BNL-NUREG-63202

CONF-960989--2

HUMAN FACTORS CHALLENGES FOR ADVANCED PROCESS CONTROL[1]

William F. Stubler
John M. O'Hara

Brookhaven National Laboratory
Upton, New York 11973 USA

To be presented at the
Annual Meeting of the Human Factors and Ergonomics Society
Philadelphia, PA
September 2-6, 1996

[1]This paper is based on research conducted under the sponsorship of the U.S. Nuclear Regulatory Commission. The views presented in this paper represent those of the authors alone, and not necessarily those of the NRC.

HUMAN FACTORS CHALLENGES FOR ADVANCED PROCESS CONTROL[1]

William F. Stubler
John M. O'Hara
Brookhaven National Laboratory
Upton, New York, 11973

New human-system interface technologies provide opportunities for improving operator and plant performance. However, if these technologies are not properly implemented, they may introduce new challenges to performance and safety. This paper reports the results from a survey of human factors considerations that arise in the implementation of advanced human-system interface technologies in process control and other complex systems. General trends were identified for several areas based on a review of technical literature and a combination of interviews and site visits with process control organizations. Human factors considerations are discussed for two of these areas, automation and controls.

INTRODUCTION

Human-system interface (HSI) technologies for process control have exhibited rapid and significant advances in the past decade. Existing facilities are replacing or significantly upgrading analog control systems with digital control systems. Conventional technologies (e.g., broad panels and hardwired instruments) have given way to digital instrumentation and control (I&C) and computer-based HSI technologies. Designs for new facilities are largely based on these technologies. In the nuclear power industry, advanced digital control systems and HSI technologies are major features in the latest generation of light water reactors that are under development and in upgrades of existing plants. Potential benefits of these technologies include improved plant reliability, operating performance, and safety and reduced operator workload. However, if these technologies are not properly implemented, they may introduce new challenges to performance and safety (National Academy of Science, 1995; O'Hara and Brown, 1994; Stubler, Roth, and Mumaw, 1991).

Brookhaven National Laboratory, under sponsorship of the U. S. Nuclear Regulatory Commission (NRC), is currently engaged in a project to identify human factors considerations associated with these technology changes. The objective of this project is to evaluate the significance of these considerations to nuclear power plant safety and support the development of human factors review guidance, where needed, to augment existing guidance, such as the Human System Interface Design Review Guideline (O'Hara, Brown, Stubler, Wachtel, and Persensky, 1996). The first phase of this project included a survey of human factors considerations associated with trends in advanced HSI technologies and digital control systems for a range of complex human-machine systems, especially in the process control domain. While the details of specific tasks in other industries may be different from those in nuclear power plants, the general demands placed on personnel for monitoring, fault detection, diagnosis, decision-making, and response selection and execution are quite similar across many complex human-machine systems. Operating experience and empirical studies were key sources of information. This paper describes the survey of human factors considerations and some key findings.

METHODOLOGY

The primary means of data collection were a review of technical literature and a combination of interviews and site visits with organizations and individuals having experience with advanced HSI and control system technologies. The literature review consisted of a focused review of system design descriptions, HSI-related human performance research, and HSI-related operational events. This literature addressed new control room designs as well as specific HSI technologies. The focus was on defining design trends and potential human performance issues.

Telephone and on-site interviews were conducted with plant personnel, control room technology manufacturers, and U.S. and foreign nuclear regulatory agencies.

[1] This paper is based on research conducted under the sponsorship of the U.S. Nuclear Regulatory Commission. The views presented in this paper represent those of the authors alone, and not necessarily those of the NRC.

Visits to operating facilities provided the opportunity to view the use of the HSI technologies and interview operations, maintenance, training, and I&C design personnel. These visits included one nuclear power plant that had been recently upgraded; two nuclear power plant training simulators; two multi-unit fossil fuel power plants with control rooms that range from fully-integrated, advanced designs to traditional analog designs; and two multi-unit petrochemical plants with fully-digital control systems. Interviews were conducted using a semi-structured format that addressed specific HSI and control system technologies and the process by which the upgrades were implemented.

FINDINGS

The review found trends in the following areas for fully-integrated, digital HSIs:

- Enhanced automation for plant control and protection functions
- Computer-based controls (e.g., via mouse, keyboard, and touch screen)
- Computer-based alarm systems
- Computer-based, graphical displays
- CRT, flat panel, and large-screen display devices
- Compact workstations or consoles for operators and supervisors
- Multi-unit control rooms (e.g., control centers for two to four plants are located in one room).

While some facilities have undergone complete replacements of their control rooms with advanced digital HSI technologies, other facilities have chosen to upgrade selected portions of their control rooms. These are called hybrid control rooms because they contain mixtures of technologies (e.g., hardwired, analog interfaces and computer-based, digital technologies). Our findings related to two of these areas, automation and computer-based controls, are discussed below.

Changes In Automation

Characteristics of automatic control systems being implemented in process control industries include:

- Multiple plant components, which were formerly controlled separately, are now controlled together via higher-level control capabilities.
- Multiple variables are integrated and processed to provide more precise control capabilities (e.g., advanced control, multi-variable control).
- Alignment of plant equipment, such as fluid or electrical systems, is performed automatically.

These capabilities are complemented by digital control systems that maintain variables within closer control ranges (e.g., less oscillation and drift), increase or decrease variables at a rate set by the operator (e.g., programmable ramp rate), and provide automatic testing, calibrating, and validating of sensor data. Increases in automation has tended to move the operator away from direct involvement in the control of the system to one of a supervisor, who monitors the status and performance of automatic control systems.

The following are some of the human performance considerations associated with automated systems:

Automation Complexity and the Operator's Mental Model. The introduction of automation often increases the complexity of the plant design and, thus, may place higher demands upon personnel for understanding how the plant works. Problems may arise because the operator lacks a good mental model of the behavior of the automated system, i.e., why it does what it does. Operators need to understand how information is processed by the automated system so they can determine whether the output is appropriate for the task situation and to determine whether the automated system is operating properly.

The lack of a proper mental model of how an automated system works may result in operator actions that bypass the automated system. For example, as automatic control systems use more complicated rules or strategies for processing input and developing outputs, operator understanding of and confidence in these systems may decrease. Operators may conclude that the automatic control system has malfunctioned, when it is in fact operating correctly. Experience in various process control domains has indicated that operators may revert to manual control and maintenance personnel may bypass (disable) automatic systems when they lack confidence that the automatic control system will operate correctly. Better means are needed to provide personnel with accurate mental models of how these automated systems function.

The lack of a proper mental model of how an automated system works may also result in operator actions that produce unexpected consequences. Problems may include: (1) intended actions that were improperly planned, and (2) unintended-unanticipated operator actions. The following is an example of an intended action that was improperly planned. A digital system was controlling a batch reaction on a chemical plant during the night when daylight savings time ended and the clocks had to be set back by one hour. When the operator reset the clock of the digital control system so that it indicated 2:00 AM instead of 3:00 AM, the digital control system shutdown the plant for one hour until the clock indicated 3:00 AM again (Kletz, 1993). This event occurred because the application engineer at the plant did not fully understand the requirements of the control system design or the operator's needs in the task environment. As a result, inadequate instructions were provided to the operator.

An example of unintended-unanticipated operator action occurred at a non-power reactor. A trainee simultaneously depressed a "Pulse" mode button and an "Up" button for control rod withdrawal. The result was that a rod was driven out of the core, a rod movement that was inconsistent with a rod withdrawal interlock for that mode of operation. The withdrawal continued even after the "Up" button was released. This continued withdrawal is inconsistent with the design intent of the control system. This problem had not been previously discovered because it was thought to be inconsistent with the operational design of the reactor and the buttons were located on the console in such a way that it would be unusual to depress the two simultaneously (NRC, 1993).

Feedback from the Automated System and Situation Awareness. Many problems associated with human interaction with automated systems have been attributed to poor situation awareness. Awareness of the status of the plant and the control systems is difficult to maintain in highly automated systems because the operator is largely removed from the control loop. This situation stems, in part, from inadequate feedback to the operator regarding the status of the automatic system (Norman, 1990). Three types of events resulting from inadequate feedback from automatic systems may include: (1) lack of operator awareness of a slowly degrading system for which an automatic control system is compensating, (2) system lockups with an absence of indication, and (3) mode errors.

Detection of systems that are experiencing slow degradation has been a contributing factor in events in many complex human machine systems, including commercial aviation (Norman, 1990; Bainbridge, 1987). Monitoring for system degradation may be difficult with advanced automation because the function of automatic control systems is to maintain a specific level of performance. Thus, automation tends to mask the symptoms of degradation such that the operator may not become aware of the degraded condition until it exceeds the capabilities of the automatic control system. This problem occurs in process control because the sensors for alarms and displays tend to measure plant process state (e.g., flows, pressures, temperatures) rather than the condition of the plant equipment. New alarm systems are exploring ways of detecting the early stages of problem states, such as initiating alarms for plant process variables that are experiencing unusual oscillations or trending toward alarm setpoints (Davey, Feher, and Guo, 1995). However, little automated support currently exists for assisting the operator in detecting mismatches between equipment states and plant process variables (e.g., the controller demands a valve to be fully open but the flow is minimal).

Lockups, with an absence of indication, is a failure mode to which digital control systems are susceptible. Often, when the control system for an analog indicator fails, the needle of the indicator falls to the bottom of the scale (e.g., to zero). This provides the operator with an indication that a failure has occurred. When digital control systems lock up (e.g., processors either stop processing or perform infinite calculations), there may be no obvious indications for the operators. Lockups may be caused by many things including a power interruption, voltage change, or improper operator input. Operators may not be aware that a failure has occurred because the display may have stopped at a reading that is in the normal operating range. (Digital control systems do have alarms for failures of digital processors, but these alarms may not address all cases or always operate as intended.) If a control system lockup occurs after a component has received a signal to actuate but before the movement is complete, then the operator may not have good indication of the state of the component. For example, if the control system locks-up after a closed valve receives a signal to open, it may be difficult for the operator to determine whether the valve is closed, open, or partially open. In two events involving lockups of plant alarm systems, the failures were not detected until other plant anomalies were brought to the attention of the operators by other means (Galletti, 1996).

Mode errors are an increasing phenomenon associated with automated systems (Woods, Johannesen, Cook and Sarter, 1994). Automated systems may have multiple modes in which the inputs used by the automated system and output provided by the automated system are different. As a result, a system's response to plant conditions or operator inputs may be different depending upon the characteristics of the current operating mode. Undesirable events may occur when the operator expects the automatic system to respond in a certain way to plant conditions or an operator input, but the system responds differently. System designs that feature multiple modes increase memory and knowledge demands because the operator must know and remember the effects of inputs and the meanings of indications for the current mode. Also, demands on situation assessment and awareness are increased because the operator must maintain awareness of the current mode and actions or conditions that may change it. The difficulties associated with these demands are largely determined by the quality of feedback regarding mode status that is provided by the control system, characteristics of agents (e.g., crew members and plant systems) that interact with the system, and task context (e.g., time pressure, workload, and multiple interleaving tasks).

Vigilance, Workload, and Skill. Another effect of utomation on personnel performance stems from the omewhat paradoxical relationship between the skills that n operator needs to understand and supervise automated ystems and the day-to-day monitoring tasks they are equired to perform. Monitoring is often considered omething people do not do particularly well because igilance is difficult to maintain. Monitoring plant variables nd detection of anomalies requires operator alertness. Iowever, because automated control systems tend to emove the operator from direct control of the plant, perator alertness is often reduced. This lack of alertness nay contribute to the failure of the operator to detect a otential event in its early stages. While workload during eriods of normal operation may be low, high cognitive vorkload often results during process disturbances. The vorkload associated with transitions from monitoring utomated systems to assuming manual control during a ault in an automated system may be extraordinary. urther, due to lack of practice, there is a potential erosion f the skills required to perform the task in the event of utomated system failure. These workload demands and otential erosion of the skills may greatly complicate perator response to the event.

omputer-Based Controls

Many digital control systems feature computer-ased ("soft") controls. Some attributes of soft controls nclude connections with the control system that are medi-ted by software rather than direct physical connections, unctions that are variable and context-dependant rather nan statically defined, and device locations that are virtual e.g., within the display system structure) rather than patially dedicated. Control actions may be performed hrough soft controls in a variety of ways such as:

- Direct manipulation of virtual devices (e.g., push buttons on a display screen) using a pointing interface, such as a touch screen, mouse, trackball, or light pen.
- Entry of commands or data via keyboard (e.g., typing a controller setpoint)
- Manipulation of physical control devices that perform variable functions (e.g., a push button that has a fixed location and functions that are defined by the operating context).

wo human performance considerations associated with oft controls are: (1) control action slips, and (2) control xecution constraints.

Slips may be defined as errors in which one action s intended but another is done (Norman, 1981 & 1983). oft controls have characteristics that may increase the ikelihood of a control action slip occurring, compared to conventional controls. One type of slip, description errors, occurs when the appropriate action is not sufficiently described by the user interface. One example is "wrong control component" errors. When control actions are executed via a multi-purpose interface such as a CRT or a programmable digital controller, operators sometimes select the wrong control point in a plant system (e.g., a similar looking component in another control loop). Thus, they provide control input to the wrong system component (Shaw, 1993). Conventional hardwired controls have spatially-fixed locations in the control panel, which provide the operator with cues about their identity and function. For example, they are often spatially organized by plant systems. Also, the use of diverse physical input devices with different input methods (e.g., pushing buttons, turning knobs) provides operators with a rich variety of tactile cues to prevent slips associated with activating the wrong control. These cues may be much less effective or non-existent in soft controls. Soft controls tend to have virtual rather than physical locations and their input methods tend to be more limited; i.e., button pushes and key presses. The lack of visual distinctness of soft controls may also contribute to wrong component errors. This problem is aggravated by the reuse of display formats (e.g., control input devices and representations of system components in a control loop) to save user interface development costs. These similarities may increase the likelihood of errors.

Slips also occur in tasks that require actions to be performed in a particular sequence. Sequence-related control errors include omitting steps and performing steps in the wrong order. These errors may occur as a result of delays in system response or interruptions from competing tasks (Shaw, 1993). They may also result from capture errors (Norman, 1981) in which the required sequence of operation is very similar to but different from another, well-practiced sequence. Capture errors can result in operators performing a well-practiced sequence rather than the desired sequence, which may result in undesirable manipulations of controlled equipment. The likelihood of capture errors may be greater when a standard dialog style for human-computer interaction is not consistently applied within or across HSI components.

Other control action slips, which may arise from characteristics of the HSI design, include data entry errors and accidental activations. Data entry errors can result in errors of magnitude when providing input values. For example, analog controllers often require the operator to turn a knob to obtain a setpoint value. The rotation of the knob causes the values to be changed sequentially and the number of turns provides the operator with feedback regarding the degree to which the setpoint has been changed from its last value. When this input operation is replaced by a keyboard, large input errors may be made by transposing digits or adding or deleting digits. Also, the keyboard provides little tactile feedback regarding the magnitude of the input value. Some factors that contribute to accidental activations include inadequate activation logic (e.g., failure to use a scheme that causes the button to be activated upon release of the pointing interface), poorly demarcated buttons, and ineffective verification steps.

Control execution constraints refer to operator burdens associated with control actions that are performed via computer-based user interfaces. Control actions performed through a computer-based user interface usually must be performed as a series of steps. For example, first a control loop must be selected. This is often performed by positioning a pointing device over a symbol that represents the desired plant component. Then a control input field must be accessed, such as a window that displays the current control settings and input fields for changing these settings. Then the operator must provide a command or a control value to each input field (e.g., via buttons or a keyboard). Finally, the operator may have to verify that the inputs are correct. These steps must be repeated for each control action. Although the time required for each control action may not be large, the overall effect of the sequential access and operation of controls may be disruptive, especially when multiple components must be controlled simultaneously or in rapid succession. This may impede the ability of operators to respond quickly in high-tempo situations, such as an upset condition (Shaw, 1993).

CONCLUSION

The human factors considerations described in this paper for automation and computer-based controls, as well as the other areas identified through the survey, are being evaluated for importance to nuclear power plants. These considerations may also be relevant to other new process control facilities and existing facilities as they are upgraded or modernized. These considerations may be important when facilities upgrade portions of their control rooms, rather than performing total replacements, because the resulting hybrid design is likely to contain a mixture of HSI technologies with different characteristics and modes of operation. Upgrades that are not designed in an integrated fashion (e.g., do not strive for consistency in information retrieval and control execution and do not share information effectively between components) may place additional burdens on plant personnel.

REFERENCES

Bainbridge, L. (1987). Ironies of automation. In J. Rasmussen, K. Duncan, and J. Leplat (Eds.), *New Technology and Human Error* (pp. 271-283). New York: Wiley.

Davey, E. C., Feher, M. P., and Guo, K. Q. (1995). An improved annunciation strategy for CANDU plants. In *Proceedings of the Topical Meeting on Computer-Based Human Support Systems: Technology, Methods, and Future* (pp. 321-328). La Grange Park, Ill.: American Nuclear Society.

Galletti, G. S. (1996). Human factors issues in digital system design and implementation. In *Proceedings of the 1996 American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies.* La Grange Park, IL: American Nuclear Society.

National Academy of Science (1995). *Digital instrumentation and control systems in nuclear power plants: Safety and reliability issues.* Washington, D. C.: National Academy Press.

Kletz, T.A. (1993). Computer Control - Living with Human Error. *Reliability Engineering and System Safety, 39* (3), 257-261.

NRC (1993). NRC Information Notice 93-57: *Software Problems Involving Digital Control Console Systems at Non-Power Reactors.* Washington, D.C.: Nuclear Regulatory Commission.

Norman, D. (1990). The "problem" with automation: Inappropriate feedback and interaction, not 'over-automation'. *Philosophical Transactions of the Royal Society of London, 377*, 585-593.

Norman, D. (1983). Design rules based on analyses of human error. *Communications of the ACM, 26*, 254-258

Norman, D. (1981). Categorization of action slips, *Psychological Review, 88*, 1-15.

O'Hara, J., Brown, W., Stubler, W., Wachtel, J., and Persensky, J. (1996). *Human system interface design review guideline* (NUREG-0700, Rev 1.). Washington, D.C.: U.S. Nuclear Regulatory Commission.

O'Hara, J. and Brown, W. (1994). *Advanced Human-System Interface Design Review Guideline* (NUREG/CR-5908). Washington, D.C: Nuclear Regulatory Commission.

Shaw, J. (1993). Distributed control systems: Cause or cure of operator errors. *Reliability Engineering & System Safety, 39*(3), 263-271.

Stubler, W. F., Roth, E. M, and Mumaw, R. J. (1991). Evaluation issues for computer-based control rooms. In *Proceedings of the Human Factors Society 35th Annual Meeting* (pp 383-387). Santa Monica, CA: Human Factors Society.

Woods, D., Johannesen, L., Cook, R., and Sarter, N. (1994). *Behind human error: Cognitive systems, computers, and hindsight* (CSERIAC SOAR 94-01). Wright Patterson Air Force Base, Ohio: Crew Systems Ergonomics Information Analysis Center.