INL/CON-15-34404
PREPRINT

Computerized Operator Support System – Phase II Development

ANS NPIC-HMIT

Thomas A. Ulrich, Ronald L. Boring, Roger T. Lew, Kenneth D. Thomas

February 2015

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

Computerized Operator Support System – Phase II Development

Thomas A. Ulrich, Ronald L. Boring, Roger T. Lew, Kenneth D. Thomas
Idaho National Laboratory
PO Box 1625, Idaho Falls, Idaho 83415-3818, USA
thomas.ulrich@inl.gov; ronald.boring@inl.gov; roger.lew@inl.gov; kenneth.thomas@inl.gov

ABSTRACT

A computerized operator support system (COSS) prototype for nuclear control room process control is proposed and discussed. The COSS aids operators in addressing rapid plant upsets that would otherwise result in the shutdown of the power plant and interrupt electrical power generation, representing significant costs to the owning utility. In its current stage of development the prototype demonstrates four advanced functions operators can use to more efficiently monitor and control the plant. These advanced functions consist of: (1) a synthesized and intuitive high level overview display of system components and interrelations, (2) an enthalpy-based mathematical chemical and volume control system (CVCS) model to detect and diagnose component failures, (3) recommended strategies to mitigate component failure effects and return the plant back to pre-fault status, and (4) computer-based procedures to walk the operator through the recommended mitigation actions. The COSS was demonstrated to a group of operators and their feedback was collected. The operators responded positively to the COSS capabilities and features and indicated the system would be an effective operator aid. The operators also suggested several additional features and capabilities for the next iteration of development. Future versions of the COSS prototype will include additional plant systems, flexible computer-based procedure presentation formats, and support for simultaneous component fault diagnosis and dual fault synergistic mitigation action strategies to more efficiently arrest any plant upsets.

Key Words: computerized operator support system, human factors, nuclear power plant

1 INTRODUCTION

The nuclear power industry relies on highly trained operators to monitor and maintain safe and efficient nuclear power generation. Operators undergo extensive training and licensing to ensure they have the adequate expertise to alleviate plant upsets. Indeed, operators are quite adept at diagnosing and resolving these upsets. However, some upsets can occur so quickly that the operators cannot respond before a plant shutdown is required. For example, a leak within the demineralizer loop of the chemical and volume control system (CVCS) can pose a significant challenge to operators, as such a leak can rapidly misadjust reactor coolant chemistry, leading to a positive reactivity event and a costly plant shutdown. During shutdown, the plant cannot generate power, which induces a significant loss in revenue due to the lack of electrical power generation. Furthermore, the utility is obligated to compensate for the loss of electrical supply by generating or purchasing power from other sources to offset their lack of electricity production. Additionally, the plant faces costs from repairs or replacement of the faulty components responsible for the leak with expensive offsite experts brought in to quickly conduct repairs. Avoiding the costs of these unexpected shutdowns is paramount to ensuring the economical viability of reliable nuclear power electricity production.

The analog indication and control scheme found within the aging control rooms of U.S. nuclear power plants can hinder operators' abilities to respond to these rapid plant upsets. Many of these control rooms were designed with technology dating back to the 1960s [1]. The analog indicators and controls are arranged by system, but beyond this general grouping strategy, there is often little functional or task-based organization. In many cases, packing the necessary electronics into the back panel areas in line with

a Tetris-like process dictated the arrangement of the instrumentation and controls (I&C) on the main control boards. As a result, the interface is often less than ideal for portraying plant statuses. There is little to no prioritization of information to support a given task at a point in time, which forces the operators to constantly seek out pertinent information. Operators are typically interested in the system status as a whole rather than the individual indications relaying information about a particular dimension of a component. For example, a pressurizer has several dimensions including the percentage level full, pressure, and temperature. The dimensions in isolation have little meaning. The operators must integrate the individual dimensions to create an overall component status representation and then integrate the components of that system into an overall system status representation. The integration places significant mental workload and time requirements on the operators, limiting the operators' abilities to mitigate a rapid upset with sufficient time to avoid a plant shutdown.

The operators must maintain situation awareness between each crewmember and within the context of current procedures tracked by the senior reactor operator. The procedures consist of if-then rules governing actions to mitigate predefined plant upsets. The procedures dictate which information is needed as well as any control actions needed for a given situation. The operator must locate the information or control on the boards and verify the information against the procedure or complete the prescribed action. Following this fashion, the operator must pull together information from several discrete locations, which takes time and mental effort that could be used more directly dealing with the plant upset.

Yet another limitation resulting from the analog display format concerns the prediction of future states of plant systems. Operators predict future states of the plant in a manner analogous to driving a car while using the rearview mirror as opposed to the windshield. The driver must use rearview mirror information regarding where the car has been to steer the car in the forward direction, which is obviously not the most effective method for driving a vehicle. Miraculously, operators are quite good at using prior plant states to infer future plant states. Even more amazing is that the operators are able to infer this future state by merely looking at a brief snapshot of the current state of the plant. The I&C represent the current plant state. In general they do not record nor convey their previous states. Historical information, in the form of trend lines, is available from select chart recorders about the control boards or from the plant process computer, to the extent the indicators are trended. Space limitations and cost created the dearth of chart recorders, with the few available dedicated to critical components. Similar to the paper-based procedures, the operators must integrate the dispersed historical data and any handwritten notes with the array of I&C spread throughout the control boards.

What strategies can the nuclear power industry employ to combat these limitations and reduce the likelihood of costly plant shutdowns? A seemingly desirable option is providing the operators with additional training focused on rapid upset shutdown avoidance. However, providing additional training proves fruitless given the operators are already highly trained. Perhaps, no training can effectively overcome the human mental limitations and time sensitivity facing an operator during these rapid plant upsets. Additionally, increasing training requirements to cover new types of scenarios, such as severe accidents, may paradoxically serve to decrease operator familiarity with more common upset conditions and core plant functions. The time available for training is finite, and it is necessary to optimize that training to best serve the day-to-day needs of the plant.

The work of one of the fathers of the human factors field, Alphonse Chapanis, provides strong evidence supporting this notion. During World War II, an unusual number of B-17 aircraft pilots confused the flaps and landing gear levers while approaching runways for landing. Landing required pilots to extend the flaps just prior to touch down for the purpose of reducing speed and increasing wing lift. Pilots accidentally manipulated the landing gear lever instead of the flaps, since the two levers were located close together and out of sight behind of the pilots' view. Furthermore, the levers themselves were physically similar in shape. As a result, planes crash-landed without the landing gear extended. Despite extensive additional training efforts, pilots continued to confuse the two levers. Alphonse Chapanis and his colleagues solved the confusion problem by adding a wheel shape to the landing gear lever and a wing

shape to the flaps lever [2]. Modifying the levers, as opposed to additional training, alleviated the lever confusion. Within the nuclear power process control context, a similar approach can be adopted to aid the operators in handling rapid plant upsets and avoiding plant shutdown. This approach entails incorporating automation in the form of a computerized operator support system (COSS).

2 COMPUTERIZED OPERATOR SUPPORT SYSTEM

2.1 Background

Quinn et al. advocate the benefits of automating operator actions for plant upsets [3]. Quinn et al. identified situations in which alternate configurations and actions can mitigate the need for extreme measures, such a plant shutdown, when there is time to do so. These situations are sometimes limited by the ability of the operator to accurately diagnose the cause of the upset and take the needed actions in the short available time. Any delays in procedure-based manual control actions can possibly result in the protection setpoints being reached, leading to an automatic reactor trip or other safety system actuation. Even when the operator is successful in arresting a plant upset and averting the need for safety actions, the time required may negatively impact plant operations.

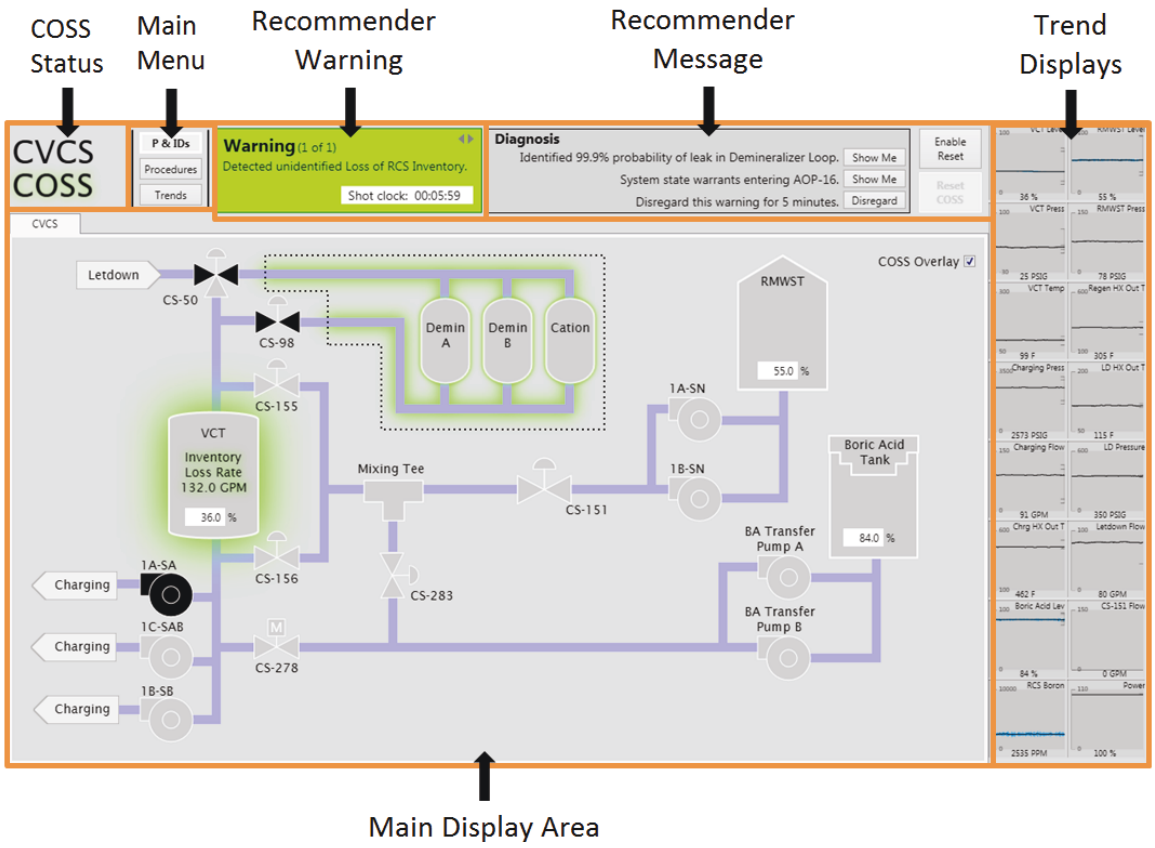
Automation, specifically in the form of COSS development, has been underway in a number of safety-critical applications and has gained widespread acceptance in certain fields, particularly aviation. Traffic Collision Avoidance Systems (TCAS) initially provided pilots with information regarding the altitudes and flight paths of other aircraft, but the current version provides both traffic advisories and resolution advisories comprised of course corrections to avoid any pending collisions [4]. An operator advisory system has been implemented at a natural gas plant in Sicily, operated by Isab Energy Company on behalf of ERG Power & Gas. Within the nuclear power field, an advanced COSS was proposed but never implemented for a German power plant [5]. Furthermore, the nuclear industry has recognized the potential value of COSS as evidenced by the International Atomic Energy Agency's report detailing the benefits such a system would imbue on operator performance [6].

2.2 A COSS Prototype for Nuclear Power Applications

A prototype was developed at Idaho National Laboratory (INL) to establish the key components of an effective COSS. This prototype featured an advanced CVCS linked to the Human Systems Simulation Laboratory (HSSL) at INL [7]. The detection, validation, diagnosis, mitigation, monitoring, and recovery features of the COSS are embodied within four underlying elements—the digital alarm system, computer-based procedures, CVCS piping and instrumentation diagram (P&ID) system representation, and a recommender system for mitigation actions. Each of these elements was selected to help fulfill the goals of both synthesizing the disparate indication information into a cohesive representation and providing the operator with automatic diagnostic and mitigation strategies for plant upsets. To create the four underlying elements, the COSS relies on two primary components—PRODIAG and a COSS prototype. PRODIAG, a process diagnosis system developed by Argonne National Laboratory, is the component that detects plant faults and suggests mitigation actions [8]. As depicted in Figure 1, the digital interface for the COSS prototype is the visual component that displays all the relevant information to support the operator in monitoring and making adjustments to the plant in order to handle plant upsets and maintain plant conditions during normal operations.

The COSS provides the operator with intuitive synthesized component and system state representations, plant upset root cause diagnoses and optimized mitigation and solution recommendations to quickly arrest the plant upset. Specifically, the COSS detects plant upset symptoms, validates the symptoms as an actual fault rather than a sensor failure, diagnoses the upset root cause, determines appropriate mitigation actions to counter the plant upset, monitors the symptoms after the execution of the mitigation actions to ensure a plant upset resolution, and finally suggests actions to return the plant to pre-fault conditions. The COSS also provides the operator with automation to eliminate some of the more

Figure 1. Annotated COSS display featuring areas of concern highlighted on the P&ID, a recommender warning and suggested mitigation action messages.



tedious or time-consuming operator tasks. This is achieved with the aid of a mathematical model of the system and diagnostic algorithms to support its automatic functions. An advanced digital interface is used to convey system states, diagnoses, recommended mitigation actions, and automation controls. Though the COSS emphasizes the use of automation to aid the operator, at all times the operator retains full autonomy for all actions in accordance with licensing regulations.

2.2.1 Simulator Environment

The HSSL located at INL is a full-scope, reconfigurable research simulator capable of digitally replicating nearly any nuclear control room. The HSSL features touchscreen glasstop bays linked together to give a full-scale rendition of the front panels of the main control room of nuclear power plants [7]. The COSS prototype is embedded as a picture-in-picture display in one of the simulator bays of the HSSL [9]. Developing the COSS within the context of the HSSL provides a realistic environment for operator studies and enhances the validity of the concept as well as the practical applicability. The COSS itself was developed using Microsoft Visual Studio and Windows Presentation Foundation for creating a library of visual objects for use within the COSS [10].

2.2.2 PRODIAG and CVCS Model

PRODIAG consists of a mathematical model of a typical CVCS. The model was designed to be representative of a generic CVCS plant configuration with typical I&C. In order to be economically feasible, minimizing the amount of new indication is vital, as each additional instrument added to the plant to support PRODIAG functions can entail a potentially costly modification to the existing physical components. Furthermore, any costly license amendments resulting from significant modifications and changes in concept of operations to the CVCS should be avoided. Therefore, the model was designed to mimic a generic CVCS plant configuration and its associated instrumentation with only minor modifications. The CVCS model in the COSS prototype is nominally coupled with the PRODIAG system, which consists of conservation of mass equations that allow PRODIAG to detect deviations in enthalpy within the system, i.e., leaks within the system that result in a loss of mass or heat. The initial prototype represents only a limited implementation of the standalone PRODIAG code to demonstrate how a COSS might take advantage of PRODIAG within a narrow range of example scenarios.

2.2.3 Interface Design

The digital interface consists of a visual representation of all the information contained within the COSS. The interface was designed with a dullscreen philosophy in which the majority of display screen elements use white, black, and shades of grey [11]. Fully saturated colors are reserved to add salience to display screen elements representing critical pieces of information. The interface follows a multi-windowed display format, which includes primary display views for CVCS 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. Each specific display element is discussed in subsequent sections below.

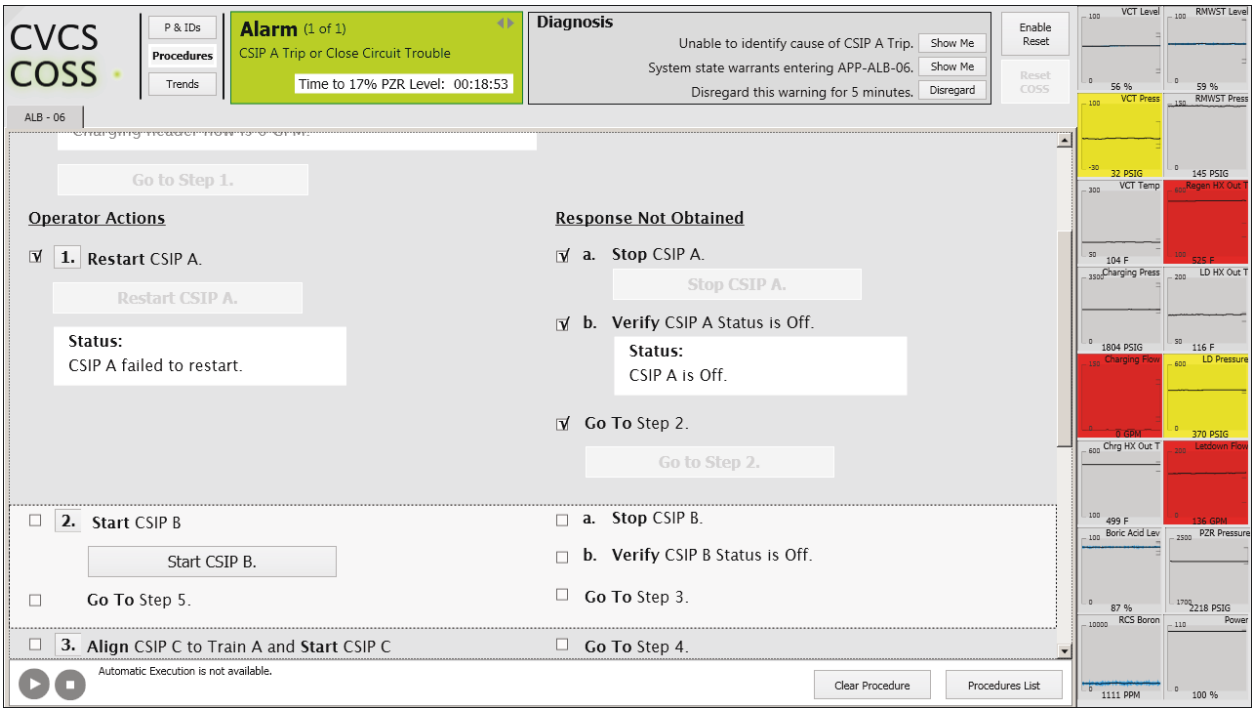
2.2.3.1 Digital Alarm System

The digital alarm system element consists of a warning system and an area dedicated to presenting trend annunciator alarm panels. The warning system displays text messages describing the symptoms of a potential fault detected by PRODIAG. At this point in the process, the symptoms could be due to sensor failure since the COSS has merely detected a trending deviation in the indication for a component. The COSS then performs a validation process to determine if the symptoms triggering the warning are 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. Once the validation has established there is an actual fault, the text warning message is replaced with a more specific message identifying the root cause of the plant upset. Based on the root cause determination, the warning system provides the operator with a shot clock that denotes the amount of time until a critical point is reached that would necessitate a significant operator action, such as a plant trip. 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 strategy, but with less time the operator may opt for a more conservative and safer mitigation action to ensure plant safety and protect plant equipment. The warning and recommendations are illustrated in the top portion of the screen in Figure 2.

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 traditionally separate functions into a synthesized aid for the operator. The trend annunciator alarm panels combine the standard annunciator alarms found in operating nuclear power plants with trend displays. Retaining the standard annunciator alarms is important since an experienced 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 setpoints 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 the alarm presentation concept by including additional alarm levels in conjunction with trend displays overlaid on top of the annunciator tile. The trend line bends from the standard flat line observed during normal operations to a curved line that pops out for the operator against the other trend annunciator alarms without deviating trend lines. As the trend continues to deviate and eventually crosses the warning setpoint, the background of the annunciator panel changes from the dullscreen grey to fully saturated yellow. Once the trend crosses the alarm setpoint, the annunciator panel changes from saturated yellow to red. These alarms are illustrated on the righthand area of the screen in Figure 2.

Figure 2. Computer-based procedures and Trend Alarm.



2.2.3.2 Computer-Based Procedures

The computer-based procedures resemble traditional paper-based procedures found in the main control rooms of Westinghouse pressurized water reactors. The paper-based procedures follow a two-column format. The left column is sequentially followed when desired parameter values are observed via 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 the criteria for proceeding with each step are met. Parameter values that are traditionally scattered across indicators 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 has been shown to reduce 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 prescribed step or column requires additional actions that reduce the chance for operator errors such as proceeding to an incorrect step or column. The computer-based procedures developed for the COSS prototype are illustrated in the main display area in Figure 2. Note that these are considered "Type 3" procedures that provide both embedded indicators and soft controls into the procedure display [12].

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, each separate tab corresponding to a different procedure. Furthermore, the COSS tracks the operator's progress through the procedures, which allows the operator to focus specifically 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 of the traditional setting 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.

Additionally, 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 direct focus to other areas of operation. Maintaining 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 may cue additional procedures or cancel out of a given procedure.

2.2.3.3 Piping and Instrumentation Diagram System Representation

The COSS provides the operators with system diagrams in the form of Piping and Instrumentation Diagram Systems (P&IDs) (see main display area in Figure 1). 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 indications and any controls associated with the component. This manual manipulation of the components within the P&ID view is separate from 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 if needed.

2.2.3.4 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 potential 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, as discussed previously. Additionally, once the root cause is determined, the recommender module will provide information regarding the confidence of determining the root cause in the form of a probability percentage. This critical information alerts the operator to situations in which the diagnostic and prognostic capabilities of the COSS might be limited. For such unexampled events, the operator should exert caution and proceed with a safe but conservative shutdown action.

2.3 Initial Operator Testing and Feedback

A group of four licensed reactor operators was presented with the COSS and walked through each of the features. Each of the operators was allowed to interact with the COSS to familiarize themselves with the different features. After interacting with the COSS, the operators were prompted to provide feedback. Overall, the operators reported a positive reaction to the COSS, both in terms of the design of the interface and the feature set available to the operators. This positive reaction to the COSS, though preliminary, is very promising, since the COSS concept is quite new and will require user acceptance and buy-in before it could be adopted or implemented across the U.S. fleet of nuclear power stations.

3 NEXT STEPS

3.1 Additional Feature Set for COSS 2.0

A number of features will be tested in future iterations of the COSS prototype, but there are two main concepts that will be focused on during the next phase of development. These two advanced concepts are: (1) task-based context support and (2) integrated fault mitigation support combining mitigation strategies into a single optimized sequence.

The context support feature is an extension of some of the current COSS goals. One of the main objectives of the COSS as an operator aid is to provide useful contextual information concerning a particular fault. The context is invaluable to support the operator in diagnosing the fault and determining the most appropriate actions for a complex system with a high amount of interrelated components. In the current COSS prototype, the operator can quickly access contextual information via navigation to the P&ID view. The P&ID view displays the faulted component, which is highlighted to attract the operator's attention. The P&ID view provides the operator with system schematic-based diagrams depicting the faulted component and surrounding interconnected components that may be affected by the fault. A task-based context support system extends beyond providing an additional view of contextual information, by intelligently extracting and displaying relevant portions of the P&ID within the computer-based procedure view. Presenting relevant subsections of the P&ID view within the procedure steps eliminates the need for navigating to another view and holding the pertinent information in memory for comparison against information contained within a separate view. In addition to displaying a subsection of the P&ID, the task-based context support system will also display pertinent parameters for components or processes that might be needed as context for a procedure step. These additional parameters include automatically displaying technical specifications not traditionally included with the procedures as well as some process specific guides, such as curve books the operators must reference independently of the procedures in the current plant configuration.

The integrated fault mitigation support feature is envisioned to handle situations in which multiple faults occur simultaneously or near simultaneously. In the current version, the COSS prototype handles multiple faults by prioritizing the faults in terms of the time remaining until a critical threshold requiring a reactor trip is reached. The fault with the shortest amount of time is moved to the top position for the operator to address. After the most immediate fault is mitigated, the operator is prompted to take actions to restore the plant to pre-fault conditions, such as adding fluids to a leaking system after the leak has

been isolated. The integrated fault mitigation support moves beyond prioritization and recovery actions by essentially combining the recovery actions with the mitigation actions concurrently. The COSS can accomplish this in three steps: 1) Analysis of concurrent faults or faults affecting multiple components in a cascade effect, 2) Identification of the root causes for the faults, and 3) Integration of the procedure steps required for mitigating each fault into a single sequence of steps. Integrating the necessary mitigation actions into a single sequence of procedures is not simply the combination of the procedures, but rather the relationship between the faulted components. These are analyzed based on the common effects they have within the system to arrive at a mutually beneficial strategy, simultaneously mitigating all aspects of the fault within the system. Developing the software capable of optimizing the mitigation strategy is not trivial and will require extensive modification of the PRODIAG system from its current form in the COSS, but it is a worthwhile goal to strive for in future COSS development.

Further, the presentation format of computer-based procedures is another interesting area to explore in future COSS development. Rather than following the two-column format established with the existing paper-based procedures, a flow chart format of presentation may prove more useful with the digital format. As the computer-based procedures can dynamically change the presentation of steps for a given procedure, the presented format needs only to display information relevant to the state of the plant as it relates to the procedure. As a result, unique display formats can be adopted. Flowcharts are an interesting concept that merits further exploration within the COSS computer-based procedures. The flowchart presentation format fits well with the task-based context support system concept given that the system intelligently displays all relevant components along with the procedure steps. These related components are essentially flowcharts of the interconnectivities between components within a system. Using the P&ID representations of the components and interconnectivities serves as natural structure for organizing the procedure steps in line with ecological information displays [13]. There will be times in which the procedures move the operator to a P&ID view much farther away from the currently viewed components in terms of interconnectivity, but displaying the path of interconnectivities to these distant components serves a vital role of familiarizing new operators with the physical composition of the systems and components in addition to maintaining high levels of situation awareness for skilled operators.

3.2 Extension to Additional Plant Systems

The COSS currently includes the single model of a generic CVCS. In order for the COSS to be an effective aid for operators it needs to be capable of handling a wide array of plant upsets. Including additional systems within PRODIAG is important to expand these capabilities. Due to potential regulatory hurdles working with safety systems, non-safety systems are the most promising candidates for inclusion within future COSS development. These systems have the least impact on safety and potential licensing issues [14]. One system that fits the criteria is the component cooling water system (CCWS). The CCWS dissipates core decay heat from components post-accident and serves as a protective barrier against radioactive release by preventing any leakage of reactor coolant from the primary system to the service water system. The CCWS consists of two redundant parallel trains each with one pump and heat exchanger. A third pump is available as a backup in case the other two pumps fail. The CCWS is capable of dissipating heat by removing heat from the reactor coolant pumps and heat exchangers located along the plants primary reactor coolant system. Other systems of potential interest include the turbine control, feedwater, and steam bypass systems. The COSS framework may also be ideally situated to support grid related activities beyond the main control room and non-nuclear systems in process control.

3.3 Future Operator Testing

The first phase of testing the COSS prototype future iteration entails eliciting operator feedback. Similar to the first usability evaluation, operators will be allowed to explore the interface after a brief demonstration of its features. The operators will be able to interact with the interface and ask any questions to clarify the functionality of its features, navigation schemes, or information presentation.

Afterwards a questionnaire will be provided to the operators to systematically capture their initial impressions of the prototype as well as suggestions for improvement. A general set of questions designed to capture the acceptability of a computerized aid across the nuclear industry will also be included to assess how best to integrate a COSS prototype into an exemplary plant in the future.

A more rigorous second testing phase is planned as well, in which the operators' performance completing specific tasks will be compared to the traditional concept of operations used in existing plants with conventional control boards and procedures. This benchmark testing is made possible with the use of the HSSL to mimic all of the necessary legacy plant panels required for monitoring and manipulating a generic pressurized water reactor [14]. The operators will be presented with plant upset symptoms such as the loss of reactor coolant resulting from the leaking demineralizer flange. The simulator is capable of recording the time of the fault, the time at which each operator action was taken, and the time and parameter value for key plant components of interest to each particular plant upset. Additionally, human observers will capture the dialogue between the crew to form a representation of their situation awareness of the plant as well as track their progress through the paper-based procedures. For the benchmark the operators will be faced with the same plant upset; however, they will be aided by the COSS. The same timing, operator actions, and parameter values will be recorded. The goal of the comparison is to establish any performance differences between the conventional and COSS operations. Additionally, subjective measures like operator preference will be administered to compare operator impressions of the two systems. These measures will help establish the usability, utility, and viability of the COSS designs and determine the extent to which the COSS should be considered for actual deployment in control rooms.

4 CONCLUSIONS

An initial operator aid in the form of a COSS prototype has been proposed and discussed in this paper. The first iteration of the interface design has been presented along with the rationale for such an operator aid. Intelligent operator aids such as the COSS are capable of detecting plant upset symptoms, diagnosing faulted components based on those symptoms, and providing the operator with a mitigation strategy to quickly arrest the problem. In this paper, we have presented the core concepts of the COSS prototype we are developing for use to support reactor operators in main control rooms at nuclear power plants. These elements include the graphical representation of information in the human-machine interface and the underlying detection algorithms to guide response and mitigation to upsets at the plant. We have presented the results of the first phase of development and outlined additional steps that will be taken to refine the design of the COSS and enhance its functionality across control room operations. It must be noted that the creation of a prototype is only the starting point toward actual deployment at plants. This research does not presume that the features of the COSS are within the current licensing basis of the plants. Rather, the purpose of this research is to explore features that could aid the reliable and safe operation of plants, but with the additional research and validation necessary to establish both the technical and licensing basis for a COSS in current control rooms.

5 ACKNOWLEDGMENTS

This work was supported by a grant from the U.S. Department of Energy's Nuclear Energy Enabling Technologies program on Advanced Sensors and Instrumentation. The authors acknowledge co-recipient, Dr. Richard Vilim, of Argonne National Laboratory. This paper focuses on the interface aspects of the COSS prototype, although future papers will more closely couple the interface with Dr. Vilim's PRODIAG system.

represents that its use would not infringe privately-owned rights. Idaho National Laboratory is a multi-program laboratory operated by Battelle Energy Alliance LLC, for the United States Department of Energy under Contract DE-AC07-05ID14517.

6 REFERENCES

1. T. Ulrich, R. Boring, W. Phoenix, E. DeHority, T. Whiting, J. Morrell, R. Backstrom, *Applying Human Factors Evaluation and Design Guidance to a Nuclear Power Plant Digital Control System, INL/EXT-12-26797*, Idaho National Laboratory, Idaho Falls (2012).
2. N. Joyce, "Alphonse Chapanis: Pioneer in the Application of Psychology to Engineering Design," *Association for Psychological Science* (2013).
3. T. Quinn, R. Bockhorst, C. Peterson, G. Swindlehurst, *Design to Achieve Fault Tolerance and Resilience, INL/EXT-12-27205,* Idaho National Laboratory, Idaho Falls (2012).
4. U.S. Department of Transportation, *Introduction to TCAS II, Version 7.1*, Federal Aviation Administration, Washington, DC (2011).
5. W.E. Büttner, "Advanced Computerized Operator Support Systems in the FRG," *IAEA Bulletin, Autumn* (1985).
6. International Atomic Energy Agency, *Development and Implementation of Computerized Operator Support Systems in Nuclear Installations*, Vienna (1994).
7. R. Boring, V. Agarwal, K. Fitzgerald, J. Hugo, B. Hallbert, *Digital Full-Scope Simulation of a Conventional Nuclear Power Plant Control Room, Phase 2: Installation of a Reconfigurable Simulator to Support Nuclear Plant Sustainability, INL/EXT-13*-28432, Idaho National Laboratory, Idaho Falls (2013).
8. R.B. Villim, Y.S. Park, A. Heifetz, W. Pu, S. Passerini, A. Grelle, "Monitoring and Diagnosis of System Faults," Nuclear Engineering International, November, pp. 24-27 (2013).
9. K. Thomas, R. Boring, R. Lew, T. Ulrich, R. Vilim, *A Computerized Operator Support System Prototype, INL/EXT-13-29651*, Idaho National Laboratory, Idaho Falls (2013).
10. R. Lew, R.L. Boring, T.A. Ulrich, "A prototyping environment for research on human-machine interfaces in process control," *Proceedings of the International Symposium on Resilient Control Systems (Resilience Week)*, Denver (2014).
11. H. Haukenes, Ø. Veland, L.Å. Seim, N.T. Førdestrømmen, "Petro-HAMMLAB display: Design-design rationale, experiences," Paper C2.16, *Proceedings of the Enlarged Halden Program Group Meeting*, Lillehammer (2001).
12. IEEE Standards Association, *IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilties, IEEE Std 1786-2011,* New York (2011).
13. K.J. Vicente, "Ecological interface design: Progress and challenges," *Human Factors,* **44**, pp. 62-78 (2002).
14. R. Boring, J. Joe, *Baseline Human Factors and Ergonomics in Support of Control Room Modernization at Nuclear Power Plants, INL/EXT-14-33223,* Idaho National Laboratory, Idaho Falls (2014).