CONF-870832--8

Presented At
American Nuclear Society Topical Meeting
Artificial Intelligence and other Innovative
Computer Applications in the Nuclear Industry
Snowbird, Utah
August 31 - September 2, 1987

CONF-870832--8

DE88 004920

An Expert System for Sensor Data Validation and Malfunction Detection

Siavash Hashemi[1], Brian K. Hajek, Don W. Miller
Nuclear Engineering Program
The Ohio State University
Columbus, Ohio 43210

Introduction

Nuclear power plant operation and monitoring in general is a complex task which requires a large number of sensors, alarms and displays. At any instant in time, the operator is required to make a judgment about the state of the plant and to react accordingly. During abnormal situations, operators are further burdened with time constraints. The possibility of an undetected faulty instrumentation line, adds to the complexity of operators' reasoning tasks.

Failure of human operators to cope with the conceptual complexity of abnormal situations often leads to more serious malfunctions and further damages to plant (TMI-2 as an example). During these abnormalities, operators rely on the information provided by the plant sensors and associated alarms. Their usefulness however , is quickly diminished by their large number and the extremely difficult task of interpreting and comprehending the information provided by them. The need for an aid to assist the operator in interpreting the available data and diagnosis of problems is obvious.

Recent work at The Ohio State University Laboratory of Artificial Intelligence Research (LAIR) and the nuclear engineering program has concentrated on the problem of diagnostic expert systems performance and their applicability to the nuclear power plant domain. We have also been concerned about the diagnostic expert systems performance when using potentially invalid sensor data. Because of this research, we have developed an expert system that can perform diagnostic problem solving despite the existence of some conflicting data in the domain. This work has resulted in enhancement of a programming tool, CSRL[1, 2], that allows domain experts to create a diagnostic system that will be to some degree, tolerant of bad data while performing diagnosis. This expert system is described here.

Diagnosis in CSRL

The developed expert system is capable of diagnosing the coolant system malfunctions of a simplified General Electric Boiling Water Reactor-6 (BWR/6) with Mark III containment. This model is developed by using Final Safety Analysis Report (FSAR) and other related documents of the Perry Nuclear Power Plant, near Cleveland, Ohio.

---

1. Currently at IntelliCorp, MountainView, CA

Problem solving in this domain has a generic character and typically has the task of classifying a given case into a diagnostic statement. In classification, the form of the required knowledge is of the form of a hierarchy of malfunction hypotheses[3]. In this hierarchy of malfunctions, the top levels are more general diagnostic classes, and the bottom levels correspond to more specific cases (a type/subtype arrangement of the malfunctions). The set of the tip nodes in this hierarchy will then be thought of as the diagnostic conclusions relevant to the system.

The coolant system malfunctions are arranged in a class/subclass hierarchical malfunction tree (Fig. 1). Each node on this tree is called a malfunction specialist and contains domain specific knowledge (or a knowledge base). Each specialist also contains information about how to utilize its knowledge base which is called the control knowledge.

Utilizing the above two sources of knowledge, diagnosis is performed on this malfunction hierarchy. The problem solving strategy of this classification system is a top-down examination of the hierarchy, termed "Establish-Refine"[4].

Establish refine can be thought of as the examination of the "appropriateness" of a particular malfunction of the hierarchy. If that malfunction is found appropriate (i.e. Established), then its submalfunctions are also asked to establish (i.e. Refine). If a specialist is not established, then none of its subnodes need be examined and that part f the tree can bee pruned. Thus, the arrangement of the specialists on this hierarchical tree is of importance.

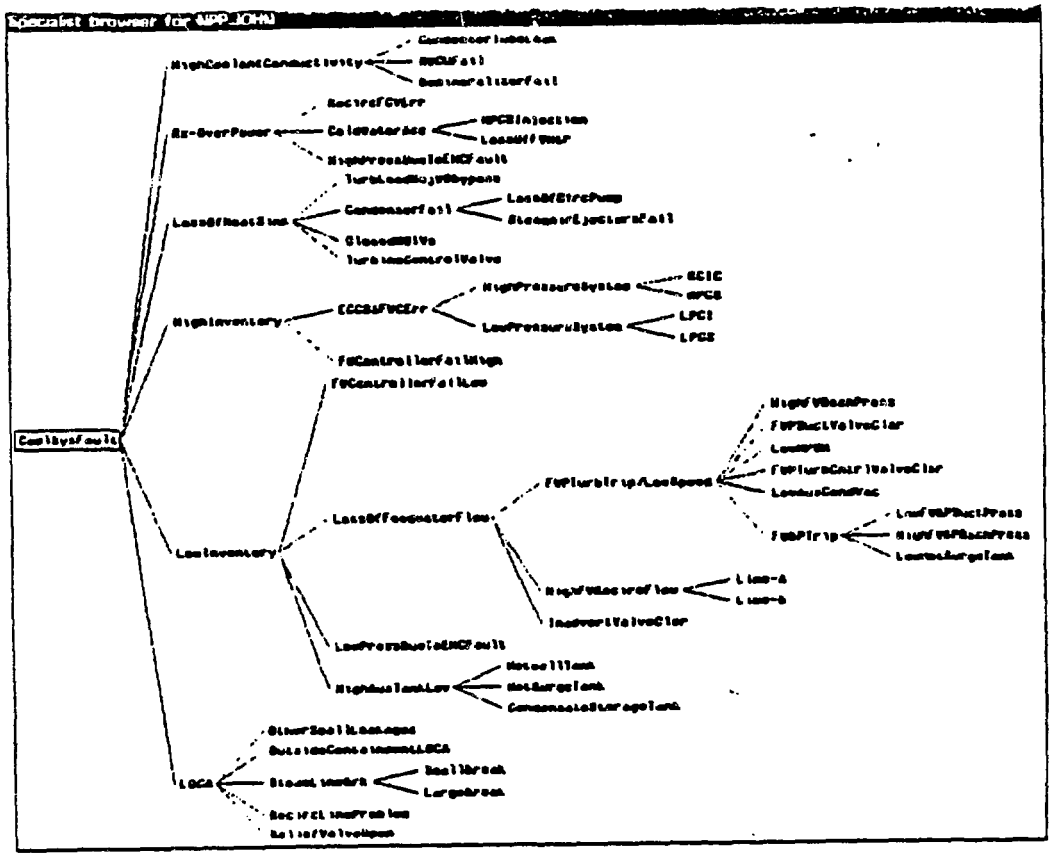

FIG 1. HIERARCHY OF MALFUNCTION SPECIALISTS

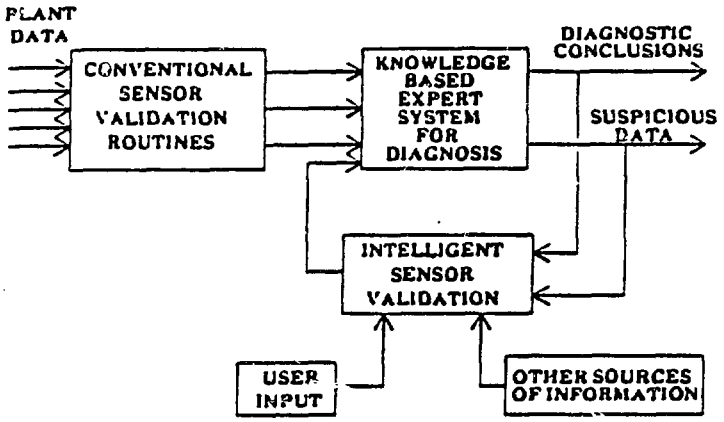

FIG 3. SENSOR VALIDATION ROUTINE BLOCK DIAGRAM

2. The second level of validation is beyond hardware redundancy and is accomplished through expectations derived during malfunction diagnosis. "That is, in the process of exploring the space of possible malfunctions, initial data and intermediate conclusions set up expectations of the characteristics of the final answer"[6]. This method of validation uses analytical redundancies and local versus system loop condition and is aimed at more subtle failures (such as instrumentation calibration drifts), and failures that are not detectable through the first stage of validation (such as common cause failures). This technique is described below.

During the design stages of this system, a great deal of attention was paid to ensure the system's ability of reaching a diagnostic conclusion based on partially complete data sets as well as potentially incorrect input parameters. To reach this goal, all relevant and useful sources of information for each malfunction hypothesis (specialist) were identified. Next, the relationship between them are determined and proper combinations of this information are utilized in establishing or rejecting the malfunction hypotheses. As an example, in order to detect a large Loss Of Coolant Accident (LOCA), the containment and the reactor pressure vessel parameters as well as the turbine-generator, suppression pool, main steam line and feedwater parameters are considered. In this fashion, having only a partial list of valid parameters, a fairly accurate diagnosis is still possible.

One of the important factors to be noted here is that some combinations of the input data values can be marked as not capable of occurring or highly unlikely, due to violation of "normal expectations" of malfunctions[6, 7]. That is, in the process of matching the malfunction patterns to data, certain combinations of data do not make sense in the given domain. As an example, turbine/generator electrical output must be zero (or decreasing rapidly), if the Main Steam Isolation Valves (MSIVs) are closed.

Thus, the process of faulty sensor identification involves three steps. These steps are:

1. The first step is to set some expectations by using local knowledge, or the context of other nodes.

2. The second step is to use these expectations to flag particular data values as questionable. And,

3. The third step is the process of validating (accepting) or rejecting the questionable sensor values based on the relational redundancies available in other parts of the plant.

The evaluation of malfunction appropriateness is based on knowledge embedded in each malfunction node of the hierarchy. In essence, each node is capable of performing a simple kind of problem solving that evaluates whether the malfunction at this node exists, given the currently available data. This is accomplished by the knowledge groups of each node (Fig 2). Each knowledge group contains domain expertise in the form of, "what pattern of data must exist for this malfunction to be labeled appropriate? Furthermore, if the indicated pattern found, how must the appropriateness of the malfunction be modified?"

Appropriateness measure of each node is obtained by utilization of the confidence factors. These confidence factors range from -3 to +3 with significances ranging from "DEFINITELY NOT" to "DEFINITE", respectively. Confidence values are represented in the "VALUE" column of the Figure 2.

Should the confidence value of a node be determined as +2 or +3, then the subnodes of that particular specialist are also examined. If the node's confidence factor is determined to be between -1 to +1, further analysis of its subnodes are only possible if further data be available, or no other conclusive diagnostic conclusion is obtained. If the confidence value of a node is -2 or -3, the subnodes of that particular specialist are ignored until later steps into the diagnostic reasoning.

Up to this point, it has been assumed that the input data are a set of valid and reliable data. These input data are assumed to have gone through the standard data validation routines (Fig. 3) and are in general, reliable. However, due to common cause failures, the input data may be faulty, and thus, some of the data may require further analysis. The past studies have also shown that sensor data validation and diagnosis are integral components to one another and one can not be accomplished without the other, in an efficient manner. Thus, sensor data validation is added to this expert system and is described next.

Sensor Data Validation

Sensor data validation can be thought of as a two stage function. Each stage is capable of identifying a certain class of faulty sensors. The two stages are as follows:

1. This stage of data validation which is mainly dependent on comparison of redundant sensor signals (such as "like sensor"comparisons, fail safe assumptions, auctioneering, and so on) and is aimed at identification of gross failures of the instrumentation channels (such as shorts, open circuits, connector or detector failures). These techniques are based on various kinds of redundancy in sensor hardware and are discussed elsewhere[5].

SRVopen KG of ReliefValveOpen

Expressions of table
1- (AskYNU? "Are there any SRVs open")
2- (AskHLN? "What is the suppression pool temperature")
3- (AskTrend? "What is the suppression pool temperature trend")
4- (AskHLN? "What is the suppression pool water level")

1	2	3	4	VALUE	SENSOR
T	(or H HH)	(or I II)	(or H HH)	3	---
(or F U)	(or H HH)	(or I II)	(or H HH)	3*	1
(or F U)	N	(or I II)	?	1*	1 4
?	?	?	?	-3	---

FIG 2. AN EXAMPLE OF A KNOWLEDGE GROUP IN MODIFIED CSRL

The expectations derived during diagnosis are utilized as an extra source of redundancy, in addition to various conventional sensor hardware redundancies. These expectations are embodied in the specialists' knowledge groups and are formed and encoded a priori. The knowledge groups were then modified to check the malfunction pattern fit to the input data, and flag the parameters that lie outside the expectations as suspicious. The suspicious data are then subjected to further analysis. This concept is demonstrated in the last column of Figure 2.

The knowledge group rows that do not meet the expected symptoms are identified as containing suspicious data by addition of a "*" in their confidence values, as can be seen from Figure 2. The * alarms the computer (and the user) that this row may contain invalid data and thus, the confidence factor of this knowledge group may change as a result of sensor data validation.

Should a knowledge group row be identified as containing suspicious data, one of the following two cases must be valid:

- The set of expectations are not valid at that particular instant of time (eg. IF LARGE LOCA THE RPV WATER LEVEL=LOW is no longer valid if we are on the recovery path of a large LOCA).
- The set of symptoms are not valid at this particular instant of time which leads to the conclusion "THE XYZ (GROUP OF) SENSOR(S) HAVE FAILED".

In order to determine which one of the above situations is true, further analysis on the suspicious sensors is necessary. This analysis utilizes the following resources:

- Logical conclusions drawn from diagnosis,
- Logical conclusions drawn from available data,
- Analytical calculations,
- Causal relationships between unlike parameters

These extra sources of information about the suspicious sensors are used to either validate or reject suspicious data and are arranged in the order of preference for each individual sensor. In this fashion, the routines with minimum cost, highest reliability, or minimum effort can be executed first, depending of each individual sensor. Note that this methodology is relying on unlike sensor data comparison and thus, common cause failures or instrumentation channel drifts are no longer problems.

One important factor to avoid in this routine is that validation of one sensor should not rely on information supplied by another sensor which is also in the suspicious sensors list. That is, one has to rely on the "potentially valid" data as redundancy, as opposed to "potentially faulty".

Once the faulty sensors are identified, there are two routes that can be taken:

1. Replace that faulty data with the new (and validated) value and resume diagnosis after informing the user, or
2. Ignore that faulty data (mark it as Unknown) and resume diagnosis after informing the user.

These two methods must lead to the same diagnostic conclusion (because a real plant can only have one state at a time). However, the first method is adapted for this project, due to ease of implementation.

An Illustrating Example

An inadvertent closure of the MSIVs (Closed MSIVs malfunction node of Fig. 1) is considered as an example. If the MSIVs close, the Safety Relief Valves (SRVs) should cycle, in order to relieve and maintain pressure in the RPV. For this scenario, it is assumed that one of the SRVs fails to reclose after opening.

TO make this scenario more complicated for malfunction diagnosis, it is also assumed that the direct indications of SRV and MSIV positions have failed and read CLOSED and OPEN, respectively. That is, the control board lights do not change status from their pre-event indications.

During the first run of the diagnostic system, the LOCA node has fired with a confidence factor of 0* to show more evidence is required to either establish or reject the LOCA possibility. Further up in the tree, the ClosedMSIVs and TurbineControlValve nodes fire with confidence factors of 0* and 3*, respectively. This means that there is a mild indication of MSIV closure and therefore, a strong evidence for the wrong turbine control valve position.

During the sensor signal validation step, the list of suspicious data is inspected and validated. Backup information for the SRV position is obtained from the local suppression pool temperature profile and SRV-downcommer pressure (Perry specific). The backup information for the MSIV position was obtained from matching the steam flow rate, RPV pressure and turbine electrical output.

After validation of the suspicious data, the new values are replaced in the database and new diagnosis indicated the correct state of the plant [Fig 4]. The new confidence factors indicate that no more suspicious data exists.

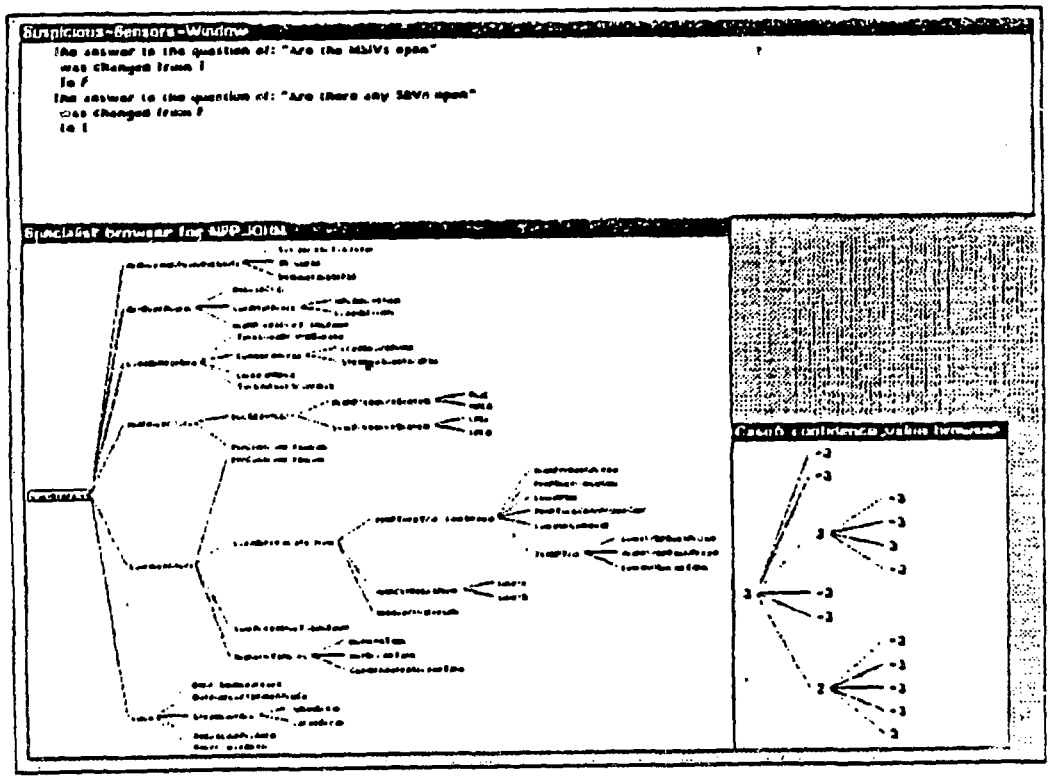

FIG 4. INADVERTENT CLOSURE OF MSIVS AFTER VALIDATION

Conclusions

This expert system is capable of performing diagnosis and sensor data validation, in an efficient manner. This expert system is tolerant to faulty input parameters to a certain extent, and provides an additional sensor validation routines to the nuclear power plant personnel.

Acknowledgments

The authors wish to acknowledge Professor B. Chandrasekaran for his insights and assistance in developing these ideas. We would like to also acknowledge Mr. John Stasenko for his attempts to expand the knowledge base of this expert system. This work was supported in parts by NSF, DOE, and internal grants.

References

1. T. Bylander, S. Mittal, B. Chandrasekaran, "CSRL: A Language for Expert Systems for Diagnosis", Proc. of IJCAI 83, Los Altos, CA, PP 218-21.

2. B. Chandrasekaran, "Decomposition of Domain Expert Knowledge into Knowledge Sources: the MDX Approach", Proc 4th National CSCSI/SCEIO, Sakatoon, Canada, May, 1982.

3. B.K. Hajek, S. Hashemi, D.D. Sharma, B. Chandrasekaran, D.W. Miller, Artificial Intelligence Enhancement to Safety Parameter Display Systems", Proc. 6th Power Plant Dynamics, Control and Testing Symposium, Knoxville, Tenn, April, 1986.

4. B. Chandrasekaran, "Towards Taxonomy of Problem Solving Types", AI Magazine, Vol 4, No. 1, Winter/Spring 1983. J.J. Deyst, R.M. Kanazawa, J.P. Pasquenza, "Sensor Validation: A Method to Enhance the Quality of Man/Machine Interface in Nuclear Power Stations", IEEE Transactions on NS, Vol NS-28, No. 1, Feb. 1981.

5. B. Chandrasekaran, W.F. Punch, "Data Validation During Diagnosis, a Step Beyond Traditional Sensor Validation", Proc. AAAI, Seattle, WA, 1987.

6. B. Chandrasekaran, W.F. Punch, "Hierarchical Classification: Its Usefulness for Diagnosis and Sensor Validation", Proc 2nd AIAA/NASA/USAF Symposium on Automation, Robotics, and Advanced Computing, Feb 1987.