 45, No. 4, pp. 336-340). Sage CA: Los Angeles, CA: SAGE Publications.

Tufte, E. (1983). The Visual Display of Quantitative Information. Quoted in "ET Work on Sparklines". Retrieved from http://www.edwardtufte.com/bboard/q-and-a-fetch-msg?msg_id=000AI

Ulrich, T. A., Boring, R. L., & Lew, R. (2015). Control Board Digital Interface Input Devices—Touchscreen, Trackpad, or Mouse? Resilience Week Proceedings, 168-173.

Ulrich, T. A., Boring, R. L., Werner, S., & Lew, R. (2017, July). A comparison of an attention acknowledgement measure and eye tracking: application of the as low as reasonable assessment (ALARA) discount usability principle for control system studies. In International Conference on Augmented Cognition (pp. 251-260). Springer, Cham.

Ulrich, T.A., Boring, R.L., Lew, R.T., and Thomas, K.D. (2015b). Computerized operator support system—Phase II development. 9th International Topical Meeting on Nuclear Power Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC&HMIT), pp. 2193-2202.

Ulrich, T., Lew, R., Medema, H., Boring, R., & Thomas, K. (2015a). A Computerized Operator Support System Prototype, INL/EXT-15-36788. Idaho Falls: Idaho National Laboratory.

Ulrich, T., Werner, S., Lew, R., & Boring, R. (2016, July). COSSplay: Validating a Computerized Operator Support System Using a Microworld Simulator. In International Conference on Human-Computer Interaction (pp. 161-166). Springer International Publishing.

Vicente, K., Rasmussen, J. (1992). Ecological Interface Design: Theoretical Foundations. IEEE Trans. on Systems, Man and Cybernetics, 22, 589-606.

Vicente, K. (2002). Ecological Interface Design: Progress and Challenges. Human Factors, 44, 62-78.

U.S. Nuclear Regulatory Commission. (2002). Human-System Interface Design Review Guidelines, NUREG-0700, Rev. 2.

Villim, R. B., Park, Y. S., Heifetz, A., Pu, W., Passerini, S., & Grelle, A. (2013, November). Monitoring and Diagnosis of Equipment Faults. Nuclear Engineering International Magazine, 24-27.