12

-12

BNL--47229

DE92 011545

COMPUTER-BASED DIAGNOSTIC MONITORING TO ENHANCE THE HUMAN-MACHINE INTERFACE OF COMPLEX PROCESSES

Inn S. Kim
Engineering Technology Division
Department of Nuclear Energy
Brookhaven National Laboratory
Upton, New York 11973, U.S.A.

February 1992

Presented at the

8th Power Plant Dynamics, Control & Testing Symposium
Knoxville, Tennessee
May 27-29, 1992

APR 1 3 1992

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

COMPUTER-BASED DIAGNOSTIC MONITORING TO ENHANCE THE HUMAN-MACHINE INTERFACE OF COMPLEX PROCESSES*

Inn S. Kim
Engineering Technology Division
Department of Nuclear Energy
Brookhaven National Laboratory
Upton, New York 11973, U.S.A.

ABSTRACT

There is a growing interest in introducing an automated, on-line, diagnostic monitoring function into the human-machine interfaces (HMIs) or control rooms of complex process plants. The design of such a system should be properly integrated with other HMI systems in the control room, such as the alarm system or the Safety Parameter Display System (SPDS). This paper provides a conceptual foundation for the development of a Plant-wide Diagnostic Monitoring System (PDMS), along with functional requirements for the system and other advanced HMI systems. Insights are presented into the design of an efficient and robust PDMS, which were gained from a critical review of various methodologies developed in the nuclear power industry, the chemical process industry, and the space technological community.

INTRODUCTION

The principal role of humans (i.e., the operating crew) in a process plant, such as a nuclear power plant or a chemical processing plant, is to make decisions.[1] Other core areas of human performance (e.g., monitoring, controlling) assigned to the operator initiate, support, or are otherwise ancillary to decision-making.

Recent catastrophic events in the process industries suggest that the human-machine interface (HMI), e.g., process-parameter and alarm displays in the control room, have a great impact on the operator's decision-making. The most critical decisions are those that must be made in emergencies.[1]

To support the operator's decision-making (i.e., cognitive or knowledge-based behaviors) during emergencies, there was a worldwide surge of effort in the late 1970s and early 1980s to develop disturbance analysis systems.[2-5] If properly validated and installed in control rooms, such systems would be an invaluable aid to the operators so that they could quickly diagnose and correct disturbances in the plant processes. However, the research did not lead to the installation of diagnostic monitoring systems in control rooms. The major obstacle was the lack of a reliable methodology to develop such a system. The prerequisite of computer hardware and software engineering techniques for the computerized systems is now available, due to remarkable advances in the technology.

---

*Work performed under the auspices of the U.S. Department of Energy.

The purpose of this paper is to provide a conceptual foundation for the development of a Plant-wide Diagnostic Monitoring System (PDMS) from the perspective of human-machine interface. Our focus will be placed on functional requirements and on-line diagnostic monitoring methodology. To meet this purpose, Section 2 briefly describes three basic HMI systems, i.e., displays, manual controls, and written materials. Section 3 presents the functional requirements for advanced HMI display systems, including the PDMS, with emphasis on the need to integrate the design of the PDMS with other systems. Section 4 discusses the methodology for plant-wide, on-line diagnostic monitoring, with insights into the design of an efficient and robust PDMS that were gained from a critical review of various methodologies.

MAJOR HUMAN-MACHINE INTERFACE SYSTEMS

To aid the operator's decision-making, monitoring, and control tasks, the control rooms of process plants are typically equipped with three basic HMI systems, i.e., displays, manual controls, and written materials.[6]

Displays

A display is any instrument or device that presents information to any human sense organ (e.g., visual, auditory). A typical HMI consists of annunciated and unannunciated displays. The latter include meters, digital readouts, chart recorders, graphs, indicator lights, computer printouts, and video presentations. Annunciated displays, accompanied by attention-getting signals when they change state, are sometimes called alarms.

The annunciator or alarm system is the classical means of informing the operators of unusual operating conditions. However, studies and operational experience have uncovered a variety of common problems with conventional, hardwired alarm systems; e.g., too many nuisance alarms, or annunciation of too many conditions that should not be part of an integrated warning system.[7,8] Advanced displays based on computer technology, such as computerized alarm display systems or diagnostic monitoring systems, are under development and may be installed in future nuclear power plants. These advanced systems are discussed in Section 3.

Manual Controls

Manual controls are those devices by which humans enter their inputs to a system, e.g., an electrical switch in the control room to control a motor-operated valve or a pump. With the advent of advanced displays, soft controls, such as computer-driven switches or touch screens, may be used for manual inputs to the control system along with the dedicated hard switches.[8]

Written Materials

The control rooms of process plants typically contain written materials such as normal and emergency operating procedures. These procedures will guide the operators, especially when they actively perform control tasks.

FUNCTIONAL REQUIREMENTS FOR ADVANCED HMI DISPLAY SYSTEMS

This section discusses the functional requirements for an advanced alarm system, a safety-status display system, and a plant-wide diagnostic monitoring system, focusing on the need to integrate the design of the PDMS with other HMI display systems.

Functional Requirements for an Advanced Alarm System

A study, which was performed following the U.S. Nuclear Regulatory Commission's action plan developed as a result of the TMI-2 accident, laid out the design philosophy and functional criteria for advanced alarm systems.[9] Accordingly, an annunciator system must:

- Minimize the potential for deviations in the plant systems and processes to develop into significant hazards.

To fulfill this requirement, an annunciator system, which may consist of either or both conventional hardwired and computerized systems, must meet the following four functional criteria:

- The system should alert the operators to the fact that there is a deviation in the plant systems or processes.
- The system should inform the operators about the priority and the nature of the deviation.
- The system should guide the operator's initial response to the deviation.
- The system should confirm, in a timely manner, whether the operator's response corrected the deviation.

However, there is a significant overlap between the functions of an advanced alarm system and a PDMS. Some of the functions for the alarm system, such as identifying the nature of the deviation and guiding the initial response, can be performed more effectively by the PDMS, than by the alarm system. Hence, a proper match must be made in allocating functions to the HMI systems, as we will discuss later.

Functional Requirements for a Safety-Status Display System

Safety-status display systems, such as Safety Parameter Display System (SPDS) or Critical Function Monitoring System (CFMS), have been introduced into the control rooms of nuclear power plants to help operators assess the plant's safety status quickly. The SPDS was made a requirement at U.S. nuclear power plants following the accident at TMI Unit 2. The principal functional requirements for an SPDS are:[10]

- The system shall continuously display information from which the plant's safety status can be assessed by control room personnel who are responsible for avoiding degraded and damaged core events.

- The minimum information provided shall be sufficient to inform plant operators about the following functions:

  Reactivity control
  Reactor core cooling and heat removal from primary system
  Reactor coolant system integrity
  Radioactivity control
  Containment conditions

The Nuclear Regulatory Commission (NRC) review was initially directed only at identifying serious safety questions or inadequate analysis. However, subsequent reviews of operating SPDSs revealed several problem areas, including: 1) display of invalid and inaccurate information, 2) discontinuous display of plant safety status, 3) inadequate verification and validation program, 4) poor software maintenance, 5) poor operator acceptance, 6) potentially misleading information, and 7) inadequate coverage of critical plant variables.

Functional Requirements for a Plant-Wide Diagnostic Monitoring System

The functional requirements for an on-line diagnostic monitoring system are taken from references 2 and 4:

- Real-Time Operation: The system shall operate in a real-time environment.

- Timely Analysis: The system shall provide a timely analysis, and present the results to the operators within the time-frame of the disturbances.

- Interface with the Plant: The system shall have access to plant process information, either directly or through the process computer. The need to add additional instrumentation must be carefully balanced against the cost of such instrumentation.

- Identification of the Plant Operational Mode: The system shall identify the mode of plant operation and analyze only those disturbances associated with this mode. A disturbance for one mode may be a normal event for another mode. (In this context, the system also shall identify on-line the specific operating configurations of the plant systems, because the propagation of the disturbance depends on the specific configurations, such as the operating status of pumps or valves, and the operational modes of controllers.)

- Disturbance Detection: The system shall examine the on-line plant data for changes in status that indicate disturbances. When a disturbance is detected, the system shall automatically start its analysis.

- Disturbance Analysis: The system shall provide the capability of determining the nature, cause, and consequences of the disturbance, and the corrective actions.

- Interface with the Operator: The system results shall be presented automatically to the operator through a proper mechanism, such as a computer-driven CRT (cathode ray tube) or video display. No other interaction with the operator shall normally be required. However, the operator should be able to query the system to determine how the results were obtained.

In addition to these functional requirements, a PDMS shall be able to:[11]

- Handle systems containing a few thousand components, connections, and processes.
- Detect and diagnose multiple system faults on-line, including those in sensors and controls (for both automatic and manual modes).
- Handle unforeseen situations by reasoning with a causal model based on the structure and function of the engineered system.
- Provide advice in time to achieve the desired operating conditions, or at least to prevent a worsening of conditions.
- Support the operator in obtaining a broader comprehension of the plant systems and their current states.

Advanced instrumentation and control (I&C) systems, being designed for the next generation nuclear power plants, incorporate fault detection, diagnosis, isolation, and correction capabilities to some extent.[12] If a PDMS is developed for a plant with such advanced I&C systems, the system shall be able to:

- Monitor the performance of the advanced I&C system in detecting, diagnosing, isolating, and correcting faults.
- Diagnose the malfunction of the advanced I&C system and recommend corrective actions.

The advanced I&C systems also tend to use hierarchical and intelligent controllers. The PDMS shall be able to:

- Perform diagnostic monitoring of the hierarchical and intelligent control system, e.g., fault diagnosis of inter-controller communication.

Efforts are also being made to develop early fault detection systems to detect the onset of mechanical deficiencies or abnormal deviations of processes (and systems), using techniques such as acoustic, vibration, and noise analysis, or monitoring of loose parts.[13] The PDMS shall:

- Use the information from and communicate with the early fault detection system to enhance the diagnostic monitoring capabilities.

Overall Functional Requirements for HMI Display Systems

All the HMI display systems for a control room, e.g., alarm system, safety-status display system, and PDMS, shall satisfy, as a whole, the overall functional requirements for HMI display systems. We discuss these requirements in this section, based on the HMI issues in nuclear power plants that were identified by a multidisciplinary expert team.[14]

- The HMI systems shall reduce the need for guesswork by the operator in:
    - Monitoring (i.e., sensing and interpretation) tasks
    - Information-processing tasks
    - Decision-making tasks
    - Control tasks
    - Diagnostic and remedial-action tasks

- The display design of the HMI systems shall include:
    - Display of process states
    - Diagnostic information
    - Maintenance states of component equipment

- The design of the HMI shall help the operator detect abnormalities and prevent accidents by presenting:
    - Trend information
    - Information on critical safety functions
    - Precautionary alarms
    - Information on the functioning of automatic protective devices

- The HMI design shall give the operator the flexibility to test the system in various ways, in order to validate the diagnosis and remedial actions.

- The HMI design shall be integrated with the operator's mental model of the system.

- The HMI design shall provide a dynamic allocation of functions between the operator and HMI systems,[1] including:
    - Selection of automatic or manual control of the interface
    - Automatic default transfer to safe condition
    - Capability for manual override

- The HMI design shall be tailored to the operational roles of the users in normal and emergency operations.

- The HMI design shall promote a match between the HMI display systems, engineered control systems (including advanced I&C systems), and the operating staff for control capabilities, fault detection capabilities, emergency operating strategies, and fault isolation and correction capabilities.

METHODOLOGY FOR PLANT-WIDE, ON-LINE DIAGNOSTIC MONITORING

Critical Review of Various Diagnostic Methodologies

A comparison of various methodologies for on-line diagnostic monitoring was made to identify their characteristics and differences.[15] The methodologies were classified into three categories:

(1) Event-oriented: fault tree,[16] cause-consequence tree,[2] cause-consequence diagram[3]

(2) Process-oriented: digraph,[17] logic flowgraph methodology,[18] MIDAS[19-20]

(3) Model-based: KATE,[21] MOAS-II[22-23]

The advantages and shortcomings of each methodology, except MIDAS and KATE, were discussed elsewhere to shed light on the necessary and desirable characteristics of a more advanced methodology.[15]

The MIDAS (Model-Integrated Diagnostic Analysis System) methodology performs process monitoring and malfunction diagnosis of continuous chemical processes. MIDAS employs a deep-knowledge approach, based on reasoning about causality and constraints. Qualitative causal models, based on a similar concept as digraph[17] mentioned above, represent local relationships between process variables, and indicate the probable propagation paths of malfunction. Quantitative constraint equations can model global relationships, such as overall material and energy balances, that cannot be represented by causal models. On-line diagnosis in MIDAS uses the process model, called event graph, where an event is any significant, observable change in process behavior or condition (e.g., change of trend of a parameter is increasing). An issue remaining for further development is that event models become too complicated for large interconnected systems.

The KATE (Knowledge-based Autonomous Test Engineer) methodology was developed for NASA's Systems Autonomy Program at Kennedy Space Center. It is a model-based reasoning tool that can perform real-time system monitoring, signal validation, fault location and diagnostics, and automatic control and reconfiguration. The KATE, which is a type of simulation-based or expectation-driven technique, works as follows:

- KATE simulates the physical system using first principles, i.e., fundamental knowledge about the system, such as structural and functional information. The simulation model, which consists of commands (i.e., inputs to the physical system used to control it), components, and measurements, generates expected values at the measurements.

- The process is monitored by comparing the expected values with the measured readings. Any substantial deviation from a predicted value signifies a disturbance.

- When a disturbance is detected, the diagnostic process is invoked. KATE uses the simulation model to determine those components whose failure could explain the discrepant readings. The compiled suspects are examined using a generic algorithm, until the KATE system obtains the smallest set which could be derived without additional measurements.

The KATE methodology can be used for on-line diagnostic monitoring of electronic, pneumatic, or mechanical systems. However, it cannot yet diagnose malfunction in process systems with complex feedback loops. Another drawback of this technique is that only snapshot sensor data are used for diagnostic monitoring; as such, it lacks temporal reasoning, which plays an important role in diagnostic reasoning during fault-driven transients.

From the review of the various on-line diagnostic monitoring methodologies, we obtained general insights into an efficient and robust PDMS; these are presented next.

Insights on Developing an Efficient and Robust PDMS

Rasmussen defines the ultimate purpose of diagnosis as linking the observed symptoms to the actions which will serve the current goal properly. Hence, diagnosis involves:

- Monitoring the process to observe any symptom or disturbance, namely, any significant change in the behavior of monitored process parameters,
- Determining the cause which initiated the observed system misbehavior, and
- Formulating a corrective action (either to be performed by the operator or the control system actuator) to meet the current goal, by isolating or rectifying the fault, or by mitigating its consequences.

In the past, diagnostics often was referred to as disturbance analysis, in contrast to alarm analysis.[25] The major difference between these two is that the former is mainly performed using analog (i.e., continuous) process parameters directly, whereas alarm analysis is done using binary alarm signals, e.g., on or off, transformed from the analog parameters. Therefore, disturbance analysis allows a more thorough analysis of system malfunction.

However, most diagnostic methodologies developed have failed to appreciate the role of process monitoring. Monitoring is the first step that should be properly performed. Process monitoring through the on-line sensor data not only triggers diagnostic function in the diagnostic system, but also can act as an important barrier against further propagation of the malfunction.[15] In other words, the incorporation of an elaborate process-monitoring scheme into the PDMS, independent of the diagnostic module, will help to ensure that the system is robust against unanticipated failures in cases where the complex conditions cannot be diagnosed quickly or because of the limitation of the diagnostic module. Therefore, sufficient considerations should be given to process monitoring; this is why we adopted the term diagnostic monitoring, not simply diagnosis.

The insights gained from the critical review of various on-line diagnostic methodologies are presented below.

(1) Scope and Level of Modeling Detail

A modern, large technical process, such as a nuclear power plant, typically consists of many systems. Even for a full-scope application, all of these systems do not necessarily have to be treated equally. We should first perform a detailed engineering analysis to determine the scope and level of modeling detail required to develop a PDMS.[2] For example, detailed diagnostic monitoring may be needed for those systems which were found to be major contributors to plant safety and availability. The early and correct diagnosis of disturbances in the systems will greatly contribute to achieving the plant goals, by avoiding unnecessary challenges to the plant protection system, safety systems, and operators.

The plant also may comprise a large number of process parameters, e.g., about 1,000 - 2,000 analog process parameters with many binary parameters.[13] Among these analog parameters, only a selected set can be normally monitored; for example, the logical method of selecting process monitoring points, which was employed in MOAS-II, may be useful.[22]

To develop a PDMS, the level of modeling detail in diagnosis also should be determined at the outset. Hierarchy is an inherent characteristic of a large process plant. In a nuclear power plant, for example, hierarchical relationships can be easily found; i.e., the levels of subcomponent (e.g., valve stem, plug, diaphragm, or pump shaft), component (e.g., valve, pump, sensor, or controller), subsystem, system (e.g., reactor coolant or feedwater system), function (e.g., reactor cooling or containment heat removal), and plant. Malfunction in the plant usually occurs at a low level in the hierarchy, i.e., at the subcomponent or component level. The disturbance at the low level, e.g., the leakage of a check valve (the initiating event of the lowest level in the TMI accident),[26] will propagate through the subsystem, system, and then the plant, if there is no intervention. An important criterion in determining the diagnostic resolution is that the result of the on-line diagnosis should be useful to mitigate the effects of the malfunction on the plant, quickly avoiding further propagation.

(2) Knowledge and Information

Once the scope and level of modeling detail is determined, then we should obtain information about the plant systems and processes, e.g., design knowledge, plant topology, or heuristics for efficient diagnostic monitoring from experienced operators. Some important lessons from past studies are:[19-23]

- In a process plant, fault propagates following causality, i.e., relationships between cause and effect, based on the underlying physical principles. Therefore, the causal relationships between process variables can be used as an effective tool to model the fault propagation paths.
- Use of deep knowledge, i.e., underlying physical knowledge such as conservation equations (mass or energy balances), pump curves, or control algorithms, can significantly improve the diagnostics. However, shallow knowledge, i.e., plant-specific experiential compilations of the underlying principles such as heuristics or rules of thumb, also can be an efficient shortcut to problem solving in certain situations.

The knowledge may be acquired in parallel to model development discussed below, because necessary knowledge can be identified while developing models that will be used on-line by the PDMS.

(3) Model Development

There are four major functions that a PDMS should perform: process monitoring, sensor data validation, fault diagnosis, and corrective measure synthesis.[22] Validation of sensor data is needed, not only because sensors are primary information sources on which diagnostic monitoring is based, but because the real-time inference process may be corrupted by erroneous data from malfunctioning sensors, leading to misdiagnosis which must be avoided.

In a PDMS, sensors should be validated preferably in the global context of diagnosis, because the information gained from the validation can be effectively used to diagnose the cause of the system fault. The method of sensor validation depends on the type of instrumentation at a particular process point. There may be many redundant sensors for important process points, e.g., typically 4 redundancies for pressurizer pressure and steam-generator level at a nuclear power plant. These redundant sensors can be validated by elaborate methods, e.g., such as generalized consistency checking,[27] multi-dimensional process hypercube comparison,[27] or parity-space technique.[28]

However, in a process environment consisting of a few like-measurements, such as that found in the secondary side of a nuclear power plant, a less elaborate method may be applied, as used in MOAS-II.[22-23] The MOAS-II method is based on the effective use of coherent relationships among process parameters developed from deep knowledge, in an inductive logic structure.

Most of the diagnostic methodologies developed thus far used only one type of model, e.g., cause-consequence tree[2] and digraph,[17] to perform all the four major functions discussed above, giving a complicated model, even for a small-scale system. However, it will be more effective to use different models to perform the different functions, especially for a plant-wide application.

For example, there is a significant difference in the effect of failures of sensors and hardware (other than sensors, i.e., such as pumps, valves, or control circuits) on the operation of the process.[15,22] Hardware failures usually propagate through the plant process and cause its condition to deteriorate. On the contrary, sensor failures do not typically cause any deterioration of the process. Therefore, these two types of failures should be separately treated, taking into account their unique characteristics.

If the PDMS under development is to incorporate a diagnostic module for an electrical system, an approach different from that for a flow system may need to be developed. The KATE expectation-driven methodology discussed in the previous section, or the NSSS-DS methodology[29] based on simulation of Boolean models of the system, may be used to diagnose failures in electrical systems.

(4) Implementation

Once the models are developed, they should be implemented, using a programming technique, into a PDMS. The trend in implementing diagnostic methodologies is to use the advanced computer technique, i.e., knowledge engineering or expert systems.[30] The advantage of using this technique mainly comes from: 1) its symbolic processing capability; 2) the transparent knowledge representation; 3) the superior capability of reasoning; 4) the ease in software maintenance compared to the conventional programming technique (because the knowledge base is separated from the inference mechanism); and 5) the relative ease of providing explanations upon request from the user.

The expert systems technique also provides for diverse knowledge structures. For example, the G2 real-time expert system shell[31] incorporates a production system, i.e., IF-THEN-ELSE rules, and a frame or object-oriented system. The production system is suitable for implementing logic models, for both inductive and deductive reasoning. The object-oriented system can be used to model process entities, e.g., sensors, components, or systems, as objects or classes. For the object of a sensor, we can define appropriate slots, e.g., a scan interval or currency interval (of the sensor value). Where much numerical computation is needed, e.g., in models using lots of deep knowledge, conventional programming environment, such as FORTRAN or C, also can be used together with the expert system programming techniques.

(5) On-Line Process Data

The reasoning for diagnostic monitoring is performed by applying the on-line data of the plant systems and processes to the models, based on the inference structure built into the PDMS. Most data used in the system will be analog values, i.e., quantitative or continuous values. Diagnosis in conventional methodologies, e.g., based on only causality models, uses only <u>qualitative data</u> transformed from the raw, quantitative process data. However, these <u>quantitative data</u> also can be effectively used, particularly in the application of deep process knowledge. Both of these data should be properly used for diagnostic monitoring;[19-20,22-23] e.g., for process monitoring, qualitative data, such as high, low, or normal, can be effectively used.

Most diagnostic methods, including the logic flowgraph[18] and KATE,[21] were designed to interpret a snapshot of plant states at a single time-point. However, dynamic process information during transients, which were caused by process malfunction, often provides important cues for solving the diagnostic problem, and therefore, should be properly used, especially for systems with interconnected control loops.[19-20,22-23]

(6) Verification and Validation

A reliable method for verification and validation of expert systems has not been fully developed.[32] However, the expert systems developed from explicit models, such as those used in model-based diagnostic methodologies, can be verified and validated far more easily than model-free expert systems.

Furthermore, if the PDMS incorporates an elaborate process monitoring scheme that is independent of the diagnostic module, this monitoring module can work as a backup for the diagnostic module. Another defense-in-depth also can be achieved by the safety-status display system, which monitors key safety parameters independently from the diagnostic and monitoring modules.

REFERENCES

1. H.E. Price, R.E. Maisano, H.P. Van Cott, "The Allocation of Functions in Man-Machine Systems: A Perspective and Literature Review," NUREG/CR-2623, ORNL/Sub/81-9027/1, June 1982.

2. C.H. Meijer and B. Frogner, "On-Line Power Plant Alarm and Disturbance Analysis System," EPRI Report, NP-1379, April 1980.

3. W. Bastl and L. Felkel, "Disturbance Analysis Systems," in Human Detection and Diagnosis of System Failures, J. Rasmussen and W.B. Rouse (ed.), Plenum Press, New York, 1981, pp 451-473.

4. J.M. Gallagher, Jr., J.P. Leider, S. Crunk, et al., "Disturbance Analysis and Surveillance System Scoping and Feasibility Study," EPRI Report, NP-2240, July 1982.

5. A.B. Long, "Technical Assessment of Disturbance Analysis Systems," Nuclear Safety, Vol. 21, No. 1, January-February 1980, pp 38-50.

6. A.D. Swain and H.E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, SAND80-0200, August 1983.

7. W.L. Rankin, E.G. Duvernoy, K.R. Ames, et al., "Near-Term Improvements for Nuclear Power Plant Control Room Annunciator Systems," NUREG/CR-3217, PNL-4662, April 1983.

8. J.M. O'Hara, W.S. Brown, and I.S. Kim, "Advanced Alarm Systems in Nuclear Power Plants: Background Review," BNL Technical Report, A-3967, March 1991.

9. W.L. Rankin, T.B. Rideout, and T.J. Triggs, "Computerized Annunciator Systems," NUREG/CR-3987, PNL-5158, June 1985.

10. S.H. Weiss, W.H. Regan, Jr., and J.W. Roe, "Experience with Operator Aids for Nuclear Power Plants in the United States of America," Proc. Man-Machine Interface in the Nuclear Industry (Tokyo, February 1988), IAEA-CN-49/74, International Atomic Energy Agency, Vienna, 1988, pp 323-329.

11. J.D. Erickson, "The Role of Intelligent Systems in Space," Proc. Frontiers in Innovative Computing for the Nuclear Industry (AI91), Jackson, Wyoming, September 1991.

12. B.R. Upadhyaya, E.M. Katz, and T.W. Kerlin (ed.), Proc. 7th Power Plant Dynamics, Control & Testing Symposium, Knoxville, Tennessee, May 1989.

13. W. Bastl, H. Schuller, and D. Wach, "High Performance and Safety of Nuclear Power Plants by Means of Early Fault Detection," Proc. Man-Machine Interface in the Nuclear Industry (Tokyo, February 1988), IAEA-CN-49/4, International Atomic Energy Agency, Vienna, 1988, pp 305-322.

14. J. DeBor and R. Swezey, "Man-Machine Interface Issues in Nuclear Power Plants: Report on a Workshop Held on January 10-12, 1989," NUREG/CR-5348, SAIC-89/1114, July 1989.

15. I.S. Kim, "On-Line Process Failure Diagnosis: The Necessity and a Comparative Review of the Methodologies," Proc. Safety of Thermal Reactors, Portland, Oregon, July 1991, pp 777-783.

16. G.A. Martin-Solis, P.K. Andow, and F.P. Lees, "Fault Tree Synthesis for Design and Real Time Applications," Trans. Institution of Chemical Engineers, Vol. 60, 1982, pp 14-25.

17. S.A. Lapp and G.J. Powers, "Computer-Aided Synthesis of Fault-Trees, IEEE Trans. on Reliability, April 1977, pp 2-13.

18. S. Guarro and D. Okrent, "The Logic Flowgraph: A New Approach to Process Failure Modeling and Diagnosis for Disturbance Analysis Applications," Nuclear Technology, Vol. 67, December 1984, pp 348-359.

19. F.E. Finch, O.O. Oyeleye, and M.A. Kramer, "A Robust Event-Oriented Methodology for Diagnosis of Dynamic Process Systems," Computers and Chemical Engineering, Vol. 14, No. 12, 1990, pp 1379-1396.

20. "Overview of Current Research Projects at LISPE (Laboratory for Intelligent Systems in Process Engineering)," Department of Chemical Engineering, Massachusetts Institute of Technology, Cambridge, Massachusetts, May 1989.

21. R.A. Touchton, N. Subramanyan, A. Lane, and P.H. Subramanian, "Nuclear Power Applications of NASA Control and Diagnostics Technology," EPRI Report, NP-6839, Vols. 1-3, May 1990.

22. I.S. Kim, M. Modarres, and R.N.M. Hunt, "A Model-Based Approach to On-Line Process Disturbance Management: The Models," Reliability Engineering and System Safety, Vol. 28, 1990, pp 265-305.

23. I.S. Kim, M. Modarres, and R.N.M. Hunt, "A Model-Based Approach to On-Line Process Disturbance Management: The Application," Reliability Engineering and System Safety, Vol. 29, 1990, pp 185-239.

24. J. Rasmussen, "Models of Mental Strategies in Process Plant Diagnosis," in Human Detection and Diagnosis of System Failures, J. Rasmussen and W.B. Rouse (ed.), Plenum Press, New York, 1981, pp 241-258.

25. F.P. Lees, "Process Computer Alarm and Disturbance Analysis System: Review of the State of the Art," Computers and Chemical Engineering, Vol. 7, No. 6 (1983), pp 669-694.

26. "Analysis of Three Mile Island-Unit 2 Accident," Nuclear Safety Analysis Center, NSAC-1, July 1979.

27. B.R. Upadhyaya, T.W. Kerlin, and P.J. Gaudio, Jr., "Development and Testing of an Integrated Signal Validation System for Nuclear Power Plants," Vol.1, Executive Summary, Final Report prepared for the U.S. Department of Energy by the University of Tennessee, DOE/NE/37959-34, September 1989.

28. C.H. Meijer, J.P. Pasquenza, J.C. Deckert, et al., "On-Line Power Plant Signal Validation Technique Utilizing Parity-Space Representation and Analytic Redundancy," EPRI Report, NP-2110, November 1981.

29. S.W. Cheon, H.G. Kim, W.J. Kim, et al., "Development of an Expert System for Failure Diagnosis of Primary Side Systems," Nuclear Technology, Vol. 97, January 1992, pp 1-15.

30. D.A. Waterman, A Guide to Expert Systems, Addison-Wesley Publishing Co., Reading, Massachusetts, 1986.

31. Version 1.1 of the G2 User's Manual, Gensym Corporation, Cambridge, Massachusetts, 1988.

32. L. Miller, E. Groundwater, and S. Mirsky, "Development of Guidelines for the Validation and Verification of Expert Systems," Trans. 19th Water Reactor Safety Information Meeting, NUREG/CP-0119, February 1992.