INL/EXT-15-36788

A Computerized Operator Support System Prototype

Thomas Ulrich, Roger Lew, Heather Medema, Ronald Boring, and Ken Thomas

September 2015

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

INL/EXT-15-36788

A Computerized Operator Support System Prototype

Thomas Ulrich, Roger Lew, Heather Medema, Ronald Boring, and Ken Thomas

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

Executive Summary

A computerized operator support system (COSS) was developed to realize the benefits of automating operator actions for transients described in a report published by the Idaho National Laboratory in September of 2012, entitled *Design to Achieve Fault Tolerance and Resilience*. The report identified situations in which providing additional automation in lieu of operator actions would be advantageous. It recognized that managing certain plant upsets is sometimes limited by the operator's ability to quickly diagnose the fault and to take the needed actions in the time available. A COSS is a collection of technologies to assist operators in monitoring overall plant performance and making timely, informed decisions on appropriate control actions for the projected plant condition. The COSS does not supplant the role of the operator, but rather provides rapid assessments, computations, and recommendations to reduce workload and augment operator judgment and decision-making during fast-moving, complex events.

This report describes the current COSS development efforts to extend the functionality of the initial COSS prototype and further demonstrate its benefits. The prototype depicts a model COSS system that addresses a sequence of general tasks required to manage any plant upset: detection, validation, diagnosis, recommendation, monitoring, and recovery. The model serves as a framework for assembling a set of technologies that can be interrelated to assist with each of these tasks.

The prototype COSS was developed to demonstrate the concept and provide a test bed for further research. The prototype is based on four underlying elements consisting of a digital alarm system, computer-based procedures, PI&D system representations, and a recommender module for mitigation actions. The original prototype simulated an interface to a sensor validation module and a fault diagnosis module. These two modules will be fully integrated in the next version of the prototype.

A revised version of the prototype is now operational at the Idaho National Laboratory using the U.S. Department of Energy's Light Water Reactor Sustainability (LWRS) Human Systems Simulation Laboratory (HSSL). The HSSL is a full-scope, full-scale glass top simulator capable of simulating existing and future nuclear power plant main control rooms. The COSS is interfaced to the Generic Pressurized Water Reactor (gPWR) simulator with industry-typical control board layouts. The glass top panels display realistic images of the control boards that can be operated by touch gestures. A section of the simulated control board was dedicated to the COSS human-system interface (HSI), which resulted in a seamless integration of the COSS into the normal control room environment.

Two COSS demonstration scenario have been developed for the prototype involving the Chemical & Volume Control System (CVCS) of the Pressurized Water Reactor (PWR) simulator. The two scenarios involve a primary coolant leak outside of containment that would require tripping the reactor if not mitigated in a very short timeframe. The COSS prototype presents a series of operator screens that provide the needed information and soft controls to successfully mitigate the event.

The revised prototype includes overview screens to provide the operator with high level system status and provide context for COSS actions and recommendations. Additionally, the revised prototype communicates directly with the gPWR simulator to support simulated scenarios for future COSS evaluation. Future efforts will continue to develop additional functionality, such as what-if prediction aids, incorporate additional scenarios, and conduct a comprehensive human factors based evaluation to both qualitatively and quantitatively describe the benefits of a COSS on operator performance.

This page intentionally left blank

Table of Contents

LIST OF FIGURES

This page intentionally left blank

ACRONYMS

ABWR	Advanced Boiling Water Reactor
ANL	Argonne National Laboratory
AOP	Abnormal operating procedure
APC	Advanced process control
COPS	Computerized Operating Procedure Systems
COSS	Computerized Operator Support System
CVCS	Chemical & Volume Control System
DASS	Disturbance Analysis and Surveillance System
DCMS	Damage Control Management System
DCS	Distributed Control System
EPRI	Electric Power Research Institute
FAA	Federal Aviation Administration
FC	Flight controller
GPS	Global Positioning System
gPWR	Generic pressurized water reactor
HMI	Human machine interface
HSI	Human-system interface
HRP	Halden Reactor Project
HSSL	Human Systems Simulation Laboratory
I & C	Instrumentation and control
IAEA	International Atomic Energy Agency
IEEE	Institute of Electrical and Electronics Engineers
IFSS	Intelligent Flight Support System
IGCC	Integrated gasification combined cycle
INL	Idaho National Laboratory
INPO	Institute for Nuclear Power Operations
IPMS	Integrated Platform Management System
ISS	International Space Station
JADE	Java Application Development Environment
KDSS	Knowledge-based Decision Support System
LWRS	Light water reactor sustainability
MCDSS	Medical Computerized Decision Support System
MCC	Mission Control Center
MCR	Main control room
MCS	Module control system
MFC	Multi-function console
MPS	Module protection system
NEI	Nuclear Energy Institute
NPM	NuScale Power Module
NPP	Nuclear power plant
OPC	Object linking and embedding for process control
PCS	Plant control system
PI & D	Piping and instrumentation diagram
PID	Proportional integral derivative controller
PLC	Programmable logic controller
PSA	Probabilistic safety analysis
PWR	Pressurized water reactor

RA	Resolution advisories
RTU	Remote terminal unit
SA	Situational awareness
SABARS	Situation Awareness Behavioral Rating Scale
SAGAT	Situation Awareness Global Assessment Technique
SART	Situation Awareness Rating Technique
SME	Subject matter expert
SOER	Significant Operating Experience Report
SOP	Standard operating procedure
SPAM	Situation Present Assessment Method
TA	Traffic advisory
TAWS	Terrain Avoidance and Warning System
TCAS	Traffic Collision Avoidance System
TCP/IP	Transmission control protocol/internet protocol
TLX	Task Load Index
WPF	Windows Presentation Foundation

1. INTRODUCTION

For nuclear power plants, there is a trade-off in control philosophy between automatic system control and operator control, reflecting 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 thresholds for protective actions that will be automatically invoked if the thresholds are exceeded. These automatic actions generally have to be conservative 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 plant processes automatically maintain important plant parameters at the desired operating setpoints by making adjustments to plant components such as valve positions and control rods. These control actions relieve the plant operators from the burden of continuous, tedious manual control of these components.

For less time-critical events more nuanced operator actions are preferred because it is especially important to keeping the plant on-line and producing electricity. These less-time critical situations occur with higher frequency and are less severe than those dealt with by the automatic plant protection systems. In many of these situations human operators may be capable of 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 was published by the INL in September of 2012, entitled *Design to Achieve Fault Tolerance and Resilience*, which described the benefits of automating operator actions for transients. The report identified situations where there are alternate configurations and actions that can mitigate the need for a safety actuation if there is time to do so (Quinn et al., 2012). 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 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 operator control actions can possibly result in the protection thresholds being reached 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. Prolonged inaction to transient events may increase the risk of equipment damage or make it more challenging to arrest the plant excursion and return to within normal operating parameters. Over time, operator performance is expected to increase through better instrumentation and control, training and protocols, increases in system reliability, and better human machine interfaces.

Distributed control systems and with the addition of sophisticated computer algorithms capable of analyzing, diagnosing faults and a database system able to suggest mitigations to complex and fast-moving situations 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 beneficial to currently-operating nuclear plants, as well as new nuclear power plants. 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 take an advisory role in conjunction with a sophisticated plant monitoring and diagnosis system.

2. COMPUTERIZED OPERATOR SUPPORT SYSTEMS

2.1 Introduction

Currently operating nuclear power plants (NPP) can be conceptualized as human machine systems. As such, human operators are essential components to the operation of the plant. A NPP is an engineered system. It contains sub-systems: reactor, main steam supply, turbine, etc. Those sub-systems are comprised of components. The components have inputs and outputs and perform particular functions. For example the reactor contains a reactor pressure vessel. That vessel contains piping for feedwater and piping for steam travelling to the steam generators. Aside from the major components needed to make the system functional NPPs are equipped with instrumentation sensors and controllers. The instrumentation and control along with the human systems interface and operators can be conceptualized as the central nervous system of a plant. A plant might have 10,000 sensors and detectors and 5,000 kilometers of cabling (Hashemian, 2011). The controllers and operators are the brains of the operation taking the sensory information and forming control outputs analogous to motor demands.

Reactors currently operating in the US were designed mostly of fairly simple single variable setpoint controllers. Operators specify a setpoint value at the main control room board. The controller attempts to match the setpoint to an instrument sensor value by outputting an electrical signal based on the error between the setpoint and the sensor value. The electrical signal, for example, could control the position of a valve to maintain a tank at the level defined by the setpoint. In a PWR several controllers operate independently of one another; working diligently to maintain pressurizer level and pressure, steam generator levels, average loop temperature, volume control tank level as well as numerous other variables. NPPs also contain protection systems that trip the plant when critical parameters are reached to maintain the plant within the engineered operation envelope. When the plant is generating power and the grid is stable the control systems require minimal intervention from operators.
Human operators are necessary and intrinsically coupled to the operation of NPP for a variety of reasons. NPPs operate on cyclical refueling cycles where the plants are taken offline for maintenance and refueling. The shutdown and startup processes require operators to monitor plant status while directing field operations and making control manipulations from the MCR. Other maintenance and control operations such as maintaining the correct boron concentration (of a pressurized water reactor (PWR)) over the fuel cycle is mediated entirely by operators. Most importantly, operators are necessary to diagnose and respond to abnormal operating conditions caused by internal equipment failures, human actions, environmental conditions, or grid disturbances. Some of these events may be major and requiring shutting down the plant, but other events may not pose an immediate risk. In these non-catastrophic situations, maintaining power production reduces risk of cascading grid blackouts and economic losses to the plant.

Situational awareness is critical to the safe operation of NPPs. It requires an accurate understanding of the current plant state, operating configuration, the intricacies of the plant process and control systems, the physics of the plant processes (nuclear, thermal, fluid, and electrical), and the current operating margins with respect to safety and regulatory limits. The current US fleet of NPP consists of control technologies reaching obsolesce. Existing NPPs are facing a critical time in which many NPPs have exceeded their original licensing lifespan. The aging fleet of U.S. NPPs is actively modernizing to continue operation under extended plant licenses and remain financially viability within the competitive energy production market. As part of those efforts, NPPs are retrofitting instrumentation and distributed control systems. Over the past 30 years advances have been made in instrumentation, control systems, and human machine interfaces. Old systems are becoming difficult and expensive to maintain. New systems offer increased reliability resulting in fewer service disruptions.

2.1.1 Historical Overview of Industrial Control Systems

The control systems technology originally implemented in LWR reactors were designed and built at the dawn of distributed control systems. In this era, electronic analog control systems had been around for 20+ years with their first applications in oil and gas in the 1950s (McKim, 2011). With their relatively established track record, analog control systems were used for safety critical functions (U.S. Nuclear Regulatory Commission, 2013). Analog controllers contained hardwired circuits that made changing control logic difficult. The components in analog controllers are also prone to drift over time changing how the controller is tuned (McKim, 2011). Programmable logic controllers (PLCs) are controllers that use microprocessors and code to implement control logic remedying the limitations of analog controls. PLCs were first developed in the early 1960s, and began to proliferate in the 1970s as microcomputers became much cheaper (Segovia, 2013). Early PLCs connected to instruments and devices using dedicated wires running serial TTY communication protocol. Like their analog predecessors dedicated cable runs needed to be made between the sensors and controller and the controller and field devices. Dedicated connections limited flexibility and required more space for wires. When PLCs were first introduced they were viewed as unreliable and there was difficulty in convincing people that something the size of a shoebox could replace a row of cabinets filled with mechanical relays (Segovia, 2013).

PLCs naturally led to the emergence of distributed control systems (DCS) in the 1980s. DCS is an architectural framework for deploying instrumentation and control. Instead of dedicated wire runs the equipment is networked to reduce wiring complexity. Typically two segmented networks exist. One contains the field instrumentation, devices, and controllers communicate digitally and in real-time over a communication network. This network is often referred to by the genericized trademark Fieldbus. In the 1990s there were several competing implementations for Fieldbus networks. Several dozen vendors still exist but adhere to eight types specified in IEC 61158. In a second transmission control protocol/internet protocol (TCP/IP) network the PLCs are networked together with supervisory control, process control, and human machine interface equipment (Segovia, 2013).

Second generation DCS began moving toward Microsoft Windows based platforms in the 1990s (McKim, 2011). DCS became more sophisticated by automating more control of the process. By analogy a setpoint PLC is like a manual home thermostat. A second generation DCS is like a programmable thermostat. With a manual thermostat a user must remember to setback the temperature when they leave the house or go to sleep to save energy. The programmable thermostat automates such functionality according to a programmed schedule. Digital control systems in LWRs were reserved for non-safety critical auxiliary systems and plant process monitoring even into the 1990s (Segovia, 2013; U.S. Nuclear Regulatory Commission, 2013) but are now making there into the market.

The latest generation DCS are distinguished by containing advanced process control (APC; McKim, 2011). APC refers to control technologies beyond automation with PID controllers, and programmed control logic. APC includes concepts like automated controller tuning, neural nets, multivariable control, and model predictive control (McKim, 2011; Hebert, 2012). Returning to our thermostat analogy, a third generation DCS would be a thermostat like the Nest. The Nest thermostat learns the patterns and preferences of its occupants and set the temperature accordingly. In process control APC techniques are generally much more challenging to implement; experts suggest APC may not be worth the effort for every application. However, when properly implemented and maintained, APC can offer performance beyond human abilities (Hebert, 2012).

It is only within the last decade that US NPPs have begun adopting second generation DCS. Equivalent systems have seen use in oil and gas for 2+ decades. As a concrete example Schneider Electric (formally Invensys) has a Tricon Turbine Control System. Modern DCS are specially configured to support the Standard Operating Procedures (SOP) of the plants by automating some of the processes that would

previously be controlled entirely by the operator (Hitzel & Block, 2003). . Turbine rotors are light weight to optimize their efficiency and the casing is relatively heavy. When starting the turbine the rotor must be warmed slowly to prevent differential expansion between the rotor and casing. With first generation DCS operators needed to manually check rotor temperature and modulate throttle valve steam flow to make sure the rotor did not warm too quickly. The Tricon automates this process by modulating steam flow to follow a programmed rotor warming curve (Invensys, 2011). Currently available DCS offer other tangible benefits over there analog counterparts. Modern DCS are more reliable because they use solid state components, redundant modules, and redundant communication networks. Over the past several decades instrumentation has also become more affordable allowing redundant sensors for critical variables. DCS can use this redundancy to select or aggregate from the multiple sensors. Because they are digital the process variables can be recorded to historian databases and are more easily shared with personnel outside the control room.

The alarm systems and management capabilities of DCS have changed dramatically. Existing NPPs were designed with light board annunciator panels. Each alarm corresponds to a physical tile. Over time operators become adept at assessing the state of the plant by quickly assessing these annunciator panels. However the panels are not without their limitations. The number of alarms that can be represented is constrained by the physical space available and the operator's processing capabilities. HMIs are generally designed to represent the processes that are being controlled. The alarms can be embedded in the display such that the graphically depiction of the alarm maps to critical instrument as well as the value of that instrument. Many faults will trigger a cascade of alarms making it difficult for operator's to diagnose the root cause of the alarm. DCS HMIs can identify and report the first out reducing potential confusion.

2.1.2 Modernization

The history of control systems reveals a pattern of increased automation of plant processes. In the context of nuclear modernization there are a variety of reasons to think it is unlikely that existing plants will ever become fully automated or even fully digital. Plants systems are being upgraded in piecemeal fashion. Plants operate for 18-24 months before being shut down for short periods to conduct refueling, maintenance and upgrades. Upgrading all the control systems and main control room in that time frame is not feasible. Employing digital instrumentation and control (I & C) presents some unique challenges. Greater interaction among subsystems can increase the likelihood of common cause failure; digital systems also present more of a cyber-security risk (IAEA, 2011). Most importantly, NPPs are operated under a highly regulated safety culture. This culture has produced an impressive track-record of safety for US nuclear power. However, the high consequences associated with possible mishap increase the risk from experimenting with state-of-the-art control technologies. Small scale industrial processes can be designed and engineered from conception to take advantage of APC and may have much lower risk of catastrophe. In such settings, even small gains in efficiency can lead to tremendous savings.

Ironically, more advanced instrumentation and control systems often result in more process variables for operators to monitor to maintain situational awareness. The old paradigm of dedicating physical space in the control room for each indicator quickly exceeds the limits of human information processing. This is a daunting task for even the most experienced operators and could become a significant concern in the future as a wave of new operators replace the aging nuclear workforce. The solution is to equip control rooms with modern human machine interfaces (HMIs) that can present information to operators in a tailored and organized fashion.

The push towards modernization of the MCR provides a unique opportunity to explore and implement new HMI technologies to take advantage of advances of instrumentation and control. As control systems are updated, more information will be available to operators. Providing more information does not necessarily improve operator performance and can even result in performance decrements if implemented

poorly. Of primary importance is that the HMIs take into consideration the overall human machine system. Incorporation of digital control systems may alleviate operators from some of the more tedious and tasks, but the coordination between plant subsystems is codified by paper procedures and implemented by operators.

2.1.3 Need for an Operator Support System

Thus far we have discussed advances in digital control systems as well as the basic structure and operation of control systems in nuclear power. HMIs are self-described as the interface between the human and the machine. It allows operators to monitor what the DCS is doing and interact with the process that is being controlled. HMIs that can effectively present information will aid operators in assessing the current plant status, safety margins, and deviations from expected operations. Several avenues of improvement exist for HMIs. Technology can also recommend actions to mitigate undesirable plant events and trends and return the plant to a safe operating condition with the least amount of upset possible. Lastly, preventing operator errors by tracking the operator actions within the context of the plant conditions to verify her actions as appropriate or prompt the operator if she fails to notice the need for an action.

We define a operator support system (COSS) as an enhanced DCSHMI with 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 have the following features:

- Monitoring plant states to detect off-normal conditions
- Diagnosis of plant faults
- Prediction of future plant states
- Recommendation of mitigation alternatives based on embedded expert knowledge
- Decision support in selecting appropriate mitigation actions
- Computer-based procedures with soft controls

Another common term for this collection of technologies is “operator advisory system.” For the purpose of this research project, operator advisory system is generally synonymous with the concept of COSS. A number of other similar terms are sometimes used to convey the same concept, such as an operator assistant or operator support system. Other more specific concepts like “recommender systems” or “advanced alarm systems” are well established in industry and research but represent only a sub portion of the multifaceted functionality encompassed by the COSS concept.

However, as a class of related technologies, an important distinction to be noted is that they assist 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.

As the control room becomes more advanced through the modernization process, the COSS will eventually become engulfed by the control system itself so that in a sense it exists throughout the entirety of the MCR. Conceptually, it will still be a separate entity because its functionality and role are beyond what is traditionally considered the control portion of the system. This futuristic seamlessly integrated COSS will likely not come to fruition for many years, especially since utilities have expressed their intent for following small increment upgrades as their modernization approach over a more expensive full MCR change out with a full digital MCR featuring some of functionality embodies by the COSS. As a starting point during this initial research and development period, the COSS will remain as a separate system that

communicates with the existing MCR to support the operator while handling plant upsets. Furthermore, the regulatory environment will need to shift away from its current position, which prohibits operators from controlling the plant via computer-based procedures with soft controls. As such, the COSS must be positioned within a specific location on the control boards, as opposed to being distributed throughout the entire MCR. Simply addressing the issue of where to position the COSS for its application with the Chemical and Volume Control System is but one of many human factors design considerations that must be addressed in order to create an effective operator support system. A discussion and strategy for addressing the human factors issues associated with designing a COSS will follow, but first it is important to examine some analogous decision support systems designed for other domains.

2.1.4 Feasibility and Current Trends

Our previous efforts have focused on exploring how the COSS envisioned in this document could support operators by demonstrating how the HMI would integrate into the control room and operation of the plant. At this stage attention is focused to addressing the feasibility of whether such technology could be developed and the logistics involved with such an effort.

The previous sections have outlined how COSS would be beneficial to existing plants seeking modernization. In addition to existing Generation II plants, it is clear that late Generation II and early Generation III/+ despite incorporating fully digital control systems are operated in a fundamentally similar to Generation II reactors. Operators will use procedures to coordinate activities between operators and subsystems. This legacy is deeply rooted nuclear power operations. Late fully digital Generation II and early Generation III control rooms of plants that came online in the late 1990s and early 2000s, such as the Kashiwazaki-Kariwa-6 and -7 Advanced Boiling Water Reactors (ABWR), are a hybrid of mechanical indicators and controls and digital HMIs (IAEA, n.d.). Hashemian (2011) cites software as being one of the key limitations to adoption. In control systems without digital HSIs the failure modes are known and easier to design for. With software the number of errors and possible operating characteristics are more difficult to account for in the design and implementation process. Software also makes integrated control systems more prone to common cause failures. Lastly, software presents new cyber-security vulnerabilities. So despite control systems being entirely digital, control rooms from that era remained hybridized to limit risks associated with software.

Despite these limitations the industry as a whole is starting to embrace digital I & C. Defense-in-depth strategies can alleviate many of the concerns and the additional benefits in reliability, configurability, and maintainability Hashemian (2011). Generation III plants like Westinghouse Advanced Passive Reactor (AP1000) have already incorporated an Advanced Control Room comprised of large digital displays and sitting operator workstations (Chapter 18 of DCD). The primary and secondary control systems are independent but are functionally integrated to enhance response to plant transients and to automate some of the coordinating functionality typically performed by operators. For example, the reactor power control can respond to the following load change transients:

- step load change of plus or minus 10 percent
- ramp load increases or decreases up to 5 percent per minute
- daily load following profiles from 50% to 100% with 2 hour transition durations
- grid frequency response (Chapter 7 of DCD).

AP1000 operators are also trained to operate the plant under manual control. Staffing requirements for US plants are subject to NRC 10 CFR Part 5 and operations would be procedure-based and resemble how operations are conducted in current plants during abnormal operations. Current trends suggest that modern DCS systems are beginning to integrate many of the essential features of COSS, and suggest a

future for the enhancements described in this paper. Namely, statistical sensor validation, fault detection and diagnosis, and mitigation recommendations based on expert knowledge.

The economics of implementing COSS are easy to justify. As we will later describe the COSS would need to encapsulate an expert knowledge database containing appropriate actions for every possible fault in the plant. Compiling, validating, and maintaining such a database would likely increase the cost over a traditional DCS by several fold. Downtime costs for existing nuclear reactors costs in the region of $500,000 to $1,000,000 per day (McKim, 2011). Over the operating life of a plant the potential for avoiding downtime justifies the cost of implementation even when considering the "one off" nature of Generation II plants. Generation III plants have a commitment to standardization and are being designed for a 60+ year operating lives that would make the economics of COSS even easier to justify (Goldberg & Rosner, 2011).

For Generation IV reactors may be more likely to employ control systems that fully automate standard operating procedures to coordinate processes across plant systems. For example when. There are many reasons for making such a conjecture. One is simplicity. The procedures that are followed are an abstraction of control flow diagrams intended to keep the plant within a quantified operational envelope. They were developed because digital control systems were not available to perform the control logic. Non-nuclear power process control has embraced fully automated DCS and seen tangible benefits in system reliability, quality control, and operational costs. Secondly, removing the operator as the coordinating actor between subsystems will benefit probability risk analysis. Lastly, labor savings will lower operating costs and improve profitability. This would be especially true with small modular reactor designs. If each small reactor reactors three operators the profitability is dramatically decreased compared to if each requires < 1 operator. Nuscale's plant design overview (2014) submitted to the NRC expresses their intent to have each operator "monitor and control multiple units." In preparation for such possibilities the Nuclear Energy Institute (2011) has prepared a position paper for the NRC titled "Control Room Staffing for Small Reactors." The paper stipulates that because currently designed SMRs rely on passive safety systems and human factors engineering is being used to reduce operator workload, "task analyses of operator workload for SMRs may indicate an appropriate control room staffing complement different from that of the current LWRs and existing regulations." Nuscale's control system architecture does not follow the tradition of segregating primary and secondary controls. It organizes plant control and safety into four systems: module control system (MCS), plant control system (PCS), module protection system (MPS), and plant protection system. The MCS and PCS would work in conjunction to control and monitor plant wide nonsafety systems. Nuscale conceptualizes each small modular reactor, turbine/generator, and associated systems as a Nuscale Power Module (NPM). In the control room the interface is describe (in verbatim) as supporting the following task based operational activities:

- initiate NPM startup
- initiate NPM shutdown
- set or correct set points that control the NPM or plant functions
- take corrective actions if any NPM or plant system does not operate as intended
- provide permission for the control systems to continue on past predefined hold points in major operations using automated control system functions.

We previously made an analogy between DCS technologies and household thermostats. Now suppose another analogy with DCS technologies as automobiles. A first generation DCS is akin to cruise control that simply holds the throttle at a set position. A second generation DCS is akin to cruise control that uses the vehicles speedometer in a feedback loop. A third generation DCS would be adaptive cruise control that is able to detect distance to other vehicles and act accordingly. Generation IV reactor control systems

may be akin to semi-autonomous vehicles driving with human supervisors and intervention when necessary.

Much like autonomous vehicles the role of human operators in nuclear power and other critical infrastructure is a matter of both technological capability and philosophy. The point here is partially to open dialogue, but more importantly to point out the potential role of COSS over the remaining life of Generation II and future lives of Generation III/+ reactors.

2.2 Relevant COSS Examples

The previous section discussed distributed control systems and discussed how COSS fits into the lineage of digital instrumentation and control from a bottom-up perspective. Here we discuss COSS development from a theoretical top-down perspective by examining case studies and identifying the essential concepts that support operators. Various COSS technologies have been underway since at least the 1980s in a number of safety-critical applications and has gained widespread acceptance in certain fields, particularly aviation. The following are some notable examples of the use of this technology from a diverse set of air transportation, marine transportation, robotics, medicine, and spaceflight exploration, and process control domain applications.

2.2.1 Traffic Collision Avoidance System (TCAS)

As an example from the aviation industry, the use of Traffic Collision Avoidance Systems (TCAS) is now mandated for U.S. passenger-carrying aircraft (30 seats or greater) (U.S.DOT, 2011). The first version of this (TCAS I) provided the pilot with only traffic advisories (TAs), meaning information on the altitudes and flight paths of other aircraft in the immediate vicinity. The current version (TCAS II) provides both traffic advisories and resolution advisories (RAs). An RA is a recommendation on control actions to change course and thereby avoid the pending collision. For example, a RA might be to climb at a certain rate (feet/minute). When both aircraft involved in a potential collision are equipped with TCAS II, the two TCAS units communicate with each other and coordinate their RAs such that complementary RAs are selected. In other words, the units ensure that a secondary collision path is not created.

TCAS has the form of a COSS in that it:

- Receives data from the operating environment
- Estimates time to reach critical thresholds
- Monitors for potential safety issues
- Provides routine updates on safety status
- Detects and diagnoses a critical safety issue
- Provides recommendations to the operator (pilot) to avert the situation
- Monitors for successful resolution.

TCAS has undergone extensive evaluation studies to fine tune the collision avoidance algorithms to reduce nuisance alerts. It was recognized that a high rate of unnecessary alarms would undermine the credibility of the system with the flight crews. Over time, the technology has improved to where most countries have now mandated the use of TCAS for their national airlines.

Also of interest has been the way manufacturers of avionics have integrated the TCAS into the digital instrumentation that is typical on newer aircraft with “glass cockpits.” Rather than just rely on text-based messages, the recommended control actions are superimposed on key flight instruments (such as the

attitude indicator and the vertical speed indicator) using a color scheme to assist the pilot's immediate comprehension of what evasive maneuvers are needed. Again, these are recommendations for which the pilot can opt not to take, but the proven reliability of the technology along with the sophisticated presentation of the recommendations have driven a widespread acceptance of the use of TCAS among pilots and aviation regulatory authorities. This stands out as a real success story of an operator advisory system being a proven complement to a human operator.

2.2.2 Terrain Avoidance and Warning System (TAWS)

A similar example from aviation is a Terrain Avoidance and Warning System (TAWS) that alerts a pilot to what the Federal Aviation Administration (FAA) terms "controlled flight into terrain" (U.S. Department of Transportation, 2009). This is when an airplane that is completely airworthy is unintentionally flown into terrain due to lack of awareness by the flight crew. Sometimes these situations are due to adverse weather or darkness, and other times they are due to the pilot becoming distracted.

TAWS typically use a moving map that is displayed on a dedicated instrument or superimposed on general-purpose flight panel displays which depict other information, such as flight path, landmarks, weather, other nearby aircraft (from TCAS), etc. They typically use GPS inputs to know the position of the aircraft and altimeter inputs to know the altitude of the aircraft. They have on-board detailed terrain databases that can be correlated to the position and altitude of the aircraft. The terrain databases are maintained up to date, so that in addition to the natural topography, they contain the latest information on man-made features such as radio antennae and tall structures.

These systems use color to indicate the proximity to terrain features and use text and aural alerts to warn the pilots. A typical sensitivity setting for terrain below the aircraft would be to color the terrain on the map yellow if it is within 1000 feet of the aircraft and red if it is within 500 feet. Using a "look ahead" feature to avoid level flight into rising terrain, the TAWS would calculate the time to impact based on location and ground speed, typically issuing an aural alert one minute before impact.

The system passively monitors the flight path and "pushes" alerts to the pilot when needed rather than requiring the pilot to make any request of the system. In other words, it does not create any distraction in the cockpit other than when urgent action is needed. Some of the situations for which the TAWS provide alerts are:

- Excessive rate of descent
- Excessive closure rate to terrain
- Altitude loss after takeoff
- Negative climb rate
- Flight into terrain when not in landing configuration
- Excessive downward deviation from glide slope
- Premature descent
- Terrain along future portions of the intended flight route.

These systems have the features of a COSS in the sense they:

- Passively gather flight information (e.g., position, altitude, flight path)
- Process this information using models of terrain, glide slopes, etc.
- Provide routine status to the pilot through the flight displays
- Provide text-based and aural alerts (e.g., "Caution, Terrain!")

- Provide aural recommended actions (e.g., “Pull Up!”)

The use of TAWS has greatly improved flight safety across the aviation spectrum, from high performance commercial and military aircraft down to small general aviation aircraft. It is required by the FAA on most passenger-carrying aircraft.

As in the case of the TCAS, TAWS serves as an excellent example of where an operator advisory system, in this case for pilots, greatly enhances situational awareness and provides reliable recommendations during time-critical safety situations.

2.2.3 NASA Mission Control Intelligent Flight Support System

The NASA Mission Control Center (MCC) at the Johnson Space Center serves as the primary means to control manned spaceflight missions and must contend with large volumes of data in order to support the international space station missions. For example, the telemetry control systems generate gigabytes worth of data in a single day, all of which must be rapidly processed to identify the state of the spacecraft and make timely informed decisions (Tavana, 2004). The need for discerning patterns from these large data sets was evidenced during the 1986 launch of the Space Shuttle Challenger. Post-accident investigation established that the data was sufficient to identify the danger of the O-ring failure that led to the Challenger explosion, however the form it was represented failed to yield support when engineers presented their case to delay the launch. This example stresses the importance of displaying data in a clear and understandable manner.

The Intelligent Flight Support System (IFSS) was designed to graphically representing large amounts of data in a visually intuitive manner to support flight controller (FC) situation awareness. Specifically, the IFSS was intended to support Space Shuttle docking with the International Space Station (ISS) since this particular task is quite challenging due to its 3-dimensional spatial problem solving demands and the challenging task of docking two multibillion-dollar assets orbiting the earth at approximately five miles per second. The IFSS contains the following feature set:

- What-if analysis
- Goal-seeking
- Data visualization
- Expert system

The what-if analysis feature allows the FC to adjust a parameter or set of parameters and then demonstrate the impact these changes have on the overall system state. IFSS specially uses those adjusted parameters to predict the parameters for the graphical models of the international space station and the space shuttle depicted to the FC. The goal-seeking feature compliments the what-if analysis feature by providing the FC with the ability to select a desired parameter value and then display the model and associated values required to achieve that desired parameter. Graphing provides the FC with visual representations of large data sets and allows for historic trends to be revealed. Lastly, the expert system serves as a method to incorporate knowledge-based rules concerning the ISS and Space Shuttle so that the IFSS can provide advice to the FC.

2.2.4 Shipboard Damage Control System

Modern day maritime vessels use an Integrated Platform Management System (IPMS), which consists of a collection of Multi-Function Consoles (MFC) and Remote Terminal Units (RTU), to monitor and control the ships primary systems including propulsion, mechanical, electrical, auxiliary, and damage

control (Calabrese et al., 2012). Each system contains various levels of automation which reduce personnel requirements and improve overall ship efficiency. Though the damage control system incorporates automation, due to its safety implications a damage control officer, also termed operator, remains as the final decision maker during critical safety events, e.g. a fire spreading through the ventilation system. The complexity and unforeseeable nature critical safety events necessitate relying on a human problem solving abilities to ensure a safe event resolution. The Damage Control Management System (DCMS) features a knowledge-based decision support system (KDSS) that aids the operator these critical safety events by diagnosing ship status and providing appropriate procedures to handle the situation. The DCMS consists of four modules that provide the following functionality:

- Automatically acquires ship safety data from IPMS
- Filters and aggregates the data to display to the damage control operator
- Displays alarms and associated controls
- Presents suitable procedures

While monitoring the ship, the DCMS supports the operators' situation awareness by aiding them in the decision process. A typical decision making process follows the information and action flow diagram below (see Figure 1). This flow diagram is specific to the DCMS as it is used on a ship; however the general flow, i.e. the flow of information and decision making process preceding actions, can be universally applied to any complex system with an operator support system.

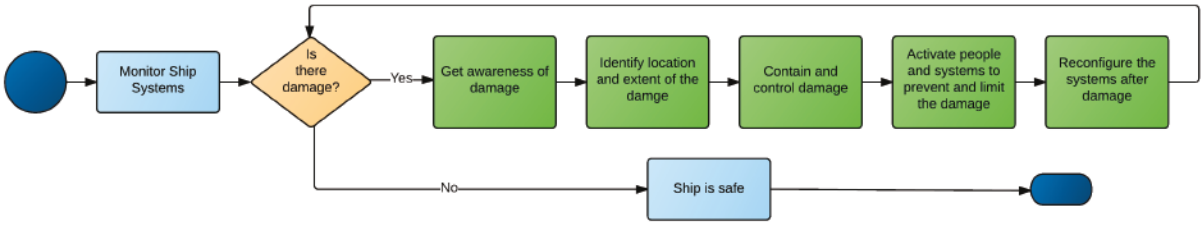

Figure 1. Decision and action flow of damage control operator (Calabrese et al., 2012)

2.2.5 Autonomous Robotic Agents and Operator Systems

The field of robotics has explored various decision support systems within the context of controlling autonomous robotic agents. The increasing use of autonomous robotic technology consisting of numerous autonomous agents performing their duties while under the supervision of a human decision maker. The resulting system is highly complex due to the plethora of information that must be effectively communicated between the robotic agents and each other as well as to the human operator. Autonomous robotic technology research carried out by Bruemmer et al. (2005) examined the fundamental challenges of sharing control and promoting collaborative understandings between humans and robots. Assessment of human workload, human error, and overall performance gathered data to provide objective means to contrast the different modes of robot autonomy and evaluate the usability of the system.

A series of experiments examined how human operators collaborated with a mixed-initiative robot control system in order to carry out a number of indoor search and exploration tasks. The research team sought to explore a collaborative setting affording opportunity for "the human and robot to predict behavior and communicate intent" with robots regarded as both peers and trusted team members. The robot interacted with the human partner at two levels of autonomy. In the safe mode, the robot movement occurred as a result of manual control but performed with a level of initiative that prevented the human operator from obstacle collision. In the shared mode, the robot was capable of relieving the human operator of direct control tasks and after processing site information, employed reactive navigation to secure a path. This

mode provided the opportunity for dynamic allocation of the roles and responsibilities with the robot both offering information and responding to the operator intervention with scripted responses, visual indications and force feedback through a joystick. One experiment carried out a performance comparison – examining the differences in performance between a scenario in which a robot takes the initiative to provide support to a human driving versus the performance achieved in a scenario with the human supporting an autonomous robot driving. Findings indicated the robot achieved greater rates of performance when driving the vehicle. A second experiment focused on the introduction of a virtual 3D map representation. While video is typically used to provide situation awareness, this leads to instances to high operator workload along with decreased communication and visibility. Unlike the video, the 3D map provided support for the collaboration efforts with reductions in both operator workload and navigational error. Findings from the third experiment elaborated on those from experiment one, indicating that collaborative control could both increase performance and reduce the likelihood of error. This occurred despite an increase in the complexity of the environment and distribution of workload to multiple operators.

The research suggested a new alternative to collaborative control and representation between humans and robots for a wide range of tasks and applications. As the findings suggest, this representation has the potential to address many issues including:

- Decreased human navigational error
- Decreased human workload
- Increase in operator's "feeling of control"
- Increase in overall performance

2.2.6 Early German Nuclear Plant COSS

An advanced concept for a COSS was proposed for certain German nuclear plants in the mid-1980s as described in a paper by W. E. Büttner titled "Advanced Computerized Operator Support Systems in the FRG (1985)." The motivation for the system was to address the burden on operators in dealing with the thousands of control modules and indications in the overall design on a nuclear plant, and to assist them in both normal operations and accident conditions. The tasks of the system are described as:

- Log and record disturbances and accidents
- Reduce the information load and present only essential alarms and messages
- Improve signal supervision and verification
- Enable a fast survey of the plant status (especially in case of accidents) and of the character and location of a disturbance
- Carry out automatic diagnosis of disturbances
- Compute process parameters that cannot be measured directly
- Support operators as they follow procedures in the operating model

This is an ambitiousset of objectives considering the state of computer technology at the time. In fact, it parallels many of the objectives of this project and modern DCS are capable of many of these features. It was recognized that a test phase was needed in order to prove that both the new and existing control room technology would work well together, and that these tests must be run on a plant simulator with actual operators participating. Information was not available on the results of these tests or any subsequent implementation in the German nuclear power plants.

2.2.7 Halden Reactor Project's Operator Assistant

A conceptual framework for an Operator Assistant support tool was described in a white paper by the OECD Halden Reactor Project (HRP) in 2012, which was based on experience from the development of various operator support systems using on-line simulation models (Berg, 2012). It addressed the benefits of using on-line simulation and advanced visualization techniques for assessment of historical data and predictive analysis. The scope of the concept was the full range of operations—normal, disturbance, and accident—as described below.

- For normal operations, provide assistance to the operators when drift in plant parameters occur and give operators early warning before operational limits are challenged. This employs various technologies in surveillance, signal validation, condition monitoring and fault detection.
- For disturbances, assist the operators in bringing the plant back to a safe state. This involves the use of technologies for computerized procedures, alarm processing, and diagnosis of abnormal situations.
- For accidents, provide prognoses and provide support for alternative actions. This involves the use of critical function monitoring and a HRP-developed computerized accident management support system.

A number of underlying methods and techniques have been applied and combined in various ways to provide these capabilities, such as:

- Data processing and signal pre-processing/conditioning
- Empirical methods for signal validation and diagnosis
- Logic processing for alarm handling and fault diagnosis
- First-principle process simulation of reactor core behavior and turbine cycle monitoring
- Accident simulations
- Risk monitoring based on probabilistic safety analysis (PSA)
- Innovative human system interfaces (HSIs) for visualizing complex systems behavior including 3D, virtual reality and augmented reality.

This work by HRP represents an important step in the development of COSS technology for advanced control rooms for nuclear power plants and builds on a number of important technology products and prototypes that have been proven through individual research projects and trial implementations.

2.2.8 Eascon Operator Advisory System

An operator advisory system has been implemented at an Integrated Gasification Combined Cycle (IGCC) power plant in Sicily, operated by Isab Energy Company on behalf of ERG Power & Gas (Eascon, 2013). This is a complex made up of 20 power units. Eascon has installed the system in a number of other process and power plant implementations in several other countries.

The system acquires and integrates information from field instruments, recognizes the current plant conditions, and then gives the operators the appropriate recommendations in order to handle any possible scenarios in the most safe and efficient way. The system provides assistance to operators for:

- Start-up, Shut-down and Emergency Operation
- Abnormal Situation Management
- Normal Operation
- Operator Training with off-line Operator Advisory System

- Generation of Standard Operating Procedures

Benefits have been demonstrated in the following areas:

- Improvement of operator skills through continuous training both in on-line and off-line mode
- Sharing of technical and operating know-how between expert and young operators
- Standardization of the operators plant conduction behavior
- Standard Operating Procedures updating

It is important to note that this COSS technology has been implemented in a number of process and power plants in various countries and found to be cost-effective in assisting plant operators with both normal and off-normal operations. It is significant that these types of operations, that are typically cost-driven, have invested in COSS technology as a means of improving the success of day-to-day operations and minimizing the probability and consequences of plant operational disturbances.

2.3 Operator Performance Driven COSS Exigency

The success of the commercial nuclear industry is founded on the principle of pursuing continuous improvement. This is particularly true in the concept of operational focus. Yet technology for control room operators is essentially unchanged over the history of the commercial nuclear industry, mainly because the technology in the control room is essentially unchanged in terms of its capabilities, with a few specific exceptions such as what was implemented in response to the Three Mile Island accident (e.g., a safety parameter display system).

Existing MCRs require the operators to filter and integrate the multitude of information flooding into the MCR. Fortunately, a perfect understanding of changing plant conditions is not necessary to manage plant upsets due to the use of symptom-based abnormal operating procedures. Rather, operators are required to match a subset of indications and alarms to procedure entry conditions, and then allow the procedures to guide the crew to the correct event diagnosis and required control actions. However, operators still have to ensure they are in the correct and appropriate procedures for the current plant conditions, and this requires maintaining situational awareness.

Human error continues to be a significant source of consternation due to the complexity of the operators' task. In 2010, the Institute for Nuclear Power Operations (INPO) issued *Significant Operating Experience Report (SOER) 10-02 Engaged, Thinking Organization (*INPO, 2010) which described a number of safety lapses that had recently occurred in the industry and highlighted a number of organizational shortcomings associated with these events. Among these were:

- Lack of monitoring and cross-checking of critical indicators
- Operators and shift managers distracted by ongoing control room activities and failing to maintain oversight
- Weaknesses in worker knowledge, and more specifically in understanding the bases of procedures, systems and components, and integrated plant operations
- Low risk awareness, particularly in off-normal plant conditions

The SOER also contained a number of recommendations to improve safety performance at the leader, supervisor, and individual levels. These included re-emphasizing a number of important principles that are foundational to the industry's safety culture including:

- Oversight of plant operations and control room crew performance, particularly control room monitoring of plant parameters
- Managing control room distractions
- Use of significant operating experience
- Use of error reduction tools
- Consideration of most-likely undesired consequences of actions
- Improved worker knowledge

Basically, the SOER recommendations relied on improvements in management systems and human performance. It did not introduce any new concepts but rather reinforced current performance expectations. However, it is reasonable to think that the safety lapses that led to the SOER were not beyond the scope of the current performance expectations, and had these expectations been fully met, many if not all of these situations would likely have been avoided, or at least greatly reduced in significance. The industry has certainly benefitted from the response to SOER 10-2 in reinforcing these expectations, and no doubt additional safety events have been avoided.

However, the ongoing problem is that the industry continues to struggle with the consistent application of these fundamental performance expectations because they rely on human performance, which is always subject to variation. The industry operating record over the recent past indicates that the trend in performance is, at best, flat, and that the means of achieving continuous improvement in plant operations has been elusive.

It is therefore reasonable to consider additional means of achieving the level of operator performance that is desired. There is no question that technology is underutilized for this purpose. In contrast, other industry sectors have amply demonstrated that technology in the form of a COSS, as an operator advisory system, can enhance operator human performance while maintaining the role and responsibility of the licensed operator as the independent and ultimate decision-maker.

The nuclear industry has long understood the potential value of COSS and has pursued various forms of it as far back as the early-1980s. One notable contribution was by the Electric Power Research Institute (EPRI), working with Westinghouse Electric Corporation and other industry partners, in developing a report entitled *Disturbance Analysis and Surveillance System (DASS) Scoping and Feasibility Study*, published in 1982 (EPRI, 1982). The proposed DASS envisioned 14 computerized functions that would assist an operator in managing disturbances that threatened nuclear safety and plant availability. Some of the notable functions were:

- Plant data indicator verification
- Disturbance detection
- Disturbance cause determination
- Disturbance propagation prediction
- Best corrective action determination
- Procedure monitoring

Another important development in COSS was the International Atomic Energy Agency (IAEA) report entitled *Development and Implementation of Computerized Operator Support Systems in Nuclear Installations (*IAEA, 1994*)*. This is a valuable reference document on the concept and practical considerations for a COSS and is just as relevant today as when it was published in 1994. Topics include:

- Concept of COSS for a nuclear installation
- Operational requirements
- Design methodology
- Verification and Validation
- Implementation
- Licensing Considerations

This IAEA report indicates that nuclear industry leaders at the time well-understood the importance and benefits of COSS technology in improving operator performance as a continuation of the application control room human factors engineering to improve operational safety.

However, progress in this direction, at least in the U.S., was apparently overcome by the more prominent focus on improving operator performance through control room protocols and the establishment of defensive barriers to prevent errors from resulting in events. And, in fairness, the state of digital technology was, at the time, marginal for being able to accomplish the objectives of a highly capable COSS.

It is now clear that there is a role for both. The challenge is to see how advanced operator advisory systems could complement the human performance protocols for control room operators. The state of technology today is such that a capable and well-designed COSS is indeed feasible, as already demonstrated in other industry sectors, notably aviation.

This project proposes a general model for a control room COSS that addresses the control room operator performance challenges that have led to undesirable events. Further, a prototype COSS has been developed to enable the study of this technology in order to refine the concept, determine the appropriate system objectives and requirements, resolve all human factors issues with the technology, and ultimately validate the COSS concept for commercial product development leading to use in a nuclear power plant control room.

2.4 Operator Cognitive Process Framework

Lee and Seong (2007) outline a framework for designing a decision support system similar to the framework outlined in the initial prototype development COSS work. This framework decomposes the operator's plant monitoring and control tasks into a series of cognitive activities, which can be supported by a decision support system, such as the COSS prototype (see **Error! Reference source not found.**). The four categories of operator cognitive processes include:

- Monitoring plant status and detecting plant upset events
- Situation Assessment
- Response Planning
- Response implementation

These four cognitive processes are traditionally performed by the operator without the aid of a COSS. Without the COSS, the operator must scan the HMI, consisting of the control boards with largely analog indicators and controls to infer the plant status. The operators rely on detailed mental models of the indicator and control states associated with different plant operating conditions to serve as comparisons for detecting deviations associated with a plant upset. This process requires a significant amount of scanning, integrating, and comparing indicator and control states against the various operators mental model. There are thousands of these indicators and controls along with multiple configurations that

translate to numerous overall plant states. The monitoring and detecting cognitive process poses a significant challenge to operators. Though, the COSS is not conceptualized as the primary HMI to display plant information, the HMI should still incorporate some aspects of the COSS concept, such as aggregating, filtering, and integrating information in to a more easily digestible form so that the operators can easily monitor the plant for disturbances.

Following the detection of a plant upset, the operator then proceeds to assess the situation and determine the root cause of the upset and the affected systems and components. Once an accurate situation assessment is made, the operator formulates an action plan to mitigate and ultimately eliminate the plant disturbance. Finally, the operator must enact the action plan by physically manipulating the system.

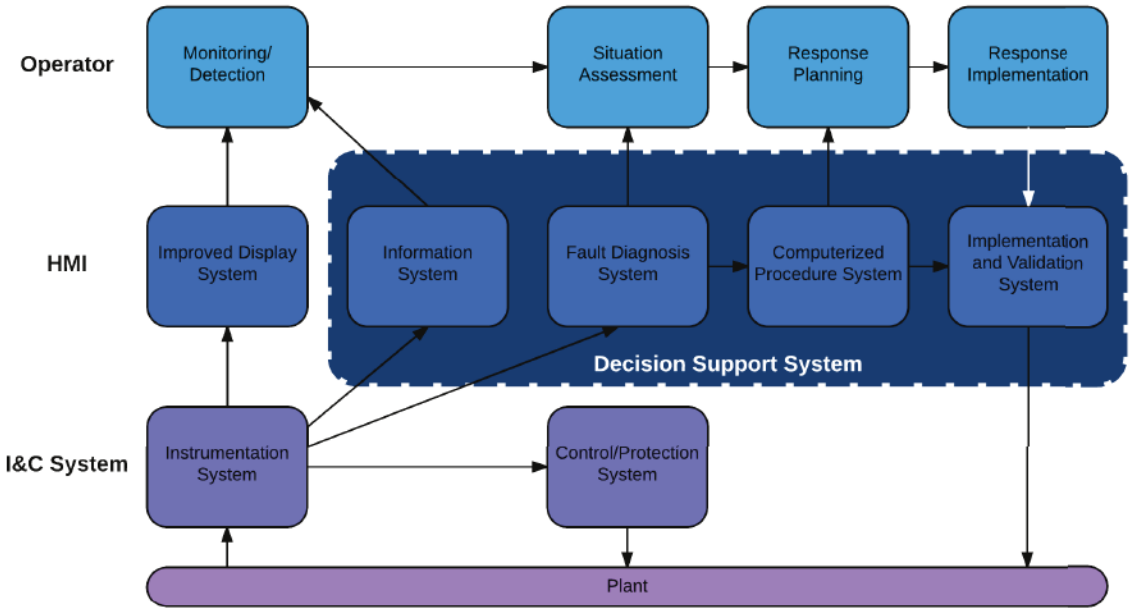

Figure 2. Cognitive Framework depicting the monitoring and controlling operator tasks while interacting MCR

The decision support system described by Lee and Seong directly supports all three of these cognitive elements with a knowledge-based expert system that can actively detect and diagnose faults, provide the operator with appropriate procedures given the fault and the current plant state, and finally aid the operator in enacting the necessary control manipulations along with verifying the success of those manipulations to return the plant to a safe and steady state.

3. CVCS COSS CONCEPTUAL MODEL FOR FAULT MANAGEMENT

3.1 Original Prototype General Concept

This particular concept of a COSS is framed as an "operator advisory system", assisting operators in diagnosing and mitigating certain plant events that, unless addressed in a timely manner, would likely result in a plant transient or reactor trip. This is most often the domain of the plant's Abnormal Operating Procedures (AOPs). These procedures are symptom-based with one or more entry conditions that have to be recognized by the operator. These would include alarm conditions, equipment faults, and plant parameter trends.

There can be time-pressure associated with these plant upsets to recognize the AOP entry conditions, enter the appropriate procedure, and then work through the diagnostic steps until the correct mitigation actions are taken to resolve the situation. In some cases, the underlying fault is not really identified at a component level, but instead the consequences of the fault are managed. For example, there might be a leak on the reactor coolant system that is identified by its symptoms (high containment humidity, high containment sump level, etc.) but the exact location of the leak cannot be determined, other than it is inside containment. However, the AOPs are structured such that the mitigation actions are effective without knowing the exact location of the leak other than determining the general location.

In all of this, the operator is the point of integration of all control room information and has to use what is termed "operator fundamental knowledge" to ensure that indeed the control room is applying the correct procedure for the plant upset. Operators are trained to use a number of human performance enhancement techniques to correctly assess the situation, such as using a questioning attitude and validating all information. In addition, there are a number of other techniques used in the control room at a crew level, such as pre-job briefs, time-outs, repeat-back communications, independent verifications, etc. While all this has proven to be very helpful and necessary, it adds to the mental workload and increases the time delay in responding to the actual plant upset.

The control room crew typically follows a general pattern in reacting to a plant fault as follows [last report].

- Detection – recognizing the symptoms of a plant fault
- Validation – determining that the symptoms are the result of a real plant fault and not a sensor failure
- Diagnosis – determining the specific plant fault
- Mitigation – either correcting or isolating the plant fault such that it is no longer a threat to plant operations or nuclear safety
- Monitoring – monitoring the symptoms of the plant fault to ensure that the mitigation has been successful
- Recovery – restoring the plant to the pre-fault conditions.

Again, the control room procedures, particularly the AOPs, assist the operator with these tasks provided that the correct procedures have been entered. However, the procedures are not specific in certain areas and rely on the operators to perform certain knowledge-based functions, such as estimating the size of a leak based on available plant indication. For example, a leak size can be roughly determined by the percent decrease in a tank level from the known steady-state value.

Operators are exceptionally good at performing these tasks, but the high workload associated with certain plant events creates an environment in which the operator will commit errors that compound the original fault and impact the plant more so than would otherwise have occurred.

3.2 Expanded Prototype Concept Elements

The detection, validation, diagnosis, mitigation, monitoring, and recovery features of the COSS are embodied within four underlying elements consisting of a digital alarm system, computer-based procedures, piping and instrumentation diagram system representation, and a recommender module for mitigation actions. Each of these four underlying elements was selected to fulfill the goal of synthesizing the disparate indication information into a cohesive representation and providing the operator with solutions to any changes in plant conditions. Conceptually, the COSS consists of two primary components. PRODIAG is the system that can detect plant faults and suggest mitigation actions and the Interface is the visual component that displays that displays all the relevant information to support the operator in monitoring and making adjustments to the plant in order to maintain normal operating conditions.

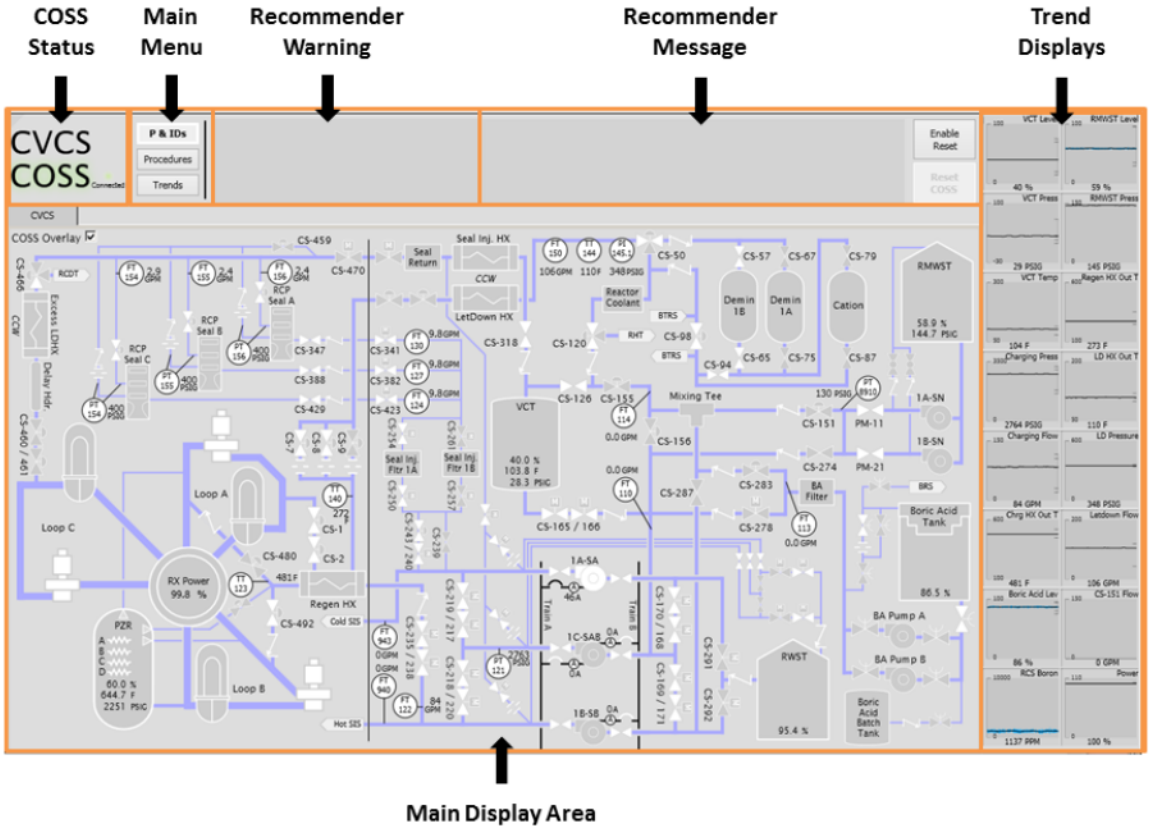

Figure 3. Annotated COSS display featuring areas of concern highlighted on the P&ID, a recommender warning and suggested mitigation action messages

3.2.1 Interface Design

The interface consists of the visual representation of all the information contained within the COSS. The interface was designed around a dullscreen approach in which the majority of screen elements use shades of grey. Fully saturated color is used for highlighting key pieces of information in order to rapidly draw the operator's attention towards information of interest. The interface follows a multi-windowed button

toggled display format, including primary display views for P&IDs, computer-based procedures, and enlarged trend displays. Dedicated areas along the top and right edges of the interface are reserved for displaying warnings, recommendations, and trend annunciator alarms. The specific display elements are discussed in the subsequent sections.

3.2.2 Digital Alarm System

The digital alarm system element of the COSS consists of a warning system and trend annunciator alarm panels. The warning system displays a textual message describing the symptoms of a potential fault detected by PRODIAG. The fault at this point could be due to sensor failure since the COSS, and in turn the underlying model of the CVCS in conjunction with PRODIAG, has merely detected a deviation or trend in the indication for a dimension of a given component. COSS performs the validation process to determine if the indication triggering the warning due to sensor failure or an actual fault. To accomplish the validation process, PRODIAG compares the trend in the indication against the rest of the components in the CVCS model to determine if the trend is physically possible, while indicates an actual fault. Once the validation has verified there is an actual fault, the textual warning message changes to a more specific identification of the root cause of the plant fault. The warning system also provides the operator with a shot clock that denotes the amount of time until a critical point is reached in the system that merits a drastic action, such as a plant shutdown. This shot clock information is important because it provides time context for the operator to determine the severity of the fault. Given more time, the operator can adopt a more liberal mitigation action, but with less time the operator may opt for a more conservative and safer mitigation action to ensure plant safety and protect equipment.

The other main component of the digital alarm system is the trend annunciator alarm panel. This portion of the digital alarm system integrates a few previously separate functions to aid the operator. The trend annunciator alarm panels combine the standard annunciator alarms found in currently operating nuclear power plants with trend displays. Retaining the standard annunciator alarms is important since a seasoned operator can use the spatial patterning of the active alarm tiles to glean an impressive amount of information concerning the current state of the plant. Annunciator alarms are triggered by predefined setpoint and are not mode specific. As a result, the combination of annunciator alarms conveys the state of the plant, for example during startup some indicators that are normally extinguished during 100% power steady state operation are illuminated even though no fault is occurring. The COSS extends this concept by including additional alarm levels in conjunction with trend displays overlaid on the annunciator tile. The trend display will bend from the standard flat line during normal operations to a curved line that pops out for the operator against the other trend annunciator alarms that are not deviating from their normal operating values. As the trend continues to deviate and crosses the warning setpoint, the background of the annunciator panel changes from the dullscreen grey to yellow. Once the trend crosses the alarm setpoint, the annunciator panel changes from yellow to red.

3.2.3 Computer-based Procedures

The computer-based procedures resemble traditional paper-based procedures found in the control rooms of nuclear power plants. The paper-based procedures follow a two-column format. The left column is sequentially followed when desired parameter values are observed based control board indication. The right column is reserved for contingency actions to take when an undesired parameter value is observed. The computer-based procedures use this format but add the additional functionality of record historian and position keeping for each procedure. The operator is liberated from tracking the procedures since the computer-based procedures guide the operator through the procedures to ensure steps are followed sequentially and that the criteria for proceeding with each step is met. Parameter values that are traditionally scattered across indication on the boards are aggregated within the COSS and displayed in a white highlighted area collocated near the step's instructions. This display format eliminates the need for

the operator to search for the desired parameter indication for that step and hold that information in memory while comparing it against the desired value stated in the procedure steps. This integration and colocation of information reduces errors. The intelligent COSS automation also highlights the appropriate selectable buttons for each step, i.e. "Next step" or "Response not obtained", as an additional method to prevent the operator from incorrectly proceeding to the wrong step or column of the procedure. The operator can override these automated prompts to proceed to an operator desired step, however overriding the automation to move away from the prescribe step or column requires additional actions that reduce the chance for operator errors such as proceeding to an incorrect step or column.

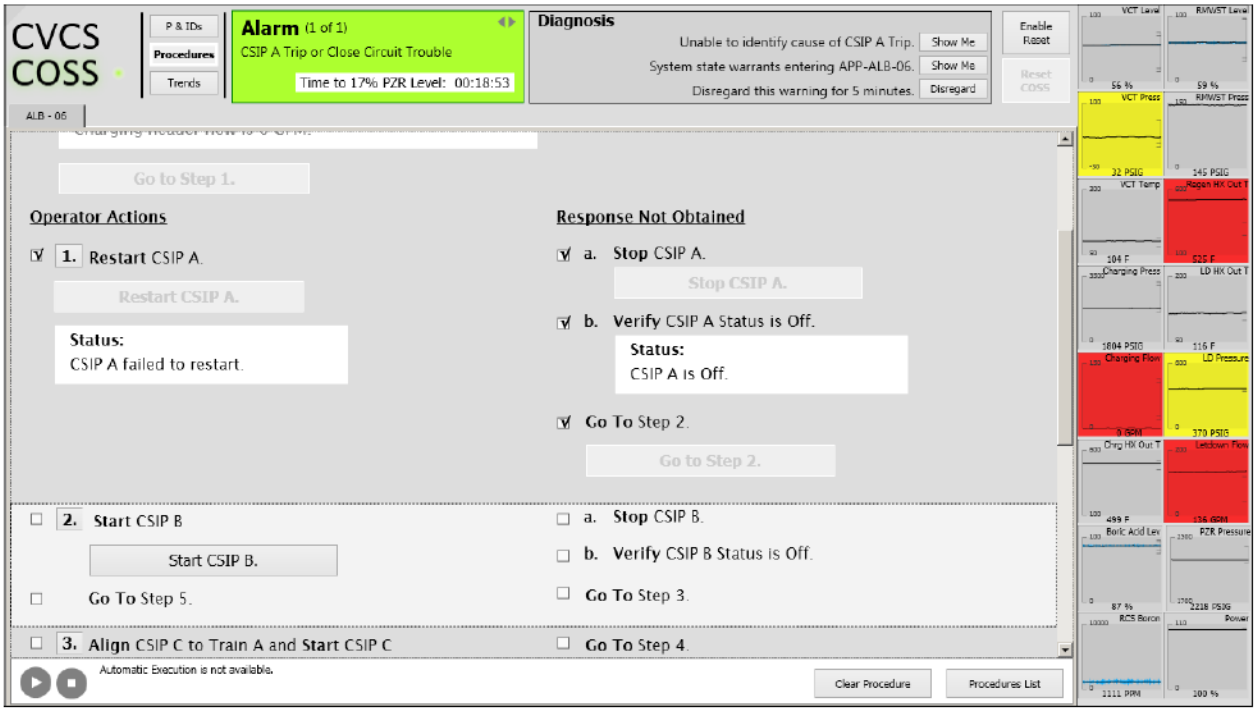

Figure 4. Computer-based procedures and Trend Alarm

The computer-based procedures also support completing multiple procedures concurrently. Often, crews complete multiple procedures at the same time. In a traditional control room, this results in the crew following and opening multiple binders of paper based procedures. The computer-based procedures on the COSS are all displayed organized within a single tabbed view. Furthermore, the COSS tracks the operators' progress through the procedures, which allows the operator to focus on the content of the procedure step. The procedures are structured in a cross referenced manner in which one procedure might require entering another procedure within a particular step of the original procedure. Adding to the complexity is the recursive nature of the procedures in which a procedure step calls for entry into another procedure and that procedure in turn instructs the operator to return to the original procedure. The COSS automates these procedure transitions and re-entries to eliminate confusion and the potential for erroneously proceeding to the wrong procedure or step.

The computer-based procedures support automated scripts consisting of multiple procedure steps. The operator can activate the automated scripts for redundant steps to save time and free him or herself to focus on other areas of operation. The operator has control of the COSS and automated procedures at all times. The operator can use the buttons along the bottom of the computer-based procedure view to stop an automated script and return to completing the procedure in the traditional step-by-step fashion. In addition to control over the automatic features of the computer-based procedure, the operator can also cue additional procedures or cancel out of a given procedure if they have the desire or need to do so.

3.2.4 Piping and Instrumentation Diagram System Representation

The COSS provides the operators with system diagrams in the form of piping and instrumentation diagrams (P&IDs). These P&IDs serve three primary purposes for the COSS. First, the P&IDs provide the operator with general system information concerning the organization and interconnectivities of the various components within a system as well as the interconnectivities between systems. Providing a visual depiction of the physical system being controlled is valuable for building and maintaining a mental model of the systems and components within systems so that the operator can quickly diagnose and take actions after a fault has occurred. Second, the P&ID view serves as a method to quickly highlight a faulted component and the nearby affected components. Third, the P&ID view supports the operator in performing manual actions on components. The operator can select a component on the P&ID view to display a pop-up menu containing parameter indication and any controls associated with the component. The manual manipulation of the components within the P&ID view is separate than the controls found within the computer-based procedures. Operators are able to navigate to the P&ID view to fine tune component controls independently of a procedure.

3.2.5 Recommender Module

The recommender module, in conjunction with the digital alarm system, comprises the core of the COSS functionality as an operator aid. The recommender module provides the operator with suggested mitigation actions based on the diagnosed and verified root cause determined by the warning system. The mitigation actions are presented as entry options into computer-based procedures selected for the particular root cause of the fault. The operator is provided with multiple mitigation action options and can select the desired option by choosing the "Show me" button next to each option. Selecting this button cues the computer-based procedure view of the COSS. In addition to suggesting mitigation actions, the recommender module also displays diagnostics information about the COSS. For example, the recommender module area will display "Validating…" while the root cause is being determined. Additionally, once the root cause is determined, the recommender module will provide information about the confidence of determining the root cause in the form of a probability percentage. This information is important to convey to the operator situations in which the COSS might beyond its diagnostic and prognostic capabilities in which the operator should exert caution and proceed with a safe but conservation shutdown action.

3.2.6 Overview Display

This current version of the COSS includes a second display for overview information. This display is intended to consist of an entirely separate physical display from that of the primary COSS display. The overview display is intended to augment the operators' interactions with the primary COSS display by providing contextual information concerning the general plant status. The current implementation consists of a single overview display; however future iterations are envisioned to consist of hierarchical screens in addition to the plant overview. This would support the operator in activities such as drilling down from the system status level to more detailed information concerning more specific subsystems as well as individual components. Additionally, this overview display will provide a means to link future COSS displays into an aggregated framework. As additional systems are incorporated into the functionality of the COSS display more detailed screens will be developed to display task-based information. The plant overview is designed as a safety parameter display system as specified by NUREG-0737 and provides the following:

(i) **Reactivity control** is maintained by current analog controls on the board, the plant overview provides reactor power and rod position indicators

(ii) Reactor core cooling and heat removal from the primary system can be monitored using the loop temperature trend graph as well as the RCP pump statuses.
(iii) Reactor coolant system integrity can be monitored via the RCS Pressure, Tavg, and Pressurizer indicators.
(iv) Radioactivity conditions in the main steam lines are provided for each loop
(v) Containment conditions can be monitored using the containment pressure sparkline trend and indicator (CNM Pressure)

In addition to class 1E safety statuses the overview provides information related to the secondary loop (valve statuses, gross generation, impulse pressure, breaker statuses, SG levels, feed water flow, main steam flow), and safety-support systems (RWST level, RHR pump statuses).

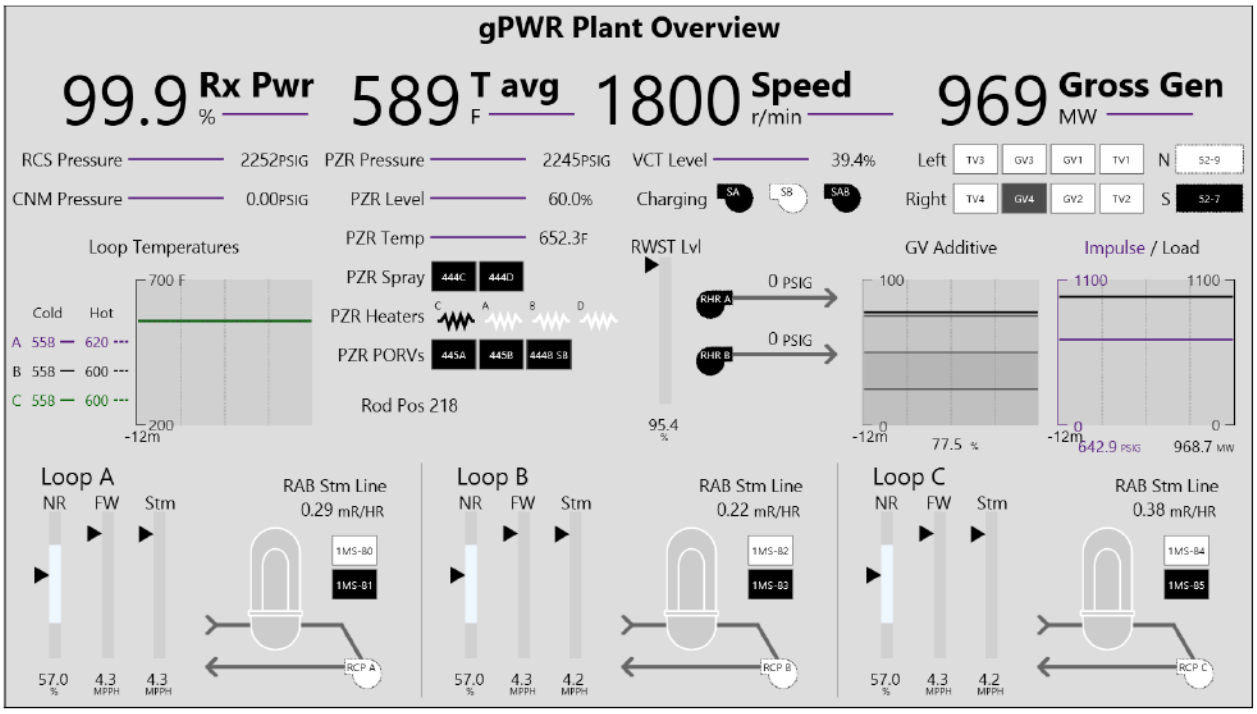

Figure 5. Overview display containing general plant status

3.3 Technical Considerations

Previously discussed COSS prototypes focused on demonstrating how operators would interact with such a system without extended analysis into how COSS would integrate with PRODIAG. Here we discuss how PRODIAG (implemented in Java) *could* and eventually will be merged with a COSS prototype implemented in Windows Presentation Foundation (.NET) for the Chemical and Volume Control System (CVCS) of GSE's virtual generic Pressurized Water Reactor (gPWR). The discussion will focus on the particularities involved with making this configuration function.

3.3.1 PRODIAG

Given a properly described process control system, PRODIAG can continuously monitor the system to detect noisy or faulty sensors. When off-normal process operating conditions occur, PRODIAG can identify and output the identity of the possible component faults.

3.3.2 COSS

COSS is a collection of technologies that support a process control operator in maintaining situational awareness regarding the process they are monitoring, informing the operator when off-normal process operating conditions occur, and providing guidance to assist the operator in mitigating the fault and validating that the fault has been mitigated.

Here we decided to implement the COSS prototype with Microsoft Windows Presentation Foundation (WPF; Lew, 2014). WPF is Microsoft's de facto standard for developing desktop applications and is intrinsically linked to Microsoft's .NET framework. WPF uses a *Code-Behind* model in which the visual look and feel of the interface is segregated from how the visual components are wired together. The Common Language Runtime component of the .NET can produce machine code from several programming languages: Visual Basic, C++, C#, F#, Python (IronPython). WPF also comes pre-equipped with most of the standard and advanced interface modalities one might wish to integrate into a modern DCS. These factors allow for rapid prototyping and an agile software development model. A second compelling reason for using WPF is the robust and well-documented code base. The underlying framework has been heavily optimized for performance, reliability, and security.

3.3.3 GSE gPWR

This project used the Generic Pressurized Water Reactor (gPWR) simulator as the test bed for the CVCS COSS prototype. The plant simulator was licensed from GSE Systems and the control displays have been tailored to fit the bays using GSE's JADE (Java Application Development Environment) software toolkit. The control boards of the gPWR emulate those of a 1000 MWe 3-loop Westinghouse PWR built in the 1980s. The layout and controls are typical of this vintage of plant. Provides graphical user interface mimicking the physical control boards normal found in the main control room (MCR) as well as providing an Instructor/Engineering graphical user interface for running the simulator from particular initial conditions and triggering malfunction events.

3.3.4 General Functional Description

The end product of the integration is a system where (see Figure 2 for Flow Diagram):

1. PRODIAG monitors the CVCS system of gPWR
2. When a fault occurs PRODIAG detects and the fault and data pertaining to the fault is acquired by COSS
    a. Fault data from PRODIAG is structured in a manner that is convenient for machines rather than humans, the exact format to be decided upon
    b. Either through the SimExec database and/or combination of third party database
3. The COSS upon receiving the fault cross-references the fault with an Expert Knowledge System
    a. If expert knowledge exists
        i. A template for presenting the fault data is used to convey the fault to the operators
        ii. Additional logic considering variables and factors not considered by PRODIAG to diagnose the fault or potential faults
        iii. A tailored procedure may be available to the operators to mitigate the fault (e.g. additional step to move diverter valve to bypass demin loop.)

iv. Convey information on critical plant variables that need to be monitored. COSS in-turn will monitor those variables and estimate the time until critical decision points are meet

b. In the event no expert knowledge pertaining to the fault exists
   i. A generic template is used to convey the fault information in natural human language
   ii. The operator must decide what actions or procedures are needed to correct the fault.

4. Operators take action to mitigate the fault
   a. PRODIAG continuously monitors the fault and notifies the COSS if the system returns to a steady-state
   b. In the event the fault is not mitigatable or the plant slips outside safe operating boundaries other actions would be taken to ensure safe plant operation

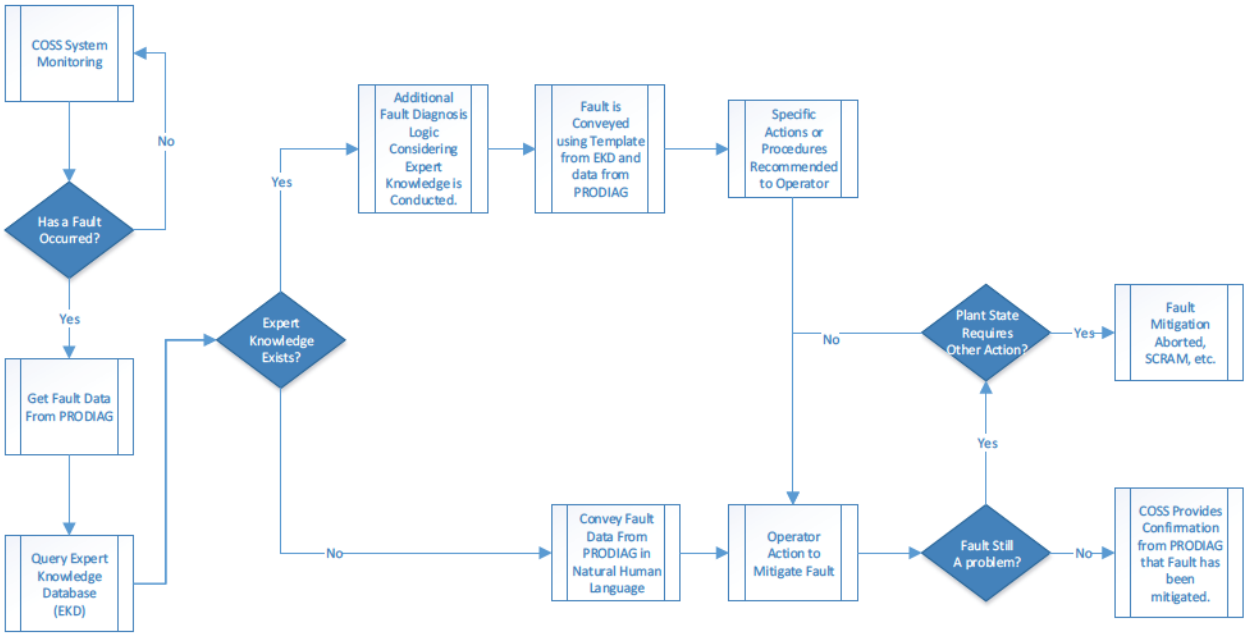

Figure 6. COSS/Operator Centric Program Flow for a single fault

3.3.5 Physical Architecture

The end goal is to deploy the integrated PRODIAG / COSS system in the full-scale full-scope nuclear control room simulator (here after HSSL Simulator) within the INL's Human Systems Simulation Laboratory (HSSL; see Figure 6). The HSSL Simulator consists of a centralized server running the GSE gPWR and several *bays* emulating the control boards of a nuclear power plant. One or more bays would run the COSS and communicate with gPWR via network protocols. PRODIAG will also communicate via network protocols to support development (communication with a gPWR server on the INL network over a VPN connection) and to support the final deployment. At any given time multiple instances of the COSS executable may be ran simultaneously, but only one instance of PRODIAG is anticipated to be running.

The HSSL is a full-scope, full-scale glass top simulator capable of simulating existing and future nuclear power plant main control rooms. Developing the COSS within the context of the HSSL provides a

number of advantages. First, by simulating a physical control board, the location and size of the COSS display can be iteratively evaluated to determine the optimal placement and sizing. The second advantage is scalability. The functionality of the COSS can be expanded to include other systems, such as the turbine control system, which may not be modeled on part-task simulations. Lastly, embedding the COSS within a high fidelity testing environment enables the demonstration to reflect how the actual technology would be used by providing a realistic environment for operator studies. Consequently, integrating the COSS with the HSSL enhances the validity of the concept as well as the practical applicability.

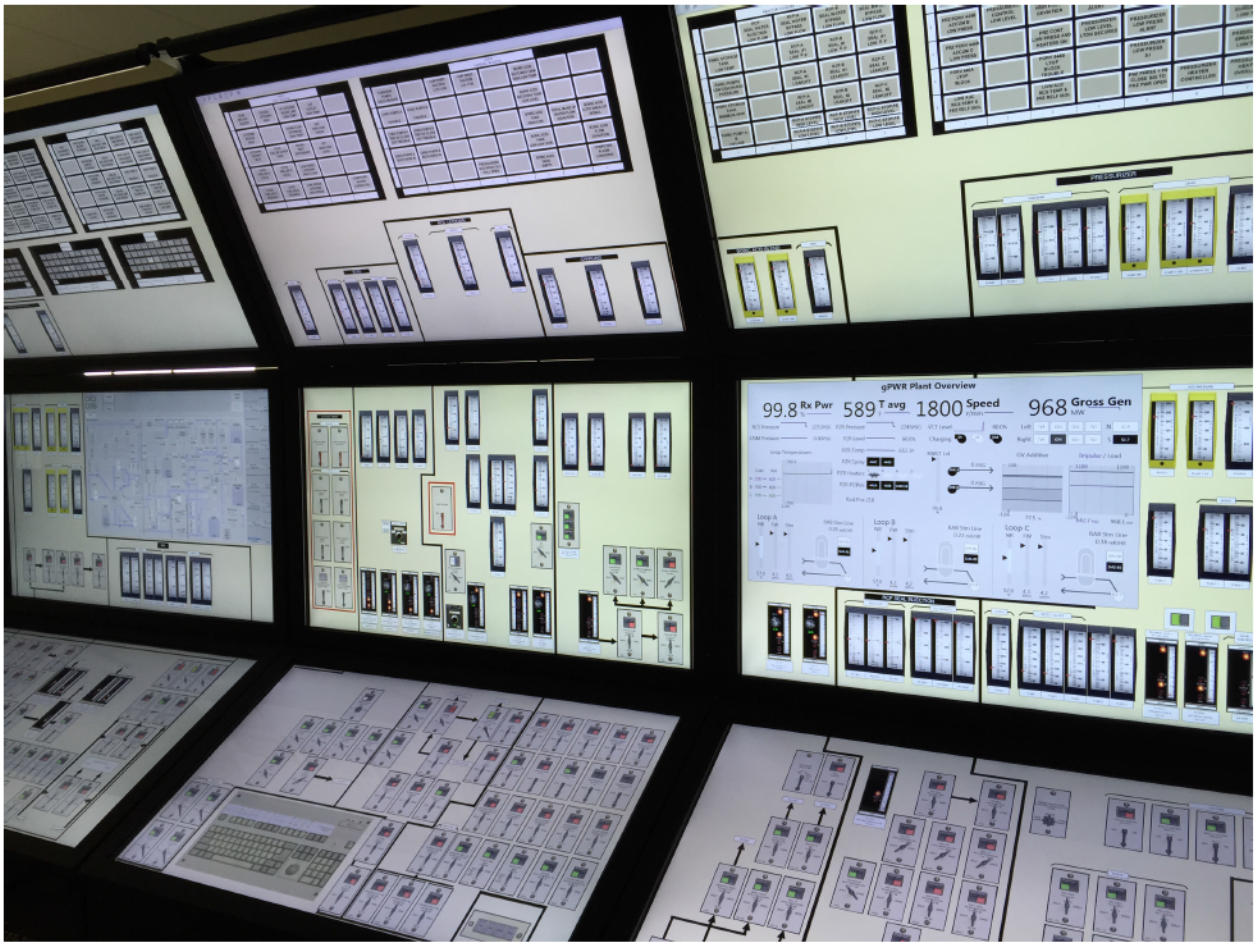

Figure 7. CVCS COSS prototype (left) and plant overview screen (right) embedded in the HSS

The full-scope full-scale glass top simulator consists of fifteen virtual panel bays. Each bay contains three 46-inch high definition displays. The displays are arranged in a convex arc relative to the operator. The lower two displays are touch capable allowing users to interact with simulated physical controls in a natural manner. The HSSL simulator is both physically and digitally reconfigurable. This allows it to represent a variety of nuclear simulators running on a variety of simulation platforms, and to arrange the bays to physically map the control rooms of the actual plants.

The COSS DCS is displayed as a picture-in-picture embedded on a vertical display of a simulator bay. This solution mimics the effect of adding a touch panel display to the analog control boards of an actual plant. A primary limitation is the resolution afforded on the displays in the bays. The available resolution for the entire 46-inch display is equivalent to the resolution expected of a 23-inch DCS display at the plant. As such, the HSI was designed to be legible even when scaled to half the resolution found in an actual DCS. Another limitation of embedding the COSS DCS into the context of the control boards is the

limited real estate available for displays. Given the large number of indicators and controls on typical NPP control boards, it becomes very difficult to make space available at the boards. While ideally it would be possible to have multiple displays available for the COSS, practically speaking, most plants are challenged even to make room available for the addition of one display on a panel. To realistically emulate this constraint, the COSS DCS is designed to fit on a single display.

3.3.6 Data Flow

An envisioned data flow is provided in the diagram below. GSE's gPWR plant model consists of two primary components: a database (SimExec) storing the process variables with several communication interfaces and the plant model simulating the numerous sub-systems and plant processes. The COSS would interface SimExec to read and depict the process variable states normal obtained from physical sensors. The COSS would also be able to control components normally controllable from the MCR. PRODIAG can enhance the human machine interface (HMI) by providing additional information related to the system's state such as depicting the presence of flow through piping and components on piping and instrumentation diagrams. (Other potential state information that could be provided by PRODIAG?). Human operator's interfacing the COSS are anticipated to need/what diagnostic information pertaining to the operation of PRODIAG. This diagnostic information would be provided as optional *layers* on the P&ID view the COSS will provide data quality metrics and confluence metrics so operators have some insight into what PRODIAG is doing behind the scenes. The intended purpose would be to allow operators to look under-the-hood, see the gears are turning, and develop trust for the system. Might also could provide additional diagnostic information to operator. Would essentially provide an Engineer's view of PRODIAG/MSET, would not be displayed by default to avoid overwhelming operators with visual clutter.

Lastly, but perhaps mostly importantly fault diagnostic information should be provided by PRODIAG to the COSS. The technical details of how this is accomplished will be adjourned until the next section. The envisioned data flow is for PRODIAG to specify fault related information in a generic manner related to the capabilities and constraints of PRODIAG. The Expert System and COSS will be responsible for taking this information and conveying it in a manner that is interpretable and actionable by the human operators. This approach is envisioned as optimal because one of PRODIAG's strengths is the ability to handle generic systems by learning process trends without explicit customization.

3.3.7 Communication Technical Details

3.3.7.1 COSS ←→ gPWR

The COSS is implemented as a .NET WPF application has two-way communication with gPWR using GSE's GII dynamic link library via a C++/CLR .NET wrapper library developed by the INL (GIINET). The GIINET wrapper exposes a fully managed .NET interface allowing users to communicate with SimExec without declaring unsafe code blocks and platform invocations.

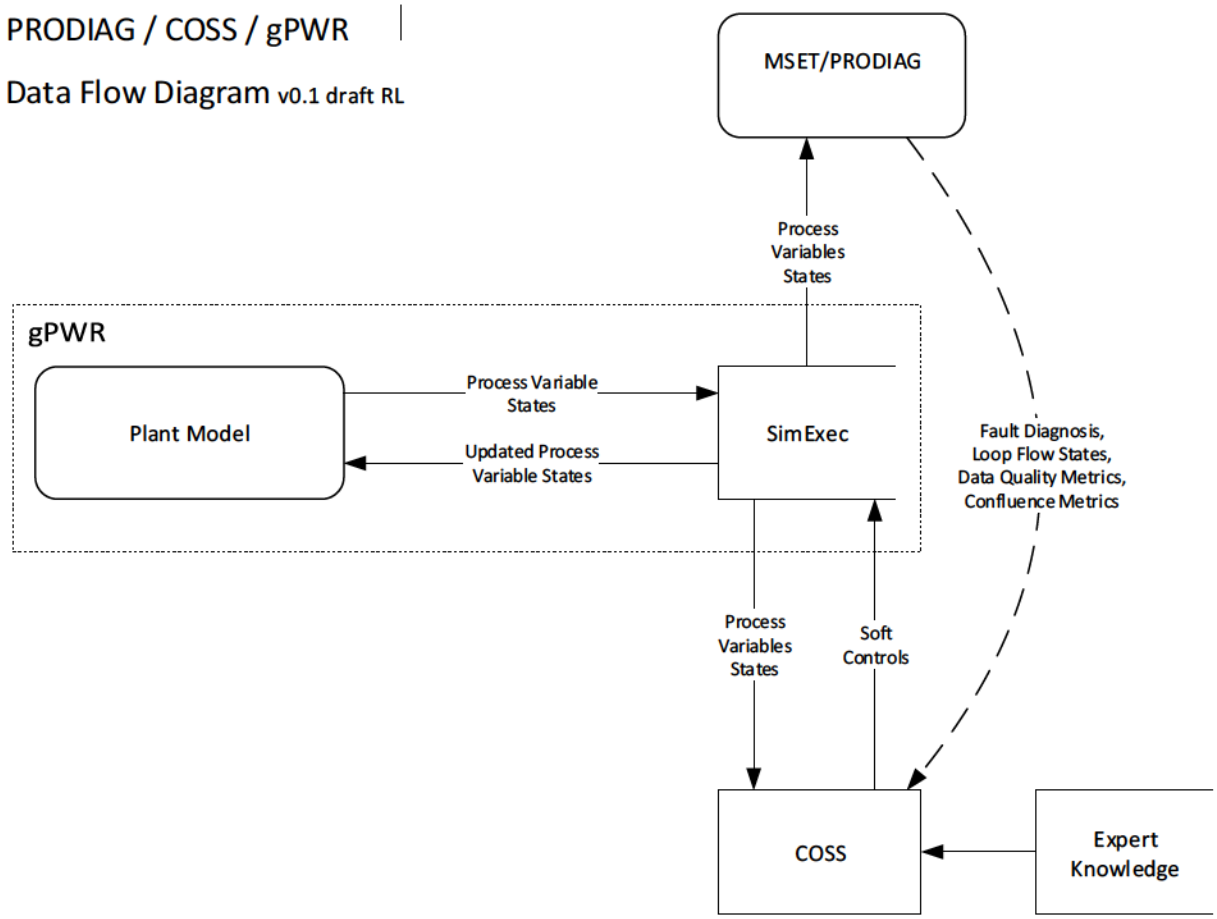

Figure 8. Diagram demonstrating the flow of data between major components

3.3.7.2 PRODIAG ← gPWR

PRODIAG could request process variable state information from gPWR through a variety of mechanisms. The *Front End* (Instructor Station, operator station (panel mimics)) of gPWR is implemented in Java. The front end components communicate through a Java library provided by GSE. Since PRODIAG is implemented in Java one possibility is to use this interface to obtain data from gPWR; however; no documentation exists on how to use the Java libraries developed by GSE. Another possibility is to wrap GII or GIINET to make them callable from Java. On the surface wrapping GIINET might be easier but it may be complicated by the fact GIINET takes advantage of .NET's Object type to make generic requests without having to know the datatype of the requested variable.

3.3.7.3 PRODIAG → COSS

As previously discussed PRODIAG needs to communicate information back the COSS. The loop flow state, data quality metrics, and confluence metrics could be passed through SimExec by adding additional variables (*point values*) to the database. The fault data also needs to be relayed to the COSS. SimExec could be used to this information, but may somewhat inflexible in this regard. It is essentially functions as a table with predefined point names and datatypes (int, float, string) without the ability to represent data in more flexible, versatile, hierarchical formats (e.g. JSON, yaml).

This page intentionally left blank

4. CVCS COSS EVALUATION APPROACH

4.1 Introduction

The COSS should ultimately improve operator performance and overall system performance by reducing operator workload and errors. The COSS is able to aid operator performance via advanced information aggregation and display to techniques to provide the operator with the crucial plant information at the appropriate time to enable effective operator actions. Providing critical plant information in a time sensitive manner is imperative to provide the operators with sufficient time to mitigate potential plant problems before more conservative and drastic actions must be taken, which can result in the plant being taken offline. To ensure that the COSS is in fact improving operator performance as opposed to simply adding another system that now taxes the operators' capabilities and may even reduce performance, several performance evaluations are planned for the next phase of the COSS development.
The current COSS prototype version includes communication functionality between the COSS prototype and the gPWR simulator. Communication between the two pieces of software allows the COSS prototype to acquire and display values in real time from the gPWR as it is running. This communication is fundamental for operator performance evaluation, because it allows for human-machine interaction examinations of the COSS display concepts within the surrounding context of the simulated control panels displayed on the glasstop panels of the bays comprising the HSSL.

Operator performance comparisons can be made by examining the performance of the operator with a current existing system, simulated by the gPWR followed by examining the performance of the operator with the COSS. This method of examination has been conducted in number of studies including several conducted by the authors using the HSSL. Specifically, the authors have collaborated with a utility undergoing a turbine upgrade, which entailed main control room interface upgrades including a new digital turbine control system. As outlined by the verification and validation process required for NUREG-0711 licensing, INL acted as an independent evaluated to compare operator performance on the existing turbine control system against the new digital turbine control system to ensure that no performance decrements resulted from the upgrade. Indeed, the upgrade resulted in several performance enhancements.

4.2 Comprehensive Evaluation Approach Overview

Several individual aspects of the COSS, which will be discussed in the next several sections will be combined into a comprehensive evaluation approach. The evaluation will consist of observing the operators during simulated scenarios and recording their behavior within the context of the simulator and all its components and associated variables. This evaluation will include an examination of the performance enhancement experienced by the operators due to the advanced data displays and aggregated data displays provided by the COSS. These performance enhancements will be further examined by evaluating the operators' situation awareness acquisition and measuring the amount of trust and reliance the operators place on the COSS.

4.3 System Fault Diagnositics Accuracy

Before evaluating any aspects of operator performance, the system itself must be verified in terms of providing accurate information and diagnosis of faults. PRODIAG is the underlying mechanism that supports the COSS's prediction capabilities to provide the operator with timely diagnostic information. This report is primarily concerned with the display and human-machine interaction aspects of COSS; however, the underlying algorithms and logic that support the ability for the COSS to display this information merits some consideration. Argonne National Laboratory (ANL) is currently developing and

validating PRODIAG. Additional specific details concerning PRODIAG can be found in ANL/NE-12/57 (Vilim et al., 2012).

4.4 Operator Performance Constructs and Evaluation Strategies

Within the field of process control and nuclear power generation, a number of metrics have been developed to evaluate operator performance. These metrics typically include the cognitive constructs of mental workload and situation awareness. Mental workload refers to the amount of mental effort required for a task. The most common measure of mental workload is the NASA-TLX, which quantifies the amount of mental effort required for a task of a specified length along 6 dimensions (Hart, 1988). The NASA-TLX is a widely accepted gold standard for mental workload and can be applied to nearly any domain including nuclear process control. Within the context of the COSS evaluation, the operators would complete the NASA-TLX following the end of each scenario. The mental workload during scenarios using the COSS and scenarios using traditional control practices are compared. The presence and magnitude of the reduction in mental workload resulting from the COSS serves as evidence for potential operator performance improvements.

4.4.1 Automation Trust and Compliance

As automation becomes increasingly ubiquitous in the control room the operator's role shifts from a manual action performer to a more supervisory role in which the operator monitors the automation and augments automation decisions during unforeseen or ambiguous plant conditions. This human-automation interaction can lead to positive performance outcomes; however it can also lead to performance decrements in which the operator finds himself or herself out of the loop and unaware of both the state of the plant and a path to return the plant to normal operating conditions. The extent that the operator trusts and complies with automation can serve as a measure of the quality of the human-automation interaction between the COSS and the operators. Trust refers to the extent that the operators believes the accuracy of the information presented and decisions selected by the COSS.

4.4.2 Performance Enhancements

Measuring performance in a nuclear process control setting can be difficult because there are multiple paths to success. These multiple paths result from the high level of interdependency between both systems and components within systems. Additionally, a significant number of components and systems exist to maintain important energy production efficiency and ensure high levels of safety within nuclear process control. These additional system and components add to the path options available to an operator during a given situation. There are a number of clearly defined plant condition boundaries, which the operators maintain critical plant systems within. In the most basic sense, the performance of the operator can be determined based on whether they cross any of these boundaries while presented with a component fault during a predefined scenario. Fortunately, to the benefit of safe and efficient nuclear generated electricity, the operators are exquisitely trained such that they rarely manipulate the plant condition to exceed these boundaries. As a result of the exceptional performance standards achieved by operators, operator performance evaluations based on maintaining plant conditions within these boundaries does not provide sufficient variability for making meaningful conclusions concerning the performance enhancements resulting from the COSS.

A better approach to evaluating operator performance is comparing critical component state prior to the fault with their states following the fault. The performance is the magnitude of difference between the component states pre- and post-fault. This affords direct comparisons between an scenario in which the operators have access to the COSS and scenarios in which the operators use the traditional control boards.

Evaluating operator performance in this manner requires identifying critical plant parameters to serve as the basis for the performance comparisons and then analyzing the simulator logs that record these variables during the scenario.

Another common approach for performance evaluations involves using subject matter experts (SMEs; Lau, 2015). The SMEs collaborate with the researchers to both qualitatively and quantitatively describe the operator's performance while being observed by the SMEs during the scenarios. The SMEs are typically seasoned former operators with extensive expertise in both plant operation and training operators. The SMEs are provided with a performance metric including a rubric to evaluate operator behaviors during the scenario. Since there are multiple paths to success, the SME identify discrepancies between the optimal path they define and the operators observed path. The SMEs are briefed on the scenario details prior to the scenario observations so that they fully understand the optimal path and can adequately evaluate the discrepancies observed during the scenario. Typically, multiple SMEs are used to help reduce subjective bias. The multiple ratings are analyzed to ensure good inter-rater reliability to maintain a valid measure of performance.

4.4.3 Operator Situation Awareness

Situation awareness is an important performance evaluation metric within nuclear process control. Indeed, prominent regulation within nuclear process control mandates that the control room design and any new additions, such as the COSS, should aid operators as they acquire and maintain situation awareness (NUREG-0711). There are multiple competing models of situation awareness, but Endsley's model is the most widely accepted within the human factors field and many practitioners have adopted her three-level SA model (1995a). Endsley's three-level model defines SA as the "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (1995a). Level one consists of identifying the elements in the environment, level two consists of integrating the elements into a comprehensive representation in relation to task goals, and level three consists of projecting the future states of the integrated elements within the environment. The model is hierarchically organized such that each level requires the successful completion of the level below it. This hierarchical organization provides the model with the capability to isolate breakdowns in SA that occur in a particular situation or system as well as evaluate how the system's interface supports each level of SA. Numerous techniques have been developed to measure SA. A review of SA measures by Stanton et al. classified 30 different specific measures of SA into four main techniques, which are freeze probe, real-time probe, self-rating, and observer rating (2005). Each of the 30 specific measures consists of some variant of these four main techniques developed for a specific domain or to evaluate SA within the framework of a specific model.

Self-rating. Self-rating is one basic technique used for evaluating SA. The self-rating technique consists of individuals rating themselves on multiple dimensions of their subjective SA post simulation. The situation awareness rating technique (SART) uses ten dimensions to rate SA (Taylor, 1990). The ten dimensions of SA in the SART are instability of the situation, complexity of the situation, variability of the situation, arousal, concentration of attention, division of attention, spare mental capacity, information quantity, and familiarity with the situation. Individuals rate themselves on a seven-point scale for each dimension of SA. The ease of administration and lack of intrusion on the primary task are the two main advantages of the self-rating technique. However, the self-rating technique collects participant data after the trial has ended, which potentially causes a number of issues. Self-ratings may be distorted due to an individual's biased perception of their performance during the simulation (Endsley, 1995b). Furthermore, individuals must remember their mental state when rating themselves on the various dimensions, which confounds self-ratings with working memory and recall abilities. When rating the different dimensions of SA, individuals must condense dynamic moments of SA throughout the simulation into a single average value for each SA dimension. Additionally, the subjective self-report ratings may not necessarily correlate

with performance during the simulation. Participants can potentially rate themselves highly on the SA dimensions; however their performance may have in fact been poor.

Observer Ratings. Observer ratings are another subjective measure widely used to evaluate SA. The observer rating technique consists of SMEs observing and rating participants' SA during the simulation (Salmon et al., 2009). The SME rates the participants' SA on predefined observable behaviors. Observer ratings are advantageous since they require minimal intrusion on the primary simulation task and can be conducted in industry with professionals completing real life tasks as opposed to completing simulations. An example of an observer rating technique is the Situation Awareness Behavioral Rating Scale (SABARS) used by Matthews and Beal (2002) to measure SA of infantry soldiers in field training exercises. Bias in the observation and recording are potential disadvantages of the observer rating technique. Replication of experiments is virtually impossible without the original subject matter expert, which makes comparisons between studies and disciplines difficult.

Freeze Probe. The freeze probe technique is the most widely used objective SA measurement. The freeze probe technique consists of administering SA related queries while the simulation is suspended or frozen (Endsley, 1995b). The queries to evaluating SA are created by first conducting a detailed cognitive task analysis to ensure that the SA related queries meaningfully relate to SA deemed necessary for the successful completion of a given task (Endsley, Selcom, Hardiman, & Croft, 1998). In complex tasks, subject matter experts are consulted both during the task analysis and to evaluate the relevance of the generated SA related queries. The individuals responses reported during the freeze probe are compared to the actual state of the system at that particular point in time, as defined by the experimenter, to yield an overall SA score for a task. SA query responses may contain information about the value of a component with relatively static properties, such as an alarm that is either in the on or off state. Additionally, the responses may contain information about the rate and direction of change for a component with more dynamic properties, such as a speedometer in a car. Scores from multiple tasks can be used to quantify the amount of SA at various time points during the simulation. The primary benefit of the freeze probe technique is the immediate objective SA assessment periodically throughout the simulation as opposed to measurements of SA at the end of the trial. The situation awareness global assessment technique (SAGAT) is an example of a well-known freeze probe technique designed with queries that specifically evaluate SA at each of the three levels of Endsley's SA model. (Endsley, 1995b). Queries from the SAGAT developed for use in aviation consist of questions concerning a pilot's knowledge of the aircraft's airspeed, altitude, attitude, and location (Endsley, Selcom, Hardiman, & Croft, 1998). The SAGAT developed for use within the military aviation domain contains the same queries found within the general aviation domain in addition to combat queries such as the location, altitude, airspeed and potential threat level of other aircraft (Endsley, Selcom, Hardiman, & Croft, 1998). There is more evidence correlating performance with the SAGAT freeze probe technique than any other SA measurement (Salmon et al., 2009). Despite the strong correspondence between assessed levels of SA and performance, the validity of the freeze probe technique is questionable. Skeptics have criticized the SAGAT and its underlying freeze probe methodology due to the potential invasion on the primary simulation task. Furthermore, the freeze probe query captures other factors in addition to SA. Disambiguating working memory and recall from SA construct as assessed with the freeze probe queries is not possible (Salmon et al., 2009). The SA information must be retained in working memory while the simulation is frozen and the queries are administered. Newer techniques sensitive to different cognitive aspects of SA are needed to isolate SA construct for an accurate assessment.

Real-time Probe. The real-time probe technique is another SA measure that relies on providing participants with SA related queries (Salmon et al., 2009). Unlike the freeze probe technique, the real-time probe does not suspend the simulation. This technique was developed to mitigate the intrusion on the primary task induced by suspending the simulation. The content of the answers and the response time in providing the answers are used to generate a score for the level of SA. The situation present assessment

method (SPAM) is an example of a real-time probe technique used to evaluate SA in air traffic controllers (Durso et al., 1998). The SPAM is remotely administered over the telephone to air traffic controllers. The response times for correct answers are used to assess the level of SA. A shorter response time reflects the air traffic controller with a high level of SA since the air traffic controller can mentally recall the information or efficiently direct his or her attention towards the necessary indicator to retrieve the information quickly. Longer response times reflect lower levels of SA since the air traffic controller cannot mentally recall the information and does not efficiently locate the information quickly. The time that it takes the air traffic controller to answer the telephone provides mental workload information. Longer times to answer the telephone reflect higher levels of mental workload on the assumption that the air traffic controller is more engaged in controlling aircraft in his or her airspace and cannot immediately answer the telephone. The mental workload indicator provides an additional component for analysis, since SA has been shown to differ by the amount of mental workload (Soliman, 2010). The real-time probe suffers similar issues as the freeze probe. The queries intrude upon the primary simulation task. Completing the secondary task of answering probe questions concurrently with the primary task still involves a potentially significant amount of distraction. Additionally, cognitive elements such as working memory are indiscriminately captured by the real-time probe. As with the freeze probe technique, there is no way to differentiate these cognitive elements from the SA construct.

All four of these measurement approaches are intended be used to varying extents for evaluating the COSS in terms of its implications for operator SA. The freeze probe and real time probe measurement techniques should not be used concurrently since this would result in significant intrusion upon the primary task of controlling the nuclear control process. As such, the freeze probe shall be administered since it will not distract the operators while he or she is actively interacting with the control boards and COSS. Though the freeze probe does generate interference by stopping the operators from their control task, it does so in a manner that they are accustomed to through their training. While undergoing training scenarios the simulator is often frozen and aspects of the current scenario are discussed by the operators and the instructors. Since operators are accustomed to these scenario pauses, the freeze probe technique will generate an acceptably minimal amount of interference during the evaluation scenarios.

4.5 Microworld Operator Performance Evaluation

The authors of this report are collaborating with the University of Idaho to evaluate some of the COSS concepts prior to a more in-depth evaluation with operators. The collaboration involves supporting a graduate student on his dissertation, which involves situation awareness assessment and methodology development along with advanced interface concepts development and evaluation. The collaboration benefits the COSS development work directly because it provides an opportunity to examine some of the COSS interface concepts to ensure that they adhere to good human factors design principles. Furthermore, the COSS interface concepts can be evaluated within the context of theoretical psychophysics and cognitive psychology in order to ensure that they also follow these principles in order to create an effective interface to aid operators.

Examining the COSS in the university setting affords a number of advantages. First, the number of participants that can be recruited to interact with the COSS is much larger and the participants are more accessible and inexpensive. This allows for a more in-depth investigation of basic COSS interface design concepts before they are evaluated with trained, licensed, and experienced operators. The participants available in the university setting are primarily undergraduate students at the university. These student participants do not have the experience or knowledge that seasoned operators possess, however, since the same basic information theory and cognitive processing components are present within student participants. These underlying cognitive components are universal for the population at large, which allows the student participants to serve as representative interface users. Still, careful consideration must

be made in the construction of the COSS concept evaluation scenarios to ensure that they are understood by the student participants. Evaluating the entire COSS interface may require too much nuclear process control-specific knowledge, but individual COSS concepts can be evaluated in isolation without requiring extensive nuclear process control expertise.

5. CONCLUSIONS

This new iteration of the COSS represents substantial development efforts to add additional functionality and fidelity to the prototype. Ultimately, the goals of the COSS efforts are to demonstrate the benefits of operator aids that improve operator performance by augmenting operator cognitive abilities via alerting the operators to fast transient situations, providing clear success paths to mitigate abnormal plant conditions resulting from faults, and synthesizing information to display to the operator. The revised COSS includes an additional display, i.e. the overview display, to support the operator during the monitoring task. The overview display also provides the operator with contextual information concerning the general plant status in fast transient situations. This contextual information aids the operator's understanding as he or she begins to interact with the COSS during time-sensitive situations. The revised COSS also includes additional backend development that provides it with the capability to communicate with the gPWR simulator. This communication is a vital factor for supporting future evaluations in which the operator interacts with the COSS during a scenario involving the surrounding simulated control boards. The COSS is able to aggregate information from the simulator into the COSS and display live values during this scenario.

Future directions for the COSS development include adding additional functionality to support more integration with the gPWR simulator as well as incorporating PRODIAG system into the COSS infrastructure. The current implementation mimics the PRODIAG capabilities, which is effective for evaluating how this collection of technologies may improve operator performance. To fully evaluate such a system, the PRODIAG system should be allowed to operate in conjunction with the COSS visual elements to monitor, diagnose faults, identify mitigation actions, and convey this information to the operator. Another future development effort is aimed at including additional task-based displays. The overview displays provide a general plant status; however, these task-based displays will provide component information and procedure steps collectively. The incorporated information creates a centralized interface to provide all of the relevant information for a set of common and critical tasks performed by the operators.

This page intentionally left blank

6. References

Berg, O. (2012). Operator Assistant – A Conceptual Outline, OECD Halden Reactor Project, HWhP-032.

Bruemmer, D.J., Few, D.A., Boring, R.L., Marble, J.L., Walton, M. & Nielsen, C. (2005). "Shared Understanding for Collaborative Control," IEEE Transactions on System, Man and Cybernetics, Part A. Systems and Humans, vol.35, no.4, pp. 505-512, Jul. 2005.

Büttner, W. E. (1985). Advanced Computerized Operator Support Systems in the FRG, IAEA Bulletin, Autumn, 1985.

Calabrese, F., Corallo, A., Margherita, A., & Zizzari, A.A. (2012). A knowledge-based decision support system for shipboard damage control. *Expert Systems with Applications*, 39(9) 8204-8211.

Durso, F. T., Hackworth, C. A., Truitt, T., Crutchfield, J., & Manning, C. A., (1998). Situation awareness as a predictor of performance in en route air traffic controllers, *Air Traffic Quarterly*, 6, 1-20.

Eascon Corporation web page, http://www.eascon.it, Bologna, Italy, 2013.

Electric Power Research Institute (EPRI), "Disturbance Analysis and Surveillance System (DASS) Scoping and Feasibility Study," EPRI NP-2240, Palo Alto, California, July 1982.

Endsley, M. R. (1995a). Towards a theory of situation awareness in dynamic systems. *Human Factors*, 37, 32-64.

Endsley, M.R. (1995b). Measurement of situation awareness in dynamic systems. *Human Factors*, 37, 65-84.

Endsley, M. R., Selcon, S. J., Hardiman, T. D., & Croft, D. G. (1998). Proceedings from the 42nd Annual Meeting of the Human Factors & Ergonomics Society '98: *A comparative analysis of SAGAT and SART for evaluations of situation awareness*. Chicago, IL.

Goldberg, S. M., & Rosner, R. (2011). *Nuclear Reactors: Generation to Generation*. American Academy of Arts and Sciences, Cambridge, MA.

Hart, S. G. & Staveland, L. E. (1988). Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. In P. A. Hancock & N. Meshkati (Eds.) *Human Mental Workload*. Amsterdam: North Holland Press.

Hashemian, H.M. (2011). Nuclear power plant instrumentation and control. In Dr. P. Tsvetkov (Ed.), *Nuclear Power - Control, Reliability and Human Factors* (3), , ISBN: 978-953-307-599-0, InTech, doi: 10.5772/18768. Retrieved from: http://www.intechopen.com/books/nuclear-power-control-reliability-and-human-factors/nuclear-power-plant-instrumentation-and-control.

Hebert. D. Advanced Process Control Ain't Easy, Control, 2012.

Hitzel, R. & Block, F. (2003). Retrofitting steam turbines with modern control platforms. *PowerGEN 2003,* Las Vegas, NV.

International Atomic Energy Agency, "Development and Implementation of Computerized Operator Support Systems in Nuclear Installations," Vienna, Austria, September 1994.

International Atomic Energy Agency, "Development and Implementation of Computerized Operator Support Systems in Nuclear Installations," Vienna, Austria, September 1994.

International Atomic Energy Agency. (2011). Computer security at nuclear facilities, IAEA, Vienna.

International Atomic Energy Agency, "Development and Implementation of Computerized Operator Support Systems in Nuclear Installations," Vienna, Austria, September 1994.

International Atomic Energy Agency, "Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook," Vienna, Austria, 1999.

Institute of Nuclear Power Operations (INPO), SOER 10-2 Engaged, Thinking Organization, Atlanta, GA, 2010.

Institute of Electrical and Electronics Engineers (IEEE), IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities, IEEE 1786, New York, New York, 2011.

Invensys, 2011. Tricon Turbine Control System, Invensys Whitepaper PN-I-NC-0103.

Lau, N., Jamieson, G. A., Skraaning, G. (2015). Empirical evaluation of the process overview measure for assessing situation awareness in process plants. *Ergonomics*.

Lee, Seong Kon, Gento Mogi, and Jong Wook Kim. "Decision support for prioritizing energy technologies against high oil prices: a fuzzy analytic hierarchy process approach." *Journal of Loss Prevention in the Process Industries* 22.6 (2009): 915-920.

McKim, G., Yeager, M., and Weirich, C. (2011). DCS Upgrades for Nuclear Power Plants, Invensys Whitepaper PN I-NV-0104.

Matthews, M. D., & Beal, S. A. (2002). Assessing Situation Awareness in Field Training Exercises. U.S.Army Research Institute for the Behavioural Sciences. Research Report 1795. Nuclear Energy Institute (2011). Position paper: Control room staffing for small reactors.

Nuscale (Nov 7, 2014). Nuscale plant design overview. Revision 0. RP-1114-9375.

Oxstrand, J. & Le Blanc, K. (2012). Computer-Based Procedures for Field Workers in Nuclear Power Plants: Development of a Model of Procedure Usage and Identification of Requirements. Idaho National Laboratory External Report. INL/EXT-12-25671, Rev. 0.

Quinn, T., Bockhorst, R., Peterson, C., & Swindlehurst, G. (2012). "Design to Achieve Fault Tolerance and Resilience," INL/EXT-12-27205. Idaho Falls: Idaho National Laboratory.

Salmon, P. M., Stanton, N. A., Walker, G. H., Jenkins, D., Ladva, D., Rafferty, L. & Young, M. (2009).Measuring situation awareness in complex system: Comparisons of measures study. *International Journal of Industrial Ergonomics*, 39, 490-500.

Segovia, V. A. and Theorin, A. (2013) History of Control. History of PLC and DCS, http://www.control.lth.se/media/Education/DoctorateProgram/2012/HistoryOfControl/Vanessa_Alfred_report.pdf.

Soliman, A. M. (2010). Exploring the central executive in situation awareness. *Psychological Reports*

106(1), 105-118.

Salmon, Paul M., et al. (2005). "Measuring Situation Awareness in Complex Systems: Comparison of measures study."

Tavana, M. (2004). Intelligent flight support system (IFSS): A real-time intelligent decision support system for future manned spaceflight operations at Mission Control Center. *Advances in Engineering Software, 35,* 301-313.

Taylor, R. M. (1990). Situational awareness rating technique (SART): the development of a tool for

aircrew systems design (AGARD-CP-478) pp3/1 -3/17. In: Situational Awareness in Aerospace

Operations. NATO-AGARD, Neuilly Sur Seine, France.

Ulrich, T., Boring, R., Phoenix, W., DeHority, E., Whiting, T., Morrell, J., & Backstrom, R. (2012). "Applying Human Factors Evaluation and Design Guidance to a Nuclear Power Plant Digital Control System," INL/EXT-12-26797. Idaho Falls: Idaho National Laboratory.

U.S. Department of Transportation, Federal Aviation Administration, Introduction to TCAS II Version 7.1, 2011.

U.S. Department of Transportation, Federal Aviation Administration, Advanced Avionics Handbook, FAA-H-8083-6, 2009.

U.S. Nuclear Regulatory Commission (July 16, 2013). *History of Digital Instrumentation and Controls*, http://www.nrc.gov/about-nrc/regulatory/research/digital/history.html

Vilim, R.B., Heifetz, A.M., Park, Y.S., & Choi, J. (2012). "Description of Fault Detection and Identification Algorithms for Sensor and Equipment Failures and Preliminary Tests Using Simulations", ANL/NE-12/57, November 30, 2012.

Vilim, R.B., Heifetz, A.M., Yun, D., & Yacout,L. (2013). "Description of Algorithms for Detecting Sensor Degradation and Preliminary Tests Using Simulations," ANL/NE-13-2, February 1, 2013.