CONF-830658--1

DE83 014010

REVIEW OF DECISION AIDS FOR NUCLEAR-PLANT OPERATORS*

R. A. Kisner
Instrumentation and Controls Division
Oak Ridge National Laboratory
Oak Ridge, Tennessee

Paper for use at Workshop on Decision Processes
in Operation Planning and Fault Diagnosis
June 9-10, 1983
GA Technologies, Inc.
San Diego, California

*Research sponsored by Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission under Interagency Agreement DOE 40-550-75 with the U.S. Department of Energy under contract W-7405-eng-26 with the Union Carbide Corporation.

Review of Decision Aids for Nuclear-Plant Operators*

R. A. Kisner

Instrumentation and Controls Division
Oak Ridge National Laboratory
Oak Ridge, Tennessee 37830

INTRODUCTION

Many approaches are being explored to improve the safety and operability of nuclear-plant operations. One approach is to supply high-quality, relevant information by means of computer-based diagnostic systems to assist plant operators in performing their operational and safety-related roles. Privately and federally funded research has resulted in the development of operational aid concepts** to improve plant monitoring, diagnostic and corrective capabilities, and operator-process communication. Many of these concepts have passed from the idea state to the point of testing.

The evaluation of operational aids to ensure safe plant operations and verify improved performance is made difficult by the lack of reliable quantitative performance measures and plant function-analysis data. This lack exists, in part because the nuclear power industry has not uniformly adopted a rigorous systems approach, as characterized by the aerospace/aircraft industry. As a result, to obtain these data for design use requires post-engineering synthesis; that is, reconstruction of the original design process.

Furthermore, a situation the reverse of the systems approach has evolved: many operational aid systems are being developed without adequate analysis of the operator's role, the system's function, and the operator's tasks. This is analogous to having solutions in search of problems. Analysis, would help point to specific functions and tasks for which the operator may require assistance, especially those in the areas of decision making and fault diagnosis.

A project has been under way at ORNL to collect limited data on a diversity of operational aids, and to provide a method for evaluating the safety implications of the functions of proposed decision aids. This report will discuss the methods for aid evaluation now under study, and will outline data collection to date.

---

*Research sponsored by Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission under Interagency Agreement DOE 40-550-75 with the U.S. Department of Energy under contract W-7405-eng-26 with the Union Carbide Corporation.

**Decision aids for the purposes of this study are limited to computer-based systems that transcend the fundamental monitoring and control instrumentation of the control room. Such aids allow the operator to delegate such tasks or functions in broad areas of (1) supervision of plant operations, (2) maintenance of equipment, and (3) coordination of support activities.

METHOD

Several alternative approaches can be employed by the NRC in the evaluation of potential functions of operational aids:[1]

1. No review - No prior NRC approval is necessary. The supposition is that any responsible effort to implement an operational aid represents a net improvement in operational safety.

2. No adverse effects - NRC approval is necessary before testing and implementation of the operational aid. The aid is considered non-safety-related. It must not be required for safety, and failures must not significantly affect the ability of plant safety systems to function as required or cause plant conditions more severe than would exist without the aid.

3. Improved safety - Prior NRC approval is necessary before testing and implementation of the operational aid. The supposition is that an improvement in safety is required and that the licensee must demonstrate that the aid represents such an improvement. Satisfaction of specific criteria is required.

A general list of functions which can be carried out by operational aids could be useful to support these approaches, especially the latter two. Such a list might contain functions which can improve safety as well as those which would produce adverse effects. Several sources exist for generating a limited list of such tasks and functions:

1. Workload time-line analysis of operating crews: Tasks that contribute to workload peaks and overload can be identified, and by induction, needed decision-aid functions can be generated.

2. Error analyses of operating crews: Error-prone tasks can be extracted, and by induction, needed aid functions can be generated.

3. Operator emergency response models:[2] General functions that support safety goals during an emergency can be broken down deductively into subfunctions and tasks, which may be relegated to an aid.

4. Operator function classification:[2] The overall functions of an operating crew, derived from a context-free taxonomy, can be examined systematically to identify certain functions amenable to computer-based assistance.

5. Analysis of operational aids used in other industries: The experience gained in non-nuclear industries can be transferred by analogy.

A possible methodology for evaluation of an individual aid is (1) compare its functions with those determined to be effectual, ineffectual, or hazardous (this is a theoretical verification of the efficiency of specific functions), and (2) test its ability to carry out its specified functions at a simulator or other facility (this is an experimental verification). The ORNL project is primarily concerned with step one. A major work in support of step two is a project funded by the Electric Power Research Institute (EPRI) to develop the experimental design for evaluating the effectiveness of operational aids. Coordination of these two projects is presently occurring.

DATA

One of the subtasks of the ORNL project is to collect and classify information pertaining to computer-based operational aids, primarily those aids that in some way support the cognitive behavior of the plant crew. This limited data base can assist in identifying the spectrum of possible functions and serve as the foundation of a comprehensive data base for future review processes.

Information about specific operational aids under development by various groups is incomplete and has been difficult to obtain. To enlarge and improve the data base, therefore, a questionnaire was prepared and used to canvass a limited number of organizations. The questionnaire included the following catagories:

1. Problem definition
2. Function
3. Design
4. Plant Interface and Environment
5. Performance
6. Operation
7. Maintenance and Testing
8. User Training
9. Documentation
10. Work Status

RESULTS

Data for this summary were taken from the following operational aid systems:

1. AIDS - Abnormal Incident Decision Support (Atomic Energy of Canada)
2. DASS III - Disturbance Analysis and Surveillance System (EPRI-NPD, Electric Power Research Institute)
3. DCS - NUCLENET Display Control System (General Electric)
4. DMA - Diagnosis of Multiple Alarms (Savannah River Laboratory)
5. ESSS - Ebasco Safety Surveillance System (Ebasco Services)
6. HALO - Handling Alarms with Logic (Halden Reactor Project)
7. ODDS - Operational Diagnostics and Display System (Idaho National Engineering Laboratory)
8. PIE - Plant Incident Evaluation (General Atomic)
9. SAS - Safety Assessment System (Wisconsin Electric Power)
10. STAR - Disturbance Analysis and Surveillance System (GRS/Federal Republic of Germany)

The following general summary of the data is organized according to the major headings of the questionnaire.

Problem Definition. Six problem areas have been identified by the respondents:

1. Alarms cause operator confusion during normal and abnormal operation, with the number of alarms being great and their relevance not always clear.

2. Data rate (the quantity of information presented to the operator per unit of time) is high during fault conditions.

3. Data structure in the control room is suboptimal, bordering on no structure at all, which forces operators to expend effort on collecting and converting data.

4. Integration of systems, equipment, and information (inside and outside the control room) is not accomplished to a satisfactory degree.

5. Delayed detection of a deviation from normal leads to a degradation of plant safety (often because the inception of an event can be traced back to the deviation of one or two parameters).

6. Incorrect diagnosis by the crew is a possibility even with ample time allowed for corrective action.

Functions. Numerous aid functions have been incorporated by the aid designers. Following is a list of functions compiled from the ten aids reviewed. No one aid incorporated all of these functions.

Discrete Alarms

1. Grouping alarms for operational or safety priority/ significance.
2. Grouping alarms for specific modes of operation or conditions of the plant.
3. Suppression of nuisance and redundant alarms.
4. Recognition of specific sequential and combinational patterns of alarms.

Data

1. Validation of sensor data.
2. Compression and grouping of data.
3. Graphic display (P&ID, Functions, Messages).
4. Trend analysis and display of parameter trends.

Integration

1. Systems - Indication of configuration
   - Identification of mode and lineup
   - Indication of safety and control systems availability

- Verification of operation
- Indication of process status
- Margin to technical specifiction

2. Components
   - Monitoring of specific equipment
   - Monitoring for prediction of failure

3. Procedures
   - Computer retrieval of procedures
   - Monitoring procedure execution by the operator
   - Recommendations to the operator for a specific task/action

DIAGNOSIS

1. Early detection and warning of disturbance.
2. Identification of the cause of disturbance.
3. Identification of the event in progress by probabilistic means.
4. Indication of the presense of non-anticipated circumstances for normal diagnosis.
5. Prediction of the propagation of disturbance.
6. Prediction of the consequences of intended operator actions.

The system users for the aids surveyed are indicated as the operators, shift supervisors, shift technical advisor, plant engineers, and various combinations. The conditions under which the aid would be used also varied from aid to aid: some are primarily for normal conditions only, some for abnormal conditions, and others for both. Most designers are reluctant to allow control of the plant by an operational aid; however one aid is capable of scramming the reactor.

Design. Some aids are designed to exist as separate, standalone devices; others are intended to be integrated into the control boards. In some cases the option is left to the utility customer. Most designers are using modular software; some indicate the use of verification and validation. Almost universally the cathode-ray tube (CRT) is used for operator interface. Many aids have been prototyped on minicomputer systems; however, most designers indicate the use of microcomputers for production equipment. Of the prototype aids now in existence, some have been tested on simulators and a few have been tested in operating plants.

Plant Interface and Environment. Many of the aids will require an equipment room for computers and peripherial equipment because they are sensitive to ac power fluctuation, high temperature, high humidity, and dust. The aids require a tie-in to plant sensor signals; in some cases, additional sensors are required. The installation times for the aids generally extend over several plant outages.

Performance. Several respondents indicate goals of 99% equipment reliability. Predominant failure areas named were CRT, computer memory, data acquisition system, computer mainframe, and latent logic. Mean-time-between-failures (MTBF) and mean-time-to-repair (MTTR) data are generally not known. Response times of aids to a change in process state ranged from one second up, with no upper limits indicated in many cases.

Response to an operator command ranged from one to three seconds for most aids. Input data verification was considered to be a necessity by some, with diverse schemes being employed to qualify data; some, however, did not specifically mention data verification as a part of the aid system.

Operation. Most aids employ CRT and function keyboard interfaces, and most are user interactive. Few designers, however, have considered the interaction between the aid and existing procedures. Some have involved operators with the design of the aid or the testing process. Most designers consider the presence of existing control panels as sufficient information for independent verification of the conclusions rendered by an aid. Some go further by building in *scrutability* (i.e., give the user a means to trace the development of an analysis). Regarding operator workload, no respondent could list specific operational tasks eliminated by aids.

Maintenance and testing. Many aids are weak in this category. Some, however, indicate self-testing mechanisms.

Training. Operator training is needed for all systems. Some of the aids are self-explanatory, while others require that the operator be trained for the aid's use on a plant simulator. Designers vary in their opinions concerning how much knowledge should be required of the operator regarding the aid's method of performing its analysis. Some experience indicates that the more complete and detailed the operator's knowledge of the aid, the more the operator can follow the conclusions of the aid and make use of its information.

Documentation. Most aid designers have not addressed this subject thoroughly since many aids are still in the conceptual design stage. Also, many designers plan to leave documentation to the customer.

Work Status. Of the ten aids examined, three were installed and working at a power plant, two were installed at a plant simulator, and two were in the prototype stage. The remaining four were in the conceptual or laboratory development stage.

CONCLUSIONS

Responses varied widely in detail, thus forcing distillation of the salient features of many operational aids from information sources other than the initial questionnaire. These sources included technical and management presentations, technical papers and reports, personal discussions, taped responses, sales brochures, system specifications and schematics, and other documents. The data base is dynamic, not static, owing to the nature of current trends in operational aid development. The information contained in it is subject to review and revision by the developing organizations. More systems are pending review and entry into the data base; hence the list is incomplete.

Without a clear description of the functions, tasks, and team organizations of operations personnel, it is difficult to determine how best to provide them with computer-based assistance. The evaluation of computer-based aids developed on the basis of partial knowledge is equally difficult. Nevertheless, such systems are being developed and their effectiveness and safety value must be assessed. This can be done to a limited extent by the methods described.

REFERENCES

1. R. DiSalvo, "Regulatory Approaches to Disturbance Analysis and Surveillance Systems," February 23, 1981, internal report, Office of Research, United States Nuclear Regulatory Commission.

2. R. A. Kisner and P. R. Frey, "Functions and Operations of Nuclear Power Plant Crews," NUREG/CR-2587, April 1982.