

Conf-910714--11

BNL-45947

ON-LINE PROCESS FAILURE DIAGNOSIS:

BNL--45947

THE NECESSITY AND A COMPARATIVE REVIEW OF THE METHODOLOGIES*

DE91 011718

Inn S. Kim

Engineering Technology Division
Brookhaven National Laboratory
Upton, New York 11973

ABSTRACT

Three basic approaches to process failure management are defined and discussed to elucidate the role of diagnosis in the operation of nuclear power plants. The rationale for the necessity of diagnosis is given from various perspectives. A comparative review of some representative diagnostic methodologies is presented and their shortcomings are discussed. Based on the insights from the review, the desirable characteristics of advanced diagnostic methodologies are derived from the viewpoints of failure detection, diagnosis, and correction.

The on-line diagnosis can be done at several different levels, e.g., at the level of component, subsystem, function, or event. For instance, a diagnosis can be made at event level to determine which event has occurred among those predefined in the emergency operating procedures (EOPs), e.g., loss of coolant accident (LOCA) or loss of main feedwater (LOFW) events.

However, the on-line diagnosis (hereafter called diagnosis) that will be discussed in this paper means diagnosis at component level, i.e., the determination of the basic cause of the process disturbance. The diagnosis will be done by a computerized diagnostic system by integrating and processing the on-line process sensor data available from the plant data acquisition system. Its purpose is to take control of the incipient process failure at a very early stage.

I. BACKGROUND AND INTRODUCTION

When applied to an engineering system or process, the term diagnosis means the determination of the cause(s) of an undesirable state, a system failure, or a process--temperature, pressure, water level, etc.--failure. The diagnosis can be performed in different dimensions such as off-line or on-line. The off-line diagnosis is done to find the root cause of the malfunction so that the operability of the equipment can be restored.

To look at the role of the diagnosis in the operation of nuclear power plants, consider the following three levels of approach to process disturbance management:

- Level 1: event-oriented approach
- Level 2: symptom-based approach
- Level 3: diagnosis- and symptom-based approach

On-line (process) diagnosis is carried out to control the outcome of the on-going failure or disturbance of the process as soon as possible and with minimum adverse consequences. In contrast to off-line diagnosis, there is usually a limited time to perform the on-line diagnosis because the incipient failure will continue to propagate through the process, deteriorating it further and further with time. Hence, the on-line diagnosis should be restricted to the level required to identify those systems or components whose status can be changed to reduce or eliminate the problem.¹

Level 1 represents the earliest approach, which is not being used any more. Level 2 is the current approach, and Level 3 is the desirable approach that may be realized in the future.

The Level-One event-oriented approach was used prior to the accident at Three Mile Island (TMI). The event-oriented EOPs are a good example of the incorporation of this concept. They were developed based on the major categories of perceivable plant transient events such as LOCA

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

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.

MASTER

or LOFW events, partly owing to the availability of information on the thermal-hydraulic and phenomenological behaviors following those hypothesized events through the plant safety analyses.

To use the EOPs during a plant emergency, the operator should have first identified the event, e.g., whether a LOGA, LOFW, or other transient, from the predefined event categories. In the meantime, the March 28, 1979 TMI accident gave an important lesson: namely, that the correct identification of the evolving transient during a major plant upset can be a difficult task to the operator in such a highly information-intensive and critical situation; a misidentification of the event and the subsequent operator action can lead to serious consequences.

The Level-Two symptom-based approach emerged from the TMI lesson and is currently being used in nuclear power plants. The concept of "symptom-based" has been incorporated into symptom-based EOPs, as a substitute for event-oriented EOPs, and also into the integrated display systems such as safety parameter display systems (SPDSs) or critical function monitoring systems (CFMSs). The aim of these procedures or computer systems is not to manage the process failure at its early stage, but to maintain the safety of the plant.

To use the symptom-based EOPs during an emergency, the operator no longer needs to identify the event, but only needs to monitor the symptoms and safety functions in terms of key process variables, and follow the flowchart-type procedures based on the identified symptoms. However, this approach, without any diagnosis, is a passive approach to the management of process disturbances, because the operator must wait until the symptoms are manifested following the inception of a failure condition.

The Level-Three approach adds diagnosis to the symptom-based approach to provide a comprehensive entity. The diagnosis can serve as an added line of defense against the propagation of disturbances. With diagnostic capabilities, the operator can pro-actively respond to process failure without simply waiting until the symptoms become apparent. The symptom-based procedures and systems will still play an important role as the second line of the defense against process failures or plant upsets.

In essence, the difference between Level-Two and Level-Three approaches is diagnosis. It is the purpose of this paper to present a comparative review of diagnostic methodologies that can be used to develop a computer-based diagnostic system. Section 2 briefly presents the rationale for the necessity of diagnosis from three different perspectives, i.e., fault propagation, plant risk, and accident prevention and management.

Section 3 compares some representative methodologies for failure diagnosis and management. Section 4 discusses the desirable features of advanced diagnostic methodologies that are derived from the insights gained from the comparative review of the methodologies. Section 5 gives the concluding remarks.

II. RATIONALE FOR THE NECESSITY OF DIAGNOSIS

There has been debate between professionals in the nuclear power community on the role of diagnosis in nuclear power plant operation and process management.^{2,3} Some professionals believe diagnosis is unnecessary, arguing that plant operators only need better "blueprints", such as symptom-based EOPs, to guide them through safe shutdown operations and procedures. In connection with the controversy, this section provides the rationale for the necessity of on-line process diagnosis from three different viewpoints, i.e., fault propagation, probabilistic risk assessment, and accident management.

A. Fault Propagation

Process disturbance in a continuous process plant such as a nuclear power plant is a "dynamic" phenomenon which propagates with time. If the incipient failure is not detected and rectified in a timely manner, it will further deteriorate the plant process. Moreover, the propagation of the disturbance through the process may challenge plant protection systems, safety systems, and plant operators. If the systems or operators do not properly respond when confronted with challenges, additional failures or operator errors will lead the plant into a more serious condition, making the recovery very difficult.

Therefore, it is very important to intervene in the propagation of the fault at the earliest stage possible. The earlier the escalating fault is detected and corrected, the more likely the process will be restabilized or recovered within a short time. Diagnosis makes possible the early detection and correction of the escalating fault. The early management of process disturbances through diagnosis will therefore enhance not only the plant's productivity but also its safety by avoiding unnecessary challenges to plant protection systems, safety systems, and operators.

B. Plant Risk

The benefits of an on-line fault diagnostic system can also be understood from the point of view of plant risk. According to the probabilistic risk assessments (PRAs) of nuclear power plants, initiating events are one of the critical elements that drive the plant risk.

The diagnostic system can keep an incipient failure from escalating into an initiating event of the PRA. For example, the failure of a main feedwater control circuit can be diagnosed and corrected before it propagates through the process and escalates into the loss of main feedwater event. Several studies have also shown that a large portion of events are preventable if their occurrence is recognized and stopped early in the progression.⁴ Thus, the use of a diagnostic system in the control room will reduce the frequencies of the initiating events, resulting in a reduction in the average plant risk, and thereby, in an improvement in operational safety.

C. Accident Prevention and Management

Accident management is that set of actions taken by the plant operating crew to gain control of the outcome of an abnormal event at the earliest possible time and with the minimum adverse consequences.⁵ It consists of two different parts, i.e., accident prevention and mitigation. Accident prevention can be considered as being the following two types of operator actions: (i) those that are routinely performed during normal operation to prevent any failure condition from occurring; (ii) those that are carried out during off-normal condition to prevent an incipient failure from escalating into an accident. The diagnostic system helps to diagnose the failure condition so that the operators can rectify it as soon as possible and with minimum adverse consequences.

III. DIAGNOSTIC METHODOLOGIES

The technological prerequisite of computer hardware and software engineering techniques for a computerized diagnostic system is now available due to remarkable advances in the techniques, including artificial intelligence and expert systems. The major obstacle to the development and installation of a diagnostic system in the control room of a nuclear power plant is the lack of a reliable methodology for diagnosis.

This section discusses in a comparative manner some representative methodologies which are classified into three major categories: event-oriented, process-oriented, and model-based methodologies. The shortcomings of each are also pointed out to shed light on the necessary and desirable characteristics of a more advanced methodology.

A. Event-Oriented Methodology⁴

There was a surge of interest in diagnostic systems or disturbance analysis systems (DASs) worldwide in late 1970s and early 1980s. During this period, several DASs were developed, including the EPRI-DAS by the Electric Power Research Institute (EPRI), and the STAR system by Gesellschaft für Reaktorsicherheit (GRS) of Germany and the OECD Halden Reactor Project.

These systems are based on an event-oriented fault propagation model, i.e., cause-consequence tree (CCT) or cause-consequence diagram (CCD).

A CCT/CCD is a formal representation of logical, causal, and temporal relationships among plant disturbances in terms of plant process parameters and component/system statuses. Once built and implemented into a DAS, the disturbance model then can be used in real time as an event template to monitor the plant process through the on-line process sensor readings that are continuously or periodically fed from the plant instrumentation and control (I&C) or data acquisition system. If the on-line process data match the low-level event template of the disturbance model, then the next-level template is scanned by the DAS, and so on. When a message set embedded in the model is encountered during the on-line scanning of the DAS, the message set is then presented to the operator on a cathode ray tube. The message set contains information such as plant status, predicted consequences, suggested recovery, and cause of disturbance. The disturbance model also may include time delays to model the minimum time that is expected to elapse between events.

The DAS developments were important in establishing the base computer technology from which many of the present operator aids have developed.⁶ However, in terms of the basic methodological schemes used, the diagnostic method based on the disturbance model of a CCT or CCD has the following drawbacks:

- 1) No systematic or structured algorithm is used for diagnosis. For example, to include a low-biased failure of a flow sensor in the model, the analyst should determine, without any aid, how the failure can be diagnosed on-line based on the information that is accessible from the data acquisition system.
- 2) In essence, the disturbance model contains only the paths of event propagations that are conceivable by the analyst. Hence, it cannot properly handle unanticipated events.⁵
- 3) A single huge model, e.g., a CCT in the EPRI-DAS, is used for many different types of functions such as diagnosis of sensor and equipment failure and incorporation of all the messages to be presented to the operator. Thus, it is very hard to construct or modify the model because of its inherent complexity and inflexibility.
- 4) A large set of on-line data from the data acquisition system are simply superimposed on the model during one update cycle without any selected use of the sensor data

Furthermore, the diagnostic or disturbance analysis is performed using the "snapshot-type" data without taking into account the dynamics of the sensor data.

B. Process-Oriented Methodologies

Over the years, many different types of process-oriented methodologies for diagnosis were proposed. A common characteristic of these methodologies is their systematic representation of the fault-propagation structure. Compared to other methodologies, these possess superior capabilities for process representation.

1. Digraph-Based Methodology⁷

A digraph is a set of nodes connected by signed branches. The nodes represent process variables or certain types of failures, and the branches or directed edges indicate cause-effect relationships between the nodes. The signs on the directed edges represent the direction of deviations of the two process variables from normal values. A positive sign indicates that the deviations occur in the same direction, while a negative sign denotes that the deviations occur in the opposite direction.

Various attempts have been made to use the digraph model for on-line diagnosis of failure. One of the most typical approaches is to use a fault tree which is derived off-line or on-line from the digraph.⁷ Such a fault tree is different from the ones typically used in PRAs in that it may contain, in addition to the equipment failure events, the events representing process variable deviations, sensor failure events, or other events that are not normally modeled in the PRA fault trees. The branches of the process fault tree or the cut sets for a top event, the occurrence of which has been detected by the on-line sensor data, then is searched in real time to diagnose the failure.

2. Logic Flowgraph Methodology⁸

The logic flowgraph is similar to digraphs in the way of representing fundamental causality relations of the process. However, in addition to this causality network, the logic flowgraph methodology (LFM) also introduces another model, called condition network, to explicitly represent the conditions whose occurrence can change or modify the course of process causality flow in the fundamental causality network. Thus, the LFM can be used to model the complex cause-effect relations existing between plant physical parameters, control variables, protective devices, and failure mechanisms.

For on-line diagnosis of failure, the logic flowgraph is stored in a computer, combined with input signals from the plant instrumentation, and automatically analyzed on-line to produce diagnostic trees and recovery trees. A diagnostic

tree for the top event corresponding to an arising situation or process condition is developed, and used on-line to find out what caused the top event of the diagnostic tree to occur by validating or eliminating tree branches on the basis of the process instrumentation. After providing the plant operators with diagnostic information, the logic flowgraph stored in the computer memory then is used to derive a recovery tree by setting the top variable and the other variables that have been perturbed to their unperturbed values. The computer processing of this recovery tree produces information on the recovery of the failure.

Although the LFM is based on a logic flowgraph which has higher process-modeling capabilities than the conventional digraph, the two process-oriented methodologies are similar in their diagnostic algorithm in that a tree derived from a fault-propagation model is used for diagnosis. These methodologies have the following shortcomings.

- 1) Essentially all the information or knowledge for the diagnosis is contained in a single fault-propagation or disturbance model, i.e., a digraph in the digraph-based method, and a logic flowgraph in the LFM. Hence, there is a problem of modeling complexity. This problem is greater in the LFM as a side effect of its higher capabilities for process modeling. For this reason, a computer program was designed to allow computer-assisted construction of the logic flowgraph.
- 2) All the available information should be used for diagnosis. However, the diagnosis is performed only on the basis of causality relationships among process variables and parameters that are modeled in the disturbance model.
- 3) The fault tree or diagnostic tree derived from the fault propagation structure is an instantaneous "snapshot" of a set of system states. As a result, the diagnosis does not take into account the dynamic information of the plant process variables that may sometimes provide further clues when properly used.

C. Model-Based Methodology -- MOAS-II^{9,10}

The MOAS-II model-based methodology is quite different from the other methodologies discussed in that it uses several different models for different functions that are needed for failure diagnosis and management. The failure models used on-line are sensor failure diagnosis trees (SFDTs) and hardware failure diagnosis (HFD) modules. The SFDTs are used specifically for sensor failure diagnosis, while the HFD modules for hardware (except sensors) failure diagnosis.

The SFDTs are developed using sensor validation criteria (SVCs), i.e., coherent relationships among the sensor data based on deep knowledge such as conservation equations. The combined use of the SVCs in the framework of an SFDT allows sensor failures to be diagnosed. On the other hand, the HFD modules are developed from a model called a simplified directed graph (SDG), which is a simplified version of the conventionally used digraph; as such, it is easier to construct or modify than the digraph or logic flowgraph. Thus, the modeling of fault propagation is simplified, mainly because sensor and hardware failures are modeled separately.

Another conceptual difference in diagnosis between the MOAS-II methodology and especially the process-oriented methodologies is the following. In process-oriented methodologies, the diagnosis is carried out with a fault tree or diagnostic tree that is derived from the fault propagation model for the top event indicating a deviation in a process variable or parameter, e.g., high temperature at a process point. A deviation in any variable or parameter that is modeled in the disturbance model may become the top event, the cause of which will be determined on-line by the diagnostic system. However, the diagnosis in the MOAS-II methodology focuses only on the important process variables. The process disturbance pattern in terms of these variables is identified on-line, and the failure hypotheses contained in the relevant HFD module are checked one by one until a hypothesis is verified based on the on-line sensor data.

The MOAS-II methodology has the following shortcomings:

- 1) To prepare HFD modules, the failure hypotheses for each identified process-disturbance pattern should be extracted off-line from the fault propagation model, i.e., the SDG; this process may require a great deal of effort since no aid is provided.
- 2) The method for diagnosing sensor failure in the framework of SFDTs is tailored to the process environment consisting of "few like-measurements". The method should be extended such that it can easily accommodate redundant sensors.

IV. DESIRABLE CHARACTERISTICS OF ADVANCED DIAGNOSTIC METHODOLOGIES

Based on the comparative review of various diagnostic methodologies, the desirable characteristics of advanced methodologies are derived and summarized below from the three elements of failure management, i.e., failure detection, diagnosis, and correction.

Failure Detection

To diagnose a failure, the anomalous process condition caused by the failure should be first detected by a process monitoring scheme. Process monitoring, typically, has not been given sufficient considerations in developing diagnostic methodologies. It not only triggers the diagnosis, but also can serve as a barrier against further fault propagation. The reason for the possibility of further propagation in spite of the diagnostic system is that the content of the diagnostic package may be incomplete or the diagnosis may not be completed fast enough. Thus, proper messages should be provided to the operator when the process has deteriorated too much, even if the cause of the failure condition is not yet determined. Preferably, this process surveillance function should be incorporated into a module which is independent from the diagnostic module.

It is also important to design an effective process-monitoring scheme to reduce unnecessary burden on the computer and also improve computational efficiency. For example, only the sensors for important process variables, such as controlled variables, can be monitored during normal operation. Furthermore, the normally monitored sensors need not be scanned at the same interval, e.g., 5 seconds. The optimal intervals for different sensors can be determined from the dynamic characteristics of the process. The scan intervals may be shortened to monitor transient behaviors when the associated sensors indicate abnormalities.

Failure Diagnosis

Instrumentation failure is a common problem in nuclear power plants. The erroneous data acquired from malfunctioning sensors may corrupt the real-time inference process of the diagnostic system, resulting in a misdiagnosis which must be avoided at all costs.⁴ Therefore, provisions should be made so that sensor data can be validated and, furthermore, sensor failures can be diagnosed.

In developing a model for diagnosis, it is extremely important to first recognize the difference in the characteristics of sensor and hardware failures. Hardware failures usually propagate through the plant process and deteriorate the process condition. On the contrary, sensor failures do not cause any deterioration of the process, unless the sensors are used in the plant control system. Therefore, a fault-propagation model can be developed considering only hardware failures, and sensor failures that affect the process directly, if any. The model will represent the effects of the failures on the process variables and parameters, and the subsequent fault-propagation paths through the process based on the underlying physical principles and process characteristics.

Validation of sensor data often has been considered separately from the failure diagnosis. However, it should be, preferably, performed in the global context of the diagnosis, since the information gained from the sensor validation can be useful for the diagnosis.

Deep knowledge of the process can be effectively used to diagnose failure as was demonstrated elsewhere.^{10,11} To use such knowledge, the raw, quantitative process data should be directly used, where possible, without being transformed to qualitative data such as high, low, or normal. Hence, provisions should be made to use this deep knowledge in terms of quantitative data.

Failure Correction

The ultimate goal of a diagnostic system is to present appropriate messages to the operators so that they can control the outcome of a failure condition at the earliest possible time and with minimum adverse consequences. Hence, sufficient considerations should be given to the messages. For example, in addition to the diagnosis messages indicating the cause(s) of failure, other messages, such as the following, may be provided to the operators:

- messages that present an operational aid, e.g., the recommendation of verification points to check or specific operating procedure to follow, and
- messages that pre-alarm the operators before something serious, e.g., severe process degradation or a plant trip, is likely to occur.

When messages are incorporated in several modules, such as those for process monitoring and failure diagnosis, conflicting messages may result during the inference process.¹⁰ Hence, provisions should be made to avoid the formulation of such conflicting messages.

In addition to those characteristics discussed in relation to failure detection, diagnosis, and correction, the advanced methodologies should be transparent, easy-to-modify, easy-to-implement, robust to unanticipated failures, such as complex multiple failures. Separation of sensor and hardware failure diagnoses greatly helps towards the first three requirements. The incorporation of an elaborate process-monitoring scheme helps to ensure that the diagnostic system is robust against unanticipated failure conditions, in cases where the complex conditions cannot be diagnosed in due time or because of the limitation of the diagnostic module.

Expert system techniques can also help to achieve the characteristics of transparency and easy modifiability. The major characteristic of expert systems is the separation of the knowledge base from the inference mechanism. As a result,

the expert systems are transparent in knowledge representation and, thereby, easy to modify, compared to systems based on conventional programming techniques. Although a reliable method for the verification and validation of expert systems has not been fully developed, diagnostic systems based on explicit models such as those described in this paper can be verified and validated far more easily than model-free expert systems. Therefore, a diagnostic methodology can preferably be implemented into an expert system to take advantage of the techniques. The important role of expert systems in failure diagnosis has also been proved in the FALCON (Fault Analysis Consultant) project, conducted in the chemical process industry.¹¹

V. SUMMARY

The on-line diagnosis of process failure enables a process failure to be arrested at the earliest possible time and with the minimum adverse consequences. The early management of process failure will result in dual benefits in nuclear power plant operation, namely, 1) the improvement of safety by preventing the occurrence of accidents by intervening in the development of a minor failure into a major accident, and 2) the improvement of plant availability by avoiding unnecessary reactor scrams.

REFERENCES

1. 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.
2. S. Guarro, "Comment: Safe Shutdown or Fault Diagnosis? Some Thoughts on Goals and Philosophy for Nuclear Plant Management Systems," Reliability Engineering and System Safety, Vol. 28 (1990) 311-314.
3. I.S. Kim, M. Modarres, and R.N.M. Hunt, "Comment: Toward the Practical Use of Expert System Technique for Process Disturbance Management," in Ref. 2, 314-317.
4. C.H. Meijer and B. Frogner, "On-Line Power Plant Alarm and Disturbance Analysis System," EPRI Report NP-1379, Final Report, April 1980.
5. R. DiSalvo, M. Leonard, M. Manahan, and J. Wreathall, "Management of Severe Accidents: Perspectives on Managing Severe Accidents in Commercial Nuclear Power Plants," NUREG/CR-4177, BMI-2123, Vol. 1, May 1985.
6. D.G. Cain, "Review of Trends in Computerized Systems for Operator Support," Nuclear Safety, Vol. 27, No. 4 (October-December 1986) 488-498.

7. N.H. Ulerich and G.J. Powers, "On-Line Hazard Aversion and Fault Diagnosis in Chemical Processes: The Digraph + Fault-Tree Method," IEEE Transactions on Reliability, Vol. 37, No. 2 (June 1988) 171-177.
8. 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) 348-359.
9. I.S. Kim, M. Modarres, and R.N.M. Hunt, "A Model-Based Approach to On-Line Process Disturbance Management: The Methodology," in Ref. 2, 265-305.
10. 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) 185-239.
11. P.S. Dhurjati, D.E. Lamb and D.L. Chester, "Experience in the Development of an Expert System for Fault Diagnosis in a Commercial Scale Chemical Process," Proc. First Intl. Conf. on the Foundations of Computer-Aided Process Operations, Park City, UT, 1987.