CONSISTENCY-BASED DETECTION AND DIAGNOSIS FOR DISCRETE EVENTS SYSTEMS: TOWARDS THE TAKING INTO ACCOUNT OF MODELLING ERRORS

Carmen Guadalupe Lopez Varela
Audine Subias and Michel Combacau

I. PROBLEMATIQUE

In the field of the Model Based Diagnosis (MBD), some approaches are based on a model of the systems including its behaviour in presence of failure events and making hypothesis of exhaustiveness of the failures. Other approaches are based on a normal behaviour model making hypothesis of a model which is correct and complete. In both cases, an error in the model inevitably results in the sudden detection of a symptom (loss of consistency model/reality) and could blame the correct operation of the systems whereas the real origin of the symptom is on the model level which is erroneous. These symptoms having their origin in the errors of the model (false symptoms) are confused with the symptoms caused by the components systems dysfunctions (true symptoms).

II. OBJECTIVE

Our objective is to develop a diagnosis method for Discrete Event Systems based on models describing the normal behaviour of the supervised system, by taking into account the possibility of error modelling on these models. In our consistency-based approach any behaviour observed different from the behaviour specified in the models is regarded like a symptom. To deal with the error problem in the models, we make the assumption that the received observations are free of errors. Taking into account this hypothesis, to the apparition of inconsistency with respect to the models, only are questioned the supervised systems operation and the system models used like reference of the correct behaviour. The detection stage corresponds to a rupture of consistency between the system models and the observations. We integrate in our approach the stage of configuration identification of the models like an intermediate stage between detection and the diagnosis, to the distinction between truths and false symptoms. The diagnosis stage corresponds to the modification of the system models to restore the consistency between the reality and the reference. Figure 1 shows a general representation of our approach.

III CONTEXT AND POSITIONING

Our work is within the framework of the detection and diagnosis of failures in the Discrete Event Systems (SED). For this kind of systems, the diagnosis is generally regarded as a set of path which explains the observations. MBD approaches, called "diagnosers" [4], [5], [6], [7], [8], [9], are based on a system model to determine the occurrence of the failures from the observations resulting from the systems operation. Most of the models used in these approaches, represent the normal and the faulty behaviour of the systems. This work makes the assumption of exhaustiveness of the failures affecting to the system. Given that the anticipation of all the possible failures of systems is a difficult task, this assumption becomes a limitation for these approaches: the failures which are neither impossible to anticipate nor represented in the model, can't be detected and can't be diagnosed. Other MBD approaches use a correct behaviour models and then they tackle the diagnosis problem like a consistency problem between the observations and the model [10], [11], [12], [13]. These approaches do not take into account the possibility of errors on the used models, susceptible to generate detection of sudden symptoms detections or to mask some failures.

IV STATE OF THE WORK

1. The detection function

The principle of this stage of our approach is to verify the consistency between the observations resulting from the system operation and the models which describe the normal system behavior. Thus, it compares the events sequence observed (reality), and the sequence generated by the normal behavior models. This comparison constitutes the detection stage.

1.1 Rupture of the consistency

An observation resulting from the process which does not correspond to the behavior into the model breaks the consistency between reality and the reference, this inconsistency is generally interpreted like process dysfunction. However, there are three possible causes which can explain the rupture of the consistency between reality and the models:

- **A change of characteristics of the process.** This is interpreted by an unusual response followed of a request by the control device. It is a functional failure in the classical sense of the term: the controlled process does not behave as it is indicated by its functional specification. The origin of a failure is generally search as component fault or a variation of the environment (for example, a suddenly human intervention on the process).
- **A false model.** This covers the modeling errors introduced into the normal behavior model in the design stage. Two kinds of errors are possible: the description of surplus behaviors, i.e. of behavior which in reality are not normal and the deficit of description which indicate the miss or lack of behaviors into the model which are normal and possible in the reality of the system.
- **False observations.** It is either a false lecture of sensors, or of errors in the information transmission between the sensors and the monitoring system. This lecture is interpreted by the monitoring like a signature of a process evolution which did not take place actually.

1.2 Models for the detection

To highlight a rupture of the consistency we are based on three models:

- **a observations model noted MOD_{OBS}**, built on line with the observations received from the process. This model represents the set of the all possible path of states in which the process can be after a sequence of observations,

- **a expected behavior model noted MOD_{CA}**, which represents the process behavior to be observed under normal operation condition i.e. the correct behavior,
- **the control model noted MOD_C**, it describes the way in which the process must be used to satisfy the set of requests imposed by the user of the system.
-

2.- The configuration identification of the system models

2.1 Discrepancy between the set of paths of the system models

In the detection stage, an observation can be coherent with one model only; this fact can be explained by the modeling errors in the MOD_{CA} or (exclusively) in MOD_C. The modeling errors can appear in two ways: it can be produced by a surplus or by a deficit of information. Anyway, both errors result in a set of states into the model which does not have a correspondence with the second model. In other words, the modeling errors generate discrepancies between state spaces (and thus of the behaviors) of two models considered. Figure 2 schematizes the three possible situations giving the discrepancies between MOD_{CA} and MOD_C.

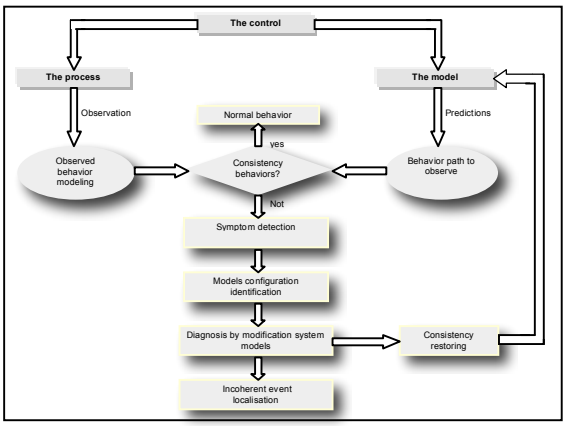

Fig. 1 General representation of the consistency- based approach of detection and diagnosis

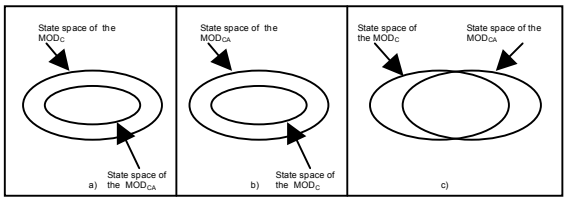

Fig. 2 Representations of the configurations between the paths of MOD_{CA} and MOD_C

- The case a) can be interpreted as an error on the control model MOD_C having the effect to claims to the process abnormal behaviors which do not have sense and then they are not included in MOD_{CA}. This situation can also be regarded as an error into the MOD_{CA} which is incomplete and does not represent certain process behaviors although they are normal behaviors.
- The case b) can be attributed to the certain normal behavior lacks of the process into the control model. The error can be also into the MOD_{CA} which represents impossible behaviors under normal operation.
- In the case c) both models can contain the two kinds of errors: surplus behaviors and actually abnormal, can be modeled into $MOD_{CA,}$ but MOD_C can be also incomplete.

2.2 The principle of models configuration identification

Before considering the diagnosis stage, which follows the detection of an inconsistency, it is necessary to distinguish inconsistencies caused by modeling errors; they give place to false symptoms, and inconsistencies caused by process malfunctions which appear by truth failure symptoms. Two problems arise to carry out this distinction:

- First problem: it is necessary to have the means to discriminate between truth and false symptoms,
- Second problem: it should be considered that all the system models configurations (MOD_{CA} and MOD_C) are possible.

To solve the first problem, a third model of the system is used. This model is called real behavior model and is noted MOD_{CR}. MOD_{CR} represents all the real and normal behaviors of the system in a complete and correct way. By using this third model, it is possible to distinguish the false symptoms from truth symptoms. With MOD_{CR} any incoherent observation caused by an error into MOD_{CA} and/or MOD_C will be coherent with MOD_{CR} and, any incoherent observation with MOD_{CA} and/or MOD_C caused by a process dysfunction will be also incoherent with MOD_{CR}. However, the taking into account of the second problem mentioned complicates the distinction of the symptoms. The third model MOD_{CR} must be integrated in all the possible configurations between MOD_C and MOD_{CA}.

The identification stage which is an important stage of our approach is based on the graph exploitation build from the resulting information of the observations. In the graph having seven-depth levels, at most seven observations producing different information is necessary to identify the models configuration corresponding with the observation. When the set of configuration is identified, the distinction between the false and the truth symptoms is realized. Naturally, as long as the seven information are not collected, an uncertainty on the models configuration will be present and the conclusion will be uncertain too.

3. The diagnosis function

The diagnosis stage in our approach is dedicated to restoring the consistency between reality and reference. Given the hypothesis of correct observations and the possibility of errors into the models, it is necessary to restore consistency between reality and reference, to modify the reference, i.e. the system models MOD_{CA} and MOD_C. The purpose of these modifications is that these models can represent again the observed behavior such as it is in the observation model MOD_{OBS}. Thus, the diagnosis stage will be a diagnosis stage by the system models modification; these models are implemented by Petri nets. This diagnosis stage supposes to find a set of modified incidence matrices,

called matrices of Restore of consistency (noted C_{RC}), allowing to eliminate inconsistencies and to cover the new observed behavior which is not represented into the initial models. These modifications must respect the following constraints:

- The new found matrices must respect the representation of the last behaviours which were found like coherent.
- The modifications carried out must guarantee some properties of Petri net of the system model. These properties are obtained from knowledge (minimal) of the supervised system. For example the properties captured into the place invariants as well as the properties represented into the initial model like boundedness, reversibility and liveness.

Different kinds of models modifications are possible to restore consistency:

- ***Modification of the weights of arcs***. The objective is to modify the effects of the transitions fire on the marking, i.e the coefficients of the incidence matrix C, without modifying the matrix dimension (number of rows and columns), that to say, without changing the sets of places P and transitions T from the model. More specifically this modification is carried out in the incidence matrix PRE because in the model an inconsistency is represented by a transition associated to the observed event which cannot be fired because it is not enabled. The fire of this transition requires to modify the weight of the arcs connecting the transition to its input places and to connect it to the marked places into the current marking of the net.
- ***Modification of the sets of places P and transitions T.*** It is necessary to modify the number of rows and columns of the incidence matrix by increasing them or by decreasing them, without changing the matrix coefficients of the net elements which are not modified. In fact, in this kind of modification, the new places and new transitions are integrated to the net such that the realized modification allows representing the observed behavior.
- ***Modification of the marking.*** Here, the modification is into the marking of the Petri net such that the new marking enable the associated transition to the observed event.

It is possible that the modifications made into the incidence matrices induce new properties in the models, properties that are not present in the initial model of the systems. Moreover, the new behaviors obtained after models modifications, will include the initial behaviors associated with consistent observations, but also will include a new subset of behaviors associated with judged inconsistent observations integrated into the model. Thus, this incidence matrix modification leads to obtaining an enhanced behavior model of the system, including the normal behavior. Our diagnosis method develops in particular the restoring consistency by coefficients modification of the incidence matrix PRE.

PUBLICATIONS

[1] C. G. Lopez-Varela, A. Subias and M. Combacau "An adapted FMEA-based approach for failure diagnosis in distributed architectures*," IMACS World Congress Scientific Computation, Applied Mathematics and Simulation IMACS,* july 2005.

[2] C. G. Lopez-Varela, A. Subias and M. Combacau, " Diagnostic Distribué à base de modèles" EDSYS, May 2006.

[3] C. G. Lopez-Varela, A. Subias and M. Combacau, " Approche de détection basée cohérence : modèles pour le diagnostic" 3ème Colloque International Francophone Performance et Nouvelles Technologies en Maintenance, PENTOM, july 2007

REFERENCES

[4] Sampath, M, Sengupta R, S. Lafortune, K. Sinnamohideen and D.C. Tenketzis "Diagnosticability of discrete-event systems*," IEEE Transactions on Automatic Control* 40(9), pp. 1555-1575, 1995.

[5] Debouk R., S. Lafortune and D. Teneketzis " Coordinates decentralized protocols for failure diagnosis of discrete event systems " Theory and Application 10, 33-86, 2000.

[6] Genc S., and S. Lafortune "Distributed diagnosis of discrete event systems using Petri nets" *in Application and Theory of Petri Nets, (series Lecture Notes in Computer Science),* Vol. 2679, pp316-336, Springer Verlag, 2003.

[7] Baroni, P, Lamperti, G, Pogliano and Zanella M, "Diagnosis of a class of distributed discrete event systems" *IEEE transaction on systems, Man, and Cybernetics – Part A: Systems and Humans* 30(6), 2000.

[8] Su, R., W.M. Wonham, J. Kurien and S. Koutsoukos, "Distributed diagnosis for qualitative systems" *In Proceeding of the International Workshop on discrete event systems- WODES, IEEE Computer Society,* pp 169-174, 2002.

[9] Pencolé Y, "Decentralized diagnoser approach: application to telecommunications networks", *In Eleventh International Workshop on Principles of Diagnosis- DX,* pp. 185-192, 2000.

[10] Holloway L. and Krogh B., «Fault Detection and diagnosis in Manufacturing Systems: A Behavioral Model Approach», *IEEE Second International Conference on Computer Integrated Manufacturing*, New York, USA, 21 - 23 May 1990, p. 252 - 259.

[11] Ashley J., Holloway L., «Diagnosis of Conditions Systems using Diagnostic Causal Network», *IEEE International Conference on Systems, Man and Cybernetics*, Tucson, USA, 7 - 10 october 2001, vol. 5, p. 2799 - 2804.

[12] Soldani S., Combacau M., Thomas J. and Subias A., «Intermittent fault detection trough message exchanges: a coherence based approach», *17th International Workshop on Principles of diagnosis DX - 06*, Burgos, Spain, 26-28 june 2006, p. 251-256.

[13] Tabakow I., «Using Place Invariants and Test point to Isolate Faults in Discrete Event Systems», *Journal of Universal Computer Science,* Springer 2007, vol. 13, n° 2, p. 224 -243.