Proceedings of the Korean Nuclear Society Autumn Meeting
Seoul, Korea, October 1998

# A New Perspective into Root-Cause Analysis and Diagnostics

Inn Seock Kim, Tae Kwon Kim, and Min Chull Kim

Hanyang University
Department of Nuclear Engineering
17 Haengdang, Sungdong, Seoul 133-791, Korea

## Abstract

A critical review of diagnostic and root-cause analysis methods, developed in nuclear, chemical process, aviation industries, was made. Based on this review, the insights into both off-line and on-line diagnostics, and also root-cause analysis are preseted from a new perspective. This perspective may be applied for various purposes, including real-time on-line process diagnosis, root-cause analysis of reactor scrams, diagnosis of severe accidents, or situation identification of an on-going emergency at a nuclear site.

## 1. BACKGROUND AND INTRODUCTION

The term diagnosis is widely used, not only in medical field or day-to-day living, but also in various fields of engineering. The Webster dictionary defines it as an investigation or analysis of the cause or nature of a condition, situation, or problem. In engineering fields, it may be more appropriately defined as the determination of the cause or root-cause of an undesirable state, an equipment failure, a system failure, or a process failure. Thus, we may regard the two terms, diagnosis and root-cause analysis, as being synonymous, although they sometimes have been used in different contexts.

As man-made equipment, system, or process eventually degrades over time, a failure will be brought about sooner or later. The failure then should be diagnosed at the earliest possible time to maximize its availability, or prevent it from escalating into a hazardous situation.

The failure diagnosis can be performed in different dimensions, such as off-line or on-line. The off-line diagnosis is carried out to find the root cause of the malfunction so that the operability of the equipment can be restored. The on-line diagnosis is done by manipulating on-line measurements or process attributes, such as on-line status of process equipment, to control the outcome of the on-going failure or disturbance of the process as soon as possible and with minimum adverse consequences.

The purpose of this paper is to present a new perspective into root-cause analysis and diagnostics. Although the perspective has been drawn mainly from the review of various on-line diagnostic methodologies and our experiences with developing such diagnostic systems, it also can be applied to off-line diagnosis or root-cause analysis.

The perspective presented herein can be used in carrying out an off-line or on-line diagnosis of equipment, system, or process. Specific examples include, but are not limited to, the following:

1) Failure diagnosis of a main feedwater system[1-5]

2) Failure diagnosis of a turbine lubrication oil system[6]

3) Performance degradation analysis or root-cause analysis of diesel generators[7]
4) Root-cause analysis of a reactor scram[8]
5) Diagnosis or situation identification of a severe accident[9]
6) Situation identication of a plant under site emergency by the regulatory body[10]

## 2. NEW PERSPECTIVES

### 2.1 Dynamic Versus Snapshot Data

On-line diagnosis is basically performed by analyzing real-time data from the process equipment or the plant, based on certain logic or knowledge embedded in the diagnostic system. The values of process sensors would be within certain bounds during normal operation, partly due to the plant control system or some inherent feedback mechanism, if any; however, the plant status may significantly change in a major process upset, going out of the bounds.

Most diagnosis methods,[11] including cause-consequence tree, logic flowgraph and KATE, were designed to interpret a *snapshot* of plant states at a single time-point. A snapshot is only partially informative and even misleading, because processes often exhibit nonmonotonic behaviors, including compensatory (normal -> high -> normal) and inverse (normal -> high -> low) responses.[12] *Dynamic* process information during transients, caused by process malfunction, often provides important cues for solving the diagnostic problem, and therefore, should be properly used, especially for systems with interconnected control loops.

### 2.2 Qualitative Versus Quantitative Data

For process monitoring or pattern recognition of process disturbances, qualitative data transformed from the raw, quantitative process data, such as high, low, or normal, may be useful. Diagnosis in conventional methods, e.g., primarily based on causality models, was made using only qualitative data; the measurement-pattern-based diagnosis algorithm developed by Shiozaki et al.[13] is a typical example.

However, quantitative process data also may be useful in making diagnosis, especially in relation to the use of dynamic data and deep knowledge of the process. There is an increasing trend of using quantitative process information as well as qualitative data for diagnosis, partly because of the high processing capabilities of modern computers.

### 2.3 Deep Versus Shallow Knowledge

One of the most important steps in developing a diagnostic system is to acquire and properly incorporate knowledge about the target process in the diagnosis system so that the knowledge can be effectively and efficiently used for on-line diagnosis in real time, An important lesson from past studies is that use of *deep knowledge*, i.e., underlying physical knowledge, such as conservation equations (mass or energy balance), pump performance curves, or control algorithms, can significantly improve the diagnostics.

For example, in MOAS II,[2-5] a coherent relationship, called sensor validation criterion (SVC), is formulated among the values of sensors around a pump (e.g., sensors for suction and discharge pressure, flow, and pump speed) based on the head-capacity relationship of the pump. This SVC is then used along with other SVCs, e.g., based on mass balance applied to several flow sensors around the pump, as a basis for sensor fault diagnosis. Similar coherent relationships among process variables and parameters based on deep knowledge of the process also are used in MOAS II for on-line verification of failure hypotheses in diagnosing hardware (except sensors).

However, shallow knowledge, i.e., plant-specific experiential compilations of the underlying principles, such as heuristics rules of thumb, also be an efficient shortcut to problem solving in certain situations. For example, given certain familiar symptoms in terms of patterns of several important measurement, an experienced operator may come up with a list of possible causes. Once this kind of shallow knowledge is available and properly validated, it may be used together with deep knowledge for diagnostic monitoring. Diagnosis in MOAS Ⅱ is based on mostly deep process knowledge; however, shallow knowledge, if available, can be incorporated in the knowledge base of MOAS Ⅱ, since the situation-specific nature of the approach eases the incorporation.

### 2.4 Causality and Fault Propagation: Role and Need for a Simplified Model

In operating equipment or systems of a process plant, fault propagates following *causality*, i.e., relationships between cause and effect, based on the underlying physical principles. Because an inherent nature of diagnosis is that it involves deductive reasoning to infer the cause which brought about the effect or observed system misbehaviors, the causal relationships between process variables, i.e., qualitative simulation of the faults, can be used as an effective tool for diagnosis.

One of the most typical approaches to modeling the causality or fault propagation structure is directed graph or diagraph[11] which has a superior capability of process representation. Various diagnostic methods, primarily based on digraph or its variant (e.g., signed directed graph,[12] logic flowgraph[11]) were developed over the years; a logic model, such as fault tree, was then derived from the fault-propagation structure for use as a template for diagnosis or root-cause analysis. However, as a side effect of higher process-modeling capability, these methods became more and more complicated, even for a small-scale system. This complexity mainly stems from: (1) excessive dependence of the diagnostic system on the fault-propagation structure by using it for various purposes, including sensor failure diagnosis or hardware (except sensors) failure diagnosis, and (2) incorporation of various attributes of the process, such as the correlation between process variables and sensors, and the operational modes of controllers.

On the contrary, MOAS Ⅱ uses a simplified variant of digraph, called *simplified directed graph* (SDG), to model propagation of faults through the process. This simplification was made possible by the use of several different models for different functions needed for failure diagnosis and management. The failure models used on-line are sensor failure diagnosis trees (SFDTs) and hardware failure diagnosis (HFD) modules. The SFDTs are used specifically for sensor failure diagnosis, while the HFD modules for hardware (except sensors) failure diagnosis. Because sensor failures are treated by a different model, they do not need to be included in the SDG. Also, the fault propagation structure, i.e., the SDG, does not have to include all the attributes of the process, because some of the process attributes are taken into account in other models, e.g., process monitor trees (PMTs), Therefore, only essential causalities of the process can be modeled in terms of process variables, also without incorporating too many process attributes in the model.

Figure 1 shows an example of an SDG developed for the main feedwater system of a pressurized water reactor (PWR) plant,[2-4] employing a complex feedback control mechanism, i.e., auctioneering cascade control. The SDG consists of process-variable nodes, failure-mode nodes, and special nodes (i.e., auctioneer highest and common discharge header of feed pump bank), which are interconnected by arrows indicating the direction of influence between them. The signs on the arrows represent the direction of deviations of the two process variables from normal values. A positive sign indicates that the deviations occur in the same direction, while a negative sign denotes that the deviations occur in the opposite direction. The definition of the process variables and the failure modes in the SDG is given in Tables 1 and 2, respectively.

### 2.5 Importance of Effective Process Monitoring in Managing Failures

To diagnose failure in the process, the anomalous process condition caused by the failure should be first detected by a process monitoring scheme, Process monitoring, typically, has not been given sufficient considerations in developing diagnostic methods, It not only triggers the diagnosis, but also can serve as a barrier against further fault propagation. The process may continue to deteriorate in spite of the diagnostic system, because the diagnostic package may be incomplete (e.g., a certain failure mode of the process, especially multiple failures, may not be covered by the diagnostic system) or the real-time diagnosis may not be completed fast enough. Thus, even if the failure cause is not yet determined, a proper message should be provided to the operator when the process has deteriorated too much, so that a corrective measure can be taken, Preferably, this process surveillance function should be incorporated into a module which is independent from the diagnostic module, so that the process surveillance can continue independently according to a certain scheme. It is also important to design an *effective and efficient process-monitoring scheme* to reduce unnecessary burden on the computer and improve computational efficiency.

In MOAS Ⅱ, process monitor trees (PMTs) are used to monitor process behaviors in real time. A PMT does not need to be developed for every measurement. Only those measurements, i.e., process monitoring points, which were found to be important in the goal tree-success tree (GTST) model for the process, can be continuously or periodically monitored. For example, in the feedwater control system, the differential pressure sensors measuring △P across the feed regulating valves do not need to be continuously monitored. Much more important sensors than those, from a standpoint of process disturbance management, are discharge pressure sensors of the feedwater pumps and water level sensors of the steam generators. PMTs not only monitor the process condition, but also indicate which specific model (among various models for fault diagnosis or system reconfiguration) should be activated depending on the process condition. Where necessary, an appropriate message may be fired directly from the PMTs.

Figure 2 shows and example of a PMT for flow sensor FT401 in the main feedwater system of a PWR.[3] In this PMT, the value of the FT401 sensor is discretized into five abnormal value bands, and six headings are used to design a monitoring scheme for each band. To illustrate the on-line use of PMT, suppose that a scan interval of 5 seconds has been assigned to the FT401 PMT. The value of FT401 will be obtained through the data acquisition system every 5 seconds. This value is then checked against the predefined abnormal value bands. No data processing or inferencing will be performed, if the value is normal, i.e., does not belong to any abnormal band. For instance, if the FT401 value falls between L(3650pgm) and NL(5500gpm), then the trend of change is examined using the current value and some historical values. Only when the sensor value is nonincreasing, i.e., stagnant or decreasing, further inferencing will be performed by the real-time expert system following the logic structure of the FT401 PMT. If the value is increasing (i.e., toward the normal value band), the tree will not be activated any more. Five seconds later, the dynamic process variable will be re-examined in the same manner as was done in the previous scan.

Suppose the process condition is such that the FT401 value is now in the range between L (i.e., 3650 gpm) and LL (i.e., 2800 gpm); say, 3200 gpm. Validation of this value will then be performed because sensor validation is the first heading encountered after the inference engine of the diagnostic system has actuated the piece of the PMT indicating LL～L. If the sensor is validated, then the operational mode of flow controller FC401 will be checked. If FC401 is in automatic mode and also the status of control valve CV401 is closed (see the bold-faced branch of the PMT in Figure 2), then a message set, denoted as PMT-FT401-LL.L-1, is presented to the operator. This set contains the following messages: [PA] feed pump suction flow low (FT401 = 3200gpm), feed pump 11 trip at 2800gpm; [DG] feed pump 11 minimum flow CV401 fails closed; [OA] manually open CV401, verify feed pump 11 suction flow increasing.[3] Because it is indicated in the actuated branch that there is no need for diagnosis and for POM (plant operational mode) change in this specific case, neither any diagnosis model nor the module to determine the optimum POM will be activated from this PMT.

## 2.6 Provisions for Sensor Validation and Failure Diagnosis

Instrumentation failure is a common problem in process plants. The erroneous data acquired from malfunctioning sensors may corrupt the real-time inference process of the diagnostic system, resulting in a misdiagnosis which must be avoided at all costs.1 Therefore, provisions should be made so that sensor data can be validated, and furthermore, failures of the sensors can be diagnosed.

There now exist various techniques for sensor validation and sensor fault identification. Typical methods are Kalman filtering, parity space, like-sensor comparisons, and limit checking. Most of these methods apply for such a process environment where quite many like-measurements exist. MOAS II provides a method that can be applied for a process environment consisting of few like-measurements. This method is based on the effective use of the coherent relationships among process variables and parameters, discussed earlier, in the structure of a sensor failure diagnosis tree model.

## 2.7 Division of Sensor and Hardware Failure Diagnoses

In developing a model for diagnosis, it is extremely important to first recognize that there is a significant difference between sensor and hardware failures in terms of their resulting dynamic impact on the process. Hardware failures usually propagate through the plant process and cause the process condition to deteriorate. On the contrary, sensor failures, in general, do not cause any direct deterioration of the process, unless the sensor data are used as inputs to the plant control system and the controllers are in the automatic modes.

Hence, different models and techniques are needed to diagnose sensor and hardware failures. In MOAS II, sensor failures are diagnosed mostly by sensor failure diagnosis trees, while hardware failures are diagnosed in hardware failure diagnosis modules which are developed from the SDG described above.

## 2.8 Provisions to Control Real-Time Inference

A real-time diagnostic system, especially based on a number of different modules separately used on-line (e.g., MOAS Ⅱ), should be capable of performing many different inference processes almost simultaneously, because, while an inference process is being performed in a module, another inference process may be required to be carried out in another module. A problem may arise if these *multiple inference processes* are not properly controlled. When messages are incorporated in several modules, such as those for process monitoring and failure diagnosis, conflicting messages may be sometimes formulated during the inference process.[3,4]

Hence, provisions should be made to avoid the formulation of such conflicting messages. Furthermore, the control of multiple inference processes also may be necessary to prevent deterioration of computational efficiency by unnecessary multiple activations of the modules, as was the case in MOAS Ⅱ. In the MOAS-Ⅱ real-time expert system, the inference process is controlled by several local and global flags; a sensor failure diagnosis flag or a hardware failure diagnosis flag for local inference control inside each module, and a system status flag for global inference control across modules.

## 3. CONCLUSION

Various novel perspectives have been presented herein that may be useful in carrying out off-line diagnosis, on-line diagnosis, or root-cause analysis. In the case of off-line applications including root-cause analysis, an effective and efficient diagnostic scheme shall help enhance the availability of the relevant equipment or system, by reducing the time to restore the failed item. In the case of on-line applications, the use of such scheme enables a process failure to be arrested as quickly as possible and with the minimum adverse consequences. The early management of process failure will result in dual benefits in the plant operation, namely, 1) the improvement of safety by preventing the occurrence of accidents by intervening in the development of a minor failure into a major accident, and 2) the improvement of plant availability by avoiding unnecessary reactor scrams.

**Acknowledgment**

This work was supported by the Research Institute of Industrial Sciences, Hanyang University.

## REFERENCES

1. Meijer, C.H. and Frogner, B., On-line power plant alarm and disturbance analysis system. EPRI Report, Electric Power Research Institute, Palo Alto, CA, NP-1379 (April 1980).
2. Kim, I.S., Modarres, M. & Hunt, R.N.M., A model-based approach to on-line process disturbance management: The models. *Reliablility Engineering and System Safety*, Vol. 28 (1990), pp265-305.
3. Kim, I.S., Modarres, M. & Hunt, R.N.M., A model-based approach to on-line process disturbance management: The models. *Reliablility Engineering and System Safety*, Vol. 29 (1990), pp185-239.
4. Kim, I.S., A model-based approach to on-line process disturbance management. Ph.D. Dissertation, University of Maryland, 1988.
5. Kim, I.S., Grini, R., and Nilsen, S., A new surveillance and diagnosis system for NORS based on the MOAS II methodology. OECD Halen Reactor Project, HWR-386, October 1994.
6. Kang, C.W., Lee, J.B., Sui, Y. and Golay, M.W., An advisory Bayesian belief network-based expert system for on-line component monitoring. Probabilistic Safety Assessment and Management -- PSAM 4, A. Mosleh and R.A. Bari (eds), September 13-18, 1988, New York City, USA.
7. 김태운, 김길유 외, 정비최적화 기술개발 (월성1호기 예비디젤발전기), 월본(발전) 757.05-2216, 1997.9.
8. Chu, "Root Cause Guidebook: Investigation and resolution of power plant problems. Failure Prevention, Inc., San Clemente, CA, USA.
9. 김인석, 김명기, 권종주, 홍승열, 장순흥 외, 원전 사고관리계획 방향 정립 연구, 전력연구원 TR.96NJ11.97.77, 1997.10.
10. 원자력 안전백서, 정부간행물 97-4-1-3, 과학기술처, 1997.8.
11. Kim, I.S., On-line process failure diagnosis: the necessity and a comparative review of the methodologies. Proc. Safety of Thermal Reactors, Portland, Oregon, July 1991.
12. Finch, F.E., Oyeleye, O.O. & Kramer, M.A., A robust event-oriented methodology for diagnosis of dynamic process systems. *Computers and Chmical Engineering*, Vol. 14 (1990), pp1379-96.
13. Shiozaki, J. et al. An improved algorithm for diagosis of system failures in the chemical process, *Computers and Chemical Engineering*, 9:3 (1985) pp285-293.

Table 1
Process Variables Used in the SDG

| IDENTIFIER | PROCESS VARIABLE |
|---|---|
| S401 | Speed of Feed Pump 11 |
| S402 | Speed of Feed Pump 12 |
| P402 | Discharge Pressure of Feed Pump 11 |
| P403 | Discharge Pressure of Feed Pump 12 |
| P11 | Upstream Pressure of Feed Regulating Valve CV511 |
| P12 | Upstream Pressure of Feed Regulating Valve CV512 |
| P21 | Downstream Pressure of Feed Regulating Valve CV511 |
| P22 | Downstream Pressure of Feed Regulating Valve CV512 |
| CV511 | Opening of Feed Regulating Valve CV511 |
| CV512 | Opening of Feed Regulating Valve CV512 |
| F511 | Downstream Flow Rate of Feed Regulating Valve CV511 |
| F512 | Downstream Flow Rate of Feed Regulating Valve CV512 |
| L511 | Downcomer Level of Steam Generator 11 |
| L512 | Downcomer Level of Steam Generator 12 |
| PD511 | Differential Pressure across Feed Regulating Valve CV511 |
| PD512 | Differential Pressure across Feed Regulating Valve CV512 |

Table 2
Failure Modes in the SDG

| IDENTIFIER | FAILURE MODE |
|---|---|
| FM1 | Speed Controller SC401 Output fails Low |
| FM2 | Speed Controller SC401 Output fails High |
| FM3 | Speed Controller SC402 Output fails Low |
| FM4 | Speed Controller SC402 Output fails High |
| FM5 | Differential Pressure Controller PDC511 Setpoint fails Low |
| FM6 | Differential Pressure Controller PDC511 Setpoint fails High |
| FM7 | Differential Pressure Controller PDC511 Output fails Low |
| FM8 | Differential Pressure Controller PDC511 Output fails High |
| FM9 | Differential Pressure Controller PDC512 Setpoint fails Low |
| FM10 | Differential Pressure Controller PDC512 Setpoint fails High |
| FM11 | Differential Pressure Controller PDC512 Output fails Low |
| FM12 | Differential Pressure Controller PDC512 Output fails High |
| FM13 | Flow Controller FC511 Setpoint fails Low |
| FM14 | Flow Controller FC511 Setpoint fails High |
| FM15 | Flow Controller FC511 Output fails Low |
| FM16 | Flow Controller FC511 Output fails High |
| FM17 | Flow Controller FC512 Setpoint fails Low |
| FM18 | Flow Controller FC512 Setpoint fails High |
| FM19 | Flow Controller FC512 Output fails Low |
| FM20 | Flow Controller FC512 Output fails High |
| FM21 | Differential Pressure Sensor PDT511 fails Low |
| FM22 | Differential Pressure Sensor PDT511 fails High |
| FM23 | Differential Pressure Sensor PDT512 fails Low |
| FM24 | Differential Pressure Sensor PDT512 fails High |

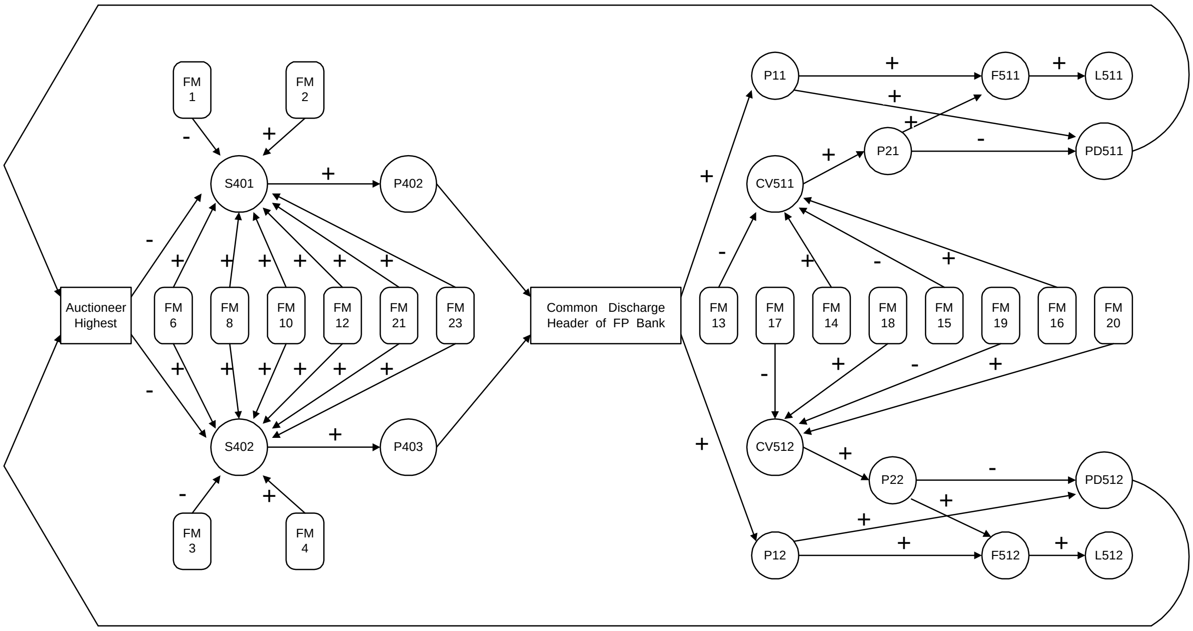

Figure 1. An example of Simplified Directed Graph(SDG) to model fault propagation structure of the feedwater control system of a PWR

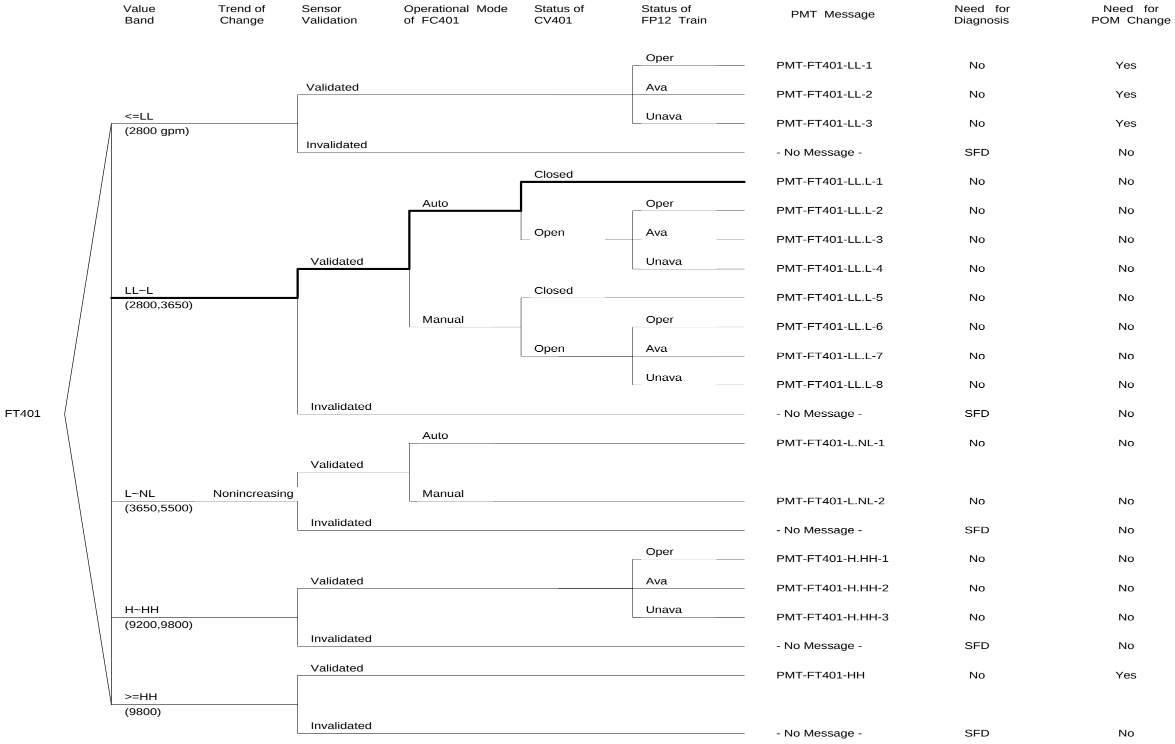

Figure 2. An example of Process Monitor Tree(PMT) for flow sensor FT401