INL/CON-14-32523
PREPRINT

A Computerized Operator Support System Prototype

Proceedings of the Human Factors and Ergonomics Society Annual Meeting 2014

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

October 2014

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

A Computerized Operator Support System Prototype

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

Proceedings of the Human Factors and Ergonomics Society Annual Meeting 2014 58: 1899
DOI: 10.1177/1541931214581397

A COMPUTERIZED OPERATOR SUPPORT SYSTEM PROTOTYPE

Thomas A. Ulrich, Roger Lew, Ronald L. Boring, and Ken Thomas
Idaho National Laboratory, Idaho Falls, Idaho 83415, USA

A computerized operator support system (COSS) is proposed for use in nuclear power plants to assist control room operators in addressing time-critical plant upsets. A COSS is a collection of technologies to assist operators in monitoring overall plant performance and making timely, informed decisions on appropriate control actions for the projected plant condition. A prototype COSS was developed in order to demonstrate the concept and provide a test bed for further research. The prototype is based on four underlying elements consisting of a digital alarm system, computer-based procedures, piping and instrumentation diagram system representations, and a recommender module for mitigation actions. The initial version of the prototype is now operational at the Idaho National Laboratory using the Human System Simulation Laboratory.

INTRODUCTION

Nuclear power plants (NPPs) face a trade-off in control philosophy between automatic systems versus operator control. Some automatic systems are used when there is insufficient time for operators to diagnose and respond to fast-moving events. The plant operates in an envelope of conditions that are supervised by the plant protection system, in the form of setpoints for protective actions that will be automatically invoked if the thresholds are exceeded. These automatic actions are designed to put the plant to a safe and known condition, such as a reactor trip. Other automatic actions are part of the plant control system (PCS), which maintains important plant parameters at the desired operating points by adjusting plant components, such as valve positions and pump speeds. The PCS relieves the operators from the burden of continuous, tedious manual control of these components.

A previous report by Quinn et al. described the benefits of automating operator actions for plant transients (2012). The report identified situations in which alternate configurations and actions can mitigate the need for extreme measures, such 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 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 transient and averting the need for safety actions, the time required may negatively impact 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. 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 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 faults and plant transients. Development of such technology could prove to be enormously beneficial to the currently operating nuclear plants, as well as the array of new types of nuclear plants that are now being built or proposed. This would result in better management of plant upsets, improved operator performance, and ultimately make a positive impact on the industry's fundamental objectives in the areas of nuclear safety, production, and cost management.

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 version provides both traffic advisories and resolution advisories comprised of course corrections to avoid any pending collisions (U.S. DoT FAA, 2011).

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 (Buttner, 1985). 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 (IAEA, 1994).

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

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 plant parameter trends.

The operator is the point of integration of all control room information and has to use what is termed "operator fundamental knowledge" to ensure that indeed the control room is applying the correct procedure for the plant upset. Operators are trained to use a number of human performance enhancement techniques to correctly assess the situation, such as using a questioning attitude and validating all information. In addition, there are a number of other techniques used in the control room at a crew level, such as pre-job briefs, time-outs, repeat-back communications, independent verifications, etc. 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 will commit errors that compound the original fault and impact the plant more so than would otherwise have occurred.

The control room crew typically follows a 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 COSS prototype design considerations for a chemical volume control system (CVCS) are discussed.

COSS PROTOTYPE DEVELOPMENT

Design Elements

In order to demonstrate the COSS, a functional prototype was developed using a digital control system (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 CBP closely mimics the paper-based procedures for abnormal and emergency operations, including the common two-column format with a left hand column for the preferred operator action and a right hand column for response not obtained. 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 displayed 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 level) before they are alarmed. The recommender system interacts with the digital alarm system, CBP system, and P&ID displays, directing the operator to relevant information and available actions and procedures.

Design Philosophy

The CVCS was selected as the system to model for the prototype, in part because it is modeled in an available Process Diagnosis (PRODIAG) system capable of fault diagnosis (Pu et al., 2013) and because it is one of the systems that has been successfully implemented in DCSs as part of control room modernization (Ulrich et al., 2012). For example, the DCS for a CVCS at a recently modernized NPPincorporates elements of a 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. Rather, it monitors overall plant or system activity and advises the reactor operator on the correct course of action, including the correct procedure path to take. The recommender system augments the CBP by directing the operator to the appropriate procedure based on the fault diagnosis.

Full Scope Simulation Environment

The COSS prototype is integrated into the U.S. Department of Energy's Light Water Reactor Sustainability Human Systems Simulation Laboratory (HSSL) located at the Idaho National Laboratory (see Figure 1). It is displayed as a picture-in-picture embedded on a vertical display of a simulator bay. For details on the HSSL, refer to Boring et al. (2013). 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.

Figure 1. The Human Systems Simulation Laboratory.

COSS PROTOTYPE

COSS Overview

The COSS prototype is capable of displaying CBPs, a CVCS main P&ID based on the CVCS DCS at an operating plant, and trend alarm panels (see Figure 2). The COSS uses a dullscreen display scheme comprised of black, white, and greys for denoting components in normal operating conditions and displaying 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. 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 color green is used exclusively by the recommender system, both for messages to the operator and for highlighting areas of concern in the P&ID display.

COSS Status

The COSS status indicator (see Figure 2) informs the operators that the COSS is functioning properly at any given point in time. 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 2 shows available views that can be displayed in the main display area. The COSS can toggle between three views: P&IDs, Procedures, and Trends. The currently selected item is highlighted with a white border for easy identification. Procedures will display the currently active procedure, with additional procedures denoted as separate tabs. The Trends button invokes a detailed view of one of the trend alarms normally found on the right of the screen.

COSS Recommender System

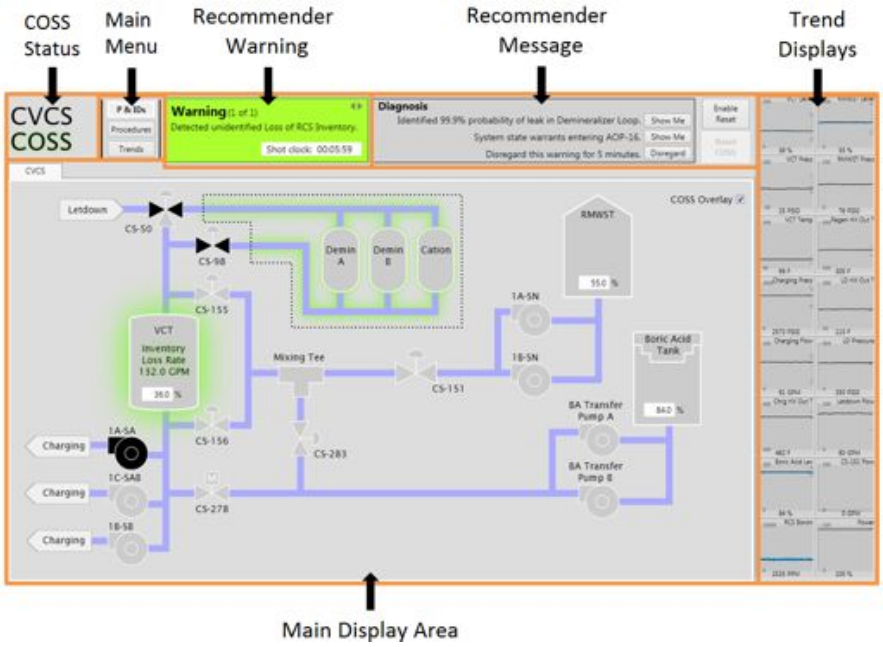
The recommender system (see Figure 2) provides a visual presentation of the detection, validation, diagnosis, and monitoring functions completed by the COSS. When the COSS detects a fault, a warning display highlighted with a green background appears in the recommender area. The warning display also contains a description of the trend that triggered the COSS to detect a fault, e.g., "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 that requires a reactor trip or other safety actuation (see Figure 2). This feature allows operator to conduct diagnostic and mitigation activities with according priority.

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 2) 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 2).

CBPs 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 nuclear power plant 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

Figure 2. Annotated COSS display featuring areas of concern highlighted on the P&ID, a recommender warning and suggested mitigation action messages.



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 check off when the operator completes the step. 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 3.

Trend Alarm Panel

The trend alarm section of the COSS serves as information rich display containing 16 trend alarms in a panel (see Figure 3). 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. The trend alarms use background color to denote any trend that has 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 reaches a particular set point, the trend alarm panel background turns yellow and eventually red as an alarm state is reached.

Figure 3. Computer based procedures and Trend Alarm.

OPERATOR FEEDBACK

An important component for the development process of futuristic concepts, such as those found within the COSS, is gaining an understanding of how operators will interact with. Additionally, operator feedback is vital because they will eventually be the end user for this system if it were to be implemented within a MCR. To this end, we were able to present the COSS to a small group of operators (three

licensed operators and one licensed instructor) and receive their feedback. In general the operators were impressed with the systems capabilities and were excited for something like the COSS to be implemented in the future. The specific feedback they provided fell into the following categories.

- *Salient Warnings* – The operators deemed the COSS warning and highlighting functions effective for drawing the operators attention in an aesthetically pleasing manner. The potential reduction in human error based on the specific fault and scripted mitigation actions were also reported.
- *Task Based Integral Screens* – The operators expressed a need for aggregating information within a central place to reduce the ping-pong effect in which the operators bounce around the control boards to acquire information. The dynamic P&ID display and CBP were reported to successfully serve this function.
- *Trend Alarms* – The operators were impressed with the trend alarms and the dual functions they provide for quickly detecting plant trends and alarm states. One operator reported using a personally customized display analogous to the COSS trend displays on his plant computer, though he noted that premade versions would be beneficial since he has the expertise to create these displays while newer less experienced operators may not.
- *Scenario Validation* – The operators compared the diagnostic process conducted in their MCR with the mimicked method the COSS uses. They confirmed that the scenario accurately reflects the actual plant behavior and diagnostic process.
- *Additional Functionality* – One operator requested additional dynamic flow indicators for the pump icons. The operators all requested customizability for the trend alarms, e.g., time course and scaling, which were previously considered, but have not been incorporated in this version of the COSS.

The feedback from the operators provided encouragement for continued development of the COSS prototype. Furthermore, the specific feedback will aid in adding additional functionality to enhance the effectiveness of the COSS as an operator aid.

DISCUSSION

Several areas of future research were identified in the development of the COSS prototype. The research will improve the underlying components of the prototype to expand its applicability to additional types of plant upsets.

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 that is currently installed in operating nuclear plants is that which is needed for plant protection and control purposes, which may not provide enough information for the COSS to make accurate diagnoses. Affordable, enhanced instrumentation would improve the accuracy of plant diagnoses and could likely 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 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 incidents). Additional capabilities of the recommender system as well as operator interactions with it will be explored in future research.

DISCLAIMER

REFERENCES

Boring, R., et al. (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.

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

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

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

Pu, W., et al. (2013). *Description of New PRODIAG Algorithms and Simulation-Based Acceptance Tests, Technical Report*, Argonne National Laboratory, Argonne, Illinois.

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.

Ulrich, T., et al. (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.