ANL/CP--75335

DE92 011839

A STRATEGY FOR MINIMIZING COMMON MODE HUMAN ERROR IN EXECUTING CRITICAL FUNCTIONS AND TASKS

Leo Beltracchi
U. S. Nuclear Regulatory Commission

and

Richard W. Lindsay
Argonne National Laboratory
P.O. Box 2528
Idaho Falls, Idaho 83403-2528

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

The submitted manuscript has been authored by a contractor of the U. S. Government under contract No. W-31-109-ENG-38. Accordingly, the U. S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U. S. Government purposes.

For Presentation at the
8th
Power Plant Dynamics, Control & Testing
Symposium

May 27-29, 1992
Knoxville, Tennessee

A STRATEGY FOR MINIMIZING COMMON MODE HUMAN ERROR IN EXECUTING CRITICAL FUNCTIONS AND TASKS

Leo Beltracchi, U S Nuclear Regulatory Commission

and

Richard W. Lindsay, Argonne National Laboratory

ABSTRACT

Human error in the execution of critical functions and tasks can be costly. The Three Mile Island and the Chernobyl Accidents are examples of results from human error in the nuclear industry. There are similar errors that could no doubt be cited from other industries. This paper discusses a strategy to minimize common mode human error in the execution of critical functions and tasks. The strategy consists of the use of human redundancy, and also diversity in human cognitive behavior: skill-, rule-, and knowledge-based behavior. The authors contend that the use of diversity in human cognitive behavior is possible, and it minimizes common mode error.

The opinions and viewpoints herein are the author's, and do not necessarily reflect the criteria, requirements and guidelines of the US Nuclear Regulatory Commission, nor the US Department of Energy.

INTRODUCTION

Prevention of error in large, complex industrial facilities such as nuclear plants is a mandatory requirement because of several factors. Plant personnel and public safety are the prime considerations in error prevention, and economic factors also are important considerations. Requirements for operational excellence are driven by economics and by the unacceptability of plant accidents. New technologies such as computers, and better understanding of large systems are supposed to provide the "tools" to minimize error.

With all the new tools available, errors continue to occur, and often the efforts made to eliminate the errors either are not, or are marginally productive. Humans still make errors at about the same rate as always (under the same conditions), yet there are many reasons why human error must be reduced in critical functions.

The Three Mile Island and the Chernobyl Accidents are costly examples of the results of human error. Each accident appears to have included several knowledgeable persons, but each group appears to have suffered from a "group" mind set, or common-mode failure where a single (erroneous) conclusion as to the conditions of a system is shared by all involved at the scene.

In critical hardware applications, such as plant protection and control systems, both redundancy and diversity are often used to insure against common mode or other types of failures. Redundancy is often used in human activities to ensure proper action, but diversity in human cognition can and often should also be used to avoid common-mode (mind set) failure problems. The problem, to date, has often been one of not knowing how to explicitly provide for or encourage diversity in human monitoring of processes.

The authors contend that it is possible to provide both redundancy and diversity in human operator behavior through the use of two persons (in critical functions) which provides the redundancy, and by using two different types of cognitive behavior which provide the diversity. If successful, this approach provides a means to prevent "mind set" or common-mode failure in humans.

As an example, the use of a step-by-step procedure by an operator typically results in rule-based behavior. To elicit knowledge-based behavior, a task may be described where the end objective is stated, and where the operator then must determine how to accomplish the task. The use of two different people, using two different types of cognitive behavior should provide both the diversity and redundancy required for human error reduction in important operations.

Much work has been done in an effort to understand human errors. For example, Rasmussen and Vicente (1) have categorized human cognitive errors and suggested means of overcoming many of these errors. They have categorized errors as follows:

1. Errors related to learning and adaptation;
2. Interference among competing cognitive control structures;
3. Lack of resources;
4. Intrinsic human variability.

They develop a variety of design guidelines for dealing with these types of error categories. These guidelines serve as the basis of the ecological interface design theory. Their theory of interface design accounts for and supports human cognition in skill-, rule-, and knowledge-based behavior. Their work strives to deal with the systemic errors in human cognition. Human behavioral theory also recognizes that it is impossible to eliminate human error because of the intrinsic human variability in performing tasks.

In a later effort, Rasmussen and Vicente (2) provide further guidance on the development of ecological interfaces. In this work, they provide a top-down design method for the development of an ecological interface. The method consists of the means-ends levels of control tasks. The various levels of the hierarchy are: 1) goals, 2) abstract function, 3) general function, 4) physical processes of equipment and components, and 5) form, location, and configuration of equipment.

Beltracchi (3) proposes an interface based on the means-ends levels of control tasks. The proposed interface aids operators in monitoring the performance of a pressurized water reactor. The abstract basis of the proposed interface is the thermodynamic law for the conservation of energy, and conservation of mass. This type of interface models operation of the plant process and plant systems. In modeling the plant, the interface aids the operator in monitoring normal and abnormal operation.

Lindsay (4) reports on the operation of a model-based display at the Experimental Breeder Reactor - II. The display incorporates information from plant sensors to form a thermodynamic model of the plant's process. The thermodynamics of the plant are depicted through the use of iconic figures, animated by plant signals, that are related to the major plant components and systems such as the reactor, intermediate heat exchanger, secondary system, evaporators, superheaters, steam system, steam drum, and turbine-generator. This display supports knowledge-based, rule-based, and skill-based reasoning for the operator.

In this work, among other things, the authors propose a strategy for operator use of an ecological interface. The purpose of the strategy is to minimize human errors in the execution of critical functions and tasks.

DISCUSSION

Automation of functions and tasks performed by humans is one method of minimizing human error. Functions and tasks that are well defined and require precision in execution are candidates for automation. For example, an automatic process control system performs a process control function with repeatable precision. Manual control of the process control function is often not as effective because of the variability or limitations in human performance.

However, automation is not the answer for all functions and tasks performed by humans. For example, human reasoning based on first principles in diagnosing a problem may not be automated as yet. Expert systems may aid a human in diagnosing a plant fault provided the system's knowledge base contains information on the fault. However, expert systems do not reason independently and adaptively based on first principles. Thus, knowledge-based behavior, as performed by humans, is, at present, generally not appropriate for automation.

Most skill and rule-based behavior performed by humans can be automated (although sometimes at a high price). To minimize errors, a human must be trained and experienced in skill- and rule-based functions and tasks. Another approach to minimize human error is to automate skill- and rule-based functions and tasks. However, it may not be cost effective or desirable to automate all skill- and rule-based tasks performed by humans. Automating all these tasks may erect barriers between the human and the facility monitored and controlled by the human.

Cognitive Behavior

Skill-based behavior is automatic; perception of a situation initiates human response without cognitive effort. On the other hand, rule-based behavior requires cognitive effort. In rule-based behavior, a match of symptoms results in the selection and execution of a procedure. Another example of rule-based behavior is the recall and use of heuristics stored in human memory. Rule-based behavior is not automatic, rather, it is deliberate and usually requires skills to execute efficiently.

Knowledge-based behavior is the most difficult of the cognitive behaviors. Reasoning based on the application of first principles and planning based on the performance characteristics of systems are examples of this behavior. Diagnosis of any unexpected failure is another example of knowledge-based reasoning.

The authors have noted that humans can perform two of the types of cognitive behaviors in near real time, skill and rule, or skill and knowledge. For example, a human may perform skill-based behavior and rule-based behavior simultaneously as in executing a procedure, where an operator performs many tasks automatically while reading and executing a procedure. Similarly, knowledge-based behavior can virtually coexist with skill-based behavior. An example would be where an operator determines a course to take by deliberate cognitive application, 'and then take the skill-based action virtually at the same time as the decision is made. Simultaneous use of knowledge-based and rule-based behavior may be a bit more difficult.

In using a personal computer-based word processor, an engineer performs knowledge-based behavior in composing a document and skill-based behavior in typing the document. This is another example of two types of cognitive behavior in near real time.
In each example of dual cognitive behavior, skill-based behavior is common. Normally, humans are single channel processors of information. However, dual mode processing is achievable because skill-based behavior is automatic and requires no apparent cognitive effort.

Based on this logic, it is then clear that humans are poor at performing rule- and knowledge-based behavior in near real time (simultaneously). Also, as the human is a single channel processor and each type of behavior, except skill-based, requires significant concentration, a human does not simultaneously perform rule- and knowledge-based behavior. It is thus logical to expect human errors when situations force the simultaneous use of rule- and knowledge-based behavior. Unless easily recognized, it is difficult for one to switch from rule- to knowledge-based behavior. To overcome these limitations, the authors propose the use of cognitive diversity.

Cognitive Diversity

The object of the following strategy is to minimize human error. Where two individuals are involved in an operation, such as controlling a nuclear plant with, for example, one person the operator and the other the supervisor, cognitive diversity should be required for critical tasks and functions. Instead of expecting a supervisor to follow a plant evolution by following the step- by-step procedures (rule based behavior) as does the operator, the supervisor should follow the operation by referring to information about the process at a level where he or she deduces proper, acceptable operation based on a knowledge of the process. This knowledge-based behavior could be reinforced by the displays presented to the supervisor wherein the display provides a model of the plant or system operation (such as a thermodynamic model). It may even be possible and desirable to write knowledge-based operational procedures for supervisory personnel as a method of reinforcing the use of cognitive diversity.

Another example could be considered from maintenance activities. A supervisor performs at least one higher level of cognitive work (e.g., rule-based behavior) in monitoring and validating a subordinate's lower level of cognitive work (e.g., skill-based behavior). For example, the supervisor could note that the maintenance technician is turning a valve the wrong direction (rule: to open, turn counterclockwise; to close clockwise), rather than simply checking the step: "Close Valve V202" as completed because he/she saw the technician move the valve actuator.

The above example is a simple one. A more complex, and "true to life" example could be where the technician is isolating a system and hanging red tags for maintenance. The technician follows an approved procedure, isolates the system and hangs the tags (rule-based behavior). As a practical matter, the technician knows that the procedure has been examined by many people, most of whom are higher in the management structure than the technician. This tends to encourage the technician not to question the procedures. If the supervisor assigned to check the job has a procedure that is not rule based, but rather is knowledge-based, then a cognitive diversity results. A knowledge-based procedure in this case could include an objective statement, and a schematic of the system and its control and power systems. The supervisor would be required to indicate on the schematic which valves, power supplies, etc. were isolated and tagged. This requires a much different approach to verification than merely repeating the rule-based procedure or even a shortened check list. With this type of cognitive strategy, there should be less chance of common-mode error because of functional diversity in cognitive behavior.

This approach is similar to the logic used to avoid common mode failure in the design of redundant hardware systems used in critical applications such as safety systems of nuclear power plants. Hardware diversity in redundant systems established a defense against common mode failure. The application of the diversity principle to humans results in different types of cognitive behavior.

There are some other interesting facets to this concept. One facet is how to use expert systems. An expert system may be viewed as a synthesizer of human rule-based behavior. If a human user unquestionably follows the results given by an expert system, the system has the locus of control. In most situations, a novice user of the expert system will perform almost as well as a human in following the results presented by the expert system. There is a danger in this approach as an expert system's knowledge base is finite and more or less rigid. Further, some of its knowledge base may be faulty, just as a human's knowledge base may be faulty. A novice user of an expert system may fall prey to these limitations.

One approach to overcome the above problem is to have the user of the expert system perform knowledge-based reasoning to validate the results of the expert system before using them. The user of course must have the mental resource capability to do this reasoning. This also means the user is not a novice. The question may arise, 'why use an expert system in the first place'? The answer is speed and consistency in obtaining results, and the diversity of using a rule-base (expert system) and knowledge-base (human), but of course subject to the limitations stated above.

There is a limit to the above strategy. When the strategy requires only the use of knowledge-based behavior, there is no higher level of functional performance to provide diversity. The human performance here will depend on the robustness of the mental resources brought to the problem. This also provides a reasonable paradigm for the identification of the need for rule based behaviors, such as the use of check sheets, procedures, etc.

If the assumption is made that the beginning of the design of a project such as a nuclear plant is based on knowledge, such as the application of first principles by the system designer, and that the methods of operation are also, in the beginning, based on knowledge, then it should follow that careful examination of the critical functions operators are to perform would require the preparation of check sheets or procedures to provide the proper diversity and redundancy. Similarly, any specific skills required to successfully perform operational duties should be identified and skill-based training provided. This approach also provides the opportunity for a top-down design method for training which originates in the first principles of the process. The traditional methodology springs from task analysis which is a bottom-up approach.

CONCLUSION

Human error is a fact of life. Proper design and training can help to reduce error to a low level which is often good enough for non-critical applications. However, for critical applications where either the safety and/or economic implications may be serious, human error cannot be tolerated. To date, the reduction of human error to zero has been, at best, a dream, and at worst a nightmare.

Understanding something about the types of human behavior: skill-based, rule-based, and knowledge-based, allows the designer to structure the human interface and/or procedures such that the chance for common-mode failure, or mindset is greatly reduced. Using a "backup" human has long been the approach to critical applications, where one person checks the work of another. The specific and deliberate use of different (diverse) cognitive behaviors during the redundant "check" operation has not been recognized for its potential in eliminating mind-set or common mode failure. The use of both human redundancy and diversity of cognitive behavior should serve to prevent unacceptable errors in critical applications.

REFERENCES

1. Rasmussen, J. and Vicente, K., "Cognitive Control of Human Errors: Implications for Ecological Interface Design," Fourth International Conference on Event Perception and Action, August 24-28, 1987, Trieste, Italy.

2. Rasmussen, J. and Vicente, K., "Ecological Interfaces; A Technological Imperative in High Tech Systems," To be published in: International Journal of Human Computer Interaction.

3. Beltracchi, L., "Conceptual Design of a Computer-Driven Display for Monitoring Reactor Coolant Mass", IEEE Transaction on Nuclear Science, Vol. 38, No. 3, pgs 923-935, June, 1991.

4. Lindsay, R., "A Display to Support Knowledge-Based Behavior," Advances in Human Factors Research on Man/Computer Interactions: Nuclear and Beyond, June 10-14, 1990, Nashville, TN.

END

DATE
FILMED
6/16/92