Journal of the Korean Nuclear Society
Volume 32, Number 3, pp.261~273, June 2000

An Integrated On-Line Diagnostic System for the NORS Process of Halden Reactor Project: The Design Concept and Lessons Learned

Inn Seock Kim
Hanyang University
17 Haengdang-dong, Sungdong-gu, Seoul 133-791, KOREA
iskim@nural.hanyang.ac.kr

(Received December 30, 1999)

Abstract

During an extensive review made as part of the Integrated Diagnosis System project of the Halden Reactor Project, MOAS (Maryland Operator Advisory System) was identified as one of the most thorough systems developed thus far. MOAS is an integrated on-line diagnosis system that 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 failure diagnosis, (3) on-line hardware (besides sensors) failure diagnosis, and (4) real-time corrective measure synthesis. The MOAS methodology was used at the Halden Man-Machine Laboratory HAMMLAB of the OECD Halden Reactor Project. The performance of MOAS, developed in G2 real-time expert system shell for the high-pressure preheaters of the NORS process in the HAMMLAB, was tested against a variety of transient scenarios, including failures of the control valves and sensors, and tube leakage of the preheaters. These tests showed that MOAS successfully carried out its intended functions, i.e., quickly recognizing an occurring disturbance, correctly diagnosing its cause, and presenting advice on its control to the operator. The lessons learned and insights gained during the implementation and performance tests also are discussed.

Key Words : diagnosis, on-line diagnosis, process diagnosis, MOAS, halden reactor project, NORS process, HAMMLAB

1. Introduction

On-line process diagnosis, or simply on-line 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.

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 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.

The rationale for the necessity of diagnosis in process plants including nuclear power plants is given from various perspectives elsewhere[1]. There has been a surge of interest, and as a result considerable research, in diagnostic systems or disturbance analysis systems (DASs) worldwide a couple of decades ago, including the EPRI-DAS by the Electric Power Research Institute (EPRI) of the USA, and the STAR system by Gesellschaft fur Reaktorsicherheit (GHS) of Germany and the OECD Halden Reactor Project. However, it did not result in a successful installation of such systems in the control room of nuclear power plants, mainly because of the lack of a reliable methodology for diagnosis[2].

Since the early efforts for developing DAS and STAR system, many different types of diagnostic systems were developed in various industries, particularly chemical processing, nuclear power, and aviation. At the OECD Halden Reactor Project which has been long focusing on the development of computerized operator support systems (COSSs), several COSSs have been developed to assist the operators in managing failures (i.e., detection, diagnosis, and correction). The COSSs developed include Early Fault Detection (EFD) [3], Detailed Diagnosis (DD) [3], and Extended Detailed Diagnosis (EDD) [4].

To integrate these systems and further enhance the techniques used, a literature review of similar COSSs was made as part of the Integrated Diagnosis System project of the HRP[5]. During this review, the integrated on-line diagnosis system MOAS (Maryland Operator Advisory System) [6,7] was identified as one of the most thorough systems developed thus far. MOAS is an integrated diagnosis system that 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 failure diagnosis, (3) on-line hardware (besides sensors) 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. In addition, the first principles, such as mass/energy conservation or control algorithms, are effectively used within the models.

The MOAS methodology was implemented at the Halden Man-Machine Laboratory HAMMLAB by: 1) developing models using the MOAS method; 2) programming the models into a real-time expert system using the G2 expert system shell, 3) establishing a data interface between the MOAS system and the NORS process of HAMMLAB; and 4) testing the performance of the MOAS system [8].

This paper first gives the design concept of

MOAS, and then describes the NORS (Nokia Research Simulator) process of HAMMLAB, the development of MOAS models and their implementation in G2[9], and the performance tests, along with the lessons learned.

2. Design Concept of MOAS

The design of an integrated diagnosis system based on the MOAS methodology evolves 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 configurations of the target process in order to model the fault propagation structure.
(6) Develop hardware failure diagnosis modules from each of the simplified directed graphs.
(7) Generate a module for the determination of plant operational mode.
(8) Design an appropriate real-time inference control scheme.

The goal-tree success-tree (GTST) model [6,7] is used to organize the knowledge of the process and its operation in a logical, hierarchical, and complete fashion. It also helps to identify process monitoring points, i.e., the sensors that should be continuously or periodically monitored by the computerized system to achieve the top objective defined in the GTST. For each process monitoring point, a process-monitor tree is developed, and then used on-line to continuously or periodically monitor the process.

Failures in sensors or sensor signals are diagnosed by applying several sensor-validation criteria (SVCs) in the structure of sensor-failure diagnosis trees (SFDT). [6,7] The SVCs are formulated from deep knowledge about the process, such as mass or energy balances, controller algorithms, coherency between the controller's output and valve opening, or the pump's characteristic curve between flow rate and pressure head.

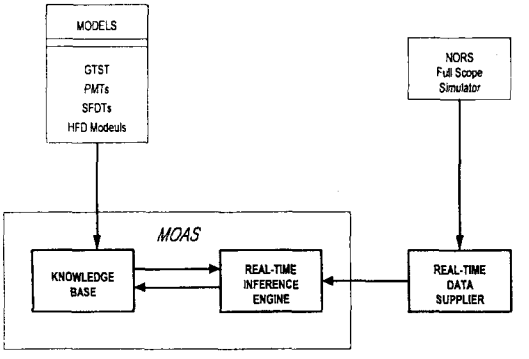

Fig. 1. Development Process and Structure of MOAS

Diagnosis of hardware (except sensors) failures in MOAS is based on hardware-failure diagnosis (HFD) modules for each of the process disturbance patterns that are identified in terms of particularly important process parameters, such as controlled variables. The HFD modules [6,7] contain failure hypotheses for the patterns, on-line verification methods to test the hypotheses, and message sets. When a specific pattern is identified on-line, MOAS activates the HFD module associated with the pattern, testing the hypotheses using the verification methods. If a failure hypothesis is verified or accepted, then the message set associated with the hypothesis is presented to the operator.

The programming of the various models using an artificial-intelligence (AI) technique or an expert-system shell constitutes the knowledge base of the real-time diagnostic expert system, as shown in Figure 1. The models facilitate not only

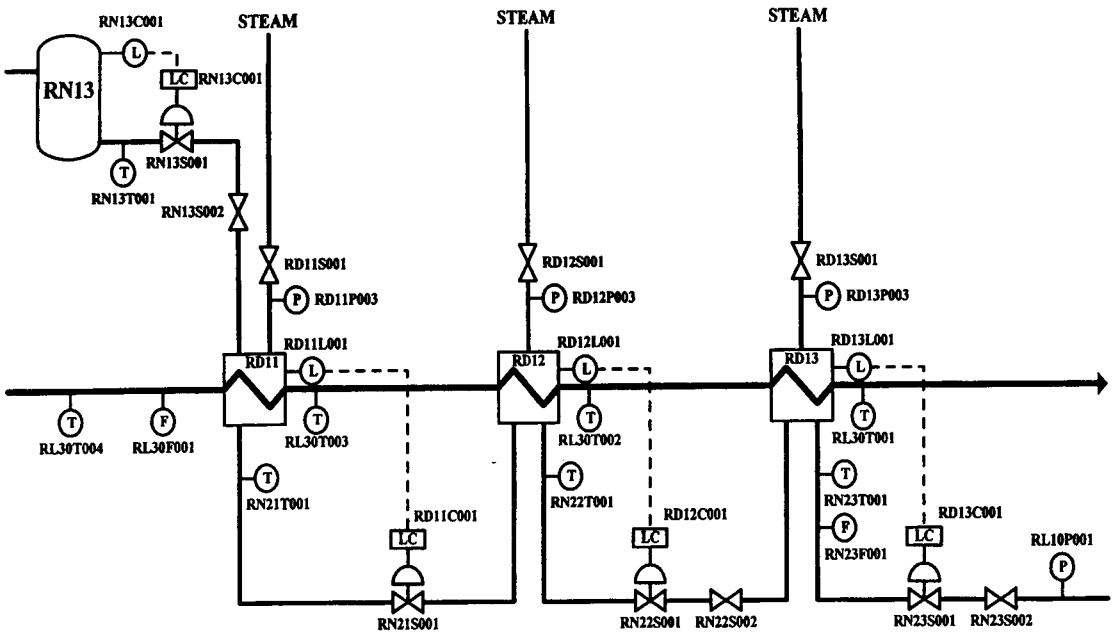

Fig. 2. NORS Target Process - the High Pressure Preheaters in the Feedwater System

the knowledge acquisition--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 system, a primary concern in the practical application of expert-system techniques. A more detailed discussion of the MOAS approach is given in references [6,7] along with its application to the main feedwater control system of a U.S. pressurized water reactor.

3. NORS Process

Figure 2 shows a schematic of RD10 high-pressure preheaters (HPPs) of the NORS (Nokia Research Simulator) process which were selected as the target process in this study. In normal full-power operation, feedwater passes from the RL10 feedwater tank through the three high-pressure preheaters. Steam extracted from several bleeding points of the SA10 high-pressure turbine is the main heating medium for the HPPs. For the RD11 HPP, the warm water from RN13 drainage collector (from the RB11 superheater and moisture separator) as well as the steam, heats up the feedwater flow. The drain flow from the RD11 and RD12 HPPs is used as the heating medium, along with the steam for the RD12 and RD13 HPPs, respectively.

The target process of Figure 2 shows the four different level controllers, RN13C001, RD11C001, RD12C001, and RD13C001, that regulate the water levels of RN13, RD11, RD12, and RD13, respectively. The levels are controlled by manipulating the outlet flows using the control valves, RN13S001, RN21S001, RN22S002, RN23S003.

A salient characteristic of the HPPs, especially for process diagnostics, is the tight coupling of the process units, i.e., three cascaded HPPs each with feedback control mechanism, which makes early

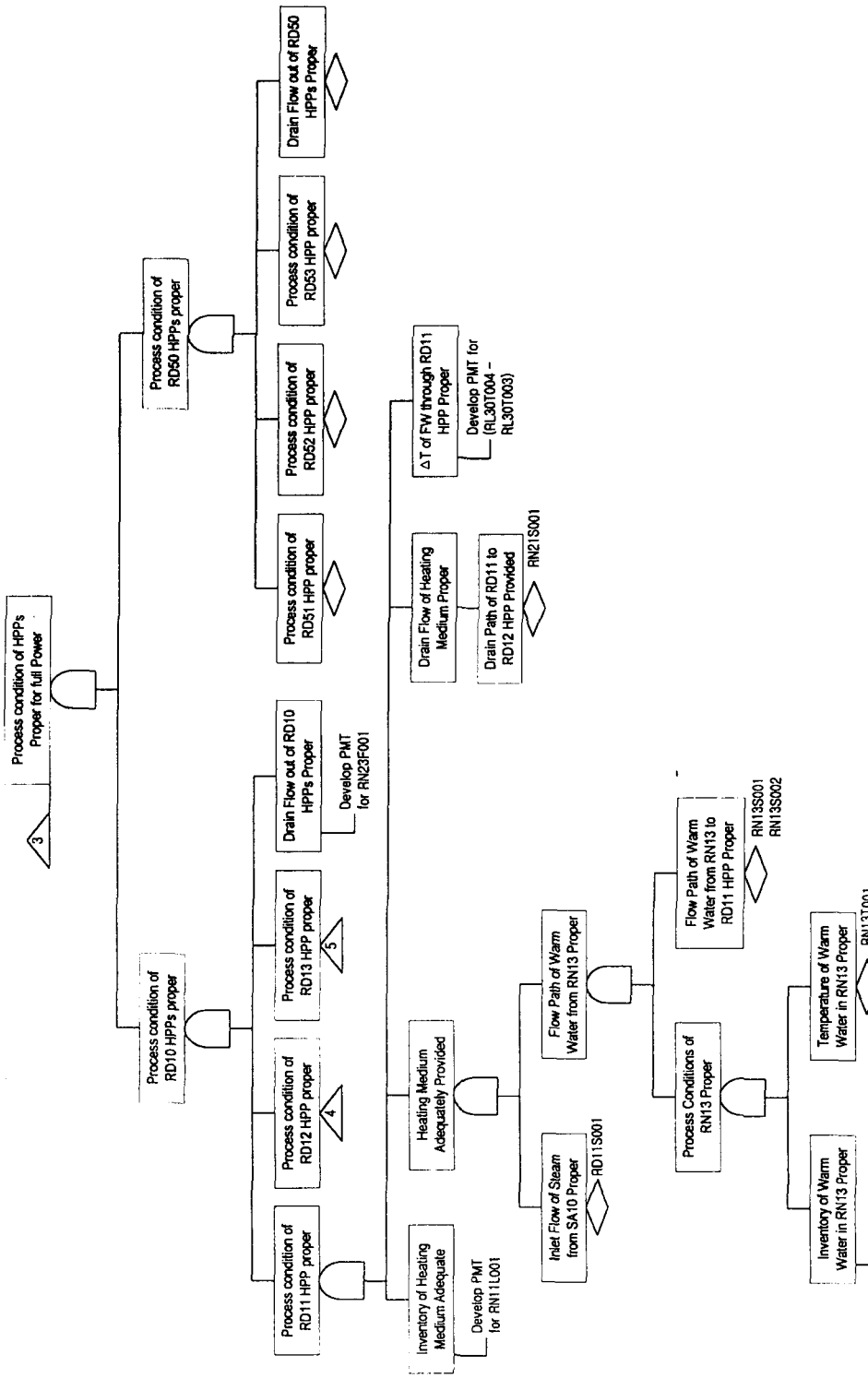

Fig. 3. Goal-Tree Success Tree for the NORS Process (Part)

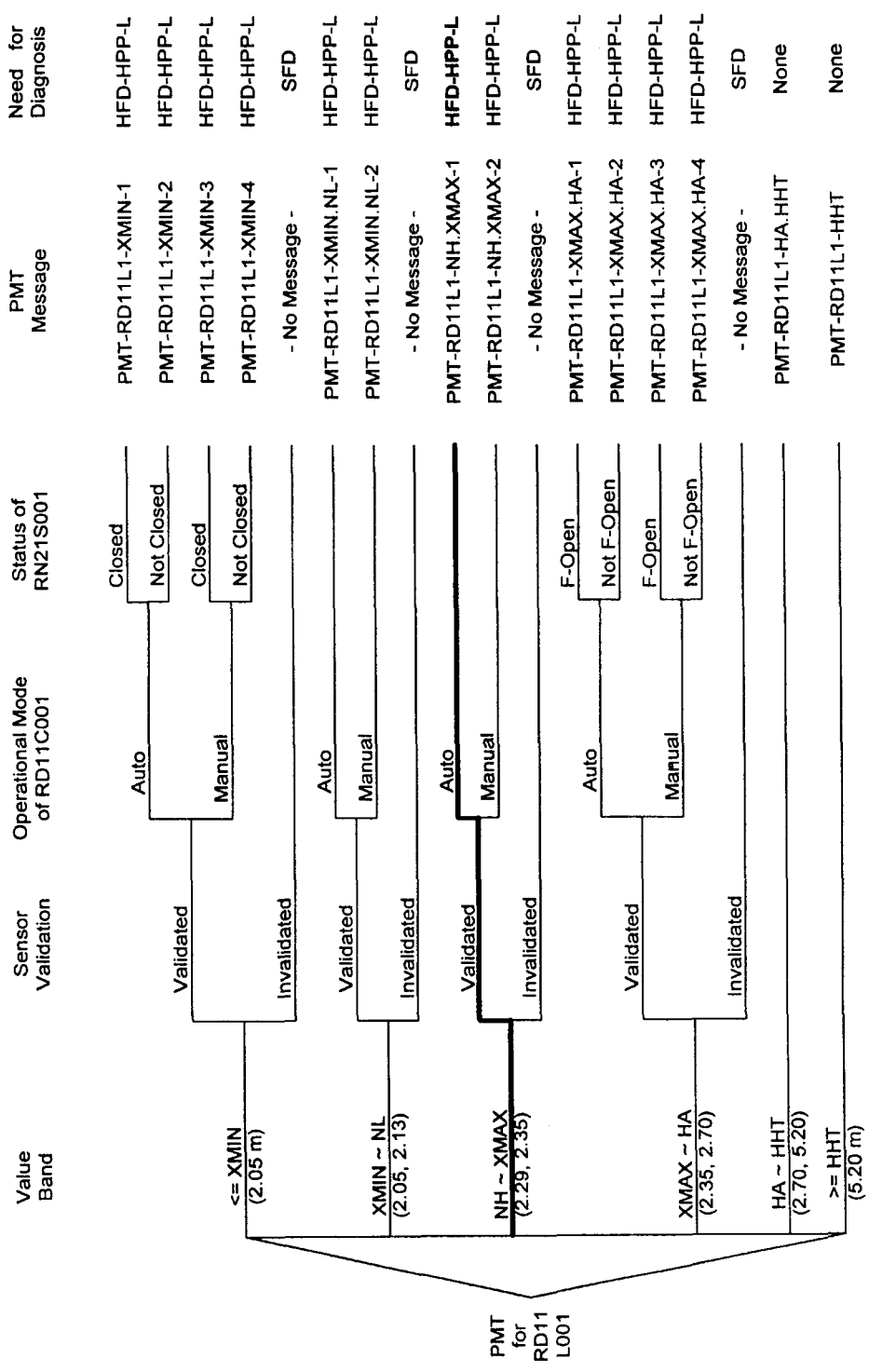

Fig. 4. Process Monitor Tree for RD11L001 Sensor

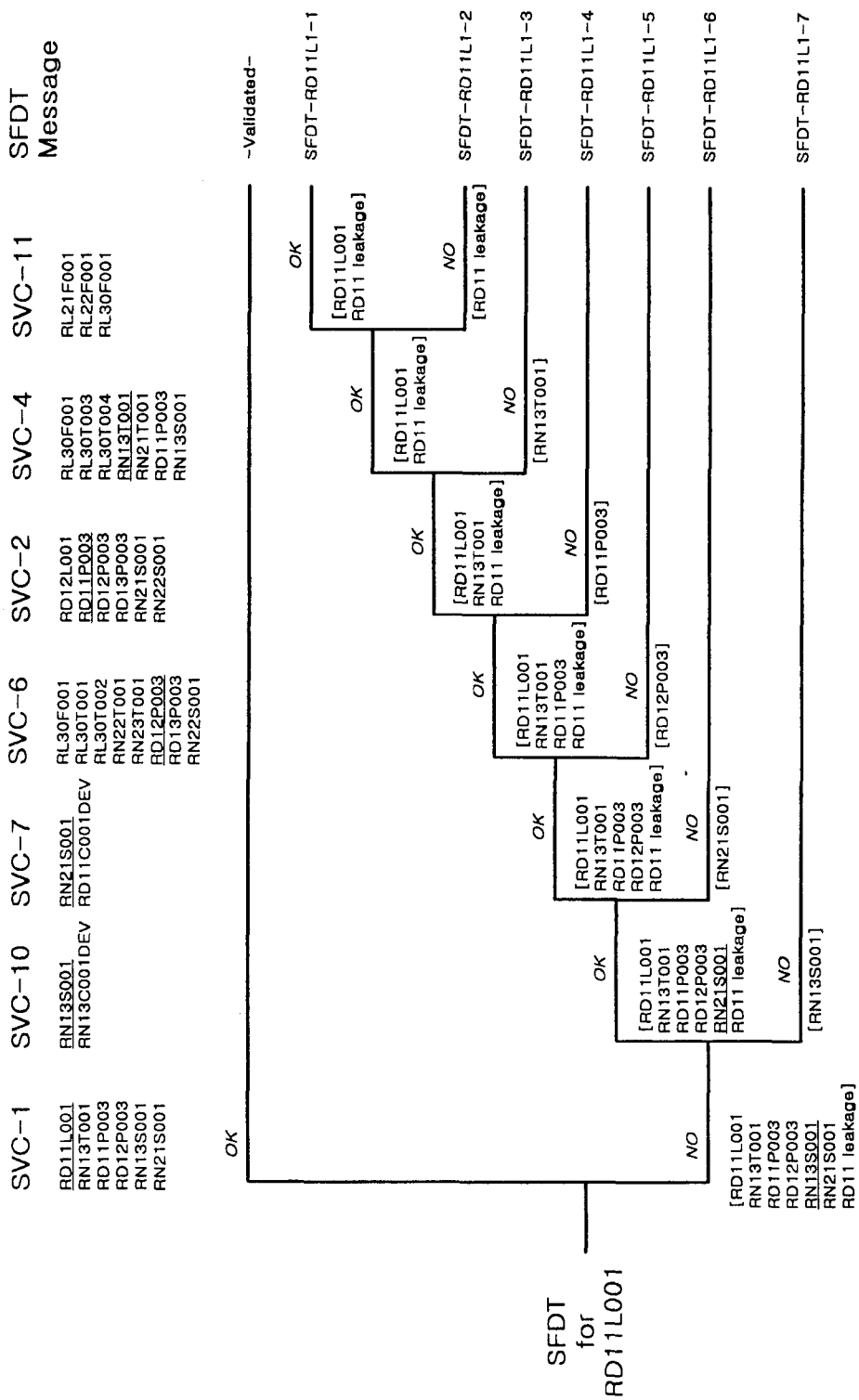

Fig. 5. Sensor Failure Diagnosis Tree

Table 1. HFD Module of RD11L001.H - RD12L001.N-RD13L001.N [8]

Failure Hypothesis[*1]	On-Line Verification	HFD Message Set[*6]
(1) FM1 RD11 Leakage	F-RD11-Mass; [*2] F-FW-Mass [*3]	[DG] RD11 Leakage [OA] Monitor RD10 Levels [PA] Auto Bypass of RD10 at 2.7m; Auto Trip of FW Pumps at 5.2m
(2) FM20 RN13C001 Output Fails High	RN13C001 in auto; F-RD13C001.H	[DG] RN13C001 Output Fails High [OA] Manually Control RN13 Level Monitor RD10 Levels
(3) FM15 RD11C001Output Fails Low	RD11C001 in auto; F-RD11C001.L[*4]	[DG] RD11C001 Output Fails Low [OA] Manually Control RD11 Level; Monitor RD10 Leve
(4) FM5 RN21S001 Fails Closed	F-RD11C001- RN21S001.H[*5]	[DG] RN21S001 Fails Closed [CM] Manually Control RN13S001 [OA] Monitor RD10 Levels

[*1] FM=Failure Mode

[*2] F-RD11-Mass : ABS [{K.RN21S001 * SQRT (RD11P003 - RD12P003) * RN21S001} - FLOW.STEAM.RD11 - {K.RN13S001 * SQRT (PRESS.RM13T001 - RD11P003) * RN13S001} + {AREA.RD11 * (RD11L001.NEW - RD11L001.OLD) * DENSITY.WATER / DELTA.T}] > RD11.MASS.TOL

[*3] F-FW-Mass : ABS[RL21F001 + RL22F001 - RF30F001] > FW.MASS.TOL

[*4] F-RD11C001.L : RD11C001DEV - CALC.RD11C001DEV < -RD11C001.TOL
where RD11COO1DEV is the actual controller output value and CALC.RD11C001DEV is the value obtained by the controller algorithm.

[*5] F-RD11C001-RN21S001.H : RD11C001DEV - RN21C001DEV > RD11C001.RN21S001.TOL

[*6] DG =Diagnosis; OA=Operational Aid; PA=Prealarming; CM=Corrective Measure

on-line diagnosis difficult. This was the major reason why we selected the RD10 HPPs for demonstrating the MOAS approach.

4. Development of MOAS Models and Implementation in G2

The various MOAS models discussed earlier were developed for the NORS process of HAMMLAB. Figures 3 ~ 5 show representative MOAS logic models for the process: a part of goal-tree success-tree for the node of "Process condition of HPPs proper for full power", and the process monitor tree for RD11L001 sensor which measures the water level of the RD11 high-pressure preheater, and the sensor failure diagnosis tree for the RD11L001 sensor, respectively.

Figure 6 depicts the simplified directed graph for the NORS process which represents the fault propagation structure in the process, and Table 1 represents the hardware failure diagnosis module

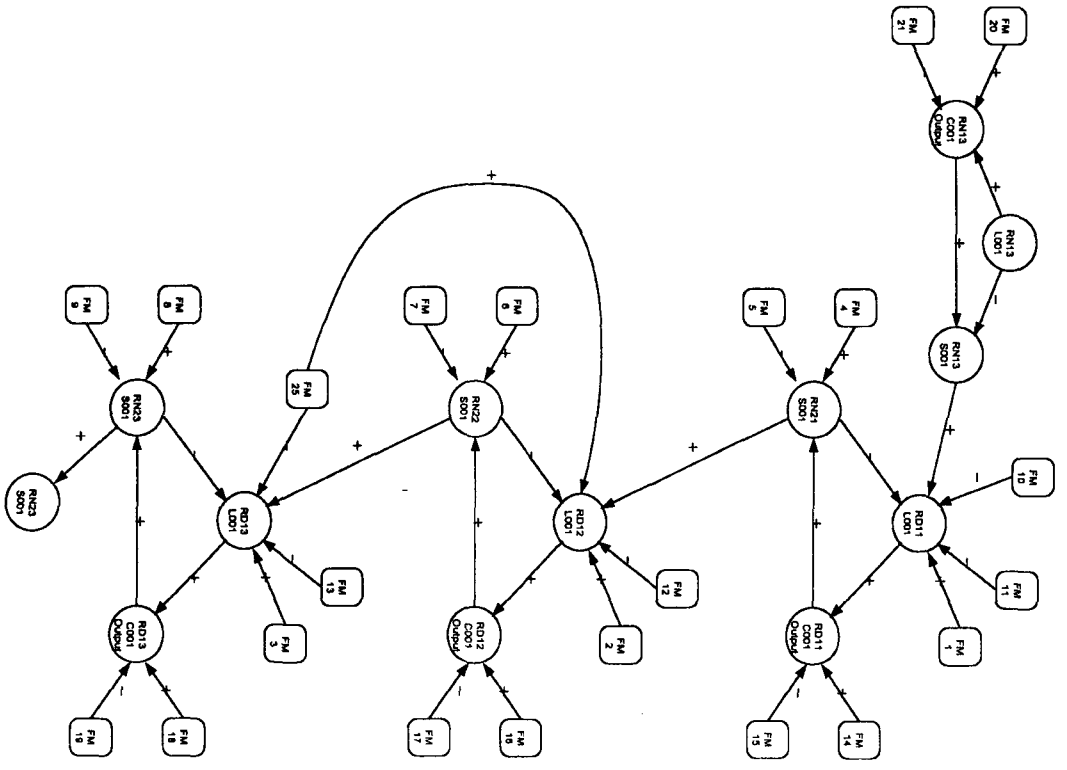

Fig. 6. Simplified Directed Graph for the NORS Process

of RD11L001.H-RD12L001.N-RD13L001.N which is the module activated when the level disturbance pattern in the RD11, RD12, and RD13 HPPs is high, normal, and normal, respectively.

These models were programmed using G2 real-time expert system shell [9] based on both object-oriented and rule-based techniques. The main components of the target process, such as high-pressure preheaters (HPPs) and sensors, are represented as objects, each of which has a table of attributes. The values of some attributes are dynamically updated as the process changes.

The MOAS models can be relatively easily implemented because of the logical and transparent nature of the models. Important considerations in this regard involve how to construct the class and object hierarchies so they can be efficiently used, how to design the real-time inference control schemes, how to avoid potential conflicts from the various models, and so on. The detailed discussion of these aspects can be found in reference [7].

5. Performance Tests

The performance of MOAS was tested against various transient scenarios from the NORS simulator, obtained by simulating malfunctions, such as stuck failures of the control valves, leakage of the tubes inside the high-pressure preheaters, and failures of the temperature, pressure, and flow sensors.

Let us assume that the drain valve of RD11 preheater, i.e., RN21S001, is stuck at 50% position at 15 seconds (Figure 7); the normal

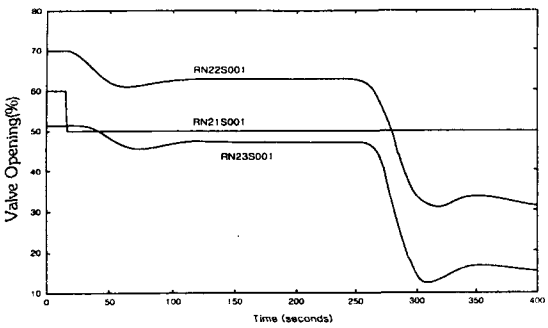

Fig. 7. Dynamic Behavior of the Control Valves

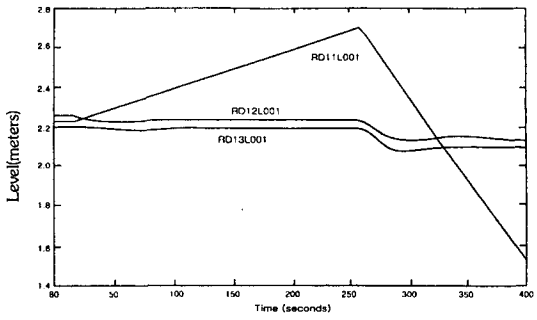

Fig. 8. Dynamic Behavior of the High Pressure Preheater Levels

position of the valve is about 60%. As shown in the figure, the level control systems of the RD12 and RD13 preheaters reduce the outlet flow by decreasing the opening of the drain valves, RN22S001 and RN23S001, to maintain their normal levels. However, the level of RD11 preheater continuously increases (Figure 8) because of the failure of the final control element, i.e., its drain control-valve RN21S001. About 250 seconds after the failure, the RD11 level will reach 2.7 m which is the setpoint for auto bypass of the RD10 HPPs and also an alarm setpoint, if no intervention has been made.

MOAS detects the rising level when it goes above the NH limit (2.29 m) defined in the RD11L001 PMT (Figure 4). The abnormal level may be detected between NH and XMAX (2.35 m), or between XMAX and HA (2.7 m), depending on the interval of scanning the PMT and how busy the data acquisition system and the inference engine of MOAS are.

Let us assume that the level is detected when it lies between NH and XMAX. The functioning of the RD11L001 sensor is first tested using SVC-1, as shown in Figure 5. Based on the mass balance for RD11, this SVC is not violated, because the mass balance, in terms of the RD11 level and the inlet and outlet flows, still is satisfied. Thus, the validated branch is followed.

Next, the operational mode of the RD11C001 controller is checked; this controller is in the automatic mode. Because the end of the tree is now reached, the message set of PMT-RD11L1-NH.XMAX-1 is presented to the operator from the PMT: [PD] RD11L001 high, [ST] RD11C001 in auto, [PA] Auto Bypass of RD10 at 2.7 m. The two-letter codes of PD, ST, and PA represent what kinds of message they are: PD means process degradation, ST component or system status, and PA prealarming. In addition, three additional codes are used in MOAS: DG to present the result of diagnosis, CM to present a course of corrective measures, OA to provide an additional operational aid, such as procedural assistance.

MOAS continues its function after presenting the messages of process degradation, status, and prealarming to the operator. As the RD11L001 PMT shows (Figure 4), there is a need to diagnose hardware failures, using the HFD-HPP-L hardware-failure diagnosis unit

The pattern of the process disturbance first is identified in terms of the levels of RD11, RD12, and RD13 HPPs, to result in HNN (i.e., high RD11 level, normal RD12 level, and normal RD13 level). Four failure hypotheses are included in the HFD module of RD11L001.H-RD12L001.N-RD13L001.N (Table 1); they are

FM1 (RD11 leakage), FM20 (RN13C001 output fails high), FM15 (RD11C001 fails low), and FM5 (RN21S001 fails closed).

Each of these failure modes is tested using the associated on-line verification method of the module. In this case, the first three failure modes are not accepted because the mass balances of F-RD11-Mass and F-FW-Mass are not violated, and also the controller outputs of RN13C001 and RD11C001 have not failed according to the comparison of the actual outputs with the outputs calculated using the control algorithms.

However, the last failure mode, i.e., FM5 (RN21S001 fails closed), is accepted because the coherent relationship between the output of the RD11C001 controller and RN21S001 valve opening is violated according to the evaluation of the expression F-RD11C001-RN21S001.H which checks coherency. Additional messages, including the result of diagnosis, then are presented to the operator: [DG] RN21S001 fails closed, [CM] Manually control RN13S001, [OA] Monitor RD10 levels.

6. Lessons Learned

The lessons learned and insights gained from the application of the MOAS technique to the NORS process of HAMMLAB are summarized below:

(1) The performance tests of MOAS in the HAMMLAB indicate that MOAS can successfully diagnose various sizes of malfunction as shown in Table 1, not simply a dichotomy of the component status, i.e., success or failure. This capability comes from the fact that MOAS effectively uses first principles and deep knowledge of the process, such as mass or energy balance equations, controller algorithms, within the various models working together as an integral unit for the single purpose of process disturbance management. The many small disturbance models, e.g., a PMT for a pressure sensor A, an SFDT for a temperature sensor B, and an HFD module for a particular process disturbance pattern, etc., work in a coherent manner for an efficient treatment of process disturbances.

(2) MOAS is intended to support the decision making process of the operator in his task of process disturbance management. As such, the message from the MOAS is simply transmitted to the operator, without a direct implementation of the conclusion through an automatic control system. However, the direct implementation of MOAS conclusion may be considered where rapid control of the process anomaly is needed or there is no human supervisor of the process as in unmanned space vehicles. MOAS employs a defense-in-depth mechanism in that the process monitoring trees supervises the state of the process independently from the diagnosis models. Should any serious deterioration happen in the process, then it either informs the operator of the deterioration or provides an appropriate signal to the plant control system.

(3) The NORS process includes several feedback control loops. The feedwater control system to which MOAS was applied previously for a US PWR employs a more complex control scheme, that is, auctioneered-highest cascading control system. In view of the successful tests of MOAS against these control systems with associated instrumentations, the basic concept of MOAS methodology may also be applicable to diagnosing failures in digital control systems

that are under consideration for wider applications to nuclear power plants.

7. Conclusions

The performance tests of MOAS at HAMMLAB of the Halden Reactor Project indicate that it successfully carries out its intended functions, i.e., quickly recognizes an occurring disturbance, correctly diagnoses its cause, and presents advice on its control to the operator. Therefore, the model-based technique can be considered for a wider scope of applications, e.g., extending to the whole secondary side of a PWR, or the entire process of the plant.

Comparing MOAS with the diagnostic systems of the HRP, particularly EFD/DD (i.e., Detailed Diagnosis coupled with Early Fault Detection), we find that the technique of sensor-failure diagnosis of MOAS, based on sensor-validation criteria in the framework of sensor-failure diagnosis trees, is similar to the EFD/DD technique. However, the latter has some potential advantages over the SFDT. Hence, one may consider replacing the SFDTs with a concise table of the EFD/DD, with some necessary arrangements to integrate it within the overall methodological framework of MOAS.

MOAS diagnoses hardware failures, based on identifying process-disturbance patterns in terms of important parameters, such as controlled variables. Then, it checks each relevant hypothesis by a certain verification method. This approach was found to be effective, especially because MOAS activates only the module which is directly relevant to the particular process condition, and, as a result, the search space is reduced considerably.

For future research, the potential value of the techniques used in MOAS may be considered for the Integrated Diagnosis System of the Halden Reactor Project, along with the EFD/DD and EDD (Extended Detailed Diagnosis) techniques. The basic concepts of MOAS, particularly its systematic approach to process monitoring, may be applied to other operator support systems being developed at Halden, e.g., Computerized Accident Management Support (CAMS).

References

1. I.S. Kim, "On-Line Process Failure Diagnosis: The Necessity and a Comparative Review of the Methodologies," International Topical Meeting on Safety of Thermal Reactors, Portland, Oregon, July 21-25 (1991).
2. I.S. Kim, "Computerized Systems for On-Line Management of Failures: A State-of-the-Art Discussion of Alarm Systems and Diagnostic Systems Applied in the Nuclear Industry," Reliability Engineering and System Safety, 44, 279 (1994).
3. ø. Berg, R.E. Grini, T. Suzudo et al., "Detailed Diagnosis Coupled to Model-Based Fault Detection in Process Plant Operation," OECD Halden Reactor Project, HWR-220, May (1988).
4. R.E. Grini, "The Integrated Diagnosis System - The Integration Aspects and Extended Detailed Diagnosis," Enlarged Halden Programme Group Meeting on Fuel Performance and Materials Testing and Man-Machine Systems Research, Storefjell, Gol, Norway, March 7-12 (1993).
5. R.E. Grini and T. Kaarstad, "Integration of Diagnosis Techniques for Process Surveillance," OECD Halden Reactor Project, HWR-317, May (1992).
6. I.S. Kim, M. Modarres, and R.N.M. Hunt, "A

Model-Based Approach to On-Line Process Disturbance Management: The Models," Reliability Engineering and System Safety, 28, 265 (1990).

7. 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, 29, 185 (1990).
8. I.S. Kim, R.E. Grini, and S. Nilsen, "A New Process Surveillance and Diagnosis System for NORS Based on the MOAS Methodology," OECD Halden Reactor Project, HWR-386, October (1994).
9. Gensym Corp., Version 3.0 of the G2 User' s Manual, Gensym Corporation, Cambridge, MA (1993).