Specialists' Meeting on Advanced Information Methods and Artificial Intelligence in Nuclear Power Plant Control Rooms

HALDEN
13-15 septembre 1994

Contribution of Qualitative Analysis and Fuzzy Sets to Industrial Process Fault Diagnosis : Application to the DIAPASON Project[1]

Jacky MONTMAIN and Lydie LEYVAL

Commissariat à l'Energie Atomique
Rhone Valley Research Center - Marcoule
Applied Computer Science Laboratory
BP 171, 30207 Bagnols-sur-Cèze Cedex, France
Phone: (33) 6679-6631 - Fax: (33) 6679-6638

Abstract : *The construction of fault indicators is the foundation of model-based fault diagnosis. The development of precise mathematical models for complex facilities is generally difficult and expensive; new and less constraining techniques, notably seeking to account for behaviour, open new perspectives for fault detection and diagnosis. The authors propose a combined approach based on quantitative processing with qualitative assessment of the results. A veritable numerical-symbolic interface then ensures a more satisfactory bolonce between the two levels of knowledge - analytic and heuristic - necessary to optimize the performance of a diagnostic procedure.*
Our supervision support system DIAPASON provides operators of industrial continuous processes with an aid to watch and diagnosis. The reasoning is based on a causal graph and on a knowledge base. After an overview of qualitative simulation, defect diagnosis and fault diagnosis, the way in which these three cooperate in DIAPASON is amplified.

21 refs 5 figs

Keywords : *Supervision, Qualitative Reasoning, Fuzzy Sets, Decisional Analysis, Fault Diagnosis*

PART I : QUANTITATIVE - QUALITATIVE COMBINED APPROACH for SUPERVISION

1. Introduction

For many years, improving the productivity of an industrial facility has involved enhanced automation of the means of production. The development of control theory, together with the incessant progress of computer systems and digital processing methods, have made it possible to increase the quality of products while reducing production costs. In normal operation, the operators' task is now reduced to simple supervision of the facility and its control and monitoring system. Conversely, in the event of an incident, an overall analysis of the situation allows the operators to make decisions quickly and effectively, for example in choosing among corrective actions or crippled-mode operation.

In order to improve the productivity of a facility today, it also appears necessary to be concerned with monitoring its availability. This has led to the development of operator aids, notably in the area of fault diagnosis. Their purpose is to ensure early detection of abnormal situations and to interpret them so the operator may control the process more efficiently.

---

[1] *The Applied Computer Science Laboratory, headed by J.M. PENALVA, has been working on the research programme DIAPASON since 1987.*

1879

2. Model-Based Diagnostic Approaches

2.1. Numerical Fault Diagnosis Models

The current trend in fault diagnosis is to estimate process behaviour by the use of a model. Conventional approaches based on numeric models are capable of detecting fault conditions (affecting components, sensors or control devices) at an early stage - well before the alarm system is activated.

The various approaches to formalizing diagnostic reasoning differ by the type of process knowledge they use. In some cases, the structure and normal operation of the components are known, but nothing is known about the reasons or the occurrence mechanisms of fault conditions; consequently, the procedure is to detect deviations from normal behaviour. In other cases, information is available only on fault conditions and their symptoms, and the task is to account for abnormal observations. Two major tendencies are in competition in designing fault indicator models.

One is based on process state variables: relations among measured variables are used to compare measurement results with calculated predictions, and thus to reveal residual differences between the observed and modeled behaviour, and allow detection [1].

The second trend is based on process structural parameters. If the cause-to-effect relation between two variables is modeled mathematically, it is characterized by one or more parameters that must be identified. The type of fault can be diagnosed by any significant change in the parameter values; the objective is to determine an incident situation corresponding to each type [2].

While an unmeasurable perturbation or a fault must be detected and identified by the diagnostic system, modeling errors (due to nonlinearities, poorly identified or unactualized parameters) and measurement system noise classically result in false alarms, making it necessary to include tolerance thresholds. This delays early detection, however, and implies the highly restrictive hypothesis that the effects of a fault condition can be distinguished from a modeling error simply by their amplitude.

Moreover, the use of identification or estimation methods is not always easy in an industrial context. Positive identification requires an adequate stimulus, and represents a significant constraint in an industrial process. Nonlinearities limit the model validity to a specific operating range, and thus tend to promote a multiple-model approach. The problem of available knowledge is accompanied by that of robustness. The difference between an ideal analytical model and the actual knowledge of an industrial facility is such that the extent and precision of the knowledge required may necessitate time and expenditure that jeopardize the feasibility of this type of fault diagnosis: the applications remain of limited size and restricted scope.

A process is compatible with fault diagnosis if it includes sensors and a system for analyzing the resulting data. It is unfortunate that diagnostic feasibility is not taken into account at the design stage like any other performance criterion. The number and location of the sensors could be defined in diagnostic terms, rather than using sensors initially provided for other purposes as is all too often the case [3].

2.2. Qualitative Fault Diagnosis Models

Faced with the increasing complexity of industrial facilities and the limits of conventional approaches, it appears reasonable to develop systems capable of manipulating incomplete data, vague or uncertain information, to ensure robust fault diagnosis despite multiple sources of false alarms. Qualitative approaches require less knowledge of the process itself; variables are quantified into discrete ranges such as {low, normal, high}, making it possible to describe simple relations among variables in a way that may prove sufficient for diagnostic reasoning.

The major drawback of these approaches is incompleteness. A single event may give rise to several interpretations, partly because of the conversion of numerical input data into discrete qualitative value ranges, and partly because of ambiguous qualitative processing (what is the result of an excessively high influence combined with an excessively low influence?) [4] [5].

2.3. A Combined Approach

We adopted a combined approach in which the process is represented by causal graph relating process variables and where the arcs are parameterized by simple qualitative notions, notably to account for the dynamics of the phenomena [6]. To represent process behaviour using this model, we replaced the numerical simulation notions of precision and calculation steps with an event-driven simulation that is better suited to the supervisor's level of abstraction: the simulation is activated only when significant events are detected at process inputs; the events are propagated in the graph using the data assigned to the arcs to determine the behaviour of the other variables; the evolution of a variable in time is then described as a succession of pertinent modifications [7].

This approach represents a tradeoff between quantitative and qualitative methods. The data are processed numerically, but the simulation results are curves that express the overall process behaviour better than exact numerical variables. The results therefore require a qualitative interpretation for fault diagnosis: this involves manipulating vague or uncertain information, ranging from erroneous measurements to purely symbolic data to modeling imprecision, in order to make the system less sensitive to noise.

Generally, in an incident situation when the operator must diagnose a fault before deciding on the most suitable corrective action, numerical data (alarm thresholds, measurements, etc.) are available, but the operator's knowledge of the process is essentially symbolic (procedures, etc.). The data flow must be interpreted and filtered before applying heuristics. We propose a numerical-symbolic interface to provide a better balance between the two levels of knowledge required to optimize the performance of a diagnostic procedure.

The operating principle of the diagnostic system based on the causal graph is the following: fault detection by comparison of the actual and simulated evolution of the variables, then filtering of the faults by testing possible correlations between the detected faults and the relations assigned to the causal graph. These two algorithms consist of purely numerical basic procedures to assess various surveillance criteria (mean square deviation, etc.), together with a qualitative interpretation layer representing the heuristics that manipulate them. Fault detection and filtering are modeled as decision-making processes in an imprecise context: the problem is to aggregate the pertinence of the elemental performance or preference criteria (e.g. curves of similar shape) to obtain the overall assessment of an action (e.g. initiate a diagnostic routine); the criteria are described by fuzzy sets to account for the vague decision-making environment.

3. Fuzzy Sets for Interpretation and Decision-Making

3.1. The Numerical-Symbolic Interface and Discontinuities in Decision Aid Systems

Any classification system based on comparison with threshold values is subject to unstable conclusions and involves a risk of error. This drawback can also affect a qualitative approach, in which instability is introduced when selecting the conversion threshold. The decision will be very different depending on whether the criterion investigated (e.g. a simulation error) is equal to a specified threshold plus or minus epsilon regardless of the amplitude of epsilon. This problem of decision-making discontinuities led us to use fuzzy sets.

Fuzzy sets provide a simple tool for interfacing low-level numerical data with high-level symbolic knowledge, since they allow for the continuous nature of the variables manipulated within a symbolic representation [8].

In this regard, Dubois indicated that the idea of using fuzzy sets arose from the need to represent loose specifications such as nonbinding constraints (for which minor violations are permissible), flexible criteria (concerning acceptable or desirable values), 'elastic' classes (often used for rough reasoning and to provide a continuous transition from one class to another), vague predicates or quantifiers (frequently used in natural languages), adjustable instructions or procedures (capable of adapting to distinct but similar situations). In each case, the objective is to enhance robustness by refusing the sharp discontinuities that would arise from the use of precise limits for the sets included in the specification: sudden transitions from acceptable to unacceptable values, from values for which a procedure is applicable to very similar values for which the same procedure is not applicable [9].

3.2. Modeling the Decision-Making Process

Fuzzy sets can also allow the development of mathematical models of imprecise or uncertain phenomena for application to decision aids. The goal is to help the decision-maker select an action that will produce the desired consequences from the standpoint of the imposed criteria and constraints [10].

The state of the environment is assumed to be known, so that each action 'a' has a known consequence described by a series of values $[m_1(a), m_2(a), ..., m_p(a)]$. Each measurement $m_i(a)$ is a measurement in the sense of criterion 'i' (cost, size, consumption, etc.). m_i defines an application of the set of possible actions 'A' on an objective scale X_i, and the set 'X' of consequences is identified with the Cartesian product $X_1 \times X_2 \times ... \times X_p$. The measurement scale X_i is either a continuous or a possibly finite discrete scale. The problem is therefore to aggregate the criteria in compliance with the decision-maker's overall assessment of the potential actions [10].

Fuzzy sets appear to be a natural means of modeling a decision-maker's wishes concerning the consequences of a choice. Clearly, the decision-maker will express a choice in linguistic terms, especially where continuous scales are involved. The overall objective may be characterized by a complex criterion (i.e. with more than one scale) that must be broken down into elemental criteria. The set of acceptable decisions 'D' is a fuzzy set of the set of possible actions, obtained by aggregating the sets of best actions Gi derived from partial objectives $G_{i=1,p}$. The membership function μ_D is such that:

$$\forall a, \mu_D(a) = [\mu_{G_1}(m_1(a)), ..., \mu_{G_p}(m_p(a))]$$

where 'h' is a fuzzy set operator to be determined (associative disjunctions and conjunctions, associative means, symmetric sums, etc.).

4. Application to Fault Detection and Filtering

4.1. Fault Detection Principle

In order to allow for the approximations of causal graph modeling and the imprecision of the measurement systems, a variable is considered faulty not only on the basis of the simulation error, as in the conventional procedure, but also by the resemblance between the shape of the actual and simulated curves and the distance between them (these criteria are our own, as they clearly depend on the model).

The fault detection decision-making environment may be compared to a situation in which three experts continuously monitor a process, each with their own criteria. The problem is to benefit from their advice and combine their suggestions to reach the optimum final decision[2]. The decision-making process may then be described in the following way. The action to be evaluated is to compare the simulated and actual evolutions. The measurements m_i(compare) are the numerical criteria associated with the value, shape and distance of the curves (p=3). The partial consequences of each of these objectives are their respective scales subdivided into previously determined symbolic ranges (e.g. major_positive error) modeled by fuzzy sets. The decision-makers' objectives can be expressed, for example, as 'a small simulation error' (objective G1), 'similarly shaped curves' (G2) and 'closely spaced curves' (G3). To aggregate these criteria, the fuzzy set operators were chosen for their algebraic properties and semantic interpretation in order to conform to the experts' points of view [12].

4.2. Fault Filtering

The decision to consider a newly observed fault as a simple consequence of the faults observed on the preceding variables in the causal graph is made after qualitative analysis of the orders of

---

[2] For KONING, *the cooperation of different heuristic knowledge in order to make the best decision may be reduced to aggregating individual opinions. Indeed, this choice is similar in many respects to individuals voting to elect the best candidate [11].*

magnitude of the contribution due to each predecessor, interpreted according to fuzzy rules. It can be shown that this algorithm may be described as a recursive procedure of the following elementary decision-making process: decide whether an antecedent is responsible for the fault observed on a detection variable (a variable for which a significant fault was detected in the sense of the preceding algorithm). The process is then applied recursively from the relevant antecedents, which are in turn considered as detection variables. The result of this procedure is the trace or signature of the fault condition in time and in the process, i.e. the subgraph excerpted from the causal graph in which the initial fault propagated from the source variable (the variable actually affected by the initial fault condition) to the detection variable [12]. This strategy is therefore capable of handling multiple fault conditions, i.e. of diagnosing several source variables responsible for a single detected fault.

5. Conclusion

In this approach, the simulation and error calculation tools are purely numerical, but the results are interpreted in a qualitative manner. Aggregating fuzzy sets provides for multicriteria decision-making analysis that is robust not only for fault detection but for fault filtering as well. The use of families of criterion aggregation operators and the introduction of fuzzy sets make it possible to deal with the imprecision of the decision-making environment; in particular, they allow significantly greater flexibility in choosing parameters for the algorithms. It should be noted that fault detection and diagnosis based on qualitative interpretation of the simulation may in some cases delay the detection of a process fault condition: this is the price of the tradeoff between early detection and robust control of false alarms.

The interpretation of several criteria may be considered as a decision-making process and reduced to a problem of aggregation. Criterion aggregation models described by fuzzy sets as decision-making aids are a promising tool for supervisory functions: supervision corresponds to the level at which an operator must make decisions in an imprecise and uncertain context, taking into account large amounts of data of various types. The decision-maker must be capable of analyzing and then interpreting the numerical and graphical data, generally in terms of orders of magnitude or qualitative values in order to relate them to the appropriate knowledge mode and evaluate the state of the process, and if necessary decide to modify the process control parameters.

PART II[3] : The SUPERVISION SUPPORT SYSTEM DIAPASON

1. Introduction

DIAPASON is a system designed to help in the supervision of continuous processes which evolve with slow dynamics, such as those used in nuclear engineering for the retreatment of nuclear fuels. It results from the ideas exhibited in part I of the paper.

DIAPASON provides the operator with a synthetic image of the process thanks to modelling inspired by qualitative physics and process control theory.

DIAPASON can predict the evolution of the process thus allowing management by anticipation : it provides the evolutions of relevant variables in the process, whether measurable or not, and gives associated explanations.

DIAPASON can promptly detect and analyse incidental situations for preventive maintenance or for effective management in degraded conditions : the results of a defect diagnosis module, based on model/process comparison, are fed into a fault diagnosis module using structural knowledge of the process.

---

[3] *This part is extracted from " A Supervision Support System for Industrial Processes", by J.M. PENALVA, L. COUDOUNEAU, L. LEYVAL and J. MONTMAIN, published in IEEE Expert, vol. 8, n° 5, October 1993.*

The process chosen as an application consists of a pulse column with its associated systems for feed, transfer and control. In fact, the validation of the prototype DIAPASON could have been easily made, because we have at our disposal a classical numerical simulator of the process ; the results presented in this paper have been realized when connected on line to the numerical simulator.

2 - Prediction

2.1 - The causal graph

The modelling is issued from works achieved by Gentil et al [6] : the model is based on a causal graph whose nodes represent the process variables and whose arcs represent causal links between those variables. Since the purpose of the model is supervision, only those variables that are useful in process management are shown, whether or not they are measurable. Figure 1 shows the causal graph of the pulse column in its emulsion stage, including its feed systems.

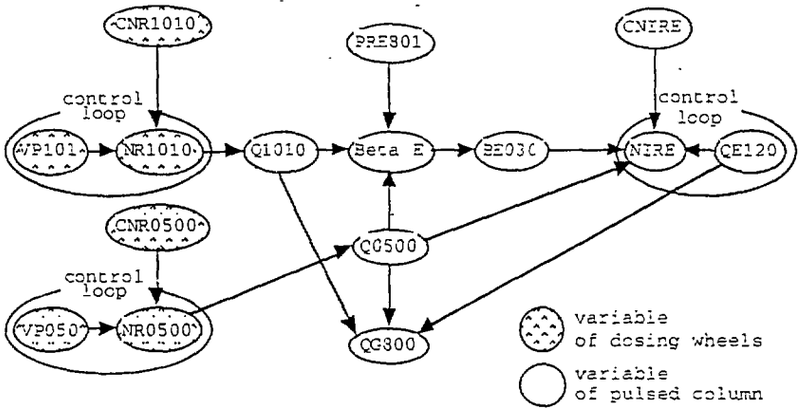

Figure 1 : The causal graph for the pulse column

2.2 - Behaviour modelling

Variable's behaviours are described by their temporal evolutions. The evolution of a variable can be represented by a piecewise linear time function obtained through a segmentation algorithm [12] (see Figure 2). An event is a portion of an evolution where the function's slope changes significantly ; it is approximated in a linear way. An evolution can thus be regarded as a chronological sequence of events.

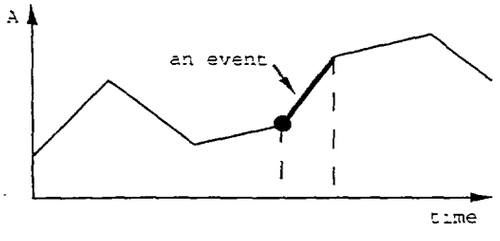

Figure 2 : Qualitative evolution of variable A

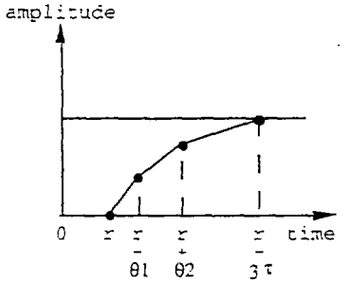

Figure 3 : First Order

Qualitative Response to a step

Each arc on the graph represents the influence of one variable on another, using notions of process control theory such as static gain, pure delay, and settling time. It makes an evolution fit an event, so as to obtain a consistent signal for the next variable. The function of an arc is called a Qualitative Transfer Function (QTF), by analogy with classical process control theory. These functions enable us to obtain a system's qualitative response to the input types (the step and the ramp, which are the elements that constitute an event). Figure 3 shows the qualitative response of a first order system to a step.

More complex QTFs have been created to represent the phenomena in a control loop : for example, to model the behaviour of the regulated and the control variables in the loop, following a disturbance or a change in the set point. The library of QTFs is growing as needs arise. It includes quite diverse functions corresponding for example to an amplifier system, a first order system, a derivative system, and even systems of higher order than 1. However, we would like to model only simple systems, in view of the objective. Indeed, it is unlikely that the operator in charge of a plant would describe the relationship between two variables linked by a single arc as a complicated system.

2.3 - Dynamic simulation

The model receives as inputs one or more significant events related to one or more input variables (which fit with the graph's roots), as well as the initial values of all the variables. The simulation consists of propagating each evolution through the graph in chronological order, event by event. Propagation stops when there are no more events left or when the simulation has reached its horizon.

Since event modelling takes into account the dynamics of phenomena, it is better adapted to process supervision than are classical qualitative physics models based only on signs. The events method also differs from the classical numerical simulation, for it represents only the relevant modifications of evolutions; the notion of the calculus step has disappeared.

2.4 - Explanations

At present, all the nodes of the graph are seen as sums of contributions. A contribution is the response to the evolution of the initial node of an arc, calculated by the arc's QTF. For example, the evolution of the level NIRE is obtained by adding the contributions of the disturbances on the control loop - the aqueous inlet flow rate Q0500 and the column weight BE030 -, and the contribution of the set variable CNIRE (see figure 4). All the contributions are retained in memory. The explanations associated with an evolution are contributions, as shown in figure 4.

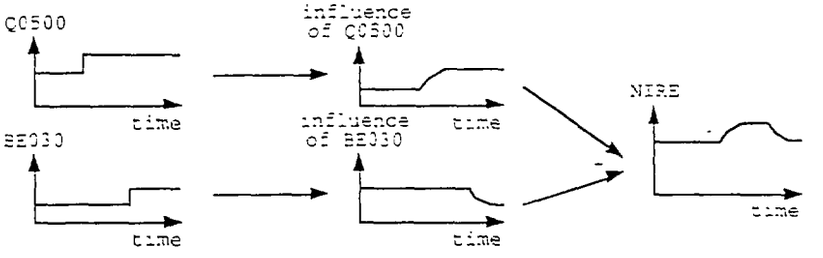

Figure 4 : Evolution of NIRE explained by the contributions of variables upstream Q0500 and BE030

3 - Defect diagnosis

Defect diagnosis involves both defect detection and isolation.

3.1 - Defect detection

The detection of abnormal modes involves a local operation with each variable, in which the difference between modeled data and process measurements over a given temporal window (the

simulation error) is individually analyzed. We say we have detected a defect when we've found a process malfunction, without searching more precisely for the actual cause of the discrepancy between the process and the model.

Starting a diagnosis with a simple comparison of simulation error and a threshold makes a system generally efficient at detecting defects, but too sensitive to various disturbances and imprecisions (that is, it leads to bad detections). To avoid this problem, we introduced qualitative notions that are more consistent with the modelling principles. Simulations results correspond to an approximated representation of process behaviour adapted to the level of abstraction relevant to supervision ; consequently, shapes or tendencies of evolutions can be as significant as precise values. This implies the use of temporal windows, so we have introduced the notion of qualitative equality between two evolutions, which makes the defect detection module more robust.

This idea relies on the qualitative interpretation of several criteria. A signed error is the first criterion for measuring the mean difference between two evolutions over a temporal window (the duration of which is at least the minimum time that can be considered significant for an event ; it is fixed by an expert after an elementary analysis of the signal). Subsequently, two evolutions have the same form if it is possible to significantly reduce the quadratic difference between the two evolutions (the second criterion). After a time and amplitude translation in the plane, the norm of the translation vector associated with this optimal readjustment constitutes the third criterion, meaning the cost of the operation.

Proceeding via the theory of fuzzy sets [15], we have designed the model to handle vague and imprecise readings. Each criterion needs a symbolic interpretation that leads to a decision. For example, the first criterion, the signed error, can be expressed as STRONGLY POSITIVE, STRONGLY NEGATIVE or ZERO. The sense of a symbolic value is characterized by its function of compatibility or its degree of relevance ($\mu : R \rightarrow [0, 1]$), which associates the compatibility of each numerical value of a criterion with a designated symbolic value. A function of compatibility is associated with each criterion.

Finally, the laws of composition between these functions allow a continuous decision to be taken for all combinations of the three criteria. In fact, the decision about whether or not there is a defect depends on three criteria that could correspond to the point of view of three different experts. The aim is to "combine" these three minds in order to make the right choice and provide a robust decision. Thus for real breakdowns, the model/process difference is normally too great for a translation in the authorized field to be able to sufficiently reduce the quadratic deviation with a low cost of readjustment. With degradations or drift failures, we generally manage to reduce the quadratic differences significantly but the cost of the operation increases with time. Other sources of errors and noise do not result in high costs or can be readjusted so that quadratic differences are virtually negligible. This approach tends to make the comparison module more robust, rather than favouring its detection precocity.

3.2 - Defect diagnosis

The second phase of the defect detection is a global analysis of all the simulation errors of the graph [16]. A defect proposed by detection is not necessarily a primary defect : it might not correspond to the genuine source of the malfunction, especially if the thresholds of the variables related by cause-and-effect relationships are poorly balanced.

Use of the causal graph

When a malfunction or a non measurable disturbance occurs, it entails a defect of the corresponding variable. Meanwhile, inappropriate thresholds or imprecise measurements might prevent immediate detection of this variable. Nevertheless, it can detect the consequences of the primary defect on one of its successors in the graph. This often happens in the case of gradual failures, when the model can still be considered valid although a slight drift has been detected.

Our purpose is to find the root variable (the one that is directly affected by the fault and whose evolution can explain all the observed defects) starting from the detection variable (the one in which the discrepancy between the real and the expected behaviours exceeds the authorized limits). This produces the sub-graph of defects propagation, which is called the suspected sub-graph.

Causal analysis of the defects

Causal analysis rests on local simulations using a causal graph. The aim is to give the reason for the detection variable's error : there might be a fault on it or on one or more of its predecessors, or one or more of its entering arcs are no more valid. The defect on each antecedent is not significant enough to be detected in the sense of our criteria, but can be responsible for the detection variable's defect owing to nonlinked thresholds.

The system begins a local simulation, where the real evolution of each antecedent is substituted for its simulated evolution over a selected temporal window. The evolution of the detection variable is calculated again, as if its predecessors were roots of the graph. It gives a new model/process error, which is compared with the initially noticed discrepancy. The substitution is said to be successful when the new error is considered to be significantly reduced. The contribution of each predecessor to this improvement has to be qualitatively interpreted, based on order-of-magnitude reasoning [17].

Once the above substitution has removed the simulation error from the detection variable, the defects between upstream and downstream variables are said to be linked. Using the selected predecessors as detection variables, continuing the testing enables us to construct the suspected subgraph until the simulation error is no longer causally linked with any predecessor's errors. A root variable has thus been found ; its input arcs are also suspected. The explanation may be either that an input arc of the root variable is physically damaged, or there is a real fault on the root variable (due to a component failure or a non measurable disturbance). In fact, the error on the root variable was not significant enough to have started the causality analysis, but was relevant enough to explain all the discrepancies on the successors.

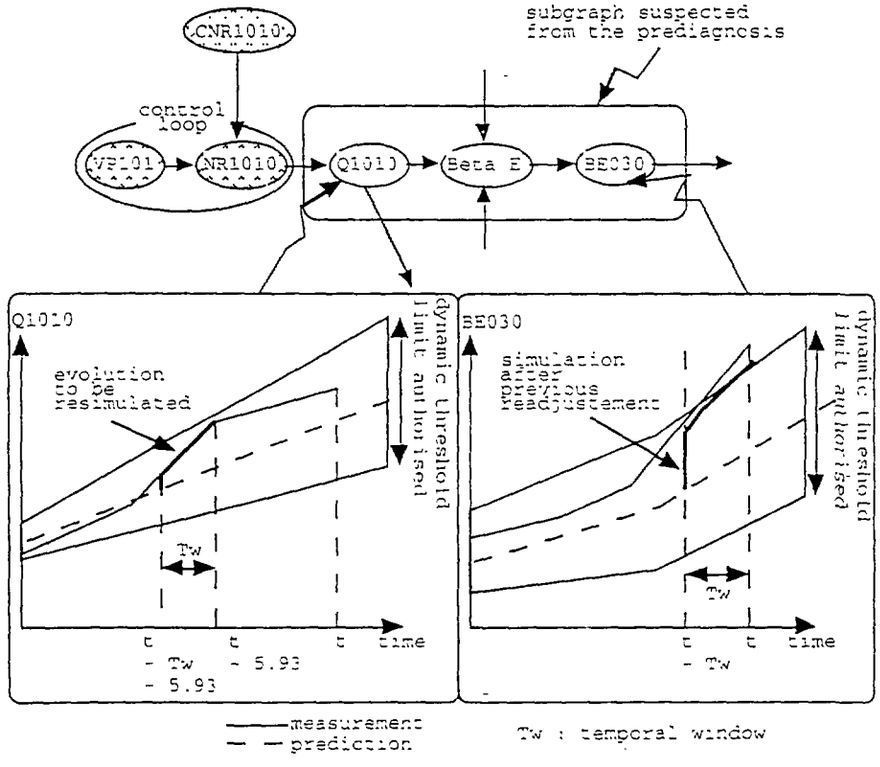

Figure 5 : Sub-graph of error propagation

Finally, the causality analysis allows us to the focus on a suspected sub-graph, whose roots are consistent candidates for the origin of the malfunctions. Figure 5 shows a suspected subgraph after DIAPASON found a significant discrepancy in the detection variable BE030. This

discrepancy is seen to be linked to the discrepancy in BETAE itself linked to the discrepancy in Q1010 ; since the test failed upstream, Q1010 must be the root variable we're looking for.

The consistency test is also useful in sorting alarm signals. Before signaling a new defect, causal analysis tries to relate it to the suspected subgraph already proposed. This is a solution to alarm cascades, in that it proposes causal chains linking all the various defects present in the graph's variables.

4. Fault diagnosis

A fault is a malfunction of a physical component, indicated by the presence of a defect. The defect diagnosis carried out thanks to the behavioural model is not sufficient to identify the malfunctioning physical components which caused the faults. This requires knowledge about structures and functions that is not present in the causal model ; heuristic reasoning is more suitable for this purpose. The fault diagnosis module uses knowledge of the process structure to identify faulty components.

On the other hand, a knowledge-based system is poorly adapted to time management : the addition of temporal logic, using Allen's predicates for example, complicates the writing of rules and particularly the validation of the base, which is a crucial phase in the case of sensitive plants. We have thus chosen to have the diagnose faults using an expert system, but to report temporal aspects using the defect diagnosis module. Temporal aspects do not raise special problems for the dynamic simulator, which rests on classical notions of control theory.

The defect diagnosis module thus activates the expert system only after observing a defect. The expert system receives an image of the process consisting of the real and predicted values of the root variables at the time of the defect, as well as the values of other variables at previous consistent dates (taking into account delays in the causal relationships). This approach reduces the diagnostic system's tasks and thus improves its performances.

4.1 - Why hypothetical reasoning ?

An experimental study of plant operators' reasoning during an incident identified three types of behaviour, each one including a phase relying on hypothesis.

Hypothetical reasoning is interesting for two reasons. First, from the operator's point of view, this is the natural way to solve problems. Also, in abductive diagnosis, the possible hypothesis are the possible causes (faults) that, with the background knowledge, imply the observations [18] [19]. The hypothetical-reasoning approach links up with that of reasoning by abduction, for which we have proposed an implementation [20].

4.2 - A solution : stratified reasoning

The solution to hypothetical reasoning, called stratified hypothetical reasoning, depends on two mechanisms :

- From a given hypothesis, we deduce logically isolated consequences (facts and predicates) in a reasoning stratum. Succeeding hypotheses are represented in successive overlapping strata, each stratum coherent up to that point. The appearance of a logical contradiction in the last opened stratum results in the destruction of this stratum (all conclusions isolated in this stratum are forgotten) and, according to the principle of reasoning ad absurdum, the negation of the hypothesis in the incoherent stratum is propagated into the surrounding stratum ;

- Concurrent hypotheses (simultaneous possibilities) are handled using classical notions of choice points and backtracking.

Various solutions have been proposed for managing work spaces that might contain contradictions. Rather than integrating hypothesis handling into its inference mechanism, one approach establishes a parallel network of all possible worlds. In some expert systems, the notion of hypothesis is artificially approached by the notion of points of view, which implies a specific handling of contexts or contradictions. Contrary to these approaches, our solution depends on axiomatic theory. The opening of a reasoning stratum can be linked up with the

definition of a specific theory whose supplementary axioms are the hypothesis : at each step, all the nested specific theories form the current work space. Closing a stratum corresponds to the proof that the set of axioms is incomplete. The problem of completeness of the set of axioms (corresponding to the rule base) comes down to the static validation of the knowledge base.

4.3 - The rules

A rule is an elementary diagnosis (associated with one component of the installation) similar to the schemes of the Knowledge-Oriented Design method. Rules permit the rapid understanding of context, and correspond to an expert's stereotyped mode of reasoning. The interpretation scheme is a collection of inferences ; recognizing a typical situation, it provides an interpretation of the phenomena observed in the objects.

A diagnostic strategy is formulated, for example, as follows :

```
If Defect ASSUME
        Failure WITH Effects THEN Consequences ELSE
        Other Failure WITH ... ELSE
        ...
        OTHERWISE The sensor showing the defect is malfunctioning.
```

The main part of the rule consists of a suite of exclusive hypotheses examined sequentially in the event of rebuttal (there is a mechanism to dynamically organize the list of hypotheses). Refuting all the hypotheses results in the conclusion at the end of the rule.

5 - Conclusion

The three modules of DIAPASON - prediction, defects diagnosis and faults diagnosis - have been developed on a SUN workstation in Ada language, except for the rules compiler written in StarLET, a predicative language based on affix grammars. All three modules are integrated in a demonstration package connected on line with a simulator of an extraction/washing process for nuclear fuels.

References

[1] P.Frank, Evaluation of Analytical Redundancy for Fault Diagnosis in Dynamic Systems, *Symposium on Advanced Information Processing in Automatic Control*, Nancy,1989.

[2] R.Isermann, Process Fault Diagnosis on Process Model Knowledge, *Symposium on Advanced Information Processing in Automatic Control*, Nancy, 1989.

[3] B.Dubuisson, *Diagnostic et reconnaissance des formes*, Traité des nouvelles technologies, Diagnostic et Maintenance, Editions Hermès, 1990.

[4] A.Charles, *Aide à la détection d'anomalies de fonctionnement des systèmes dynamiques: une approche fondée sur des modèles quantitatifs et qualitatifs*, PhD Thesis, Université de technologie de Compiègne, 1992.

[5] J.Shiosaki, H.Matsuyama, K.Tano and E.OfShima, Fault Diagnosis of Chemical Processes by the use of signed directed Graphs: Extension to Five-Range Patterns of Abnormality, *International Chemical Engineering*, vol. 25 N°. 4, pp. 651-659,1985.

[6] S.Gentil, S.Feray-Beaumont and P.Caloud, Qualitative Modeling for Process Supervision Systems, *Meeting on Cognitive Science Approaches to Process Control*, Marcoussis, 1987.

[7] L.Leyval, *Raisonnement causal pour la simulation de procédés industriels continus*, PhD Thesis, Institut National Polytechnique de Grenoble, 1991.

[8] D.Dubois and H.Prade, L'Interface entre représentations numériques et symboliques des connaissances, *Automatique et intelligence artificielle, CNRS, ed. S.Gentil and D.Dubois*, 1991.

[9] D.Dubois and H.Prade, Ensembles flous et mesures de possibilité: aspects théoriques et pratiques, *AICE I/Interfaces*, N°. 80, pp. 10-19,1989.

[10] D.Dubois, *Modèles mathématiques de l'imprécis et de l'incertain en vue d'applications aux techniques d'aide à la décision*, PhD Thesis, Institut National Polytechnique de Grenoble, 1983.

[11] J.L.Koning, Un mécanisme de gestion de règles de décision antagonistes pour les systèmes à base de connaissances, *PhD thesis*, Université Paul Sabatier, Toulouse, 1990.

[12] J.Montmain, *Interprétation qualitative de simulations pour le diagnostic en ligne de procédés continus*, PhD thesis, Institut National Polytechnique de Grenoble, 1992.

[13] L. Leyval, S. Gentil, Event Based Simulation through a Causal Graph, *IMACS Workshop on Qualitative Reasoning and Decision Support Systems*, Toulouse, 1991.

[14] B. Kuipers, The Limits of Qualitative Simulation, *IJCAI*, Los Altos, pp. 128-136, 1985.

[15] L. A. Zadeh, The Concept of a Linguistic Variable and its Application to Approximate Reasoning, *Information Sciences*, n° 8, pp. 199-249, 1975

[16] J. Montmain, S. Gentil, Qualitative Event Analysis for Fault Diagnosis, *IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes*, Baden Baden, September, 1991

[17] M. Mavrovouniotis, G. Stephanopoulos, Formal Order-of-Magnitude Reasoning in Process Engineering, *Computer and Chemical Engineering*, vol. 12, n° 9/10, pp. 867-880, 1988

[18] J. Reggia, D. Nau, P. Wang, Diagnostic Expert Systems Based on a Set Covering Model, *International Journal on Man-Machine Studies*, n° 19, pp. 437-460, 1983

[19] D. POOLE, Normality and Faults in Logic-Based Diagnosis, *IJCAI*, pp. 1304-1310, Detroit, 1989

[20] L. Coudouneau, J.M. Penalva, Fault Diagnosis in DIAPASON, a Continuous Process Control Aid System, *IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes*,Baden Baden, September, 1991

[21] J. Doyle, A Truth Maintenance System, *Artificial Intelligence*, N°. 12, pp. 231-272, 1979

Acknowledgments : We created the predictive and defect diagnosis modules of Diapason in collaboration with Pr. S.GENTIL from the Process Control Laboratory, Grenoble. The fault diagnosis module has greatly benefited from the experience of Pr. L.FRECON from the Institut National des Sciences Appliquées de Lyon.