COMPUTERIZED OPERATOR SUPPORT SYSTEM AND HUMAN PERFORMANCE IN THE CONTROL ROOM

R. Vilim and A. Grelle
Argonne National Laboratory
9700 S. Cass Ave.
Argonne, IL 60439
rvilim@anl.gov ; agrelle@anl.gov

R. Lew and T. Ulrich
University of Idaho
709 S Deakin St, Moscow, ID
rogerlew@uidaho.edu ; ulrich@uidaho.edu

R. Boring and K. Thomas
Idaho National Laboratory
2525 Fremont Ave.
Idaho Falls, Idaho 83402
ronald.boring@inl.gov ; kenneth.thomas@inl.gov

ABSTRACT

An operator aid technology to assist nuclear plant operators maintain situation awareness and detect faults earlier than would be possible using conventional control room technologies is described. Coined the Computerized Operator Support System (COSS), this technology is aimed at the human-machine interface. The COSS has been implemented as a prototype system operating in the control room environment of a full-scale simulator for a commercial nuclear power plant. A human factors assessment that involved two licensed reactor crews was performed to evaluate crew performance. This paper describes the development of the COSS, the underlying fault-detection architecture, and feedback received based on operator-in-the-loop studies.

1 INTRODUCTION

Argonne National Laboratory (ANL) and Idaho National Laboratory (INL) are jointly developing and evaluating operator aids to: (i) facilitate more timely response to plant faults and grid disturbances; (ii) achieve better management of plant upsets and improved operator performance; and (iii) ultimately improve plant safety, production, and cost management. Under this collaboration ANL has developed sensor validation and equipment fault diagnosis methods. INL has addressed the human factors aspects of assisting operators in monitoring overall plant performance and in making timely, informed decisions on appropriate control actions for the plant condition. Integration of these technologies has taken place under the concept of an *operator advisory system*. This is a software entity whose purpose is to manage and distill the enormous amount of information an operator must process to understand the plant state, particularly in off-normal situations, and how the state trajectory will unfold in time. It consists of 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.

This paper describes the prototypic Computerized Operator Support System (COSS) that has been developed and the results of tests that have included human performance assessments with nuclear plant operators working in a full-scale simulator environment.

2 PLANT PERFORMANCE AND THE OPERATOR

A commercial nuclear power plant must operate safely, reliably, and with high efficiency and availability while meeting the production demands of a central power grid. These performance goals can, however, be challenged by events external to the plant (such as grid disturbances) or internal faults (such as component degradation, component failure, and operator error). Successful recovery from these events before they result in a protection system trip (and, hence, furthering the above goals) requires the operator to correctly identify the fault and to take the correct control action all in a timely manner.

The operator is presently, however, charged with taking a symptom-based approach with the goal of stabilizing the reactor, regardless of the cause of an upset. The operator is not expected to diagnose the identity of the fault that led to the upset. This is with good reason, as the task of scanning many instruments and alarms and then correlating the trends among sensor readings to deduce the identity of the fault is a challenge. In practice the process of diagnosing a fault and following this with adherence to the corresponding paper-based procedure to recover from the fault is time-consuming and prone to error.

3 OPERATOR ADVISORY SYSTEM

Plant performance improvements may be achievable through the use of operator aids and advanced control algorithms that address plant and grid upset events that presently result in transients that can challenge the protection system. There are safety and economic advantages to reducing the probability that an upset will lead to an unplanned shutdown. For faults internal to the plant and grid events external to the plant, computer-aided equipment realignment has the potential to stabilize the plant with greater reliability and precision than is the current case.

3.1 As a Performance Aid

An operator advisory system is a means to manage the enormous amount of information an operator must process and integrate to arrive at an understanding of how the plant is operating in an off-normal situation and how its trajectory will unfold. This is a daunting task for even the most experienced operators. This system would assist the human operator with control as opposed to serving as an extension of the control system. Existing automatic control systems lack “awareness” of the plant state and the larger world in which they operate; they simply track a setpoint.

When quantitatively based, such a system has the potential to provide more accurate and timely diagnosis of component faults compared to an operator who is limited to primarily qualitative reasoning. This is important, because the longer a transient persists, the greater the degree the plant is subjected to off-normal conditions and the more of a challenge it is to arrest the plant excursion and return to within normal operating parameters. Application of such a system could minimize the impact of faults on the plant by improving human performance through timely application of appropriate mitigating actions in response to a fault. This would make it possible to manage many plant transients without incurring reactor trips and plant protection actuation, for which recovery is difficult, prolonged, and costly.

3.2 Analysis Capabilities

The operator advisory system is premised on a sequence of steps for remediation and resolution of an upset event: sensor validation, fault detection and diagnosis, mitigation, monitoring (for successful mitigation), and recovery (to pre-fault plant conditions). Each of these steps is summarized below.

Sensor Validation - Reliable and trustworthy measurements require sensor outputs be validated, i.e., tested for correctness, while failing sensors must be identified. Current industry practice largely leaves the validation of sensor readings to the operator. Validation is a challenge for the operator, as it requires scanning hundreds of sensor readings and correlating these with his mental model for the underlying physical processes. The sensor validation technology described in [1] addresses the shortcomings of existing methods.

Fault Detection and Diagnosis – As described above, an operator advisory system assists the operator in formulating a diagnosis-based rather than symptom-based response to an upset. An equipment diagnosis is provided that is consistent with sensor readings and the underlying physics of the faulted plant.

Mitigation - Fault mitigation is achieved by matching the fault to a table of validated mitigation strategies. In turn, these strategies are cross-referenced to procedures that direct the control room operators to take the needed actions to mitigate the fault. These are the same procedures that would be used in a manual mode if the advisory system was not operative. However, with the advisory system the benefit to the operator is the assistance in matching the diagnosed fault to the correct procedure and having the procedure automatically displayed on the operator's console. The operator must independently verify that the right procedure has been referenced.

Monitoring – The operator advisory system continues in a monitoring mode throughout the event. Once the applicable procedure sections have been completed, the system will determine whether they have been effective and whether plant conditions have stabilized, depending on the nature of the fault. This information will include actual values of relevant plant parameters along with short-term trend lines. This information will be reported to the operator display in real-time.

Recovery - The advisory system will assist in the recovery from the event. This will include providing a list of related off-normal plant parameters affected by the event and displaying their current values, their pre-fault values, and their target values for current operations. The system will provide a list of plant procedures needed to return the plant to conditions where plant parameters are restored.

3.3 Human Factors Aspects

The operator advisory system will function in the control room environment, a setting where human factors considerations are paramount. So, in an application such as this where the human-machine interface is central to human performance, human factors design analyses are essential. In particular, application of human factors principles can result in improved design for the flow of activities in the control room, presentation of information to operators, and workflow of the operators.

4 UPSET SCENARIOS AND IMPLICATIONS

An advisory operator system must account for certain elements if it is to be capable of reliably identifying the cause of an upset condition.

4.1 Sensing Degraded Operation

An equipment fault involves a redirection of mass, energy, and momentum (MEM) as a consequence of a physical change in the system from its normal state. In general then to diagnose a fault, a reasoning process is needed that can relate observed changes in process variables due to redirection of MEM back to the physical change in the system that corresponds to the fault.

4.2 Performing a Diagnosis

A fault diagnosis capability should address important aspects listed below.

- The conservation laws and sensor readings constitute pertinent information that can aid in the inference of the identity of a fault. That is, the ultimate diagnosis must be consistent with these sensor readings and the underlying physics of the faulted plant. So in principle it cannot return a "wrong" answer.
- The reasoning process should not be dependent on furnishing a list of candidate faults *a priori* to be processed by elimination. That is, the engine should have reasoning powers that allow it to deal with unforeseen faults, i.e., those that might be inadvertently neglected from a pre-prepared list of possible faults.
- The reasoning engine should be structured so that the plant specific input that must be provided to the algorithm is limited to process instrumentation diagram information. That is, the reasoning rules and their processing should be formulated in a way that does not require a custom redesign of the fault diagnosis system for each new plant.
- The conservation laws should be formulated in a way that avoids parametric-type models. That is, the method should be free of the need for providing engineering parameter (such as heat transfer coefficients, friction factors, etc.) values. Such parameters are process-dependent and so with their inclusion the generality sought would be lost.
- The diagnostic capability should be able to work at the system level rather than being limited to the component level. That is, a single diagnostic capability operates on a system that is an agglomeration of individual components.
- The capability should be capable of ready realignment or adaptation as life cycle changes occur or as equipment is realigned.
- The diagnostic result and the reasoning process used to arrive at it should be "explainable".

A means for accomplishing the above is described in [2]. The process described there takes as input-data the sensed process variables and uses the conservation laws that govern plant operation to determine through a reasoning process a mutually consistent faulted plant state. The reasoning process is transparent and familiar to the operator as it is very nearly the same qualitative reasoning process by which he would make a fault diagnosis given sufficient time and access to instrument readings. The system can then recommend to an operator the actions that can mitigate undesirable plant events and trends and return the plant to a safe operating condition with the least amount of upset possible.

Implementing this reasoning process in a machine to serve as an aid to the operator has potential advantages. The machine is not subject to the limitations of an operator whose vigilance performance declines with time or who can become distracted. There is fundamentally no limit to the workload the machine can handle. The machine can reason quantitatively to evaluate trends versus the less precise and more limited quantitative reasoning an operator is capable of. The machine offers the potential for a timelier, more sensitive, and more reliable diagnosis of equipment faults.

4.3 Important Dependencies

The spatial localization to which a fault can be resolved is a function of the number, types, and locations of the sensors in a system. A thermo-fluid system with pressure, temperature, and flow measured at the outlet of each component will allow for a fault diagnosis down to the component level. So the richness of the sensor set must be considered if a specific fault diagnosis capability is required for a system.

The sensitivity of fault diagnoses is a function of the uncertainty in sensor measurements. Real world measurements are affected by imprecision that is not generally present in simulations or in some training environments. Uncertainty in the measurement is a factor affecting the quality of a fault diagnosis, particularly for utility applications. Accounting for, assessing, and quantifying measurement uncertainty are important steps for qualifying the accuracy of a diagnosis.

Fault diagnosis methods that use plant data from normal operation as a baseline for comparison during subsequent operation require special consideration following equipment realignment. Realignment alters the physics of the plant and hence requires relearning the plant physics through the measurements. Hence, the components, sensors, and flow paths need to be appropriately updated to reflect the new configuration and measurement data re-taken to reflect current operation.

5 COMPUTERIZED OPERATOR SUPPORT SYSTEM

A prototypic operator advisory system that we refer to as the Computerized Operator Support System (COSS) has been developed and possesses all the attractive features identified above. This instantiation of an advisory system provides operators with the capability to see, feel, and hear how a digital human-machine interface (HMI) will respond in real-time. Real-time operation and feedback are essential to understanding and evaluating nuances in how the HMI conveys information. The development environment used for COSS provides a tremendous amount of flexibility in the number of interaction schemes and information presentation modes for study. Human performance studies with the COSS provide valuable feedback and are part of the process under which it is taking shape.

5.1 Target System

In this work, the study of human factors issues is facilitated by the selection of the Chemical and Volume Control System (CVCS) of a pressurized water reactor (PWR) as a representative system involving operator interaction in the control room. This system with its functions and operating requirements provides a target for study and refinement of the human factors that affect how the operator performs in the human-machine interface. The CVCS is a standard PWR system and provides the following high level functions:

- Maintenance of programmed water level in the pressurized reactor coolant system;
- Maintenance of seal-water injection flow to the reactor coolant pumps;
- Control of reactor coolant water chemistry conditions, activity level, soluble chemical neutron absorber concentration, and makeup;
- Emergency core cooling;
- Provide means for filling, draining, and pressure testing of the reactor coolant system.

A generic high-level piping and instrument diagram (P&ID) for the CVCS is shown in Figure 1.

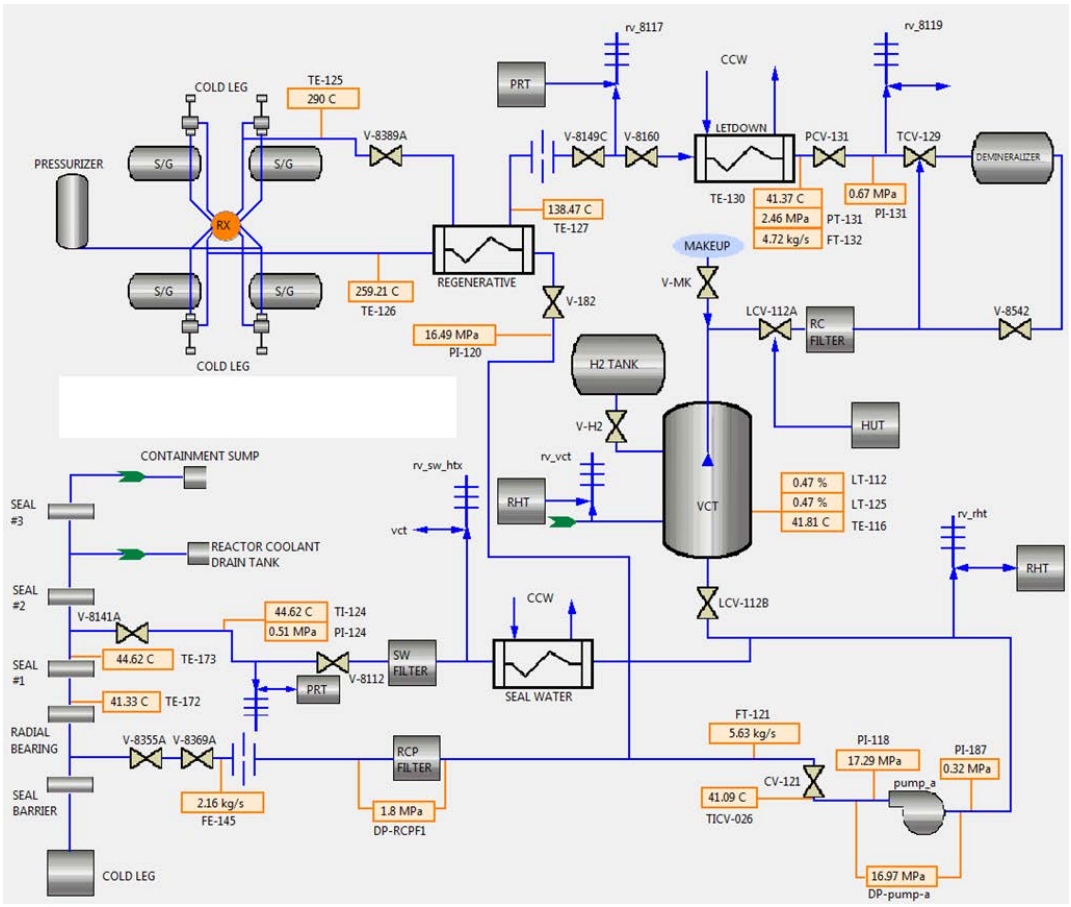

Figure 1. Representative Piping and Instrumentation Diagram for Chemical and Volume Control System

5.2 Fault Diagnosis

The fault detection and diagnosis capability implemented in the COSS is the Parameter-Free Reasoning Operator for Automated Identification and Diagnosis (PRO-AID) method and software developed at ANL.[2] PRO-AID takes data from plant sensors sampled periodically and compares trends against the steady-state condition to determine if an anomaly exists. PRO-AID is capable of diagnosing equipment faults, such as leaks and blockages, in thermal-fluid systems from the sensor data.

If an anomaly is detected, the software attempts to identify the cause through a reasoning process that involves conservation balances that relate faults to sensor trends in combination with knowledge of how plant components are connected. The spatial localization of the diagnosis is dependent on the richness of the available sensors.

One of the unique features of PRO-AID is that it only requires defining the system at the P&ID level. The PRO-AID system then trains from steady state data to be able to recognize faults.

The performance of PRO-AID has been characterized through standalone tests. Surrogate plant data was generated by introducing equipment faults into a simulation of the CVCS. The quality of the PRO-

AID diagnosis was examined as a function of the number and types of sensors, size of the fault, and magnitude of process noise.

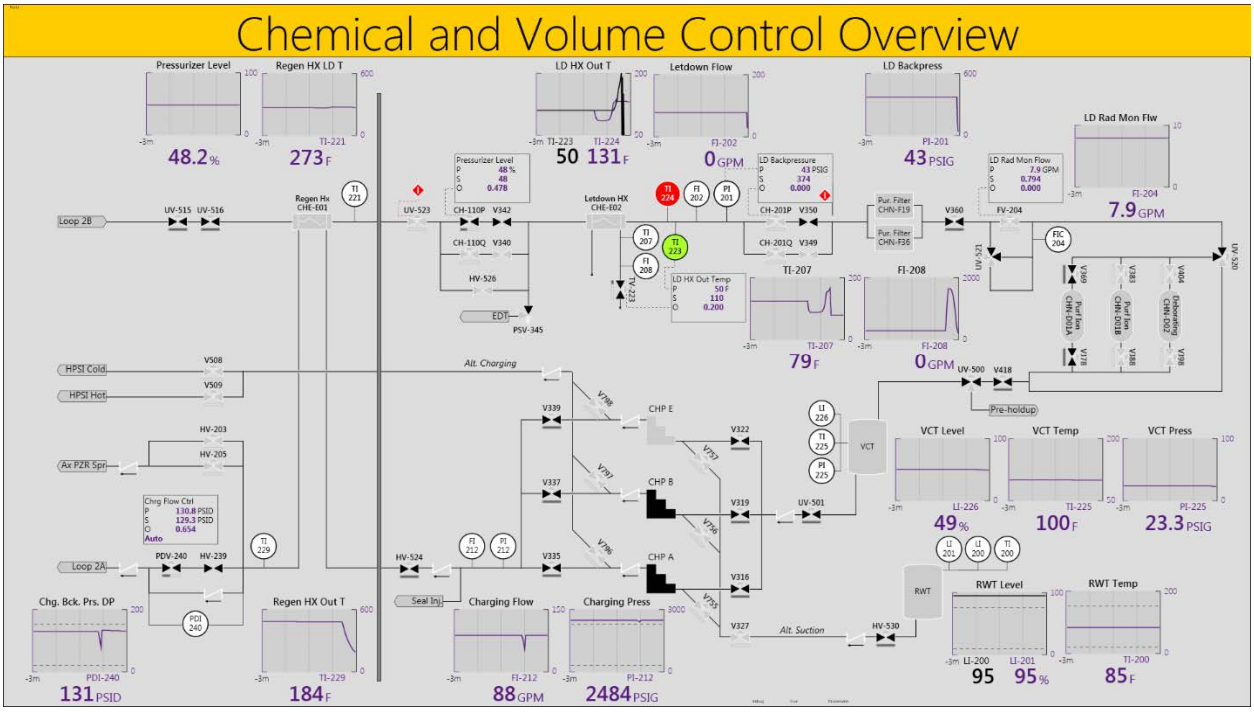

Figure 2. CVCS Large Overview Display

5.3 Features

The COSS is comprised of several digital HMI displays and screens hierarchically organized. The physical layout is comprised of two large overview displays and four smaller touch-enabled HMI displays. The left overview is for monitoring CVCS (see Figure 2). It is intended for monitoring during normal operations and conveys letdown and charging status information. The display is also aimed at supporting abnormal operations by providing visual annunciators and the status of safety injection systems. All the HMI screens were implemented in a style known as dullscreen. With the dullscreen concept, the screens appear monochromatic when the annunciators and instruments are within normal operating ranges, allowing high-contrast and salient color indications to grab the operators attention should something unexpected or noteworthy happen.

Fault detections from PRO-AID are conveyed to operators through the HMI screens using a highly salient and distinct yellow-green color. The CVCS overview is organized as a P&ID to support conveying fault diagnostics from PRO-AID. The fault diagnostics require highlighting sections of piping and components to show operators the location of a detected fault. The fault findings provide fault specific guidance to the operator, allowing mitigating actions to be performed before needing to follow procedure paths that might require taking the plant offline.

6 OPERATOR TRIALS

The prototypic COSS underwent a first evaluation workshop conducted with licensed operators from a partner plant. The workshop provided an opportunity to allow operators to interact with the COSS prototype in real-time. Implementing the COSS for the partner plant not only meant that operators would

be familiar with the system, but it also allowed comparisons to be made between hybrid digital/analog control boards and the traditional boards. An operator-in-the-loop workshop [3] examined variations of COSS where: the control room supervisor (CRS) used the COSS at their desk, and the reactor operators (ROs) had a duplicated COSS at the boards; and a second variation where the ROs used the COSS from the board and the CRS provided oversight from their desk.

The operators were tasked with diagnosing the fault and mitigating any issues. The operators performed the scenario using the traditional analog board layout and a COSS integrated layout. First the operators used the traditional board layout in order to benchmark their performance. The operators also used the COSS interface displayed within the CVCS board. A number of different measures were collected during each scenario completion. Simulator logs, eye tracking, and audio logs were taken in real time while the operators completed the scenario. Following the scenario, the operators completed a series of subjective questionnaires.

In this workshop evaluation, the live link between the PRO-AID fault diagnostics and the simulator data stream was disabled. In its place an offline batch fault diagnosis session was conducted using time series data exported from the simulator. The fault diagnostics and temporal dynamics produced by PRO-AID were then played back to the COSS prototype as if it had an underlying real-time prognostic diagnosis session in place.

Some of the findings of the operator trials are described below.

6.1 Overview Display

The overview provided by the COSS depicts the prominent components of the CVCS. The operators reported a favorable impression of the overview, but did note several issues. Specifically, the operators noted an issue with the level of abstraction portrayed within the overview of the CVCS. The overview was quite detailed and included too much information at a detailed level for it to be an effective visual aid when viewed at greater distances. The reactor operator working at the board was able to discern the specific values, i.e., valve positions, but the senior reactor operator could not discern any of these values. The operators requested that the overview screen contain fewer components and display these fewer components larger so that it could be used as a visual aid from farther away from the control board. This issue stems from a competing design goal based on the type of concept of operations adopted by the plant. Ultimately, the COSS should be designed for use at operator workstations in which the viewing distance is appropriate for an overview with this level of detail. Since the plant evaluating the COSS requires intermediate stages in which the control boards will still be a central component of the control room, overviews for the COSS must be designed to accommodate larger viewing distances.

6.2 Color

The use of color or rather the lack of color was raised as a potential issue for the overview as well as several of the other COSS screens. A dullscreen philosophy was adopted for the COSS. This dullscreen philosophy aims to reduce the use of color in order to reserve color to convey important information [4]. As the amount of color included with the interface increases, the saliency of any given color typically diminishes and reduces the effectiveness of color to draw attention. The COSS reserves color for indicating alarm states and highlighting issues detected by the prognostic system. In order to reduce color, valve positions are indicated with white and grey to denote open and closed states, respectively. The operators reported the visibility of the valve positions and had difficulty discerning the open and closed positions. A black and grey scheme was also evaluated with the operators reporting this was more salient than the white and grey since the black contrasted the grey background better than the white. Even with

the more salient dullscreen black and grey valve depiction, the operators expressed concern about their visibility in particular when glancing over at the display to quickly assess any changes in the CVCS state.

6.3 Hierarchical System Representations

The overview screen for the CVCS was densely populated with indication and controls following an information rich display philosophy. The information rich display attempts to provide a large amount of information in a small amount of space. Though this may be appropriate for some displays, the operators expressed concern that the overview displays appeared cluttered. The density of the display reduced the visibility of the overview display as distance increased. The operators suggested a reduced number of components be selected for the overview.

The level of detail to include in overviews and system mimic displays was discussed with the operators for both COSS overview displays and smaller control displays. The feedback from the operators indicated that they preferred having high level system representations consisting of only the critical components on the overview displays. The overview displays were viewed as providing a holistic plant view for rapid status acquisition by the operators. In contrast, the control displays should contain more detailed system depictions. The COSS overview and control screens were deemed more similar to the control display level of detail, which is also related to why the operators expressed concerns for the high density and information rich overview display.

6.4 Reliability and Trust

A critical insight provided by the operators reiterated the importance that trust plays when introducing new forms of automation into a process. Several strategies can be employed to bolster accurate operator trust in the COSS. First, the COSS diagnostics should be configured to reflect the actual diagnostic capabilities it possesses. False alarms should be minimized to prevent the operators from discounting the warning messages as nuisance alarms. Since the COSS is an advisory system, it should not add to the operator's workload by requiring him to unduly disregard its warning messages. Excessive false alarms within the COSS can lead to the "one-armed operator" problem currently facing operating crews in which one operator must stand tethered to the silence-alarm button, since the alarm continues to sound though the information associated with the alarm has already been acknowledged and provides no additional operational value. Second, the diagnosis should be clearly conveyed to the operator, such that he or she can infer the underlying rationale for the diagnosis and the contributing components. This is achieved both through warning message text consisting of clear and plain explanations of component names and states that contribute to the issue. Additionally, the system representation and highlighting helps convey the underlying components for a fault and allows operators to rapidly gain the context of the surrounding system to assess the validity of the diagnosis. The operators reported positive impressions of the COSS implementation that highlights the fault related components and commented on the necessity of this information in relation to operator trust.

6.5 Crew Coordination

Computer-based procedures guided the operators as the scenario progressed. As a result, the operators spent the majority of their time in front of the COSS interface. This proved quite different from the current concept of operations in which the operators move around the control board and relay information back to the senior reactor operator through three-way communication. The operators used the physical movement time required to move from one board location to another to communicate the information they obtained from the last board location. Without this movement, the operators had to build time into their completion of the procedures to relate information, which is something that they were unaccustomed to doing. One operator reported that he was concerned about a keyhole effect in which they

become too focused on the COSS interface and fail to notice an event occurring somewhere else in the control room. Though this is a potential issue, it is unlikely to lead to any significant problems since the system provides automatic detection and warning which then redirects the operators' attention to the necessary information.

7 CONCLUSIONS

The information obtained from the evaluation using a representative nuclear power plant will be incorporated into the CVCS-COSS and evaluated with licensed crews. Additional work is required to continue the COSS development to make it available for nuclear industry use. The PRO-AID system will continue to undergo testing for additional systems and in so doing characterize how plant configuration of the sensors and components affects the quality fault diagnosis in terms of sensitivity and spatial localization.

Adding a second or more industry collaborators is important. Additional utility collaborators will help garner industry attention and buy-in. The COSS technology represents a substantial shift from the current concept of operations at existing plants and will require some license amendments. Given the regulatory environment, it is crucial to gain industry buy-in in order to identify champions that will help shape the regulatory process so that other plants can follow suite and realize the benefits of a COSS system.

8 REFERENCES

1. R.B. Vilim and A.M. Heifetz, "Advancing On-Line Monitoring Capabilities for Sensor Validation and Estimation," *Proceedings of ICAPP 2014*, Charlotte, NC, April 6-9, 2014.
2. R.B. Vilim, Y.S. Park, and A. Grelle, "Parameter-Free Conservation-Based Equipment Fault Diagnosis," 9th International Conference on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies, Charlotte, NC, February 23-26, 2015.
3. R. Lew, T.A. Ulrich, and R.L. Boring, "Nuclear Reactor Crew Evaluation of a Computerized Operator Support System HMI for Chemical and Volume Control System," Human-Computer Interaction International Conference, Vancouver, BC, Canada, July 9-14, 2017.
4. H. Haukenes, O. Veland, L. A. Seim, and N. T. Førdestrømmen, "Petro-Hammlab Overview Displays: Design-Design Rationale-Experiences," *Enhanced Halden Programme Group (EHPG) at Lillehammer*, 2001.

ACKNOWLEDGEMENTS

The submitted manuscript has been created by U Chicago Argonne, LLC, Operator of Argonne National Laboratory ("Argonne"). Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE- C02-06CH11357. This work was supported by the U.S. Department of Energy, Office of Nuclear Energy, under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.