JPL Publication 91-6

Diagnostic Reasoning Techniques for Selective Monitoring

L. S. Homem-de-Mello
R. J. Doyle

March 1, 1991

NASA
National Aeronautics and
Space Administration

Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

JPL Publication 91-6

Diagnostic Reasoning Techniques for Selective Monitoring

L. S. Homem-de-Mello
R. J. Doyle

March 1, 1991

NASA

National Aeronautics and
Space Administration

Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

The research described in this publication was carried out by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement by the United States Government or the Jet Propulsion Laboratory, California Institute of Technology.

Abstract

This publication presents an architecture for using diagnostic reasoning techniques in selective monitoring. Given the sensor readings and a model of the physical system, a number of assertions are generated and expressed as Boolean equations. The resulting system of Boolean equations is solved symbolically. Using a priori probabilities of component failure and Bayes' rule, revised probabilities of failure can be computed. These will indicate what components have failed or are the most likely to have failed. This approach is suitable for systems that are well understood and for which the correctness of the assertions can be guaranteed. Also, the system must be such that assertions can be made from instantaneous measurements. And the system must be such that changes are slow enough to allow the computation.

Contents

Appendixes

List of Figures

1 Introduction

Complex physical systems can be difficult to monitor because the number of sensor signals may exceed the human operators' ability to handle them.

One solution to managing overwhelming amounts of sensory information is the use of computer aids that preprocess the incoming data and direct the operators' attention to the most critical parts of the physical system at any given time. Causal reasoning [10] and information quantification [11] are examples of techniques that lead to computer aids to selective monitoring.

Diagnostic reasoning techniques can also be used to preprocess the sensor data and detect which parts of the physical system require more attention because components have failed or are most likely to have failed.

This publication presents an architecture for using diagnostic reasoning techniques in selective monitoring. The diagnosis process starts with the generation of as many assertions as possible, given the sensory information. These assertions are expressed as Boolean equations and are combined, symbolically, into a simplified disjoint sum form. Using a priori probabilities of failure for each component and Bayes' rule, revised probabilities of failure are computed. These are then used to focus the operators' attention on those components known to have failed or which are most likely to have failed. This method is robust in the sense that even when a priori probabilities are not accurate, if there is enough evidence showing that a component has or has not failed, the value computed for the revised probability of failure will be 1 or 0, respectively. It has the advantage of decoupling diagnostic reasoning into the generation of assertions and inference. The latter can be seen as solving a set of Boolean equations for what the well-developed machinery of Boolean algebra can be used. This method is suitable for physical systems that are well understood and for which accurate models exist.

The Boolean representation is only used for the inference. The generation of assertions still requires more powerful tools which can be either reason maintenance systems or domain-dependent methods. The latter seems to be more effective in domains that are well understood and for which good theories exist.

2 Approach

Consider a physical system Σ made up of C interconnected components, $c_1, c_2, \cdots, c_C$.

Figure 1 shows the diagnosis module of the selective monitoring system. The inputs include the sensor readings, a model of Σ, and the (a priori) probabilities of component failures. The output is the set of revised probabilities of component failure given the evidence that can be deduced from the sensor readings.

Let d_i be a logical variable that indicates the status of component c_i. It is true (T) if c_i is faulty and false (F) otherwise. In this analysis, a component is considered faulty if and only if it exhibits anomalous behavior. From the point of view of monitoring what is important is whether or not the physical system is working properly at any given time.

Let N be the number of sensors in Σ and $s_1, s_2, \cdots, s_N$ their values at a given time.

An analysis of the sensor values, using a model of Σ, allows I assertions about the status of the components to be made. The method of analysis may be different from one domain to another. It is assumed that all assertions are correct. Although it is not necessary that the set of assertions be complete, that is that all correct assertions be made, the more assertions the better the conclusions that will be drawn.

Regardless of which method is used for the analysis, each assertion can be expressed as a Boolean equation $f_i(d_1, d_2, \cdots, d_C) = \mathrm{T}$. Therefore, the set of all assertions is a system of Boolean equations. The conjunction of all equations must also be satisfied, that is

$$\prod_{i=1}^{I} f_i(d_1, d_2, \cdots, d_C) = \mathrm{T} \qquad (1)$$

where the product is the logical operation AND[1]. Equation 1 can be rewritten in disjunctive normal form [12] as

[1] In this publication, products and sums are used as both arithmetic and logical operations. It will be clear from context which is which.

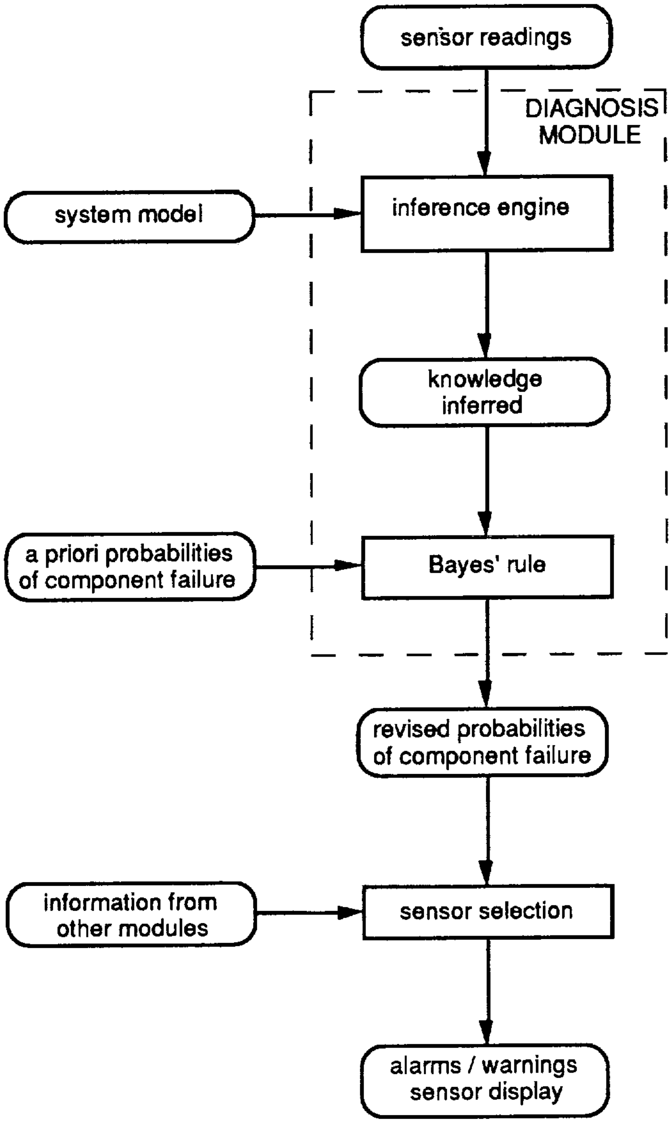
sensor readings
DIAGNOSIS MODULE
system model
inference engine
knowledge inferred
a priori probabilities of component failure
Bayes' rule
revised probabilities of component failure
information from other modules
sensor selection
alarms / warnings sensor display

Figure 1: The diagnosis module of the selective monitoring system

$$\sum_{j=0}^{2^C-1} \prod_{k=0}^{C-1} \gamma_{j\,k} \cdot e_j \;=\; \mathrm{T} \tag{K}$$

where

$$\gamma_{j\,k} \;=\; \begin{cases} d_{k+1} & \text{if } b_{j\,k} = 1 \\ \overline{d_{k+1}} & \text{if } b_{j\,k} = 0 \end{cases}$$

with $(b_{j\,(C-1)}\, b_{j\,(C-2)} \cdots b_{j\,0})_2$ being the binary representation of j. As in equation 1, a product is the logical operation AND; a sum is the logical operation OR. The logical variable e_j is either T or F depending on whether or not the conjunction $\prod_{k=0}^{C-1} \gamma_{j\,k}$ appears in the disjunctive normal form of equation 1.

Equation K summarizes what has been asserted about Σ given the sensor readings and the system model, and using the available analysis tools. Equation K can be represented by the integer Θ whose binary representation is $(\theta_{2^C-1}\, \theta_{2^C-2} \cdots \theta_0)_2$, where

$$\theta_j \;=\; \begin{cases} 0 & \text{if } e_j \;= \mathrm{F} \\ 1 & \text{if } e_j \;= \mathrm{T} \end{cases} \tag{2}$$

Let $p(c_i)$ be the (a priori) probability of failure for component c_i. It is assumed that $p(c_1), p(c_2), \cdots, p(c_C)$ are independent. Let $p(c_i|K)$ be the conditional probability of failure for c_i given that equation K is satisfied. From Bayes' rule:

$$p(c_i|K) \;=\; \frac{p(K|c_i) \cdot p(c_i)}{p(K)} \tag{3}$$

where $p(K|c_i)$ is the conditional probability that equation K is satisfied given the failure of c_i, and $p(K)$ is the (a priori) probability that equation K is satisfied.

Since it was assumed that $p(c_1), p(c_2), \cdots, p(c_C)$ are independent, it is straightforward to compute the (a priori) probability that equation K is satisfied:

$$p(K) \;=\; \sum_{j=0}^{2^C-1} \left[\left(\prod_{k=0}^{C-1} \rho_{j\,k} \right) \cdot \theta_j \right] \tag{4}$$

where

$$\rho_{j\,k} = \begin{cases} p(c_{k+1}) & \text{if } b_{j\,k} = 1 \\ & \text{(i.e., if } \gamma_{j\,k} = d_{k+1}\text{)} \\ 1 - p(c_{k+1}) & \text{if } b_{j\,k} = 0 \\ & \text{(i.e., if } \gamma_{j\,k} = \overline{d_{k+1}}\text{)} \end{cases} \tag{5}$$

with $(b_{j\,(C-1)}\, b_{j\,(C-2)} \cdots b_{j\,0})_2$ being the binary representation of j, and θ_j being as defined in equation 2.

Similarly, it is straightforward to compute the conditional probability that equation K is satisfied given the failure of component c_i:

$$p(K|c_i) = \sum_{j \in C_i} \Big[\Big(\prod_{\substack{k=0 \\ k \neq i}}^{C-1} \rho_{j\,k} \Big) \cdot \theta_j \Big] \tag{6}$$

where $C_i = \{j \mid [b_{j\,i} = 1]\}$, $(b_{j\,(C-1)}\, b_{j\,(C-2)} \cdots b_{j\,0})_2$ is the binary representation of j, $\rho_{j\,k}$ is defined in equation 5, and θ_j is defined in equation 2.

With the probabilities $p(c_i)$, $p(K)$, and $p(K|c_i)$, it is possible to compute $p(c_i|K)$ (the conditional probability of failure for c_i given that equation K is satisfied) by using equation 3.

3 Implementation issues

The approach outlined in the previous section requires the a priori probabilities of failure for each component. These can be obtained from the manufacturers or from previous experience [17]. It should be noted that the approach is robust in the sense that even when the a priori probabilities are not accurate, if equation K contains enough evidence to conclude that component c_i has failed, the value computed for $p(c_i|K)$ will be 1.

In practice, the computation of equations 4 and 6 need not be carried out going over all the 2^C terms for the summation. Only the terms for which θ_j is 1 will be added. A table computed off-line can store for each Θ a list of the terms that should be added. Furthermore, the products in equations 4 and 6 can be computed in parallel.

Further gains in computational efficiency are possible if equation 1 is written in simplified *disjoint sum form* [2,13], instead of disjunctive normal form, that is[2]

$$\sum_{j=0}^{D} g_j(d_1, d_2, \cdots, d_C) \;=\; \mathrm{T} \qquad (K')$$

where $g_j(d_1, d_2, \cdots, d_C)$ is a conjunction of (not necessarily all) the logical variables $d_1, d_2, \cdots, d_C$, some of which may be negated, and

$$a \neq b \;\; \Rightarrow \;\; g_a(d_1, d_2, \cdots, d_C) \cdot g_b(d_1, d_2, \cdots, d_C) \;=\; \mathrm{F}.$$

Equation K' is a disjunction of $D+1$ conjunctions. Equations K and K' are equivalent, but in most cases the latter includes fewer (i.e., $D+1 \leq 2^C$) and shorter terms. Equation K' can be computed by symbolic manipulation of equation 1.

As in equation 4, it is straightforward to compute the (a priori) probability that equation K' is satisfied:

$$p(K') \;=\; \sum_{j=0}^{D} \prod_{k \in \mathcal{K}'_j} \rho'_{j\,k} \qquad (7)$$

where $\mathcal{K}'_j = \{k \mid d_k \text{ or } \overline{d_k} \text{ is in } g_j\}$, and

$$\rho'_{j\,k} \;=\; \begin{cases} p(c_{k+1}) & \text{if } d_{k+1} \text{ is in } g_j \\ 1 - p(c_{k+1}) & \text{if } \overline{d_{k+1}} \text{ is in } g_j \end{cases} \qquad (8)$$

Similarly, as in equation 6, it is straightforward to compute the conditional probability that equation K' is satisfied given the failure of component c_i:

$$p(K'|c_i) \;=\; \sum_{j \in \mathcal{J}_i} \prod_{\substack{k \in \mathcal{K}'_j \\ k \neq i}} \rho'_{j\,k} \qquad (9)$$

where $\mathcal{J}_i = \{j \mid [0 \leq j \leq D] \wedge [\overline{d_i} \text{ is not in } g_j]\}$. $\mathcal{K}'_j$ and $\rho'_{j\,k}$ are the same defined above.

[2] Unlike the disjunctive normal form, the disjoint sum forms are not unique. The same logical function can have more than one disjoint sum form.

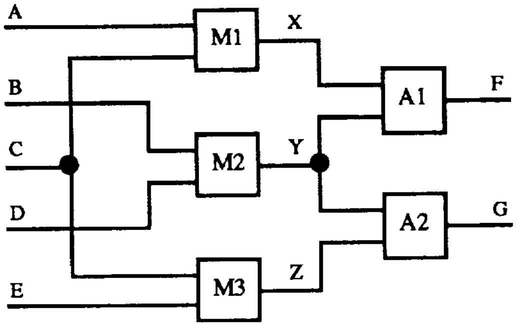

Figure 2: A digital circuit example

As before, with the probabilities $p(c_i)$, $p(K')$, and $p(K'|c_i)$, it is possible to compute $p(c_i|K)$ (the conditional probability of failure for c_i given that equation K' is satisfied) by using equation 3. If equation K' contains enough evidence to conclude that component c_i has failed, the value computed for $p(c_i|K)$ will be 1.

4 Digital circuit example

Figure 2 shows one digital circuit that has been used in previous work on automatic diagnosis [4,6]. It has five inputs and two outputs. The circuit's inputs are connected to the inputs of three multipliers. The outputs of the multipliers are connected to the inputs of two adders. The outputs of the two adders are the circuit's outputs.

Suppose that the circuit is being monitored and that sensors have been placed at the five inputs and at the two outputs.

Let m_1, m_2, m_3, a_1, a_2 be the logical variables that indicate the status of components M1, M2, M3, A1, A2, respectively. For a full correspondence with the notation used in the previous sections let $d_1 = m_1$, $d_2 = m_2$, $d_3 = m_3$, $d_4 = m_1$, $d_5 = a_2$.

Upon measuring A = 3, B = 2, C = 2, D = 3, E = 3, F = 10, and

G = 12, the following assertions can be made[3]:

$$m_1 + m_2 + a_1 = \mathrm{T} \tag{10}$$

which says that M1 is faulty or[4] M2 is faulty or A1 is faulty,

$$m_1 + m_3 + a_1 + a_2 = \mathrm{T} \tag{11}$$

which says that M1 is faulty or M3 is faulty or A1 is faulty or A2 is faulty, and

$$\overline{m_2} \cdot \overline{m_3} \cdot \overline{a_2} + m_2 \cdot m_3 + m_2 \cdot a_2 + m_3 \cdot a_2 = \mathrm{T} \tag{12}$$

which says that there cannot be only one of M2, M3, A2 failing; or, equivalently, either M2, M3, and A2 are not faulty, or at least two of them are faulty. It should be noted that this last assertion was not made in previous work [8], because it is domain-dependent, and also because in previous work if a component does not exhibit anomalous behavior nothing can be asserted[5].

The three assertions 10 to 12 can be combined, yielding

$$\begin{aligned} &(m_1 + m_2 + a_1) \cdot (m_1 + m_3 + a_1 + a_2) \\ &\cdot (\overline{m_2} \cdot \overline{m_3} \cdot \overline{a_2} + m_2 \cdot m_3 + m_2 \cdot a_2 + m_3 \cdot a_2) = \mathrm{T} \end{aligned}$$

whose disjoint sum form is

$$\begin{aligned} &m_2 \cdot a_2 + m_1 \cdot \overline{m_2} \cdot \overline{m_3} \cdot \overline{a_1} \cdot \overline{a_2} \\ &+ m_2 \cdot m_3 \cdot \overline{a_2} + m_1 \cdot \overline{m_2} \cdot m_3 \cdot \overline{a_1} \cdot a_2 \\ &+ \overline{m_2} \cdot m_3 \cdot a_1 \cdot a_2 + \overline{m_2} \cdot \overline{m_3} \cdot a_1 \cdot \overline{a_2} = \mathrm{T} \end{aligned} \tag{13}$$

Assuming that the (a priori) probabilities of failure for all components, $p(m_1)$, $p(m_2)$, $p(m_3)$, $p(a_1)$, and $p(a_2)$ are equal to 0.01, the a priori probability that equation 13 is satisfied (see equation 7) is:

$$\begin{aligned} p(\mathit{13}) &= 0.01^2 + 0.01 \cdot 0.99^4 + \\ &\quad 0.01^2 \cdot 0.99 + 0.01^3 \cdot 0.99^2 + \\ &\quad 0.01^3 \cdot 0.99 + 0.01 \cdot 0.99^3 \end{aligned}$$

[3] See appendix A for how these assertions can be generated automatically.

[4] The *or* is inclusive.

[5] As mentioned in section 2, in the approach presented in this publication, if a component does not exhibit anomalous behavior, it is assumed to be not faulty.

The conditional probability that equation 13 is satisfied given the failure of M1 (see equation 9) is:

$$\begin{aligned} p(\mathit{13}|\,m_1) &= 0.01^2 + 0.99^4 + \\ & \quad 0.01^2 \cdot 0.99 + 0.01^2 \cdot 0.99^2 + \\ & \quad 0.01^3 \cdot 0.99 + 0.01 \cdot 0.99^3 \end{aligned}$$

The conditional probability of failure for M1 given that equation 13 is satisfied can be computed from Bayes' rule (see equation 3):

$$p(m_1 \,|\, \mathit{13}) = \frac{p(\mathit{13}|\,m_1) \cdot p(m_1)}{p(\mathit{13})} = 0.497$$

Similarly, the conditional probabilities of failure for the other components, given that equation 13 is satisfied, are:

$$\begin{array}{rclcrcl} p(m_2 \,|\, \mathit{13}) &=& 0.010 & \qquad & p(m_3 \,|\, \mathit{13}) &=& 0.005 \\ p(a_1 \,|\, \mathit{13}) &=& 0.497 & \qquad & p(a_2 \,|\, \mathit{13}) &=& 0.005 \end{array}$$

The above revised probabilities tell the operator to focus on components M1 and A1 which are most likely to have failed.

Of course if more sensors are available, a better assessment of the probabilities of component failure is obtained. Suppose there is an additional sensor at X. Upon measuring X = 6, three additional assertions can be made[6]:

$$\overline{m_1} = \mathrm{T} \tag{14}$$

which says that M1 is not faulty,

$$m_2 + a_1 = \mathrm{T} \tag{15}$$

which says that A1 is faulty or M2 is faulty, and

$$m_3 + a_1 + a_2 = \mathrm{T} \tag{16}$$

which says that A1 is faulty or A2 is faulty or M3 is faulty.

[6] See appendix A for how these assertions can be generated automatically.

The conjunction of the six assertions, (10) to (12) and (14) to (16), in disjoint sum form, is

$$\begin{aligned} & \overline{m_1} \cdot m_2 \cdot a_2 + \overline{m_1} \cdot \overline{m_2} \cdot \overline{m_3} \cdot a_1 \cdot \overline{a_2} \\ + & \overline{m_1} \cdot \overline{m_2} \cdot m_3 \cdot a_1 \cdot a_2 + \overline{m_1} \cdot m_2 \cdot m_3 \cdot \overline{a_2} \; = \; \mathrm{T} \end{aligned} \tag{17}$$

The a priori probability that equation 17 is satisfied (see equation 7) is:

$$\begin{aligned} p(\mathit{17}) \; = \; & 0.01^2 \cdot 0.99 + 0.01 \cdot 0.99^4 + \\ & 0.01^3 \cdot 0.99^2 + 0.01^2 \cdot 0.99^2 \end{aligned}$$

As before, the conditional probabilities that equation 17 is satisfied given the failure of each component can be computed by using equation 9. And the conditional probability of failure for each device, given that equation 17 is satisfied, can be computed by using Bayes' rule (equation 3). The results are:

$$\begin{array}{rclcrcl} p(m_1 \mid \mathit{17}) & = & 0 & & & & \\ p(m_2 \mid \mathit{17}) & = & 0.020 & & p(m_3 \mid \mathit{17}) & = & 0.010 \\ p(a_1 \mid \mathit{17}) & = & 0.980 & & p(a_2 \mid \mathit{17}) & = & 0.010 \end{array}$$

The above revised probabilities tell the operator to focus on component A1 which is very likely to have failed. They also tell the operator not to worry about component M1 which is known not to have failed.

If there is yet an additional sensor at Y indicating Y = 4, three additional assertions can be made[7]:

$$m_2 \; = \; \mathrm{T} \tag{18}$$

which says that M2 is faulty,

$$\overline{a_1} \; = \; \mathrm{T} \tag{19}$$

which says that A1 is not faulty, and

$$m_3 + a_2 \; = \; \mathrm{T} \tag{20}$$

which says that M3 is faulty or A2 is faulty.

[7] See appendix A for how these assertions can be generated automatically.

The conjunction of the nine assertions, (10) to (12), (14) to (16), and (18) to (20), in disjoint sum form, is

$$\overline{m_1} \cdot m_2 \cdot \overline{a_1} \cdot a_2 + \overline{m_1} \cdot m_2 \cdot m_3 \cdot \overline{a_1} \cdot \overline{a_2} \;=\; \mathrm{T} \tag{21}$$

The a priori probability that equation 21 is satisfied (see equation 7) is:

$$p(\mathit{21}) \;=\; 0.01^2 \cdot 0.99^2 + 0.01^2 \cdot 0.99^3$$

As before, the conditional probabilities that equation 21 is satisfied given the failure of each component can be computed using equation 9. And the conditional probability of failure for each device, given that equation 21 is satisfied, can be computed by using Bayes' rule (equation 3). The results are:

$$\begin{array}{rcl@{\qquad}rcl} p(m_1 \,|\, \mathit{21}) & = & 0 & & & \\ p(m_2 \,|\, \mathit{21}) & = & 1 & p(m_3 \,|\, \mathit{21}) & = & 0.503 \\ p(a_1 \,|\, \mathit{21}) & = & 0 & p(a_2 \,|\, \mathit{21}) & = & 0.503 \end{array}$$

The above revised probabilities tell the operator to focus on component M2 which is known to have failed, and on components M3 and A2 which are likely to have failed. They also tell the operator not to worry about components M1 and A1 which are known not to have failed.

Of course if there is a sensor at Z, a complete diagnosis can be made.

This example shows the strengths and weaknesses of the proposed approach. The nine measurements indicate that M2 failed, and that M3 or A2 (or both) failed. Furthermore the failure of M2 is compensated by the failures of M3 or A2 (or both). This is a very unlikely situation. Assuming that there are 16 possible outputs for each component and that all failing modes are equally likely, the probability of this situation is

$$2 \cdot 0.99^3 \cdot 0.01 \cdot \frac{0.01}{15} + 0.99^2 \cdot 0.01^2 \cdot \frac{0.01}{15} \;=\; 1.3 \times 10^{-5}$$

which is three orders of magnitude smaller than the probability that only component A1 has failed ($0.99^4 \cdot 0.01 = 0.96 \times 10^{-2}$). With only seven measurements, the approach would not help the operator in this unlikely situation. In other words, the approach is good for the more likely failures. The approach does not help when the very unlikely fault situations occur.

5 Discussion

Previous approaches used reason maintenance systems for diagnosis. The approach presented in this publication divides the diagnosis task into two subtasks: the generation of assertions and inference. Moreover, previous approaches used probabilistic analysis to assess the likelihoods of each diagnosis (i.e., each solution to the system of Boolean equations K). In this publication, the probabilistic analysis is used to assess the likelihoods of failure for each component. This section addresses these issues.

5.1 Generation of assertions

For the first task, the generation of assertions, two kinds of tools can be used: reason maintenance systems or domain-dependent analysis tools. The latter generates the assertions directly while the former searches. For example, for electric circuits, the direct methods include those based in nodal analysis, loop analysis, etc. But the same assertions that are obtained by using those methods can also be generated by writing Kirchoff's laws, device laws, and a description of the circuit in PROLOG.

The choice of what tool is more effective depends on the specifics of the applications. For systems such as electric circuits, that are well understood and for which accurate models exist, domain-dependent methods seem to be more efficient. Another advantage of domain-dependent methods is their ability to make assertions not only when there is a difference between prediction and observation, but also when there is an agreement. Furthermore, typically more assertions can be made with domain-dependent methods than with domain-independent methods. Equation 12 is an example of an assertion that would not be made by domain-independent methods.

It should be noted that reason maintenance systems are not 100% domain independent. The module that predicts values (in order to compare with measurements) is domain dependent. Furthermore, it seems that the inference strategy of those systems can be extended to incorporate domain-dependent rules such as *if the measurement agrees with the prediction, there can not be only one component failing* for the adder/multiplier domain. But writing such rules in a general-purpose formalism may be somewhat complex. The "consistent belief rule" and the "nogood inference rule" used by Struss and Dressler [18] are examples of additional rules that incorporate fault models, that is, that incorporate a description of the behavior exhibited by the components when they fail. The "circumscribed diagnosis engine" presented by Raiman [16] is another example of an extension to reason maintenance systems; it enables the generation of assertions not only from differences but also from agreements.

5.2 Inference

For the second subtask, the inference of component status given the assertions, sentential logic is sufficient. Previous methods also used reason maintenance systems for the inference [8,16,18]. Since first-order logic encompasses sentential logic, those approaches worked. But the overhead costs of using a more general tool can be large.

There is a correspondence between the approach presented in this publication and previous approaches. For example, the minimal diagnosis concept used in previous work [7] is related to the terms of the minimized form of equation K.

Viewing diagnosis as solving a set of Boolean equations is simpler than previous approaches. Many theorems used in those approaches have corresponding theorems in Boolean algebra. With the approach presented in this publication, the well-developed machinery of Boolean algebra can be directly used for diagnosis. Moreover, a simpler formulation also facilitates focusing on the real computational issues.

Furthermore, the search can be avoided by manipulating the assertions symbolically. An analogy can be made between numerical and symbolic methods in algebra or calculus, and search and symbolic methods in logic. Like numerical methods (e.g., for solving systems of nonlinear equations), search methods are robust and quite general. But search methods also have drawbacks that are analogous to the large amounts of computation and convergence problems of numerical algorithms. Symbolic methods, both in calculus and in logic, are not as general, but when they can be used they are usually more efficient. Appendix B compares search and symbolic methods for problem solving.

5.3 Probabilistic analysis

Probabilistic analysis has also been used in previous research on automatic diagnosis [1,3,8,15].

Some previous work focused on medical and similar kinds of diagnosis where the physical system is not well understood [3,15]. In that work, the assertions that can be made from the manifestations have a degree of uncertainty. Work in this area aims at the generation of plausible hypothesis taking into account the uncertainty of the assertions.

In other previous work [1,8] which, like this publication, focused on well-understood physical systems, the goal has been to find a set of measurements, as small as possible, yet sufficient to diagnose all faults. Entropy measures were used to assess the amount of information each measurement can provide. These measures in turn used probabilities of failures for individual components. The prospective measurements were ranked in decreasing order of the amount of information they can provide. Since the actual amount of information provided by a measurement depends on the outcome, measurements are actually ranked by the expected (in the probabilistic sense) amount of information they will provide.

While in diagnosis the goal is to have a (as small as possible) set of assertions such that the number of terms in equation K' is 1 (i.e., $D = 0$), the goal in monitoring is to direct attention to the parts of the system that seem to have problems. For monitoring, no choice of measurements need to be made since the sensors are fixed when the system is built. The probabilistic analysis in monitoring is not aimed at maximizing the amount of information which is fixed. It is aimed at refining the probabilities of failure of individual components.

6 Conclusion

Diagnostic reasoning can be decoupled into the generation of assertions from the sensor readings and the system model, and the manipulation of these assertions. The latter can be seen as solving a system of Boolean equations. While previous approaches to automatic diagnosis used search, the approach presented in this publication consists of solving the system of equations symbolically.

Unlike diagnosis where one can make further measurements until a decision is made, in selective monitoring the measurements are fixed. Using a priori probabilities of component failure and Bayes' rule, revised probabilities of failure can be computed. These will indicate what components have failed or are the most likely to have failed. The method is robust in the sense that even if a priori probabilities are not accurate, if there is enough evidence showing that component c_i has failed, the value computed for $p(c_i|K)$ will be 1.

This approach is suitable for systems that are well understood and for which the correctness of the assertions can be guaranteed. Also, the system must be such that assertions can be made from instantaneous measurements. Furthermore, the system must be such that changes are slow enough to allow the computation.

A number of aspects must be considered in selective monitoring and diagnostic reasoning is just one of them. Other aspects include, for example, the ability to anticipate problems or failures and the ability to detect abnormal conditions that are not caused by component failures. Future work will explore the combination of the technique presented in this publication with those of previous work [10,11], and with other techniques such as expert systems [14] and neural networks [9].

PAGE______INTENTIONALLY BLANK

Appendixes

A Digital circuit analysis

Assertions (10) to (12), (14) to (16), and (18) to (20) introduced in section 4 can be generated automatically as follows.

To each sensor node in the circuit, there corresponds an AND/OR graph in which the OR nodes, which are circular, correspond to nodes in the circuit; and the AND nodes, which are rectangular, correspond to components. Figures 3, 4, 5, and 6 show the AND/OR graphs for nodes F, G, X, and Y, respectively.

For each solution tree of each AND/OR graph, the value of the root can be computed from the value of the leaves. If the computed value does not agree with the measurement, one can make the following assertion:

$$d_a + d_b + \cdots + d_h \quad = \quad \mathrm{T}$$

where $d_a, d_b, \cdots d_h$ are the logical variables that indicate the status of the components corresponding to the AND nodes of the solution tree. This assertion corresponds to the fact that at least one of the components corresponding to the AND nodes has failed. If the computed value agrees with the measurements, one can make the following assertion:

$$\overline{d_a \cdot \overline{d_b} \cdots \overline{d_h} + \overline{d_a} \cdot d_b \cdots \overline{d_h} + \cdots + \overline{d_a} \cdot \overline{d_b} \cdots d_h} \quad = \quad \mathrm{T}$$

This assertion corresponds to the fact that there cannot be only one component corresponding to the AND nodes failed.

PRECEDING PAGE BLANK NOT FILMED

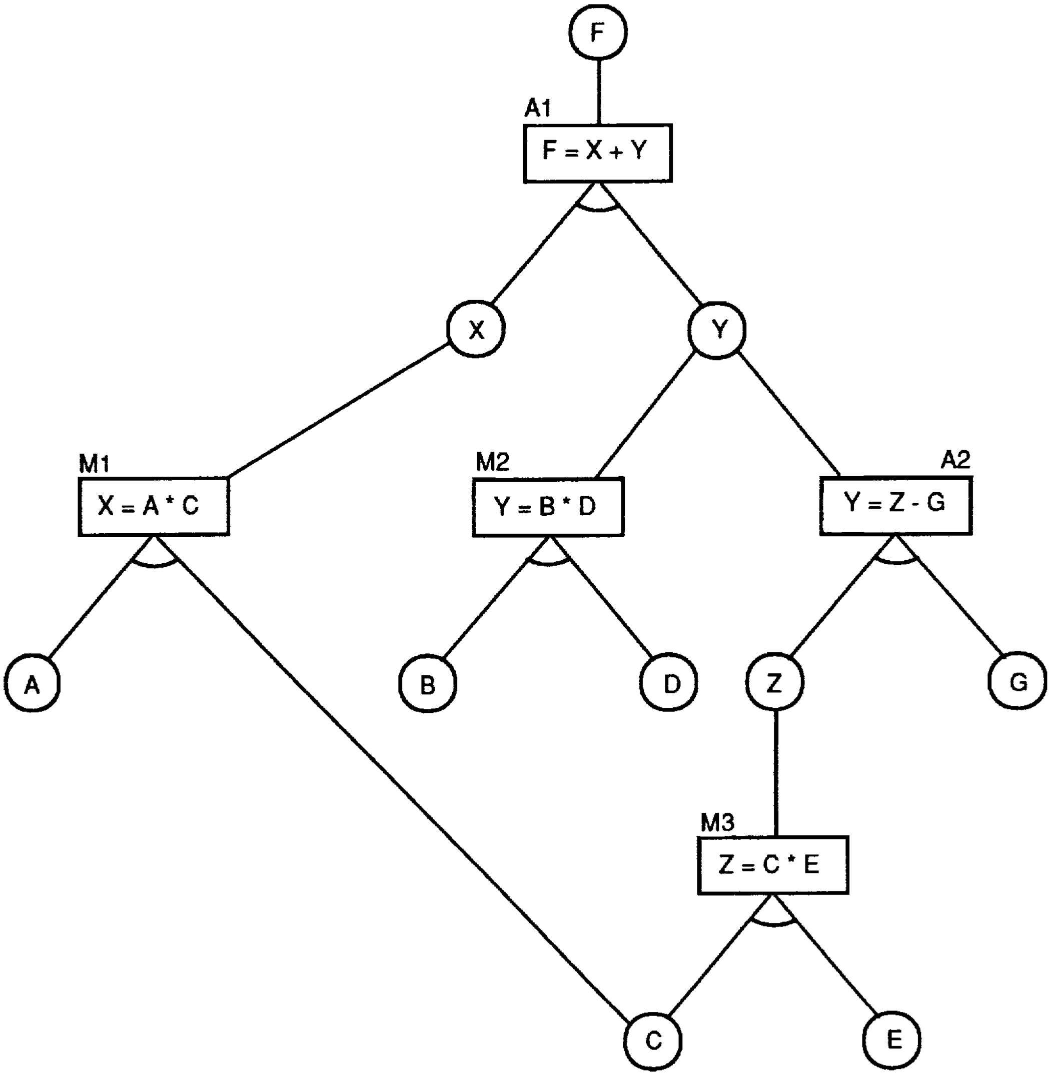

Figure 3: AND/OR graph for node F of the circuit shown in figure 2

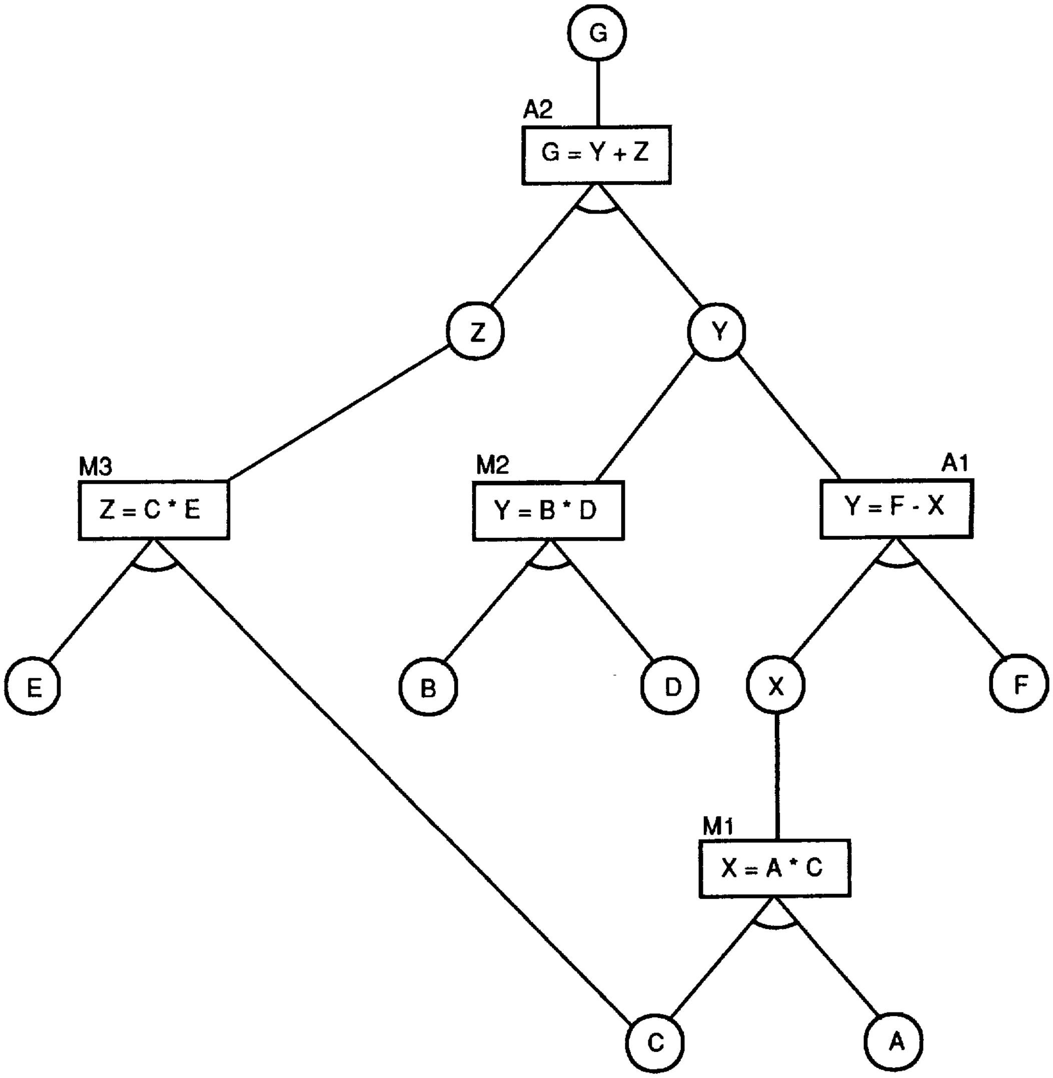

Figure 4: AND/OR graph for node G of the circuit shown in figure 2

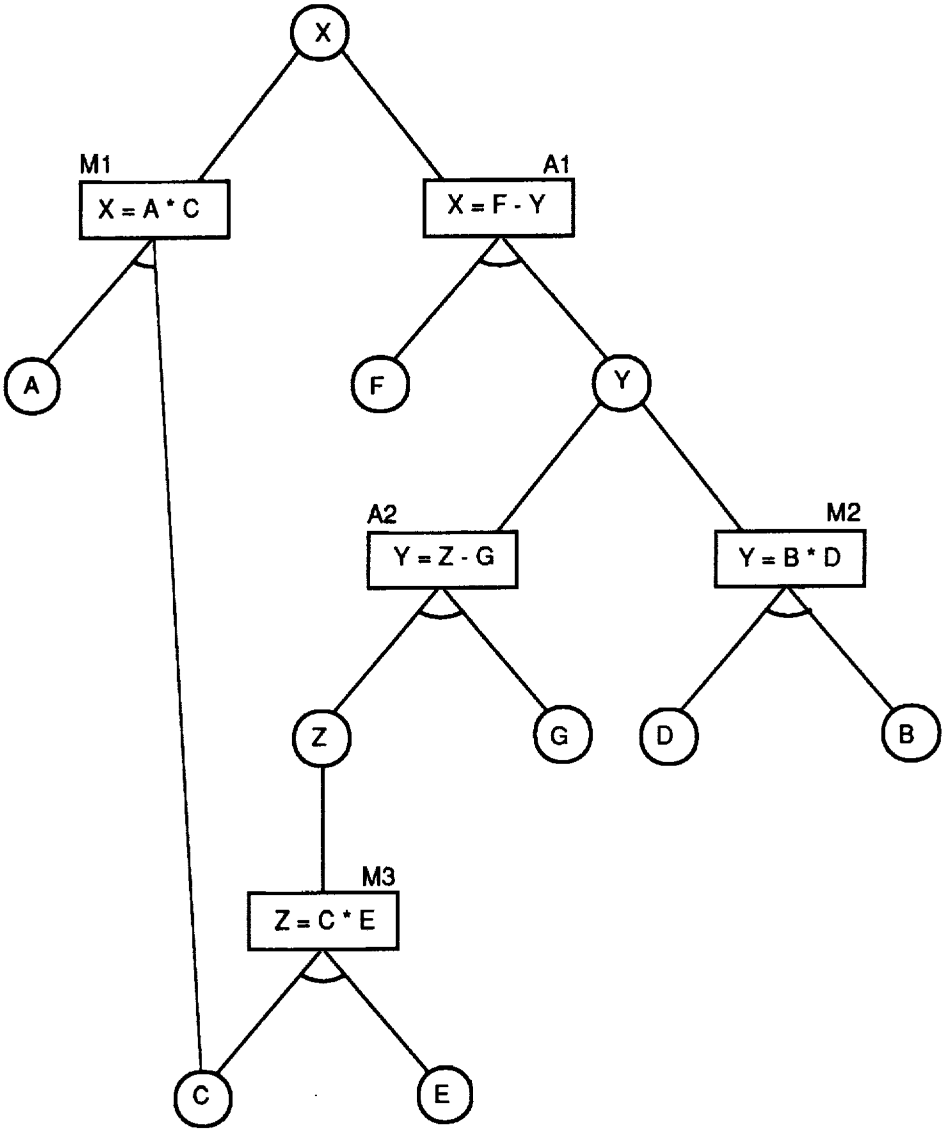

Figure 5: AND/OR graph for node X of the circuit shown in figure 2

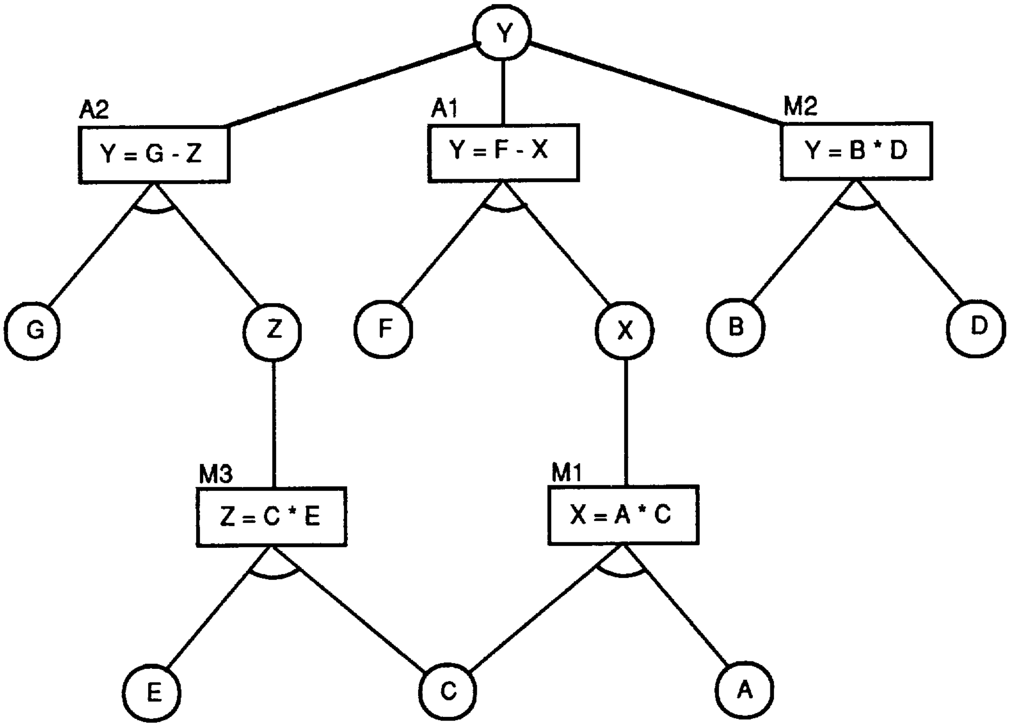

Figure 6: AND/OR graph for node Y of the circuit shown in figure 2

PAGE________INTENTIONALLY BLANK

Appendixes (continued)

B A comparison between search and symbolic manipulation approaches to problem solving

Consider the following problem, borrowed from [5]:

(1) $x \in \{0,1\}$ (2) $a = e_1(x)$
(3) $y \in \{0,1\}$ (4) $b = e_1(y)$
(5) $z \in \{0,1\}$ (6) $c = e_1(z)$
(7) $a \neq b$ (8) $b \neq c$

where the function e_1 is very expensive to compute.

The search approach to solve this problem is to enumerate all possibilities and try each one until a solution is found. Although techniques such as chronological backtracking can be used to improve the efficiency of this search, this process will typically involve extensive computation.

The symbolic manipulation approach to solve this problem is to write Boolean equations corresponding to conditions (7) and (8) above:

$$\begin{aligned} (\overline{x} + \overline{y}) \cdot (x + y) &= \mathrm{T} \\ (\overline{y} + \overline{z}) \cdot (y + z) &= \mathrm{T} \end{aligned}$$

The conjunction of these equations is also true:

$$\begin{aligned} (\overline{x} + \overline{y}) \cdot (x + y) \cdot (\overline{y} + \overline{z}) \cdot (y + z) &= \\ \overline{x} \cdot y \cdot \overline{z} + x \cdot \overline{y} \cdot z &= \mathrm{T} \end{aligned}$$

Therefore, the problem has two solutions: $\{x = 0 \quad y = 1 \quad z = 0\}$ and $\{x = 1 \ \ y = 0 \ \ z = 1\}$.

PAGE ______ INTENTIONALLY BLANK

References

[1] A. A. Aly and N. A. Elsayedaly. An Efficient Algorithm for Optimal Design of Diagnostics. *IEEE Trans. on Reliability*, R-32(5):426–432, 436, Dec. 1983.

[2] F. Beichelt and L. Spross. Comment on "An Improved Abraham-Method for Generating Disjoint Sums". *IEEE Trans. on Reliability*, R-38(4):422–424, Oct. 1989.

[3] M. Ben-Bassat et al. Pattern-Based Interactive Diagnosis of Multiple Disorders: The MEDAS System. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, PAMI-2(2):148–160, Mar. 1980.

[4] R. Davis. Diagnostic Reasoning Based on Structure and Behavior. *Artificial Intelligence*, 24:347–410, 1984.

[5] J. de Kleer. An Assumption-based TMS. *Artificial Intelligence*, 28: 127–162, 1986.

[6] J. de Kleer. Using Crude Probability Estimates to Guide Diagnosis. *Artificial Intelligence*, 45:381–391, 1990.

[7] J. de Kleer, A. K. Mackworth, and R. Reiter. Characterizing Diagnoses. *AAAI-90 Proc. of Eighth Nat. Conf. on Artificial Intelligence*, pp. 324–330, Aug. 1990.

[8] J. de Kleer and B. C. Williams. Diagnosing Multiple Faults. *Artificial Intelligence*, 32:97–130, 1987.

[9] A. B. Dobrzeniecki and L. M. Lidsky. Reasoning About Sensor Signals Using Artificial Neural Networks. *Proc. of Int. Symposium on Artificial Intelligence, Robotics and Automation in Space*, pp. 149–152, Nov. 1990.

[10] R. J. Doyle et al. Sensor Selection in Complex System Monitoring using Information Quantification and Causal Reasoning. In B. Faltings and P. Struss (editors), *Recent Advances in Qualitative Physics*, MIT Press, 1991.

[11] R. J. Doyle, S. M. Sellers, and D. J. Atkinson. A Focused, Context-Sensitive Approach to Monitoring. *IJCAI-89 Proc. of Eleventh International Conference on Artificial Intelligence*, pp. 1231–1237, Aug. 1989.

[12] H. B. Enderton. *A Mathematical Introduction to Logic.* Academic Press, 1972.

[13] M. O. Locks. A Minimizing Algorithm for Sum of Disjoint Products. *IEEE Trans. on Reliability*, R-36(4):445–453, Oct. 1987.

[14] N. Muroi, Y. Miyamoto, and I. Akeyama. Approach in Construction of Diagnostic Expert System for Environmental Control Equipment in Space. *Proc. of Int. Symposium on Artificial Intelligence, Robotics and Automation in Space*, pp. 171–174, Nov. 1990.

[15] Y. Peng and J. A. Regia. A Probabilistic Causal Model for Diagnostic Problem Solving, Part II: Diagnostic Strategy. *IEEE Trans. on Systems, Man and Cybernetics*, SMC-17(3):395–406, May/Jun. 1987.

[16] O. Raiman. A Circumscribed Diagnosis Engine. *AAAI '90 Workshop on Model-Based Reasoning*, pp. 9–14, Aug. 1990.

[17] M. L. Shooman. *Probabilistic Reliability: An Engineering Approach.* McGraw-Hill, 1968.

[18] P. Struss and O. Dressler. "Physical Negation" - Integrating Fault Models into the General Diagnostic Engine. *IJCAI-89 Proc. of Eleventh Int. Conf. on Artificial Intelligence*, pp. 1318–1323, Aug. 1989.

TECHNICAL REPORT STANDARD TITLE PAGE

1. Report No. 91-6	2. Government Accession No.	3. Recipient's Catalog No.

4. Title and Subtitle DIAGNOSTIC REASONING TECHNIQUES FOR SELECTIVE MONITORING	5. Report Date March 1, 1991 6. Performing Organization Code
7. Author(s) L.S. Homem-de-Mello and R.J. Doyle	8. Performing Organization Report No.
9. Performing Organization Name and Address JET PROPULSION LABORATORY California Institute of Technology 4800 Oak Grove Drive Pasadena, California 91109	10. Work Unit No. 11. Contract or Grant No. NAS7-918 13. Type of Report and Period Covered JPL Publication
12. Sponsoring Agency Name and Address NATIONAL AERONAUTICS AND SPACE ADMINISTRATION Washington, D.C. 20546	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

This publication presents an architecture for using diagnostic reasoning techniques in selective monitoring. Given the sensor readings and a model of the physical system, a number of assertions are generated and expressed as Boolean equations. The resulting system of Boolean equations is solved symbolically. Using a priori probabilities of component failure and Bayes' rule, revised probabilities of failure can be computed. These will indicate what components have failed or are the most likely to have failed. This approach is suitable for systems that are well understood and for which the correctness of the assertions can be guaranteed. Also, the system must be such that assertions can be made from instantaneous measurements. And the system must be such that changes are slow enough to allow the computation.

17. Key Words (Selected by Author(s)) 186. Engineering (General); 232. Mathematical and Computer Science (General). Artificial Intelligence; Boolean equations; Probability; Sentential Logic; Physical Systems; Mathematical Analysis	18. Distribution Statement Unclassified; unlimited.

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 32	22. Price