Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online
CONFERENCE PAPER ARCHIVE

IFAC-PapersOnLine 48-21 (2015) 308–313

Diagnosability evaluation by model-checking

Marangé, P.*, Philippot, A.**
Pétin, J.F.* and Gellot, F.**

** CRAN, CNRS UMR 7039, University of Lorraine*
France (Tel: (33) 38-368-4420; e-mail: pascale.marange@univ-lorraine.fr).
***CReSTIC, University of Reims Champagne-Ardenne, France (e-mail:*
alexandre.philippot@univ-reims.fr)

Abstract: In order to improve the availability and reliability of manufacturing systems, the diagnosis method is primordial. The literature around the diagnosis of Discrete Event Systems (DES) have proposed different approaches and diagnosability assessment. This paper presents a local modelling of diagnoser and a diagnosability evaluation by Model-Checking. This approach avoids the combinatory explosion problem of global approaches.

Keywords: Diagnosis, Discrete-event Systems, Modelling, Verification.

1. INTRODUCTION

In recent years, researches around diagnosis have expanded in the academic and industrial world due to the increasing complexity of the systems, but also the costs of maintenance policy. To improve the availability and reliability of installations, it is necessary to develop systematic approaches to diagnosis to detect and isolate defaults. Moreover, it has become important to develop approaches for assessing the performance of these diagnosis methods in terms of detection, localization and identification of a fault in a finite delay. Among the diagnosis approaches, literature has shown particular interest around the model-based approaches to the DES diagnosis and the notion of diagnosability.

The aim of this paper is to provide an assessment of diagnosability by model-checking. This approach consists in analyze dependence of local models in order to establish a distribution of the diagnosis. A model checker is then used to verify a number of properties on the failed states reachability. These properties allow us to assess the diagnosability of proposed models. This evaluation is firstly made locally. In case where the system is not locally diagnosable, local diagnoser evolves in a modular diagnoser. An assessment of modular diagnosability is then done. Finally, global diagnosability is checked. In addition, we see that the verification by model checking can assess K-diagnosability and give counterexample to complete the diagnoser. A state of the art on the DES diagnosis approaches and diagnosability notion are listed in section 2. In section 3, the proposed approach to formalize local diagnosers is presented and a diagnosability verification approach by model-checking is exposed. Section 4 illustrates on an academic example, the various concepts discussed in this paper. Before leaving our conclusions and research perspectives, section 5 provides a discussion around the contribution.

2. STATE OF THE ART

The diagnosis field is an important aspect in systems engineering. This importance is not only due to operational safety but also the need to achieve the objectives of maintenance. The objective of this section is to present a state of the art of Discrete Event Systems diagnosis approaches.

2.1 Literature approaches

DES diagnosis approaches can be classified according to the "without model" and "model-based" methods. The methods without model involve the availability of data from recordings made throughout the operation. They often come from expert systems (Tzafestas and Watanabe, 1990), (Alonso-Gonzalez et al., 2010). Therefore, the acquisition of knowledge from experts can be difficult and time consuming before have sufficient knowledge to obtain a reliable diagnosis is uncertain. The model-based methods compare the expected behavior represented by a model of the system, called diagnoser (Sampath, 1995) (Reiter, 1987) (Roth et al., 2009), (Cabasino et al . 2013). The modelling task is often tedious, and quality of the model influence the quality of results returned by the diagnoser. These approaches can also be distinguished by the way the system is modeled (in normal and/or abnormal operation) as well as the modelling tool used (Petri Net, Bayesian Net, automata …). In the context of this paper, the works presented are based on the use of a model-based approach by finite state automata.

Approaches with representation of the faults in the model are a large part of the literature work. The observer model, often called diagnoser, must inform user of system status in the form of labels (Debouk et al., 2000) (Genc and Lafortune, 2003). Originally proposed in (Sampath, 1995), these approaches have two main steps: Make a model of normal and anormal behavior of the system, after build a labeled diagnoser providing information on the behavior of the system.

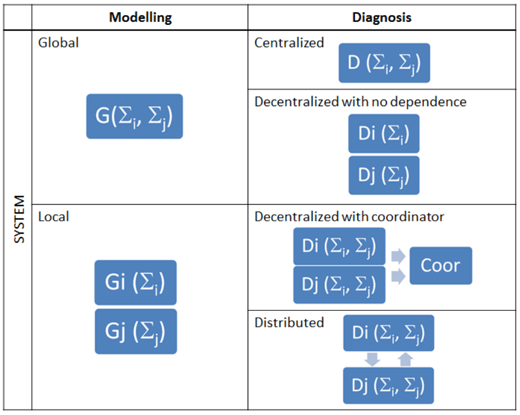
These approaches are only discrete in the sense that no other information than that given by the sensors and actuators is present. However, it is sometimes necessary to enrich the

10.1016/j.ifacol.2015.09.545

knowledge of the system through temporal or delayed information. The model-based approaches using templates or chronic have been then developed (Holloway and Chand, 1994) (Pandalai and Holloway, 2000) (Milne et al., 1994).

The main trouble of model-based approaches remains in the size of the models to use and to implement. Table 1 shows the classically possible architectures. A global model of the system G can be decompose by local models G_i ($i \in 1,.. n$) in the case of complex systems. Definition of a global diagnoser D containing all the observations of the system (centralized approaches) can be made. But it is possible to obtain the decentralization of information across several local diagnosers D_i ($i \in 1,.. n$). However, when several local diagnosers are present, they should not be contradictory. If their observation Σ_i is exclusively local to the diagnoser D_i, the final decision is then a simple concatenation of local decisions. However, if the local diagnoser requires external information $D_i(\Sigma_i, \Sigma_j)$, we need to ensure the consistency of this information and remove ambiguities making. Therefore, you must use either a decisions coordinator noted Coor (in the form of high-level rules, for example), or communicate the status of this information between local diagnosers (distributed approaches).

Table 1: Diagnosis Architectures



	Modelling	Diagnosis
SYSTEM	Global $G(\Sigma_i, \Sigma_j)$	Centralized $D(\Sigma_i, \Sigma_j)$
		Decentralized with no dependence $Di(\Sigma_i)$ $Dj(\Sigma_j)$
	Local $Gi(\Sigma_i)$ $Gj(\Sigma_j)$	Decentralized with coordinator $Di(\Sigma_i, \Sigma_j)$ $Dj(\Sigma_i, \Sigma_j)$ Coor
		Distributed $Di(\Sigma_i, \Sigma_j)$ $Dj(\Sigma_i, \Sigma_j)$

For centralized structure (Sampath, 1995), the disadvantage is the combinatory explosion limiting the application in the case of complex systems. Decentralized and distributed structures can solve this problem (Su and Wonham, 2000) (Qiu, 2005) (Pencolé et al., 2001), but raise other issues in the audit capacity to diagnose all faults.

2.2 Concepts of diagnosability

The use of approaches to diagnosis is essential for complex systems. However, it is important to define whether a system can diagnose with certainty a number of faults in a finite delay. In other words, diagnosability assesses all identified faults are identifiable and locatable in a finite number of events. This is called diagnosability. Indeed, before applying a method on a system, we need to check whether it has sufficient information to perform the diagnosis.

In the Meera Sampath's thesis, a DES is said diagnosable for a set of partitions and for a set of observable events, if it is possible to detect the occurrence of any fault of a partition in a finite delay :

$$(\forall i \in \Pi_f)(\exists n_i \in \aleph)[\forall s \in \Psi(\Sigma_{fi})](\forall t \in L/s):$$
$$[||t|| \geq n_i \Rightarrow w \in P_L^{-1}[P(st)] \Rightarrow \Sigma_{fi} \in w]$$

where $L/s = \{t \in \Sigma^* \mid st \in \mathrm{L}\}$ is the set of all sequences of events after s. $\Psi(\Sigma_{fi})$ is the set of all sequences of events that ends with an event of default in Π_f. $\mathrm{P_L}^{-1}[\mathrm{P}(st)]$ is the set of all sequences of events that have a projection, an observable sequence of events, equivalent to st in a finite delay ni.

From the work on the decentralized diagnosis (Debouk et al. 2000), authors present a local diagnosis where the objective is to diagnose each component separately and obtain an equivalent diagnosability of the centralized case. This is called local diagnosability where observability is local. However, if two components are each diagnosable locally, the system may not be globally diagnosable with respect to the overall observability of the system.

Regarding distributed structures, joint diagnosability is found in (Qiu, 2005). This is an extension of the co-diagnosability since it is based on the local information of each diagnoser but also the information of neighboring diagnosers. Sometimes called modular diagnosis in literature.

Other definitions exist for diagnosability. In this paper, we summarize the following cases:

1. Local Diagnosability: Failure F_i is said locally diagnosable in a ***subsystem*** $\boldsymbol{G_i}$ iff there exists a finite sequence of observable events ***subsystem*** $\boldsymbol{G_i}$ after the F_i occurrence, F_i is occurred with certainty.
2. Modular Diagnosability: Failure F_i is said modularly diagnosable in a ***subsystem*** $\boldsymbol{G_i}$ and only one iff there exists a finite sequence of observable events of the ***system*** $\boldsymbol{G}$ after the F_i occurrence, F_i is occurred with certainty.
3. Global Diagnosability: Failure F_i is generally said diagnosable in a ***system*** $\boldsymbol{G}$ iff there exists a finite sequence of observable events of the ***system*** $\boldsymbol{G}$ after the F_i occurrence, F_i as occurred with certainty.

2.3 Evaluation of diagnosability

Before checking diagnosability of a system, (Sampath, 1995) has identified two conditions:

1. There is at least one state of the diagnoser which the diagnoser decides with certainty the occurrence of a fault belonging to partition Π_{Fi}.
2. There must not be any cycles called "indeterminate" for which the diagnoser is unable to determine with certainty the occurrence of a fault.

In (Jiang et al., 2001), an algorithm for testing the diagnosability a system has been defined. This is to build for a system G, an automaton G_d by synchronous composition of a diagnoser G_o with himself called twin plant. The algorithm then checks that for every cycle of G_d there diagnoser in a cycle which all states are uniquely labeled. Other methods, for the construction of a non-deterministic automaton G_d in (Yoo and Lafortune, 2002) or empty test in a Büchi automaton in (Tripakis 2008), have been proposed but for centralized approaches.