Human centered design for nuclear power plant control room modernization

Paulo V. R. Carvalho (paulov@ien.gov.br), Jose O. Gomes (joseorlandogomes@terra.com.br), Marcos R. S. Borges (mborges@nce.ufrj.br)
Graduate Program in Informatics
Federal University of Rio de Janeiro
Cidade Universitária, Rio de Janeiro, Brazil

Abstract

The use of nuclear power plants to produce electric energy is a safety-critical process where ultimate operational decisions still relies with the control room operators. Thus it is important to provide the best possible decision support through effective supervisory control interfaces. A human centered design approach, based on cognitive task analysis methods, was used to observe the operators training on the nuclear power plant simulator of the Human System Interface Laboratory (LABIHS). We noted deficiencies in graphic interface design, alarm system and in the integration between the computerized interfaces and the hardcopy (paper) procedures. A new prototype of the interface including graphics, alarms and digital procedures was designed as an alternative to the current hardcopy procedure manuals. The design improves upon the graphical layout of system information and provides better integration of procedures, automation, and alarm systems. The new design was validated by expert opinion and a performance comparison with the existing design.

Introduction

In control theory, systems can be modeled as interrelated components that maintain the system's stability by feedback loops of information and control. The plant's overall performance has to be controlled in order to produce with safety, quality, and low cost. In such an arrangement both controllers (human and automatic) play fundamental roles such as to establish system goals, to know the system status, and its behavior in the near future. This is done through continuous observation/feedback/communication loops where the agents construct their system model of behavior in order to compare with system status, to be able to act on the system to produce the desired outcomes. In this control mode, the human operator has a supervisory role related to the automatic controller. The operator has access to system state information, using the control room indicators, VDUs, strip charts, alarms and the automation controller status, and may have direct ways to manipulate the controlled process, and automatic systems interact with some sections of the plant rapidly and reliably.

However, automatic systems cannot cover the whole operational range of the plant including design basis events. For example, if the configuration of the plant changes for maintenance or accidents, the applicability of the controller might be limited. In that case, humans set up an operational strategy, supervise the automatic systems, and control the plant manually as necessary. Therefore there is a need of a human centered approach in the modernization of current analog interfaces of nuclear power plant control rooms.

The goal of this article is to describe a human centered approach to evaluate and design control room interfaces of safe-critical systems. The research aims the modernization of nuclear power plant control rooms in the design of the graphic interfaces, the layout and informativeness of the alarm system, and the integration of electronic procedures into the control/display environment (Carvalho et al., 2008).

Many nuclear power plants (NPP) around the world are modernizing with new systems and equipment such as upgrading the instrumentation and control (I&C) system from analog to digital technology. Generally, as part of these upgrades, control rooms are being modernized and computer-based interfaces are being introduced, such as software-based process controls, touch-screen interfaces, computerized procedures, and large-screen, overview displays.

This research is connected to the life extension process of a Brazilian nuclear power plant. The plant is a Westinghouse, 600 MWE pressurized water reactor designed in the 60s that suffers a continuous modernization and life extension processes. This overall research aim is to investigate how advanced (digital) interfaces can be used in the modernization of the analog instrumentation and human/system interaction (HSI).

This article is divided as follows. In the next section we review the modernization approach based on control room modernization. The third section is dedicated to methods and materials used in the research of human factors in NPP operations. Section 4 presents the results and a set of recommendations for a new interface aimed to modernization of control rooms. Section 5 presents the evaluation of the new interface design, focusing on human factors, and section 6 presents a discussion and some lessons learned. Finally, Section 7 concludes the paper.

Human centered interface design in NPP control room modernization

The nuclear power plant control room operators observe and manipulate an extremely complex system. The task requires walking along a large control panel, taking readings from gauges and adjusting knobs and levers. Many of today's control rooms have replaced or augmented older, more cumbersome control panels with visual display units (VDUs) with graphic interfaces. VDUs can simplify the human machine interface, but they also introduce new design challenges. Digitalization of previous analog man-machine interfaces imposes new coordination demands on the operational teams (Vicente et al., 1997). These issues lead to new situations of human-human and human–system interaction. In order to

run such system effectively, efficiently, and safely, much research has been developed taking into account human performance, new technological possibilities, and types/levels of automation in a system, design of human–machine interfaces etc. (e.g. Sheridan, 2002; Nachreiner et al., 2006).

After the Three Mile Island (TMI) accident in 1979 NPP regulators around the world recommend the use of human centered approach to human systems interface design to ensure that the man-machine interfaces, control room layout, procedures, training and other human related issues meet the task performance requirements, and are designed to be consistent with human cognitive and physiological characteristics (Rouse, 1984). The human aspects related to the control room design such as operating experience review, function analysis and allocation, task and activity analysis, staffing qualifications, training, procedures should be developed, designed, and evaluated on the basis of a systems analysis that uses a "top-down" approach, starting at the "top" of the hierarchy with the plant's high-level mission and goals (O'hara & Brown, 2004).

However, most of the modernization processes has been driven to a large extent by the technology. The modernization of the turbine control in the NPP under study can be viewed an example of technological driven approach. A new computerized turbine control system was purchased to replace the old analog controllers. Although the new system perform its functions better than the old one, it is also true that the installation of computer screen and keyboard along with the analog instruments in the hardwired panel, as shown in figure 1, lead to human-system interaction problems.

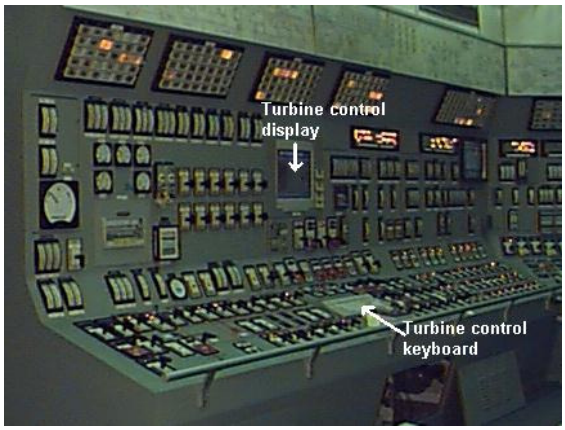

Figure 1: Turbine display and keyboard together with analog instrumentation.

The human-centered approach exploits the technical innovations to achieve an optimum human – artifact interactions, aiming at improving the appropriateness of the technological solutions (Hancock & Chignell, 1995). The human centered approach to the design of human-system interfaces considers the impacts of the introduction of new technology on the humans in the system and on the overall behavior of the system, from the beginning and continuously throughout the design process (Brunélis & Blaye, 2008). The approach requires specific activities that should take place during the system design. These activities are: 1) to understand and specify the context of use; 2) to specify the user and organizational requirements; 3) to produce design solutions and to evaluate designs against requirements. The human-centered design process should start at the earliest stage of the project (e.g. when the initial concept for the product or system is being formulated), and should be repeated iteratively until the system meets the requirements. It is not sufficient to verify the quality with which the design process is carried out (concerned with whether certain design phases were carried and certain documents produced to meet the design requirements). Considering that the in human-centered design approach, technology should be comprehended from the point of view of providing tools for human activity (Flach et al., 1995), it requires a dynamic performance evaluation, to assess the appropriateness of this technology in the aimed use.

Materials and methods

The construction of the NPP under study started in 1972, the first criticality of the nuclear reactor occurred in 1982 and the plant commercial operation started in 1985. Since then, it generated 40 million MWh of electric energy. Into the modernization and life extension plant program an upgrading of I&C and Human System Interface (HSI) systems is planned.

In order to support the application of the human centered design approach in the modernization of the Brazilian NPPs, the Brazilian Nuclear Energy Commission (CNEN), developed an experimental facility for human system interface design and human factors research and development, the Human System Interface Laboratory (LABIHS). LABIHS facility is ready to conduct NPP operators' performance evaluations, and research on human-system interaction in complex domains. The LABIHS consists of an advanced control room, an experimenter's gallery room and other auxiliary rooms. The advanced control room has nuclear reactor simulator software, graphical user interface design software, a hardware/software platform to run and provide the adequate communication between the software, and the operator interface - VDUs and controls needed to operate the simulated process.

To simulate the plant under study, a Westinghouse PWR type digital compact simulator is used. In this simulator, modeling scope and fidelity are equivalent to a full scope simulator, but the full control room is not replicated. An Integrated Hardware/Software Platform runs the simulator program and transfers data throughout the computerized environment. The basic operator workplace is formed by 4 VDUs, each one with mouse and keyboard. An overview display, based on direct beam projector, is also provided in the control room. A graphical user interface design tool (GUI) for HSI design is also available for development and testing of different types of interfaces. The Instructor Station complements LABIHS architecture. The LABIHS control room is shown in figure 2.

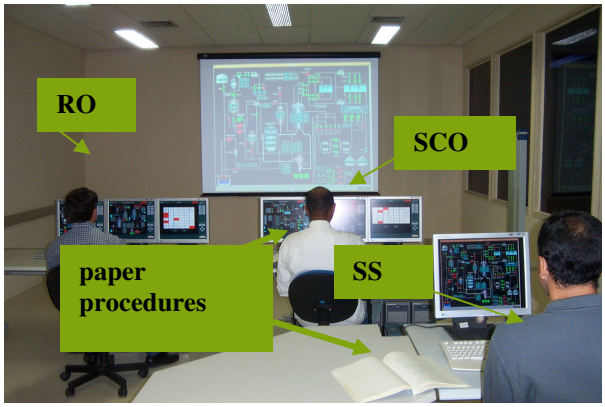

Figure 2: LABIHS control room. RO means Reactor operator, SCO Secondary system operator, SS Shift supervisor

Research method

In this research, we use LABIHS to investigate the nature of operator–system interaction in a digital interface during abnormal events to contribute to operational safety and efficiency through enhanced interface design. We use the interface evaluation procedure proposed by Hollnagel (1985) because it is consistent with most of human-machine interface evaluation requirements in the Human Factor Engineering (HFE) guidelines and programs that are currently used in nuclear industry, such as NUREG -0700 rev1 (O'Hara et al, 1996) and NUREG-0711 (O'Hara et al., 1994). The evaluation procedure has three phases. The first phase is the conceptual evaluation of the interface. It can be carried out by experts using tools like task analysis; operational experience review in similar systems; safety analysis reports; functional specification; drawing showing displays, panels, workstation, graphical interfaces and diagrams showing flows of information. In the second phase an heuristic evaluation is made based on some well known interface evaluation criteria (eg. Nielsen, 1993). The system is represented by samples taken from preliminary performance recordings, using results of runs with the real system or prototype. It is a static simulation. It concentrates on the way in which the information is presented to the operator and involves some form of basic system operator interaction. In the third phase, the entire process is simulated, and the operators' performance is evaluated. In this phase operators have a degree of psychological involvement and we can see how they react to the simulated process in a realistic manner. It requires a simulated work setting, a detailed experimental planning, including training, data acquisition, analysis systems such as computer logs (process state, process events), operator log (human machine interface events, keyboard, mouse) and audio, video recorder (verbal protocols, communication).

A final evaluation occurs during the plant commissioning tests in the plant site. At that moment any changes in control room interfaces will much more difficult and costly than it would be in the early phases (Santos et al., 2005).

Participants

One operator crew participate in this research under different operating conditions: start up, planned shutdown and in postulated accidents. The LABIHS control room operating crew is composed by 3 operators: the Shift Supervisor, Reactor Operator (RO) and the Secondary Circuit Operator (SCO). The Shift Supervisor have a deep background in nuclear engineering, participated in the LABIHS's HSI design, and have a huge experience in the simulator operation. The RO and SCO are instrumentation technicians who have been trained in LABIHS operation for 2 years before this study. They have no previous experience in the reference plant operation.

The operation of nuclear power plants

The operation of a nuclear power plant falls under four basic phases: startup, normal operation, planned shutdown, and emergency operation that begins after reactor automatic shutdown, when incidents/accidents occur. Although important events occur in all modes of operations, we focused the observation on periods of higher activity, such as startup and emergency operation.

Under normal conditions, NPP operations are well coordinated and based on procedural instructions. In this ''nominal'' operating mode, the SS reads the procedural instructions aloud to the RO and SCO who then execute the instructions (Carvalho et al, 2006).

Performance evaluation

During 30 hours of direct observations, we observed how the operators interacted with the simulated PWR in various modes of operation. The LABIHS is equipped with a ceiling-mounted camera which captures the majority of the room, including the two operators' stations and the main presentations screen (fig. 2). We placed a tripod-mounted Mini-DV camcorder to record whichever operator would be likely to have the most active role. A hand-held digital camera was used to film particular details of interest that were not sufficiently captured by the other two cameras.

The research team, with 3 analysts, was divided to pair up with the employees of the simulator. One analyst accompanied the primary operator; the second accompanied the secondary operator; and the third accompanied the simulator supervisor. The operation of a nuclear power plant fall under 4 basic phases: startup, normal operation, shutdown, and incidents/trips (unplanned automatic shutdown)/accidents. Although important events occur in all modes of operations, we focus on periods of higher activity - startup and incident/accident.

During the startup phase observations, we encouraged the operators to verbalize their goals, actions, and concerns to improve our understanding of the technical system. However, during the simulated accidents, we tried not to interfere with the operators so as to elicit true response behavior. During the simulated accidents, the supervisor and two senior LABIHS researchers were also present. This placed noticeably increased pressure on the

operators, and also led them to justify their actions verbally after the scenario was completed.

We paid particular attention to the tasks dictated by the procedure manual and to the operators' actual activity. We search for particular deficiencies in the support of operator response to abnormal system states, and then we redesigned the operator interface to improve upon the graphical layout of the information, the navigation across screens, the alarm presentation, acknowledgement and response, and to integrate these with computer-based procedures that dynamically correspond with real-time system information. Comprehensive debriefing interviews with the operators and supervisor and was carried out to validate the conclusions taken.

Results and recommendations for modernization

Graphical interface design

Figure 3a shows a typical control screen of the original interface for one subsystem of the plant, in this case, the Chemical and Volume Control System (CVCS). Multiple objects with bright, contrasting colors compete for the operator's attention on the cluttered screen. In many places in the interface, red is associated with a state of alarm or failure. However, this association is undermined by the red color of some valves, pumps, and indicators which are operating normally (red means valve closed; the same color pattern used in the reference plant). Additionally, the red components are highly salient, even when the components do not require operator's attention. Excessive labels contribute to clutter. For example, the blue RCP Seal information box displays the same variables for each of the three RCP seals, but uses nine labels – one for each variable display field. It increases the visual distance between readouts, making comparisons of the values more difficult. The high salience of the large pump icons detracts from the operator's ability to perceive other elements on the screen. They are not frequently manipulated and they only display two pump states (on and off). The sharp contrast between the white lines representing the pipes which connect system elements and the black background contributes to the clutter of the screen without providing much information. The white-on-black color scheme is also used for pump and valve labels, as well as the system variable values. The similarity in color detracts from the salience of these labels and values. Flow directions of are not clearly indicated. The lack of distinction between pipes with and without flow does not contribute to the principle of pictorial realism, i.e., that a visual representation should accurately symbolize the entity it is intended to represent. To determine the path of coolant, operators must trace the white line pumps through which the line passes to ensure that all are open or on, respectively. While the on/off color distinction is clear, there is no redundant indicator of a valve's state, nor does the interface support the synthesis of individual valve states into an overall depiction of flow; each valve must be independently analyzed, increasing the operator's cognitive load. Label legibility is poor due to all-capital text. This also increases label's space requirement without providing additional information. Also, the shine used to produce the 3D graphical effects for the tanks and reactor core decreases contrast and reduces legibility for the white labels that overlay these graphics. There are many different unit names for the same physical variable (e.g., gallons/minute, liters/second and Kg/second), and are many variables without units. The positions of variable values display and related components (pumps, valves) are not uniform among displays, and the same lack of uniformity and consistence appears on the graphical representation of the plant components. Some plant components are not correctly identified and labels positions and formats are not consistent across displays.

There are also many problems related to navigation among displays. The navigation process using the arrow buttons is not clear, because operators don't know the display they will go on and the History/Previous buttons are not working properly (indicating the previous navigated displays). The interface design does not highlight which elements (e.g., pumps, valves) can be manipulated, which are locked out or which are automatic. The operator may be operating under the assumption that a certain valve can be manipulated, finding out latter, when trying to manipulate the valve, that this it is not possible.

Operators show difficult with the navigation using graphic links. Links between some displays do not represent clearly the process flow. Therefore operators always returned to the Main Menu display, searching for the adequate navigation button, because they prefer the navigation buttons rather than graphic links. This back and forth situation augments navigation time between the displays.

Plant component control (ON, OFF, START, INCREASE, DECREASE, STOP) starts with a mouse click on the equipment icon (valves, pumps). After that, a pop-up window appears on the screen, showing the respective control buttons. Then, the control operation should be carried out by clicking on the respective control button. However, observing the control actions of the operators in valves and pumps, we note that sometimes the pop-up windows appeared on the process viewing area of the displays (not in the control panel area), covering plant variables, and interfering with the readings of displayed information.

The redesigned interface (fig. 3 b) is based on the deficiencies noted in the evaluation. They include improved aesthetics and mock-up designs of new functionality. While we have not coded the components into the simulator software, we do not expect significant compatibility problems. The components consist of borders, text boxes, and colors – all of which are supported by the simulator's graphics builder software. The component functionality is also expected to be compatible, as it largely mimics functions (such as linking, highlighting, and displaying real-time system variable values) observed in the original simulator.

Issues with the legibility of labels were addressed by using mixed-case fonts which use less space and provide redundant coding of written information: the shape of the words provides another cue for recognition, aside from the sequence of the letters. To further aid legibility, the 3D graphical tanks, pressurizer, and reactor core were replaced with simpler, flat representations. This allows

for increased legibility of the labels, as well as the inclusion of a graphical indicator for the fluid level in the Volume Control Tank (VCT), Pressurizer (Prz), and Reactor Core. The graphical indicator does not require much visual space on the screen, and provides the operator with redundant information on the fluid level of the component. Understanding the context of a reactor core coolant level of 6.5 meters, for example, is aided by the blue bar showing the level of fluid relative to full (top) and empty (bottom) states. (see fig. 3 b).

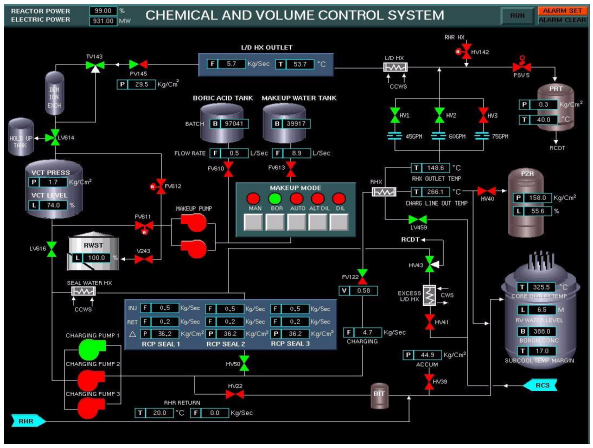

Figure 3a: Original simulator CVCS display.

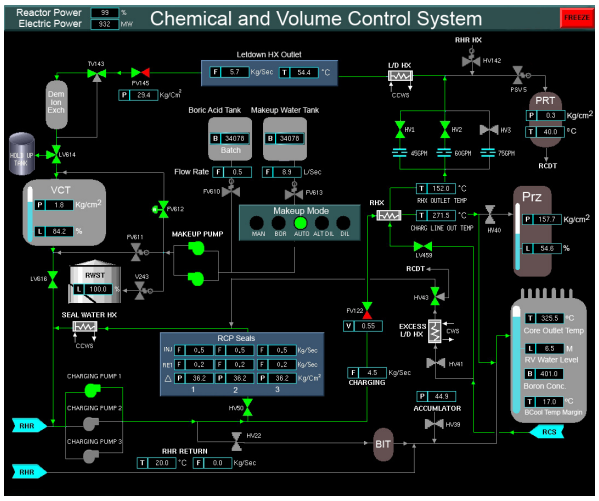

Figure 3b: Graphical improvements on CVCS screen.

The changes aim to improve operator situational awareness, and reduce the likelihood of human error. We remedied the overload of red icons by updating the valve and pump color scheme. Grey is used to reduce salience of closed valves and pumps which are off. Redundant coding is provided by rotating closed valves perpendicular to the pipe, while open valves remain parallel. The size of the pump icons is reduced. While still easy to locate, the off pumps and closed valves do not attract unnecessary attention from a broad overview. The frequently manipulated variable flow valves remain unchanged, providing distinction that helps the operator to quickly locate them. We also simplified the controls for the green "Makeup Mode" control box in the center of the screen. The circular indicators now serve as buttons as well as indicators, obviating the need for the Grey buttons. Also, now only the indicator showing the current mode is lit green. The other indicators which were previously red are toned down to black, so that they do not distract the operator. The RCP seal information box has also been simplified to bring the variable displays into closer visual proximity, and excessive labels have been removed to decrease clutter. The pipes have been re-colored to decrease the salience of pipes which with no coolant flow and to emphasize the pipes with flow. Pipes with coolant flow are bolded and shaded the same color green as the switched-on pumps and open valves. As a result, the emergent feature is a green circuit where there is flow of reactor coolant. The pipes with no flow have been subdued from white to Grey so that they will not interfere with the reading of labels and variables.

Alarm system design

When an abnormal state of a variable occurs, the simulator initiates an audible alarm, as well as a flashing red "Alarm Set" indicator at the top right corner of the screen in use. The alarm indicators are located on two separate specific alarm screens. They are arranged as tiles in a grid where active alarms are indicated by a flashing red tile (fig 4 a). This arrangement reproduces in the simulator the main alarm annunciation tiles used in the reference (analog) interface of the real plant. The existing system does not support quick alarm identification. The text descriptions on the alarms tiles are written in English abbreviations, which may cause delays in the identification for Portuguese speaking operators. The alarm set indicator does not provide any detailed information about the nature of the alarm which is sounding (the same situation that occurs in the actual plant). The operator must always navigate to both alarm screens to determine which alarms were activated. Additionally, the grid arrangement has no apparent organization or order. Related alarms are not grouped on the screen nor are alarms divided logically across the two alarm screens. Finally, all alarms are displayed identically, making it difficult to distinguish between alarms on the basis of severity and importance. All alarms are annunciated by the same sound.

The new prototype interface includes an extensive revision of the original alarm system. The major changes are captured in the revised alarm screen (fig. 4 b). The alarms have been divided into two panels, distinguishing reactor and turbine trip alarms from all others. Within each panel the alarms are organized by the location of their activator in the system. For example, the charging flow indicator is located on the CVCS screen and hence, on the alarm screen, it is under the CVCS column heading. Each alarm tile is a dynamic interface component. This reduces the required number of alarm tiles, allowing all of them to fit on one screen. Instead of a button each for pressurizer pressure high and pressurizer pressure low, the redesign simply uses pressurizer pressure. Depending on the alarm (high or low), the alarm tile displays the appropriate text. Each sounding alarm tile also keeps track of how many seconds since the alarm was set off using a small counter in the upper-left corner of the tile. The trend graphs on

the alarm screen saves time and provides better diagnostic information. The acknowledging system has also been improved to allow single-alarm acknowledgement (by clicking on a sounding alarm tile), while retaining the "ACK" button to acknowledge all alarms.

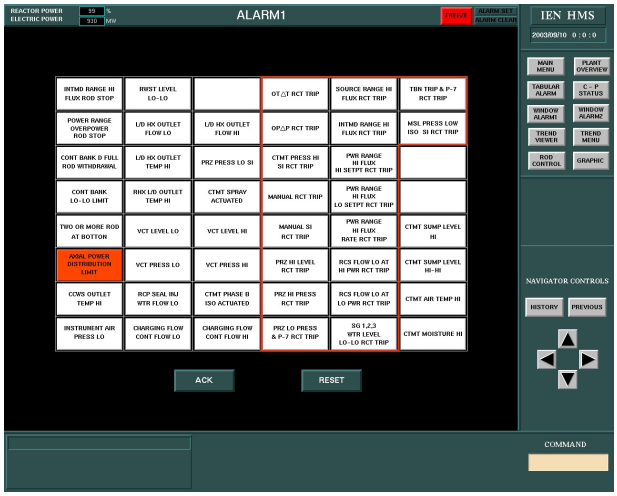

Figure 4a: Original alarm screen.

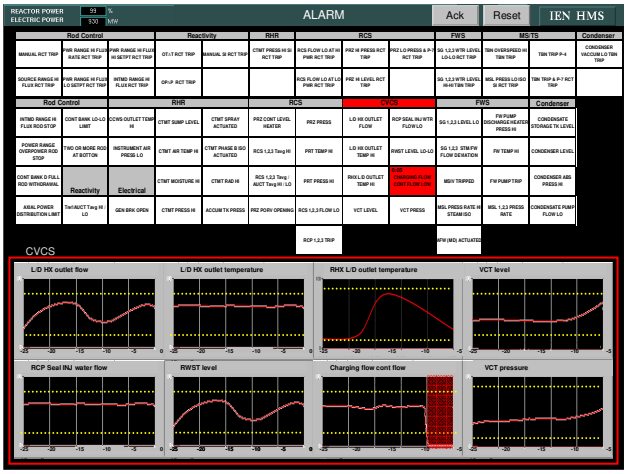

Figure 4b: Redesigned alarm screen.

Each alarm tile acts as a link; clicking the sounding alarm tile navigates to the appropriate screen. On the relevant screen, a red box flashes several times, drawing attention to the area triggering the alarm. Additionally, the alarms relating to the current screen are displayed in chronological order of occurrence as tiles to the right of the schematic diagram. Clicking on these tiles flashes the red box several times box around the area of concern. The navigation buttons have been revised to provide easier access to all the operations screens. While the system is in an alarm state, the related navigation buttons at the bottom of the screen are displayed in red, effectively doubling as an alarm overview. Clicking on the red alarm button navigates to the alarm screen (fig. 4 b).

Digital procedure system design

Procedures guide the operators as they face unfamiliar situations. The simulator uses hardcopy procedure manuals in the form of one-dimensional checklists and step-by-step guides. Non-compliance with procedures was observed frequently. In these situations, operators often improvised around the formal procedures to achieve their system goals, which in some cases can enhance system safety. We observed one operator consistently using a hand-written sheet to aid him through various procedures. The procedures are often constraint-based, requiring the operator to maintain multiple system variables within a specified range. The current interface does not support this task. Instead, it relies on the operator's cognitive ability to monitor system variables and recall acceptable ranges which change frequently during operation. For example, one procedure requires the operator to locate two variables, manually calculate the difference, and judge whether the difference exceeds a safe upper bound which depends on the current mode of operation. Finally, the layout of data in the simulator is inadequate for perceiving and comparing the rate at which a variable of interest is arriving at its limit.

Due to strict procedural adherence requirements, instead of requiring decision support, operators often benefit from tools that reduce errors of omission. The Procedure Guidance Component (PGC) supports operator's process control effectiveness, by converting the procedure manual into an online, navigable guide (Fig. 5). Clicking on any procedure in the left column produces a detailed text description of the procedure. It also reports relevant system statistics and links to useful screens elsewhere in the simulator. This tool adds interactivity to what was previously only a hardcopy procedure manual.

The second component, the Emergency Guidance Component (EGC), is used during emergencies in which the root problem is unknown. The EGC is a reworking of the Strategic Manual Operations flow diagrams provided by LABIHS (for example, see Fig. 6). Clicking on event objects on the left provides response instructions on the right. The operator may scroll up or down through the flow diagram and response instructions using the click and drag technique common to document viewer applications. The continuity provided through the scrolling feature obviates the need for page turning, which takes time and artificially divides what, in reality, is a continuous process. The logic that runs the simulator can be used to support the EGC. Because some decision nodes are based on system variables, the system can often suggest an appropriate decision based on the current system state. The system's suggestion is displayed in a green box to the right of the flow diagram and above the response instructions. It includes the suggested action and the rationale for proposing it. In addition, the operator can trace the decision path because the system fades the paths which have not been taken to a neutral grey, leaving a bold black decision path. Digitizing the emergency procedures enables the implementation of additional support features. The response instructions often involve "if-then" statements. For example, if the pressurizer level reaches 8 meters, then open valves X and Y. Because the simulator knows system variable values, it can guide "if-then" decision-making by placing

a red box around “then” actions when the “if” conditional is met.

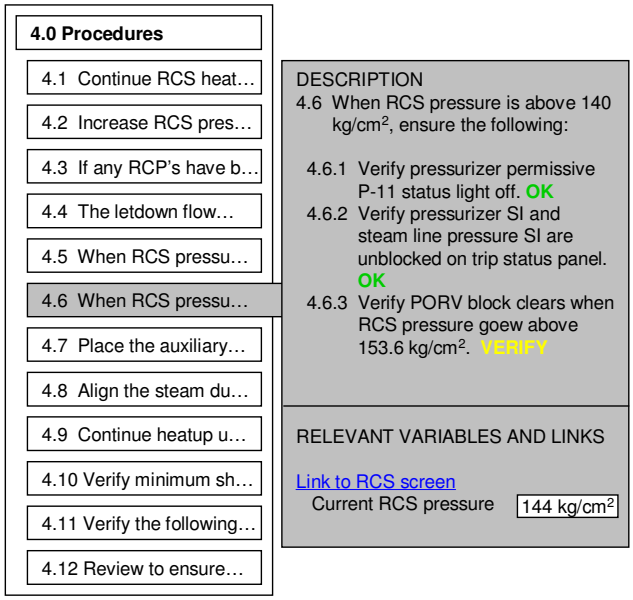

Figure 5: Procedure component guidance.

The Procedure and System Overview (PSO) screen was created to display the PGC and the EGC (Fig 6). The operator may tab between the PGC and the EGC, which reduces short-term memory requirements when compared to hardcopy procedures. On the right side of the PSO, graphical representations of relevant variables are displayed. These are dictated by the current procedure. For example, during a Loss of Coolant Accident (LOCA) the system will keep track of main system pressure, pressurizer pressure, etc. In addition to providing support during emergencies, it aids accident prevention by supporting operator awareness.

In the hardcopy procedures, decision nodes do not have any response instructions because they are implicitly “ifthen” nodes. The digital version shows these “if-then” relationships efficiently by displaying them in the response instructions panel. The response instructions of action nodes include “if-then” relationships as well. Some “if” statements refer to the system state (e.g., if valve X is open) while others ask the operator to wait for a variable to reach a set point before taking action. Unlike the hardcopy version, the new system displays these variables proximally and outlines in red the response instructions when the “if” conditions are met.

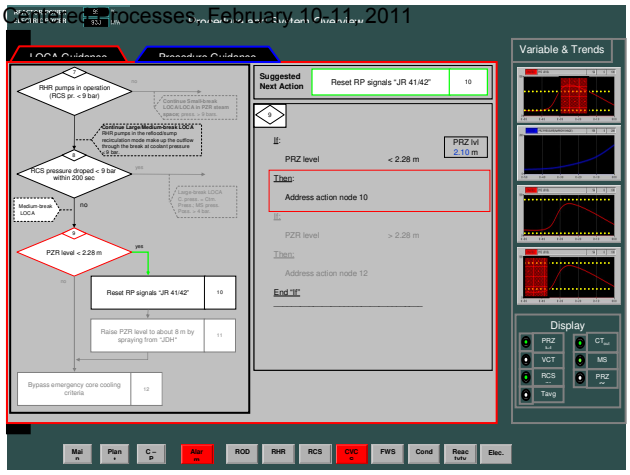

Figure 6: Procedure and System Overview screen displaying the EGC.

Evaluation of the new interfaces

We evaluated operator performance in the new designed interface (figure 6) during accident simulations (Loss of Coolant Accidents – LOCA and Steam Generator Tube Rupture - STGR). A LOCA occurs when there is a pipe rupture in the Reactor Coolant System and the STGR accident occurs when there is a leak in the steam generator tubes. The old LABIHS interface design provided the performance benchmark.

Initially we measure the time that operators need to identify the accident using both interfaces. The time interval between automatic reactor shutdown (reactor trip) and the correct accident identification is very important for a safer operation (Carvalho & Oliveira, 2009). When the reactor is tripped, the operators carry out the standard post trip actions, according to emergency procedures to identify what accident happened, in order to define adequate actions to keep the system under control and minimize the damage that the accident may cause. Using the data obtained from simulator logs it was possible to measure the time interval from the reactor trip until the correct accident identification in both interfaces.

The time spent by the operators to identify the LOCA and SGTR accidents, through the existing interfaces, was 362 seconds and 490 seconds, respectively. The time spent by the operators to identify the LOCA and SGTR accidents, through the new interfaces, was 338 seconds and 428 seconds, respectively. The results show that the time interval from the reactor trip until the identification of the SGTR and LOCA accident decreased when the operators used the new interfaces to identify the accident. The number of screens used during the identification also change. In the existing LABIHS interface the SCO used 13 screens to identify the LOCA and 25 to identify the STGR. In the new interface this numbers fall to 8 and 10, respectively, showing a considerable reduction in navigation actions.

In another experiment, after the LOCA identification, operators are tasked with bringing the system under control by following a LOCA flow diagram procedure. Currently this diagram is available in hardcopy and portable document format. The format requires the operator to shuffle among various pages. The flow diagrams and the response instructions are located on separate pages, either requiring the operator to flip back and forth at least once per node or to take up desk space by laying them side by side. The standard hardcopy

procedures are bound, therefore requiring the flip method. Given a medium-break LOCA, to get to step 12 of the diagram requires at least 4 flips between the diagram pages and the response pages and viewing 23 pages (2 diagram pages and 21 response pages). Using the new design, operators can see the flow diagram, the currently selected node's response instructions and the alarm screen together (fig. 7). The redesign requires no page turns, and because it is linked to the alarm system, the operator does not have to search for the appropriate binder or page number to carry out the actions.

Figure 7: Operator working with the redesigned interfaces.

Discussion and lessons learned

We believe that the performance evaluation of the operators` activities in real work is absolutely necessary for human system interface evaluation in nuclear industry.

Activity can defined as the set of behaviors and resources that operators use to accomplish their goals during daily work. Traditional ethnographic methods enable the understanding of activities through observation of communications, gestures and postures. Using ethnographic methods, an observer locates classes of behavior that are recognizable and repeated during work. The methods also allows the observers to identify not only the previous described tasks (prescribed work), but also side activities not formulated in the frame of the task description (Marmaras and Pavard, 1997). The data obtained through direct observation, or with the aid of cameras and audio recorders, is the set of signals picked up by the operators in the information field and how they use these signals to manipulate the control room interfaces. A further analysis of the data set obtained, can show how operators transform the interface information into actions and decisions (Carvalho et al., 2006).

However, the most of methods currently used (including we use in this research) were adequate for describing individual activities developed in a well-defined sequence. However, the work in a NPP control room involves multiple and often conflicting (in goals and time) lines of activities (Carvalho et al, 2006). There are many differences between prescribed and described tasks and real work activities (how the tasks are actually done). Even in a rigid work setting like nuclear power plants, the actual work in control rooms is characterized by adaptations, improvisation and ad hoc procedure modifications (Carvalho et al., 2007; La Porte & Thomas, 1995) because the work demands and resources available rarely correspond to what was anticipated when the task was developed, thereby rendering the task description or operational procedures unworkable (Hollnagel, 2006). Therefore, using the traditional observational methods it is very difficult for the observers to capture the multiple actions pathways of real work activities, describing the many simultaneous tasks and tasks adaptations that people have to do to cope with reality.

Another methodological difficult is the collective/collaborative characteristic of the work done in a NPP control room. The observation procedure normally used is suitable when there is one observer and one worker. However, most work done in control rooms involves multiple operators who use many different cooperative mechanisms (Vidal et al, 2010). Therefore, for an adequate observation of the real work, we need tools to support an observation procedure in which many observers, in collaboration, are able to observe the activities of many subjects (Junior et al, 2010).

Conclusions

The human centered approach in complex industrial system design, evaluation and validation should be applied in the design process in which the system is produced, and in the system itself. In this research we investigate the human system interface of a nuclear power plant simulator to compare design solutions during the early design phase. The methodology used was based on observations of the operators' performance in the LABIHS simulator. Performance evaluations based methods can be used considering the fact that the appropriateness of a given system expresses itself in the quality of the overall performance of the system is assessed. Normally, performance evaluation is something that is carried out towards the end of a given design process. The LABIHS facility aims to conduct the performance evaluation earlier in the design process. A specific goal of LABIHS is to enable the evaluation of system performance as early as possible. Considering that the reference plant human system interface design has not formally started yet, this objective was already achieved with this research. Even considering that is very difficult to say when the performance of a cognitive system is at an acceptable level, our evaluation has shown some improvement possibilities in the existing design. Some of them related to basic human factors design principles such as:

- Displays with information that are difficult to read (inadequate font sizes and formats, color contrast etc.);
- Cluttered or overloaded displays with many numeric information – graphic information would be better;
- Inadequate icons size considering their function;
- Confusing and unstructured presentation of displays with set points and actual parameter values, leaving the task of searching and detecting such deviations to the operator, instead of directly showing deviations of actual values from set points;
- Static information presentation where a presentation of past dynamics (e.g. trends) and future developments of process parameters

(prediction) would be required for an effective task performance;

- Mix of different media to present operational information – digital displays and paper procedures – requiring different cognitive resources to cope with.

As expected the performance evaluation has shown that the design solutions used (alarm systems, procedures, graphic displays) actually have effects on the usage. Therefore we reinforce the claim of the human factors and ergonomics community that the design solutions should be made considering the appropriate use of the system, emphasizing that work practices in real settings. What we really need are systems that support actions of human operators, and their ability to adapt and adjust to novel situations. To do so, systems must be designed considering that the user, and the usage of the system need to be taken account in all the phases of the design process, from the design of process technology to the design of user interfaces, in a user-centered or activity-based design process.

Acknowledgments

The authors gratefully acknowledge the support of the Brazilian Research Council (CNPq) and of Rio de Janeiro Research Support Foundation (FAPERJ). The research was performed at Instrumentation and Human Reliability Division of the Nuclear Engineering Institute, Brazil (DICH / IEN).

References

Brunélis, T., and Blaye, P. (2008). Towards a human centred methodology for dynamic allocation of functions. *Proceedings of the Third International Conference on Human Centered Processes (HCP 2008)* (pp. 243-256).

Carvalho, P., Santos, I., Gomes, J., Borges, M., Guerlain, S. (2008). Human factors approach for evaluation and redesign of human–system interfaces of a nuclear power plant simulator. *Displays 29*, 273-284.

Carvalho P., Vidal, M.C. ; Carvalho, E. F., 2007, Nuclear power plant communications in normative and actual practice: A field study of control room operators' communications. *Human Factors and Ergonomics in Manufacturing, 17 (1) 43–78*.

Carvalho, P., Vidal, M., Santos, I. (2006). Safety implications of some cultural and cognitive issues in nuclear power plant operation. *Applied Ergonomics 37 (2)*, 211-223.

Carvalho, P., Oliveira, M. (2009). A computerized tool to evaluate the cognitive compatibility of the emergency operational procedures task flow. *Progress in Nuclear Energy, 51,*409-419.

Flach J., Hancock P., Caird J., Vicente K. (Eds.) (1995). *Global perspectives on the ecology of human-machine systems*. Hillsdale, N. J.: Lawrence Erlbaum Associates.

Hancock P. & Chignell M. (1995). On human factors. In: J. Flach, P. Hancock, J. Caird, K.J. Vicente, (Eds.) *Global perspectives on the ecology of human–machine systems.* Hillsdale, N.J.: Lawrence Erlbaum Associates,14-53.

Hollnagel, E. (1985). *A Survey of man-Machine System Evolution Methods.* (HWR 148) Norway: OECD Halden Reactor Project.

Hollnagel, E. (2006). Task Analysis: why, What and How. In: G. Salvendry (Ed.) *Handbook of Human Factors and Ergonomics-3rd ed.* New Jersey: John Wiley & Sons.

Junior L. C., Borges M., Carvalho, P., (2010) A Mobile Computer System to Support Collaborative Ethnography: An Approach to the Elicitation of Knowledge of Work Teams in Complex Environments. *Lecture Notes in Computer Science, Volume 6257/2010, 33-48*.

La Porte, T. & Thomas, C. (1995) Regulatory Compliance and the Ethos of Quality Enhancement: Surprises in Nuclear Power Plant Operations, *Journal of Public Administration Research and Theory*, n.5, pp. 109-137.

Marmaras, N. and Pavard, B. (1997). A Methodological Framework for Development and Evaluation of Systems Supporting Complex Cognitive Tasks. *Journées Européenees des Techniques de I`Informatique, 8, 13-20.*

Nachreiner F., Nickel P., Meyer I. (2006). Human factors in process control systems: The design of human–machine interfaces. *Safety Science,44*, 5-26.

Nielsen, J. (1993) *Usability Engineering*. Boston: Academic Press.

O´Hara J., Higgins J., Stubler W., Goodman C., Eckinrode R., Bongarra J. and Galletti G. (1994). *Human factors engineering review program model (NUREG-0711 rev.1).* Washington.D.C.: US Nuclear Regulatory Commission.

O´Hara J., Brown W., Stubler W., Wachtel J. and Persensky J. (1996). *Human-system interface review guideline (NUREG-0700 rev.1).* Washington.D.C.: US Nuclear Regulatory Commission.

O'hara J. & Brown M. (2004). *Incorporation of human factors Engineering analyses and tools into the design process for digital control Room upgrades* (BNL-72801-2004-CP). New York: Brookhaven National Laboratory.

Santos, I. J. A., Carvalho, P.V., Grecco, C. H., Victor, M. and Mol, A. C. (2005a). A Methodology for Evaluation and Licensing of Nuclear Power Plant Control Rooms. *In Proceedings of the 2005 International Nuclear Atlantic Conference, INAC*, Santos, SP, Brazil.

Sheridan, T. (2002). *Humans and Automation System Design and Research Issue.* Santa Monica: Wiley/HFES.

Vicente, K., Mumaw R., Roth, E. (19997). *Cognitive Functioning of Control Room Operators – Final Phase.* Ottawa: Atomic Energy Canadian Bureau.

Vidal, M.C.R., Carvalho P.V.R., Santos M., Santos, I.J.L. 2009, Collective work and resilience of complex systems. *Journal of Loss Prevention in the Process Industries, 22, 537-548*.