ERGONOMICS IN THE DESIGN OF PROCESS CONTROL SYSTEMS
DIGITAL INTERFACES

Paulo Victor Rodrigues de Carvalho (CNEN/IEN)
paulov@ien.gov.br
José Orlando Gomes (UFRJ)
jgomes@pep.ufrj.br; gomes.7@osu.edu
Isaac Luquetti dos Santos (CNEN/IEN)
luquetti@ien.gov.br

Nuclear power production is a safety-critical process where ultimate execution of process change decisions lie with the operators. Thus it is important to provide the best possible decision support through effective supervisory control operator interfaces. This requires an ergonomics approach in the modernization of analog instrumentation and control systems of the existing nuclear power plants. In this article, using cognitive task analysis (CTA) approach, we observed operators working on an advanced control room of a nuclear power plant digital simulator and noted several opportunities for improvement in the human/system interfaces related to the graphics design and alarm systems. A redesigned prototype was constructed as an alternative to the current simulator screens. The design improves upon the graphical layout of system information and provides better integration of the alarm system. The design was validated by expert opinion and a scenario-based comparison. We claim that the use of ergonomics in the design of process control systems throughout the industry presents many opportunities for improvements with regard to system effectiveness, efficiency, reliability and safety.

Palavras-chaves: Interface design, Nuclear power plant operation, Cognitive task analysis
1. Introduction

Ergonomics are not playing the role they deserve in the design of process control systems making them less controllable than they could be if human factors were adequately incorporated. The use of ergonomics approach in the design of process control systems throughout the industry presents many opportunities for improvements with regard to system effectiveness, efficiency, reliability and safety.

Nachreiner et al. (2006) used the following quote “The control room displays did not help the operators to understand what was happening” from a major accident in a chemical process plant (HSE, 1997) as an indication that, at least, not all process control graphic interfaces represent the state of the art in human factors/ergonomics design approach. Nachreimer et al. (op. cit.) also claimed that, especially in the design of VDU-based control system (graphic screens) human factors or ergonomics principles already known must be applied according to the existing legislation in European countries. In this research, we focused on the design and layout of the graphics on the simulators screens of a nuclear power plant simulator, and the integration of the alarm system into the control/display environment.

Nuclear power plant (NPP) control room operators observe and manipulate a complex system comprising about ten thousand parameters. In conventional control rooms, operators walk along a large control panel, taking readings from gauges and manipulating knobs and levers. Modern control rooms have been upgraded with visual display units (VDUs). Unlike the old analog control rooms, in the new “advanced” interfaces all operators can access almost all the information about the plant from his/her workplace (Vicente et al, 1997). Digitization of previous analog human-system interfaces imposes new coordination demands on operational teams (e.g. the need for communication to construct situation awareness) leading to new situations of human-human and human–system interaction. In order to run such systems effectively, efficiently, and safely, (often conflicting goals) much research has been developed taking into account human performance, technological possibilities, types/levels of automation in a system, design of human–machine interfaces, etc. (see Parasuraman et al., 2000; Sheridan, 2002; Woods,1996; Nachreiner et al., 2006).

The overall research aim is to investigate how advanced (digital) interfaces should be evaluated and designed in order to be used in the modernization of the analog instrumentation and human/system interface (HSI) systems. The research presented in this article focused on the development of operator support systems during emergency situations. In particular, we focused on crucial safety problems related to the design and layout of the graphics on the screen, and the layout and informativeness of the alarm system.

2. The ergonomics in HSI design

The HSI design of advanced interfaces must use a human-centered approach based on ergonomics, to exploit the technical innovations for the optimum human – artifact interactions, aiming at improving the appropriateness of the technological solutions (Hancock and Chignell 1995). Innovations in technology should be used to enhance the shared human intelligence and the possibilities for human to interact with the environment. The HSI design is especially important in processes of modernization of old analog instrumentation and control systems, as is happening in Brazilian nuclear power plants. As noted by many authors (e.g., Bainbridge 1987; Zuboff, 1988), the development of technology is usually comprehended from the point of view of its capability of replacing human work by automation. Yet, by improving measurements, transmission, copying and representation of
information, new technology also increases the role of information displays as the mediator between the human actor and the object of activity. Advanced controls that automate large portions of control tasks complicates interpretation of the state of the environment and calls for improved intellectual skills. Hence, it is the new technology’s ability of to inform that paradoxically emphasizes the role of the human and the need of the human-centered approach for HSI design.

Some of the most important consequences of a transition from the traditional analogue instrumentation and control technology to digital technology transition with regard to the HSI are:

− Large amounts of process information and an abundance of alarm information in disturbance situations challenge the operators’ comprehension of the process state and its expected course in operational situations. The term “situation awareness” is often used for this complex of activities (Endsley 1995, Endsley & Garland 2000);
− The space for information presentation is small which necessitates a sequential use of information (the keyhole effect; Woods 1995; Guerlain, 2007);
− “Soft control” is expected to increase secondary tasks which may increase mental effort and work load (Pirus 2003; Woods 1995b);
− Feedback from the system must be optimized. Too fast and inappropriate feedback may increase mental load (Norman, 1990; O’Hara, 2003);
− Systems may fail, understanding the functions of automated systems must be ensured (O’Hara, 2003);
− Identifying, correcting and recovering from errors may become more difficult which endangers the reliability of the sociotechnical system (O’Hara 2003).

3. Method

3.1 Research setting

The research has been carried out in the Human System Interface Laboratory (LABIHS). The LABIHS facility conducts research on human-system interaction in the nuclear power domain. Its goal is to improve user interface support for operator tasks, with the intention of promoting safer and more efficient NPP operation after the modernization processes. The LABIHS simulates, in an advanced (digital) control room (figure 1), physical processes that are similar to the ANGRA I Brazilian first constructed nuclear power plant. The construction of ANGRA I started in 1972, the first criticality (the first fission reaction in the reactor core) occurred in 1982, and the plant commercial operation started in 1985. Since then, it has generated 40 million MWh of electric energy. The plant nowadays is replacing the steam generator and will continue in operation for at least the next 20 years, needing a modernization of control room systems.

The LABIHS’ advanced control room consists of nuclear reactor simulator software, graphical user interface design software, a hardware/software platform to run and provide the adequate communication between these software systems, and the operator interface - VDUs and controls needed to operate the simulated process.

To simulate the plant under study, a Westinghouse PWR digital compact simulator is used. The compact simulator provides a means of operations training in a simplified form. 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 a mouse and keyboard. An overview display, based on direct beam
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 the LABIHS architecture. The instructor station system uses a window-based multitasking menu-driven interface to provide real-time data and commands related to the simulated environment. Using the instruction station event scenarios can be simulated, including (small) loss of coolant accidents, total loss of electrical supply, steam generator tube rupture, and reactivity accidents.

![LABIHS control room](image)

**Figure 1 – LABIHS control room.**

### 3.2 Data collection and evaluation

The user-centered approach focuses on the LABIHS operator’s performance evaluation during selected tasks. Direct observations, interviews, and scenario evaluations are the techniques used to evaluate the performance in the LABIHS HSI. During 30 hours of observations, we observed how the operators interacted with the simulated PWR in various modes of operation. We paid particular attention to the tasks dictated by the procedure manual and to the operators’ actual activity. We searched 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. Comprehensive debriefing interviews with the operators and supervisor were carried out to validate the findings.

**Participants.** One operator crew participated in this research under different operating conditions: start up, planned shutdown and in postulated accidents. The LABIHS control room operating crew is composed of only 3 operators (different from the reference plant that has 5 operators) – the Shift Supervisor, Reactor Operator (RO) and the Secondary Circuit Operator (SCO). The panel operator that exists in the reference plant because of the bigger size of analog control panel, and Foreman responsible for administrative tasks are represented in the simulator crew. The Shift Supervisor has a deep background in nuclear engineering (D. Sc.), participated in the LABIHS’s HSI design and has extensive 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 but have no previous experience in the reference plant operation.

**Observation procedure.** The LABIHS is equipped with a ceiling-mounted camera which captures the majority of the room, including the two operators’ stations and the main projector, is also provided in the control room.
presentations screen. For this study, we also placed a tripod-mounted Mini-DV camcorder to record whichever operator would be likely to have the most active role. We also occasionally employed a hand-held digital camera to film particular details of interest that was 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. However, in many of the cases, the operators conducted the simulations without the supervisor present. In these cases, one analyst observed the overall proceeding and attempted to capture the communications and interactions between the two operators.

The operation of a nuclear power plant falls 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 focused on periods of higher activity. After discussion with the operators, we learned that startup induces the most activity, providing the best opportunity to build familiarity with the system. The startup phase can be further subdivided into four steps. Although these steps are not an inherent part of the physical system, they are clearly present in the minds of the operators and are reflected in the procedures, and thus constitute an important cognitive division of the system as a whole:

- Cold Shutdown to Hot Shutdown;
- Hot Shutdown to Hot Standby;
- Hot Standby to 2% Power (“Plant Startup”);
- Operations greater than 2% Power.

After observing startup simulations, we then observed several simulated incidents and accidents. 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 led the operators, to justify their actions verbally after the scenario was completed. We did not study the shutdown phase in depth, due to time limitations and its similarity to startup.

Heuristic and scenario based evaluation. Based on the observations results, we evaluated the original LABIHS displays using heuristic techniques, (Nielsen, 1993). The heuristic evaluation focused on evaluating the graphic designs, usability and consistency of the existing displays and the navigation among screens. We also noted the use of non-computer-based information (e.g., paper procedures). The goal of the analysis was to determine whether the current tools supported operator tasks as observed. The new displays, developed after the study recommendations, were preliminary evaluated using a scenario-based performance comparison, using the original design as a performance benchmark.

4. Results

4.1 Graphic design evaluation

Figure 2 shows a typical control screen 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 R…, C…, P… (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 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 (Besnard and Greathead, 2003). 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.

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. 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.

4.2 Alarm system evaluation
It has been said that nuclear plant operation is characterized by 99% boredom and 1% panic. The 99% boredom of continuous normal operation requires effective surveillance and long term control strategies. The 1% panic requires means and measures that are entirely different from those that are adequate for normal or slightly disturbed situations. Situations like alarm flooding are well known (Woods, 1995a; Carvalho et al., 2006), but the HSI designers of nuclear plants or large chemical complexes still design alarm systems to function well only during normal operation. As such, in this research we focused on how the simulator operators deal with alarms during emergency situations. 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. This arrangement reproduces in the simulator the main alarm annunciation tiles used in the reference plant. The alarms are located on two separate alarm screens. They are arranged as tiles in a grid where active alarms are indicated by a flashing red tile. The existing system does not support quick alarm identification. 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.

5. Recommendations for a new HSI prototype

The redesigned interface is based on the deficiencies noted in the previous section. 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.

5.1 Graphic Design Improvements

We propose several changes to the schematic-based control screens (for an example, see Fig. 3). These 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. 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.

![Figure 3 – The new CVCS display.](image)

5.2 Alarm System Improvements

The prototype includes an extensive revision of the original alarm system. The major changes are captured in the revised alarm screen (Fig. 4). 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. 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 (Fig. 8). 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.

![Figure 4 – The new alarm display.](image)

5.3 Scenario Evaluation of new prototype

The prototype has not yet been implemented, so scenario-based evaluation was used. To gauge performance, we evaluated the design using two representative scenarios. The LABIHS interface design provided the performance benchmark.

Stuck Valve Incident Scenario. The first scenario is a hypothetical incident involving a stuck valve with a malfunctioning indicator in the interface. In this scenario, the FV122 valve is in automatic mode and closed (correctly) due to high pressure in the pressurizer. When the pressurizer pressure drops, the FV122 valve is supposed to reopen. However, the valve is stuck closed. The interface (due to a glitch) incorrectly displays it as open. The initial symptom of this issue is the sounding of the Charging Flow Low (CFL) alarm. In the original design, when the alarm sounds one or both operators navigate to both of the alarm screens, noting the CFL alarm. One operator must then use the main menu to navigate to the CVCS screen to diagnose the problem. Seeing FV122 “open” and automatic, the operator may check FV616 and the charging pumps. Seeing these open and on, respectively, the operator may check the Volume Control Tank (waiting to see up or down movement). At this point the operator may request field verification of the computer readings. This would identify that FV122 is closed, contrary to the interface display.

In the redesigned interface, only the reactor operator goes to the alarm screen because the alarm bar shows that the problem is in the CVCS screen, which is the reactor operator’s responsibility. With only one alarm screen, one click allows the operator to observe the CFL alarm. The alarm arrangement and tile timer informs the operator which screens to go to and how long the alarm has been sounding. The trends on the alarm screen give a graphical representation of the magnitude of the problem, whether it is likely to become worse, and, if so, at what rate. With just these trends, the operator may begin to hypothesize the root problem even before navigating to the CVCS screen. For example, the Volume Control Tank
graph displaying a downward trend coupled with the low charging flow could indicate a leak on the outflow side, whereas an upward trend could indicate a closed valve on outflow side. At this point the operator navigates to the CVCS screen to diagnose the problem. The operator can go to the CVCS screen by clicking on the blinking alarm instead of having to use the main menu. Upon arrival, the flashing red box will direct the operator’s attention to the alarm’s trigger, in this case the charging flow indicator. Depending on the simulator logic, the gray colored piping may show that flow is not going through FV122, pin-pointing the root problem.

Loss of Coolant Accident Scenario. A loss of coolant accident (LOCA) occurs when there is a pipe rupture in the Reactor Coolant System (RCS). This causes the reactor to trip (shutting down power production) automatically. The 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 mediumbreak 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).

The redesign addresses this issue by putting the flow diagram and the currently selected node’s response instructions. The redesign requires no page turns, and since it is linked to the alarm system, the operator does not have to search for the appropriate binder or page number.

6. Conclusions

The human factors/ergonomics requirements for 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 a part of the produced system (the human system interface - HSI) in order to validate the design solutions taken during the design phase. The methodology used was based on field studies and observations of the operators’ performance in the LABIHS simulators. 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 sooner 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 I&C has not started yet this objective is already achieved in this research.

Even considering that is very difficult to say when the performance of the joint cognitive system is at an acceptable level, our evaluation has shown some improvement possibilities in the HSI original design. Some of them are related to basic ergonomic design principles like:

- 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 an affect on the usage. Considering that, we claim that the design solutions should be made considering the appropriate use of the system, emphasizing that work practices in complex industrial settings should not be based on the notion of human as the weakest link in the system and in applying the left over principle. We need 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 of 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.

Acknowledgements

The authors gratefully acknowledge the support of National Advice of Scientific and Technological Development (CNPQ - Conselho Nacional de Desenvolvimento Científico e Tecnológico) and CAPES/FIPES. The research was performed at Instrumentation and Human Reliability Division of the Nuclear Engineering Institute, Brazil (DICH / IEN).

References


