

**Qualitative Fault Diagnosis in Systems with
Nonintermittent Concurrent Faults:
A Subjective Approach**

**Behrouz Homayoun Far
Matsuroh Nakamichi**

**Reprinted from
IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS
Vol. 23, No. 1, January/February 1993**

Qualitative Fault Diagnosis in Systems with Nonintermittent Concurrent Faults: A Subjective Approach

Behrouz Homayoun Far, *Member, IEEE*, and Matsuoh Nakamichi

Abstract—Major approaches to automatic fault diagnosis of industrial plants are either subjective or objective. Subjective approaches imitate and synthesize the way that human experts diagnose faults. Objective approaches automate a portion of diagnosis task that human's cognitive limitation does not allow handling it efficiently. Currently available subjective fault diagnosis techniques suffer from certain drawbacks such as: lack of knowledge for modeling and reasoning with the required levels of detail; inefficiency in utilization of sensory data; and poor in learning experienced schemas. A subjective approach to fault diagnosis, using qualitative modeling and reasoning within the multiple view of the system is introduced. The focus is on automation of the cognitive skills of human experts, that include utilizing conceptual models to detect inherent redundancy in system behavior; qualitative reasoning to predict future states; and information selection to avoid computation overload.

I. INTRODUCTION

MAJOR APPROACHES to automatic fault diagnosis of industrial plants and processes are either subjective or objective. Subjective approaches imitate and synthesize the way that human experts diagnose faults. Objective approaches automate a portion of the fault diagnosis task that human's cognitive limitation does not allow handling it efficiently, mainly because of limited capacity of the short term memory and inefficiency in managing precise calculation. Subjective approach to fault diagnosis is the main theme of this paper.

Human experts when engaged with a goal-oriented task, try to achieve the goal within the constraints imposed by the task and avoid cognitive overload through selective utilization of their accessible knowledge [45]. It is believed that they possess a conceptual (mental reference) model of how the objects in the external world work based on standard operating procedures. Such models can further be applied to novel or unanticipated situations [69]. The form of knowledge in the conceptual models is qualitative and its structure is hierarchical. A main goal of our research is developing methods for systematic generation and reasoning with the conceptual models. As in fault diagnosis a big portion of external world's

Manuscript received April 13, 1990; revised June 8, 1991. This work was supported in part by the Science and Technology Agency of Japan and in part by Japan Atomic Research Institute.

B. H. Far is with the Computing and Information Systems Center, Japan Atomic Energy Research Institute, Tokai-Mura, Ibaraki 319-11 Japan.

M. Nakamichi is with the Faculty of Engineering, Chiba University, 1-33 Yayoi-cho, Chiba, 260 Japan.

IEEE Log Number 9202110.

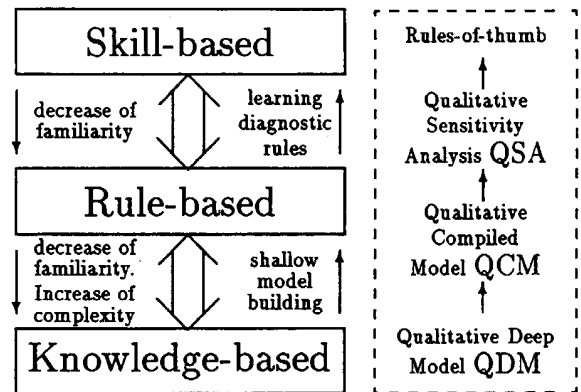


Fig. 1. Hierarchical model of human behavior and associated modeling and reasoning techniques.

data comes from the sensors, we have considered modeling with the maximum transparency to the sensory data.

Conceptual models have a hierarchical structure defined best by the skill-rule-knowledge (S-R-K) levels [50], [51] (see Fig. 1). In the S-R-K perspective, skill-based level denotes almost routine performance. In this level, human performance is governed by stored patterns of predefined instructions [53]. Such context specific patterns are called rules-of-thumb (or symptomatic rules), that map directly from an observation to a hypothesis. We introduce a method for systematic generation of such rules.

Rule-based level represents more conscious behavior when handling familiar problems. Rule-based behavior is conventionally described by decision tables, digraphs, fuzzy sets and natural language models [37]. The model for this level is a set of stored rules. We introduce the qualitative compiled model (QCM) and qualitative sensitivity analysis (QSA) [18], as the modeling and reasoning techniques for this level.

Knowledge-based level accounts for tasks for which common patterns in stored knowledge form do not exist and reasoning should start from the so called first principles. Qualitative deep model (QDM), methods for soliciting candidate faults, concurrent fault hypothesis validation and assessment of the situation, systematically explore different aspects of this level. To summarize, the subjective qualitative fault diagnosis (SQFD) technique is introduced, featuring:

- Modeling human expert's knowledge within the S-R-K hierarchical framework.
- Extending conventional qualitative models to include the

coordination and timing of events and using conventional qualitative simulation to generate complete set of normal and abnormal behaviors from the extended qualitative model and qualitative interpretation of sensory data.

- Generating passive component of the knowledge base [45] (i.e., compiled model) from the active component (i.e., qualitative deep model).
- Model-based learning of fault diagnosis heuristics (i.e., rules-of-thumb).
- Generating concurrent fault hypotheses, testing them for validity and deriving what may be affected by valid faults.

The organization of this paper is as follows: in Section II qualitative reasoning, conceptual modeling and learning are briefly reviewed. In Section III some important fault diagnosis techniques are surveyed and compared with the SQFD. Section IV gives a perspective of the SQFD. The knowledge-based (deep) modeling and reasoning technique is described in Section V and in Section VI a method for validating concurrent fault hypotheses is suggested. The rule-based (compiled) modeling and reasoning technique is introduced in Section VII and in Section VIII an assessment technique for updating the data base is presented. Finally, Section IX concludes by addressing some future research directions.

II. BACKGROUND

A. Qualitative Modeling, Reasoning, Simulation, and Interpretation

Qualitative reasoning (QR) attempts to formalize common sense knowledge of the physical world, and reason with that knowledge [6], [23]. QR refers to the inferring and decision making methods by means of qualitative data and models. Qualitative data describes a physical change symbolically, mainly only by a three valued quantity space $(-, 0, +)$. A qualitative model is a set of expressions composed of qualitative variables and qualitative relations. Variables are either continuous and continuously differentiable functions of time (i.e., reasonable variables [39]), or discrete with an ordered set of landmark values [47], [67]. Qualitative relations represent trends or functional relations (e.g., monotonic increase, decrease, etc.), ordering relations (e.g., bigger, smaller, etc.) and dependencies (e.g., influences [23]). Qualitative models provide the basis for simulation and reasoning [6]. Qualitative simulation (QS) uses a qualitative model and qualitative causal calculus to simulate and interpret the behavior of physical systems [9], [14], [23], [39], [47]. QR has to be elaborated significantly to be fully utilized in complex tasks such as fault diagnosis [63]. Some extension issues are: qualitative interpretation of the sensory data; generating and testing fault hypotheses; incorporating synchronization and time in the qualitative model; and learning diagnostic procedures. In qualitative interpretation, a finite set of reference patterns are recognized within the data. Methods for qualitative interpretation of a closed and temporally ordered set of numerical data have already been introduced [24]. In hypothesis generation and test the assumption-based truth maintenance (ATMS) has

been applied to test fault hypotheses [15] and extended it to account for hierarchies and multiple tests [64]. The ways of extending qualitative models to include synchronization and timing of events and learning diagnostic procedures by qualitative sensitivity analysis [17], [18] are issues discussed in this paper.

B. Conceptual Models

Conceptual models account for human understanding capabilities [2], reflecting how objects in the external world interact and behave [55]. Detailed survey on detection, diagnosis and compensation models of human problem solving and models of human performance are available [53], [56]. The skill-rule-knowledge (S-R-K) framework [50]–[52], is a unified view of various levels of human problem solving (see Fig. 1). The models comprising either of levels of the S-R-K are qualitative in nature [58], correspond to decreasing level of familiarity with the task [53], and account for the trade off between the problem solving task and mental workload.

A distinguished feature of reasoning with conceptual models is their strength when applied to making statements about trends of change, causal dependencies, and ordering of events within a certain level of abstraction. Qualitative simulation (QS) is a way of deriving behavior and functions from the model within a certain level. However, poor performance may be achieved when the conceptual models are used to manipulate numerical data or reasoning when shifting among the levels. Qualitative reasoning and simulation techniques are required to have the capability of handling the latter (see Section IV).

C. Knowledge Acquisition and Learning

In system diagnosis literature, poor skill learning, i.e., inefficiency in utilizing experiences gained from a comprehensive analysis of the plant, is reported [21], [22]. An observation shows that in many cases the same or similar faults may happen frequently [34]. Learning diagnosis procedures and augmentation and refinement of the knowledge, when dealing with similar cases, are important issues [1]. There are three stages of skill learning: autonomous, associative and cognitive, as counterparts of the S-R-K levels, respectively [58]. Among learning paradigms, model-based learning best suits fault diagnosis of man-made systems because a collection of problem solving experiences as well as a model of the normal system already exist. In this sense, knowledge acquisition for associative and cognitive levels of learning addresses transition between levels of the conceptual model. For instance, acquiring the deep qualitative model, generating compiled model from the deep qualitative model and generating rule-of-thumb from the compiled model. In this paper, we account for the latter cases (see Section VII).

III. CONVENTIONAL FAULT DIAGNOSIS: A COMPARATIVE SURVEY

Human's performance (in terms of speed, accuracy and

efficiency) in fault diagnosis¹ degrades drastically with the increase of size and complexity of the plant [57], [72]. In order to increase the reliability of decisions made by the operators and meeting the performance issues, partial automation of fault diagnosis tasks is desirable. An automated fault diagnosis system may include, various forms of data on physical components and instrumentation, models of behavior, failure modes of the components, fault trees and state transition diagrams, thresholds and limit values of the variables, experienced or predicted schemas, heuristic rules to limit the search space, etc. Both subjective and objective fault diagnosis systems involve generation and evaluation of signals for given fault hypotheses. Models, embodying individual entities (i.e., mathematical or symbolic generalization of the signals and their relationships), are found useful. Two classes of representation models, quantitative and qualitative, are considered in the system diagnosis literature. Qualitative models can predict the ordering of events and direction of changes, while quantitative models can give numerical predictions [66]. Fault diagnosis techniques, utilizing quantitative models, vary depending on the selection of individual entities (i.e., measurable signals, nonmeasurable variables or characteristic quantities, etc.) [4], [11], [12], [25], [35], [72]. Recently, techniques have been emerged using qualitative models [15], [27], [40], [54]. They are the outcomes of the merger of new AI paradigms (e.g., assumption-based truth maintenance ATMS, nonmonotonic reasoning, etc.), expert system technology and qualitative simulation techniques. These systems are either structure-oriented [21], [42] or procedure-oriented [28], [29], and can be classified based on using *shallow* models [62], [59], *deep* models [15], [40], or a combination of both [1], [22].

A. Structure-Oriented Approach

A common underlying assumption in qualitative model-based fault diagnosis techniques is that of structural composition, i.e., the system is broken down to its structural components and description of system behavior is derived from its structure. They first isolate a faulty region in the system and then employ additional test (e.g., heuristic rules or assumption verification) to verify the fault hypothesis and identify the exact problem [43] (see Fig. 2). In this sense, *shallow* techniques may involve reasoning from the compiled behaviors of the various components. *Deep* techniques may include more sophisticated models of the components including knowledge of the variables interaction or functional relations [43].

¹The term *fault diagnosis* means observing an error and deriving possible faults causing that error. In some texts the former task is called *fault detection* and the latter is named *fault diagnosis* (e.g., [35]). Detection, diagnosis and correction together are called *fault management* [37].

The terms *fault* and *error* are used in the sense that an error occurs when system deviates from its specified normal behavior, and the error is caused by a fault [60]. The fault is assumed to be *atomic* (either happens fully or not) *nonintermittent* (i.e., lasts over a considerable long time, as opposed to transient faults) and *logical* (i.e., affecting the system behavior). *Parametric faults* causing a gradual change in performance, such as changing speed or aging [7], are not accounted for in this paper.

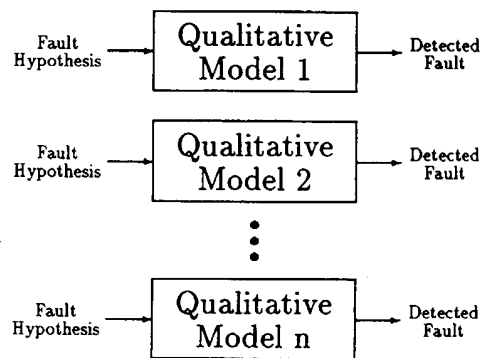


Fig. 2. Qualitative structure-oriented approach to fault diagnosis.

Structure-oriented fault diagnosis techniques have certain drawbacks, such as: counter intuitive diagnosis² [48]. Furthermore, inefficiency in knowledge representation and utilization of sensory data together may lead to computation overload, making it difficult to design time-critical fault diagnosis systems [44], [72].

It is stated that in structure-oriented approach, representation by structure and functions does not make apparent the relation between an observed behavior and a fault [31]. Specially, in a concurrent faults case, a fault in a local component can be propagated to the others, producing secondary symptoms and activating multiple alarms. Determining the behavior of the system due to each particular fault and then combining them to produce the behavior for concurrent faults is a necessity. In SQED we have considered ways of explicitly representing deviations of the behavior for concurrent faults and methods of avoiding ambiguities when simulating the behavior.

B. Procedure-Oriented Approach

In procedure-oriented approach a process is defined by a sequence of actions. The set of all behaviors of a process constitutes the actions [28], [29]. This definition of process is useful only when the relation between the actions and other modeling primitives, such as variables, can be established. In procedural fault diagnosis, the knowledge has an invocation and a body (see Fig. 3). The invocation is external to the body and test expressions are internal. They both may address a fault. Invocation is a logical expression that includes functions that examine the current goals and facts. Invocation can be either goal-oriented (i.e., for a fault hypothesis: proving that a fault exists), or fact-oriented (i.e., for an observed symptom). A test is a logical expression including functions for evaluating the newly established facts. A main problem is that without establishing a hypothesis, conducting a particular test is impossible because the body including specialized inference procedure can only be accessed when the invocation expression is evaluated to true. Another problem with procedural fault diagnosis is that it cannot learn diagnosis strategies. We found it useful to define the processes as a sequence of qualitative variables related by qualitative operations in the

²In complex and dynamic systems with numerous components, a fault can be propagated to the other subsystems and reasoning within the subsystem might lead to intuitively right but ultimately wrong fault hypotheses (see [48]).

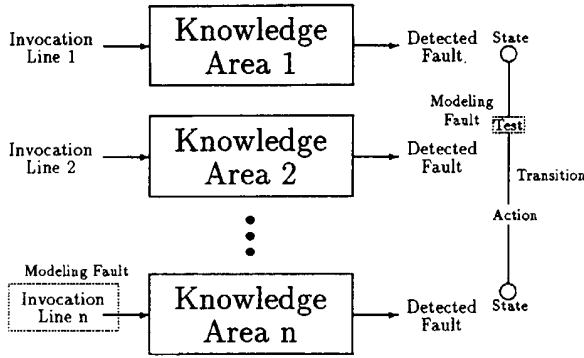


Fig. 3. Procedure-oriented approach to fault diagnosis.

- **Cognitive overload**
Decision making based on:
 - Large amount of data
 - Rapid changes of data
- **Information accessibility**
Data for decision making is to be inferred along causal chains.
- **Control directedness**
Initiating actions whose effects are propagated on causal chain to a target available
- **Counter-intuition**
Limitation in anticipating plant response due to:
 - Nonlinearities in anticipating plant response
 - Neglecting influence of overlapping processes
 - Long time delays in systems response

Fig. 4. Fundamental problems manifesting human performance in fault diagnosis.

deep level representation (see Section V), and we show that such representation (deep level) can produce the sequence of actions in another level of abstraction (compiled level). Also ambiguity between the invocation and test expressions is avoided.

C. Subjective Approach

Subjective approach describes and imitates the way that human performs fault diagnosis, with concentration on either imitating the behavior or achieving the same level of performance. Human performance in fault diagnosis degrades with the increase of the size of the plant and complexity of its behavior. Fig. 4 depicts some fundamental problems manifesting the performance [19].

The mental workload [61] (cognitive overload [48]) due to a large amount of monitored data, is the main limiting factor of the performance, leading to cognitive tunnelling and incorrect decisions. The control directness problem [34] arises when the effects of a correction action is propagated along the causal chains until reaching the target point on which the action cannot be direct. The information accessibility problem arises when the information needed to confirm a fault hypothesis is not directly accessible and must be inferred indirectly. Human

operators come up with diagnosis decisions by comparing observed behavior with the desired response. The counter intuition problem arises when the ability to anticipate the plant’s response is narrowed down by a number of factors, such as mutual influence of the overlapping processes, nonlinearities in the plant’s dynamics and long time delays in system response. Two ways of enhancing the performance are [38]:

- Utilizing conceptual models of the plant that allow detecting redundancies in system behavior and predict the future states
- Utilizing efficient information selection and transformation tools to avoid cognitive (computation) overload.

Some symptomatic fault diagnosis systems, coding human experts’ knowledge, are the first generation of subjective systems. However, they apparently come short when trying to achieve the human’s performance level. Systems including models of human behavior [3], [10] have been appeared. Categories of fault detection, diagnosis and correction from the S-R-K perspective are defined [37], indicating a need for more powerful knowledge-based level fault detection and diagnosis techniques.

In SQFD we focus on knowledge and rule-based levels of the S-R-K, and show that the control directness and information accessibility problems can be removed by using the qualitative deep model and qualitative interpretation of sensory data. Decomposing the deep model removes problems with the overlapping processes. Finally, the qualitative nature of the model is a way of dealing with nonlinearities in plant dynamics.

Most of the existing researches have been concentrated on systems related to only one of the S-R-K levels [37] with some exceptions, such as integrated diagnostic model (IDM) [22]. SQFD is different from IDM in the sense that the passive component of knowledge (i.e., compiled model) is generated directly from the deep qualitative model and the deep level representation is semantically richer.

IV. SQFD: SUBJECTIVE QUALITATIVE FAULT DIAGNOSIS

SQFD embodies a hierarchy of two interacting fault diagnosis techniques: *deep* for the knowledge-based level and *compiled* for the rule-based level of the R-S-K (see Fig. 5).

The techniques are explained with a simplified plant, shown in Fig. 6. In this plant, liquids can be pumped from one tank to the other due to the pressure differences and proper setting of the control valves, CV_1-CV_6 . The valves are controlled by local feedback loops. When an abnormality in behavior is observed, the fault diagnosis system is responsible for finding discrepancies between the normal and abnormal behaviors and deciding upon corrections.

A. Knowledge-Based Level

Model of the normal system is a digraph called qualitative deep model (QDM). QDM embodies qualitative processes (QP). Behavioral fragments (BF) are defined as characteristic behavior of the QP’s. Behavior of the normal system is the set of BF’s and derived from QDM by qualitative simulation. Most of the problems in process malfunction are caused by failure

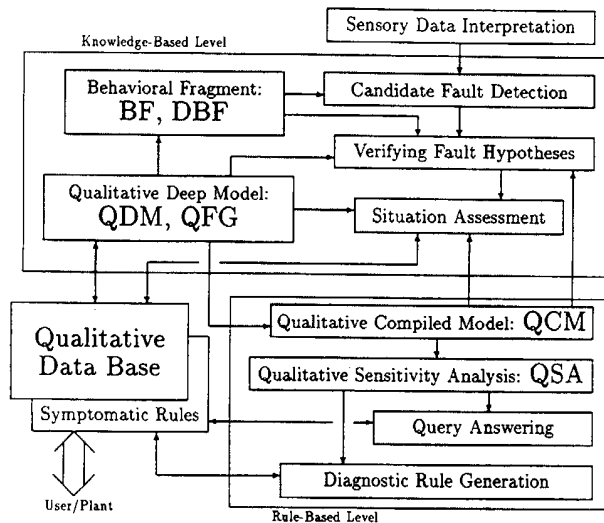


Fig. 5. Subjective qualitative fault diagnosis (SQFD) system.

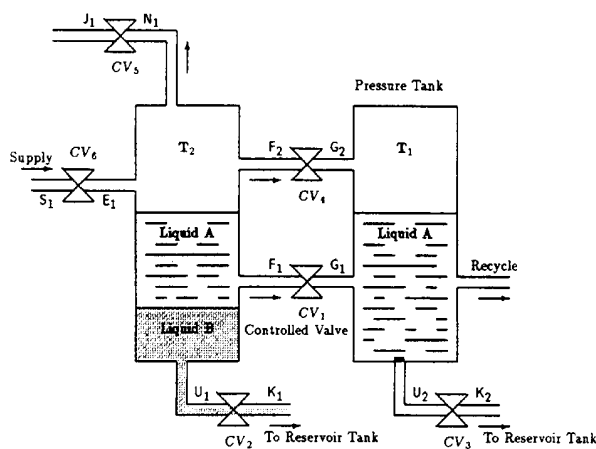


Fig. 6. Double pressure tank system.

of the control and instrumentation components (e.g., leaking a valve). Such components have a defined set of potential failure modes [22], [26], called failure modes of system components, Ψ . Faults, addressing failure modes are modeled by *dependency constraints*, which are the antecedents of the conditional arcs of QDM. From QDM and Ψ one can derive diversified behavioral fragments (DBFs), a set of behaviors of the malfunctioning system, different from BFs. Observed behavioral information, $\hat{\Theta}$, is provided by the sensors and interpreted qualitatively [24]. The problem is finding whether $\hat{\Theta}$ is similar to either BFs or DBFs, and soliciting candidate faults. If $\hat{\Theta}$ is qualitatively *similar* to one of the behaviors of the BF set, it can be a possible behavior of the normal system. On the other hand, if it is similar to a behavior of the DBF set, it can be a possible behavior of the faulty system and the invocation part of the fault arc is the causes of malfunctioning.

In this level, behavioral information are recorded for the qualitative variables. Sensory data is also recorded and qualitatively interpreted for the variables, therefore comparison of an observed behavior with a recorded normal or perturbed behavior is reduced to comparing a limited number of landmark values and dependency constraints for the two behaviors, resulting less computation overload (see Section V).

B. Rule-Based Level

Qualitative compiled model (QCM) of the normal system and a set of components' malfunctions, Ψ , are given. QCM embodies rules describing processes activated by the normal system. Each rule is composed of antecedent and consequent propositions. Ψ involves propositions addressing failure modes of the components. The set of predicted behaviors, Γ_c , is derived from QCM using causal ordering (CO) technique [36]. CO derives ordering among the propositions for a given set of initial settings treated as facts. The elements of Ψ are treated as new hypotheses and from QCM and Ψ one can derive another set of behaviors of the faulty system, $\tilde{\Gamma}_c$, different from Γ_c . Qualitative sensitivity analysis (QSA) technique checks the sensitivity of behavior to faults and preserves the results in the form of a diagnostic rule [16].

C. Hierarchy of Knowledge- and Rule-Based Levels

A hierarchy of knowledge- and rule-based levels can offer substantial advantage over a single one. A basic feature of this technique is that first, QCM is extracted from the QDM and then diagnostic rules are generated from QCM. Generated diagnostic rules are different from the heuristic rules, in the so called *symptomatic* (experience based) fault diagnosis, in the sense that they have an underpinning model, being more accurate and reliable than heuristic rules. Such diagnostic rules can be used in an ordinary symptomatic expert diagnosis system. Generating and validating concurrent fault hypotheses and assessment of situation are additional features of the hierarchical system.

V. KNOWLEDGE-BASED QUALITATIVE MODELING AND REASONING

The knowledge-based level allows reasoning from the interaction of the variables at the process level. Some concepts such as qualitative deep model (QDM), qualitative flow graph (QFG), qualitative process (QP), behavioral fragment (BF) and diversified behavioral fragment (DBF), are defined. They lead to an insightful understanding of the system's behavior and functions.

A. Qualitative Deep Model

QDM is composed of a set of expressions involving three primitives: *qualitative variables* and two types of *qualitative operations*. Qualitative variables are counterpart of physical quantities, such as temperature and pressure, representing characteristics of the system's inner environment. Variables are measurable and have a defined domain of variation. A qualitative variable (shown by $[X], [Y]$, etc.) has a finite ordered set of paired landmark values and distinguished time points. They are displayed in the form of a graph or a finite sequence of pairs (L^k, T^k) ,

$$(L_X^0, T_X^0), (L_X^1, T_X^1), \dots, (L_X^n, T_X^n) \quad (1)$$

where L_X^k and T_X^k are the k th landmark value and distinguished time point of variable $[X]$.

TABLE I
CLOCK AND DEPENDENCY CONSTRAINTS FOR EXTENDED
QUALITATIVE EXPRESSIONS ^a

QDM Expression	Clock Constraint	Dependency Constraint
$[Y] = O[X] \pm O[Z]$	$y^2 = x^2 = z^2$	$y^2: [X] \rightarrow O \rightarrow [Y]$
$y^2: [Z] \rightarrow O \rightarrow [Y]$ “when” (L_N^i)	$y^2 = x^2(-n - n^2)$	$y^2: [X] \rightarrow O \rightarrow [Y]$
$[Y] = O[X]$ “default” ($O[Z]$)	$y^2 = x^2 + z^2(1 - x^2)$	$x^2: [X] \rightarrow O \rightarrow [Y]$ $z^2(1 - x^2): [Z] \rightarrow O \rightarrow [Y]$

^a X, Y, Z , and N are qualitative variables. x, y, z , and n are their mod-3 values ($-1, 0, +1$), respectively. L_N^i is the i th landmark value of the variable N .

Relation between the qualitative variables is defined by qualitative operations. There are two types of operations: *ordinary* and *coordinative*. Ordinary operations show a *functionality* or an *influence* on a qualitative variable. The functions are monotonic increase (M^+) and monotonic decrease (M^-) [39]. Influence is a proportionality to the derivative of a qualitative variable. The influences are positive influence (I^+) and negative influence (I^-).

Coordinative operations model the protocol-based relations and timing. We have found them necessary because first, in many man-made systems the relation between components (and their corresponding models) are governed by defined protocols rather than pure physical laws. Secondly, coordinative operations depict the relative timing of qualitative variables and when they get to a new landmark value without necessarily recording all the distinguished time points.

Definition 1—(Qualitative Deep Model (QDM)): QDM is a set of expressions of the following form:

$$[Y] = O[X]D'[N]$$

where $[Y], [X]$ and $[N]$ are qualitative variables; O is an ordinary qualitative operation; $O \in \mathcal{O}$, $\mathcal{O} = \{M^+, M^-, I^+, I^-\}$; D is a coordinative operation (“when” and “default”):

- “when” operation: $[Y] = O[X]$ “when” L_N^i ; implying that $[Y] = O[X]$ only when $[N]$ is evaluated to its landmark value L_N^i .
- “default” operation: $[Y] = O[X]$ “default” $O[Z]$; implying that generally $[Y] = O[X]$, but in special cases that $[X]$ is not present, then $[Y] = O[Z]$.

Y, X and N are qualitative variables; L_N^i is the i th landmark value of N .

In special cases $[N]$ can be a variable with only two landmark values evaluated to *true* or *false*.

QDM for the system shown in Fig. 6 is given in Appendix I.

For each coordinative operation *clock* and *dependency* constraints are defined [5]. Clock and dependency constraints can only be evaluated to one of the following represented by mod-3 integers [5]:

- *present* (± 1): indicating that two events can occur concurrently;
- *absent* (0): indicating that two events cannot occur concurrently;
- *true* (+1): indicating that an event has occurred;
- *false* (−1): indicating that an event has not occurred.

Table I depicts the clock and dependency constraints for coordinative operations.

Faults are modeled by clock and dependency constraints and errors by landmark values of qualitative variables. Distinguishing between these two is necessary because naturally an error is measurable, but a fault is not. Errors, such as low pressure in tanks, etc., are derived by limit and trend analysis of the variables, to which a sensor can be attached. However, a fault, such as clogging or leaking a valve, cannot be measured directly and can only be manifested through other measurable variables (see Footnote 1).

B. Qualitative Flow Graph

QDM cannot show explicitly indirect influences of variables and how perturbation can be propagated through the model. For such cases graph representation has been found useful [72]. Formally, we define qualitative flow graph (QFG) as a digraph embodying the QDM expressions and the notion of fault. In QFG, nodes are qualitative variables and arcs are conditional ordinary qualitative operations, whose antecedents are dependency constraints.

Definition 2—(Qualitative Flow Graph): QFG is a digraph represented by four sets:

$$QFG = \{\mathcal{V}, \mathcal{A}, \mathcal{O}, \mathcal{C}\}$$

where \mathcal{V} is a set of nodes standing for the qualitative variables; \mathcal{A} is a set of arcs relating the two nodes; \mathcal{O} is a set of ordinary qualitative operations; \mathcal{C} is a set of dependency constraints for coordinative qualitative operations given in Table I.

All the arcs of the QFG are conditional. A conditional arc is

$$A : C \rightarrow O.$$

For each arc, $A \in \mathcal{A}$, if for $C \in \mathcal{C}$, $\mathcal{E}(C) = 1$ holds, then $O \in \mathcal{O}$ is enabled, where $\mathcal{E}(C)$ is an evaluation of the constraint C .

QFG offers higher semantic richness than digraphs used in other fault diagnosis techniques (such as [72], [62], etc.) \mathcal{C} resembles the predicates and functions labeling the arcs of a recursive transition network (RTN) for the procedural knowledge [29]. \mathcal{O} and \mathcal{V} resemble the transitions and actions in RTN. But in QFG the way that the processes are activated and interact is dependent to the existing faults and governed by clock and dependency constraints. Thus QFG integrates the model of the normal system with the deviations due to faults. Another advantage of using QFG is its flexibility when coping with modifications, degradation and rearrangement of the system, as in such cases only some of the constraints are modified.

C. Qualitative Process

QFG is a network of overlapping qualitative processes. A qualitative process (QP) is a finite, connected, unidirectional string of arcs of QFG, relating an input node to an output one. An input node is the one with an in-degree-zero. Similarly, an output node is the one with an outdegree zero. Thus a process shows how qualitative variables can affect each other.³ Qualitative processes are extracted from the QFG by *decomposition*, i.e., assigning the shared nodes and arcs between two processes to both of them. There are 16 processes for the tank system given in Appendix I.

The notion of process has acquired different meanings in qualitative reasoning literature.⁴ A key point in fault diagnosis is distinguishing the effects of a fault on the network of the overlapping processes. By exploiting the conventional definition of process and qualitative simulation, a number of possible behaviors are generated and a one-to-one relation between a fault and a characteristic behavior of the system cannot be established. For the sake of removing the ambiguity in simulation, the network of overlapping processes is decomposed and the characteristic behavior for each process is derived. Then by applying faults one by one another set of faulty behavior is derived. Such behavioral information serve as the basis for detecting faults.

D. Behavioral Fragment

Behavioral fragment (BF) is the characteristic behavior of a process and is defined as the record of landmark values for the displayed⁵ qualitative variables belonging to that process.

Definition 3—(Behavioral Fragment): Behavioral fragment BF_{P_j} of a process P_j , is a finite sequence of landmark values (L_V^k) , of the form:

$$BF_{P_j} = \{\forall V \in P_j | (L_V^0, L_V^1, \dots, L_V^n)\} \quad (2)$$

$$BF_{P_j} = \left\{ \forall V \in P_j | \biguplus_{k=0}^n (L_V^k) \right\} \quad (3)$$

L_V^k is the k th landmark value of a displayed qualitative variable V ; and \biguplus is a symbol for abbreviating (2) to (3).

BFs are derived by qualitative simulation (QS) in two steps:

- Dependency constraint satisfaction on the arcs of the processes.
- Landmark value identification of the qualitative variables.

First, the simulator looks for the antecedents of the conditional arcs that can satisfy the given situation. Through clock and dependency analysis one can verify which of the arcs of the processes are activated and can take part in simulation. Then processes whose enabling conditions of their arcs are not yet satisfied are deleted. On the next step, a conventional

³ Similar to the definition of process in system engineering, cf. [35].

⁴ Weld has defined continuous and discrete processes by two sets of preconditions and influences [68]. Preconditions govern when the process can be active and influences show how various quantities are modified through an active process. In Forbus' terms a qualitative process is specified by five parts: individuals, preconditions, quantity conditions, relations and influences [23].

⁵ i.e., those variables considered important to be tracked or recorded.

simulation program derives landmark values for each variable of the remaining processes.

For the processes of the tank example, and for the displayed qualitative variables the BFs are given in Appendix I.

E. Qualitative Observed Behavior

An observed behavior for a qualitative variable V is read by the sensors and is interpreted qualitatively as a finite sequence of pairs (L_V^k, T_V^k) , having the form given in (1) [24].

Assumption 1: For a set of qualitative processes \mathcal{P} , every observed behavior $\hat{\Theta}$, is associated with a subset of processes $\hat{\mathcal{P}}$, i.e., $\hat{\Theta}$ can be derived by qualitative simulation on the $\hat{\mathcal{P}}$.

As stated before, faults are modeled by the antecedents of the conditional arcs of the processes. We define here the relation between the observed behavior and the *fault arcs*.

Definition 4—(Fault Arc): For an observed behavior, $\hat{\Theta}$, associated with $\hat{\mathcal{P}}$, a fault arc is the one whose dependency constraint is evaluated to a different value than that of the processes \mathcal{P} . For c_F and $O \in \mathcal{O}$,

$$FA = \{\exists j, a_F: (c_F \rightarrow O) | \mathcal{E}(c_F)_{P_j} \neq \mathcal{E}(c_F)_{\hat{P}_j}\}$$

where $\mathcal{E}(c_F)_{P_j}$ and $\mathcal{E}(c_F)_{\hat{P}_j}$ are evaluations of the constraint c_F for the process P_j and \hat{P}_j , respectively.

FA is the set of fault arcs. P_j and \hat{P}_j are processes belonging to the \mathcal{P} and $\hat{\mathcal{P}}$, respectively. For each $a_F \in FA$, c_F addresses a fault.

F. Diversified Behavioral Fragment

The deviations from the behavior of the normal system, i.e., characteristic behaviors of the faulty system are defined by the diversified fragments (DBF). DBFs reflect the effect of propagation of a fault in a set of processes. Similar to BFs, DBFs are also derived by qualitative simulation when applying the conditional arcs one by one.

Definition 5—(Diversified Behavioral Fragment): Diversified behavioral fragment for the process P_j is

$$\exists c_F, \forall V \in P_j, \quad DBF(c_F)_{P_j} = \left\{ \biguplus_{k=0}^n L_V^k(c_F) \right\}$$

where V is a displayed qualitative variable and c_F is a fault arc.

DBFs for the pressure tank system are given in Appendix I.

C. Detecting Candidate Faults

Candidate faults are detected by comparing the observed behaviors with the BFs (behaviors of the normal system) and DBFs (behaviors including a fault), using *similarity* concept, defined qualitatively below.

Definition 6—(Similarity): For a qualitative variable V belonging to a process P_j , two different behaviors, $(\biguplus_{k=1}^n L_V^k)$ and $(\biguplus_{k=1}^n \tilde{L}_V^k)$ are called "similar" if, either

$$\forall k, L_V^k = \tilde{L}_V^k$$

or

$$\forall k, \partial L_V^k > 0 \rightarrow \partial \tilde{L}_V^k > 0$$

$$\forall k, \partial L_V^k < 0 \rightarrow \partial \tilde{L}_V^k < 0$$

$$\forall k, \partial L_V^k = 0 \rightarrow \partial \tilde{L}_V^k = 0.$$

The ∂L_V^k indicates the direction of change between the two neighboring landmark values.

Lemma 1 (Candidate Fault Detection): For an observed behavior $\tilde{\Theta}$ of a qualitative variable V ,

- For each process P_j , where $V \in P_j$, compare $\tilde{\Theta}$ with the portion of the $BF_{P_j}(V)$ for the qualitative variable V .
- If the $BF_{P_j}(V)$ and $\tilde{\Theta}$ are similar, conclude that $\tilde{\Theta}$ is a possible behavior of the normal system, or the fault is undetectable.
- Otherwise, for each process P_j , compare $\tilde{\Theta}$ with the $DBFs$ of the qualitative variable V .
- If a DBF is similar to $\tilde{\Theta}$, the fault arc c_F of the $DBF(c_F)_{P_j}$ embodies the fault.

Let's consider two cases of an observed behavior (4): no change (Case 1.1) and decrease (Case 1.2) of the liquid level in tank T_2 (Fig. 6). Such behaviors are interpreted qualitatively, by the expressions (5) and (6), respectively.

$$\tilde{\Theta}_1 = \{H_{T_2} | \tilde{L}_{HT_2}^1, \tilde{L}_{HT_2}^2\} \quad (4)$$

$$\text{Case 1.1: } \tilde{L}_{HT_2}^2 = \tilde{L}_{HT_2}^1 \quad (5)$$

$$\text{Case 1.2: } \tilde{L}_{HT_2}^2 < \tilde{L}_{HT_2}^1 \quad (6)$$

Applying Lemma 1 and comparing with the BFs in Appendix I shows that BF_{P_4} and BF_{P_7} are similar to (6), indicating that it can be a possible behavior of the normal system. Equation (5) is not similar to any of the BFs. Comparing (5) with the $DBFs$ in Appendix I, recorded for the variable H_{T_2} , shows that three similar behaviors exist: $DBF(\omega_{CV_1}^2 = 0)_{P_4}$, $DBF(\omega_{CV_2}^2 = 0)_{P_7}$, and $DBF(\omega_{CV_6}^2 = 0)_{P_9}$. Fault arcs for the affected process are possible single candidate faults:⁶

$$(\omega_{CV_1}^2 = 0: \text{ CV}_1 \text{ clogged})$$

$$(\omega_{CV_2}^2 = 0: \text{ CV}_2 \text{ clogged})$$

and

$$(\omega_{CV_6}^2 = 0: \text{ CV}_6 \text{ clogged}).$$

Candidate fault set for each case is given as follows.

$$\text{Case 1.1: } (\tilde{L}_{HT_2}^2 = \tilde{L}_{HT_2}^1) \rightarrow \{(\omega_{CV_1}^2 = 0), (\omega_{CV_2}^2 = 0), (\omega_{CV_6}^2 = 0)\}$$

As another example, observed behavior can be recorded for a number of displayed variables rather than only one. For instance, let us consider the case that the pressure in T_2 is

⁶Note that ω_{CV_i} is a mod-3 integer but Ω_{CV_i} indicates a qualitative state variable of the valve CV_i .

steady and there is no flow of air from T_2 to T_1 , or in qualitative terms:

$$\tilde{\Theta}_2 = \{(A_{\text{out}/T_2} = 0), (P_{T_2} = P_{T_2}^o)\}.$$

Comparing $\tilde{\Theta}_2$ with the BFs indicates that this cannot be a possible normal behavior. Comparison with the $DBFs$ shows two similar cases, $DBF(\omega_{CV_4}^2 = 0)_{P_{12}}$ and $DBF(\omega_{CV_4}^2 = 0)_{P_{13}}$, as well as $DBF(\omega_{CV_5}^2 = 0)_{P_{14}}$ and $DBF(\omega_{CV_5}^2 = 0)_{P_{15}}$.

$$\text{Case 2.1: } (A_{\text{out}/T_2} = 0) \rightarrow \{(\omega_{CV_4}^2 = 0), (\omega_{CV_5}^2 = 0)\}$$

$$\text{Case 2.2: } (P_{T_2} = P_{T_2}^o) \rightarrow \{(\omega_{CV_4}^2 = 0), (\omega_{CV_5}^2 = 0)\}.$$

A fault hypothesis is a subset of candidate faults. Below we introduce a method for validating such hypotheses.

VI. VALIDATING CONCURRENT FAULT HYPOTHESES

A fault hypothesis is any combination of the candidate faults. In experts system literature, the Dempster-Shafer (DS) theory of evidence has been applied to verify the hypotheses [32], [33], [71]. However, DS-based methods are useful in situations where the elements comprising the hypotheses are mutually exclusive, and the hypothesis set can be narrowed down by accumulation of evidences. In concurrent fault case the mutual exclusiveness condition may not hold and the validation problem for each observed behavior is selecting a subset of candidate faults that if occurred simultaneously, could produce the observed behavior.

For each qualitative process, there exists a relation holding between a candidate fault and a landmark value of an output (or displayed) variable of that process, derived from $DBFs$. For instance, for the process P_4 and for the candidate fault (CV_1 clogged), the following relation holds (provided that it is the only fault):

$$(\omega_{CV_1}^2 = 0) \rightarrow (H_{T_2} = H_{T_2}^o).$$

The following proposition indicates how such relations can be used to verify a fault hypothesis.

Proposition 1—(Validating Fault Hypotheses-1): For a hypothesis composed of a number of concurrent candidate faults and for the processes embodying those faults, if the union of the range of variation of an output or displayed variable is identical to that of the observed behavior for that variable, the fault hypothesis can be considered valid.

The proof is straightforward: for each variable, each process is responsible for a portion of the behavior, given in terms of landmark values and ranges between the neighboring landmark values, and their union is the possible range of variation if such a behavior is identical to the observed one. Therefore one can derive that all those faults whose effects lead to such behavior actually exist. Let's test the validity of the fault hypotheses for the candidate faults derived in Section V-C. For the Case 1.1, there are three processes active: P_4 , P_7 and P_9 . Test result of the combinatorial faults is given in Table II. For instance, \mathcal{H}_1 is valid. Hypotheses \mathcal{H}_3 , \mathcal{H}_4 and

TABLE II
TEST RESULTS FOR FAULT HYPOTHESES OF CASE 1.1

$\mathcal{H}_1: (\omega_{CV_1}^2 = 0) \wedge (\omega_{CV_2}^2 = 0) \wedge (\omega_{CV_6}^2 = 0)$ Test: $[H_{T_2} = H_{T_2}^o]$	(level maintained)
$\mathcal{H}_2: (\omega_{CV_1}^2 = 0) \wedge (\omega_{CV_2}^2 = 0) \wedge (\omega_{CV_6}^2 = 1)$ Test: $[H_{T_2}^o \leq H_{T_2} \leq H_{(T_2)\max}]$	(level increased)
$\mathcal{H}_3: (\omega_{CV_1}^2 = 0) \wedge (\omega_{CV_2}^2 = 1) \wedge (\omega_{CV_6}^2 = 0)$ Test: $[H_{(T_2)\min} \leq H_{T_2} \leq H_{T_2}^o]$	(level decreased)
$\mathcal{H}_4: (\omega_{CV_1}^2 = 1) \wedge (\omega_{CV_2}^2 = 0) \wedge (\omega_{CV_6}^2 = 0)$ Test: $[H_{(T_2)\min} \leq H_{T_2} \leq H_{T_2}^o]$	(level decreased)
$\mathcal{H}_5: (\omega_{CV_1}^2 = 0) \wedge (\omega_{CV_2}^2 = 1) \wedge (\omega_{CV_6}^2 = 1)$ Test: $[H_{(T_2)\min} \leq H_{T_2} \leq H_{(T_2)\max}]$	(level controllable)
$\mathcal{H}_6: (\omega_{CV_1}^2 = 1) \wedge (\omega_{CV_2}^2 = 0) \wedge (\omega_{CV_6}^2 = 1)$ Test: $[H_{(T_2)\min} \leq H_{T_2} \leq H_{(T_2)\max}]$	(level controllable)
$\mathcal{H}_7: (\omega_{CV_1}^2 = 1) \wedge (\omega_{CV_2}^2 = 1) \wedge (\omega_{CV_6}^2 = 0)$ Test: $[H_{(T_2)\min} \leq H_{T_2} \leq H_{T_2}^o]$	(level decreased)

\mathcal{H}_7 are not valid because the ultimate level of material in T_2 decreases which is in contradiction with the observed behavior (5). Similarly, \mathcal{H}_2 is not valid because the level increases. \mathcal{H}_5 and \mathcal{H}_6 are interesting cases in which H_{T_2} can have any value between the maximum and minimum allowable levels, i.e., H_{T_2} is *controllable*.

Definition 6—(Qualitative Controllability): A qualitative variable is controllable if the union of its ranges of variation for the processes it appears in covers the whole allowable range of variation of that variable.

Controllability, in qualitative terms, indicates whether a particular behavior can be achieved or not. It implies that a variable can have any behavior between the maximum and minimum range of variation. However, the problem of how the behavior is achievable (precise set points and fine regulation) cannot be answered.

Proposition 2—(Validating Fault Hypotheses-2): For a hypothesis composed of a number of concurrent candidate faults and for the processes embodying those faults, if the fault hypothesis leads to controllability of an output or displayed variable, that hypothesis is valid.

From Proposition 2 one can derive that \mathcal{H}_5 and \mathcal{H}_6 are also valid hypotheses. Note that \mathcal{H}_1 indicates that three concurrent faults may exist, but \mathcal{H}_5 and \mathcal{H}_6 may narrow them down to one, suggesting that either clogging CV_1 or CV_2 may be an acceptable explanation for the observed behavior of the Case 1.1.

For the case 2.1, the active processes are P_{12} and P_{15} . Test results are given in Table III. The only acceptable hypothesis is

$$\mathcal{H}_3: (\omega_{CV_4}^2 = 0) \wedge (\omega_{CV_5}^2 = 0).$$

This implies that CV_4 and CV_5 are both clogged.

For the case 2.2, the active processes are P_{13} and P_{14} . Test results are given in Table IV. Again either $(\omega_{CV_4}^2 = 0)$ or $(\omega_{CV_5}^2 = 0)$ cannot produce the observed behaviors if they are a single fault. But concurrent occurrence of them gives an acceptable explanation for both observed behaviors of the cases 2.1 and 2.2.

TABLE III
TEST RESULTS FOR FAULT HYPOTHESES OF CASE 2.1

$\mathcal{H}_1: (\omega_{CV_4}^2 = 0) \wedge (\omega_{CV_5}^2 = 1)$ Test: $[A_{out/T_2} \leq A_{(out/T_2)\max}]$	(flow increased)
$\mathcal{H}_2: (\omega_{CV_4}^2 = 10) \wedge (\omega_{CV_5}^2 = 0)$ Test: $[A_{out/T_2} \leq A_{(out/T_2)\max}]$	(flow increased)
$\mathcal{H}_3: (\omega_{CV_4}^2 = 0) \wedge (\omega_{CV_5}^2 = 0)$ Test: $[A_{out/T_2} = 0]$	(flow maintained)

TABLE IV
TEST RESULTS FOR FAULT HYPOTHESES OF CASE 2.2

$\mathcal{H}_1: (\omega_{CV_4}^2 = 0) \wedge (\omega_{CV_5}^2 = 1)$ Test: $[P_{(T_2)\min} \leq P_{T_2} \leq P_{T_2}^o]$	(pressure decreased)
$\mathcal{H}_2: (\omega_{CV_4}^2 = 1) \wedge (\omega_{CV_5}^2 = 0)$ Test: $[P_{(T_2)\min} \leq P_{T_2} \leq P_{T_2}^o]$	(pressure decreased)
$\mathcal{H}_3: (\omega_{CV_4}^2 = 0) \wedge (\omega_{CV_5}^2 = 0)$ Test: $[P_{T_2} = P_{T_2}^o]$	(pressure maintained)

VII. RULE-BASED QUALITATIVE MODELING AND REASONING

In this section methods for developing the qualitative compiled model (QCM), generating diagnostic rules, and model-based query answering are introduced. First, the qualitative processes are lumped and transformed to the QCM and then diagnostic rules are generated from the QCM by qualitative sensitivity analysis (QSA).

A. Qualitative Compiled Model

Qualitative compiled model (QCM) is the outcome of the goal seeking approach to modeling, in which the main principle of abstraction is identifying input/output relation between the modeling elements [41]. For each qualitative process two of the nodes are considerably important: the input node and the output node, standing for the input and output qualitative variables. Qualitative processes are lumped to a single arc ($A : C \rightarrow O$), that connects the input and output nodes. The antecedent C is derived by multiplying all the dependency constraints of the individual arcs of that process

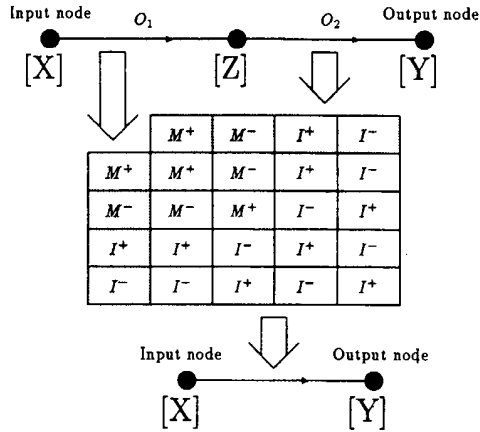


Fig. 7. Reduction rules for lumped processes.

and the consequence O reveals the overall relation holding between the two end nodes of the process by combining the intermediate qualitative operations using the reduction rules given in Fig. 7.

A lumped process depicts the relation between landmark values of the input and output qualitative variables. Intuitively, if the overall operation M^+ or M^- holds between two qualitative variables $[X]$ and $[Y]$, namely, $[Y] = M^+[X]$ or $[Y] = M^-[X]$, one can derive that increase of the value of X will result an increase (or decrease) in Y , or on the other hand, steady X will produce steady Y . Therefore, a landmark value of $[X]$ is related to a landmark value of $[Y]$. In case of I^+ (or I^-), a steady X will produce a monotonically increasing (decreasing) Y , therefore there is a mapping from a landmark value of one to an interval bounded by two neighboring landmark values of the other. These are saved as single antecedent/single consequence *crude causal rules* in the ρ_{cc} set.

The relation between the antecedent and consequent of the crude causal rules denotes sufficient conditionality, i.e., validity of antecedent implies validity of consequence. The negative rules are assumed to be valid. However, there is no strict implication, i.e., validity of a consequence does not necessarily lead to the validity of its antecedent [8]. Therefore ρ_{cc} set includes both the causal rules as the result of lumping processes and their negations. Then antecedents of the crude rules having the same consequence are conjoined to form a *combinatorial rule*. ρ_{com} is the set of combinatorial rules, accounting for the overlapping processes. QCM is the union of the ρ_{cc} and ρ_{com} .

$$QCM = \rho_{cc} \cup \rho_{com}$$

Each QCM rule has the form,

$$\mathcal{R}: (p_i \wedge p_j \wedge \dots \rightarrow p_k)$$

where (\wedge) is the logical connective “and,” and p_i, p_j and p_k are the antecedent and consequence propositions, addressing either a landmark value or an interval bounded by two neighboring landmark values of a qualitative variable. QCM rules for the pressure tank system are given in Appendix II.

B. Qualitative Sensitivity Analysis

It is a fundamental assumption that human being has a preference for reasoning based on state information [56]. States of the QCM are given by complete subsets of propositions that embody the true propositions according to the order of truth propagation. The causal ordering (CO) technique [36] can derive the complete subsets for a given set of initial facts and hypotheses. All the propositions belonging to a complete subset possess the same ordering rank (r). The normal behavior of the system is the sequence of states ordered according to the increasing rank.

Sensitivity is a factor demonstrating the relevance of the effects of perturbation on the QCM. Perturbation is defined qualitatively in terms of an external event forcing a landmark value of a qualitative variable shift to its neighboring ones. For example, in the case of CV_1 and CV_3 closed, a leak from either valves makes the $H_{T_1}^o$ shift toward either $H_{(T_1)\max}$ or $H_{(T_1)\min}$. QSA is a technique to detect possible effects of such landmark shift on the other variables. QSA can derive sensitivity of the higher rank landmarks, due to perturbation affecting the lower rank ones [18].

Definition 7—(Qualitative Sensitivity): Let L_U^i and L_U^{i+1} be two neighboring landmark values of a qualitative variable U . Let L_V^j and L_V^{j+1} be the two neighboring landmark values of another qualitative variable V . Suppose that perturbation is introduced to L_V^j , causing L_V^j to shift to L_V^{j+1} . Then L_U^i is called sensitive to such perturbation, if L_V^j is an antecedent for L_U^i , in a causally ordered network, and if L_U^{i+1} happens to have the same rank with the L_U^i on the same network. This is shown by:

$$(L_U^i, L_U^{i+1}) \aleph (L_V^j, L_V^{j+1}) \quad (7)$$

where (\aleph) is the symbol denoting the qualitative sensitivity.

Lemma 2—(Qualitative Sensitivity Analysis): Qualitative sensitivity analysis is carried out as follows:

- Derive complete subsets by the causal ordering (CO) for the union of the initial fact and hypothesis sets, $\mathcal{F} \cup \mathcal{H}$.
- Treat each new perturbation as a new hypothesis and derive the perturbed complete subsets for the new set of facts and hypotheses, by CO.
- Check the complete subsets for the existence of the landmark values of a variable having the same rank.

For the pressure tank system the initial fact set, indicating the order of opening the control valves, is

$$\mathcal{F} = \{(\Omega_{CV_1} > 0), (\Omega_{CV_4} > 0), (\Omega_{CV_5} = 0), (\Omega_{CV_2} > 0), (\Omega_{CV_3} > 0), (\Omega_{CV_6} > 0)\}. \quad (8)$$

The hypothesis set, \mathcal{H} , is composed of some assumptions such as the initial pressure in the tank T_2 is higher than T_1 .

$$\mathcal{H} = \{(P_{T_2}^o > P_{T_1}^o)\}.$$

For the QCM given in Appendix II, and for the aforementioned fact and hypothesis sets the complete subsets are

derived:

$$\begin{aligned}
(r = 1) &\Rightarrow \{(\Omega_{CV_1} > 0), (\Omega_{CV_4} > 0), (\Omega_{CV_5} = 0), \\
&\quad (\Omega_{CV_2} > 0), (\Omega_{CV_3} > 0), \\
&\quad (\Omega_{CV_6} > 0), (P_{T_2}^o > P_{T_1}^o)\} \\
(r = 2) &\Rightarrow \{(U_1 > 0), (U_2 > 0), (J_1 = 0), \\
&\quad (0 < F_{out/T_2} \leq F_{out/T_2}^{max}), \\
&\quad (P_{T_1}^o < P_{T_1} \leq P_{(T_1)max}), \\
&\quad (0 < A_{in/T_1} \leq A_{in/T_1}^{max})\}.
\end{aligned}$$

Suppose that perturbation is introduced to the proposition $(\Omega_{CV_4} > 0)$. The neighboring landmark, that is $(\Omega_{CV_4} = 0)$, is treated as a new hypothesis, added to the $\mathcal{F} \cup \mathcal{H}$. Causal ordering derives the new ordering for the new $\mathcal{F} \cup \mathcal{H}$:

$$\begin{aligned}
(r = 1) &\Rightarrow \{(\Omega_{CV_1} > 0), (\Omega_{CV_4} > 0), \\
&\quad (\Omega_{CV_4} = 0), (\Omega_{CV_5} > 0), \\
&\quad (\Omega_{CV_2} > 0), (\Omega_{CV_3} > 0), \\
&\quad (\Omega_{CV_6} > 0), (P_{T_2}^o > P_{T_1}^o)\} \\
(r = 2) &\Rightarrow \{(0 < F_{out/T_2} \leq F_{out/T_2}^{max}), \\
&\quad (P_{T_1}^o < P_{T_1} \leq P_{(T_1)max}), \\
&\quad (P_{(T_1)min} \leq P_{T_1} < P_{T_1}^o), \\
&\quad (0 < A_{in/T_1} \leq A_{in/T_1}^{max}), (A_{out/T_2} = 0), \\
&\quad (P_{T_2}^o < P_{T_2} \leq P_{(T_2)max}), (A_{in/T_1} = 0), \\
&\quad (J_1 = 0), (U_2 > 0), (U_1 > 0)\}.
\end{aligned}$$

In this case the landmark values of the variables A_{in/T_1} and P_{T_1} appear to have the same rank, therefore according to Definition 7, they are sensitive to perturbation introduced to $(\Omega_{CV_4} > 0)$,

$$\begin{aligned}
&[(A_{in/T_1} = 0), (0 < A_{in/T_1} \leq A_{in/T_1}^{max})] \\
&\quad \mathfrak{N}[(\Omega_{CV_4} > 0), (\Omega_{CV_4} = 0)] \quad (9)
\end{aligned}$$

$$\begin{aligned}
&[(P_{(T_1)min} \leq P_{T_1} < P_{T_1}^o), (P_{T_1}^o < P_{T_1} \leq P_{(T_1)max})] \\
&\quad \mathfrak{N}[(\Omega_{CV_4} > 0), (\Omega_{CV_4} = 0)]. \quad (10)
\end{aligned}$$

C. Diagnosis Rule Generation

Diagnostic rules are empirical associations between an observed behavior and the possible faults [49]. QSA is applied to generate diagnosis rules. Suppose that p , q , r , and s are the corresponding propositions for the landmark values L_U^i, L_U^{i+1}, L_V^j , and L_V^{j+1} in (7), respectively. Let p and r represent a rule in the compiled model of the normal behavior. Then the other two propositions can depict a diagnostic rule in the sense that the cause of observing a malfunction (i.e., in this case shown by proposition q) is a perturbation in one of its direct or indirect antecedents (i.e., indirect cause is the proposition s in this case). The diagnostic rule is

$$q \leftarrow s$$

or in descriptive form: "If q is observed, its possible cause is s ."

Lemma 3—(Generating Diagnostic Rules): The diagnostic rules are generated as follows:

- Derive all the sensitive cases, for a given perturbation and record them in the form of (7).
- Replace the landmark values with the corresponding propositions for each sensitive case.
- Delete the propositions representing a relation in the QCM rules. Remaining propositions represent a diagnostic rule having the form of

$$(q_1 \vee q_2 \vee \dots \vee q_n) \leftarrow s$$

which implies that s is a possible cause of the accumulated evidences $(q_1 - q_n)$.

Applying Lemma 3 to (9)–(10) and deleting the originally related landmark values in them leads the following rule:

$$[0 = A_{in/T_1}] \vee [P_{(T_1)min} \leq P_{T_1} < P_{T_1}^o] \leftarrow [\Omega_{CV_4} = 0].$$

This can be interpreted as: "If the net pressure of the tank T_1 is reduced, check the flow of air into the tank. If the flow is halted, then deduce that the pressure valve CV_4 is possibly clogged."

D. The Query System

Sensitivity analysis can also be applied to give answer to "what ... if" questions. For the same system let's find the answer to the question: "What will happen if the pressure valves CV_4 is clogged while CV_5 is opened?" The propositions $(\Omega_{CV_4} = 0)$: " CV_4 is clogged" and $(\Omega_{CV_5} > 0)$: " CV_5 is opened" are treated as a new hypothesis and the causal ordering derives the new ordering.

$$\begin{aligned}
\mathcal{F} \cup \mathcal{H} &= \{(\Omega_{CV_1} > 0), (\Omega_{CV_4} > 0), (\Omega_{CV_4} = 0), \\
&\quad (\Omega_{CV_5} > 0), (\Omega_{CV_5} > 0), (\Omega_{CV_2} > 0), \\
&\quad (\Omega_{CV_3} > 0), (\Omega_{CV_6} > 0), (P_{T_2}^o > P_{T_1}^o)\}. \quad (11)
\end{aligned}$$

Complete subsets including perturbation are

$$\begin{aligned}
(r = 1) &\Rightarrow \{\mathcal{F} \cup \mathcal{H}\} \\
(r = 2) &\Rightarrow \{(0 < F_{out/T_2} < F_{out/T_2}^{max}), (U_1 > 0), \\
&\quad (U_2 > 0), (P_{(T_1)min} \leq P_{T_1} < P_{T_1}^o), \\
&\quad (P_{T_1}^o < P_{T_1} \leq P_{(T_1)max}), (A_{in/T_1} = 0), \\
&\quad (0 < A_{in/T_1} \leq A_{in/T_1}^{max}), (J_1 = 0), \\
&\quad (0 < A_{out/T_2} \leq A_{out/T_2}^{max}), (J_1 > 0), \\
&\quad (A_{out/T_2} = 0), (P_{T_2}^o < P_{T_2} \leq P_{(T_2)max}), \\
&\quad (P_{(T_2)min} \leq P_{T_2} < P_{T_2}^o)\}.
\end{aligned}$$

Sensitive cases are

$$\begin{aligned}
 & [(A_{in/T_1} = 0), (0 < A_{in/T_1} \leq A_{(in/T_1)max})] \mathcal{N} \\
 & \quad [(\Omega_{CV_4} = 0), (\Omega_{CV_4} > 0)] \wedge [(\Omega_{CV_5} = 0), (\Omega_{CV_5} > 0)] \\
 & [(P_{(T_1)min} \leq P_{T_1} < P_{T_1}^o), (P_{T_1}^o < P_{T_1} \leq P_{(T_1)max})] \mathcal{N} \\
 & \quad [(\Omega_{CV_4} = 0), (\Omega_{CV_4} > 0)] \wedge [(\Omega_{CV_5} = 0), (\Omega_{CV_5} > 0)] \\
 & [(A_{out/T_2} = 0), (0 < A_{out/T_2} \leq A_{(out/T_2)max})] \mathcal{N} \\
 & \quad [(\Omega_{CV_4} = 0), (\Omega_{CV_4} > 0)] \wedge [(\Omega_{CV_5} = 0), (\Omega_{CV_5} > 0)] \\
 & [(P_{(T_2)min} \leq P_{T_2} < P_{T_2}^o), (P_{T_2}^o < P_{T_2} \leq P_{(T_2)max})] \mathcal{N} \\
 & \quad [(\Omega_{CV_4} = 0), (\Omega_{CV_4} > 0)] \wedge [(\Omega_{CV_5} = 0), (\Omega_{CV_5} > 0)] \\
 & [(J_1 = 0), (J_1 > 0)] \mathcal{N} \\
 & \quad [(\Omega_{CV_4} = 0), (\Omega_{CV_4} > 0)] \wedge [(\Omega_{CV_5} = 0), (\Omega_{CV_5} > 0)].
 \end{aligned}$$

Applying Lemma 3 derives the following rule:

$$\left\{ \begin{array}{l} (A_{in/T_1} = 0) \\ (P_{(T_1)min} \leq P_{T_1} < P_{T_1}^o) \\ (P_{T_2}^o < P_{T_2} \leq P_{(T_2)max}) \\ (A_{out/T_2} = 0) \\ (J_1 > 0) \end{array} \right\} \begin{array}{l} \vee \\ \vee \\ \vee \\ \vee \\ \vee \end{array} \leftarrow \{(\Omega_{CV_4} = 0 \wedge (\Omega_{CV_5} > 0))\}.$$

This is interpreted as: “Clogging of the pressure valve CV_4 while CV_5 is opened may possibly halt the flow of air out of T_2 and into T_1 , reduce the pressure of tank T_1 , increase of pressure of tank T_2 , and a flow of compressed air from T_2 to the reservoir tank.”

VIII. SITUATION ASSESSMENT

Situation assessment⁷ is verifying the current state of the world. During situation assessment, the existing data base of facts is evaluated against the valid fault hypotheses and updated.

It is assumed that the valid faults add to the data base of already existing facts. A set of facts is preserved and updated (similar to *STRIPS* [20] or *possible worlds* [30]). This is different from the ATMS-based diagnosis [15] in the sense that we start with a valid fault hypothesis. In assessment technique, the proposition addressing antecedents or consequences of QCM rules can be an element of the qualitative data base (QDB). Valid faults are treated as new hypotheses, \mathcal{H} , added to the initially given fact set, \mathcal{F} . Apparently, in the $\mathcal{F} \cup \mathcal{H}$ all the hypotheses must hold but some of the existing facts may not hold any more. Then a complete data base (in the formal logic sense) [13] is generated that satisfies the QCM rules, and has no contradiction with the hypotheses \mathcal{H} . The idea is preserving the existing facts as much as possible until the point that the inconsistency of the QDB by adding any of the facts can be proved [30]. A consistency checking algorithm compares the hypotheses with the already existing facts, \mathcal{F} , detects the facts that are in conflict with \mathcal{H} , removes them and saves the rest in the unchanged (NC) set. The union of QDB and NC is the new fact set, reflecting what has been affected

⁷This definition of situation assessment is different from that of Thorndyke, in which situation assessment was used as almost synonym to compiled model-based fault detection (see [65]).

by faults (QDB set) and what has not (NC set).

$$\mathcal{F} = QDB \cup NC.$$

Definition 8—(Complete QDB): The QDB is complete if having three properties:

- Facts in the QDB are not contradictory.
- Facts in the QDB satisfy the QCM rules.
- Adding any new fact to the QDB that violates a rule of QCM, also contradicts an existing fact in the data base.

The consistency algorithm checks if the negation of any proposition p of \mathcal{H} already exists in the fact set. If so, the $(\neg p)$ will be deleted from \mathcal{F} and the rest are saved in the NC set.

Let's consider a valid fault hypothesis for the example Case 1.1, such as:

$$\mathcal{H} = \{(\Omega_{CV_1} = 0), (\Omega_{CV_2} = 0), (\Omega_{CV_6} = 0)\}.$$

The fact set \mathcal{F} is given in (8). The complete data base satisfying QCM rules and Definition 8 is given as

$$\begin{aligned}
 QDB = \{ & (\Omega_{CV_1} = 0), (K_2 > 0), (P_{T_1}^o < P_{T_1} \leq P_{(T_1)max}), \\
 & (\Omega_{CV_2} = 0), (K_1 = 0), (H_{(T_1)min} \leq H_{T_1} < H_{T_1}^o), \\
 & (\Omega_{CV_6} = 0), (F_{out/T_2} = 0), \\
 & (0 < A_{in/T_1} \leq A_{(in/T_1)max}) \}.
 \end{aligned}$$

Consistency checking detects the conflicts between \mathcal{F} and \mathcal{H} :

$$NC = \{(\Omega_{CV_4} > 0), (\Omega_{CV_5} = 0), (\Omega_{CV_3} > 0), (P_{T_2}^o > P_{T_1}^o)\}.$$

where $QDB \cup NC$ reflects the current state of the world.

This updated data base can explain the outcome of fault propagation. For instance, the answer to the questions such as: “What happens to pressure in T_1 in Case 1.1?” is derived from the data base that includes: $(P_{T_1}^o < P_{T_1} \leq P_{(T_1)max}) \in QDB \cup NC$, indicating that the pressure will increase.

IX. CONCLUSION

The subjective qualitative fault diagnosis (SQFD) embodying the *deep* and *compiled* model-based techniques for detecting concurrent faults, diagnostic rule generation, query answering, generating and testing concurrent fault hypotheses and situation assessment was introduced. A hierarchy of the deep and compiled levels resembles the problem solving behavior of human experts in the S-R-K framework. SQFD can serve as a knowledge-based aiding system, managing to minimize the cognitive overload of the human operators by reducing the inferences that they have to make when diagnosing faults.

SQFD can detect most of the faults with short propagation time. After running a number of times on the same class of faults, the system becomes more efficient because it shifts automatically from the knowledge level to the skill level. However, a main problem is dealing with the long time lag in fault propagation: in some cases the effects of fault propagation in the network of overlapping processes can be observed after a long delay, even when the initial cause has already been removed. Detecting fault in those cases is an active research

work. Modeling propagation delays by the clock constraints of the extended qualitative model is currently under investigation.

APPENDIX I

QUALITATIVE DEEP MODEL OF THE PRESSURE TANK SYSTEM

A. Qualitative Deep Model

A controlled valve has a single state variable, Ω_{CV_i} , $\forall CV_i$, ($\Omega_{CV_i} > 0$): valve enabled; ($\Omega_{CV_i} = 0$): valve disabled;

Concerning the tanks, there is a uniform supply of material to T_2 through CV_6 . Pressure of T_2 is controlled by CV_4 and CV_5 . Overall level of the two phase material (material A and B) in T_2 is controlled by CV_1 and CV_2 . Pressure of T_1 is controlled by CV_4 . Level of the material in T_1 is controlled by CV_1 and CV_3 .

Qualitative variables are $F_1, G_1, U_1, K_1, U_2, K_2, F_2, G_2, J_1, N_1, S_1$, and E_1 , representing flow-in and flow-out for the controlled valves CV_1 – CV_6 , respectively; $\Omega_{CV_1}, \Omega_{CV_2}, \Omega_{CV_3}, \Omega_{CV_4}, \Omega_{CV_5}$, and Ω_{CV_6} are state variables of the valves; P_{T_2} and P_{T_1} are net pressure of T_2 and T_1 ; P_1 and P_2 are pressure losses of T_2 ; F_{in/T_2} and F_{in/T_1} are flow of material into T_2 and T_1 ; H_{T_2} and H_{T_1} are overall level of material in T_2 and T_1 ; H_{A/T_2} and H_{B/T_2} are level of material of type A and B in T_2 ; F_{out/T_2} and A_{out/T_2} are flow of material and air out of T_2 ; F_{T_1} and A_{in/T_1} are net flow of material and air into T_1 :

$$\begin{aligned}
[F_1] &= [G_1] = M^+[\Omega_{CV_1}] \text{ "when" } (\Omega_{CV_1} > 0) \\
[U_1] &= [K_1] = M^+[\Omega_{CV_2}] \text{ "when" } (\Omega_{CV_2} > 0) \\
[U_2] &= [K_2] = M^+[\Omega_{CV_3}] \text{ "when" } (\Omega_{CV_3} > 0) \\
[F_2] &= [G_2] = M^+[\Omega_{CV_4}] \text{ "when" } (\Omega_{CV_4} > 0) \\
[J_1] &= [N_1] = M^+[\Omega_{CV_5}] \text{ "when" } (\Omega_{CV_5} > 0) \\
[S_1] &= [E_1] = M^+[\Omega_{CV_6}] \text{ "when" } (\Omega_{CV_6} > 0) \\
[P_1] &= I^- [G_2] \text{ "when" } (\Omega_{CV_4} > 0) \\
[P_2] &= [I^- [N_1] \text{ "when" } (\Omega_{CV_5} > 0) \\
[F_{in/T_2}] &= M^+[E_1] \text{ "when" } (\Omega_{CV_6} > 0) \\
[H_{A/T_2}] &= I^- [G_1] \text{ "when" } (\Omega_{CV_1} > 0) \\
[H_{B/T_2}] &= I^- [U_1] \text{ "when" } (\Omega_{CV_2} > 0) \\
[P_{T_1}] &= I^+ [G_2] \text{ "when" } (\Omega_{CV_4} > 0) \\
[F_{in/T_1}] &= M^+[G_1] \text{ "when" } (\Omega_{CV_1} > 0) \\
[F_{out/T_1}] &= M^+[U_2] \text{ "when" } (\Omega_{CV_3} > 0) \\
[P_{T_2}] &= M^+[P_1] + M^+[P_2] \\
[H_{T_2}] &= M^+[H_{A/T_2}] + M^+[H_{B/T_2}] \\
[F_{T_1}] &= M^+[F_{in/T_1}] + M^- [F_{out/T_1}] \\
[F_{out/T_2}] &= I^+[U_1] + I^+[F_1] \\
[A_{out/T_2}] &= I^+[N_1] + I^+[F_2] \\
[H_{T_1}] &= I^+[F_{T_1}] \\
[H_{T_2}] &= I^+[F_{in/T_2}] \\
[A_{in/T_1}] &= I^+[G_2]
\end{aligned}$$

B. Clock Constraints

$$\begin{aligned}
f_1^2 &= g_1^2 = \omega_{CV_1}^2 (-\omega_{CV_1} - \omega_{CV_1}^2) \\
u_1^2 &= k_1^2 = \omega_{CV_2}^2 (-\omega_{CV_2} - \omega_{CV_2}^2) \\
u_2^2 &= k_2^2 = \omega_{CV_3}^2 (-\omega_{CV_3} - \omega_{CV_3}^2) \\
f_2^2 &= g_2^2 = \omega_{CV_4}^2 (-\omega_{CV_4} - \omega_{CV_4}^2) \\
j_1^2 &= n_1^2 = \omega_{CV_5}^2 (-\omega_{CV_5} - \omega_{CV_5}^2) \\
s_1^2 &= e_1^2 = \omega_{CV_6}^2 (-\omega_{CV_6} - \omega_{CV_6}^2) \\
p_1^2 &= g_2^2 (-\omega_{CV_4} - \omega_{CV_4}^2) \\
p_2^2 &= n_1^2 (-\omega_{CV_5} - \omega_{CV_5}^2) \\
f_{in/T_2}^2 &= e_1^2 (-\omega_{CV_6} - \omega_{CV_6}^2) \\
h_{A/T_2}^2 &= g_1^2 (-\omega_{CV_1} - \omega_{CV_1}^2) \\
h_{B/T_2}^2 &= u_1^2 (-\omega_{CV_2} - \omega_{CV_2}^2) \\
p_{T_1}^2 &= g_2^2 (-\omega_{CV_4} - \omega_{CV_4}^2) \\
f_{in/T_1}^2 &= g_1^2 (-\omega_{CV_1} - \omega_{CV_1}^2) \\
f_{out/T_1}^2 &= u_2^2 (-\omega_{CV_3} - \omega_{CV_3}^2) \\
p_{T_2}^2 &= p_1^2 = p_2^2 \\
h_{T_2}^2 &= h_{A/T_2}^2 = h_{B/T_2}^2 \\
f_{T_1}^2 &= f_{in/T_1}^2 = f_{out/T_1}^2 \\
f_{out/T_2}^2 &= u_1^2 = f_1^2 \\
a_{out/T_2}^2 &= n_1^2 = f_2^2 \\
h_{T_1}^2 &= f_{T_1}^2 \\
h_{T_2}^2 &= f_{in/T_2}^2 \\
a_{in/T_1}^2 &= g_2^2
\end{aligned}$$

C. Dependency Constraints

$$\begin{aligned}
\omega_{CV_1}^2: [\Omega_{CV_1}] &\rightarrow M^+ \rightarrow [G_1] \\
\omega_{CV_2}^2: [\Omega_{CV_2}] &\rightarrow M^+ \rightarrow [U_1] \\
\omega_{CV_3}^2: [\Omega_{CV_3}] &\rightarrow M^+ \rightarrow [U_2] \\
\omega_{CV_4}^2: [\Omega_{CV_4}] &\rightarrow M^+ \rightarrow [G_2] \\
\omega_{CV_5}^2: [\Omega_{CV_5}] &\rightarrow M^+ \rightarrow [N_1] \\
\omega_{CV_6}^2: [\Omega_{CV_6}] &\rightarrow M^+ \rightarrow [E_1] \\
\omega_{CV_4}^2 (-\omega_{CV_4} - \omega_{CV_4}^2): [G_2] &\rightarrow I^- \rightarrow [P_1] \\
\omega_{CV_5}^2 (-\omega_{CV_5} - \omega_{CV_5}^2): [N_1] &\rightarrow I^- \rightarrow [P_2] \\
\omega_{CV_6}^2 (-\omega_{CV_6} - \omega_{CV_6}^2): [E_1] &\rightarrow M^+ \rightarrow [F_{in/T_2}] \\
\omega_{CV_1}^2 (-\omega_{CV_1} - \omega_{CV_1}^2): [G_1] &\rightarrow I^- \rightarrow [H_{A/T_2}] \\
\omega_{CV_2}^2 (-\omega_{CV_2} - \omega_{CV_2}^2): [U_1] &\rightarrow I^- \rightarrow [H_{B/T_2}] \\
\omega_{CV_4}^2 (-\omega_{CV_4} - \omega_{CV_4}^2): [G_2] &\rightarrow I^+ \rightarrow [P_{T_1}] \\
\omega_{CV_1}^2 (-\omega_{CV_1} - \omega_{CV_1}^2): [G_1] &\rightarrow M^+ \rightarrow [F_{in/T_1}] \\
\omega_{CV_3}^2 (-\omega_{CV_3} - \omega_{CV_3}^2): [U_2] &\rightarrow M^+ \rightarrow [F_{out/T_1}]
\end{aligned}$$

D. Qualitative Processes:

There are 16 qualitative processes shown in the following. For each conditional arc, the antecedent is written above the

consequence that is an ordinary qualitative operation.

$$\begin{aligned}
 P_1 &: [\Omega_{CV_3}] \rightarrow M^+ \rightarrow [U_2] \rightarrow [K_2] \\
 P_2 &: [\Omega_{CV_3}] \rightarrow M^+ \rightarrow [U_2] \rightarrow M^+ \rightarrow [F_{out/T_1}] \rightarrow M^- \\
 &\rightarrow [F_{T_1}] \rightarrow I^+ \rightarrow [H_{T_1}] \\
 P_3 &: [\Omega_{CV_1}] \rightarrow M^+ \rightarrow [G_1] \rightarrow M^+ \rightarrow [F_{in/T_1}] \rightarrow M^+ \\
 &\rightarrow [F_{T_1}] \rightarrow I^+ \rightarrow [H_{T_1}] \\
 P_4 &: [\Omega_{CV_1}] \rightarrow M^+ \rightarrow [G_1] \rightarrow I^- \rightarrow [H_{A/T_2}] \rightarrow M^+ \\
 &\rightarrow [H_{T_2}] \\
 P_5 &: [\Omega_{CV_1}] \rightarrow M^+ \rightarrow [G_1] \rightarrow M^+ \rightarrow [F_1] \rightarrow I^+ \\
 &\rightarrow [F_{out/T_2}] \\
 P_6 &: [\Omega_{CV_2}] \rightarrow M^+ \rightarrow [U_1] \rightarrow I^+ \rightarrow [F_{out/T_2}] \\
 P_7 &: [\Omega_{CV_2}] \rightarrow M^+ \rightarrow [U_1] \rightarrow I^- \rightarrow [H_{B/T_2}] \rightarrow M^+ \\
 &\rightarrow [H_{T_2}] \\
 P_8 &: [\Omega_{CV_2}] \rightarrow M^+ \rightarrow [U_1] \rightarrow [K_1] \\
 P_9 &: [\Omega_{CV_6}] \rightarrow M^+ \rightarrow [E_1] \rightarrow M^+ \rightarrow [F_{in/T_2}] \rightarrow I^+ \\
 &\rightarrow [H_{T_2}] \\
 P_{10} &: [\Omega_{CV_4}] \rightarrow M^+ \rightarrow [G_2] \rightarrow I^+ \rightarrow [P_{T_1}] \\
 P_{11} &: [\Omega_{CV_4}] \rightarrow M^+ \rightarrow [G_2] \rightarrow I^+ \rightarrow [A_{in/T_1}] \\
 P_{12} &: [\Omega_{CV_4}] \rightarrow M^+ \rightarrow [G_2] \rightarrow I^+ \rightarrow [A_{out/T_2}] \\
 P_{13} &: [\Omega_{CV_4}] \rightarrow M^+ \rightarrow [G_2] \rightarrow I^- \rightarrow [P_1] \rightarrow M^+ \rightarrow [P_{T_2}] \\
 P_{14} &: [\Omega_{CV_5}] \rightarrow M^+ \rightarrow [N_1] \rightarrow I^- \rightarrow [P_2] \rightarrow M^+ \rightarrow [P_{T_2}] \\
 P_{15} &: [\Omega_{CV_5}] \rightarrow M^+ \rightarrow [N_1] \rightarrow I^+ \rightarrow [A_{out/T_2}] \\
 P_{16} &: [\Omega_{CV_5}] \rightarrow M^+ \rightarrow [N_1] \rightarrow [J_1]
 \end{aligned}$$

E. Behavioral Fragments

$$\begin{aligned}
 BF_{P_1} &= [\Omega_{CV_3}:0, (\Omega_{CV_3} > 0)], [U_2:0, (U_2 > 0)], \\
 &\quad [K_2:0, (K_2 > 0)] \\
 BF_{P_2} &= [\Omega_{CV_3}:0, (\Omega_{CV_3} > 0)], [U_2:0, (U_2 > 0)], \\
 &\quad [F_{T_1}:0, (F_{T_1} < 0)], \\
 &\quad [H_{T_1}:H_{T_1}^o, (H_{(T_1)min} \leq H_{T_1} < H_{T_1}^o)] \\
 BF_{P_3} &= [\Omega_{CV_1}:0, (\Omega_{CV_1} > 0)], [G_1:0, (G_1 > 0)], \\
 &\quad [F_{T_1}:0, (F_{T_1} > 0)], \\
 &\quad [H_{T_1}:H_{T_1}^o, (H_{T_1}^o < H_{T_1} \leq H_{(T_1)max})] \\
 BF_{P_4} &= [\Omega_{CV_1}:0, (\Omega_{CV_1} > 0)], [G_1:0, (G_1 > 0)], \\
 &\quad [H_{T_2}:H_{T_2}^o, (H_{(T_2)min} \leq H_{T_2} < H_{T_2}^o)] \\
 BF_{P_5} &= [\Omega_{CV_1}:0, (\Omega_{CV_1} > 0)], [F_1:0, (F_1 > 0)], \\
 &\quad [F_{out/T_2}:0, (0 < F_{out/T_2} \leq F_{(out/T_2)max})] \\
 BF_{P_6} &= [\Omega_{CV_2}:0, (\Omega_{CV_2} > 0)], [U_1:0, (U_1 > 0)], \\
 &\quad [F_{out/T_2}:0, (0 < F_{out/T_2} \leq F_{(out/T_2)max})] \\
 BF_{P_7} &= [\Omega_{CV_2}:0, (\Omega_{CV_2} > 0)], [U_1:0, (U_1 > 0)], \\
 &\quad [H_{T_2}:H_{T_2}^o, (H_{(T_2)min} \leq H_{T_2} < H_{T_2}^o)] \\
 BF_{P_8} &= [\Omega_{CV_2}:0, (\Omega_{CV_2} > 0)], [U_1:0, (U_1 > 0)], \\
 &\quad [K_1:0, (K_1 > 0)] \\
 BF_{P_9} &= [\Omega_{CV_6}:0, (\Omega_{CV_6} > 0)], [E_1:0, (E_1 > 0)], \\
 &\quad [H_{T_2}:H_{T_2}^o, (H_{T_2}^o < H_{T_2} \leq H_{(T_2)max})] \\
 BF_{P_{10}} &= [\Omega_{CV_4}:0, (\Omega_{CV_4} > 0)], [G_2:0, (G_2 > 0)], \\
 &\quad [P_{T_1}:P_{T_1}^o, (P_{T_1}^o < P_{T_1} \leq P_{(T_1)max})] \\
 BF_{P_{11}} &= [\Omega_{CV_4}:0, (\Omega_{CV_4} > 0)], [G_2:0, (G_2 > 0)], \\
 &\quad [A_{in/T_1}:0, (0 < A_{in/T_1} \leq A_{(in/T_1)max})]
 \end{aligned}$$

$$\begin{aligned}
 BF_{P_{12}} &= [\Omega_{CV_4}:0, (\Omega_{CV_4} > 0)], [G_2:0, (G_2 > 0)], \\
 &\quad [A_{out/T_2}:0, (0 < A_{out/T_2} \leq A_{(out/T_2)max})] \\
 BF_{P_{13}} &= [\Omega_{CV_4}:0, (\Omega_{CV_4} > 0)], [G_2:0, (G_2 > 0)], \\
 &\quad [P_{T_2}:P_{T_2}^o, (P_{(T_2)min} \leq P_{T_2} < P_{T_2}^o)] \\
 BF_{P_{14}} &= [\Omega_{CV_5}:0, (\Omega_{CV_5} > 0)], [N_1:0, (N_1 > 0)], \\
 &\quad [P_{T_2}:P_{T_2}^o, (P_{(T_2)min} \leq P_{T_2} < P_{T_2}^o)] \\
 BF_{P_{15}} &= [\Omega_{CV_5}:0, (\Omega_{CV_5} > 0)], [N_1:0, (N_1 > 0)], \\
 &\quad [A_{out/T_2}:0, (0 < A_{out/T_2} \leq A_{(out/T_2)max})] \\
 BF_{P_{16}} &= [\Omega_{CV_5}:0, (\Omega_{CV_5} > 0)], [N_1:0, (N_1 > 0)], \\
 &\quad [J_1:0, (J_1 > 0)]
 \end{aligned}$$

F. Diversified Behavioral Fragments

Possible malfunctions of a control valve in the example are either leaking when the valve is set closed, or clogged when it is set opened. Two classes of faults are considered for each valve.

- Clogged when enabled; in this case a valve CV_i behaves as if it is disabled.
- Leaking when disabled; in this case a valve CV_i behaves as if it is enabled.

The malfunction set is composed of

$$\Psi = \left\{ \begin{array}{ccc} (\omega_{CV_1}^2 = 0) & (\omega_{CV_2}^2 = 0) & (\omega_{CV_3}^2 = 0) \\ (\omega_{CV_1}^2 = 1) & (\omega_{CV_2}^2 = 1) & (\omega_{CV_3}^2 = 1) \\ (\omega_{CV_4}^2 = 0) & (\omega_{CV_5}^2 = 0) & (\omega_{CV_6}^2 = 0) \\ (\omega_{CV_4}^2 = 1) & (\omega_{CV_5}^2 = 1) & (\omega_{CV_6}^2 = 1) \end{array} \right\}$$

$\omega_{CV_1}^2 = 0$ ($\omega_{CV_1}^2 = 1$): CV_1 clogged (leaking);
affecting processes P_3, P_4 and P_5 ;

$\omega_{CV_2}^2 = 0$ ($\omega_{CV_2}^2 = 1$): CV_2 clogged (leaking);
affecting processes P_6, P_7 and P_8 ;

$\omega_{CV_3}^2 = 0$ ($\omega_{CV_3}^2 = 1$): CV_3 clogged (leaking);
affecting processes P_1 and P_2 ;

$\omega_{CV_4}^2 = 0$ ($\omega_{CV_4}^2 = 1$): CV_4 clogged (leaking);
affecting processes P_{10}, P_{11}, P_{12} and P_{13} ;

$\omega_{CV_5}^2 = 0$ ($\omega_{CV_5}^2 = 1$): CV_5 clogged (leaking);
affecting processes P_{14}, P_{15} and P_{16} ;

$\omega_{CV_6}^2 = 0$ ($\omega_{CV_6}^2 = 1$): CV_6 clogged (leaking);
affecting processes P_9 .

DBFs for the pressure tank system are

$$\begin{aligned}
 DBF(\omega_{CV_3}^2 = 0)_{P_1} &= (\Omega_{CV_3}:0, K_2:0) \\
 DBF(\omega_{CV_3}^2 = 1)_{P_1} &= (\Omega_{CV_3}:0, K_2 > 0) \\
 DBF(\omega_{CV_3}^2 = 0)_{P_2} &= (\Omega_{CV_3}:0, (H_{T_1}:H_{T_1}^o)) \\
 DBF(\omega_{CV_3}^2 = 1)_{P_2} &= (\Omega_{CV_3} > 0), (H_{(T_1)min} \leq H_{T_1} < H_{T_1}^o) \\
 DBF(\omega_{CV_1}^2 = 0)_{P_3} &= (\Omega_{CV_1}:0), (H_{T_1}:H_{T_1}^o) \\
 DBF(\omega_{CV_1}^2 = 0)_{P_3} &= (\Omega_{CV_1} > 0), (H_{T_1}^o < H_{T_1} \leq H_{(T_1)max}) \\
 DBF(\omega_{CV_1}^2 = 0)_{P_4} &= (\Omega_{CV_1}:0), (H_{T_2}:H_{T_2}^o) \\
 DBF(\omega_{CV_1}^2 = 0)_{P_4} &= (\Omega_{CV_1} > 0), (H_{(T_2)min} \leq H_{T_2} < H_{T_2}^o) \\
 DBF(\omega_{CV_1}^2 = 0)_{P_5} &= (\Omega_{CV_1}:0), (F_{out/T_2}:0)
 \end{aligned}$$

$$\begin{aligned} DBF(\omega_{CV_1}^2 = 1)_{P_5} &= (\Omega_{CV_1} > 0), \\ &(0 < F_{out/T_2} \leq F_{(out/T_2)max}) \\ DBF(\omega_{CV_2}^2 = 0)_{P_6} &= (\Omega_{CV_2}: 0), (F_{out/T_2}: 0) \\ DBF(\omega_{CV_2}^2 = 1)_{P_6} &= (\Omega_{CV_2} > 0) \\ &(0 < F_{out/T_2} \leq F_{(out/T_2)max}) \end{aligned}$$

$$\begin{aligned} DBF(\omega_{CV_2}^2 = 0)_{P_7} &= (\Omega_{CV_2}: 0), (H_{T_2}: H_{T_2}^o) \\ DBF(\omega_{CV_2}^2 = 1)_{P_7} &= (\Omega_{CV_2} > 0)(H_{(T_2)min} \leq H_{T_2} < H_{T_2}^o) \\ DBF(\omega_{CV_2}^2 = 0)_{P_8} &= (\Omega_{CV_2}: 0), (K_1: 0) \\ DBF(\omega_{CV_2}^2 = 1)_{P_8} &= (\Omega_{CV_2} > 0)(K_1 > 0) \\ DBF(\omega_{CV_6}^2 = 0)_{P_9} &= (\Omega_{CV_6}: 0), (H_{T_2}: H_{T_2}^o) \\ DBF(\omega_{CV_6}^2 = 1)_{P_9} &= (\Omega_{CV_6} > 0)(H_{T_2}^o < H_{T_2} \leq H_{(T_2)max}) \\ DBF(\omega_{CV_4}^2 = 0)_{P_{10}} &= (\Omega_{CV_4}: 0), (P_{T_1}: P_{T_1}^o) \\ DBF(\omega_{CV_4}^2 = 1)_{P_{10}} &= (\Omega_{CV_4} > 0)(P_{T_1}^o < P_{T_1} \leq P_{(T_1)max}) \\ DBF(\omega_{CV_4}^2 = 0)_{P_{11}} &= (\Omega_{CV_4}: 0), (A_{in/T_1}: 0) \\ DBF(\omega_{CV_4}^2 = 1)_{P_{11}} &= (\Omega_{CV_4} > 0)(0 < A_{in/T_1} \leq A_{(in/T_1)max}) \\ DBF(\omega_{CV_4}^2 = 0)_{P_{12}} &= (\Omega_{CV_4}: 0), (A_{out/T_2}: 0) \\ DBF(\omega_{CV_4}^2 = 1)_{P_{12}} &= (\Omega_{CV_4} > 0) \\ &(0 < A_{out/T_2} \leq A_{(out/T_2)max}) \\ DBF(\omega_{CV_4}^2 = 0)_{P_{13}} &= (\Omega_{CV_4}: 0), (P_{T_2}: P_{T_2}^o) \\ DBF(\omega_{CV_4}^2 = 1)_{P_{13}} &= (\Omega_{CV_4} > 0), (P_{(T_2)min} \leq P_{T_2} < P_{T_2}^o) \\ DBF(\omega_{CV_5}^2 = 0)_{P_{14}} &= (\Omega_{CV_5}: 0), (P_{T_2}: P_{T_2}^o) \\ DBF(\omega_{CV_5}^2 = 1)_{P_{14}} &= (\Omega_{CV_5} > 0)(P_{(T_2)min} \leq P_{T_2} < P_{T_2}^o) \\ DBF(\omega_{CV_5}^2 = 0)_{P_{15}} &= (\Omega_{CV_5}: 0), (A_{out/T_2}: 0) \\ DBF(\omega_{CV_5}^2 = 1)_{P_{15}} &= (\Omega_{CV_5} > 0) \\ &(0 < A_{out/T_2} \leq A_{(out/T_2)max}) \\ DBF(\omega_{CV_5}^2 = 0)_{P_{16}} &= (\Omega_{CV_5}: 0), (J_1: 0) \\ DBF(\omega_{CV_5}^2 = 1)_{P_{16}} &= (\Omega_{CV_5} > 0)(J_1 > 0). \end{aligned}$$

APPENDIX II

QUALITATIVE COMPILED MODEL OF THE PRESSURE TANK SYSTEM

A. Lumped Processes

$$\begin{aligned} P_1: [K_2] &= M^+[\Omega_{CV_3}] \\ P_2: [H_{T_1}] &= I^-[\Omega_{CV_3}] \\ P_3: [H_{T_1}] &= I^+[\Omega_{CV_1}] \\ P_4: [H_{T_2}] &= I^-[\Omega_{CV_1}] \\ P_5: [F_{out/T_2}] &= I^+[\Omega_{CV_1}] \\ P_6: [F_{out/T_2}] &= I^+[\Omega_{CV_2}] \\ P_7: [H_{T_2}] &= I^-[\Omega_{CV_2}] \\ P_8: [K_1] &= M^+[\Omega_{CV_2}] \\ P_9: [H_{T_2}] &= I^+[\Omega_{CV_6}] \\ P_{10}: [P_{T_1}] &= I^+[\Omega_{CV_4}] \\ P_{11}: [A_{in/T_1}] &= I^+[\Omega_{CV_4}] \\ P_{12}: [A_{out/T_2}] &= I^+[\Omega_{CV_4}] \\ P_{13}: [P_{T_2}] &= I^-[\Omega_{CV_4}] \end{aligned}$$

$$\begin{aligned} P_{14}: [P_{T_2}] &= I^-[\Omega_{CV_3}] \\ P_{15}: [A_{out/T_2}] &= I^+[\Omega_{CV_3}] \\ P_{16}: [N_1] &= M^+[\Omega_{CV_3}] \end{aligned}$$

B. Qualitative Compiled Model

$$\begin{aligned} \mathcal{R}_1: (\Omega_{CV_3} > 0) &\rightarrow (K_2 > 0) \\ \mathcal{R}_2: (\Omega_{CV_3} > 0) \wedge (\Omega_{CV_1} = 0) &\rightarrow (H_{(T_1)min} \leq H_{T_1} < H_{T_1}^o) \\ \mathcal{R}_3: (\Omega_{CV_1} > 0) \wedge (\Omega_{CV_3} = 0) &\rightarrow (H_{T_1}^o < H_{T_1} \leq H_{(T_1)max}) \\ \mathcal{R}_4: (\Omega_{CV_1} > 0) \wedge (\Omega_{CV_2} > 0) \wedge (\Omega_{CV_6} = 0) \\ &\rightarrow (H_{(T_2)min} \leq H_{T_2} < H_{T_2}^o) \\ \mathcal{R}_5: (\Omega_{CV_1} > 0) \wedge (\Omega_{CV_2} > 0) \\ &\rightarrow (0 < F_{out/T_2} \leq F_{(out/T_2)max}) \\ \mathcal{R}_6: (\Omega_{CV_2} > 0) &\rightarrow (K_1 > 0) \\ \mathcal{R}_7: (\Omega_{CV_6} > 0) \wedge (\Omega_{CV_1} = 0) \wedge (\Omega_{CV_2} = 0) \\ &\rightarrow (H_{T_2}^o < H_{T_2} \leq H_{(T_2)max}) \\ \mathcal{R}_8: (\Omega_{CV_4} > 0) &\rightarrow (P_{T_1}^o < P_{T_1} \leq P_{(T_1)max}) \\ \mathcal{R}_9: (\Omega_{CV_4} > 0) \wedge (\Omega_{CV_5} > 0) \\ &\rightarrow (0 < A_{out/T_2} \leq A_{(out/T_2)max}) \\ \mathcal{R}_{10}: (\Omega_{CV_4} > 0) &\rightarrow (0 < A_{in/T_1} \leq A_{(in/T_1)max}) \\ \mathcal{R}_{11}: (\Omega_{CV_4} > 0) \wedge (\Omega_{CV_5} > 0) &\rightarrow (P_{(T_2)min} \leq P_{T_2} < P_{T_2}^o) \\ \mathcal{R}_{12}: (\Omega_{CV_5} > 0) &\rightarrow (J_1 > 0) \\ \mathcal{R}_{13}: (\Omega_{CV_3} = 0) &\rightarrow (K_2 = 0) \\ \mathcal{R}_{14}: (\Omega_{CV_1} = 0) \wedge (\Omega_{CV_2} = 0) &\rightarrow (F_{out/T_2} = 0) \\ \mathcal{R}_{15}: (\Omega_{CV_2} = 0) &\rightarrow (K_1 = 0) \\ \mathcal{R}_{16}: (\Omega_{CV_4} = 0) &\rightarrow (P_{(T_1)min} \leq P_{T_1} < P_{T_1}^o) \\ \mathcal{R}_{17}: (\Omega_{CV_4} = 0) \wedge (\Omega_{CV_5} = 0) &\rightarrow (A_{out/T_2} = 0) \\ \mathcal{R}_{18}: (\Omega_{CV_4} = 0) &\rightarrow (A_{in/T_1} = 0) \\ \mathcal{R}_{19}: (\Omega_{CV_4} = 0) \wedge (\Omega_{CV_5} = 0) &\rightarrow (P_{T_2}^o < P_{T_2} \leq P_{(T_2)max}) \\ \mathcal{R}_{20}: (\Omega_{CV_5} = 0) &\rightarrow (J_1 = 0). \end{aligned}$$

ACKNOWLEDGMENT

We should thank Dr. Mitsuji Sampei of Chiba University for interesting discussions that helped us refine ideas presented in this paper. The environment of Computing and Information Systems Center (CISC) of Japan Atomic Energy Research Institute (JAERI) provided valuable support and stimulation for this project. We had useful discussions with Messrs. Kiyoshi Asai (Office of Planning, JAERI), Masayuki Akimoto, Minoru Fujii, Kenji Higuchi, Etsuo Kume, Takayuki Ohtani and Shaw Kambayashi (CISC). We are grateful to them all. Finally, we should thank the anonymous referees who provided us with helpful comments on an earlier version of this paper.

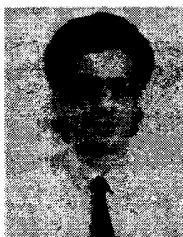
REFERENCES

- [1] A. Abu-Hanna and Y. I. Gold, "Adaptive multilevel diagnosis and modeling of dynamic systems," *Int. J. Expert Syst.*, vol. 3, no. 1, pp. 1-30, 1990.
- [2] L. Bainbridge, "Types of Representation," in *Tasks, Errors and Mental Models*, L. P. Goodstein, H. B. Andersen, and S. E. Olsen, Eds. London: Taylor and Francis, 1988, ch. 4, pp. 70-91.

- [3] S. Baron, C. Feehrer, R. Muralidharan, R. Pew, and P. Horwitz, "A framework for modeling supervisory control behavior of operators of nuclear power plants," in *Proc. Workshop Cognitive Modeling of Nuclear Plant Control Room Operators*, ORNL TM-8614, Dedham, MA, Aug. 1982, pp. 36-51.
- [4] M. Basseville, "Detecting changes in signals and systems—A survey," *Automatica*, vol. 24, no. 3, pp. 309-326, 1988.
- [5] A. Benveniste and P. LeGuernic, "Hybrid dynamical systems theory and the SIGNAL Language," *IEEE Trans. Automat. Contr.*, vol. 35, pp. 535-546, May 1990.
- [6] D. G. Bobrow, Ed., Special Issue on Qualitative Reasoning About Physical System, *Artif. Intell.*, vol. 24, 1984.
- [7] M. A. Breuer and A. D. Freidman, *Diagnosis and Reliable Design of Digital Systems*. Computer Science Press, 1976.
- [8] A. W. Burks, "The logic of causal propositions," *Mind*, vol. LX, pp. 363-382, 1951.
- [9] T. Bylander, "A critique of qualitative simulation from a consolidation viewpoint," *IEEE Trans. Syst., Man, Cybern.*, vol. 18, pp. 252-263, Mar./Apr. 1988.
- [10] P. C. Cacciabue and U. Bersini, "Modeling human behavior in the context of a simulation of man-machine systems," in *Training, Human Decision Making and Control*, J. Patrik and K. D. Duncan, Eds. New York: Elsevier Science, 1988, pp. 223-241.
- [11] E. Y. Chow and A. S. Willsky, "Analytical redundancy and the design of robust failure detection systems," *IEEE Trans. Automat. Contr.*, vol. AC-29, pp. 603-614, 1984.
- [12] R. N. Clark, "Instrument fault detection," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 14, pp. 456-465, 1978.
- [13] J. Cunningham, "Comprehension by model-building as a basis for an expert system," in *Expert Systems '85, Proc. 5th Tech. Conf. British Comput. Soc.*, Specialist Group on Expert Systems, British Inf. Soc. Ltd., 1985, pp. 259-272.
- [14] J. D. DeKleer and J. S. Brown, "A qualitative physics based on confluences," *Artif. Intell.*, vol. 24, pp. 7-83, 1984.
- [15] J. D. DeKleer and B. C. Williams, "Diagnosing multiple faults," *Artificial Intell.*, vol. 32, pp. 97-130, 1987.
- [16] B. H. Far, M. Nakamichi, and M. Sampei, "Automatic diagnostic rule generation for rule-based controllers by qualitative sensitivity analysis," *Trans. Inst. Elec. Japan*, vol. 110C, no. 10, pp. 661-669, Oct. 1990.
- [17] B. H. Far, "Functional reasoning, explanation, and analysis," *JAERI-M 91-225*, Japan Atomic Energy Res. Inst., Tokai, Japan, Jan. 1992.
- [18] B. H. Far, M. Nakamichi, and M. Sampei, "Qualitative sensitivity analysis," *J. Japanese Soc. Artificial Intell.*, vol. 6, no. 1, pp. 84-95, Jan. 1991.
- [19] B. H. Far, M. Nakamichi, and M. Sampei, "Qualitative supervisory control featuring cognitive capabilities of the domain practitioners," in *Proc. 2nd Makuhari Int. Conf. High Technology (MIGHT'91)*, Chiba, Japan, Feb. 1991, pp. 135-138.
- [20] R. E. Fikes and N. J. Nilsson, "STRIPS: A new approach to the application of theorem proving to problem solving," *Artif. Intell.*, vol. 2, pp. 189-208, 1971.
- [21] P. K. Fink, "Control and integration of diverse knowledge in a diagnostic expert system," in *Proc. 9th Int. Joint Conf. Artif. Intell. (IJCAI'85)*, Los Angeles, CA, 1985, pp. 426-431.
- [22] P. K. Fink and J. C. Luths, "Expert systems and diagnosis expertise in the mechanical and electrical domains," *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-17, pp. 340-349, May/June 1987.
- [23] K. D. Forbus, "Qualitative process theory," *Artificial Intell.*, vol. 24, pp. 85-168, 1984.
- [24] K. D. Forbus, "Interpreting observations of physical systems," *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-17, pp. 350-359, May/June 1987.
- [25] P. M. Frank, "Fault diagnosis in dynamic systems using analytical and knowledge based redundancy—A survey and some new results," *Automatica*, vol. 26, no. 3, pp. 459-474, 1990.
- [26] J. B. Fussel, "A formal methodology for fault tree construction," *Nuclear Sci. and Eng.*, vol. 52, pp. 421-432, 1973.
- [27] M. R. Genesereth, "The use of design descriptions in automated diagnosis," *Artificial Intell.*, vol. 24, pp. 411-436, 1984.
- [28] M. P. Georgeff and U. Bunollo, "Procedural expert systems," in *Proc. 8th Int. Joint Conf. Artif. Intell. (IJCAI'83)*, Karlsruhe, Germany, 1983, pp. 151-157.
- [29] M. P. Georgeff and A. L. Lansky, "Procedural knowledge," *Proc. IEEE*, vol. 74, no. 10, pp. 1383-1397, 1986.
- [30] M. L. Ginsberg and D. E. Smith, "Reasoning about action—I: A possible worlds approach," *Artificial Intell.*, vol. 35, pp. 165-195, 1988.
- [31] F. Gomez and B. Chandrasekaran, "Knowledge organization and distribution for medical diagnosis," *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-11, pp. 34-42, Jan. 1981.
- [32] J. Gordon and E. H. Shortliffe, "The Dempster-Shafer theory of evidence," in *Rule-Based Expert Systems*, B. C. Buchanan and E. H. Shortliffe, Eds. Reading, MA: Addison-Wesley, 1984, ch. 13, pp. 272-292.
- [33] T. P. Hamilton, "An application of qualitative physics to diagnostics in advanced helicopters," *Abstracts Qualitative Physics Workshop*, Urbana-Champaign, IL, 1987.
- [34] J. M. Hoc, "Strategies in controlling a continuous process with long response latencies: Needs for computer support to diagnosis," *Int. J. Man Machine Studies*, vol. 30, pp. 47-67, 1989.
- [35] R. Isermann, "Process fault detection based on modeling and estimation methods—A survey," *Automatica*, vol. 20, no. 4, pp. 387-404, 1984.
- [36] Y. Iwasaki and H. A. Simon, "Causality in device behavior," *Artificial Intell.*, vol. 29, pp. 3-32, 1986.
- [37] G. Johannsen, "Categories of human operator behavior in fault management situations," in *Tasks, Errors and Mental Models*, L. P. Goodstein, H. B. Andersen, and S. E. Olsen, Eds. London: Taylor and Francis, 1988, ch. 16, pp. 251-258.
- [38] J. L. Knight, "Manual control and tracking," in *Handbook of Human Factors*, G. Galvandy, Ed. New York: Wiley, 1987, ch. 2.7, pp. 183-217.
- [39] B. Kuipers, "Qualitative simulation," *Artificial Intell.*, vol. 29, pp. 289-338, 1986.
- [40] B. Kuipers, "Qualitative reasoning with causal models in diagnosis of complex systems," in *Artificial Intelligence, Simulation, and Modeling*, L. E. Widman, K. A. Loparo and R. A. Nielsen, Eds. New York: Wiley, 1989, ch. 10, pp. 257-274.
- [41] M. Lind, "System concepts and the design of man-machine interfaces for supervisory control," in *Tasks, Errors and Mental Models*, L. P. Goodstein, H. B. Andersen, and S. E. Olsen, Eds. London: Taylor and Francis, 1988, ch. 18, pp. 269-277.
- [42] R. Milne, "Fault diagnosis through responsibility," in *Proc. 9th Int. Joint Conf. Artificial Intell. (IJCAI'85)*, Los Angeles, CA, 1985, pp. 423-425.
- [43] ———, "Strategies for diagnosis," *IEEE Trans. Syst. Man, Cybern.*, vol. SMC-17, no. 3, pp. 333-339, May/June 1987.
- [44] ———, "Artificial intelligence for online diagnosis," *Proc. IEE*, vol. 134, Pt. D, no. 4, pp. 238-244, 1987.
- [45] T. P. Moran, "An applied psychology of the user," *Computing Surveys*, vol. 13, no. 1, pp. 1-11, Mar. 1981.
- [46] N. H. Narayanan and N. Viswanadham, "A methodology for knowledge acquisition and reasoning in failure analysis of systems," *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-17, no. 2, pp. 274-288, Mar./Apr. 1987.
- [47] T. Nishida and S. Doshita, "Reasoning about discontinuous change," in *Proc. 6th National Conf. Artif. Intell. (AAAI'87)*, Seattle, WA, July 1987, pp. 643-648.
- [48] A. Paterson, P. Sachs, and M. Turner, "ESCORT: The application of causal knowledge to real-time process control," in *Expert Systems '85, Proc. 5th Tech. Conf. Brit. Comput. Soc. Specialist Group on Expert Systems*, British Inform. Soc. Ltd., 1985, pp. 79-88.
- [49] M. J. Pazzani, "Failure driven learning of fault diagnosis heuristics," *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-17, pp. 380-394, May/June 1987.
- [50] J. Rasmussen, "On the structure of knowledge—A morphology of mental models in a man-machine system context," *Riso Report Riso-M-2357*, Riso Nat. Lab., Denmark, 1979.
- [51] ———, "The role of hierarchical knowledge representation in decision making system management," *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-15, pp. 234-243, Mar./Apr. 1985.
- [52] J. Rasmussen and L. P. Goodstein, "Decision support in supervisory-control of high-risk industrial systems," *Automatica*, vol. 23, no. 5, pp. 663-671, 1987.
- [53] J. Reason, "Framework models of human performance and error—A consumer guide," in *Tasks, Errors and Mental Models*, L. P. Goodstein, H. B. Andersen, and S. E. Olsen, Eds. London: Taylor and Francis, 1988, ch. 2, pp. 35-49.
- [54] R. Reiter, "A theory of diagnosis from first principles," *Artificial Intell.*, vol. 32, pp. 57-95, 1987.
- [55] J. Rothenberg, "The nature of modeling," in *Artificial Intelligence, Simulation and Modeling*, L. E. Widman, K. A. Loparo and R. A. Nielsen, Eds. New York: Wiley, 1989, ch. 2, pp. 75-92.
- [56] W. B. Rouse, "Models of human problem solving: Detection, diagnosis and compensation for system failures," *Automatica*, vol. 19, no. 6, pp. 613-625, 1983.
- [57] W. B. Rouse and S. H. Rouse, "Measures of complexity of fault diagnosis tasks," *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-9, pp. 720-727, Nov. 1979.
- [58] P. M. Sanderson and K. Harwood, "The skills, rules and knowledge classification: A discussion of its emergence and nature," in *Tasks*,

- Errors and Mental Models*, L. P. Goodstein, H. B. Andersen, and S. E. Olsen, Eds. London: Taylor and Francis, 1988, ch. 1, pp. 21–34.
- [59] P. Schaefer, "Higher level causal reasoning for diagnosis," in *Proc. IEEE Int. Workshop Artificial Intell. Indus. App.*, Hitachi, Japan, May 1988, pp. 33–38.
- [60] D. P. Siewiorek and L. K. Lai, "Testing of digital systems," *Proc. IEEE*, vol. 69, no. 10, pp. 1321–1333, Oct. 1981.
- [61] T. B. Sheridan, "Supervisory control," in *Handbook of Human Factors*, G. Salvendy, Ed. New York: Wiley, 1987, ch. 9.6, pp. 1243–1268.
- [62] J. Shiozaki, B. Shibata, H. Matsuyama, and E. Oshima, "Fault diagnosis of chemical processes utilizing signed directed graphs improvement by temporal information," in *Proc. IEEE Int. Workshop Artificial Intell. Ind. App.*, Hitachi, Japan, May 1988, pp. 461–466.
- [63] J. Shrager, D. Jordan, T. Moran, G. Kiczales, and D. Russell, "Issues in the pragmatics of qualitative modeling: Lessons learned from a xerographics project," *Commun. ACM*, vol. 30, no. 12, pp. 1036–1047, 1987.
- [64] P. Struss, "Extensions to ATMS-based diagnosis," in *Artificial Intelligence in Engineering: Diagnosis and Learning*, J. S. Gero, Ed., Elsevier, 1988, pp. 3–28.
- [65] P. W. Thorndyke, "A rule-based approach to cognitive modeling of real-time decision making," in *Proc. Workshop Cognitive Modeling of Nuclear Plant Control Room Operators*, ORNL TM-8614, Dedham, MA, Aug. 1982, pp. 147–155.
- [66] B. Wahlstrom, "On the use of models in human decision-making," in *Tasks, Errors and Mental Models*, L. P. Goodstein, H. B. Andersen, and S. E. Olsen, Eds. London: Taylor and Francis, 1988, ch. 10, pp. 161–170.
- [67] D. S. Weld, "Comparative analysis," *Artif. Intell.*, vol. 36, pp. 333–373, 1988.
- [68] D. S. Weld, "Combining discrete and continuous process models," in *Proc. 9th Int. Joint Conf. Artificial Intell. (IJCAI'85)*, Los Angeles, CA, 1985, pp. 140–143.
- [69] M. D. Williams, T. P. Moran, and J. S. Brown, "The role of conceptual models in nuclear power plant operation," in *Proc. Workshop Cognitive Modeling of Nuclear Plant Control Room Operators*, ORNL TM-8614, Dedham, MA, Aug. 1982, pp. 107–116.
- [70] A. S. Willsky, "A survey of design methods for failure detection systems," *Automatica*, vol. 12, pp. 601–612, 1976.
- [71] J. Yen, "GERTIS: A Dempster-Shafer approach to diagnosing hierarchical hypotheses," *Commun. ACM*, vol. 32, no. 5, pp. 573–585, 1989.
- [72] W. C. Yoon and J. M. Hammer, "Deep reasoning fault diagnosis: An aid

and a model," *IEEE Trans. Syst., Man, Cybern.*, vol. 18, pp. 659–676, July/Aug. 1988.



Behrouz Homayoun Far (S'87–M'90) received the B.Sc. and M.Sc. degrees in electronic engineering in 1983 and 1986, respectively, from Tehran University, Tehran, Iran. He has received the Ph.D. degree from Chiba University, Chiba, Japan, in 1990.

He is a Research Fellow at Japan Atomic Energy Research Institute (JAERI). He was awarded a post doctoral fellowship from the Japanese Science and Technology Agency. His research fields are in qualitative and temporal reasoning, knowledge acquisition and analytic learning and their applications in robotics, control and cognitive engineering.

Dr. Far is a member of the Association for Computing Machinery, IEEE Computer Society, Japanese Society for Artificial Intelligence, Japanese Society of Instrumentation and Control Engineers, and the Information Processing Society of Japan.



Matsuroh Nakamichi was born on April 30, 1928. He received the B.Eng. degree in electrical engineering in 1953 from the Tokyo Institute of Technology and joined the Hitachi Ltd. in the same year. He received the Dr.Eng. degree in 1961 from the Tokyo Institute of Technology.

He has been with the Faculty of Engineering of Chiba University, since 1961, where he is now a Professor in the Department of Electrical and Electronic Engineering. The research fields of his interest are fail safe logic circuits and systems, fault tolerant control systems and fault diagnosis of logic circuits and systems.

Professor Nakamichi is a member of Institute of Electrical, Information and Communication Engineers of Japan, Institute of Electrical Engineers Japan, Society of Instrumentation and Control Engineers, Illumination Institute of Japan and Japan Society for Fuzzy Theory and Systems.