AECL-10149

ATOMIC ENERGY OF CANADA LIMITED

ÉNERGIE ATOMIQUE DU CANADA LIMITÉE

AN APPLICATION OF FIRST-PRINCIPLES DIAGNOSIS TO A THERMALHYDRAULIC SYSTEM

UNE APPLICATION DU DIAGNOSTIC ÉTABLI D'APRÈS DES PRINCIPES PREMIERS À UN SYSTÈME THERMOHYDRAULIQUE

P.A. LAPOINTE and J. CHUNG

Chalk River Nuclear Laboratories

Laboratoires nucléaires de Chalk River

Chalk River, Ontario K0J 1J0

March 1990 mars

ATOMIC ENERGY OF CANADA LIMITED

AN APPLICATION OF FIRST-PRINCIPLES DIAGNOSIS TO A THERMALHYDRAULIC SYSTEM

by

P.A. Lapointe and J. Chung*

Instrumentation & Control Branch
Chalk River Nuclear Laboratories
Chalk River, Ontario K0J 1J0

1990 March

*Professional-Experience-Year Student
from University of Toronto

AECL-10149

ÉNERGIE ATOMIQUE DU CANADA LIMITÉE

UNE APPLICATION DU DIAGNOSTIC ÉTABLI D'APRÈS DES PRINCIPES PREMIERS À UN SYSTÈME THERMOHYDRAULIQUE

par

P.A. Lapointe et J. Chung*

RÉSUMÉ

Les progrès récents en technologie des ordinateurs tels que ceux en intelligence artificielle et des multisupports (multimedias) interactifs, offrent de nouvelles possibilités d'accroître la sûreté des installations nucléaires et d'améliorer le rendement du personnel d'exploitation de façon considérable. Énergie atomique du Canada limitée (EACL) est en train d'établir une structure à laquelle on intégrera des approches récentes aux systèmes de soutien aux opérateurs. On a mis au point un prototype de système d'accès à l'information et d'affichage de celle-ci, de conseil et diagnostic en temps réel ainsi que des procédures interactives d'exploitation pour les centrales; il s'appelle le "Système d'Aide aux Opérateurs" (Operator Companion). Cette présente communication, concerne les travaux exécutés pour la réalisation du module de détection et diagnostic des défauts qui fait partie du "Système d'Aide aux Opérateurs".

On a réalisé un premier prototype du module pour un circuit simple de transfert de chaleur. On s'est servi d'une représentation de physique qualitative combinée à un diagnostic établi d'après des principes premiers faisant intervenir la technique de suspension des contraintes. Il fallait de l'information temporelle; on a intégré celle-ci au diagnostic à l'aide d'un graphe orienté pour enregistrer la dépendance des évènements. Ce graphe permet de modifier dynamiquement le modèle qualitatif pour refléter les variations du système au cours du temps. Bien qu'elle ne soit pas entièrement formelle, notre méthode a permis d'intégrer avec succès l'information temporelle pour établir le diagnostic et ainsi assurer l'identification des éléments défectueux tout en limitant le nombre de candidats erronés des essais effectués.

Dans cette communication, on résume les concepts du diagnostic qualitatif, décrit le schéma spécial établi pour le raisonnement temporel et présente un récapitulatif des résultats obtenus.

Instrumentation et Contrôle
Laboratoires nucléaires de Chalk River
Chalk River, Ontario K0J 1J0
1990 mars

* Étudiant de l'Université de Toronto en stage de formation professionnelle d'un an

ATOMIC ENERGY OF CANADA LIMITED

AN APPLICATION OF FIRST-PRINCIPLES DIAGNOSIS TO A THERMALHYDRAULIC SYSTEM

by

P.A. Lapointe and J. Chung*

ABSTRACT

Recent advances in computer technology, such as artificial intelligence and interactive multimedia, offer significant new opportunities to enhance nuclear plant safety and improve the performance of the operations staff. Atomic Energy of Canada Limited (AECL) is developing a framework on which newer approaches to operator support systems will be implemented. A prototype system has been developed for plant information access and display, on-line advice and diagnosis, and interactive operating procedures; it is called the Operator Companion. This paper describes the work performed for the development of the fault detection and diagnostic module within the Operator Companion.

An early prototype of the module was developed for a small heat transfer circuit. A qualitative physics representation coupled with first-principles diagnosis using constraint suspension was utilized. Temporal information was required; it was integrated into the diagnosis using a type of directed graph to record event dependencies. This graph dynamically altered the qualitative model to reflect changes in the system over time. Although not completely formal, our method has successfully integrated the time diagnostic information to permit the identification of the faulty components and limit the number of spurious candidates in the tests performed.

This paper summarizes the qualitative diagnosis concepts, describes the special temporal reasoning scheme developed, and presents a summary of the results obtained.

Instrumentation & Control Branch
Chalk River Nuclear Laboratories
Chalk River, Ontario K0J 1J0

1990 March

*Professional-Experience-Year Student
from University of Toronto

AECL-10149

TABLE OF CONTENTS

1. INTRODUCTION

Nuclear power plants have become increasingly complex as designers and operators strive to achieve balances between power plant production and safety goals, and between manual and automatic control. Atomic Energy of Canada Limited (AECL) is developing new control centre concepts for its CANDU[1] nuclear power plants that incorporate advanced technologies, such as artificial intelligence and expert systems, to maximize the strengths of both the human and the machine during normal and abnormal operating conditions.

An environment has been developed into which newer approaches to operator support systems will be integrated; it is called the Operator Companion [1]. This environment provides access and display to plant information, on-line advice and diagnosis, and interactive operating procedures. This paper presents experimental work performed to develop a fault detection and diagnostic module for the Operator Companion.

Expert systems have been very successful in providing computing solutions in areas where experience has traditionally played a large part. Conventional software techniques are difficult to use with problems where no algorithmic solution method exists, or where parameters are ambiguous or missing. An expert system encodes the knowledge of a domain expert and relies on this knowledge for its functionality.

Model-based representations have been advocated recently as providing solutions for some of the shortcomings of early expert systems. These first-generation systems reasoned with unstructured associative knowledge: the aim of the model-based representation is to provide the reasoner with an internal model of the universe of discourse which encodes more fundamental knowledge than a set of empirical rules.

Our prototype module is for a small heat transfer circuit; it is based on a model representation using qualitative physics [2], and first-principles diagnosis using constraint suspension [3]. Because of the dynamic nature of the sub-system modelled, temporal information must be integrated into the diagnosis. A special graph representation records event dependencies and alters the qualitative model, to reflect changes in the system over time. An object-oriented (OO) language for PCs, Smalltalk/V 286 [4], has been used for the developments.

This paper summarizes the qualitative diagnosis concepts, describes the special temporal reasoning scheme developed, and presents a summary of the results obtained.

2. QUALITATIVE PHYSICS AND DIAGNOSIS

The qualitative physics modelization used is based on De Kleer and Brown [2]. Qualitative physics is a relatively new field of artificial intelligence research that attempts to encode non-formal (or common sense) physical reasoning. Its identifying characteristic is the abstraction of quantities and functions from real-valued domains to discrete ones.

The qualitative physics we have used abstracts real values for parameters into qualitative ones based on the mapping:

$$\{[-\infty,0),0,(0,+\infty]\} \rightarrow \{\ -,0,+\ \}$$

A functional abstraction is performed by defining the operations of qualitative addition and multiplication; the transfer table for qualitative addition is given in Figure 1. In this way, much of the detail present in quantitative analysis is removed. Qualitative functions are composed of

---

[1]CANDU: CANada Deuterium Uranium, Registered Trademark.

qualitative differential equations called *confluences*. A confluence represents a qualitative constraint on a set of variables and their qualitative derivatives.

Z_1 \ Z_2	+	0	-
+	+	+	?
0	+	0	-
-	?	-	-

$Z_3 = Z_1 + Z_2$

Figure 1: Qualitative Addition Table

The qualitative physics proposed by De Kleer and Brown is component-based. A hierarchical approach may be used to build complex components. The qualitative model has been used for diagnosis. A first-principles approach to diagnosis is taken, whose problem is to "determine those system components which, when assumed to be functioning abnormally, will explain the discrepancy between the observed and correct system behaviour" [5]. Constraint suspension is a method of diagnosis that uses a constraint model of the observed system. In our case, this is a qualitative model. The system is described with a set of qualitative constraints - confluences - that apply on qualitative variables. Suspension of sets of confluences is taken to reflect the failure of certain components. If the remaining constraints become simultaneously satisfiable[2], the components represented by the suspended sets are possible failure candidates. The prototype system assumes that only a single fault is present.

Constraint propagation [6] tests the consistency of the network of interrelated constraints that represent the model. When ambiguities occur (because of the nature of the qualitative arithmetic), assumptions are made to resolve the ambiguity [2]. In the qualitative algebra, this requires the generation of solutions for the assumed values: -, 0 and +. An assumption-based truth-maintenance system [7,8,9] efficiently tracks the creation of the assumptions produced. A simple backtracking search then resolves independent assumptions made during constraint propagation.

3. TEMPORAL INFORMATION

Temporal information had to be included in the diagnostic system as the transient behaviours of heat transport systems take a significant amount of time and thus can not be ignored. This transient behaviour is mostly due to the propagation time of the temperature perturbations with the fluid transport. A traditional approach is to use a multi-states representation with simulation of all possible state transitions [10]. This methodology has good theoretical background merits but requires a lot more modelling and programming, and it is computer intensive.

The aim was to create a diagnostic scheme incorporating temporal behaviour and using the constraint satisfaction, assumptions generation and truth-maintenance algorithms. The approach selected does not require the enumeration of fault states, and only the quasi-static single-state component model is utilized. Each component is modelled using a single set of confluences with qualitative derivatives only. An external scheme, higher than the component level, addresses the temporal behaviour.

---

[2]Satisfiable means that we could find at least one set of values for the variables that will satisfy all the constraints considered.

The central idea of the scheme is to cut some constraints of the network, to remove the inconsistency between sensor values during the time the temperature effect takes to propagate.[3] Diagnostics can then be performed by normal component constraints suspension conducted on top of the time-suspended network. As qualitative events occur in time, the system uses a special directed graph (described in Section 4), to identify which constraints need to be time-suspended.

Figure 2 shows a simple arrangement of pipes connected to a hot-water tank, with the assumption of no heat loss. The water flow is assumed to be at a constant rate. Temperature sensors S1 and S2 are located at pipe joints b and c, respectively. In the event of some behavioural malfunction in the hot-water tank, such as no more hot water in the tank, the temperature will drop at the output of the tank (malfunction making δT_a = -)[4]. The effect of the malfunction will be detected at sensor S1 (δT_{S1} = -) after some delay.

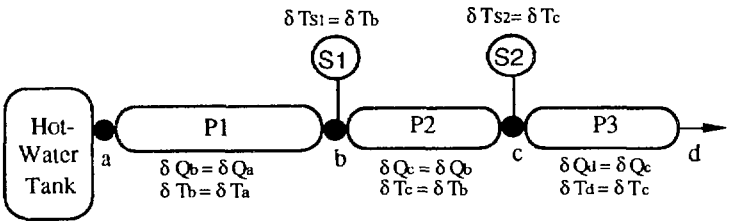

Figure 2: Hot-water Tank Example

At this point, we have two inconsistencies for the perturbation confluences. The first inconsistency is caused by the faulty behaviour upstream to the sensor (meaning before the sensor) and is indicated by the set of confluences: $\delta T_a = 0$ (for the normal tank behaviour), $\delta T_b = \delta T_a$ (pipe behaviour), $\delta T_{S1} = \delta T_b$ (sensor behaviour) and δT_{S1} = - (sensor indication). The constraint suspension diagnosis will remove the "upstream" inconsistency upon finding that any of the components represented by these confluences can be faulty (tank, pipe, or sensor).

The second inconsistency (manifested here with: δT_{S1} = -, $\delta T_{S1} = \delta T_b$, $\delta T_c = \delta T_b$, $\delta T_{S2} = \delta T_c$ and $\delta T_{S2} = 0$) is a natural consequence of the time required for the temperature perturbation to go from sensors S1 to S2. This inconsistency can be removed by excluding the pipe P2 confluence ($\delta T_c = \delta T_b$). The pipe itself is not faulty, rather it is in a transport-delay qualitative state ($\delta Q_c = \delta Q_b$ and $\delta T_c = 0$).

As we opted to not use a multi-states representation, a method had to be found whereby the causality path (the chain of confluences) between the two sensor measurements (δT_{S1} and δT_{S2}) could be cut in some way. The idea of affecting a specific component like a pipe is not general enough. Instead, we decided to modify the sensors. The sensor S2 monitoring for the temperature effect from S1 should be cut during the propagation interval. But, the sensor S2 must also continue to constrain the temperature perturbation value of the pipe P3 input to zero. To achieve this approach, temperature sensors are modelled in a special way (see Figure 3). The temperature effect will be propagated *through* the sensor, not just monitored by it.

---

[3] In this paper, we refer to that process by the expressions "ensuring the time-consistency" or "time-suspending constraints".

[4] δT_a represents the qualitative derivative for the temperature at node "a".

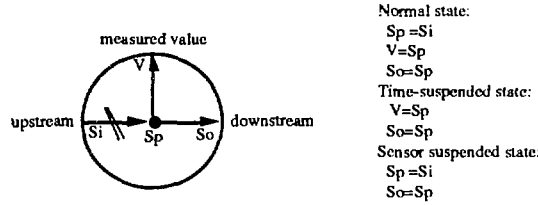

Figure 3: Complex Sensor Component

The constraint link to the sensor is time-suspended by removing the constraint Sp = Si. This sensor representation assumes some orientation of the sensors with flows that should be known a priori.

The same approach can be applied to flow and pressure sensors, as they can be modelled as monitors by leaving the So terminal free.

4. SENSOR TIME-SUSPENSION

We developed a specific technique to determine the time-suspension state of sensors based on other sensor events (changes in the qualitative derivative values of monitored variables). Figure 4 illustrates a thermalhydraulic loop, including a heat exchanger, a pool, a constant flow pump, some pipes and several sensors. Its function is to heat the pool. The primary side is assumed to be connected to a normally constant source of fluid. We make the following assumptions:

- all the variable values are always positive (normal behaviour),
- all confluence parameters are qualitative derivatives (model of equilibrium perturbations), and
- magnitude(T_1) > magnitude(T_5) > magnitude(T_6) (i.e., the pool is being heated).

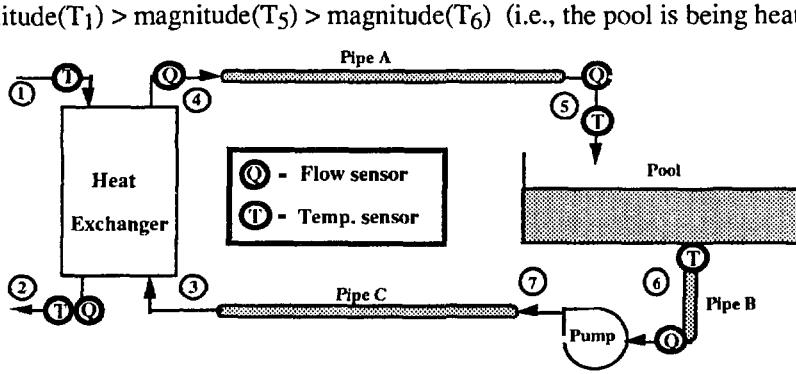

Figure 4: Simple Thermalhydraulic Loop Example

In equilibrium, all the sensor indications will initially show zero derivatives. A malfunction will first affect some state-variable derivative(s) before being observed as a sensor deviation. Only at this point is the time-suspension of sensors required. Thus, it makes sense to start from a normal directed-graph for causality [11] and propagation-delays information (see Figure 5) to derive information required for time-suspension. The graph shows state variables

(or derivatives) connected by causality relation arrows and significant propagation delays. Also, the double-circled elements represent sensors attached to state variables.

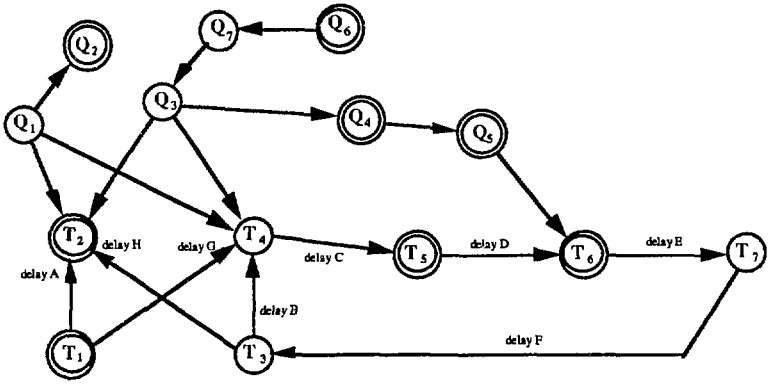

Figure 5: Time-marked Directed Graph for the Example in Figure 4

We then construct another diagram from the normal directed-graph that will contain only the sensors, though it has the same relevant causality and time information (see Figure 6). We obtain this diagram, named the *Predictor*, by the following procedure:

- For all the sensor couples, find connecting paths in the original diagram that do not include any variable directly monitored by a sensor.
- If paths are found, connect the sensor with the same causality direction and indicate the sum of the transport delays of the shortest path as the new delay.

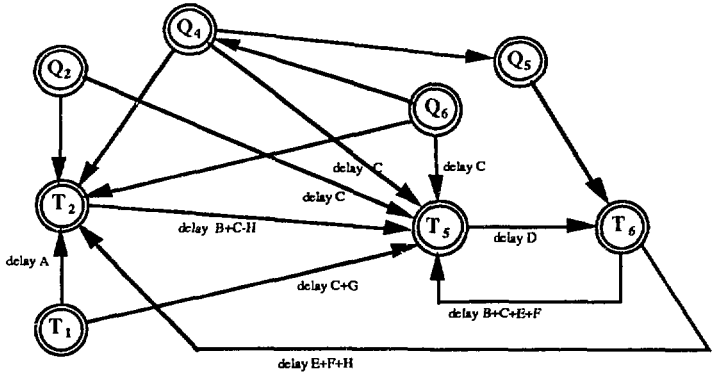

Figure 6: Predictor Graph for the Example in Figure 4

We then use the predictor as follows to diagnose from a sequence of qualitative events (the sensor perturbation values with their occurrence times):

- Process all the quasi-simultaneous events (respective to the time resolution of measurements) with the predictor: for each event, time-suspend the connected sensors.
- Generate a time-out delay larger than the propagation delay for each time-suspended sensor. If the time-out occurs for a sensor before a perturbation event, reconstrain the sensor to provide a more restricted diagnosis.

- Diagnose by suspension of component confluences on the resulting network. The diagnostic module produces a list of candidate components valid at this time.
- Process the next group of quasi-simultaneous events to obtain another candidates list and continue the sequence up to the end of the event sequence (we limit the acquisition time to a two-minute window).

5. IMPLEMENTATION

The program has been implemented on a Compaq 386/16 personal computer, with a 80287 coprocessor, in the Smalltalk/V 286 environment [4]. Smalltalk has been used because it supports good data and procedure abstraction and provides a large amount of reusable primitives. The complexity of some algorithms used is exponential, which may cause computational intractability. In the implemented system, time limits were placed on inferences to terminate the procedure in case of an exponential explosion.

6. TEST RESULTS

The prototype was tested on a small heat transfer circuit using seven different cases of simulated failures. A numerical simulation was used to generate data processed to produce event sequences[5] for input to the diagnostic system. Two different preprocessing approaches were used:

"intelligent" preprocessing: The simulation results were examined by the authors and the events extracted by an intelligent filtering.

"thresholds" preprocessing: An event is considered to have occurred when a variable exceeds a 0.1% threshold from its equilibrium value. The occurrence time of the event is computed by linear extrapolation, as illustrated in Figure 7.

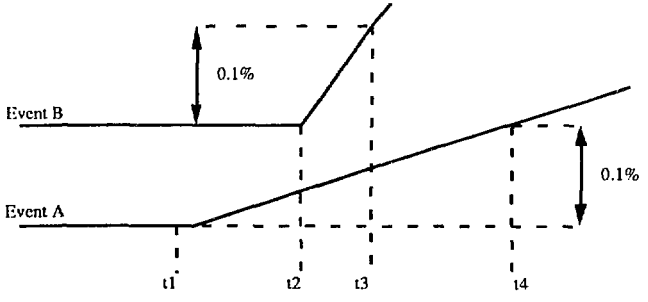

Figure 7: Ordering Problem Example

Two methods have been used to give a global interpretation of the results. The first one consists of taking the intersection of the candidates list produced by the diagnosis; it is named the time-group intersection. The other method is named the voting technique; it counts as votes

---

[5] A sequence is composed of all sensor perturbation values with their occurrence times for a simulated failure case.

the number of lists that contain each particular component. Table 1 summarizes the results for all simulated failure cases. The first column gives the failed component name, the failure nature and its relative importance. The following columns describe for both the "intelligent" and the "thresholds" preprocessing the time-group intersection and the voting-technique results.

For the "intelligent" preprocessed sequences, the simulated failed component is always an identified candidate, and other candidates in the list are usually adjacent components (physically adjacent and with no sensor in between) which are valid. For the "thresholds" preprocessing method, the time group intersection method is inadequate (producing only empty intersection lists) as some events are not detected and missing from the sequences. Finch and Kramer [12] refer to this as the absence-of-measurement problem. These events are in fact present but they are too small to be detected with the deadband technique. The voting technique helps but the discrimination between valid and invalid candidates is often only a matter of one vote difference (see PL and PK cases). To deal with the absence-of-measurement problem some heuristics will have to be used. In general, results using the voting technique show all simulated failed components as candidates. Also, some spurious candidates are produced (see the last line of Table 1) because of the ambiguity of the qualitative physics.

Table 1: Summary of Results

	"intelligent" preprocessing		"thresholds" preprocessing	
Fault simulated	Time group intersection	Voting	Time group intersection	Voting
Pipe PJ leak (5%)	OK*, one adjacent	OK, one adjacent (7)	no candidate	OK, one adjacent (4)
Pipe PL leak(20%)	OK, one adjacent	OK, one adjacent (13) six spurious (10)	no candidate	OK, one adjacent (3) six spurious (2)
Pipe PK leak (5%)	OK, one adjacent	OK, one adjacent (10) six spurious (6)	no candidate	OK, one adjacent (3) six spurious (2)
Pipe PH leak (4%)	OK, one adjacent	OK, one adjacent (6)	no candidate	OK (4), one adjacent (5)
Pipe PI leak (4%)	OK, one adjacent	OK, one adjacent (6)	no candidate	OK, one adjacent (3)
Regulation valve controller offset (+50%)	OK, one adjacent	OK, one adjacent (5)	no candidate	OK, one adjacent (3)
Heat exchanger efficiency drop (-50%)	OK, one spurious	OK, one spurious (7) one spurious (6)	no candidate	OK, one spurious (7) one spurious (6)

* "OK" means: the simulated failed component is a candidate.

7. CONCLUSIONS

A semi-heuristic time-representation approach has been created that could be applied in conjunction with qualitative modelling to the diagnosis of continuous variables systems. A prototype has been developed to explore the efficiency of the approach. The diagnostic method used with the temporal predictor graph has produced all the failure candidates required, employing a voting technique. For some specific failure cases, some spurious candidates may appear.

Although not completely formal, our method has successfully integrated the time diagnostic information to permit identification of faulty components and limit the number of spurious candidates in the tests performed. The approach is considerably more efficient than the one using qualitative simulation with a formal temporal representation. This approach can be combined with conventional expert system paradigms to achieve efficient diagnosis.

8. REFERENCES

[1] A. Natalizio, J.W.D. Anderson and H.E. Sills, "Operator Companion: Advanced Support Systems for Plant Operators", Atomic Energy of Canada Limited, Report No. AECL-9612, 1988.

[2] J. De Kleer and J.S. Brown, "A Qualitative Physics Based on Confluences" Artificial Intelligence 24, 1984, pp. 7-83.

[3] R. Davis, "Diagnostic Reasoning Based on Structure and Behavior", Artificial Intelligence 24, 1984, pp. 347-410.

[4] Digitalk Inc., Smalltalk/V 286 Object-Oriented Programming System (OOPS) - Tutorial and Programming Handbook, Los Angeles, 1988.

[5] R. Reiter, "A Theory of Diagnosis from First Principles", Artificial Intelligence 32, 1987, pp. 57-95.

[6] G.J. Sussman and G.L. Steele Jr., "CONSTRAINTS- A Language for Expressing Almost-Hierarchical Descriptions", Artificial Intelligence 14, 1980, pp. 1-39.

[7] J. De Kleer, "An Assumption-based TMS", Artificial Intelligence 28, 1986, pp. 127-162.

[8] J. De Kleer, "Extending the ATMS", Artificial Intelligence 28, 1986, pp. 163-196.

[9] J. De Kleer, "Problem Solving with the ATMS", Artificial Intelligence 28, 1986, pp. 197-224.

[10] B.J. Kuipers, "Qualitative Simulation", Artificial Intelligence 29, 1986, pp. 289-338.

[11] M. Iri, K. Aoki, E. O'Shima, and H. Matsuyama, "An Algorithm for Diagnosis of System Failures in Chemical Process", Computers & Chemical Eng., vol. 3, 1979, pp. 489-493.

[12] F. E. Finch, and M.A. Kramer, "Robust Handling of Dynamics and Multiple Failures in a Diagnostic Event Analyzer", Conference on Expert Systems Applications for the Electric Power Industry, Orlando, Florida, 1989 June.

ISSN 0067-0367

To identify individual documents in the series we have assigned an AECL- number to each.

Please refer to the AECL- number when requesting additional copies of this document

from

Scientific Document Distribution Office
Atomic Energy of Canada Limited
Chalk River, Ontario, Canada
K0J 1J0

Price: A

ISSN 0067-0367

Pour identifier les rapports individuels faisant partie de cette série nous avons assigné un numéro AECL- à chacun.

Veuillez faire mention du numéro AECL- si vous demandez d'autres exemplaires de ce rapport

au

Service de Distribution des Documents Officiels
Énergie atomique du Canada limitée
Chalk River, Ontario, Canada
K0J 1J0

Prix: A

958-90