INL/CON-14-32560
PREPRINT

The Initial Development of a Computerized Operator Support System

Resilience Week 2014

Roger Lew, Ronald L. Boring, Thomas A. Ulrich, Ken Thomas

August 2014

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

The Initial Development of a Computerized Operator Support System

Roger Lew, Ronald L. Boring,Thomas A. Ulrich, & Ken Thomas
Human Factors and Statistics
Idaho National Laboratory
Idaho Falls, ID
{roger.lew,ronald.boring,thomas.ulrich,kenneth.thomas}@inl.gov

***Abstract*—A computerized operator support system (COSS) is a collection of resilient software technologies to assist operators in monitoring overall nuclear power plant performance and making timely, informed decisions on appropriate control actions for the projected plant condition. The COSS provides rapid assessments, computations, and recommendations to reduce workload and augment operator judgment and decision-making during fast-moving, complex events. A prototype COSS for a chemical volume control system at a nuclear power plant has been developed in order to demonstrate the concept and provide a test bed for further research. The development process identified four underlying elements necessary for the prototype, which consist of a digital alarm system, computer-based procedures, piping and instrumentation diagram system representations, and a recommender module for mitigation actions. An operational prototype resides at the Idaho National Laboratory (INL) using the U.S. Department of Energy's (DOE) Light Water Reactor Sustainability (LWRS) Human Systems Simulation Laboratory (HSSL). Several human-machine interface (HMI) considerations are identified and incorporated in the prototype during this initial round of development.**

Keywords—human machine interface (HMI), computerized operator support system (COSS), chemical volume control system (CVCS), nuclear power plant (NPP)

I. INTRODUCTION

Automatic control and safety systems in Nuclear power plants (NPPs) ensure plant safety and relieve operators from mundane tasks, but potentially decrease their situational awareness of the plant. Many safety response systems are used when there is insufficient time for operators to diagnose and respond to fast-moving events. The plant operates in an envelope of conditions that are supervised by the plant protection system, in the form of setpoints triggering protective actions automatically if the thresholds are exceeded. These automatic actions are designed to put the plant in a safe and known condition, such as a reactor trip. Other automatic actions are part of the plant control system, and maintain important plant parameters in the desired operating range by making adjustments to plant components such as valve positions and pump speeds to relieve the plant operators from the burden of continuous, tedious manual control of these components. Though these automatic protective functions effectively ensure plant safety and resilience and have a proven safety record, operator performance can be improved to avoid these automatic actions.

Quinn et al. describes the benefits of automating operator actions for plant transients [1]. 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. 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. Any delays in procedure-based manual control actions can possibly result in the protection setpoints being reached, which leads 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 other plant operations.

A computerized operator support system (COSS) is a collection of capabilities to assist operators in monitoring overall plant performance and making timely, informed decisions on appropriate control actions for the projected plant condition, resulting in higher efficiency (less downtime), reduced operating costs (less manpower), and increased system reslience. They generally have the following features: (i) Monitoring a process to detect off-normal conditions; (ii) Diagnosis of plant faults; (iii) Prediction of future plant states; (iv) Recommendation of mitigation alternatives; and (v) Decision support in selecting mitigation actions.

Digital control systems (DCSs) and sophisticated computer algorithms are capable of analyzing, diagnosing, and suggesting mitigations to even the most complex and fast-moving situations. Such systems could assist the operators in achieving a more accurate and timely response to component faults and plant transients. Development of such technology could prove to be enormously beneficial to the currently operating nuclear plants, as well as advanced NPPs that are now being built or proposed. This would result in better management of plant upsets, improved operator performance, and ultimately make a positive impact on the industry's fundamental objectives in the areas of nuclear resilience, production, and cost management.

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 on the altitudes and flight paths of other aircraft, but the current versions provide both traffic advisories and resolution advisories comprised of course corrections to avoid any pending collisions [2].

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 in a German power plant [3]. 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 [4].

This paper proposes a general model for a COSS that addresses the control room operator performance challenges. Further, a prototype COSS has been developed to study and refine the concept, determine the appropriate system objectives and requirements, resolve any human factors engineering issues with the technology, and ultimately validate the COSS concept for commercial product development leading to use in a NPP control room.

II. COSS Conceptual Model

The concept of a COSS in this paper 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 parameter trends.

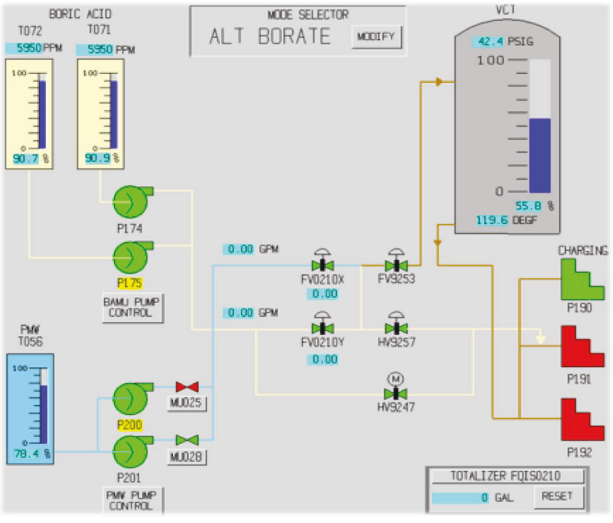

Fig. 1. Current DCS for CVCS from a modernized control room at a nuclear power plant.

The operator is the point of integration of all control room information and relies on what is termed "operator fundamental knowledge" to ensure that the control room is applying the correct procedure for the plant upset. Operators are highly trained in 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, three-way communications, independent verifications, etc. Operators are exceptionally good at performing these tasks, but the high workload and time-pressure associated with certain plant events creates an environment in which the operator may commit errors compounding the original fault and impacting the plant more so than would otherwise have occurred.

The control room crew typically follows the general pattern in reacting to a plant fault as follows:

- *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.

A well designed COSS can assist an operator at each stage of the fault response sequence to reduce workload and confirm important information. In the following sections the COSS prototype design considerations for a chemical volume control system (CVCS) are discussed.

III. COSS Prototype Development

A. Design Philosophy

The CVCS was selected as the system to model for the prototype, because it is modeled in the available Process Diagnosis (PRODIAG) system capable of fault diagnosis [5] and because it is one of the systems successfully integrated with a distributed control system as part of control room modernization [6]. Figure 1 illustrates the DCS for a CVCS at a recently modernized NPP. As can be seen, the DCS incorporates elements of a piping and instrumentation diagram (P&ID) coupled with digital indications and soft controls. Such a DCS improves operator control of the CVCS, and affords some advantages to the operator over its analog antecedents in understanding the dynamic response of the interrelated components. However, the DCS does not explicitly help the operator to diagnose and mitigate upset conditions. The distinct advantage of the various elements of the COSS is that they work together to provide the operator with a comprehensive view of the system and work alongside the operator to evaluate system states.

To realize the benefits of co-equal information sources to the operator, the different parts of the COSS are combined into a single display in the prototype. This display may take

the place of a DCS display, but the functionality, particularly the recommender system, exceeds typical DCS implementations. The recommender system does not perform actions automatically or in lieu of the operator. Rather, it monitors overall plant or system activity and advises the operator on the correct course of action, including the correct procedure path to take. The recommender system augments the computer-based procedure (CBP) by directing the operator to the appropriate procedure based on the fault diagnosis.

B. *Full Scope Simulation Environment*

The COSS prototype is integrated into the U.S. DOE LWRS HSSL located at the INL (see Figure 2). It is displayed as a picture-in-picture embedded on a vertical display of a simulator bay. For details on the HSSL, refer to [7]. 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. However, the loss of resolution and limited space availability on the board to display the COSS served as constraints to the design of the COSS as a DCS.

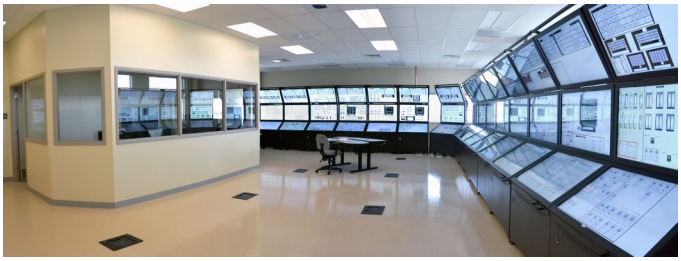

Fig. 2. The Human System Simulation Laboratory.

C. *Software Development Environment*

The Generic Pressurized Water Reactor (gPWR) full-scope nuclear plant simulator was used 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.

D. *Design Process*

A team consisting of three human factors psychologists, one software developer, and a process control expert developed the elements of the COSS. The requirements for each system were discussed initially, and preliminary mockups were sketched, while the functionality of each element and several operator scenarios relevant to CVCS operations were identified and reviewed. Each COSS element was then developed into a software specification, which was prototyped using the Microsoft Windows Presentation Foundation (WPF) and Microsoft Visual Studio. The completed specifications and prototype were carefully reviewed to ensure a consistent iconography, look and feel, color scheme, navigation, and interactivity.

The prototype represents an initial attempt to put key COSS ideas into practice. The design is not yet finalized. Thorough validation against human factors standards, operator testing, usability, and iteration of the various elements of the COSS is yet to be performed. Additionally, other modes of presenting information and controls will be benchmarked against the current design, thereby refining the design for the next version.

IV. COSS PROTOTYPE ELEMENTS

In order to demonstrate the COSS, a functional prototype was developed using a DCS architecture. A COSS is a composite system that features several distinct yet co-equally important elements. For the purposes of the prototype, four separate facets of the COSS were considered:

- *Digital Alarm System*: The COSS includes advanced alarms that are designed to combine the spatial pattern recognition afforded by traditional annunciator boards with supplemental information to help the operator understand the cause of the information. The COSS digital alarm system provides a trend display for key indicators coupled with multistate colored alarms for warning and alarm states. The alarm trend displays also incorporate a mechanism for showing sensor drift or failure.
- *Computer-Based Procedure (CBP) System*: The COSS also includes a CBP system. The CPB closely mimics the paper-based procedures for abnormal and emergency operations, including the common two-column format with a lefthand column for the preferred operator action (i.e., IF-THEN) and a righthand column for response not obtained (i.e., ELSE). The CBP builds on paper-based procedures by providing digital indicators embedded in the procedures and soft controls the operator can activate within the procedures.
- *Piping and Instrumentation Diagram (P&ID)*: The P&ID provides a schematic of key plant components in a system. This display includes visible indicators of key states (e.g., valve position pump energized, or tank level) as well as the actions available to the operator (e.g., open or close valve). The P&ID does not incorporate flow indicators, which are presented as part of the alarm trends.
- *Recommender System:* The heart of what makes the COSS distinct from advanced DCS displays is the recommender system. The recommender system monitors plant states and provides suggestions to the operator to help diagnose problems and take actions. The recommender system monitors multiple sets of sensor data and can provide early warnings of emerging system faults (e.g., rapidly lowering tank level) before an alarm triggers. The recommender system interacts with the digital alarm system, CBP system, and P&ID displays, to direct the operator to relevant information and available actions and procedures.

V. COSS PROTOTYPE

A. *Overview*

The COSS prototype displays CBPs, a CVCS main P&ID based on the CVCS DCS at an existing plant, and trend alarm panels (see Figure 3). The COSS uses a dullscreen display scheme comprised of black, white, and greys for denoting components in normal operating conditions and displaying

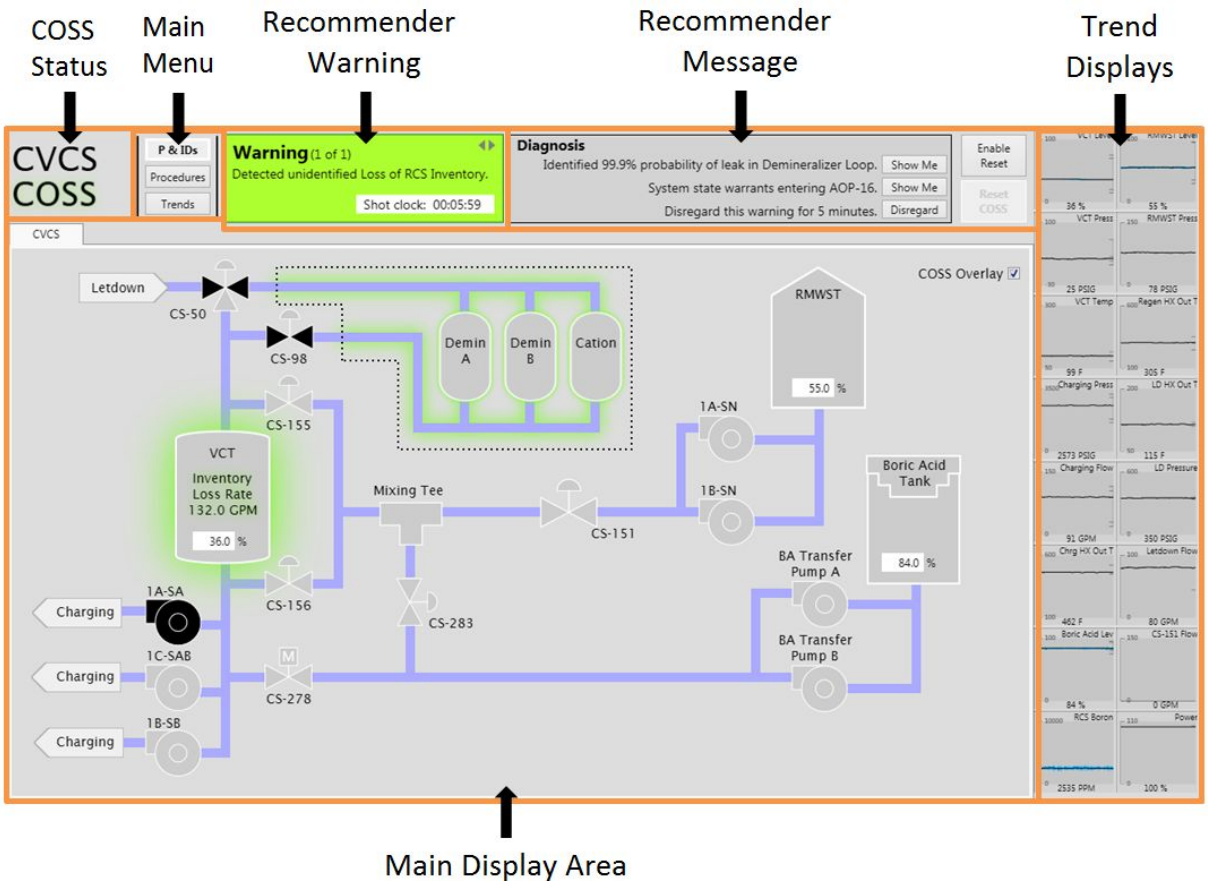

Figure 3. Annotated COSS Display.

CBPs. Dullscreen denotes a display philosophy in which only items requiring operator attention have color, while all remaining items are presented in black, white, or greys [8]. Thus, yellow and red are used judiciously to denote warning and alarm states, respectively. The color blue is used to depict potential sensor failures. The chartreuse (yellow-green) color is used exclusively by the recommender system, both for messages to the operator and for highlighting areas of concern in the P&ID display. Chartreuse was chosen because it is highly salient, similar but perceptually distinct from yellow, and not commonly used in process control interfaces (viz. green has mixed connotations in process control).

B. *Status*

The COSS status indicator (see Figure 3) informs the operators that the COSS is functioning properly. The status indicator consists of a green circle and COSS label highlighting that appears and disappears in a continuous cycle. In the event that the COSS malfunctions, the frozen state of the green circle and COSS label provide immediate feedback that the system has stopped functioning properly.

The main menu in Figure 3 shows available views that can be displayed in the main window area. The COSS can toggle between three views: P&IDs, Procedures, and Trends. The currently selected view is highlighted with a white border for easy identification. Procedures display the currently active procedure, with additional procedures denoted with separate tabs. The Trends button invokes a detailed view of one of the trend alarms normally found on the right of the screen.

C. *Recommender System*

The recommender system (see Figure 3) provides a visual presentation of the detection, validation, diagnosis, and monitoring functions. When the COSS detects a fault, a warning display highlighted with a green background appears in the recommender area. The warning display also contains a description of the trend that triggered the COSS to detect a fault, i.e. “Detected unintended loss of reactor coolant system (RCS) inventory.”

The COSS has a predictive capability that allows it to determine future trends for each component, i.e., it provides the operator with a *shot clock*. The shot clock provides the operator with the predicted amount of time before the fault reaches a safety critical set point requiring a reactor trip or other safety actuation (see Figure 3). This feature allows the operator to diagnose and select between less or more conservative mitigation activities as dictated by the amount of available time.

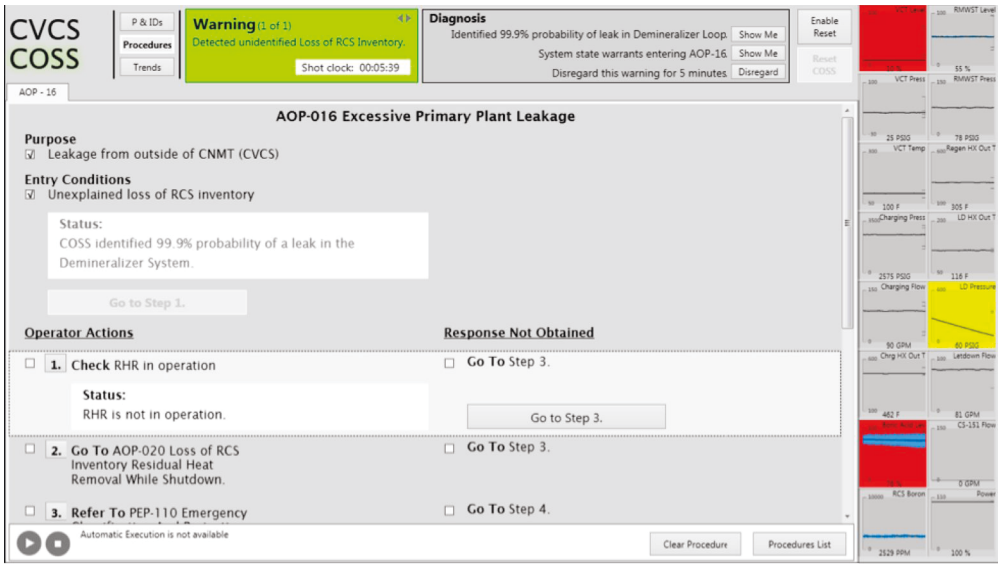

Fig. 4. Computer Based Procedures and Trend Alarms.

After the validation and diagnosis processes are complete, the message section of the recommender system provides a description of the cause of the fault, recommended action descriptions, and "Show Me" buttons that allow the operator to select particular mitigation actions. Selecting "System state warrants entering AOP-016" (see Figure 3) automatically displays the appropriate operating procedure. The operator can navigate back to the P&ID from the CBP from the recommender system or the COSS navigation menu buttons. Selecting "Identified 99.9% probability of leak in Demineralizer Loop" will display the P&ID with relevant areas of concern highlighted in green (Figure 3 and 4). CBPs (see Figure 4) are central to the COSS, since they support the primary interaction method between the operator and the system. The CBPs begin with the purpose and entry conditions as determined from the fault diagnosis. The CBPs resemble traditional paper procedures used throughout NPP operations. The procedures are displayed in a two-column format. The left column contains the operator action steps, and the right column contains the response not obtained steps. Each step in both of the columns contains a box with the information required to complete the action, buttons to navigate to the correct step, and a check box that is automatically checked off when the operator completes the step by selecting the appropriate button. The response not obtained condition has procedure navigation buttons that allow the operator to move to the appropriate step when the desired response was not obtained. A light grey box highlights the current step, and the information boxes and buttons become active as indicated by black borders and text. Previously completed information boxes and buttons are grey to indicate they are no longer updated by the COSS or capable of manipulation by the operator. The current CBP prototype allows both step-by-step execution and automatic execution of sequences of multiple steps. The run and stop buttons (denoted by ▶ and ■, respectively) are used to toggle automatic execution and can be seen along the bottom of Figure 4.

D. *Recommender System*

The trend alarm section of the COSS serves as information rich display [9] containing 16 trend alarms in a panel (see Figure 4). The trend alarms are constantly visible within the COSS to ensure the operator has immediate access to trend and current indicator values for the most critical system components. The 16 trend alarms selected for the COSS interface provide information for CVCS relevant components. The trend alarms serve as salient warning and alarm indicators in situations in which a component's sensor reaches a predetermined set point. Each trend alarm contains a trend line, warning and alarm anchor bars, and the current component value. During normal plant states the trend lines are fairly stable and flat. Deviations away from a straight line across the alarm contrast the rest of the trend line alarms within the panel to alert the operator of a fault. Due to normal plant adjustments, predicted trend deviations do not necessarily indicate an abnormal state. The trend alarms use background color to denote any trend that crossed into a warning or alarm state. The trend alarms are grey while the current value of the trend is within normal operating parameters. When a trend approach a particular set point, the trend alarm panel background turns yellow in warning and eventually red as an alarm state is reached.

VI. Human Factors Evaluation

The COSS is a forward reaching proof of concept prototype intended to help direct future design efforts in NPP control rooms. Additional functionality should be incorporated into the COSS before it would be practical to conduct an extensive human factors evaluation. The increased functionality would include additional P&ID displays to support the presentation of more CVCS components, identifying the types of faults the PRODIAG algorithms can effectively detect, and identifying procedures that can support mitigation actions for these faults. Prior to the implementation of the increased functionality, some aspects of the COSS can be evaluated for aspects of human factors engineering such as

usability and operator performance. For example, the COSS's predictive capabilities provide the operator with more time since the warning system engages the diagnosis process prior to any alarm triggering. With additional time, operator performance should increase. This could be tested for the CVCS demineralizer loop simply by running a few operating crews through the scenario using the gPWR simulator with traditional controls and then with the COSS. Time to complete the mitigation actions, accuracy of the actions, and communication between the crew are variables of interest to compare performance. In addition to a simple performance evaluation, the operators can also provide usability feedback concerning their impression of the interface in terms of the functionality, navigation, and interactions with the soft controls.

Operator feedback would be beneficial for the iterative design and refinement of the COSS in several ways. In terms of usability, the operators can provide feedback concerning the navigation between the different views of the COSS and between different operating procedures to help evaluate and minimize the number of actions required to reach an indicator, soft control, or procedure. The operators can also provide feedback concerning the operation of the soft controls. For example, the operators can identify conservative actions, which do not require a confirmation dialogue box and other actions that should require a dialogue box for confirmation to ensure unintended consequences are avoided. The P&ID presentation could benefit from operator feedback in terms of their impressions of the iconography, inclusion of particular components, and layout. For example, currently the COSS P&ID display does not depict flow between components to minimize screen clutter, but perhaps operators may find that feature useful and the tradeoff between the flow information and screen clutter is worthwhile. There are a number of questions that remain to be answered in terms of the COSS design, but at this early stage of development, the COSS serves as an initial effort in the design for advanced operator aids in NPP control rooms.

VII. Discussion

The prototype represents a software collection of the different elements of the COSS, integrated in a manner that attempts to keep the advantages of the individual elements. The assembly of these elements into the integrated COSS represents initial design decisions. However, it was found that in many cases, the COSS was a first-of-a-kind prototype, and applicable design standards could not be readily referenced. A human factors evaluation can help address unknown aspects of the design to arrive at an effective COSS.

The instrumentation currently installed in operating NPPs may not provide enough information for the COSS to make accurate diagnoses. Affordable, enhanced instrumentation would improve the accuracy of plant diagnoses and could perhaps be cost-justified by the reduction in plant upsets.

The COSS CBP closely follows traditional paper procedures, primarily adding in-line sensor information and soft controls relevant to each step. There are a number of design questions regarding the best way to present in-line information, completed steps, continuous actions steps, and soft controls, as well as the navigation between procedures and the ability of the operator to execute steps out of sequence.

There remain significant opportunities to further enhance the recommender system through its mode of communication with the operator (e.g., addition of verbal alerts), through its diagnostic algorithms (e.g., offering a more sophisticated prognostic abilities), and its ability to respond with best case recommendations even for situations that fall outside the operating procedures (e.g., positing mitigation strategies for beyond design basis accidents). Additional capabilities of the recommender system as well as operator interactions with it will be explored in future research.

Disclaimer

References

[1] Quinn, T., Bockborst, R., Peterson, C., Swindlehurst, G. (2013). Design to Achieve Fault Tolerance and Resilience. Technical Report INL/EXT-12-27205, Idaho National Laboratory, Idaho Falls.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] U.S. Department of Transportation (2011). Federal Aviation Administration, Introduction to TCAS II Version 7.1.

[3] Buttner, W.E. (1985). Advanced Computerized Operator Support Systems in the FRG. *International Atomic Energy Agency (IAEA) Bulletin*, Autumn, 1985.

[4] International Atomic Energy Agency (1994). "Development and Implementation of Computerized Operator Support Systems in Nuclear Installations," Vienna, Austria.

[5] Pu, W., Choi, J., Olson, T., Amir, E., Girju, C., Park, Y., Vilim, R., and Domel, A. (2013). Description of New PRODIAG Algorithms and Simulation-Based Acceptance Tests, Technical Report, Argonne National Laboratory, Argonne, Illinois.

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

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

[8] Veland, Ø., and Eikås, M. (2007). "A Novel Design for an Ultra-Large Screen Display for Industrial Process Control," Ergonomics and Health Aspects of Work with Computrers, Lecture Notes in Computer Science, Volume 4566, pp. 349-358.

[9] Braseth, A.O. (2011). An Empirical Qualitative Study of the Inforomatin Rich Design BWR Hammlab Large Screen Display, HWR-1023, OECD Halden Reactor Project.