SAFEPROCESS 2003

FAULT DETECTION, SUPERVISION AND SAFETY OF TECHNICAL PROCESSES

A LOGICAL FRAMEWORK FOR ISOLATION IN FAULT DIAGNOSIS

Stéphane Ploix, Samir Touaf, Jean-Marie Flaus

Laboratoire d'Automatique de Grenoble
INPG, UJF, CNRS - BP 46
38402 Saint Martin d'Hères Cedex (France)
Stephane.Ploix@inpg.fr, Samir.Touaf@inpg.fr, Jean-Marie.Flaus@inpg.fr

Abstract: After some remarks on terminology, this paper introduces a general method for fault diagnosis in complex dynamic systems, which takes advantage of the results on analytical redundancy methods from the Automatic Control community and on logical reasoning from the Artificial Intelligence community. The proposed method tackles both the problem of diagnosing complex dynamic systems with models of normal and abnormal behavior including differential equations, and the problem of providing logically sound diagnosis. Moreover, it is shown how diagnoses can be sorted.

Keywords: diagnostic reasoning, analytical redundancy relation, fault detection and isolation, dynamic systems, terminology.

1. INTRODUCTION

A fault diagnosis system aims at determining the state of a physical system from observed symptoms. Two kinds of approaches have been developed till now: the logical approach coming from the Artificial Intelligence community, described in (De Kleer and Williams, 1987; Reiter, 1987; Dague, 2001) and the FDI approach coming from the Automatic Control community, described in (Frank, 1990; Patton et al., 1989). The first one, originally dedicated to static binary systems, proposes a logically rigorous reasoning based on models representing normal behavior of the components of a physical system. This approach does not distinguish the symptom generation from the diagnostic reasoning, namely the symptoms analysis to deduce diagnoses. Another approach is the FDI approach that mainly deals with symptom generation based on models representing abnormal behavior. Elements of comparison between these approaches have been included in (Cordier et al., 2000).

The method proposed in this paper aims at capitalizing the advantages of both approaches. The step of symptom generation has been uncoupled from that of diagnostic reasoning in order to uncouple reasoning from application fields. The field of complex dynamic systems modeled by differential equations is the scope of this paper. It is well known by the AC community that, for the same subsystem, there are various techniques for symptom generation (also called fault detection) and that these techniques can be too different from logic formalism and too complex to study together with the diagnostic reasoning problem. The analytical redundancy tools are supposed to be used for fault detection.

Because different scientific communities study fault diagnosis, the terminologies differ from one community to another. For instance, some definitions suggested in (Isermann and Balle, 1997) are incompatible with the logical definition of Reiter (1987). In this paper, the following terminology has been adopted:

- A component is a physical entity considered as indivisible.
- A physical system is a set of components whose behaviors are dependent.

- A diagnosis is a plausible state of a physical system (usually expressed in terms of component states).
- A fault is an abnormal state of a component
- A failure is a fault inducing an inability to fulfill some required functions.
- A symptom is a distinguishing character providing information on the actual state of a physical system.

The design of a diagnosis system can be decomposed into three main steps.

Firstly, symptoms have to be extracted from the available information on the actual system state. Consistency between this information and reference behavioral models has to be checked with detection tests. The design of these tests corresponds to the first design step. It leads to the task usually called *fault detection* by the AC community.

Then, the symptoms coming from detection tests have to be analyzed to determine what are the possible faults in the system.

Finally, the diagnostic strategy, which will not be studied in this paper, deals with managing detection tests and diagnostic reasoning to fulfill requirements such as diagnosis reliability, time required by the diagnosis algorithms (what tests have to be triggered when?), taking into account the nature of faults (persistent or not) and so on…

In this paper, the following topics will be discussed: designing models appropriate for fault diagnosis, finding the testable subsets of the system, designing detection tests for complex dynamic systems and diagnostic reasoning.

2. MODELS FOR FAULT DIAGNOSIS

Analytical redundancy relations do not contain enough information to make logical diagnosis possible. First of all, a behavioral model does not represent all the possible behaviors but it is usually dedicated to some particular behaviors and to particular operating modes. In other words, a behavioral model may not be valid everywhere and its validity also has to be modeled. Model validity is meta-knowledge i.e. knowledge on the knowledge about the behavior. For instance, it may be known that a model does not describe the behavior when its input is higher than a given value; validity has then to be checked at any time. This meta-knowledge is of course an expert knowledge, which fully belongs to the model. Moreover, a model may represent a normal behavior or different kinds of faulty behaviors. Thus, a modeled behavior relies on assumptions on component states. These assumptions are essential for diagnostic reasoning because they provide a way to interpret results coming from detection tests: for instance, an inconsistency means that the corresponding set of assumptions, whether it contains normal or abnormal behavior assumptions, is not satisfied.

The phenomena, which, potentially, can be directly measured, will be called *physical variables*. As a corollary, these variables are model independent and are thus intrinsically different from parameters. The notation [x] in (1) means that x is a set of physical variables. The notation $\tilde{x}$ stands for known values of [x]. A known value can come, for example, from an observation or from a control variable.

For fault diagnosis, a component, denoted by C_i may be described by several elementary models:

$$EM_i\left(\left[x\right],\tilde{x}\right):\ \left(r_i\left(\left[x\right],\tilde{x}\right),v_i\left(\left[x\right],\tilde{x}\right),h_i\right) \qquad (1)$$

- $r_i\left(\left[x\right],\tilde{x}\right)$ denotes an elementary analytical relation, called constraint in (Gehin et al, 2000), representing partially or totally the behavior of a component C_i in a given state h_i. It is a relation between observable phenomena and, possibly, known values. It may be any kind of model such as differential equations, neural networks,...
- $v_i\left(\left[x\right],\tilde{x}\right)$ defines the validity condition of the relation $r_i\left(\left[x\right],\tilde{x}\right)$. The result is restricted to Boolean values (valid or invalid).
- h_i is the state of the component C_i consistent with the elementary relation and with its validity. Notation coming from circumscription theory (Mc Carthy, 1986) has been adopted: a component C_j behaving normally will be described by $h_i = \neg AN\left(C_j\right)$. If this component is altered by a fault D, it will be written as follow: $h_i = D\left(C_j\right)$. Note that the following implication always holds: $D\left(C_j\right) \Rightarrow AN\left(C_j\right)$ whereas the reverse is false.

A subsystem model is a set of elementary models EM_i (in order to simplify the notations, the variables intervening in elementary models are omitted). Its behavior is depicted by the union of the relations of all the elementary models of the considered subset. Its validity is equal to the conjunction of the validities of elementary models and, the state of the subset is equal to the conjunction of the states of the elementary models. Moreover, a subsystem exists only if there is no contradiction in validities and in states. It means that there must be some operating set points where the subsystem model is valid and where elementary model states do not contain both a state and its negation:

$$\left(\bigcup_{i\in\phi} r_i\left(\left[x\right],\tilde{x}\right), \bigwedge_{i\in\phi} v_i\left(\left[x\right],\tilde{x}\right), \bigwedge_{i\in\phi} h_i\right) \qquad (2)$$

$$\text{with } \bigwedge_{i\in\phi} h_i \not\equiv false \text{ and } \exists\tilde{x} / \bigwedge_{i\in\phi} v_i\left(\tilde{x}\right) = true$$

An electrical DC machine, powered by a digitally controlled power converter, coupled to a mechanical load behaving as shown in figure 1, has been chosen to illustrate this paper.

The available elementary models can be grouped in a set called System Description in (Reiter, 1987):

$$\begin{cases} EM_1=\left(\left[u\right]=K_u\left[u_c\right],\left\|\left[u\right]\right\|\le U_{\max},\neg AN\left(\mathrm{C}_1\right)\right)\\ EM_2=\left(\left[u\right]=R\left[i\right]+L\dfrac{d}{dt}\left[i\right]+\Phi\left[i_e\right]\left[\Omega\right],-,\neg AN\left(\mathrm{C}_2\right)\right)\\ EM_3=\left(\left[u\right]=\rho R\left[i\right]+\rho L\dfrac{d}{dt}\left[i\right]+\Phi\left[i_e\right]\left[\Omega\right],0\le\rho\le 0.95,CC\left(\mathrm{C}_2\right)\right)\\ EM_4=\left(J\dfrac{d}{dt}\left[\Omega\right]=\Phi\left[i_e\right]\left[i\right]-\left[c_r\right],-,\neg AN\left(\mathrm{C}_3\right)\right)\\ EM_5=\left(\left[t_r\right]=t_0+t_1\left[\Omega\right],\left[t_r\right]\ge t_0,\neg AN\left(\mathrm{C}_4\right)\right)\\ EM_6=\left(\left[t_r\right]=-t_0+t_1\Omega,\left[\mathrm{t}_r\right]\le t_0,\neg AN\left(\mathrm{C}_4\right)\right)\\ EM_7=\left(\tilde{u}_c=\left[u_c\right],\mathrm{LF},\neg AN\left(\mathrm{C}_5\right)\right)\\ EM_8=\left(\tilde{i}_e=\left[i_e\right],\text{-},\neg\mathrm{AN}\left(\mathrm{C}_6\right)\right)\\ EM_9=\left(\tilde{u}=\left[u\right],\mathrm{LF},\neg AN\left(\mathrm{C}_7\right)\right)\\ EM_{10}=\left(\tilde{i}=i,\mathrm{LF},\neg AN\left(\mathrm{C}_8\right)\right)\\ EM_{11}=\left(\tilde{\Omega}=\Omega,\mathrm{LF},\neg AN\left(\mathrm{C}_9\right)\right) \end{cases} \quad (3)$$

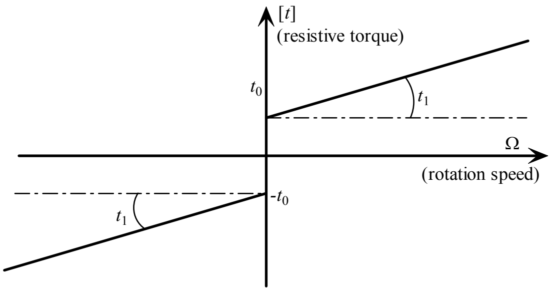

Fig. 1: Characteristics of the mechanical load

The list of component symbols in (3) is the following:

C_1: power converter C_2: electrical part C_3: mechanical part C_4: mechanical load C_5: DA converter C_6: magnetizing current C_7 : voltage sensor, C_8: current sensor, C_9: rotation speed sensor

Components C_5, C_6, C_7, C_8 and C_9 are informational components whose models are usually simple. However, they have to be modeled in order to take into account state assumptions for sensors and actuators.

Note that several different elementary models may be related to the same component. For example, models EM_2 and EM_3 are related to the electrical part of the DC machine (C_2). The first one models the normal behavior and the second one, a short circuit (state assumption $CC(C_2)$). Models EM_5 and EM_6 are another example. They rely on the same state assumption but their validity is different.

3. DETECTION TESTS

Any given subsystem model cannot always be checked because testing the consistency of a subset of elementary models requires that some physical variables be known. A test, also called detection test, dedicated to a subsystem model is a Boolean function defined on a space of known variables, based on all the analytical relations of the elementary models belonging to the subsets.

A detection test can be written as:

$$\left(t\left(\tilde{x}\right),\underset{i\in\phi}{\wedge}v_i\left(\tilde{x}\right),\underset{i\in\phi}{\wedge}h_i\right) \quad (4)$$

where $t\left(\tilde{x}\right)$ is based on a set of relations $r_i\left(\left[x\right],\tilde{x}\right):i\in\phi$; ϕ refers to the set of the involved elementary models.

Notice that a function $t\left(\tilde{x}\right)$ related to a given subset is not unique: it may be any kind of parity relations or any kind of state observers for some dynamic system. Any set of elementary models such as (2) that may yield at least one test, will be called a testable subset (TS): it defines the subset checked. A Testable Sub System (TSS) refers to the components of a Testable Subset.

A detection test is sometime called an *analytical redundancy relation* (ARR) in FDI communities. Sometimes, it is not easy to deduce a detection test or an ARR from a testable subset, especially if it contains differential equations, but elimination theory (Kapur and Lakshman, 1992) may be useful in such cases.

It is also interesting to be able to determine a priori all the testable subsets. Emphasizing structural knowledge of elementary models can solve this problem (Declerck et all, 1991) (Ploix and Follot, 2001). According to these approaches, the composition of testable subsets has been summarized in the table 1.

Table 1 – Testable Subsets of the DC motor

TS	EM1	EM2	EM3	EM4	EM5	EM6	EM7	EM8	EM9	EM10	EM11
1	x						x		x		
2		x						x	x	x	x
3			x					x	x	x	x
4				x	x			x		x	x
5				x		x		x		x	x
6	x	x					x	x		x	x
7	x		x				x	x		x	x
8		x		x	x			x	x		x
9			x	x	x			x	x		x
10		x		x		x		x	x		x
11			x	x		x		x	x		x
12		x		x	x			x	x	x	
13			x	x	x			x	x	x	
14		x		x		x		x	x	x	
15			x	x		x		x	x	x	
16	x	x		x	x		x	x			x
17	x		x	x	x		x	x			x
18	x	x		x		x	x	x			x
19	x		x	x		x	x	x			x
20	x	x		x	x		x	x		x	
21	x		x	x	x		x	x		x	
22	x	x		x		x	x	x		x	
23	x		x	x		x	x	x		x	

In order to interpret the results of a test, the non-exoneration principle has to be introduced. It is given by the two following implications:

$$\exists\tilde{X}\in\mathcal{P}\left(\tilde{x}\right)/\neg t\left(\tilde{X}\right)\wedge\left(\underset{i\in\phi}{\wedge}v_i\left(\tilde{X}\right)\right)\Rightarrow\neg\left(\underset{i\in\phi}{\wedge}h_i\right) \quad (5a)$$

$$\forall \tilde{X} \in \mathcal{P}(\tilde{x}) / t(\tilde{X}) \wedge \left(\bigwedge_{i\in\phi} v_i(\tilde{X}) \right) \Rightarrow \bigwedge_{i\in\phi} h_i \qquad (5b)$$

where $\mathcal{P}(\tilde{x})$ stands for the set of all the possible values or trajectories of $\tilde{x}$. However, the property (5b) containing an universal quantifier cannot be satisfied because the cardinal of $\mathcal{P}(\tilde{x})$ is usually infinite. This remark points out the non-exoneration principle, which can also be expressed as:

- inconsistency implies $\neg\left(\bigwedge_{j\in\phi i} h_j\right)$
- consistency only means that the clause $\bigwedge_{i\in\phi} h_i$ is plausible regarding the subset $\mathcal{X}$ of $\mathcal{P}(\tilde{x})$.

In other words, this principle means that consistency and inconsistency have to be considered separately during the diagnostic reasoning. An inconsistency has a global meaning whereas a consistency can only be interpreted with respect to the operating context. Thus, a validate inconsistency, namely an inconsistency detected whereas the validity condition is true, reveals that state assumptions cannot be true until the system state has changed by itself or by human intervention.

Consequently, the meaning of a test $t(\tilde{x})$ is summarized in table 2.

Table 2 – Interpretation of test results

	$\bigwedge_{i\in\phi} v_i(\tilde{x})$	$\neg\bigwedge_{i\in\phi} v_i(\tilde{x})$
$t(\tilde{x})$	$\left(\bigwedge_{i\in\phi} h_i\right)$ contextually	no result
$\neg t(\tilde{x})$	$\neg\left(\bigwedge_{i\in\phi} h_i\right)$	no result

There are many ways of testing a TS: several functions $t(\tilde{y})$ can satisfy (4). For dynamic functions, time windows may vary according to tests $t(\tilde{y})$.

Consider for example TS 2 in table 1. The detection test may be implemented as a parity relation with a time window width of 2 sample times:

$$\left(\begin{array}{l} \left| \tilde{i}_k - e^{-\frac{R}{L}\tau e} \tilde{i}_{k-1} - \dfrac{\left(e^{-\frac{R}{L}\tau e} - 1\right)\Phi \tilde{i}_e}{R} \tilde{\Omega}_{k-1} - \dfrac{1 - e^{-\frac{R}{L}\tau e}}{R} \tilde{u}_{k-1} \right| \leq \sigma, \\ |\tilde{u}| \leq U_{\max} \wedge LF, \neg AN(C_1) \wedge \neg AN(C_5) \wedge \neg AN(C_7) \end{array} \right)$$

It can also be a state observer with infinite time windows (but practically depending on the pole of the state observer):

$$\left(\begin{array}{l} \left\{ \begin{array}{l} \hat{i}_{k+1} = e^{-\frac{R}{L}\tau e} \hat{i}_k + \dfrac{\left(e^{-\frac{R}{L}\tau e} - 1\right)\Phi \tilde{i}_e}{R} \tilde{\Omega}_k + \dfrac{1 - e^{-\frac{R}{L}\tau e}}{R} \tilde{u}_k + K\left(\tilde{i}_k - \hat{i}_k\right), \\ \left|\tilde{i}_k - \hat{i}_k\right| \leq \sigma' \end{array} \right. \\ |\tilde{u}| \leq U_{\max} \wedge LF, \neg AN(C_1) \wedge \neg AN(C_5) \wedge \neg AN(C_7) \end{array} \right)$$

Figure 2 shows some typical results of a detection test. The upper signal corresponds to the rough test result $t(\tilde{x})$ over time. The second signal corresponds to the test validity. The last signal takes into account the test result (1st signal) and validity (2nd signal) and it also memorizes the past inconsistencies until the system state may have changed.

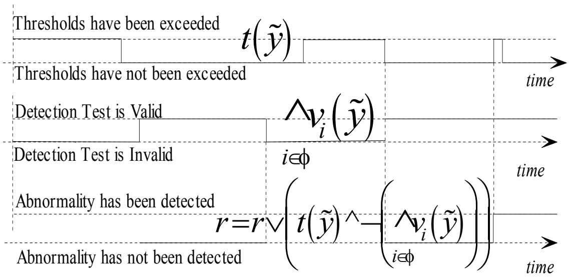

Fig. 2 – Typical results of a detection test

Figure 2 illustrates that even if an inconsistency is revealed by a detection test, a symptom is not necessary detected because the test may be invalid at the considered operating mode. On the whole, whatever the consistency result is, a test cannot provide results if it is invalid.

4. GLOBAL DIAGNOSTIC REASONING

Diagnostic reasoning analyses the available symptoms provided by detection tests in order to determine the possible system states. (Reiter, 1987) proposes a logical theory for diagnostic reasoning known as consistency based reasoning or DX approach. The logical theory for diagnosis relies on the notion of conflict. This theory has then been formalized in (De Kleer and Williams, 1987) and extended to faulty behavior in (De Kleer and Williams, 1990). The diagnostic approach proposed in this paper is an adaptation of the part of logical theory related to pure diagnostic analysis. The design of the detection test has been replaced by the one presented in section 3 in order to handle the complexity inherent to complex dynamic systems with differential equations.

A detected abnormality implies that the related state assumption is necessarily false. If a detection test (4) reveals a detected abnormality, the state assumption is false. A conflict is then a set of component state assumptions such that at least one of them is false. It can be written as:

$$\left\{\neg h_i \,/\, \bigvee_{i\in\phi} \neg h_i\right\} \quad (6)$$

For example, if a test related to TS 3 reveals a detected abnormality, the following conflict will appear:

$$\left\{\neg CC(C_2), AN(C_6), AN(C_7), AN(C_8), AN(C_9)\right\}$$

Diagnoses are deduced from the analysis of sets of revealed conflicts. A diagnosis $\mathcal{D}$ is a set of component state assumptions, $\mathcal{D}=\{\neg h_i\}$, which accounts for all the revealed conflicts $\{\mathcal{C}_n \,/\, n\in\Omega\}$:

$$\forall n\in\Omega, \mathcal{D}\cap\mathcal{C}_n \neq \varnothing \quad (7)$$

Because of the huge number of possible diagnoses, it is usual to restrict search to minimal diagnosis. A diagnosis $\mathcal{D}$ is minimal if and only if:

$$\nexists \mathcal{D}' \subset \mathcal{D} \,/\, \forall n\in\Omega, \mathcal{D}'\cap\mathcal{C}_n \neq \varnothing \quad (8)$$

Searching for all the minimal diagnoses can be performed thanks to the HS-Tree algorithm originally proposed in (Reiter, 1987) and corrected in (Greiner et al., 1989), by substituting component state assumption for each component in conflicts.

Concerning the example of the DC machine, it is now assumed that only tests based on TS 1, 2, 3, 4, 18 and 20 provide results. Tests based on TS 2, 3 and 20 reveal inconsistencies whereas other tests lead to consistent results (see table 1).

Conflicts are then:

$$\left\{AN(C_2), AN(C_6), AN(C_7), AN(C_8), AN(C_9)\right\}$$

$$\left\{\neg CC(C_2), AN(C_6), AN(C_7), AN(C_8), AN(C_9)\right\}$$

$$\left\{\begin{matrix} AN(C_1), AN(C_2), AN(C_3), AN(C_4), AN(C_5), \\ AN(C_6), AN(C_8) \end{matrix}\right\}$$

The set of global minimal diagnoses is deduced with the HS-Tree algorithm:

$\{\{AN(C_6)\},\{AN(C_8)\},\{AN(C_1),AN(C_7)\},\{AN(C_1),AN(C_9)\},$
$\{AN(C_2),\neg CC(C_2)\},\{AN(C_2)\wedge AN(C_7)\},\{AN(C_2),AN(C_9)\},$
$\{AN(C_3),AN(C_7)\},\{AN(C_3),AN(C_9)\},\{AN(C_4),AN(C_7)\},$
$\{AN(C_4),AN(C_9)\},\{AN(C_5),AN(C_7)\},\{AN(C_5),AN(C_9)\},$
$\{AN(C_1),\neg CC(C_2),AN(C_7)\},\{AN(C_1),\neg CC(C_2),AN(C_9)\},$
$\{\neg CC(C_2),AN(C_3),AN(C_7)\},\{\neg CC(C_2),AN(C_3),AN(C_9)\},$
$\{\neg CC(C_2),AN(C_4),AN(C_7)\},\{\neg CC(C_2),AN(C_4),AN(C_9)\},$
$\{\neg CC(C_2),AN(C_5),AN(C_7)\}, \{\neg CC(C_2),AN(C_5),AN(C_9)\}\}$

One of these diagnoses is necessarily true provided the elementary models are correct (but not necessarily accurate). However, because the minimal diagnoses exclusively appear in this set, some additional faults may exist.

These diagnosis may be sorted according to prior probabilities (De Kleer and Williams, 1990).

5. CONTEXTUAL DIAGNOSTIC REASONING

Because of the non-exoneration principle, even if a test (4) based on a TS leads to a validate consistency, the interpretation of the state assumption cannot be global. However, a consistency means that the related state assumption is satisfied in the observation context (but also for all past observation contexts when memorizing validate inconsistency). Contextual information is also interesting and can be extracted.

When a test is consistent and valid, its state assumption has to be considered as contextually true: $\bigwedge_{i\in\Delta} h_i = \neg\left(\bigvee_{i\in\Delta} \neg h_i\right)$.

Consequently, if this test is consistent, all the component state assumptions of the following set are likely to be false:

$$\mathcal{I} = \left\{\neg h_i \,/\, i\in\Omega\right\} \quad (9)$$

Then a diagnosis $\mathcal{D}$ is called contextually compatible with a consistent and valid test if the diagnosis does not contain any contextually impossible assumptions belonging to (9):

$$\mathcal{D}\cap\mathcal{I} = \varnothing$$

A plausibility measurement (PM) is calculated for each global diagnosis. It is equal to the number of consistent and valid tests, which are contextually compatible with the considered diagnosis.

Returning to the example, the consistent and valid tests correspond to TS 1, 4 and 18. The contextually invalid sets are:

$$\mathcal{I}_1 = \left\{AN(C_1), AN(C_5), AN(C_7)\right\}$$

$$\mathcal{I}_4 = \left\{AN(C_3), AN(C_4), AN(C_6), AN(C_8), AN(C_9)\right\}$$

$$\mathcal{I}_8 = \left\{\begin{matrix} AN(C_1), AN(C_2), AN(C_3), AN(C_4), AN(C_5), \\ AN(C_6), AN(C_9) \end{matrix}\right\}$$

The global minimal diagnosis given in part V has been sorted by decreasing plausibility.

PM=2. $\{AN(C_8)\}$, $\{AN(C_2),\neg CC(C_2)\}$

PM=1. $\{AN(C_6)\}$, $\{AN(C_1),AN(C_7)\}$, $\{AN(C_2)\wedge AN(C_7)\}$, $\{AN(C_2),AN(C_9)\}$, $\{\neg CC(C_2),AN(C_3)\}$, $\{AN(C_3),AN(C_9)\}$, $\{AN(C_4),AN(C_7)\}$, $\{AN(C_4),AN(C_9)\}$, $\{AN(C_5),AN(C_7)\}$, $\{AN(C_1),\neg CC(C_2),AN(C_7)\}$, $\{\neg CC(C_2),AN(C_3),AN(C_9)\}$, $\{\neg CC(C_2),AN(C_4),AN(C_7)\}$, $\{\neg CC(C_2),AN(C_4),AN(C_9)\}$, $\{\neg CC(C_2),AN(C_5),AN(C_7)\}$

PM=0. $\{AN(C_1),AN(C_9)\}$, $\{AN(C_3),AN(C_7)\}$, $\{AN(C_5),AN(C_9)\}$, $\{AN(C_1),\neg CC(C_2),AN(C_9)\}$, $\{\neg CC(C_2),AN(C_3),AN(C_7)\}$, $\{\neg CC(C_2),AN(C_5),AN(C_9)\}$

Even if the plausibility measurement depends on contextual information, all the global diagnoses remain. Contextual results have just been used to sort the diagnoses from the most plausible to the least. Two minimal diagnoses out of 21 have emerged: that may be very helpful for an operator.

Note that all the diagnoses whose plausibility measurement is equal to the number of consistency results are the diagnoses which would have been obtained without taking into account the non-exoneration principle.

Plausibility measurement complete the measure based on prior probabilities (De Kleer and Williams, 1990), providing that probabilities are known, by a contextual information taking into account the consistent detection tests.

6. CONCLUSION

A general method to diagnose complex dynamic systems has been presented. It is based on a logical approach that can handle models for both normal and abnormal behavior. Current detection tests dedicated to dynamic systems such as state observers, parity relations, or other kinds of tests can be used to extract symptoms because of the separation between the symptom generation and the diagnostic reasoning.

This approach requires the modeling of the system components in an appropriate way: in addition to the usual behavioral relations, related component state assumptions have to be added as well as validity conditions. Despite its simplicity, validity condition is a powerful means for modeling local behaviors.

Global and contextual information can be extracted from symptoms coming from any kind of detection test whose meaning is defined by the concept of testable subsystem.

The resulting diagnostic reasoning procedure deals with available symptoms: it can be seen as a diagnosis machine, which analyses all the available information.

Some questions related to strategy such as Which detection tests have to be performed and When? should also be tackled when designing a complete diagnosis system. Because of the multiple possible configurations and because of the complexity of the algorithms, object-oriented implementation with threads as well as multi-agent systems are particularly relevant for implementing diagnosis systems which can be conveniently decomposed into several parallel algorithms. These problems are studied by the European MAGIC project (Köeppen-Seliger et al.,2002).

ACKNOWLEDGEMENT

This work is supported by the European Commission under the project EU-IST-2000-30009 MAGIC.

REFERENCES

Cordier, M.-O., P. Dague, M. Dumas, F. Lévy, J. Montmain, M. Staroswiecki, and L. Travé-massuyès (2000). A comparative analysis of AI and control theory approaches to model-based diagnosis. *14th European Conference on Artificial Intelligence*, Berlin, Germany.

Dague, P. (2001). Théorie logique du diagnostic à base de modèles. in: *Diagnostic, Intelligence artificielle et reconnaissance de formes*, B. Dubuisson, ed., 17-104, Hermès, Paris.

De Kleer, J., and B. C. Williams (1987). Diagnosing multiple faults. *Artificial Intelligence*, **32**, pp. 97-130.

De Kleer, J., and B. C. Williams (1990). *Diagnosis with behavioral modes*. International Joint Conference on Artificial Intelligence, MI, USA.

Declerck, P., M. Staroswiecki (1991). Characterization of the canonical components of a structural graph for fault detection in large scale industrial plants. *European Control Conference'91*, Grenoble, France.

Frank, P. M. (1990). Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy - A survey and some new results. *Automatica*, **26**(3), pp. 459-471.

Gehin, A.-L., M. Assas, M. Staroswiecki, Structural analysis of system reconfiguration (2000). *Safeprocess 2000*, Budapest, Hungary.

Greiner, R., B. A. Smith, and R. W. Wilkerson (1989). A correction to the algorithm in Reiter's theory of diagnosis. *Artificial Intelligence*, **41**(1), pp. 79-88.

Isermann, R., and P. Balle (1997). Trends in the application of model-based fault detection and diagnosis of technical processes. *Control Engineering Practice*, **5**(5), pp. 709-719.

Kapur, D., and Y. N. Lakshman (1992). Elimination Methods: an Introduction. Symbolic and Numerical Computation for Artificial Intelligence, Academic Press.

Köppen-Seliger, B., X. D. Ding, and P. M. Frank (2002). MAGIC - IFATIS. *IFAC World Congress*, Barcelona, Spain.

Mc Carthy, J. (1986). Applications of circumscription to formalizing common-sense knowledge. *Artificial Intelligence*, **28**, pp. 89-116.

Patton, R., P. Frank, and R. Clark (Eds) (1989). *Fault diagnosis in dynamic systems*, Prentice Hall.

Ploix, S., and C. Follot (2001). Fault diagnostic reasoning for set-membership approaches and application. *CCA/ISIC'01*, Mexico City, Mexico.

Reiter, R. (1987). A theory of diagnosis from first principles. *Artificial Intelligence*, **32**, pp. 57-95.