MARYLAND

TECHNICAL
RESEARCH
REPORT

SRC TR 88-111

A Model-Based Approach to On-Line Process Disturbance Management: The Models

by

I. S. Kim, M. Modarres, and
R. N. M. Hunt

SYSTEMS RESEARCH CENTER

UNIVERSITY OF MARYLAND

COLLEGE PARK, MARYLAND 20742

A Model-Based Approach to On-Line Process Disturbance Management: The Models

I. S. Kim and M. Modarres
Department of Chemical and Nuclear Engineering
University of Maryland, College Park, MD 20742, USA

R. N. M. Hunt
Idaho National Engineering Laboratory, Idaho Falls
Idaho 83415, USA

ABSTRACT

A methodology is proposed which can be used to design real-time expert systems for on-line process disturbance management. This methodology encompasses diverse functional aspects that are required for an effective process disturbance management: 1) intelligent process monitoring and alarming, 2) on-line sensor data validation and sensor conflict resolution, 3) on-line hardware failure diagnosis, and 4) real-time corrective measure synthesis. Accomplishment of these functions is made possible through the integrated application of the various models, goal-tree success-tree, process monitor tree, sensor failure diagnosis, and hardware failure diagnosis models. This paper presents and discusses the various models along with the overall algorithm of the methodology. The application of the methodology to a target process, a typical main feedwater system of a nuclear power plant which employs a complex control mechanism, will be presented in a companion paper.

1 INTRODUCTION

Process disturbance management is one of the most important and difficult tasks the control room operators of large process plants should perform. It is not only because the problem at hand is complicated, but also because the operator-process interfaces of the plants are frequently designed such that the incumbent process problem far exceeds the human cognitive capability. Failure to cope with process disturbances not only leads to large capital losses, but also can have a serious impact on public safety.

Much research has been carried out, especially since the Three Mile Island Unit-2 (TMI-2) incident, to improve the operator-process interface. Notable outcomes are (1) integrated display systems such as Safety Parameter Display System (SPDS)[1] and Critical Function Monitoring System (CFMS)[2] for presenting consolidated important process parameters to the operator, (2) alarm analysis systems[3,4] for alarm processing and displays, and (3) disturbance analysis systems[5-7] for a more comprehensive treatment of disturbances.

The integrated display systems provide concise displays of the plant safety or critical function statuses; whereas, the computer-based alarm analysis systems preprocess or filter the raw alarm information acquired from the conventional alarm system. However, these systems do not diagnose the cause of the process disturbance nor present the course of operator corrective action to be undertaken.

The disturbance analysis systems (DASs) are more ambitious systems than the integrated display or alarm analysis systems, since they cover the whole problem of fault administration, i.e., fault detection, diagnosis, and correction. Two representative DASs are the EPRI-DAS[5] and the STAR system[6] jointly developed by West Germany and Norway. The main mechanisms used in both of these two systems were cause-consequence trees (CCTs) or diagrams, variations of fault trees for on-line tracking and diagnosis of disturbances using the instrument readings. The major drawbacks of the CCT approach are demonstrated by the facts that the event-chain-type trees are very complicated and difficult to build or modify and the fault diagnostic approach is neither systematic nor transparent. Another severe limitation of the CCT approach is the difficulty in modeling dynamic systems with feedback in the tree structure.[7]

As the computer techniques evolve, various attempts have been made recently to apply more advanced computer techniques such as knowledge-based expert systems[8,9] to the development of intelligent operator support systems. One of the earliest attempts to apply expert system technology to the operation of nuclear power plants was the development of REACTOR,[10] a prototype expert system to assist operators in the diagnosis and treatment of nuclear reactor accidents. The accident diagnosis by REACTOR is performed using event-oriented knowledge, which consists of a small number of known accidents and their associated symptoms. If an accident cannot be diagnosed using the event-oriented knowledge, then a function-oriented strategy based on a response tree--a graphical representation showing all the available success paths for a given safety function--is used to treat the accident.

Another recent example is a real-time expert system, DIAREX,[11] which diagnoses nuclear power plant failure and offers a corrective operational guide. The main analysis scheme of this expert system is a fault propagation tree constructed by combination of top-down fault tree analysis and bottom-up failure mode and effects analysis. However, this fault propagation tree is also an event-chain-type tree like a CCT, and therefore has similar shortcomings as the CCT approach.

In the arena of chemical industry, efforts have been devoted to process malfunction diagnosis in complex chemical processes. In order to explore the potential of expert systems for on-line fault diagnosis in commercial chemical plants, an expert system called FALCON (Fault AnaLysis CONsultant)[12-14] was developed in a joint research effort of the E.I. duPont de Nemours & Company, the Foxboro Company, and the University of Delaware. Important findings of the FALCON project indicate that expert systems technology will have a major impact on future chemical plant operation, and that for fault diagnosis the expert system has a distinct advantage over humans and can therefore outperform them.[14]

However, missing from the knowledge-based expert system approaches to fault diagnosis or disturbance analysis is an easy-to-use, transparent, and systematic methodology. In this paper, we propose such a methodology which can be used to design real-time expert systems[15-20] for on-line process disturbance management. This methodology embraces the following comprehensive aspects: (1) intelligent process monitoring and alarming, (2) on-line sensor data validation, (3) on-line sensor and hardware (besides sensors) fault diagnosis, and (4) real-time corrective measure synthesis.

In order to provide the reader with an overview of the methodology, the characteristics of the methodology will be presented along with the design steps used in building an operator advisory system for process disturbance management.

The characteristics of the proposed approach include the following:

(1) The methodology is model-based and intended to be used for building an on-line, real-time expert system.

(2) The models used in the methodology facilitate not only the knowledge acquisition process, but also the reasoning process of the expert system. These well-developed models and model-based reasoning greatly enhance maintainability of the knowledge-based system and thereby reduce the maintenance costs.[21]

(3) The various developed models work together as an integral unit for the single purpose of process disturbance management.

(4) The diagnostic schemes are transparent and systematic.

(5) Sensor data validation is performed as part of the global fault diagnosis process. Sensor validation often has been considered separately from the fault diagnosis. However, it should be performed preferably in the global context of the diagnosis,[22] since the information gained from the sensor validation process can be effectively utilized to diagnose the cause of system fault.

(6) Deep knowledge, i.e., underlying physical knowledge, is used for diagnosis instead of shallow knowledge, i.e., plant-specific experiential compilations of the underlying principles.

(7) Implementation of conventional diagnostic methods has been based only on the "qualitative" data transformed from the raw, quantitative process data. The diagnostic algorithm, which was

developed by Shiozaki et al.[23] and is discussed in Section 5 of this paper, is a typical example. However, the "quantitative" process data can be effectively used particularly in relation to the application of deep process knowledge. In the diagnostic method proposed in this paper, the quantitative process data is effectively used for diagnosis as will be shown later. The FALCON research team also claims that application of quantitative, deep knowledge based on first principles is the most effective method of malfunction diagnosis.[14]

(8) The situation-specific nature of the approach eases the incorporation of heuristics in the knowledge base. Although the applicability of heuristics is usually quite narrow, the heuristics can be an efficient shortcut to problem solving in certain situations.

The design steps of the real-time operator advisory system in terms of the proposed models evolve as follows:

(1) Construct a goal-tree success-tree model for the operation of the target process.

(2) Identify process monitoring points from the goal-tree success-tree model.

(3) Develop a process monitor tree for each of the process monitoring points.

(4) Build a sensor failure diagnosis tree for each of the process monitoring points.

(5) Construct a simplified directed graph for each of the operating configuration of the target process in order to model the fault propagation structure.

(6) Develop hardware failure diagnosis modules from each of the simplified directed graph.

(7) Generate a module for the determination of plant operational mode.

(8) Design an appropriate real-time inference control scheme.

A real-time operator advisory system, named MOAS II, has been developed based on the proposed model-based approach in PICON, a real-time expert system shell. The target process for which the methodology was applied is a typical main feedwater system of a pressurized water reactor (PWR) nuclear power plant.

MOAS II has been tested in a simulated process environment against many transient scenarios. The test results show that MOAS II successfully performs its intended functions, i.e., intelligent process monitoring and alarming, real-time fault diagnosis, and corrective measure synthesis. Therefore, such an expert system can be used as a valuable operator aid for on-line process disturbance management.

This paper presents the proposed methodology in a generic sense. The application of the approach to the target process, the rational for selecting the feedwater system as a target process, and the performance test and evaluation of MOAS II will be presented in a companion paper.

Section 2 of this paper describes the role the goal-tree success-tree model plays in process disturbance management. The models of process monitor trees, sensor failure diangosis trees, and hardware failure diagnosis modules are addressed in Sections 3 through 5, respectively. The module used for the determination of plant operational mode is discussed in Section 6, and the overall algorithm of the methodology is presented in Section 7. Conclusions are addressed in Section 8.

2 PROCESS GOAL-TREE SUCCESS-TREE MODEL

The first step in developing a real-time expert system for process disturbance management is to construct a goal-tree success-tree (GTST) model for the target process for which the expert system is being built. The concept of GTST model has been successfully applied for a variety of engineering applications,[24-29] and the procedure for developing a GTST can be found in refs 24-26. Therefore, only the role the GTST model plays in process disturbance management will be described in this paper.

By constructing a GTST model for the target process, the complex knowledge of the process and its operation can be well-organized in a logical and complete fashion. Such a well-organized knowledge structure can then be used 1) to identify process monitoring points, and 2) to develop a module for the synthesis of global corrective measures, i.e., the determination of optimum plant operational mode, following a partial loss of the process.

Process monitoring points are sensors which should be continuously or periodically monitored by the computerized operator aid in order to achieve the top objective defined in the GTST. Since the module for the determination of optimum plant operational mode is discussed in Section 6 separately, only the method of how to identify the process monitoring points from the GTST will be illustrated here.

The GTST model shown in Fig. 1 is developed as an example with a defined top objective of "Cycle Equivalent Availability Maximized." Assuming that there is a subgoal defined somewhere in the GTST model as "Feedwater Inventories in Both Steam Generators Proper," we can further develop the GTST by asking a question: How can this subgoal be achieved?. Since this subgoal can be achieved by maintaining a normal water level at each steam generator, we can obtain an equivalent subgoal, "Normal Water Level at Each Steam Generator Maintained."

This subgoal can then be broken down into two lower-level subgoals, i.e., "Normal Water Level at Steam Generator 11 Maintained" and "Normal Water Level at Steam Generator 12 Maintained." Since the normal water levels should be maintained at all times for the achievement of the top objective, we can identify that it is necessary to continuously or periodically monitor the process conditions represented in the bottom subgoals. Assuming that LT511 and LT512 are level sensors of steam generators 11 and 12, respectively, it is therefore possible to identify two process monitoring points from the GTST in this simple example.

3 PROCESS MONITOR TREE MODEL

All the generic models except the GTST, i.e., process monitor tree, sensor failure diagnosis tree, hardware failure diagnosis modules, and plant operational mode module, will be used "on-line" for process disturbance management. However, among the models used on-line, only the process monitor tree will be used "on a continuous basis" by the real-time computer system, whereas all the other models will be used only "on a demand basis."

Fig. 2 shows a specific relationship of the models used on-line. The process monitor tree model monitors the process operation continuously through the on-line sensor data fed into the model. The models of sensor failure diagnosis tree and hardware failure diagnosis modules are activated for on-line use, only when there is a demand from the process monitor tree model. On the other hand, the demand to activate the plant operational mode module may come from any of the three models, i.e., process monitor tree, sensor failure diagnosis tree, and hardware failure diagnosis modules.

This section describes development procedure and on-line use of the process monitor tree model. All the other models used on-line will be described later.

3.1 Development of PMT models

The process monitor tree (PMT) is the structure used to model an intelligent process monitoring scheme, and is constructed for each process monitoring point identified in the GTST. The steps followed during development of a PMT are as follows:

1. Determination of Appropriate Boundaries and Thereby Value Bands for the Process Monitoring Point

Fig. 3 shows sample boundaries of value bands and significant value bands for the process monitoring point, LT511, identified in the illustrative example of the previous section. The value band between NL and NH is a normal operating range, not a significant value band.

The determination of boundaries and their numerical values for process monitoring points may require extensive considerations of the process, especially when the computer-based operator support system is developed at the early design stage of the plant. If the computerized operator aid is built for retrofit to an existing plant, the various setpoints of the plant--such as alarm or trip setpoints--may be used as the boundaries of value bands in a PMT. But, in this retrofit case, the appropriate allocation of the functions should be considered among the existing alarm and trip systems and the computer-based operator support system for field applications of the computer-based system.

2. Identification of Appropriate Headings and Construction of the Tree Structure of a PMT

Fig. 4 illustrates a sample PMT constructed for the process monitoring point, LT511. The first heading of a PMT is normally value band as in the sample PMT, and significant value bands and the ssociated numerical values identified in step 1 are specified at the branches under the first heading.

The second heading identified for the PMT is trend of change, because it is considered necessary to determine the trend of change in the sensor value when it is within a certain significant value band, i.e., between L and NL or between NH and H. For instance, when the reported sensor value is between L and NL, the event is considered to be significant only if the dynamic trend of change is nonincreasing. In other words, if the sensor value lies within the value band between L and NL and increasing, then the event is insignificant. However, if it lies within the same value band but decreasing or static, i.e., neither decreasing nor increasing, then the event is significant.

Once a significant event is detected in the tree, it is necessary to perform sensor validation in order to test whether the sensor is working properly. (Sensor validation will be described in detail in Section 4.) Therefore, sensor validation is added as the third heading of the PMT. However, sensor validation need not be performed if LT511, i.e., the sensor reading reported by the LT511 sensor, is less than or equal to LLA, or larger than or equal to HHA, since it is assumed that the trip function is not incorporated in the computer-based operator support system for which the PMT is built.

The last heading, operating status of feed pump bank, is included in the tree because, depending on the status, different PMT messages need to be developed and different hardware failure diagnosis units (see Section 5) need to be specified.

Besides the headings shown in Fig. 4, other kinds of headings such as controller operational mode-- automatic or manual--or control valve status--open or closed--can also be used. For example, if it is considered necessary to check the operational mode of a controller, the heading, controller operational mode, can be added in the tree structure of the PMT.

3. Development of PMT Message Sets

As stated earlier, the tree structure of the PMT will be activated on-line at a periodic scan interval to monitor the process. If something anomalous, i.e., deviation from the normal process condition, occurs in the system, it will be detected in the PMT to result in an on-line actuation of a PMT branch--satisfaction of all the conditions along the branch. The computer-based operator aid will then have to present message(s) to the operator, in order to inform him of the abnormal situation, or to provide an operational aid or corrective measure. Therefore, development of a message set for each branch of the PMT is necessary, so that it can be presented to the operator if the branch is actuated on-line.

However, no PMT message set needs to be developed for the branch which includes the condition of sensor invalidated, since the information from the invalidated sensor is not believable (refer to Fig. 4). In this case, sensor failure diagnosis will be normally performed in the sensor failure diagnosis tree discussed in Section 4, and an appropriate message set will be transmitted to the operator from the sensor failure diagnosis tree model, not from the PMT model.

In the PMT shown in Fig. 4, PMT messages are represented with message identifiers such as PMT-LT511-LLA or PMT-LT511-LLA.L, the details of which can be found in Table 1. In the table, symbols such as PD or CM appear in front of every message. These symbols represent the taxonomic classifications of the messages, which are described separately in Section 3.2.

4. Identification of the Need for Failure Diagnosis

Occurrence of a process disturbance will be detected in the PMT models for process monitoring points. Since the process situation will become more and more deteriorated if the disturbance is not diagnosed and rectified in a timely fashion, on-line fault diagnosis should be normally performed following the detection of a process anomaly. The need for diagnosis can be specified in the PMT model.

Process disturbances may occur as a result of sensor or hardware failures. (Recall that all the components except sensors are called hardware in this paper.) Hence, provisions should be made to diagnose both kinds of failures. In the approach proposed in this paper, both kinds of failures are dealt with in separate models: namely, sensor failure in sensor failure diagnosis trees and hardware failure in hardware failure diagnosis modules.

Therefore, if diagnosis is considered necessary, the kind of diagnosis should be specified in the PMT. Sensor failure diagnosis will be normally needed, when the sensor value is not validated. In this case, "SFD" can be specified in the PMT model as shown in Fig. 4. However, if hardware failure diagnosis is considered necessary, not only the need but also the proper hardware failure diagnosis unit (see Section 5) can be specified in the PMT. For example, in the "Need for Diagnosis" column of the sample PMT model (Fig. 5), a symbol such as HFD-FWCS-11-L or HFD-FWCS-12-L indicates the hardware failure diagnosis unit, which should be used in the circumstance of system operating configuration and process disturbance as reflected by the actuated PMT branch.

5. Identification of the Need for a Change in the Plant Operational Mode Due to Severe Process Degradation

If the process condition is significantly degraded such that the plant operational mode should be changed to protect equipment(s), continue the operation, or prevent further degradation, then the need for a change in the plant operational mode "due to the severe process degradation" can be indicated in the PMT.

The ideal situation will be one in which the cause of the fault is diagnosed and corrective measures taken, before the process is deteriorated so severely that the plant operational mode should be changed based on the detection of severe process degradation. This is because the process is more likely to be restablized, if corrective actions are based on failure diagnosis rather than detection of severe process degradation.

3.2 Taxonomic classifications of messages

The decisions made by the computer-based operator aid should be presented to the operator in a form of messages. In order to improve the operator-computer interface, the messages have been classified in the following six taxonomic categories according to their nature:

(1) Process Degradation [PD]: The message in this category alerts process degradations.

(2) Diagnosis [DG]: Presents sensor or hardware failure diagnosis results.

(3) Component Status [ST]: Presents statuses of components which are important at a given time instant and for the specific plant operating mode. Examples are the operational mode of a controller

--automatic or manual--or the status of an on-off control valve--open or closed.

(4) Prealarming [PA]: Prealarms before something serious such as severe process degradation or plant trip is likely to occur.

(5) Operational Aid [OA]: Presents an appropriate operational aid such as the recommendation of verification points to be checked or operating procedures to be followed.

(6) Corrective Measure [CM]: Presents a course of optimal corrective measures.

In order to indicate the taxonomic category to which the message belongs, the abbreviation of the category will be specified for every message. For example, the message set of PMT-LT511-LLA in the sample PMT (Fig. 4) contains two kinds of messages, i.e., PD and OA, as represented in Table 1.

3.3 On-line use of PMT models

The PMT models developed off-line will be implemented into a real-time operator advisory system together with other models described later, and the operator advisory system will be used for on-line process disturbance management. Fig. 5 shows a flow chart, which describes the on-line use of a PMT model.

Once a PMT branch is actuated on-line, the PMT message set associated with the branch, if any, will be first presented to the operator. Then, other models used on-line on a demand basis, i.e., sensor failure diagnosis tree, hardware failure diagnosis unit, or plant operational mode module, will be activated depending on the kind of need indicated in the actuated PMT branch:

(1) Need for Sensor Failure Diagnosis: The sensor failure diagnosis tree, for the same sensor as that for which the PMT is built, will be activated on-line (refer to Section 4).

(2) Need for Hardware Failure Diagnosis: The hardware failure diagnosis unit indicated in the PMT branch will be activated on-line (refer to Section 5).

(3) Need for a Change in the Plant Operational Mode: The plant operational mode module will be activated on-line (refer to Section 6).

For example, the bold-faced branch in the PMT shown in Fig. 4 is actuated, if (1) LT511, i.e., the sensor value reported by the LT511 sensor, falls into the significant value band between L (i.e., -24 inches) and NL (i.e., -12 inches), (2) LT511 is nonincreasing, (3) LT511 is validated, and (4) both feed pumps have been operating. Once the PMT branch is actuated on-line, the PMT-LT511-L.NL message set will be presented to the operator first, according to the flow chart shown in Fig. 5.

Following the presentation of the message set, hardware failure diagnosis will then be performed in the hardware failure diagnosis unit HFD-FWCS-2-L, which is indicated in the actuated PMT branch. The plant operational mode module will not be activated in this case, since it is indicated in the actuated PMT branch that there is no need to change the plant operational mode upon the detection of a significant event in the PMT model. However, the plant operational mode module may be activated on-line following the completion of hardware failure diagnosis process in the hardware failure diagnosis unit. This will be further discussed in the following sections.

4 SENSOR FAILURE DIAGNOSIS TREE MODEL

Sensors play an important role in process plants. Sensor data displayed in the control room are major sources of information from which operators are able to infer process conditions. Some sensor values are used as inputs to the control or alarm systems, while others are used to trigger automatic trip mechanisms for equipment or plant protection. However, these sensors may fail to properly function, e.g., due to stuck failure or biased failure, and indicate erroneous process conditions, causing false alarms or spurious trip demands. Failed sensors may also degrade the performance of a control system directly, if the sensor signals are used as inputs to the controllers. In the case of on-line computerized operator aid systems whose dynamic decisions are based on the on-line sensor values, the real-time inference process may be corrupted by erroneous data acquired from malfunctioning sensors.

Therefore, provisions should be made to detect erroneous sensor data or sensor failures. The nuclear and aerospace industries have developed various techniques for signal validation and sensor fault identification[30-33] which are useful mostly in a process environment consisting of "many like-measurements" such as the process environment found in a nuclear reactor in a nuclear power plant. However, process signal validation and fault diagnosis method useful in a process environment consisting of "few like-measurements," like the secondary side of a nuclear power plant, is poorly dealt with in the literature.

This paper presents a method which can be used for on-line sensor data validation and sensor fault diagnosis in the process environment consisting of "few like-measurements." The proposed method is based on the effective use of coherent relationships among process variables and parameters which are formulated from deep process knowledges such as:

-- conservation equations (mass or energy balance),
-- pump performance curves,
-- control algorithmic equations for contol loops,
-- correlation between control valve opening and flow rate, or
-- redundant informations from redundant sensors (if any).

For example, one can formulate a coherent relationship among sensor values around a constant-speed pump based on the pump performance curve as follows:

$$\text{ABSOLUTE}\ [PT12 - PT11 - 0.433 * (-0.000031 * FT11^2 + 0.36 * FT11 - 152)] < \text{tolerance}$$

where PT11, PT12, and FT11 represent the suction pressure, discharge pressure, and flow sensors, respectively, and the constant 0.433 is a unit conversion factor. It is assumed here for the sake of simplicity, that the pump curve can be represented as a second-order algebraic equation. The above relationship consists of three process variables or sensor values which continuously change in the dynamic process environment during normal or off-normal operation. It is also important to recognize that a tolerance level has been imposed on the relationship to accomodate the inherent process noise, measurement error, and the uncertainty in the estimation of pump performance. In fact, even in the case of relationships based on a conservation equation or control algorithmic equation, the imposition of a tolerance level is necessary since the equations do not close exactly in a real situation.

The difference between the two pressure sensors, PT12 - PT11, represents the pressure head developed by the pump, whereas the expression, $0.433 * (-0.000031 * FT11^2 + 0.36 * FT11 - 152)$, represents the pressure head increase due to the pump as predicted by the pump performance curve. Simply speaking, the first expression, i.e., the differential pressure, reflects the "actual" pressure head increase, provided that both PT11 and PT12 sensors are functioning successfully, and the second expression reflects the "expected" pressure head increase, provided that the FT11 sensor is working properly. If the pump curve truly represents the actual performance of the pump and all the three sensors, i.e., PT11, PT12, and FT11, are functioning successfully, then the two kinds of pressure head increases should be equal to each other within the tolerance level. In other words, the above relationship must be satisfied by the three on-line sensor values as long as all the three sensors are working successfully. Therefore, the relationship can be used 1) to validate PT11, PT12, or FT11 sensor values, or 2) to test the performance of a sensor, say PT11, if the performance of PT11 is suspected at a certain time.

The coherent relationship discussed above will be called sensor validation criterion (SVC) in this paper. The sensor validation criteria (SVCs) should be formulated in terms of process variables, e.g., sensor value or position of a variable control valve, or process parameters, e.g., operational mode of a controller, that are accessible from the real-time process data base.

The determination of an appropriate tolerance level in formulating an SVC is very important for successful application of the SVC. This results from the fact that the use of too high a tolerance level can cause the SVC not to be violated even if a sensor failure occurs, while the use of too low a tolerance level can result in violation of the SVC even if no failure occurred.

If the computer-based operator support system is developed during early stages of plant design, then the determination of an appropriate tolerance level can be quite complicated, since no actual process data will exist. However, if the operator support system is developed for retrofit to an existing plant, the optimal tolerance level may be found quite easily by evaluating the expression of the SVC using the actual plant data.

For instance, in the above example relationship based on a pump curve, the left-hand side of the inequality can be evaluated using the three sensor values obtained from the plant data base during normal operation and various transient conditions under which the SVC is expected to be used. An appropriate tolerance level for the SVC can then be found such that the SVC is satisfied at all times unless any of the three sensors or the pump (this pump is included in this case, since the pump failure can also cause the violation of the SVC based on the pump curve even if all the three sensors are functioning successfully) is malfunctioning. The tolerance level should also be such that the SVC is violated if a sensor or pump failure occurs.

4.1 Development of SFDT models

As stated earlier, the proposed sensor failure diagnosis method is based on the effective use of SVCs, i.e., coherent relationships among process variables and parameters. Hence, it is first necessary to formulate SVCs before developing models for sensor failure diagnosis.

The sensor failure diagnosis tree (SFDT) model provides a framework within which the formulated SVCs can be effectively used. The method for developing an SFDT model will be illustrated here with the sample SFDT in Fig. 6.

The sample SFDT is built using three coherent relationships, SVC-1, SVC-2, and SVC-3, which consist of three, four, and three items, respectively. The constituents of the SVCs may be an on-line sensor reading, a controller output, and so forth, which are accessible through the real-time control data base.

The first step in developing an SFDT model is to select a primary sensor validation criterion (PSVC) from the SVCs containing the primary sensor. To clarify the terminology, a primary sensor is a sensor for which the SFDT is built, while a primary sensor validation criterion is an SVC by which the validity or acceptability of a primary sensor is tested. For instance, in Fig. 6, sensor A is a primary sensor, while SVC-1 is a PSVC for the SFDT.

If the PSVC is satisfied, the primary sensor is regarded as functioning properly; otherwise, it is considered to be malfunctioning. In addition, if a PSVC is violated on-line, all the constituents of the PSVC become failure suspects, and sensor failure diagnosis is performed by reducing the number of the failure suspects. Selection of an appropriate PSVC from the SVCs containing a primary sensor is, therefore, important for an effective sensor failure diagnosis. The following provides some guidelines, which may be taken into consideration, when choosing a PSVC from the SVCs:

(1) If a sensor is not included in any PSVC, the sensor failure will not be diagnosed in the sensor failure diagnosis models for the process system. Thus, the selection should involve a consideration of constituents of the SVCs.

(2) If several SVCs, from which a PSVC can be chosen, exist, then select an SVC as a PSVC, which is the most "robust" in the sense that satisfaction or violation of the SVC strictly depends on the success or failure of constituents of the SVC.

Sometimes, although rare, more than one SVC may be used as PSVCs, if the use of only one SVC is considered insufficient to validate a sensor reading. Provided this is the case, the primary sensor is considered to be functioning successfully, only if all the PSVCs for the sensor are met.

Since any SVC is an inequality statement, there are only two possibilities in regard to the satisfaction of the SVC; namely, the SVC is either satisfied, i.e., "OK" in the sample SFDT, or not, i.e., "NO" in the sample SFDT.

If the PSVC is satisfied, no SFD message set needs to be developed, because the primary sensor is validated. For instance, no SFD message set is developed for the OK branch under the SVC-1 heading of Fig. 6. Actually, sensor validation by use of a PSVC will be performed in a "PMT," when the heading of sensor validation in the tree is encountered in real time. However, the PSVC is shown in an "SFDT," not in the "PMT," because violation of the PSVC results in generation of the whole list of suspected sensors, with which the process of sensor failure diagnosis is initiated in the SFDT.

If the PSVC is not satisfied or violated, the list of suspected items resulting from the violation is specified at the NO branch under the heading of the PSVC. In the sample SFDT of Fig. 6, the functioning of three items, A, B, and C, is suspected as the result of violation of SVC-1. Thus, these suspected items are specified at the NO branch under the first heading.

Assume that there exists an SVC, which contains sensor A and has not yet been used in the SFDT--that is, SVC-2 in the sample tree. The functioning of sensor A can then be tested using the SVC-2. If SVC-2 is not satisfied, the diagnosis process is completed in this case, identifying that there is a high probability of sensor A failure. One can notice here that the violations of both SVC-1 and SVC-2 have resulted in the conclusion of sensor A failure.

As a confirmatory measure in the conclusion of sensor A failure in the SFDT model, the analyst can ask a question such as: Is it reasonable to conclude sensor A failure as a result of violations of the criteria, SVC-1 and SVC-2? Sometimes, the answer to this question may be negative. For instance, if the SVC-2 was based on A, B, and D sensors instead of A, D, E, and F sensors, then the answer would be negative, since it would be unreasonable to conclude only sensor A failure in that case--because sensor B failure could have caused such violations as well. This nonpositive answer to the question implies that, at the development stage of the SFDT, (1) the selection of sensor A from the suspected items has been inappropriate or (2) the selection of SVC-2 from the SVCs containing sensor A has been inappropriate. Thus, if the question elicits a negative answer, another suspected item other than sensor A may have to be selected for testing, or an SVC other than the SVC-2 may have to be chosen from the SVCs containing sensor A, at the development stage of the tree.

However, if the SVC-2 is satisfied, one can conclude that the suspected item, sensor A, is working successfully. Sensor A will then be removed from the list of the suspected items. Assuming further that there is SVC-3 which contains sensor B and has not yet been used, the functioning of sensor B can be next tested using the SVC-3. If the SVC-3 is met, one can conclude that the item, sensor B, is operating successfully. Hence, sensor B will be removed from the list. Since only one item, sensor C, is remaining in the list, the diagnosis process is completed in this case by concluding that there is a high probability that sensor C has failed. When the SVC-3 is not satisfied, sensor B failure can be concluded.

As shown in Fig. 6, sensor failure diagnosis message sets, not only the diagnosis result but also other messages such as prealarming or corrective measure, may be developed and can be presented to the operator.

The need for a change in plant operational mode can also be identified for each branch of the SFDT indicating sensor failure.

In the illustrative example mentioned above, only the three items, A, B, and C, were considered to be failure suspects as the result of violation of the PSVC, and the diagnosis was performed by reducing the number of failure suspects. However, the violation of a senor-value constraint such as the PSVC does not necessarily imply that there must be a sensor failure.[34] This is because certain hardware failures can also cause violation of the sensor-value constraint. Examples are (1) a pump failure causing the violation of the constraint formulated from the pump performance curve, and (2) a leakage failure causing the violation of the constraint based on mass balance of two flow rate sensors, upstream and downstream.

Therefore, if a PSVC based on a pump curve is used, the pump failure should also be included as one of the failure suspects following the violation of the PSVC. Likewise, leakage should be considered as one of the failure suspects, if a PSVC based on mass balance is violated.

4.2 On-line use of SFDT models

The SFDT model, once implemented into the computer-based operator aid, will be activated on-line, if a process monitor tree branch is actuated and the need for sensor failure diagnosis is indicated in the actuated PMT branch. The flow chart shown in Fig. 7 illustrates how an SFDT model is used on-line following the activation.

As shown in the flow chart, the first untested SVC in the SFDT model will be tested for sensor failure diagnosis first. In the sample SFDT (Fig. 6), SVC-2 is the first untested SVC, since SVC-1, i.e., the PSVC for the SFDT, has already been used to test the validity of the primary sensor A in the PMT.

If SVC-2 is satisfied, then the OK branch under the SVC-2 heading is followed (refer to Figs 6 and 7). However, since the end of the SFDT is not reached yet, another SVC, i.e., SVC-3, which is the first untested SVC at this time, will be tested next.

When SVC-3 is satisfied, the end of the SFDT is reached; therefore, the SFDT message set including the diagnosis result of Sensor C Failure will be presented to the operator. The module which determines an optimum plant operational mode will be activated on-line in this case, since it is indicated in the SFDT branch that a change in the plant operational mode is required.

If SVC-3 is not satisfied, then the SFDT message set involving the diagnosis result of Sensor B Failure will be presented to the operator. However, the plant operational mode module will not be activated in this situation, because the SFDT model indicates no need to change the plant operational mode.

On the other hand, if SVC-2 is not met, the end of the SFDT is reached. Therefore, the message set including the diagnosis result of Sensor A Failure will be presented to the operator. The plant operational mode module will be activated in this case, since the need for a change in plant operational mode is indicated in the actuated SFDT branch.

5 SIMPLIFIED DIRECTED GRAPH AND HARDWARE FAILURE DIAGNOSIS MODULES

Diagnosis is the process of dertermining the cause which initiated the observed system misbehavior. Therefore, the first step of diagnosis involves observation or detection of the system misbehavior, which is accomplished by the continuous scanning of the PMTs.

Once the misbehavior is observed, the cause must be determined to effectively manage the system malfunction. It is thus necessary to have a model which can be used to determine the cause from the observed misbehavior. Since the fault propagates with time in continuous process systems such as nuclear power plants or chemical plants, the model should be one in which system dynamic behaviors can be incorporated in terms of process variables or parameters together with basic fault origins, i.e., failure modes of process components, and system topology.

A directed graph, or digraph,[35-39] satisfies these requirements. A digraph may be described as a set of nodes connected by signed branches. The nodes of digraphs 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 the normal values. A positive sign indicates that the deviations occur in the same direction, while a negative sign expresses that the deviations occur in the opposite direction.

One of the earliest attempts to use the digraph for process analysis was made by Lapp and Powers[35] in automating the construction of fault trees for complex process systems which have contol loops. The fault trees were then used for off-line reliability or safety analysis. A recent paper by Ulerich and Powers[40] extends the work of Lapp and Powers by attempting to use the fault tree developed from a digraph for on-line hazard aversion and fault diagnosis applications.

In addition to the recent work of Ulerich and Powers,[40] there have been various attempts to use digraphs for on-line fault diagnosis over the years. One of the most typical among them is the work by Shiozaki et al.[23] Their diagnostic scheme is based upon:

(1) Construction of a digraph from the system topography,
(2) Generation of candidate faults,
(3) Qualitative simulation of the candidate faults, i.e., generation of all the abnormal measurement patterns arising during the propagation of the faults, from the digraph using their complex algorithm, and
(4) On-line diagnosis of process fault by matching the stored measurement patterns with on-line sensor data.

The "measurement-pattern-based" approach based on a digraph has the following drawbacks:

(1) A large number of measurement patterns should be constructed since an initiating fault must propagate through the system. This large number of measurement patterns result in a large search space. Furthermore, blind or exaustive search is employed in the approach to find a solution to the diagnostic problem. Therefore, the approach is inefficient because of the blind search in the large

search space.

(2) The approach may not result in the omission of the real origin of failure, as far as the real origin happens to be one of the candidate faults considered in the analysis. However, the diagnostic resolution of the approach is poor. For instance, in the pilot plant study of Tsuge et al.,[41] 23 fault candidates were obtained out of 53 possibilities. This poor diagnostic resolution develops because 1) some faults yield similar measurement patterns during the propagation of the faults through the system, and 2) the diagnosis is based on only the measurement patterns derived from the digraph without use of any deep knowledge of the process. It will be shown later that deep process knowledge can be effectively used for diagnosis.

(3) The diagnosis is based on the conventional qualitative approach; namely, the on-line, quantitative sensor data are transformed to qualitative data such as normal, high, or low, before being processed by the diagnostic algorithm. However, in the diagnosis of engineering systems quantitative process knowledge can be usefully used as will be illustrated later.

(4) One of the complexities of the approach comes from the complex representation of the fault propagation structure in the conventionally used digraph.

Although Kramer and Palowitch[42] have improved the efficiency of the algorithmic approach by Shiozaki et al.[23] by use of a rule-based format and Boolean algebra, their approach is essentially the same as that by

Shiozaki et al. and subject to similar drawbacks.

A novel approach to on-line hardware failure diagnosis will be proposed in this paper, which can overcome the drawbacks of the traditional measurement-pattern-based approaches. The characteristics of the proposed approach can be briefly described with later clarification as:

(1) The proposed method uses process disturbance patterns identified in terms of a small number of important process variables.

(2) The fault propagation structure of the system is represented in a simplified directed graph (SDG), a varient of the conventionally used digraph.

(3) The SDG is used to extract failure hypotheses for certain types of process disturbance patterns, although the conventional digraph has been typically used for deriving measurement patterns reflected in all the observable nodes in the digraph.

(4) Quantitative, deep process knowledge is applied to test the failure hypotheses on-line.

(5) The method employs a modular approach, therefore, the search space is reduced significantly to result in the improvement of computational efficiency.

Hardware failure diagnosis in the proposed method is based upon the model of hardware failure diagnosis (HFD) modules. An HFD module, which is developed for each of the identified process disturbance patterns, consists of 1) failure hypotheses derived from the SDG, 2) on-line verification methods for the failure hypotheses, 3) HFD message sets which will be presented to the operator if the failure hypotheses are verified on-line, and 4) indications of the needs to change the plant operational mode upon the verifications of the failure hypotheses.

The procedure for developing SDGs and HFD modules will be described in the following subsections, along with the way in which the developed HFD modules are used on-line in the global context of the overall methodology.

5.1 Development of signed directed graphs and hardware failure diagnosis modules

The flow chart depicted in Fig. 8 illustrates in detail steps to be taken in order to develop SDGs and HFD modules. The first step involves identification of the operating modes of the system to be considered in the analysis. Since the fault propagation structure of the system depends upon the operating mode or configuration, an SDG should be developed for each operating mode. Once an SDG is developed, HFD modules can be developed using the SDG.

The flow chart consists of two procedures for developing SDGs and HFD modules. The major steps in developing an SDG are as follows:

1. Identification of Process Variables

Process variables, which are necessary to properly represent the system causalities, must be identified first in order to develop an SDG for the selected operating mode. Examples of the process variables are pressure or flow rate at a certain point of the process line, control valve opening, and fluid level of a tank. In the sample SDG shown in Fig. 9, nodes P1, P2, P3, and P4 denote process variables identified to properly represent the fault propagation structure of the system.

2. Connection of the Process Variables

The process variables can now be connected with signed branches according to their causal influences among the process variables. In Fig. 9, for example, a directed edge is drawn from P2 to P4 with a negative sign on it, assuming that an increase (or decrease) in the process variable P2 will cause a decrease (or increase) in the process variable P4.

3. Identification of Failure Modes

Failure modes which need to be included in the analysis can first be identified. Then, all the failure modes except the ones diagnosed in the SFDTs will have to be included in the SDG or HFD modules. Two failure modes, FM1 and FM2, have been identified and included in Fig. 9.

4. Connection of the Failure Modes to the Process Variables

An SDG for the operating mode of the system can now be developed by connecting the failure modes to the relevant process variables in accordance with their causal relationships. The questions which may be useful in this step are: 1) Which process variable(s) will be immediately and significantly influenced by the occurrence of the failure mode? and 2) How will the process variable(s) be affected by the occurrence of the failure mode? A positive (or negative) sign can be drawn on the directed edge from a failure mode node to a process variable node, provided that the process variable will be significantly influenced by the occurrence of the failure mode and deviate from the normal values in the positive (or negative) direction immediately thereafter.

For example, in the sample SDG (Fig. 9), the failure mode node FM1 has been connected to the process variable node P1 with a negative sign on it, assuming that the occurrence of the failure mode FM1 will immediately influence the process variable P1 and cause it to be decreased. By the same token, the positive sign on the directed edge from FM2 to P3 can be interpreted such that the occurrence of FM2 will immediately influence P3 and cause it to be increased.

However, a certain failure mode, although it needs to be included in the HFD modules, may not be included in the SDG, because the occurrence of the failure mode does not cause a large deviation in any process variable immediately thereafter. An example may be found in the failure mode of a pneumatic control valve, "fails as is upon a loss of the pneumatic pressure," which results from the built-in design mechanism of the control valve. Such failure modes, if any, should be included in the HFD modules, so that the occurrence of the failure mode can be detected by the computerized operator aid.

Development of HFD modules using the SDG developed above proceeds in the following steps (refer to Fig. 8):

1. Identification of Process Disturbance Patterns

An HFD module will be developed for each process disturbance pattern, and the developed HFD module will be activated and used on-line for hardware failure diagnosis once the disturbance pattern is observed in the system.

Therefore, it is necessary to identify process disturbance patterns for which HFD modules will be developed.

The process disturbance patterns can be effectively represented in terms of particularly important process variables. Controlled variables in a control loop make a good example of such variables.

In Fig. 9, for example, assume that P4 is a particularly important process variable and the process disturbance pattern of the system can be represented in terms of only the process variable P4. Then, two process disturbance patterns, P4 high and P4 low, can be identified in this simple case.

Use of the process disturbance patterns contributes to modularization of the hardware failure diagnosis set, i.e., all the knowledge regarding hardware failure diagnosis, and thereby improving the computational efficiency of the real-time computer system.

2. Extraction of Failure Hypotheses from the SDG

Failure hypotheses for each process disturbance pattern can be extracted from the SDG by following the fault propagation of each failure mode on the SDG and checking whether the process disturbance pattern could have resulted from the occurrence of the failure mode.

Direct extraction of failure hypotheses from the process and instrumentation diagram (P&ID) of a system can be extremely difficult, although not impossible, especially in the case where the system contains complex control loop(s). The use of an SDG, which models the fault propagation structure of the system, will not only facilitate the extraction process significantly but also help check the completeness of the hypotheses.

The extracted failure hypotheses can then be ordered such that the more likely hypothesis will be first tested on-line by the computer system. The knowledge of recent maintenance history and failure probabilities of the components may be applied for the ordering of the hypotheses, which will improve the computational efficiency in searching for the feasible hypothesis.

3. Development of On-line Verification Methods

If a disturbance occurs in real-time, then the failure hypotheses associated with the disturbance pattern will be tested one by one to diagnose the fault which has caused the disturbance pattern. In order to make the on-line test of the hypotheses possible, an on-line verification method for each hypothesis should be developed and included in the HFD modules.

The verification methods should be in terms of process variables or parameters that are accessable through the real-time process data base. Deep process knowledge can preferably be used in developing the verification methods. For instance, the design knowledge of a control system such as control algorithmic equations can be used in diagnosing control system failure.

4. Development of HFD Message Sets

Since the diagnosis result should be transmitted to the operator, an HFD message set needs to be developed for each case of failure hypothesis. Corrective measure may also be included in the message set, and it is the situation-specific nature of this analysis that makes the incorporation of corrective measure in the message set possible.

5. Identification of the Need to Change the Plant Operational Mode

The plant operational mode may have to be changed following hardware failure in order to minimize the consequence of hardware failure or balance the plant. Therefore, it is necessary to identify whether or not the plant operational mode should be changed upon the on-line verification of the failure hypothesis.

5.2 On-line use of HFD modules

Fig. 10 shows how the HFD modules developed off-line will be used for hardware failure diagnosis on-line in the context of the overall methodology. Hardware failure diagnosis is initiated when the HFD unit indicated in the actuated PMT branch is activated on-line by the real-time computer system. An HFD unit is a collection of knowledge to be used for hardware failure diagnosis in a specific situation such that a certain type of disturbance, e.g., pressure or level disturbances, has occurred in a certain operating configuration of the system. A number of process disturbance patterns, and hence the same number of HFD modules--since an HFD module is developed for each process disturbance pattern--are contained in an HFD unit.

Once the HFD unit specified in the PMT is activated, the real-time computer system will identify the process disturbance pattern at hand from the various process disturbance patterns in the HFD unit. The HFD module for the identified process disturbance pattern will then be activated online to diagnose the system malfunction.

Upon the activation of the HFD module, the failure hypotheses in the HFD module will be tested one by one following the predefined testing order to determine the most likely cause that has brought about the disturbance pattern. If a failure hypothesis is verified or accepted by the on-line verification method, then the HFD message set associated with the verified hypothesis is presented to the operator. The module, in which an optimum plant operational mode is determined, will be activated, if the need to change the plant operational mode is indicated in the hypothesis column.

However, if no failure hypothesis is accepted, no action will be performed by the real-time computer system. That is, no message will be presented to the operator, and the plant operational mode module will not be activated even if the need for a change in plant oprational mode is indicated in the hypothesis column. Since the process condition changes rapidly during a process upset condition, a failure hypothesis in the HFD module may be accepted if the module is reactivated some time later.

6 MODULE FOR THE DETERMINATION OF THE PLANT OPERATIONAL MODE

During normal operation, the plant will be operating for a certain plant goal, e.g., a certain power level at a power plant and a certain production capacity level at a chemical process plant, with one of the associated success paths. However, occurrence of a process disturbance may challenge the plant goal and success path. If this is the case, a new optimal plant goal and its associated success path--preferably the highest priority success path among those associated with the plant goal--will have to be found in order to maximize the operability of the plant. Sometimes, the new optimal goal may be just to shutdown the plant safely without any damage to the plant, if continuation of the operation is infeasible.

There is a success criterion, e.g., in terms of the number of hardware components required or process conditions, associated with each of the plant goals, which should be satisfied for the plant goal to be viable. These criteria can be effectively represented in the logical structure of the goal-tree success-tree model. In addition, the success paths can also be effectively incorporated in the success tree part of the GTST. Therefore, the GTST model can be used as a suitable basis for developing a module for the determination of plant operational mode, i.e., plant goal and success path .

The reason why a module is developed separately for the determination of plant operational mode (POM) is as follows:

> Upon the occurrence and detection of a process disturbance, a certain process unit may have to be shutdown or isolated so as to continue the operation or reduce damage to the plant. This kind of "local" corrective action may also necessitate rearrangement of the operating configuration of the whole system to balance the plant, i.e., "global" corrective action. The determination of how to reconfigure the whole system or change the POM during process anomalies can be quite complicated depending on the system, and requires a comprehensive perspective of the

process conditions. Therefore, the knowledge needed to determine the optimum POM is extracted from the GTST and incorporated into a "module."

Since the POM may have to be changed following process anomalies such as severe process degradation, sensor failure or hardware failure, an option to indicate a need for POM change is included in process monitor trees and sensor/hardware failure diagnosis models. The POM module will be activated on-line in the following cases:

(1) When a process monitor tree branch is actuated in real-time and a need for a change in the POM due to the severe process degradation is indicated in the actuated PMT branch, or

(2) When a sensor failure diagnosis tree branch is actuated in real-time, and it is indicated in the actuated SFDT branch that there is a need to change the POM as a result of the sensor failure, or

(3) When a failure hypothesis in a hardware failure diagnosis module is verified on-line, and a need to change the POM due to the hardware failure is represented in the failure hypothesis column.

7 OVERALL ALGORITHM OF THE METHODOLOGY

All knowledge needed for on-line process disturbance management is contained in the various models described heretofore, i.e., process monitor trees, sensor failure diagnosis trees, hardware failure diagnosis and plant operational mode modules. Among the models, only PMTs are continuously scanned on-line for detection of a significant event;

whereas, the others used on demand as described in Section 3.

If a process disturbance occurs in the system, it will be detected in PMTs. Following the detection, three possibilities exist in regard to the diagnosis of the cause:

(1) No diagnosis: If the actuated PMT branch indicates that there is no need for diagnosis, then no diagnosis will be performed. This would probably result when there is a severe process degradation with the sensor value validated but with insufficient time to diagnose. Another possibility for no diagnosis could result from the case where an automatic trip occurs as the sensor value exceeds the trip setpoint.

(2) Sensor failure diagnosis: If the PMT denotes that sensor failure diagnosis is needed as a result of violation of the primary sensor validation criterion, then sensor failure diagnosis will be performed in the SFDT.

(3) Hardware failure diagnosis: If a need for hardware failure diagnosis is indicated in the actuated PMT branch, then hardware failure diagnosis will be carried out in the HFD unit indicated in the PMT branch.

Fig. 11 shows the overall algorithm of the methodology proposed in this paper, which represents how the various models work together as an integral unit for on-line process disturbance management. From this figure, we can note that:

(1) Four kinds of major functions are performed: process monitoring, sensor failure diagnosis, hardware failure diagnosis, and determination of an optimum plant operational mode.

(2) Four kinds of messages exist: PMT, SFD, HFD, and POM messages. Usually, component-level or local corrective measures are included in the PMT, SFD, or HFD message sets, whereas system-level or global corrective measures in the POM message set. For instance, if say, pump 12, is found to be malfunctioning, then a corrective measure message such as "[CM] Shutdown Pump 12" may be presented to the operator as a local corrective measure. In addition to the local corrective measure, the operating configuration of the whole system may have to be rearranged to balance the plant. In this case, the POM module will be activated and a POM message of how to reconfigure the system will be given as a sort of system-level or global corrective message.

(3) An optimum plant operational mode needs to be sought upon the occurrence and detection of the following: severe process degradation, sensor failure, and/or hardware failure. However, the operational mode may not have to be changed; for instance, in the case where a sensor failure is found and there is a redundant sensor which can replace the failed sensor on-line.

8 CONCLUSIONS

A methodology has been proposed in this paper which can be applied to the design of a real-time expert system for assisting control-room operators in coping with process abnormalities. The methodology encompasses the diverse functional aspects that are required for an effective on-line process disturbance management: (1) intelligent process monitoring and alarming, (2) on-line sensor data validation and sensor conflict resolution, (3) on-line hardware failure diagnosis, and (4) real-time corrective measure synthesis. Accomplishment of these functions is made possible through the integrated application of the various models, goal-tree success-tree, process monitor tree, sensor failure diagnosis, and hardware failure diagnosis models.

The models used in the methodology facilitate not only the knowledge acquisition process--a bottleneck in the development of an expert system--but also the reasoning process of the knowledge-based system. These transparent models and model-based reasoning significantly enhance the maintainability of the real-time expert systems, a primary concern in the practical application of expert system techniques.

In order to demonstrate the feasibility of the approach, the model-based methodology has been applied to a target process, a main feedwater system of a PWR nuclear power plant, which employs a complex control mechanism. Performance tests of the resulting expert system demonstrate that it successfully fulfills its intended objectives, timely recognition or detection of occurring disturbance, diagnosis of the disturbance cause, and presentation of optimal control advice to the operator. Therefore, the model-based technique discussed in this paper promises to lead to the development of a valuable operator aid for on-line process disturbance management.

The application of the methodology to the main feedwater system will be presented in a companion paper. Implementation of the models developed for the target process in the real-time expert system shell, PICON, will also be presented in the paper together with the results of the performance tests of the knowledge-based system in a simulated process environment.

REFERENCES

1. Woods, D.D., Wise, J.A. and Hanes, L.F. Evaluation of safety parameter display concepts, EPRI Report, Electric Power Res. Inst., Palo Alto, CA, NP-2239 (February 1982).
2. Meijer, C.H., Callaghan, V.C. and Hollnagel, E. Improved man- machine system design for nuclear power plants," Proc. ANS/ASME Conf. on Design, Construction and Operation of Nuclear Power Plants, Portland, Oregon, August 1984.
3. Lees, F.P. Process computer alarm and disturbance analysis system: Review of the state of the art, Comput. Chem. Eng. **7** (1983) 669-694.
4. MPR Associates, Inc. Power plant alarm systems: A survey and recommended approach for evaluating improvements, EPRI Report, Electric Power Res. Inst., Palo Alto, CA, NP-4361 (December 1985).
5. Meijer, C.H. and Frogner, B. On-line power plant alarm and disturbance analysis system, EPRI Report, Electric Power Res. Inst., Palo Alto, CA, NP-1379 (April 1980).
6. Felkel, L. and Roggenbauer, H. The star concept, Proc. Internat.

Meeting on Thermal Nuclear Reactor Safety, Chicago, IL, August 1982.

7. Long, A.B. Technical assessment of disturbance analysis systems, Nuclear Safety 21 (January-February 1980).

8. Waterman, D.A. A Guide to Expert Systems (Addison-Wesley Publishing Co., 1986).

9. Hayes-Roth, F., Waterman D.A. and Lenat D. (eds.), Building Expert Systems (Addison-Wesley Publishing Co., 1986).

10. Nelson, W.R. REACTOR: An expert system for diagnosis and treatment of nuclear reactor accidents, Proc. AAAI-82 (1982) 296-301.

11. Naito, N. et al. A real-time expert system for nuclear power plant failure diagnosis and operational guide, Nuclear Technology 79 (December 1987).

12. Shirley, R.S. Some lessons learned using expert systems for process control, Proc. 1987 American Control Conference, Minneapolis, MN, June 1987.

13. Dhurjati, P. et al. Experience in the development of an expert system for fault diagnosis in a commercial scale chemical process, Proc. First Internat. Conf. on Foundations of Computer Aided Process Operations, Park City, Utah, July 1987.

14. Rowan, D.A. Chemical plant fault diagnosis using expert systems technology, IFAC Kyoto Workshop on Fault Detection and Safety in Chemical Plants, Kyoto, Japan, September 1986.

15. Sauers, R. and Walsh, R. On the requirements of future expert systems, Proc. Eighth IJCAI, Karlsruhe, West Germany, 1983.

16. Odette, L.L. and Dress, W.B. Engineering intelligence into real-time applications, Expert Systems, 4:4 (November 1987) 228-239.

17. Leinweber, D. Expert systems in space, IEEE Expert (Spring 1987) 26-36.

18. Moore, R. Expert systems in process control: Applications experience, in: Applications of AI in Engineering Problems, Vol.1, ed. D. Shiram and R. Adey (A Computational Mechanics Publication, 1986) pp. 21-30.

19. Moore, R. et al. Expert systems in real-time environments, Proc. Internat. Conf. on Computer Applications for Nuclear Power Plant Operation and Control, Tri-Cities (Pasco), WA, September 1985.

20. Moore, R. et al. A real-time expert system for process control, Proc. IEEE First Conference on Artificial Intelligence Applications, Denver, Co, 1984.

21. Intellicorp, Extending expert systems technology: Model-based reasoning, Internal Report, Vol.2 No. 2 (August 1986).

22. Hajek, B.K. et al. Artificial intelligence enhancements to safety parameter display systems, Proc. Internat. Topical Meeting on Advances in Human Factors in Nuclear Power Systems, Knoxville, TN, April 1986.

23. Shiozaki, J. et al. An improved algorithm for diagnosis of system failures in the chemical process, Comput. Chem. Eng. **9**:3 (1985) 285-293.

24. Hunt, R.N. and Modarres, M. Integrated economic risk management in a nuclear power plant, Annual Meeting of the Society for Risk Analysis, Knoxville, TN, October 1984.

25. Kim, I.S. and Modarres, M. Application of goal tree-success tree model as the knowledge-base of operator advisory systems, Nucl. Eng. Des. **104** (1987) 67-81.

26. Modarres, M. and Cadman, T. A method of alarm system analysis in

process plants with the aid of an expert computer system, Comput. Chem. Eng. **10** (1986) 557-565.

27. Roush, M.L., Modarres, M. and Hunt, R.N. Application of goal trees to evaluation of the impact of information upon plant availability, Proc. ANS/ENS Topical Meeting on Probablistic Safety Methods and Applications, San Fransisco, CA, February 1985.

28. Modarres, M., Roush, M.L. and Hunt, R.N. Application of goal trees for nuclear power plant hardware protection, Proc. Eighth Internat. Conf. on Structural Mechanics in Reactor Technology, Brussels, Belgium (August 1985).

29. Chung, D.T. and Modarres, M. GOTRES: An expert system for fault detection and analysis, Reliab. Engng Sys. Safety (1988).

30. Benedict, B.J. et al. Validation and integration of critical PWR signals for safety parameter display systems, EPRI Report, Electric Power Res. Inst., Palo Alto, CA, NP-4566 (May 1986).

31. Upadhyaya, B.R. Sensor failure detection and estimation, Nuclear Safety **26**:1 (January-February 1985).

32. Blanch, P.M. and Meyer, J.E. Northeast utilities signal validation applications for safety parameter display systems, Proc. 1985 International Topical Meeting on Computer Applications for Nuclear Power Plant Operation and Control, Tri-cities (Pasco), Washigton, September 1985.

33. Tylee, J.L. Estimation of failed sensor outputs, Nucl. Sci. Eng. **96** (1987) 145-152.

34. Kim, I.S. and Modarres, M. MOAS: A real-time operator advisory system, Proc. Internat. Conf. on Artificial Intelligence and Other Innovative

Computer Applications in the Nuclear Industry, Snowbird, Utah, August 1987.

35. Lapp, S.A. and Powers, G.J. Computer-aided synthesis of fault-trees, IEEE Transactions on Reliability (April 1977) 2-13.

36. Henley, E.J. and Kumamoto, H. Designing for Reliability and Safety Control (Prentice Hall, Inc., Englewood Cliffs, NJ, 1985).

37. Andow, P.K. Difficulties in fault-tree synthesis for process plant, IEEE Trans. on Reliability, **R-29**, No. 1 (April 1980) 2-9.

38. Kumamoto H. et al. Signal-flow-based graphs for failure-mode analysis of systems with control loops, IEEE Trans. on Reliability, **R-30**, No. 2 (June 1981) 110-116.

39. Kumamoto, H. and Henley, E. Safety and reliability synthesis of systems with control loops, AIChE J. **25:1** (January 1979) 108-113.

40. Ulerich, N.H. and Powers, G.J. On-line hazard aversion and fault diagnosis in chemical processes: The digraph + fault-tree method, IEEE Trans. on Reliability (June 1988) 171-177.

41. Tsuge, Y. et al. Fault diagnosis algorithms based on the signed directed graph and its modifications, I. Chem. Eng. Symp. Ser. **92**, (1985).

42. Kramer, M.A. and Palowitch Jr., B.L. A rule-based approach to fault diagnosis using the signed directed graph, AIChE J. **33:7** (1987) 1067-1078.

ACKNOWLEDGEMENTS

This work is supported by the National Science Foundation under Engineering Research Centers Program: NSFD CDR 88003012, and by Baltimore Gas and Electric Company.

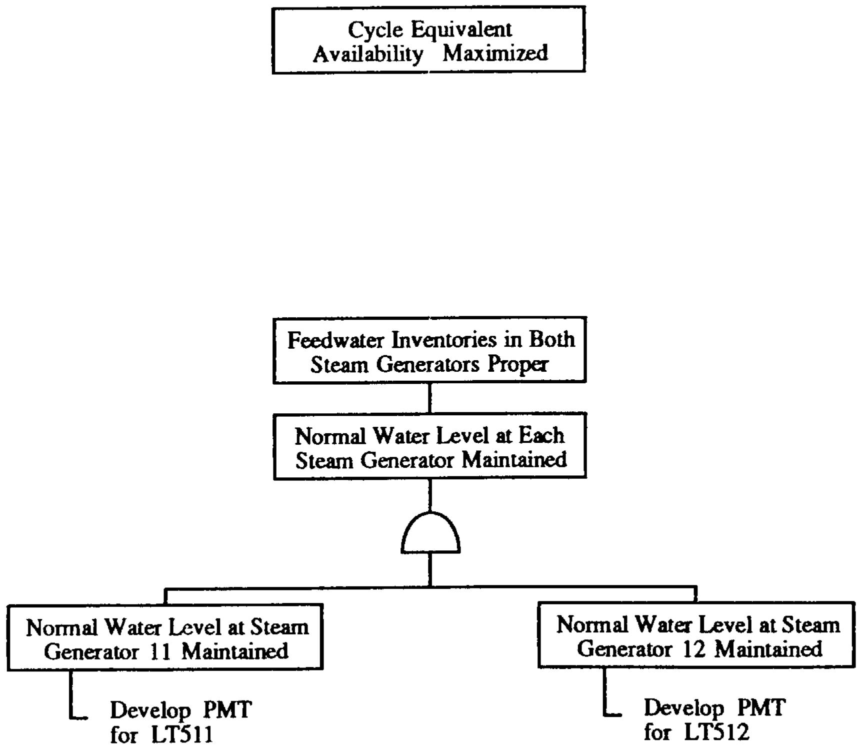

Cycle Equivalent Availability Maximized
Feedwater Inventories in Both Steam Generators Proper
Normal Water Level at Each Steam Generator Maintained
Normal Water Level at Steam Generator 11 Maintained
Normal Water Level at Steam Generator 12 Maintained
Develop PMT for LT511
Develop PMT for LT512

Figure 1. Identification of Process Monitoring Points from a GTST Model

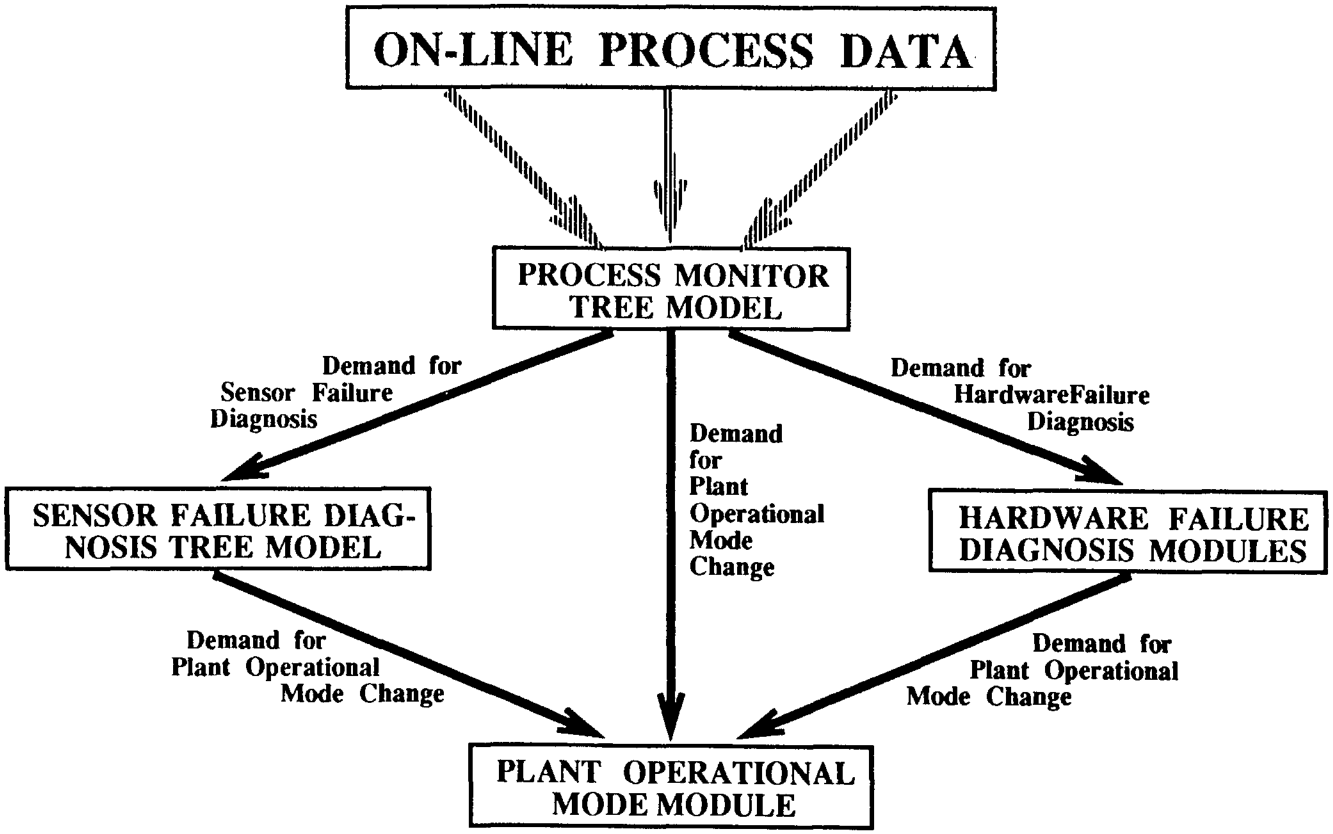
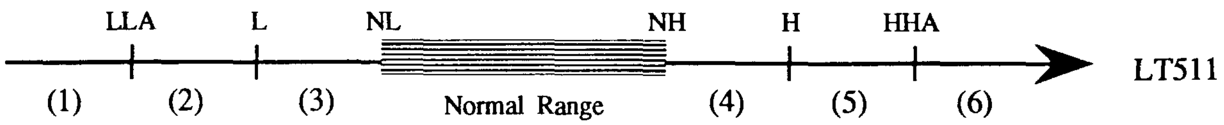

ON-LINE PROCESS DATA
PROCESS MONITOR TREE MODEL
Demand for Sensor Failure Diagnosis
Demand for Plant Operational Mode Change
Demand for HardwareFailure Diagnosis
SENSOR FAILURE DIAGNOSIS TREE MODEL
HARDWARE FAILURE DIAGNOSIS MODULES
Demand for Plant Operational Mode Change
Demand for Plant Operational Mode Change
PLANT OPERATIONAL MODE MODULE

Figure 2. Relationship of Models Used On-Line



<u>BOUNDARIES OF VALUE BANDS</u>:

LLA = Low-Low and Automatic Trip Action

L = Low

NL = Low Limit of the Normal Range

NH = High Limit of the Normal Range

H = High

HHA = High-High and Automatic Trip Action

<u>SIGNIFICANT VALUE BANDS</u>:

(1) LT511 <= LLA

(2) LLA < LT511 <= L

(3) L < LT511 <= NL

(4) NH <= LT511 < H

(5) H <= LT511 < HHA

(6) LT511 >= HHA

Figure 3. Sample Boundaries and Significant Value Bands

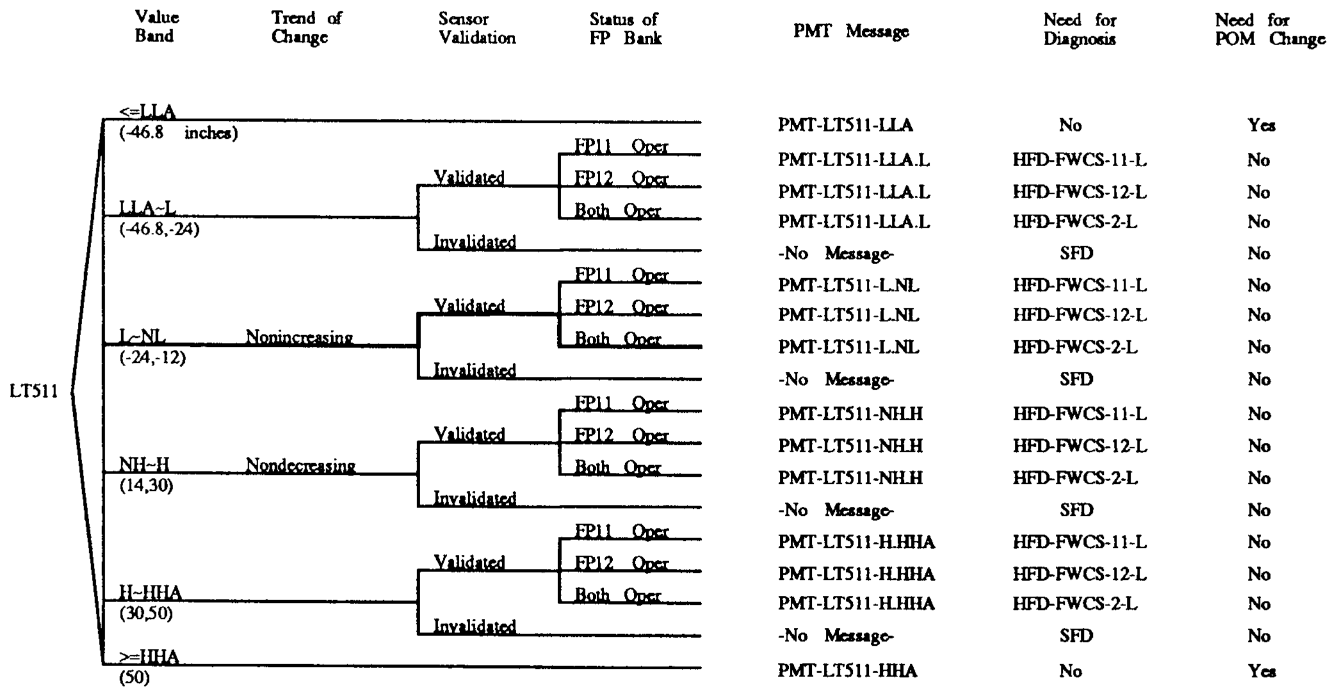


Figure 4. Sample Process Monitor Tree

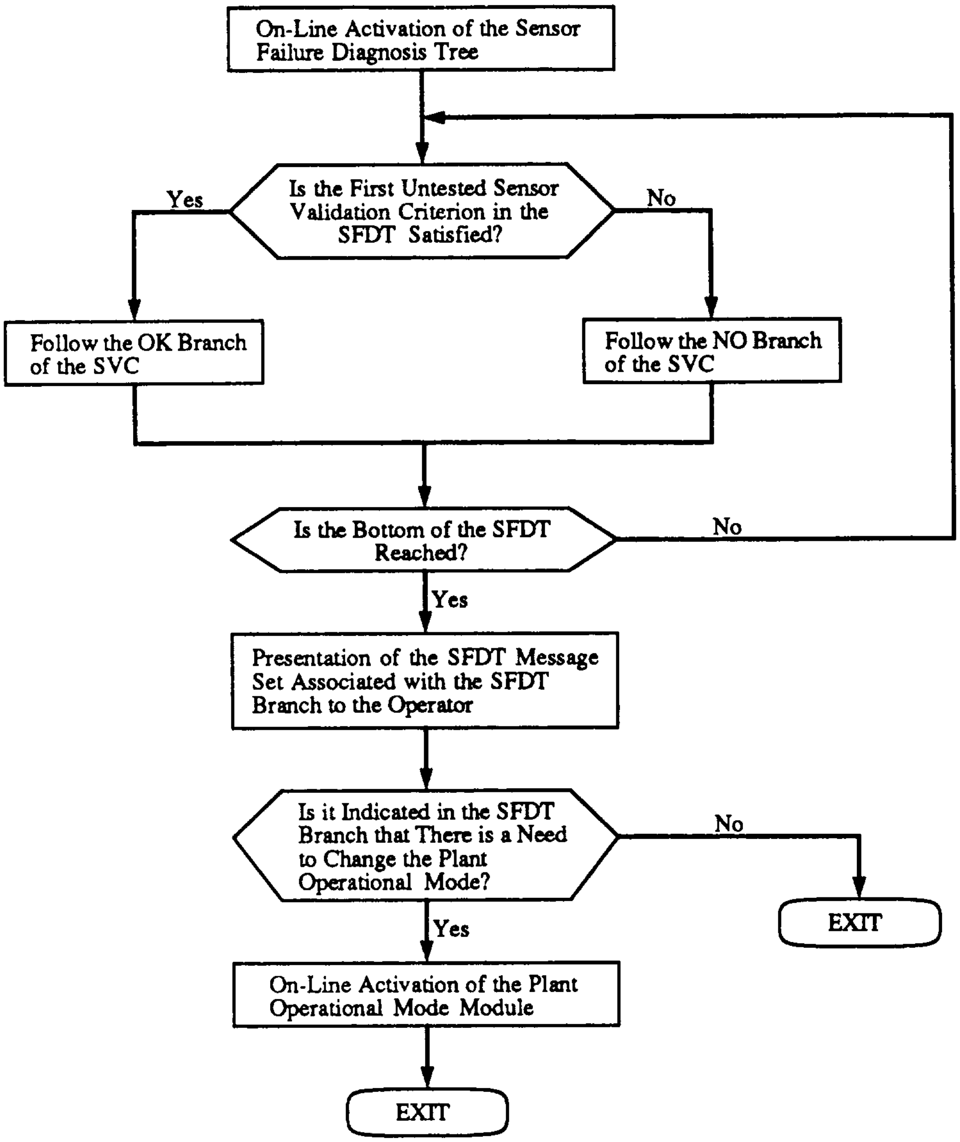

On-Line Activation of the Sensor Failure Diagnosis Tree
Is the First Untested Sensor Validation Criterion in the SFDT Satisfied?
Yes
No
Follow the OK Branch of the SVC
Follow the NO Branch of the SVC
Is the Bottom of the SFDT Reached?
No
Yes
Presentation of the SFDT Message Set Associated with the SFDT Branch to the Operator
Is it Indicated in the SFDT Branch that There is a Need to Change the Plant Operational Mode?
No
EXIT
Yes
On-Line Activation of the Plant Operational Mode Module
EXIT

Figure 5. On-Line Use of an SFDT Model

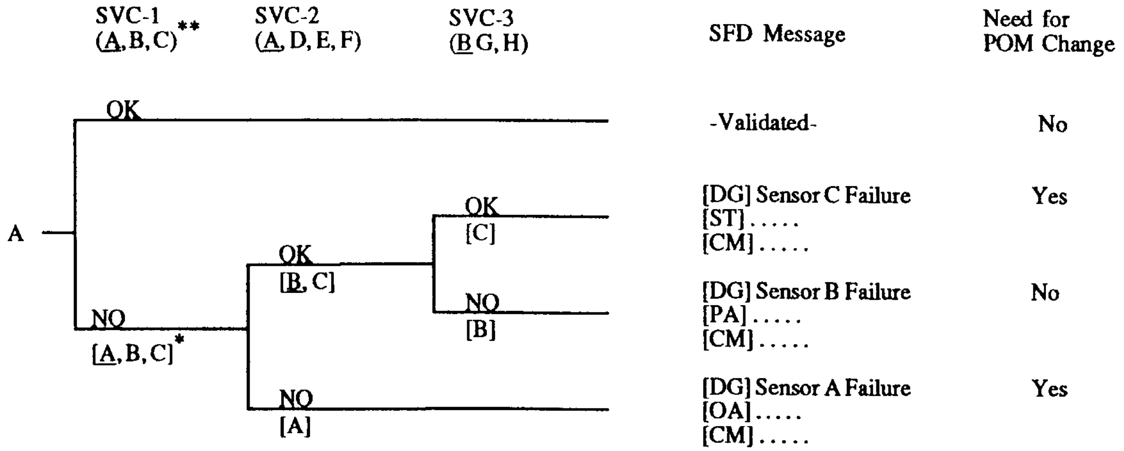


Figure 6. Sample Sensor Failure Diagnosis Tree

(* The underline in the tree structure indicates that the validity of the underlined item will be tested next.

** The underline in the SFDT heading indicates that the SVC will be used to test the validity of the underlined item.)

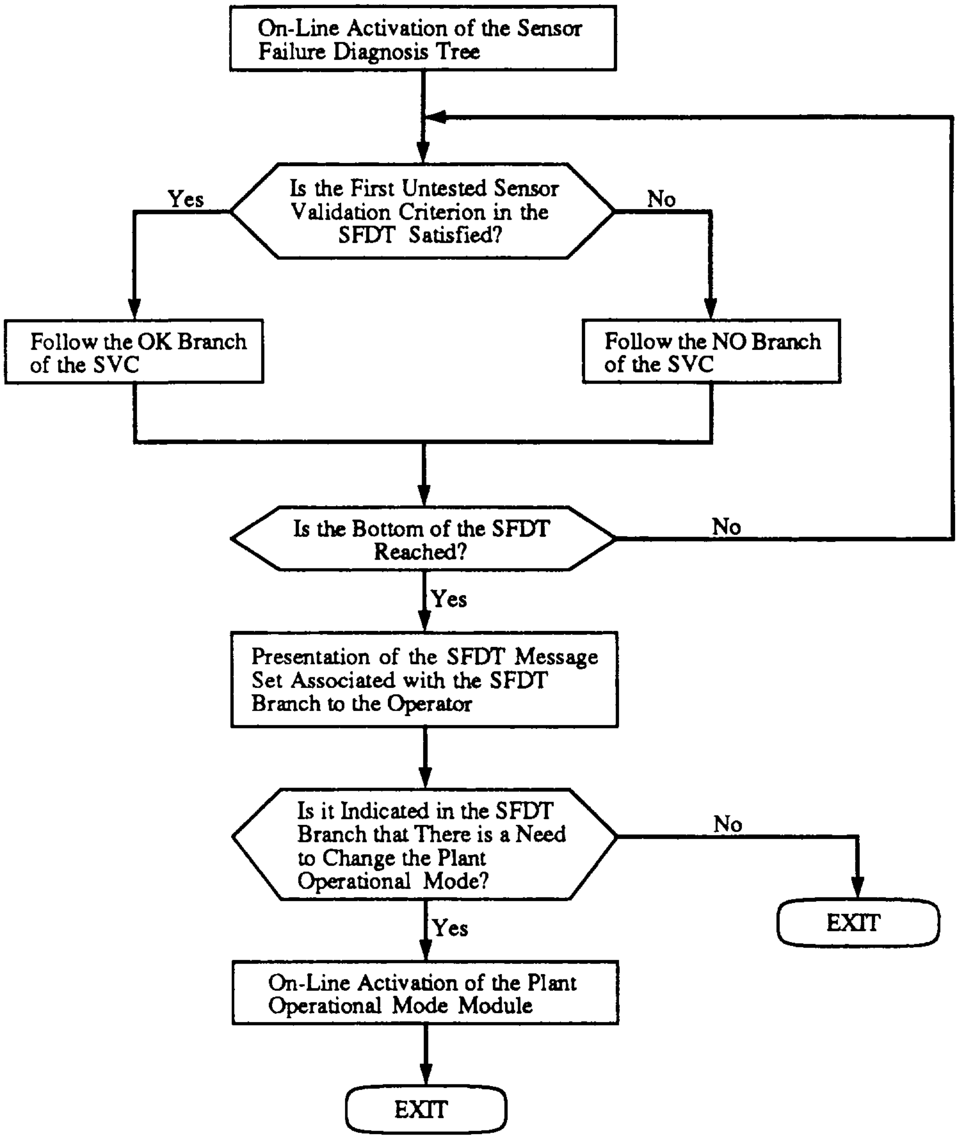

On-Line Activation of the Sensor Failure Diagnosis Tree
Is the First Untested Sensor Validation Criterion in the SFDT Satisfied?
Yes
No
Follow the OK Branch of the SVC
Follow the NO Branch of the SVC
Is the Bottom of the SFDT Reached?
No
Yes
Presentation of the SFDT Message Set Associated with the SFDT Branch to the Operator
Is it Indicated in the SFDT Branch that There is a Need to Change the Plant Operational Mode?
No
EXIT
Yes
On-Line Activation of the Plant Operational Mode Module
EXIT

Figure 7. On-Line Use of an SFDT Model

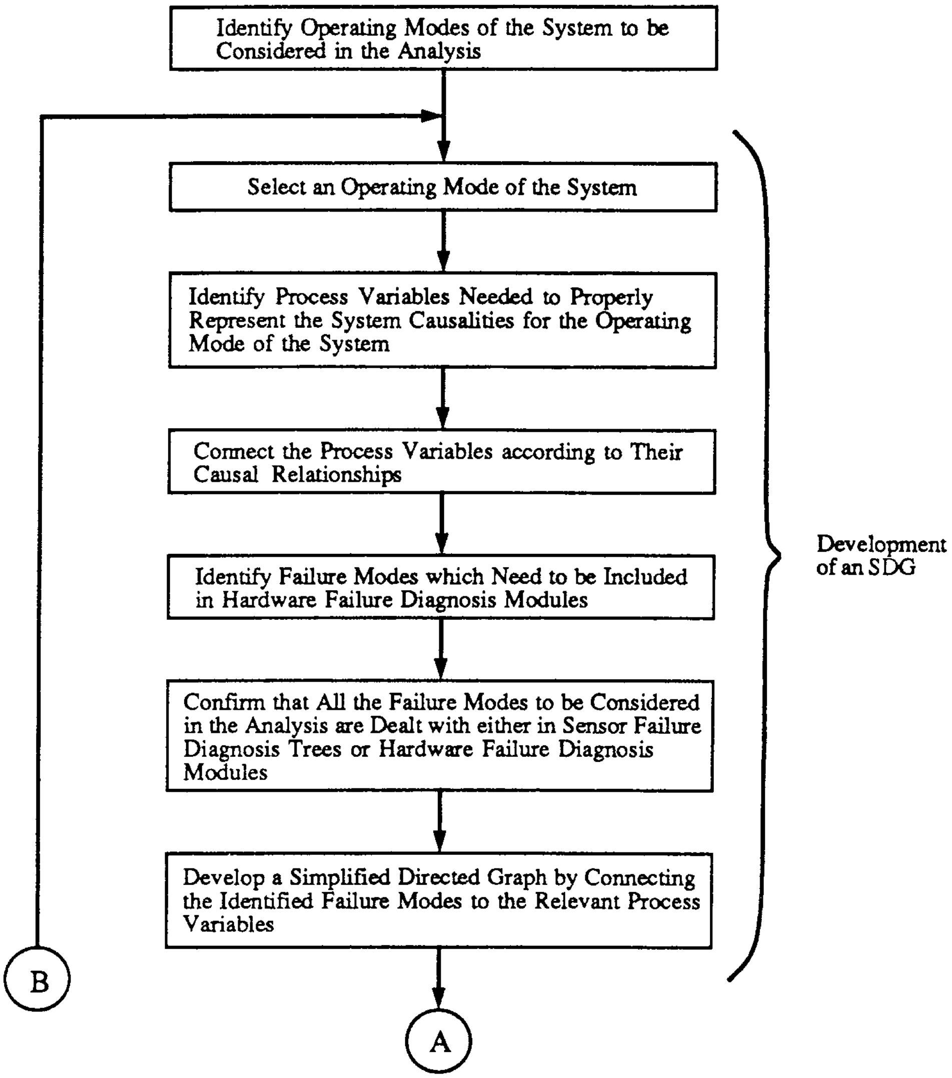

Identify Operating Modes of the System to be Considered in the Analysis
Select an Operating Mode of the System
Identify Process Variables Needed to Properly Represent the System Causalities for the Operating Mode of the System
Connect the Process Variables according to Their Causal Relationships
Identify Failure Modes which Need to be Included in Hardware Failure Diagnosis Modules
Confirm that All the Failure Modes to be Considered in the Analysis are Dealt with either in Sensor Failure Diagnosis Trees or Hardware Failure Diagnosis Modules
Develop a Simplified Directed Graph by Connecting the Identified Failure Modes to the Relevant Process Variables
Development of an SDG
B
A

Figure 8. Development of SDGs and HFD Modules

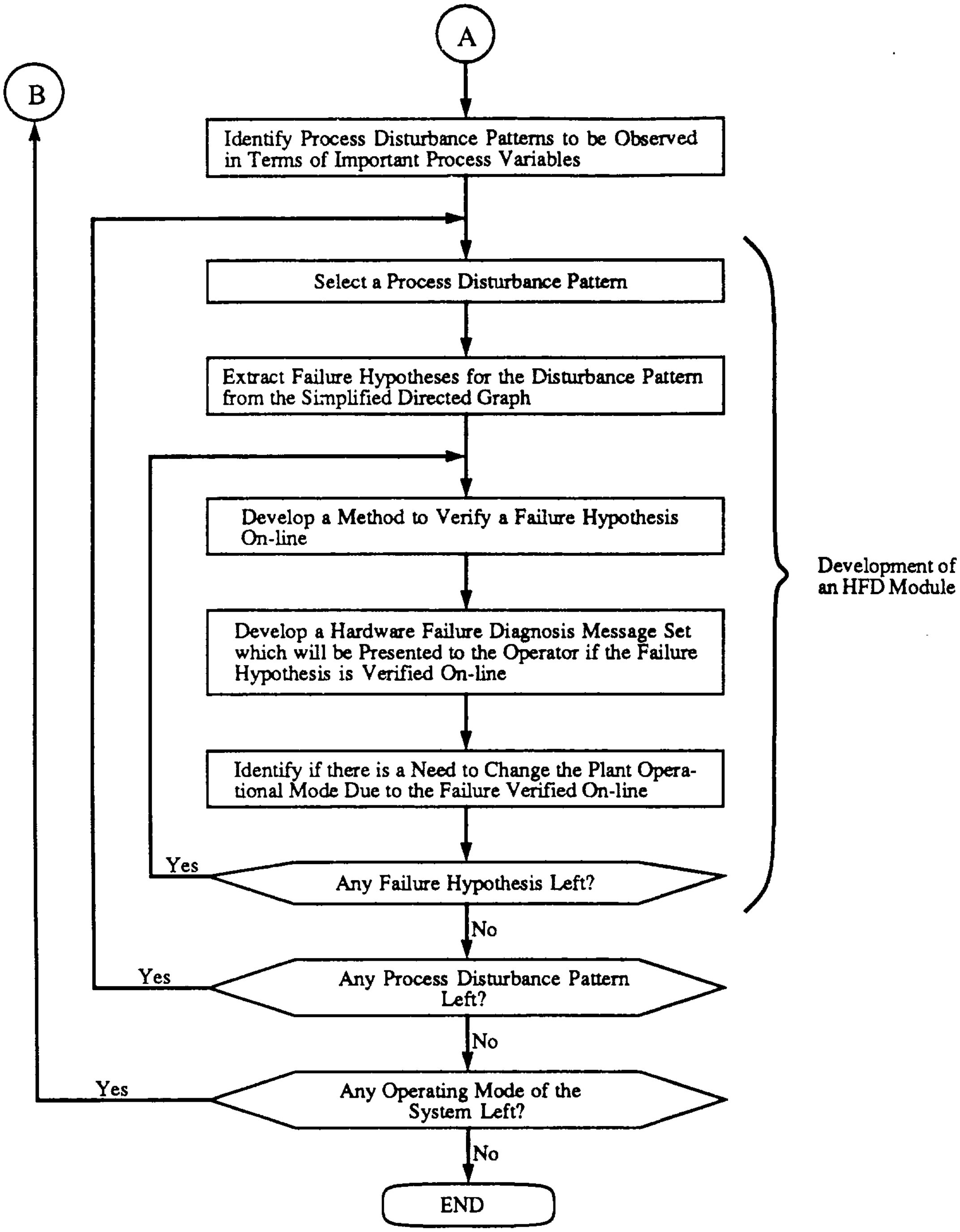

A
B
Identify Process Disturbance Patterns to be Observed in Terms of Important Process Variables
Select a Process Disturbance Pattern
Extract Failure Hypotheses for the Disturbance Pattern from the Simplified Directed Graph
Develop a Method to Verify a Failure Hypothesis On-line
Develop a Hardware Failure Diagnosis Message Set which will be Presented to the Operator if the Failure Hypothesis is Verified On-line
Identify if there is a Need to Change the Plant Operational Mode Due to the Failure Verified On-line
Development of an HFD Module
Yes
Any Failure Hypothesis Left?
No
Yes
Any Process Disturbance Pattern Left?
No
Yes
Any Operating Mode of the System Left?
No
END

Figure 8. (Continued)

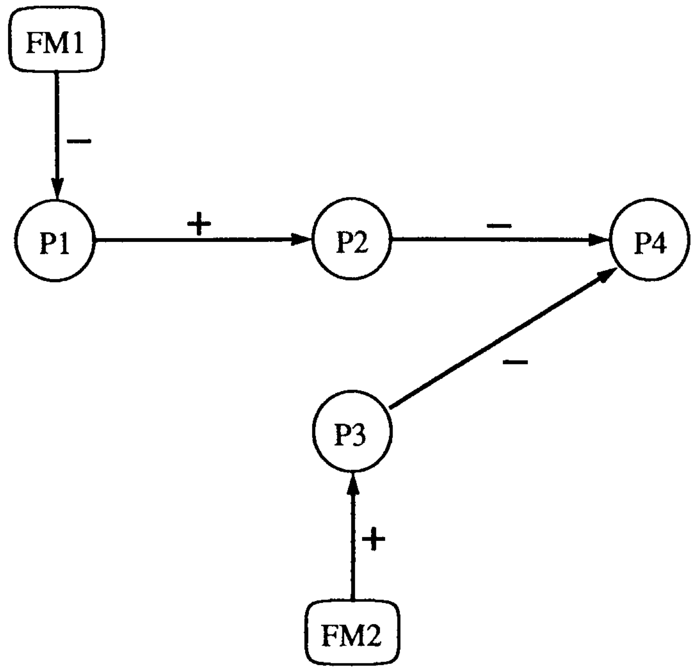


Figure 9. Typical Structure of a Simplified Directed Graph

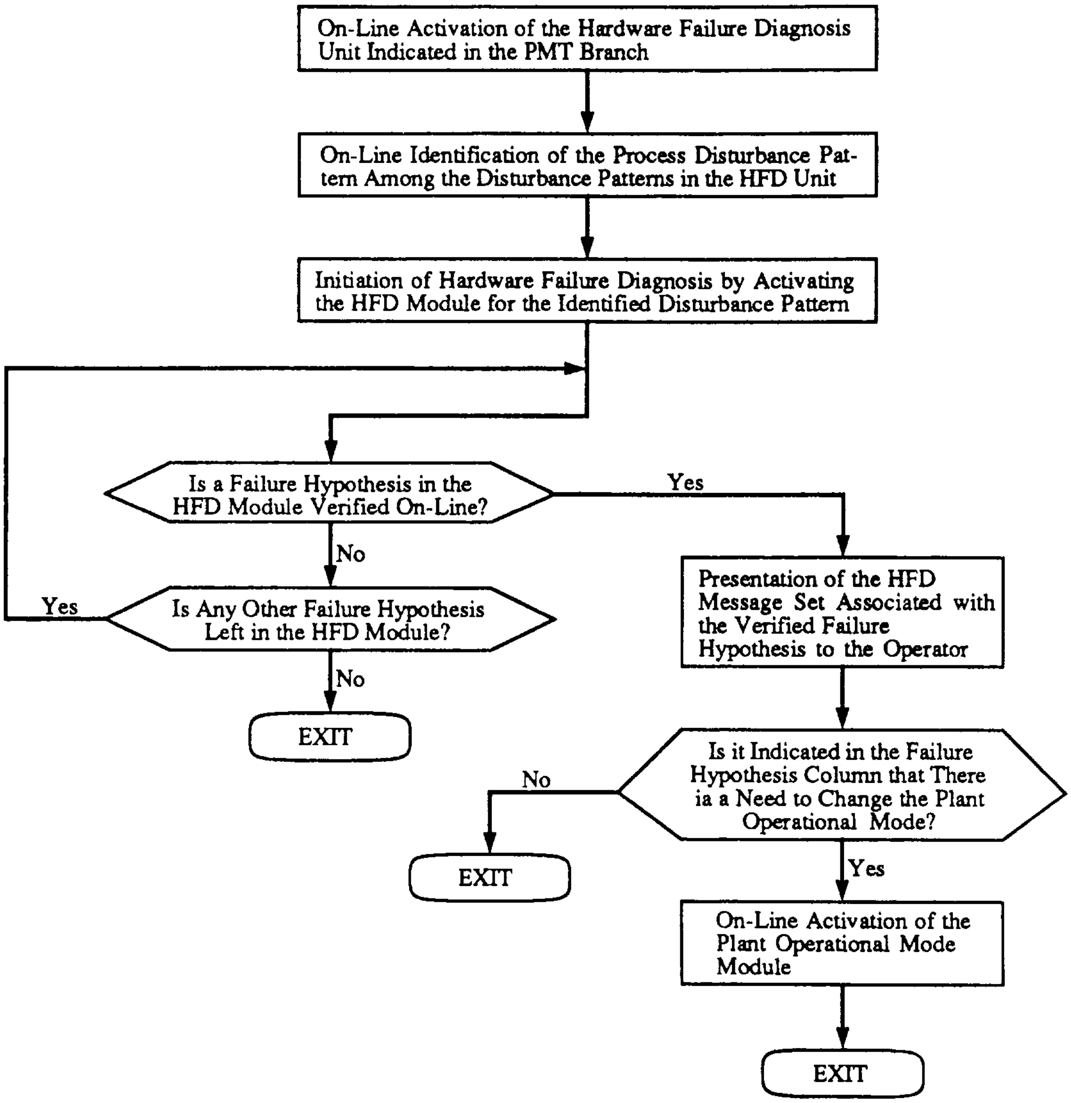

On-Line Activation of the Hardware Failure Diagnosis Unit Indicated in the PMT Branch
On-Line Identification of the Process Disturbance Pattern Among the Disturbance Patterns in the HFD Unit
Initiation of Hardware Failure Diagnosis by Activating the HFD Module for the Identified Disturbance Pattern
Is a Failure Hypothesis in the HFD Module Verified On-Line?
Yes
No
Is Any Other Failure Hypothesis Left in the HFD Module?
Yes
No
EXIT
Presentation of the HFD Message Set Associated with the Verified Failure Hypothesis to the Operator
Is it Indicated in the Failure Hypothesis Column that There ia a Need to Change the Plant Operational Mode?
No
EXIT
Yes
On-Line Activation of the Plant Operational Mode Module
EXIT

Figure 10. On-Line Use of HFD Modules

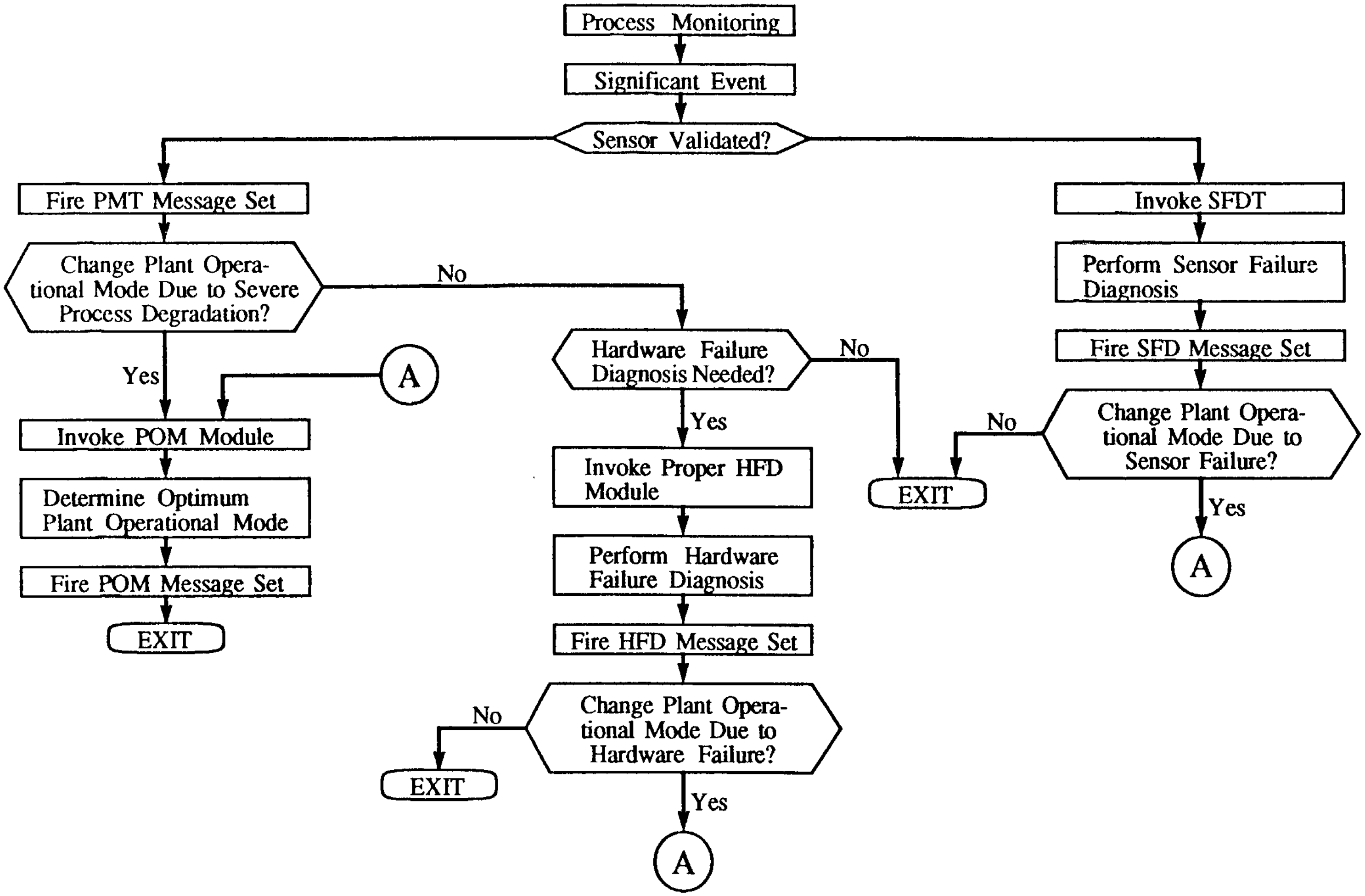

Process Monitoring
Significant Event
Sensor Validated?
Fire PMT Message Set
Change Plant Operational Mode Due to Severe Process Degradation?
No
Yes
A
Invoke POM Module
Determine Optimum Plant Operational Mode
Fire POM Message Set
EXIT
Hardware Failure Diagnosis Needed?
No
Yes
Invoke Proper HFD Module
Perform Hardware Failure Diagnosis
Fire HFD Message Set
Change Plant Operational Mode Due to Hardware Failure?
No
EXIT
Yes
A
EXIT
Invoke SFDT
Perform Sensor Failure Diagnosis
Fire SFD Message Set
Change Plant Operational Mode Due to Sensor Failure?
No
Yes
A

Figure 11. Overall Algorithm of the Methodology

Table 1.
Sample PMT Message Sets

IDENTIFIER	PMT MESSAGE SET
PMT-LT511-LLA	[PD] SG11 LEVEL LOW-LOW [OA] VERIFY REACTOR/PLANT TRIP FOLLOW POST-PLANT-TRIP IMMED ACTIONS
PMT-LT511-LLA.L	[PA] SG11 LEVEL LOW (LT511=***) REACTOR/PLANT TRIP AT -46.8 INCHES
PMT-LT511-L.NL	[PA] SG11 LEVEL MOD LOW (LT511=***) REACTOR/PLANT TRIP AT -46.8 INCHES
PMT-LT511-NH.H	[PA] SG11 LEVEL MOD HIGH (LT511=***) TURBINE/PLANT TRIP AT 50 INCHES
PMT-LT511-H.HHA	[PA] SG11 LEVEL HIGH (LT511=***) TURBINE/PLANT TRIP AT 50 INCHES
PMT-LT511-HHA	[PD] SG11 LEVEL HIGH-HIGH [OA] VERIFY TURBINE/PLANT TRIP FOLLOW POST-PLANT-TRIP IMMED ACTIONS

Note: The current sensor value will be inserted in the places of the three asterisks.