Narrowing Diagnostic Focus Using Functional Decomposition

The problem of diagnosing faults in chemical plants can be efficiently addressed by a hierarchical procedure involving successive narrowing of the space in which the fault search is conducted. A technique is presented for narrowing diagnostic focus useful in the first stages of a diagnostic search. Based on a decomposition of the process according to function, the technique assesses the functionality of process systems based on measurements of controlled and manipulated variables. A procedure for identification of possibly faulty systems and units from the system states is outlined. Detailed diagnosis, not treated in this paper, would be applied after candidate systems or units are located. An example is presented using a hypothetical chemical reaction process.

F. E. Finch, M. A. Kramer
Department of Chemical Engineering
Massachusetts Institute of Technology
Cambridge, MA 02139

Introduction

All process equipment is subject to failure. Failure can be caused by undetected initial defects, normal wear-out, or stress beyond design limits. Undetected or uncorrected failures can result in loss of product, imminent or latent safety hazards, and risk of induced failures in related equipment. Because equipment failure is a stochastic process, a continuous effort toward failure detection, diagnosis, and correction is essential for continued plant operability.

The responsibility for failure detection and diagnosis belongs to plant operators. Operators rely on training, experience, and reasoning ability to diagnose faults. Typically, operators are well trained in normal process operation and in responses to predictable failure situations. However, uncertainty in process data, unpredicted and low-probability failures, and real-time exigencies can often conspire to produce misdiagnoses and inappropriate corrective actions.

The speed and reliability of computers, as well as the centralization of relevant information in the control room, make computer-aided approaches to diagnosis an attractive alternative to exclusive reliance on plant operators. A variety of computer-based approaches to fault diagnosis have been proposed, but no single approach has been shown to be universally superior. The reader is referred to Himmelblau (1978) for an introduction to this area.

Past efforts to codify the diagnosis task can be divided into two categories: experiential and model-based approaches. The former, exemplified by the expert system, attempts to duplicate the plant-specific expertise of human diagnosticians by encoding their accumulated experience, judgment, and heuristics into rules in a structured knowledge base. In contrast, model-based approaches utilize explicit models of process behavior with a plant-independent diagnostic strategy to formulate diagnostic conclusions. A comparison of these two approaches is provided by Kramer (1986). This paper concentrates on the model-based approach.

Most previous proposals for automated fault diagnosis (with the exception of certain expert systems) model process behavior at a single level of abstraction. Nonhierarchical approaches require process models and diagnostic algorithms sufficiently detailed to resolve individual faults at the unit level. Use of detailed models means that nonhierarchical methods may become inefficient if applied to the entire plant simultaneously. An example in this class is fault detection by Kalman filtering, which can be effective at the unit level but is too complex to be applied to groups of units or at the plant level. This suggests that a multitiered, hierarchical approach to diagnosis may be more suitable for large or complex processes.

In this paper we discuss the characteristics of and motivations for a hierarchical diagnosis system. A modeling formalism is introduced to describe large and complex processes at an appropriate level of detail for early-stage diagnosis. Then, a two-stage diagnostic procedure for detecting faulty systems and units in the presence of a single fault is described. In the first stage, the potentially faulty systems of the plant are located. The second stage involves the application of rules that further narrow the fault candidate space based on the states of systems adjacent to

Correspondence concerning this paper should be addressed to M. A. Kramer.

the faulty system. Finally, we present an example of directing diagnostic focus in a chemical reaction process.

Hierarchical Diagnosis

Diagnosis can be defined as the problem of tracing process disturbances to their sources. As such, diagnosis is a search problem, complicated by the large dimensionality of the search space. Intelligent search entails structuring the search space to limit the possible avenues of investigation. Insight into knowledge representations for efficient search can be gained through examination of human techniques in diagnostic problem solving.

Rasmussen (1985) shows that human decision makers commonly reason at many levels of functional and structural abstraction. The utility of abstraction at proper levels is to reduce the perceived complexity of the device in question. Rasmussen observed abstraction in two dimensions: a structural dimension corresponding to physical groupings of components, and a functional dimension related to the purpose and behavior of the equipment. The human diagnostic process moves from a high level in both of these coordinates, where the purpose and performance of the device as a whole is considered, to a detailed level where the function and physical form of lowest-level components are analyzed.

This strategy naturally suggests hierarchical modeling of the process. The hierarchical structure supports efficient "top-down" solution procedures in which diagnostic focus is rapidly narrowed from an initially broad fault classification to a useful restricted final diagnosis. This approach is easily implemented on the computer. For example, the expert system shell PICON (Moore et al., 1984) includes a facility for transferring control between sets of rules that can be used to mimic the ability of the process operator to successively focus on smaller areas of the plant during diagnosis. Other formats for hierarchical reasoning have been described by Shum et al. (1986) and Keravnou and Johnson (1986). In the former, a hierarchy is based on the functionality of the process, and rules for narrowing focus are derived from operating experience. The latter work employs a hierarchy of physical device components, and uses a method of focusing based on the sets of symptoms associated with each component that can also be combined with experiential knowledge.

Considering the structural and functional dimensions in diagnostic reasoning, Davis (1984) argues the necessity of both structural and functional models based on the noninterconvertability of information on physical structure and information on device behavior. Theoretically, functional information should be discernible from structural descriptions, but in complex devices this transition is difficult. Davis presents a methodology for automated diagnosis of digital equipment based on models containing explicit structural and functional elements. In the present work, explicit representation of process functionality is used to mask details of system structure irrelevant at the early stages of the diagnostic task. We feel that this approach is preferable to a structural analysis that would seek a unit or units casually connected to all fault symptoms by flows of mass, energy, or information. To be completely effective, structural analysis would require complete measurement of stream variables. Moreover, such a method would be rendered ineffective by recycle streams and control feedback loops.

With these motivations, we present a method in which the process is represented as a set of abstract functional systems, each responsible for controlling certain aspects of the overall process. When abnormal measurements are detected, the implication is that one or more of these systems is malfunctional. By identification of the processing units or control system components responsible, directly or indirectly, for regulation of the measurements that are abnormal, the focus of the diagnosis can quickly be narrowed to those components. The objective of the diagnosis at this level is to identify malfunctioning systems or units, not the actual faults within the units. The detailed diagnosis of faults is not considered in this work, but could be approached with a variety of techniques, such as those described in Himmelblau (1978).

Functional Decomposition

The diagnostic strategy presented in this work utilizes a logic model of process behavior. This model is based on the function of units within the context of the process, the arrangement of the unit functions into systems, and the composition, boundaries, and interdependencies of process systems. This approach is similar to that used by Shafaghi et al. (1984) for the construction of fault trees. In this section, we present the framework for development of this model, using a functional decomposition approach.

Basic definitions

Processes are designed to achieve certain production objectives. Fulfillment of these objectives is contingent on proper operation of the various units that comprise the process. A fault, which refers to some physical degradation of a process unit, can affect the process by reducing or destroying the ability of a unit to perform critical unit functions. If a unit is unable to perform a specific function to the extent required by the process, it is termed a failure of the unit function.

An important distinction exists between a unit function, which is any one of several duties a unit performs, and the physical unit. Frequently, a single unit will perform two or more functions. For example, the unit functions of a heat exchanger include heat transfer, fluid containment, and fluid conductance. A fault in a heat exchanger may result in the failure of one or more of these functions while leaving others unaffected. This is illustrated by tube-side blockage, which affects heat transfer and tube-side fluid conductance, leaving fluid containment and shell-side fluid conductance unaffected.

The functions of several units may collectively be responsible for achieving higher level functional objectives. We define a system to be any group of unit functions that act together to fulfill a system objective or system function. If a system is unable to achieve its objective, that is termed a system failure or system malfunction.

It is useful to represent systems as sets of unit functions:

$$S_k = (U_{ij} | U_{ij} \text{ vital to achieving the system objective } k) \quad (1)$$

where U_{ij} denotes the jth unit function of unit i.

If a given unit function is vital to two or more systems, the unit function falls in the intersection of the system sets:

$$S_k \cap S_\ell = (U_{ij} | U_{ij} \epsilon S_k \text{ and } S_\ell) \quad (2)$$

Failure of a unit function may result in the malfunction of any system that contains the function. How a specific failure of a unit function affects a particular system strongly depends on the nature of the failure and the type of system involved. Some systems are resilient and can continue to meet their objectives in the presence of certain failures, while others fail in the presence of any unit function failure.

Often, systems not only rely on proper operation of their constituent unit functions to achieve their objectives but may also rely on proper operation of other systems. Recognizing this fact, we define a system S_k to be dependent on another system S_ℓ if malfunction of system S_ℓ can produce a malfunction of system S_k independent of the operating condition of the unit functions of system S_k. This situation occurs when the system objective of system S_ℓ is vital in achieving the system objective of system S_k.

It is convenient to represent a process graphically as a network of interrelated systems, as shown in Figure 1. Here, nodes represent system sets as defined in Eq. 1 and arcs represent the directed dependencies between systems, which we refer to as propagation paths. In Figure 1, system S3 is shown to be dependent on system S2, and system S4 is dependent on both systems S2 and S3. The nonempty intersection of systems S1 and S2 reveals that these systems share certain common unit functions.

In summary, systems have two sources of dependency: internal dependency on the unit functions that comprise the system, and external dependency on other systems. All system malfunctions can be traced to failures in one of these sources. Functional decomposition is the process of identifying the functional systems, their component unit functions, and their interactions.

System states and types

Systems can be classified according to their objectives, modes of operation, and position in the process. Here, we limit the analysis to three system classifications: control systems, passive systems, and external systems.

Control Systems. Control systems are characterized by an ability to actively regulate the process through manipulation of various process variables and parameters. The objective of a regulating control system is to maintain certain controlled variables $\underline{C}$ at predetermined desired (set point) values $\underline{C}_{sp}$. In effect, the control system seeks to minimize δ_c where

$$\delta_c = \underline{\beta}_c^T \cdot |\underline{C} - \underline{C}_{sp}|$$

$$\underline{\beta}_c = \text{vector of weighting factors} \qquad (3)$$

Because feedback control systems operate using a closed-loop structure that involves measurement or estimation of the controlled variables, it can reasonably be assumed that measured values of the controlled variables will be available for diagnosis.

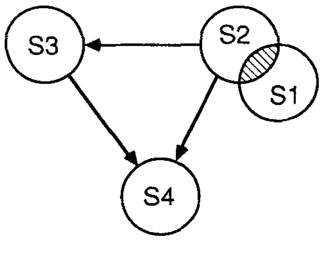

Figure 1. Process graph example.

Using Eq. (3), we can define two control system states using δ_c:

1. If $\delta_c \cong 0$, the system is functional
2. If $\delta_c \gg 0$, the system is malfunctional

If measurements of the manipulated variables of a control system are also available either by direct measurement or through knowledge of controller output or valve position, we can define additional control system states by comparing the measured values of the manipulated variables $\underline{M}$ with our expectations $\underline{M}_e$:

$$\text{Let} \quad \delta_m = \underline{\beta}_m^T \cdot |\underline{M} - \underline{M}_e|$$

$$\underline{\beta}_m = \text{vector of weighting factors} \qquad (4)$$

Equation 4 assumes that we can evaluate expected values for each of the manipulated variables under consideration. How these expectations are calculated is critical to their usefulness in the diagnosis.

In contrast to controlled variables, manipulated variables may, under normal conditions, take on a range of values to compensate for changing process conditions. Thus, no simple standard exists to judge what a manipulated variable value should be under given conditions. A variety of approaches to calculate expected values for manipulated variables can be conceptualized. For example, expected values can be computed based on knowledge of the system's controlled variables and their set points, as shown in Eq. 5:

$$\underline{M}_e = \underline{g}^1 [\underline{C}, \underline{C}_{sp}] \qquad (5)$$

This approach, illustrated in Figure 2a, provides analytical redundancy on the controller since g^1 duplicates the controller logic. Equations 4 and 5 provide diagnostic information on the state of the controller and controlled variable sensor, but no information on the broader state of the process that would be useful in a systems-level diagnosis. A second approach more

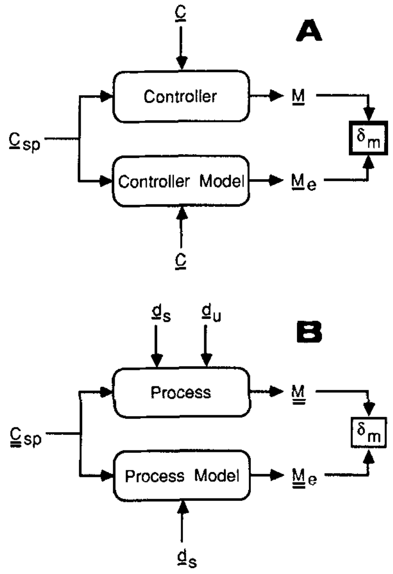

Figure 2. Comparison of expected and measured manipulated variable generation.

suited to systems analysis involves calculation of expected manipulated variable values using global knowledge of process conditions, as in Eq. 6:

$$\underline{\underline{M}}_e = \underline{g}^2[\underline{\underline{C}}_{sp}, \underline{d}_s] \tag{6}$$

where $\underline{d}_s$ = vector of measured process inputs and disturbances.

Equation 6 estimates $\underline{\underline{M}}_e$ using information on process inputs, specifically, the set points of all control systems (including set points generated in cascade control systems) as well as data on process feedstocks, environmental conditions, and other measured process disturbances. A steady state model can usually provide $\underline{\underline{M}}_e$, although empirical strategies based on experience are also possible. Any difference between $\underline{\underline{M}}_e$ and $\underline{\underline{M}}$ is indicative of errors in the process model used to compute $\underline{\underline{M}}_e$ (which can be assessed using process data), noise in the measurement of $\underline{\underline{M}}$ (which can be addressed statistically), or abnormal unmeasured disturbances to the process (e.g., faults). Thus, Eq. 6 provides analytical redundancy for the entire process as opposed to Eq. 5, which only deals with the single controller. This concept is illustrated in Figure 2b.

In the remainder of this paper, the global approach represented by Eq. 6 is used exclusively for computation of expected manipulated variable values. Diagnostic strategies using different methodologies for calculating $\underline{\underline{M}}_e$ are possible but are left to future research.

Using values of δ_c and δ_m, we can define four control system states:

1. If $\delta_c \simeq 0$ and $\delta_m \simeq 0$, the system is functional
2. If $\delta_c \simeq 0$ and $\delta_m \gg 0$, the system is stressed
3. If $\delta_c \gg 0$ and $\delta_m \simeq 0$, the system is uncontrolled
4. If $\delta_c \gg 0$ and $\delta_m \gg 0$, the system is saturated

Whereas, in the absence of manipulated variable information, system malfunction could only be detected by deviation of controlled variables from their set point values, three different malfunctional states can be distinguished with knowledge of δ_m. A stressed system indicates a failure exists that can be compensated by regulatory action. This state is quite common, due to the resilient nature of control systems, but would be undetectable without knowledge of δ_m. When a system is unable to compensate for a failure, saturation of the control system results. Alternatively, if a failure occurs in the regulatory mechanism of the control system, then the system is uncontrolled. Knowledge of δ_m allows the diagnostic system to identify these malfunction types.

Passive Systems. Passive or open-loop systems do not actively regulate the process. These systems, given appropriate inputs, simply maintain certain desired system outputs. Typically, the outputs of these systems are variables that cannot be controlled directly and are therefore controlled indirectly through control systems on which the passive system is dependent. For example, chemical reactors are often passive systems since the reaction rate and conversion are not controlled directly, but rather through control of the reaction environment (i.e., temperature, residence time, mixing environment, etc.). The reactor can be considered a passive system dependent on several control systems for proper operation. Although the distinction between the passive system and the various control systems on which it depends seems slight, the distinction can be important in diagnosis as can be seen subsequently in examples 1 and 2, which deal with such a reaction process. In general, passive systems can be identified as those systems that produce measured outputs not directly involved in process regulation. Because passive systems lack the ability to act on the process, these systems tend to be brittle in the sense that any constituent unit function failure or external disturbance will result in deviation of the system outputs from their desired values.

The parameter used to determine the state of a passive system is defined as follows:

$$\text{Let} \quad \delta_p = \underline{\beta}_p^T \cdot |\underline{P} - \underline{P}_e| \tag{7}$$

where

$\underline{P}$ = vector of measured system outputs

$\underline{P}_e$ = vector of desired system outputs

$\underline{\beta}_p$ = vector of weighting factors

For these systems, there are two possible states:

1. If $\delta_p \simeq 0$, the system is functional
2. If $\delta_p \gg 0$, the system is malfunctional

From these definitions, it can be seen that passive systems are similar to control systems for which no manipulated variable information is available.

External Systems. External systems are systems on the periphery of the process being analyzed. Usually, the external systems of a process are the various support systems on which the process depends, but in a broad sense, any system outside the process boundaries that influences process operation can be considered an external system. An external system is identified as any system, controlled or passive, on which one or more of the process systems are dependent but is outside the scope of analysis. In other words, external systems are systems whose outputs are inputs to the process being analyzed.

External systems can be either control systems or passive systems. Because the process is affected only by the outputs of these systems, the state of an external system is determined using only output variables:

$$\text{Let} \quad \delta_x = \delta_c \quad \text{(if a control system)} \tag{8a}$$

$$\text{or} \quad \delta_x = \delta_p \quad \text{(if a passive system)} \tag{8b}$$

External system state is determined as follows:

1. If $\delta_x \simeq 0$, the system is functional
2. If $\delta_x \gg 0$, the system is malfunctional

External systems are treated as passive systems in the diagnostic procedure since the mechanisms for maintenance of the system outputs are outside the scope of the analysis.

Measuring system states

Although the definitions of system states are unambiguous, actual measurement of system states can entail considerable uncertainty. Difficulty arises in deciding when δ (here referring to δ_c, δ_m, δ_p, or δ_x, depending on context) is sufficiently greater than zero to indicate a malfunction. Noisy measurements, errors in process modeling, and normal process transients will assure that δ is never exactly zero; therefore, some objective standard must be established to detect significant deviations.

Two approaches to this problem are possible. The simplest approach is to establish threshold values α for each of the mea-

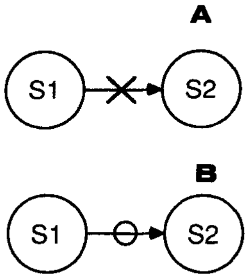

Figure 3. Graphical notation for conditional system dependency.

sured δ values. If δ is greater than the threshold, it is indicative of a significant deviation, otherwise, the deviation is assumed to be insignificant:

$$\text{If } \delta > \alpha \text{ then } \delta \gg 0 \tag{9a}$$

$$\text{If } \delta < \alpha \text{ then } \delta \simeq 0 \tag{9b}$$

Regardless of whether statistics or experience is used to determine α, the discontinuous nature of this approach can result in undesirable situations (Kramer, 1987). For example, if $\delta \simeq \alpha$, small random fluctuations in δ can result in unstable, oscillating system states. A second approach is to specify a continuous belief function for each δ:

$$\theta(\delta) \equiv \text{belief that } \delta \gg 0 \tag{10}$$

where $\theta(\delta)$ is a continuous, monotonic function with $\lim_{\delta \to 0} \theta(\delta) = 0$ and $\lim_{\delta \to \infty} \theta(\delta) = 1$.

Using fuzzy logic (Zadeh, 1965) or the mathematical theory of evidence (Shafer, 1976) it may be possible to incorporate these continuous levels of belief into the diagnostic reasoning.

In this work, system states are assumed to be known with certainty, decoupling the problem of system state measurement from the problem of diagnosis. Further research is necessary to include uncertainty in system states in the diagnostic procedure.

Conditional system dependencies

Dependencies between various process systems allow a malfunction of one system to propagate to other systems causing additional malfunctions. With an understanding of system states, we can expand the concept of system dependencies to produce a more detailed and realistic process model.

In this model, system dependencies are conditional on both the state of the system and the specific process variables being affected. If a system S1 is observed to be malfunctioning and a second system S2 is dependent on S1 through variables that are significantly deviated, then the propagation path between the two systems is active, meaning that the malfunction in S1 can propagate to S2. If the two systems are linked by variables that are not deviated, then the propagation path is inactive and the dependent system cannot be affected by the malfunction in system S1.

For control systems with a single controlled and manipulated variable and passive systems with a single output (referred to here as single-variable or SV systems), propagation path status can be determined directly from knowledge of the system state. Conditional dependencies of SV systems are expressed in the process graph shown in Figure 3. Figure 3a shows S2 to be conditionally dependent on the controlled variable of S1, whereas Figure 3b shows S2 to be conditionally dependent on the manipulated variable of S1. If S2 were dependent on both controlled and manipulated variables of S1, it would be a case of unconditional dependence as depicted in Figure 1, assuming that S1 is an SV system. For diagnostic purposes, unconditional dependence is equivalent to manipulated variable dependence.

In light of the simplicity of SV systems, it is advantageous to decompose more complex systems into SV systems whenever possible. In the following example, such a decomposition is demonstrated on a cascade control system.

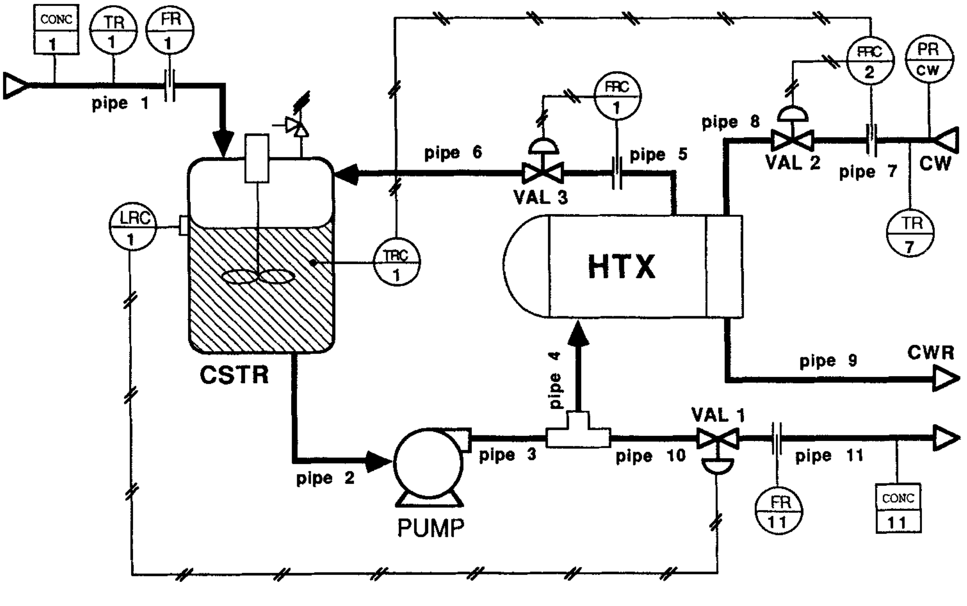

Figure 4. Flowsheet of stirred tank reactor with recycle.

Table 1. Unit Function Definitions

Function Designation	Unit Description	Function Description
U1-1	Pipe 1	Fluid conductance/containment
U2-1	Pipe 2	Fluid conductance/containment
U3-1	Pipe 3	Fluid conductance/containment
U4-1	Pipe 4	Fluid conductance/containment
U5-1	Pipe 5	Fluid conductance/containment
U6-1	Pipe 6	Fluid conductance/containment
U7-1	Pipe 7	Fluid conductance/containment
U8-1	Pipe 8	Fluid conductance/containment
U9-1	Pipe 9	Fluid conductance/containment
U10-1	Pipe 10	Fluid conductance/containment
U11-1	Pipe 11	Fluid conductance/containment
U12-1	Pump	Pressurization
U12-2		Fluid conductance/containment
U13-1	Reactor [CSTR]	Fluid containment
U13-2		Mixing
U13-3		Chemical reaction (catalysis)
U14-1	Heat exchanger [HTX]	Tube-side fluid containment
U14-2		Tube-side fluid conductance
U14-3		Shell-side fluid containment
U14-4		Shell-side fluid conductance
U14-5		Heat transfer
U15-1	Valve 1 [VAL 1]	Flow regulation
U15-2		Fluid conductance/containment
U16-1	Valve 2 [VAL 2]	Flow regulation
U16-2		Fluid conductance/containment
U17-1	Valve 3 [VAL 3]	Flow regulation
U17-2		Fluid conductance/containment
U18-1	Conc. sensor S_1	Measurement
U19-1	Flow sensor F_1	Measurement
U20-1	Temp. sensor T_1	Measurement
U21-1	Level sensor L_R	Measurement
U22-1	Temp. sensor T_R	Measurement
U23-1	Flow sensor F_5	Measurement
U24-1	Flow sensor F_7	Measurement
U25-1	Temp. sensor T_7	Measurement
U26-1	Conc. sensor S_{11}	Measurement
U27-1	Flow sensor F_{11}	Measurement
U28-1	Pres. sensor P_{cw}	Measurement
U29-1	Flow controller [FRC 1]	Computation
U30-1	Flow controller [FRC 2]	Computation
U31-1	Level controller [LRC]	Computation
U32-1	Temp. controller [TRC]	Computation

Table 2. System Definitions

Desig.	System Description	System Type
S1A	Reactor temperature control system	Control
S1B	Cooling water flow control system	Control
S2	Reactor level control system	Control
S3	Recycle flow rate control system	Control
S4	Chemical reaction system	Passive
S5A	Cooling water temperature system	External
S5B	Cooling water pressure system	External
S6A	Reactor feed flow rate system	External
S6B	Reactor feed temperature system	External
S6C	Reactor feed concentration system	External

Example 1

In this example, we present a functional decomposition for a reaction process comprised of a continuous stirred-tank reactor (CSTR) cooled by an external recycle stream as shown in Figure 4. The process objective is to indirectly maintain product concentration at a desired value by controlling temperature, residence time (level), and mixing conditions in the CSTR.

The first step in the functional decomposition of this process is the identification of all units and their respective unit functions. This is done in Table 1. In determining which functions of a unit are important, reasonable judgment must be used to distinguish important unit functions from unnecessary functions. For example, if heat loss from the CSTR were a potential problem, the "insulation" function of the reactor would be important. Here, heat loss is not considered a problem; therefore, this function is omitted.

Next, in Table 2, all process systems are identified with attention to system types. Control systems are easily recognized by their control loops. Note that the temperature control system, nominally a cascade control system, has been decomposed into

Table 3. System Composition

Function Designation	System Designation	Function Designation	System Designation
U1-1	S6A	U15-1	S2
U2-1	S2, S3	U15-2	S2, S3
U3-1	S2, S3	U16-1	S1B
U4-1	S2, S3	U16-2	S1B
U5-1	S2, S3	U17-1	S3
U6-1	S2, S3	U17-2	S2, S3
U7-1	S1B	U18-1	S6C
U8-1	S1B	U19-1	S6A
U9-1	S1B	U20-1	S6B
U10-1	S2, S3	U21-1	S2
U11-1	S2	U22-1	S1A
U12-1	S2, S3	U23-1	S3
U12-2	S2, S3	U24-1	S1B
U13-1	S2	U25-1	S5A
U13-2	S4	U26-1	S4
U13-3	S4	U27-1	S2
U14-1	S1A, S1B, S2, S3, S4	U28-1	S5B
U14-2	S1B	U29-1	S3
U14-3	S2, S3, S4	U30-1	S1B
U14-4	S2, S3	U31-1	S2
U14-5	S1A	U32-1	S1A

two SV control systems. This decomposition is contingent on the output signal of the temperature controller being available for diagnosis. This output, the set point for the cooling water flow control system, is the manipulated variable of the temperature control system.

An external system is defined for each external input variable. In this example, there are five external systems. Important process variables that are not directly regulated are typically outputs from passive systems. Here, the chemical reaction system is passive since output concentration is not directly regulated, but rather is indirectly controlled by the temperature and level control systems.

In Table 3, the unit functions are assigned to the various systems. This classification is primarily guided by Eq. 1. Namely, any unit function whose failure directly affects system function is assigned to the system set. Several characteristics of the process are apparent in Table 3, the most striking being the large number of unit functions shared by the level and recycle flow control systems, S2 and S3, respectively. This suggests a difficulty in making diagnostic distinctions between these systems.

In Figure 5, system dependencies are examined in a process graph. Shading indicates systems having nonempty intersections (i.e., systems with shared unit functions). System dependencies are identified by postulating system malfunction and determining which other systems are directly affected by the malfunction.

Diagnosis Procedure

After a logic model of the process has been developed, general diagnostic rules and procedures can be applied to identify malfunctioning systems and units. The diagnostic procedure presented here proceeds in two stages. First, a search is conducted to identify systems that are malfunction sources. Second, diagnostic rules are applied to identify which unit functions within a system are responsible for the malfunction. In this procedure, the single fault assumption is used to facilitate diagnosis.

Malfunction source identification

Because of interdependencies between systems, malfunction of one system can result in malfunction of other, dependent systems. In this way, a malfunction can propagate through a process with far-reaching effects. It is important at the beginning of the diagnosis to separate those systems that are malfunctioning due to failure of one or more of their unit functions (source systems) from those that are being affected through system dependencies. This is the problem of malfunction source identification.

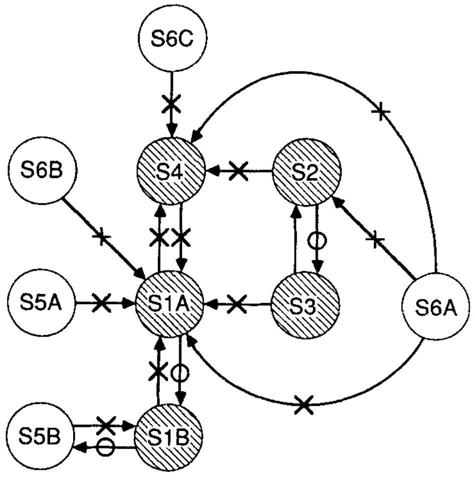

Figure 5. Process graph for stirred tank reactor system.

This problem is conceptually similar to the fault diagnosis problem in which signed directed graphs (SDG) are used to model the causal relationships between process variables (Iri et al., 1979, Shiozaki et al., 1985). In SDG-based techniques, the object is to separate those process variables that are deviated through direct action of the fault (root variables) from those that are deviated from the resulting disturbance as it propagates throughout the process. In our problem, the functional decomposition represented graphically as a network of systems and their conditional dependencies (i.e., the process graph) replaces the SDG, but the object remains to identify the system or systems directly affected by the fault.

The characteristics of the current problem that differ from the SDG are as follows:

1. The states of all nodes (systems) are assumed to be measured.

2. Arcs (propagation paths) are not "signed" but may be conditional on system states.

3. Two or more nodes can be affected simultaneously by a single unit function failure through system intersections.

4. A single fault may cause failure of multiple unit functions

Items 3 and 4 imply that a single source system cannot be assumed. We will now outline a method for determining source systems under these conditions.

The process graph shows all potential fault propagation pathways. In any given diagnostic situation, only a subset of these paths will be active. Therefore, the first step in the analysis of the process graph is to identify and eliminate from consideration all inactive propagation paths, as described above. The result is a new process graph specific to the current diagnosis problem. This new graph may be disconnected, consisting of one or more connected subgraphs. A malfunctional subgraph is defined as any connected subgraph containing one or more malfunctional systems. In subsequent analysis, only malfunctional subgraphs are important.

Trivial bounds on the number of source systems can be derived as follows:

$$B_L \leq N \leq B_U \tag{11}$$

where

N = number of source systems

B_L = number of malfunctional subgraphs

B_U = number of malfunctional systems

Reduction of the source system candidate set can be accomplished by applying the following criteria:

1. If a system is malfunctioning and there are no active propagation paths directed toward the system, then the system is a source system.

2. Under the single fault assumption, all source systems must contain unit functions of at least one common unit.

3. All malfunctioning nonsource systems within a single sub-

graph must be able to trace an active propagation path back to a source system.

There is no guarantee that these criteria will be sufficient to eliminate all spurious source system candidates. In situations where the size of the source system candidate set is greater than the number of malfunctional subgraphs, the possibility of spurious candidates cannot be excluded.

Unit malfunction identification

Under the single fault assumption, and assuming that a source system has been identified, it is often possible to further narrow the diagnosis from the complete set of unit functions of the system to a subset of the unit functions using detailed diagnostic rules. This additional fault discrimination is accomplished using the state of the source system and the observed effects produced on systems connected to the source system through either system dependencies or shared functions. This stage of the diagnosis uses generalized fault simulation to develop patterns of system states that can be expected to be observed for various classes of unit function failure.

The unit functions that comprise a control system can be subdivided into three broad classifications: control apparatus functions, sensing functions, and process functions. The control apparatus functions include all the unit functions of the controller and final control element (e.g., the valve). Sensing functions refer to the functions of the sensors and can be further divided into control-loop sensing functions and noncontrol sensing functions. Control-loop sensing functions are defined as those sensing functions that provide signals to the controller. Process functions include all other unit functions not associated with the control apparatus or sensors. Passive and external system functions can be subdivided similarly, except in the absence of a closed control loop; these systems lack control apparatus functions and control-loop sensing functions.

As presented, these classifications are quite abstract. In practice, each category typically includes only a small number of unit functions; therefore, directing diagnostic focus to one of these categories often improves the diagnosis significantly. The motivation for using abstract rather than system-specific unit function classifications is that the resulting diagnostic rules are general.

The diagnostic rules were derived by first developing a list of generic system faults. An example of such a list developed for control systems is presented in appendix A. Because of the generalized nature of the classifications, a relatively short list can account for the large majority of faults. For example, the first two faults listed—controllable and uncontrollable process function failure—are sufficient to account for all process (noncontrol, nonsensor) failures since controllability is the only parameter that affects the system state in the presence of these failures. A similar list, also presented in appendix A, is developed for passive and external systems.

The effects of each generalized fault on its host system and other systems with which the host interacts were then predicted in terms of the possible resulting system states. Inverting these data produced diagnostic rules mapping system states to potential fault candidates. Using this technique, a complete diagnostic rule-base was developed using the general faults listed in appendix A. This rule-base is presented in appendix B. Appendix B is based on pairwise simulation of interacting systems and assumes that a fault exists in one of the two systems considered (i.e., one of the two systems is a definite source system). If the source system interacts with several other systems, the rule-base is consulted for each source system/neighbor system combination.

Example 2

In this example, we use the decomposition presented in example 1 to perform a systems diagnosis for the recycle CSTR process. The first step is to introduce a fault. For this example, the fault will be partial blockage of pipe 3 resulting in inadequate recycle flow. The diagnosis starts when a system malfunction resulting from this fault is detected. This requires computation of δ's for the various process systems to determine if any significant deviations exist. Since all systems in the present example are SV systems, no weighting factors are necessary.

After significant deviations have been determined, system states are as shown in Table 4. Elimination of functional systems and inactive propagation paths produces a situation-specific process graph as shown in Figure 6. For this example, only a single malfunctional subgraph is present.

Applying Eq. 11, it is determined that there is at least one and at most four source systems. Invoking the single fault assumption does not immediately reduce the set of possible source systems since all four malfunctioning systems contain functions of the heat exchanger. However, the single fault assumption does allow some distinction to be made between the systems. For example, it is clear that neither system S1A nor system S1B could be the sole source system since no active propagation paths exist from these systems to systems S2 or S3. Therefore, either system S2 or S3 is a definite source system, whereas, systems S1A and S1B are only possible source systems. In general, three situations can arise with respect to source system classification:

1. If a single definite source system is identified, then under the single fault assumption the fault can be captured by examination of the definite source system, ignoring all other possible source systems.

2. If two or more definite source systems are identified, then under the single fault assumption the fault is captured by sequentially examining each definite source system and taking the intersection of the resulting candidate unit function failures.

3. If no definite source systems are identified, then under the single fault assumption the fault is captured only by sequentially examining all possible source systems and taking the union of the resulting candidate unit function failures.

From these conditions, it is clear that failure discrimination is

Table 4. System States

System Desig.	System State
S1A	Stressed
S1B	Stressed
S2	Stressed
S3	Saturated
S4	Functional
S5A	Functional
S5B	Functional
S6A	Functional
S6B	Functional
S6C	Functional

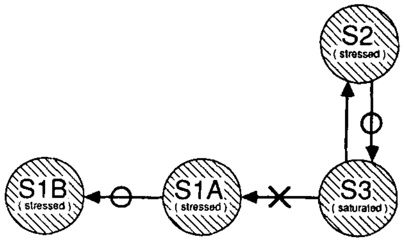

Figure 6. Malfunctional subgraph for example 2.

enhanced by maximizing the number of definite source systems identified.

In this instance, it is not possible to deduce with certainty whether system S2 or S3 is a source system. However, because systems S2 and S3 directly interact, the rules in appendix B can still be applied to analyze the interaction between these systems.

In Table B1, the interaction between systems S2 and S3 is determined to be mode *G*. This interaction mode is based on the dependencies in the original process graph, not the malfunctional subgraph. The appropriate diagnostic rules for two interacting control systems are given in Table B4. Using the known system states and the mode of system interaction, the diagnosis is narrowed to the following candidate unit function failures:

1. Process function failure of system S2 or S3
2. Control-loop sensing function failure of system S2 or S3
3. Control apparatus function failure of system S3

The actual failure is a process function failure of systems S2 and S3. Table 5 lists the unit functions that are implicated by the diagnosis.

Discussion

In this paper we have presented a method of diagnosis for chemical plants that considers the plant at the level of functional systems. The utility of abstraction at this level is to permit diagnostic focus to be quickly narrowed to the point where detailed investigations are feasible. We have concentrated on the issue of functional abstraction, neglecting structural abstraction by making exclusive use of the process units to represent structure. This choice of structural abstraction level was made implicitly by defining unit functions as the base elements of the functional decomposition. It should be noted, however, that other levels of structural abstraction can be incorporated into the functional decomposition directly or can be appended to the diagnostic procedure.

Table 5. Malfunction Candidates

Units	Unit Functions
Pipe 2	U2-1
Pipe 3	U3-1
Pipe 4	U4-1
Pipe 5	U5-1
Pipe 6	U6-1
Pipe 10	U10-1
Pipe 11	U11-1
Pump	U12-1/U12-2
Reactor	U13-1
Heat exchanger	U14-1/U14-3/U14-4
Valve 1	U15-1/U15-2
Valve 3	U17-1/U17-2
Level sensor	U21-1
Flow sensor	U23-1
Flow controller	U28-1

In example 1, we decomposed the process using the process units as the basic element of process structure. Alternative structural representations can be derived by defining structural entities such as "recycle flow path" or "cooling water flow path." These entities represent a higher order of structural abstraction that may be desirable in some diagnostic situations. To functionally decompose the process using these structural entities, we can define composite functions analogous to unit functions. In this case, the composite function of a flow path is fluid conductance/containment. Using this representation, all fluid conductance/containment functions of the individual units that comprise the flow path collapse into the flow path composite function. For example, in Table 5, the CSTR, pump, heat exchanger, valve 3, and pipes 2, 3, 4, 5, and 6 can be recognized as the recycle flow path; therefore, the fluid conductance/containment functions of these units can be collapsed into the recycle flow path fluid conductance/containment function. The result is a more concise listing of malfunction candidates in terms that are more easily interpreted by the operator. The use of structural abstraction is an interesting topic to be left for future research.

For simplicity, our discussion has emphasized the applications of the functional decomposition and its associated diagnostic procedure to continuous processes in steady state operation. The concepts presented are not limited to such processes. Process dynamics can be incorporated into the diagnostic method by using more sophisticated reference values in the computation of system states. For example, in Eq. 3 control system set points are used as reference values in determining δ_c. These reference values, valid under steady state conditions, are erroneous immediately after a set point change or similar anticipated transient. Under such conditions, a more descriptive control system reference is required. Equation 3 can be replaced by

$$\delta_c = \underline{\beta}_c^T \cdot |\underline{C} - \underline{C}_e| \tag{12}$$

where $\underline{C}_e$ = vector of expected controlled variable values.

Here, $\underline{C}_e$ models the dynamic behavior of the system and is functionally dependent on time, $\underline{C}_{sp}$, and prior operating state. $\underline{C}_e$ asymptotically approaches $\underline{C}_{sp}$ at long times. Equation 12

Table B1. Interaction Modes for Two Interacting Systems

Mode	System 1 Dependent on	System 2 Dependent on
A	None	None
B	None	Controlled var. of S1
C	Controlled var. of S2	None
D	None	Manipulated var. of S1
E	Manipulated var. of S2	None
F	Controlled var. of S2	Controlled var. of S1
G	Manipulated var. of S2	Manipulated var. of S1
H	Controlled var. of S2	Manipulated var. of S1
I	Manipulated var. of S2	Controlled var. of S1

Unconditional dependence is treated as manipulated variable dependence for diagnostic purposes

Table B2. Rules for Malfunction Diagnosis of Two Interacting Passive Systems

System 1	System 2	Candidate Malfunctions†	Modes*
Functioning	Functioning	None/LNT	All
Functioning	Malfunctioning	PRC2/SEN2	All
Malfunctioning	Functioning	PRC1/SEN1	All
Malfunctioning	Malfunctioning	PRC1 ∩ PRC2	A
Malfunctioning	Malfunctioning	PRC1	B
Malfunctioning	Malfunctioning	PRC1/PRC2	F

*All: interaction modes A, B, F; mode C is redundant with mode B and is not included

†None: no malfunction
LNT: latent (undetectable) malfunction
Null: no single fault explanation
PRC1: malfunction in process functions of system 1
PRC2: malfunction in process functions of system 2
SEN1: malfunction in sensing functions of system 1
SEN1: malfunction in sensing functions of system 2
CSEN1: malfunction in control-loop sensing functions of system 1
CSEN2: malfunction in control-loop sensing functions of system 2
CNT1: malfunction in control functions of system 1
CNT2: malfunction in control functions of system 2
PRC1 ∩ PRC2: malfunction in process functions common to systems 1 and 2
For SV systems the following assumptions hold: SEN1 ∩ SEN2 = CNT1 ∩ CNT2 = ϕ

allows the diagnostic system to account for the expected deviations from steady state conditions that occur normally during process changeovers. Analogous time-dependent functions for $\underline{M}_e$ and $\underline{P}_e$ must be used for calculation of δ_m and δ_p. In the absence of dynamic models for $\underline{C}_e$, $\underline{M}_e$, and $\underline{P}_e$, steady state models can be used with the understanding that diagnosis must be suspended when the process is not at steady state to avoid false alarms. In principle, given appropriate reference values, even batch processes should be addressable by this diagnostic procedure.

Acknowledgment

The authors gratefully acknowledge the financial support of this work by the National Science Foundation, Grant No. CBT-8605253.

Notation

B_L = lower bound on source system candidate set
B_U = upper bound on source system candidate set
$\underline{C}$ = vector of controlled variable measurements
$\underline{C}_e$ = vector of expected controlled variable values
$\underline{C}_{sp}$ = vector of controller set points for a single controller
$\underline{\underline{C}}_{sp}$ = matrix of controller set points for all controllers
$\underline{d}_s$ = vector of measured process inputs and disturbances
$\underline{d}_u$ = vector of unmeasured process inputs and disturbances
$\underline{g}^1$ = controller model function
$\underline{g}^2$ = process model function
$\underline{M}$ = vector of manipulated variable measurements for a single controller
$\underline{\underline{M}}$ = matrix of manipulated variable measurements for all controllers
$\underline{M}_e$ = vector of expected manipulated variable values for a single controller
$\underline{\underline{M}}_e$ = matrix of expected manipulated variable values for all controllers
N = number of source systems
$\underline{P}$ = vector of passive system output variable measurements
$\underline{P}_e$ = vector of expected passive system output variable values
S_k = system k, Eq. 1
U_{ij} = unit function j of unit i

Greek letters

α = threshold value for system state determination
$\underline{\beta}_c, \underline{\beta}_m, \underline{\beta}_p$ = adjustable weighting factor vectors
$\delta_c, \delta_m, \delta_p, \delta_x$ = "error" values used in system state determination
θ = belief function
ϕ = null set

Symbols

ϵ = element of
$\cap$ = intersection

Appendix A: Generalized Fault Lists

Control System Faults

1. Controllable process unit function failure
2. Uncontrollable process unit function failure
3. Controller not responding to input signals
4. Controller sending inappropriate response to input

Table B3. Rules for Malfunction Diagnosis of Interacting Passive and Control Systems

System 1 Passive	System 2 Control	Candidate Malfunctions†	Modes*
Functioning	Functioning	None/LNT	All
Functioning	Uncontrolled	CNT2	All
Functioning	Stressed	PRC2/SEN1/SEN2/CNT2	All
Functioning	Saturated	PRC2/CSEN2/CNT2	All
Malfunctioning	Functioning	PRC1/SEN1/SEN2	All
Malfunctioning	Uncontrolled	Null	A/B
Malfunctioning	Uncontrolled	CNT2	C/E/F/I
Malfunctioning	Stressed	PRC1 ∩ PRC2	A
Malfunctioning	Stressed	PRC1	B
Malfunctioning	Stressed	PRC1 ∩ PRC2/CSEN2/CNT2	C
Malfunctioning	Stressed	PRC2/CSEN2/CNT2	E
Malfunctioning	Stressed	PRC1/CSEN2/CNT2	F
Malfunctioning	Stressed	PRC1/PRC2/CSEN2/CNT2	I
Malfunctioning	Saturated	PRC1 ∩ PRC2	A
Malfunctioning	Saturated	PRC1	B
Malfunctioning	Saturated	PRC2/CSEN2/CNT2	C/E
Malfunctioning	Saturated	PRC1/PRC2/CSEN2/CNT2	F/I

*All: interaction modes A, B, C, E, F, I
†Abbreviations as in Table B2 notes

5. Valve (final control element) stuck in normal position
6. Valve (final control element) stuck in abnormal position
7. Controlled variable sensor failed normal
8. Controlled variable sensor failed abnormal and controllable
9. Controlled variable sensor failed abnormal and uncontrollable
10. Manipulated variable sensor failed normal
11. Manipulated variable sensor failed abnormal

Passive (external) system faults

1. Process unit function failure
2. Sensor failed normal
3. Sensor failed abnormal

Appendix B: Rules for Malfunction Diagnosis of Single-Variable Systems

Table B1 defines the nine different interaction modes that can exist between two conditionally dependent SV systems. The first step in using this appendix is to determine which interaction mode exists between the two systems under consideration. If the two systems are of mixed type (i.e., one control system and one passive system) let the passive system be System 1 and the control system be System 2.

In Tables B2, B3, and B4 the diagnostic rules are presented for the three possible combinations of system types. Having located the table appropriate for the system pair under consideration and the section of the table corresponding to the observed states of the systems, the Candidate Malfunctions column lists

Table B4. Rules for Malfunction Diagnosis of Two Interacting Control Systems

System 1	System 2	Candidate Malfunctions†	Modes*
Functioning	Functioning	None/LNT	All
Functioning	Uncontrolled	CNT2	All
Functioning	Stressed	PRC2/SEN2	A
Functioning	Stressed	PRC2/CSEN1/SEN2	B/F/I
Functioning	Stressed	PRC2/CSEN1/SEN2/CNT1	D/G
Functioning	Saturated	PRC2/CSEN2/CNT2	A
Functioning	Saturated	PRC2/CSEN1/CSEN2/CNT2	B/F/I
Functioning	Saturated	PRC2/CSEN1/CSEN2/CNT1/CNT2	D/G
Uncontrolled	Functioning	CNT1	All
Uncontrolled	Uncontrolled	Null	All
Uncontrolled	Stressed	Null	A
Uncontrolled	Stressed	CNT1	Dep.
Uncontrolled	Saturated	Null	A
Uncontrolled	Saturated	CNT1	Dep.
Stressed	Functioning	PRC1/SEN1	A/B/D
Stressed	Functioning	PRC1/SEN1/CSEN2	F
Stressed	Functioning	PRC1/SEN1/CSEN2/CNT2	I/G
Stressed	Uncontrolled	Null	A/B/D
Stressed	Uncontrolled	CNT2	F/I/G
Stressed	Stressed	PRC1 $\cap$ PRC2	A
Stressed	Stressed	PRC1 $\cap$ PRC2/CSEN1	B
Stressed	Stressed	PRC1/CSEN1	D
Stressed	Stressed	PRC1 $\cap$ PRC2/CSEN1/CSEN2	F
Stressed	Stressed	PRC2/CSEN1/CSEN2	I
Stressed	Stressed	PRC1/PRC2/CSEN1/CSEN2	G
Stressed	Saturated	PRC1 $\cap$ PRC2	A
Stressed	Saturated	PRC1 $\cap$ PRC2/CSEN1	B
Stressed	Saturated	PRC1/CSEN1	D
Stressed	Saturated	PRC2/CSEN1/CSEN2/CNT2	F/I
Stressed	Saturated	PRC1/PRC2/CSEN1/CSEN2/CNT2	G
Saturated	Functioning	PRC1/CSEN1/CNT1	A/B/D
Saturated	Functioning	PRC1/CSEN1/CSEN2/CNT1	F
Saturated	Functioning	PRC1/CSEN1/CSEN2/CNT1/CNT2	I/G
Saturated	Uncontrolled	Null	A/B/D
Saturated	Uncontrolled	CNT2	F/I/G
Saturated	Stressed	PRC1 $\cap$ PRC2	A
Saturated	Stressed	PRC1/CSEN1/CNT1	B/D/F
Saturated	Stressed	PRC1/PRC2/CSEN1/CSEN2/CNT1	I/G
Saturated	Saturated	PRC1 $\cap$ PRC2	A
Saturated	Saturated	PRC1/CSEN1/CNT1	B/D
Saturated	Saturated	PRC1/PRC2/CSEN1/CSEN2/CNT1/ CNT2	F/I/G

*All: interaction modes A, B, D, F, G, I
Dep.: dependent interaction modes B, D, F, G, I
Modes C, E, H are redundant with modes B, D, I, respectively, and not included
†Abbreviations as in Table B2 notes

the possible unit function failures that could result in the observed system states. In some cases, there will be several unit function groupings listed. It is then necessary to use the group that corresponds to the correct interaction mode as defined in Table B1.

Literature Cited

Davis, R., "Diagnostic Reasoning Based on Structure and Behavior," *Qualitative Reasoning About Physical Systems,* D.G. Bobrow, ed., Elsevier, Amsterdam (1984).

Himmelblau, D. M., *Fault Detection and Diagnosis in Chemical and Petrochemical Processes,* Elsevier, Amsterdam (1978).

Iri, M., K. Aoki, E. O'Shima, and H. Matsuyama, "An Algorithm for Diagnosis of System Failures in the Chemical Process," *Comp. Chem. Eng.,* **3,** 489 (1979).

Keravnou, E. T., and L. Johnson, *Competent Expert Systems,* McGraw-Hill, New York (1986).

Kramer, M. A., "Integration of Heuristic and Model-Based Inference in Chemical Process Fault Diagnosis," IFAC Workshop: Fault Detection and Safety in Chemical Plants, Kyoto (1986).

———, "Malfunction Diagnosis Using Quantitative Models with Non-Boolean Reasoning in Expert Systems," *AIChE J.,* **33,** 130 (1987).

Moore, R. L., L. B. Hawkinson, C. G. Knickerbocker, and L. M. Churchman, "A Real-Time Expert System for Process Control," *IEEE Proc. 1st Conf. Artificial Intelligence Applications,* 569 (1984).

Rasmussen, J., "The Role of Hierarchical Knowledge Repesentation in Decisionmaking and System Management," *IEEE Trans. Systems, Man, Cybernetics,* **SMC-15**(2), 234 (1985).

Shafaghi, A., P. K. Andow, and F. P. Lees, "Fault Tree Synthesis Based on Control Loop Structure," *Chem. Eng. Res. Des.,* **62,** 101 (1984).

Shafer, G., *A Mathematical Theory of Evidence,* Princeton (1976).

Shiozaki, J., H. Matsuyama, E., O'Shima, and M. Iri, "An Improved Algorithm for Diagnosis of System Failures in the Chemical Process," *Comp. Chem. Eng.,* **9,** 285 (1985).

Shum, S. K., J. F. Davis, W. F. Punch III, and B. Chandrasekaran, "An Expert System for Diagnosing Process Plant Malfunctions," IFAC Workshop: Fault Detection and Safety in Chemical Plants, Kyoto (1986).

Zadeh, L. A., "Fuzzy Sets," *Inf. Control,* **8,** 338 (1965).

Manuscript received Dec. 11, 1986, and revision received June 10, 1987.