Diagnosability analysis of hybrid systems cast in a discrete-event framework

Mehdi Bayoudh, Louise Travé-Massuyès

▶ **To cite this version:**

Mehdi Bayoudh, Louise Travé-Massuyès. Diagnosability analysis of hybrid systems cast in a discrete-event framework. Discrete Event Dynamic Systems, 2014, 24 (3), pp.309-338. 10.1007/s10626-012-0153-z . hal-01400372

HAL Id: hal-01400372
https://hal.science/hal-01400372

Submitted on 5 Feb 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Noname manuscript No.
(will be inserted by the editor)

Diagnosability analysis of hybrid systems cast in a discrete-event framework

Mehdi Bayoudh · Louise Travé-Massuyès

Received: date / Accepted: date

Abstract This paper addresses the problem of assessing the diagnosability of hybrid systems modeled by a hybrid automaton coupling methods from the continuous and the discrete event model-based diagnosis fields. The discrete states of the hybrid automaton represent the modes of operation of the system for which the continuous dynamics are specified. The diagnosability of the continuously-valued part of the model is first analyzed and the new concept of mode signature is shown to characterize mode diagnosability from continuous measurements. Continuous dynamics are then abstracted by defining a set of signature-events associated to mode signature changes, preserving this way mode diagnosability. The behavior of the abstract hybrid system is then modeled by a prefix-closed language over the original event alphabet enriched by these additional events. Based on this language, diagnosability analysis of the hybrid system is cast into a discrete-event framework and hybrid diagnosability conditions are provided. A case study based on the Attitude and Orbit Control System of a spacecraft illustrates the method [1].

Keywords Diagnosability · Hybrid systems · Mode signature · Event-based abstraction

1 Introduction

Diagnosability is the property of a system and its instrumentation guaranteeing that all anticipated faulty situations can be detected and identified without ambiguity on a bounded time window from the available measurements, which provide observations of the system [2]. In other terms, a system is diagnosable if every faulty situation leads to characteristic observable manifestations. Diagnosability assessment is key to evaluate the performances that one can expect from a diagnoser at run time and to define the appropriate set of sensors to be included in the design of a system (Frisk et al (2009); Sarrate et al (2007); Travé-Massuyès

M. Bayoudh, L. Travé-Massuyès
CNRS, LAAS, 7 avenue du colonel Roche, F-31400 Toulouse, France
Univ de Toulouse, LAAS ; F-31400 Toulouse, France
E-mail: bayoudh@gmail.com, louise@laas.fr

[1] This work was supported by Thales Alenia Space France.

[2] In this paper, we indifferently use *observation* or *measurement*, and *observed* or *measured* variable, which are terms used in the DES and the continous systems control fields, respectively.

et al (2006)). It may also be useful in the context of active diagnosis to guide the decision about the relevant control actions to be applied to remove diagnosis ambiguity (Bayoudh et al (2009a); Chanthery and Pencolé (2009); Sampath et al (1998)).

Diagnosability analysis and diagnosis are closely coupled. A diagnoser and associated diagnosability analysis indeed share the knowledge representation formalism, which determines the level of abstraction at which phenomena are modeled (Travé-Massuyès et al (2006)). But whereas diagnosis deals with one given observation (which may be a trajectory in time), diagnosability must envision all the possible observations and related root causes and is a problem of increased complexity.

In the field of discrete-event systems (DES), the first diagnosability definition was proposed by Sampath et al (1995) together with the necessary and sufficient conditions for diagnosability based on the *diagnoser*, which is a finite state machine built from the system model. Sampath et al (1995) provided the basis of later diagnosability analysis approaches that aimed to reduce the algorithmic complexity (Jiang et al (2001a), Yoo and Lafortune (2002b), Pencolé (2004) and Contant et al (2006)). Variants of the diagnosability definitions were also proposed for stochastic DES (Thorsley and Teneketzis (2005); Liu and Qiu (2008)) and for fuzzy DES (Kilic (2008)). More recently, diagnosability was studied in the framework of decentralized and distributed architectures (Pencolé and Subias (2009); Ribot and Pencolé (2008); Yan et al (2010); Melliti and Dague (2010)).

In the field of continuous systems, diagnosability is formulated in terms of fault detectability and isolability as in (Chen and Patton (1994)) and (Basseville et al (2001)), which provides a survey of definitions from different points of view. In Pérez et al (2007), diagnosability analysis is performed using quasi-static models. Nyberg (2002) and Travé-Massuyès et al (2006) anchor the analysis in a structural framework.

Bridging over these works, Travé-Massuyès et al (2006) proved that the existing definitions of diagnosability, in particular for continuous systems and for DES, can be stated as a property of the system fault signatures, and a unified definition of diagnosability, independent of the model, was established.

For hybrid systems, only few works are concerned with diagnosabilty analysis although diagnosis has received a great deal of attention in the last ten years (de Freitas (2002); Narasimhan and Biswas (2002); Hofbaur and Williams (2004b); Verma et al (2004); Benazera and Travé-Massuyès (2009)). Among the existing contributions concerned with hybrid diagnosability, Biswas et al (2006) slightly modify the classical necessary and sufficient condition for diagnosability of a DES as obtained by Sampath et al (1995), and expresses it in terms of reachability. Fourlas et al (2002) generalize the necessary and sufficient condition for diagnosability for a DES, requiring more restrictive hypotheses. Despite the claim that they deal with hybrid systems, these two works do not really account for the hybrid nature of the system as they use only a very high level discrete abstraction and ignore the continuous dynamics. On the other hand, in (Cocquempot et al (2004)), diagnosability is expressed in terms of mode discernability and is only based on the continuous dynamics.

In this paper, a hybrid system is modeled by a hybrid automaton whose discrete states represent its modes of operation for which the continuous dynamics are specified. The discrete event part (automaton) constrains the possible transitions among modes and is referred to as the *underlying DES*. The restriction of the hybrid system to the continuously-valued part of the model is defined as the *multimode system*. Considering the multimode system, diagnosability is first analyzed as the problem of mode diagnosability based on the continuous dynamics like in (Cocquempot et al (2004)), i.e. limiting the observations to continuous measurements. This is done by extending the analytical redundancy approach and introducing the concept of *mode signature*, which refines the classical concept of fault signature.

Mode diagnosability depends on mode signatures. The key idea of the paper is to abstract the continuous dynamics by defining a set of "diagnosis-aware" events, called *signature-events*, associated to mode signature changes and to use them to enrich appropriately the underlying DES. The behavior of the abstract system is then modeled by a prefix-closed language over the alphabet enriched by these additional events. The finite state machine generating this language is called *the behavior automaton*. Based on the *abstract language*, the diagnosability analysis of the hybrid system is cast into a discrete-event framework and standard methods of this field can be used. Based on this framework, a definition of hybrid diagnosability is provided and we obtain diagnosability conditions.

Our approach can be compared to the approach proposed by Daigle et al (2010a,b) which also uses fault signatures to capture the continuous dynamics. However, in (Daigle et al (2010a,b)), fault signatures are based on fault transients, i.e. they directly express the expected dynamic behavior of measured variables after the fault, abstracted in qualitative terms. Our approach differs in that it uses fault/mode signatures that are specifically constructed for diagnosis, based on standard analytical redundancy residual methods of the FDI control field and its originality relies in that it proposes a way to integrate it with equally standard methods of the DES diagnosis field. In this aspect, it just falls into the so-called Bridge framework surveyed by Biswas et al (2004).

The paper builds on the work by Bayoudh et al (2008a) and provides a proper formalization of several concepts that were just introduced in this latter paper, in particular the behavior automaton and the transition function that abstracts the continuous dynamics and leads to the automatic construction of the behavior automaton. All the concepts are illustrated through a running academic example and a case study of a real aerospace system is presented. This example nicely illustrates the fact that diagnosability of the underlying DES or of the multimode system separately provide sufficient conditions only, and shows how the diagnosability of the hybrid system can indeed be achieved gathering continuous and discrete dynamics observations.

The paper is organized as follows. Section 2 provides the hybrid modeling framework that supports our approach. In section 3, diagnosability is defined and characterized restricting the observations to continuous measurements. The abstraction of the continuous dynamics in terms of signature-events is presented in section 4. The diagnoser construction is then provided in section 5. The hybrid system diagnosability definition and conditions are given is section 6 and discussed in section 7. The case study based on the Attitude and Orbit Control System of a spacecraft is presented is section 8. Finally, section 9 concludes the paper and discusses future work.

2 Hybrid System Modeling

This paper considers hybrid systems, represented by a hybrid automaton, whose continuous dynamics switch as the system transitions from one operating mode to another. An operating mode corresponds to a discrete state of the hybrid automaton and mode changes are modeled by discrete transitions labeled by appropriate discrete events that may be observable or not. Operating modes model both nominal and anticipated faulty behaviors. An *unknown mode* can be added to model all the non anticipated faulty situations like in (Hofbaur and Williams (2004a)).

Formally, a hybrid automaton (Henzinger (1996), Lunze and Lamnabhi (2009)) is defined as a tuple :

$$S = (\zeta, Q, \Sigma, T, C, (q_0, \zeta_0)) \tag{1}$$

where:

- ζ is the set of continuous variables including state variables, input/output variables, and possibly noise, which are functions of time t. Input/output variables form the set of observable, i.e. measured, variables denoted by ζ_{OBS} [3].
- Q is the set of discrete system states. Each state $q_i \in Q, i = 1, \ldots, m$, represents a mode of operation of the system.
- Σ is the set of events that correspond to discrete control inputs, autonomous mode changes and fault occurrences. $\Sigma = \Sigma_{uo} \cup \Sigma_o$, where $\Sigma_o \subseteq \Sigma$ is the set of observable events and $\Sigma_{uo} = \Sigma \setminus \Sigma_o$ is the set of unobservable events. Events corresponding to autonomous mode changes are issued upon guards that depend on continuous variables.
- $T \subseteq Q \times \Sigma \rightarrow Q$ is the partial transition function. The transition from mode q_i to mode q_j with associated event σ_{ij} is noted $t(q_i, \sigma_{ij}, q_j)$ and we have $T(q_i, \sigma_{ij}) = q_j$ [4]. A transition $t(q_i, \sigma_{ij}, q_j)$ may be guarded by a condition given as a set of equations $\mathcal{G}(t(q_i, \sigma_{ij}, q_j)) = g_{ij}(x, \theta_g) = 0$, θ_g being a constant parameter vector. Then σ_{ij} results from the state $x(t)$ hitting the guard g_{ij} at some time instant t^* and is not observable. A reset map $\mathcal{R}_{ij}$, possibly equal to the identity, is specified. $\mathbb{T}$ denotes the set of transitions.
- $C = \bigcup_i C_i$ is the set of system constraints linking continuous variables. C_i denotes the set of constraints associated to the mode q_i, which are given in the state-space by the following continuous time state-evolution and output equations:

$$\begin{cases} \dot{x}(t) = f_i(x(t), u(t), \epsilon(t)) \\ y(t) = g_i(x(t), u(t), \epsilon(t)) \end{cases} \tag{2}$$

  where $u \in \mathbb{R}^{n_u}$, $x \in \mathbb{R}^{n_x}$, $y \in \mathbb{R}^{n_y}$ are the input, output, state vectors, respectively, and $\epsilon \in \mathbb{R}^{n_\epsilon}$ denotes some noise vector. The variables gathered in these vectors belong to ζ.
- $(\zeta_0, q_0) \in \zeta \times Q$ is the initial condition of the hybrid system.

Transitions from one mode to another result in changing the continuous dynamics driving the behavior of the system. The continuous state may or may not undergo a jump at transition time, depending on the reset map of the transition, but this information is not used by the proposed diagnosability approach, which is based on analytical redundancy relations (cf. section 3).

The set of faults is noted F. The occurrence of a fault $F_i \in F$ is modeled by a discrete event $f_i \in \Sigma_F$, where Σ_F is the set of fault events associated to the faults of F. Without loss of generality it is assumed that $\Sigma_F \subseteq \Sigma_{uo}$, since an observable fault event obviously makes the corresponding fault diagnosable. Occurence of faults lead to *faulty modes*, i.e. modes in which one or more faults are present.

In this paper, we do assume that a model of the form (2) is available for some faulty modes but not for all, typically not for those corresponding to continuous range faults for which the magnitude is unknown. We say that these modes have no behavioral model. In these cases, however, the impact of the fault can be represented and is generally known with respect to modeled behavior. It is represented by introducing a fault vector $\xi(t)$ of appropriate dimension and unknown value in (2) as follows:

$$\begin{cases} \dot{x}(t) = f_i(x(t), u(t), \epsilon(t), \xi(t)) \\ y(t) = g_i(x(t), u(t), \epsilon(t), \xi(t)) \end{cases} \tag{3}$$

[3] We assume that the set of system observable continuous variables is the same in all system modes. This assumption is generally verified when the set of system's sensors is permanent.

[4] Without loss of generality, we assume that there is only one transition from a given mode q_i to a given mode q_j. If more than one event would drive the system from q_i to q_j, we use the or logical operator to define a combined event associated to a unique transition.

For analyzing the hybrid system from the discrete-event point of view on one hand, and from the continuous points of view on the other hand, let us define :

- $M = (Q, \Sigma, T, q_0)$ as the *underlying DES*, which captures the system's inter-mode behavior through the discrete dynamics and the events Σ_o;
- $\Xi = (\zeta, Q, C, \zeta_0)$ as the *multimode system*, which captures the system's intra-mode behavior through the continuous dynamics and the continuous variables.

Example 1 The following example illustrates the hybrid modeling formalism and is used as a running example throughout the paper. The underlying DES is provided in figure 1. N models the nominal mode of the system, $qF1$ ($qF2$) and $q'F1$ ($q'F2$) model two faulty

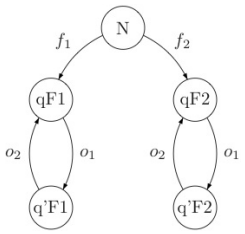

Fig. 1 The underlying discrete-event system

modes in which the fault $F1$ ($F2$) is present. o_1 and o_2 are observable events.
The continuous dynamics of each mode are given by the state-space model (4).

$$\begin{cases} \dot{x}(t) = \mathcal{A}_i x(t) + \mathcal{B}_i u(t) + \mathcal{E}_{x_i}\epsilon(t) \\ y(t) = \mathcal{C}_i x(t) + \mathcal{D}_i u(t) + \mathcal{E}_{y_i}\epsilon(t) \end{cases} \tag{4}$$

To keep the example simple, we assume linear continuous dynamics and a noise-free environment, i.e. $\epsilon(t) = 0$. The dynamic, input, output and direct-transmission matrices for the different modes $N, qF1, qF2, q'F1$ and $q'F2$ are indexed by $1, 2, 3, 4$ and 5, respectively, and are given below:

$$\mathcal{A}_1 = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}, \mathcal{A}_2 = \begin{bmatrix} -2 & 1 \\ 0 & -2 \end{bmatrix}, \mathcal{A}_3 = \begin{bmatrix} -\frac{8}{3} & \frac{4}{3} \\ -\frac{1}{3} & -\frac{4}{3} \end{bmatrix}, \mathcal{A}_4 = \begin{bmatrix} -3 & 1 \\ 0 & -3 \end{bmatrix}, \mathcal{A}_5 = \begin{bmatrix} -4 & 1 \\ 0 & -4 \end{bmatrix}$$

$$\mathcal{B}_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \mathcal{B}_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \mathcal{B}_3 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \mathcal{B}_4 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \mathcal{B}_5 = \begin{bmatrix} 2 \\ 2 \end{bmatrix}$$

$$\mathcal{C}_1 = \begin{bmatrix} 1 & 1 \end{bmatrix}, \mathcal{C}_2 = \begin{bmatrix} 0 & 1 \end{bmatrix}, \mathcal{C}_3 = \begin{bmatrix} -\frac{1}{3} & \frac{2}{3} \end{bmatrix}, \mathcal{C}_4 = \begin{bmatrix} 1 & 0 \end{bmatrix}, \mathcal{C}_5 = \begin{bmatrix} 2 & 2 \end{bmatrix}$$

$$\mathcal{D}_1 = \mathcal{D}_2 = \mathcal{D}_3 = \mathcal{D}_4 = \mathcal{D}_5 = 1$$

3 Diagnosability of the multimode system

In this section, diagnosability is analyzed based on the continuous measurements, with the new concept of *mode signature*, which refines the classical concept of fault signature. This

analysis is later used to establish the conditions for hybrid system diagnosability.
For this analysis, we consider the multimode system $\Xi = (\zeta, Q, C, \zeta_0)$ and the constraints $C_i \in C$ of each mode $q_i \in Q$ with model of the form (2), and for which ζ gathers the time-dependent continuous state, input, output and noise variables constituting the vectors x, u, y, and ϵ, respectively. The only available observations of the system are through the continuous measured variables ζ_{OBS}.

The principle of model-based diagnosis is to check the consistency between the system model and observations to derive the information relevant to fault detection and diagnosis. To do so, it is standard in the continuous systems community to calculate consistency indicators. For the multimode system, a set of consistency indicators is calculated for each mode q_i. Starting with C_i, we first compute a set of dynamic constraints in which the state variables have been eliminated. These constraints link only input and output variables u and y, their derivatives and the noise. This set is denoted C_{obs_i}. Through an appropriate statistical test accounting for the noise model, each constraint $C^k_{obs_i} \in C_{obs_i}$ is hence testable against measured variables, and called a *testable constraint* in (Ploix et al (2008)) or more commonly an *Analytical Redundancy Relation* (ARR) in (Frank (1990); Chow and Willsky (1984)). Each ARR $C^k_{obs_i}$ gives rise to a consistency indicator, so-called *residual* denoted r^k_i.

Definition 1 A dynamic constraint of the form $C^k_{obs_i}(\bar{u}(t), \bar{y}(t), \bar{\epsilon}(t)) = 0$, where $\bar{\nu}(t)$ stands for the vector $\nu(t)$ and its derivatives up to some unspecified order, is an ARR for (2), if for all ($u(t)$, $y(t)$) consistent with (2), the dynamic constraint is statistically satisfied.

The residual r^k_i is time-dependent and it is given a Boolean value by the following application:

$$r^k_i(t) = \begin{cases} 0 \text{ if } C^k_{obs_i} \text{ is satisfied by } (u(s), y(s)),\ s \leq t \\ 1 \text{ otherwise} \end{cases}$$

For linear systems, the parity space approach (Chow and Willsky (1984); Gertler (1998); Cocquempot et al (2004)) allows one to eliminate state variables from a model of the form (4) and to obtain ARRs by projection on a particular space called *the parity space*. In practice, the numerical computation of residuals is achieved in a discretized time framework $t = k.\Delta t$, where $k \in \mathbb{N}$ and Δt is the sampling period. One may use sophisticated algorithms that exist to estimate the time derivatives of measured signals (Brenan et al (1989)) or derive a discrete-time system from the original system (4). Proper evaluation of the residuals of a mode q_i requires to gather the measurements over a time window of length at least equal to $p_i.\Delta t$, where p_i is known as the parity order. For more details, the reader is referred to the appendix which provides the steps of residual generation for a mode q_i from a discrete time linear model obtained from (4).

Extensions of the parity space approach to non linear systems have been proposed (Kinnaert (2003); Staroswiecki and Comtet-Varga (2001)). Structural approaches can be useful to derive the structure of residuals (Staroswiecki (2002); Armengol et al (2009); Travé-Massuyès et al (2006); Krysander et al (2008)), and lead to sequential residual generators (Svard and Nyberg (2010)).

The faulty modes that have no behavioral model have not their own set of residuals but the knowledge of (3) allows us to determine whether the fault vector $\xi(t)$ impacts the residual values of the modeled modes and which Boolean value should be expected. In the work by Vento et al (2010, 2012), only this type of faulty modes is considered.

The theoretical signature of a fault is classically defined for a continuous system as the expected Boolean values of the system residuals generated from one single system nominal behavior model (Gertler (1998)). In this section, the concept of fault signature is revised for multimode systems.

In (Cocquempot et al (2004)), hybrid diagnosability analysis is achieved by considering the residual set of the different modes pairwise. The idea proposed in this paper is different and consists in defining a *mode signature* that takes into account the residuals of all the modes that have a behavioral model of the system at once. The theoretical mode signature of a mode captures the expected Boolean values of the residuals of the whole multimode system when the system is in this mode. It characterizes the expected behavior of this particular mode w.r.t all other modes. This concept, already introduced in Bayoudh et al (2008a), is defined from the concepts of *mirror signature* and *reflexive signature*.

The q_j-mirror signature of mode q_i is the vector of Boolean residuals of mode q_j evaluated when the system is in mode q_i. We use the term *mirror* because it represents the signature of "q_i seen in mode q_j".

Definition 2 Mirror Signature
Given the vector $R_{q_j} = [r_j^1, r_j^2, ..., r_j^{n_j}]^T$ of Boolean residuals associated to mode q_j, where n_j is the number of residuals, the q_j-mirror signature of mode q_i is given by the vector $S_{i/j} = R_{q_j}(\zeta_{OBS_{q_i}})$, where $\zeta_{OBS_{q_i}}$ denotes the incoming measured variable values of mode q_i i.e. output values that are consistent with the model of mode q_i.

The reflexive signature is the particular case of mirror signature for which $i = j$.

Definition 3 Reflexive Signature
The reflexive signature of mode q_i, $S_{i/i} = R_{q_i}(\zeta_{OBS_{q_i}})$ is the vector of Boolean residuals of mode q_i evaluated with incoming measured variable values of the same mode q_i. Obviously, from definition 1, $S_{i/i} = R_{q_i}(\zeta_{OBS_{q_i}}) = [0, 0, ..., 0]_{n_i}^T$.

Definition 4 Mode Signature
The signature of a mode q_i is the vector obtained by the concatenation of all the mirror signatures of q_i, $Sig(q_i) = [S_{i/1}^T, S_{i/2}^T, ..., S_{i/i}^T, ..., S_{i/n_r}^T]^T$, where n_r is the number of system modes with behavioral model [5].

It is now interesting to relate the concept of mode signature to the more standard concept of fault signature, which is defined as the set of all possible observations under a given fault (Travé-Massuyès et al (2006)). To do so, consider a string $s = s_1.s_2.....s_n.\sigma$ of events and let us define $\mathcal{T}(q, s)$ as the recursive application of T along the string s, i.e. $\mathcal{T}(q, s) = T(...T(T(q, s_1), s_2), ..., s_n), \sigma)$.

Definition 5 Fault signature
The signature of a fault F_i is given by the set of signatures of the system modes in which the fault is present. Assuming that the model (1) does not account for actions that repair the faults, the signature of a fault F_i is equal to the set of signatures of the modes that are reachable from a transition labeled with the fault event f_i. Formally:

$$Sig(F_i) = \bigcup_{\substack{k \in 1..m \\ u \in \Sigma^*}} \{Sig(\mathcal{T}(q_k, f_i u))\}.$$

[5] Note that in practice, shared residuals, i.e. residuals that are involved in more than one mode's residual vector, are only considered once in order to reduce the mode signature size.

Example 2 Let us consider the running example of figure 1. The continuous dynamics in each mode are linear so that the extension of the parity space approach to multimode systems is applicable (Chow and Willsky (1984); Bayoudh et al (2008b)). ARRs are obtained by eliminating the state variables. They involve the input/output variables and their successive derivatives until order 2. The residual vector of mode q_i is calculated as follows:

$$R_{q_i} = \Omega_i [y, \dot{y}, \ddot{y}]^T - \mathcal{L}_i [u, \dot{u}, \ddot{u}]^T \quad (5)$$

where $\mathcal{L}_i = \begin{bmatrix} \mathcal{D}_i & 0 & 0 \\ \mathcal{C}_i\mathcal{B}_i & \mathcal{D}_i & 0 \\ \mathcal{C}_i\mathcal{A}_i\mathcal{B}_i & \mathcal{C}_i\mathcal{B}_i & \mathcal{D}_i \end{bmatrix}$ and Ω_i chosen such that $\Omega_i \times \begin{bmatrix} \mathcal{C}_i \\ \mathcal{C}_i\mathcal{A}_i \\ \mathcal{C}_i\mathcal{A}_i^2 \end{bmatrix} = 0$.

Boolean residual vectors associated to modes $N, qF1, qF2, q'F1$ and $q'F2$ are denoted: $R_N \in \mathbb{R}^1, R_{qF1} \in \mathbb{R}^2, R_{qF2} \in \mathbb{R}^2, R_{qF'1} \in \mathbb{R}^1$ and $R_{q'F2} \in \mathbb{R}^1$.
Although modes qF1and qF2 have two distinct state-space representations, they have the same input/output behavior and $R_{qF1} = R_{qF2}$, i.e. residuals of modes $qF1$ and $qF2$ are identical. In consequence, they are taken only once in the mode signatures. Finally, the theoretical mode signatures for each mode $q_i \in \{N, qF1, qF2, q'F1, q'F2\}$ is obtained as $Sig(q_i) = [S_{i/N}^T, S_{i/qF1}^T = S_{i/qF2}^T, S_{i/q'F1}^T, S_{i/q'F2}^T]^T \in \mathbb{R}^5$ valuated for every mode as follows :

$$Sig(N)= \begin{bmatrix}0\\1\\1\\1\\1\end{bmatrix}, Sig(qF1)= \begin{bmatrix}1\\0\\0\\1\\1\end{bmatrix}, Sig(qF2)= \begin{bmatrix}1\\0\\0\\1\\1\end{bmatrix}, Sig(q'F1)= \begin{bmatrix}1\\1\\1\\0\\1\end{bmatrix}, Sig(q'F2)= \begin{bmatrix}1\\1\\1\\1\\0\end{bmatrix}$$

Note that the fault signatures of faults $F1$ and $F2$ are given by the sets $Sig(F1) = \{Sig(qF1), Sig(q'F1)\}$ and $Sig(F2) = \{Sig(qF2), Sig(q'F2)\}$.

3.1 Diagnosability from continuous observations

By analogy with fault diagnosability for single mode continuous systems (Gertler (1998)), mode diagnosability and fault diagnosability are defined in the context of multimode systems. In this context, diagnosability means that modes/faults are distinguishable from continuous observations ζ_{OBS}. Hence the results below are quite straightful:

Definition 6 Mode diagnosability from continuous observations
Two modes q_i and q_j are diagnosable if $Sig(q_i) \neq Sig(q_j)$. A multimode system Ξ is mode diagnosable if and only if all pairs of modes q_i and q_j, $i \neq j$, are diagnosable.

Definition 7 Fault diagnosability from continuous observations
Two faults F_i and $F_j, i \neq j$ are diagnosable if $Sig(F_i) \cap Sig(F_j) = \emptyset$ [6]. A multimode system Ξ is fault diagnosable if and only if all pairs of faults F_i and F_j, $i \neq j$, are diagnosable.

It is important to remark that, from the definitions of mode and fault signatures, mode diagnosability is a stronger concept than fault diagnosability.

Proposition 1 *If a multimode system Ξ is mode diagnosable, then it is fault diagnosable but the inverse is not true.*

[6] This is the well-known definition of fault diagnosability (Travé-Massuyès et al (2006)).

Example 3 Given the running example of figure 1, and considering continuous observations only, modes $qF1$ and $qF2$ are not diagnosable because they have the same mode signature: $Sig(qF1) = Sig(qF2)$, therefore the multimode system is not diagnosable (c.f. definition 6). Furthermore, the faults F_1 and F_2 are not diagnosable because $Sig(F_1) \cap Sig(F_2) = \{Sig(qF1), Sig(q'F1)\} \cap \{Sig(qF2), Sig(q'F2)\} \neq \emptyset$ (c.f. definition 7).

We will see later that the hybrid system may be overall diagnosable eventhough it is not diagnosable from the continuous observations.

4 Diagnosis-driven event abstraction of the continuous dynamics

For analysis purposes, it is often useful to abstract a system in a way that preserves the properties of interest (Alur et al (2000)). A key idea of this paper is to abstract the evolution of a set of continuous quantities relevant for diagnosis, namely mode signatures, in terms of events so that diagnosis and diagnosability analysis of the hybrid system can be cast into the discrete event framework. To do so, our hybrid framework assumes that the discrete dynamics are an order of magnitude slower than the dynamics of residual generators so that mode signatures can be properly determined once the hybrid system enters a new mode.This requirement is stated in the following assumption, which guarantees that the duration that the hybrid automaton remains in a single mode before switching to the next mode allows for proper evaluation of the residuals.

Assumption – The minimum dwell time τ of the hybrid automaton S given by (1) is greater or equal to the lengh of the time window required to calculate the highest order derivative signals involved in the determination of the residuals, i.e. $\tau \geq p_i^*.\Delta t$, where p_i^* is the maximal parity order of the modes of the hybrid system.

A set of discrete events Σ^{Sig} is defined through an abstraction function f_{Sig}. f_{Sig} associates a discrete event, called a ***signature-event***, to the mode signature change occurring when the hybrid system transitions from one mode to another as follows:

$$\begin{array}{c} f_{Sig} : Q \times T(Q,\Sigma) \longrightarrow \Sigma^{Sig} \\ (q_i, q_j) \longmapsto \delta_{ij} \end{array} \tag{6}$$

The event δ_{ij} is observable and noted Ro_{ij} if the mode signature of the source mode q_i is different from the mode signature of the destination mode q_j ($Sig(q_i) \neq Sig(q_j)$, i.e. when q_i and q_j are diagnosticable from continuous observations. δ_{ij} is unobservable and noted Ruo_{ij} otherwise [7]. Hence Σ^{Sig} is partitionned in a set of observable signature-events Σ_o^{Sig} and a set of unobservable signature-events Σ_{uo}^{Sig}.

In generating signature-events, two practical problems must be handled. The first refers to deciding whether two mode signatures are different or not. This is a tedious task that must account for the sensitivity of the residuals and for the signal-to-noise ratio. The second is that the presence of the noise term $\epsilon(t)$ in (2) may result in chattering and that the temporal window over which measurements are recorded to evaluate the residuals overlaps over two modes just after a mode change. This is controlled by a residual filter that holds-on to the current Boolean value as long as the residual is not computed to a different value during a specified number of time steps (Bayoudh et al (2008b)).

[7] Notice that, by construction, mode signatures cannot change while being in the same mode.

4.1 Abstract language and abstract trajectories

The abstraction of the continuous dynamics evolution in terms of signature-events allows one to define an abstract language based on $\bar{\Sigma} = \Sigma \cup \Sigma^{Sig}$, the extended alphabet that includes signature-events. $\bar{\Sigma}$ can be partitioned into $\bar{\Sigma} = \bar{\Sigma}_o \cup \bar{\Sigma}_{uo}$ with $\bar{\Sigma}_o = \Sigma_o \cup \Sigma_o^{Sig}$ and $\bar{\Sigma}_{uo} = \Sigma_{uo} \cup \Sigma_{uo}^{Sig}$.
The behavior of the hybrid system is then abstracted by the prefix-closed language $L(S) \subseteq \bar{\Sigma}^*$ over the event alphabet $\bar{\Sigma}$, where $\bar{\Sigma}^*$ is the Kleene-Closure of $\bar{\Sigma}$ (Ramadge and Wonham (1989)) that contains all finite strings of elements of the set $\bar{\Sigma}$ including the empty string. A trajectory of the abstract hybrid system corresponds to a string of events of the extended alphabet $\bar{\Sigma}$.

4.2 The behavior automaton

The finite state generator (Ramadge and Wonham (1989)) of the language $L(S)$ is called the *behavior automaton* and denoted $B_A(S) = (\bar{Q}, \bar{\Sigma}, \bar{T}, \bar{q}_0)$.

The behavior automaton is obtained by defining a set of *transient* modes Q_t that model the continuous dynamics reaction to the occurrence of a mode change, and hence lead to the generation of a discrete event of Σ^{Sig}. We first define the bijective function f_t that associates a transient mode to each transition $t(q_i, \sigma_{ij}, q_j) \in \mathbb{T}$ of the underlying DES $M = (Q, \Sigma, T, q_0)$. The set of transient modes is obtained as follows :

$$f_t : \mathbb{T} \longrightarrow Q_t$$
$$t(q_i, \sigma_{ij}, q_j) \longmapsto q_{ij}$$

The set of modes of the behavior automaton is then given by $\bar{Q} = Q \cup Q_t$. The partial transition function $\bar{T} \subseteq (\bar{Q} \times \bar{\Sigma} \longrightarrow \bar{Q})$ decomposes in two partial transition functions as follows:

$$\bar{T} = \bar{T}_1 \cup \bar{T}_2, \text{ with } \bar{T}_1 \subseteq (Q \times \Sigma \longrightarrow Q_t) \text{ and } \bar{T}_2 \subseteq (Q_t \times \Sigma^{Sig} \longrightarrow Q)$$

The behavior automaton $B_A(S) = (\bar{Q}, \bar{\Sigma}, \bar{T}, \bar{q}_0)$ is obtained by replacing every transition $t(q_i, \sigma_{ij}, q_j)$ of $M = (Q, \Sigma, T, q_0)$ by two transitions in sequence $t_1(q_i, \sigma_{ij}, q_{ij}) \in \bar{T}_1$ and $t_2(q_{ij}, R_{ij}, q_j) \in \bar{T}_2$, the transient mode $q_{ij} \in Q_t$ hence taking place in between q_i and q_j. This means that, on the occurence of an event $\sigma_{ij} \in \Sigma$, that triggers a transition from mode q_i to mode q_j, the system goes through a transient mode q_{ij}, and is necessarily followed by the occurrence of a signature-event $\delta_{ij} \in \Sigma^{Sig}$. The transient mode is a way to account for the hybrid automaton S dwell time τ requirement expressed in section 4. This requirement guarantees that residuals, and hence mode signatures, can be properly computed and that signature-events can be properly issued.

Example 4 Let us consider the example of figure 1, then the behavior automaton of the hybrid system is provided in figure 2. Six transient modes have been introduced : $NqF1$, $NqF2$, $qq'F1$, $q'qF1$, $qq'F2$, and $q'qF2$. Five signature-events have been obtained from the abstraction function f_{Sig} (6): Ro_{12}, Ro_{23}, Ro_{32}, Ro_{24}, and Ro_{42}.

5 The diagnoser

Having constructed the behavior automaton $B_A(S) = (\bar{Q}, \bar{\Sigma}, \bar{T}, \bar{q}_0)$, which represents an appropriate discrete-event abstraction of the hybrid system, diagnosis and diagnosability

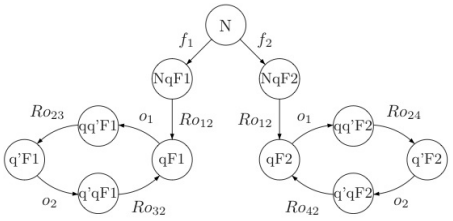

Fig. 2 The behavior automaton of the running example

analysis can be achieved with the diagnoser approach of Sampath et al (1995). The behavior automaton permits an extension of this approach to hybrid systems (Bayoudh et al (2008b)). The diagnoser is a finite state machine built from $B_A(S)$ as explained below.

First, we define a set of fault labels $\Delta_f = \{F_1, F_2, ..., F_l\}$, where l is the number of different fault types in the system [8]. The set of possible fault labels is defined as $\Delta = 2^{\Delta_f}$. Notice that the empty-set label $\emptyset \in \Delta$ should be interpreted as representing the normal behavior of the system. A label of the form $\{F_i, F_j\}$ means that at least one fault of type i and at least one fault of type j have occurred. Given $s \in \bar{\Sigma}^*$ a string of events, "$f_i \in s$" means that at least one fault event corresponding to fault F_i belongs to s. Let s_f denote the final event of a string s and $L(S, q)$ the set of all strings that originate from state $q \in \bar{Q}$.
We define:

$$L_o(S, q) = \{s \in L(S, q) \mid s = u\sigma, u \in \bar{\Sigma}^*_{uo}, \sigma \in \bar{\Sigma}_o\}$$

and

$$L_\sigma(S, q) = \{s \in L_o(S, q) \mid s_f = \sigma\}.$$

$L_o(S, q)$ denotes the set of all strings that originate from the state q and end at the first observable event. $L_\sigma(S, q)$ denotes those strings in $L_o(S, q)$ that end at the particular observable event σ.
$\bar{Q}_o = \{q_0\} \cup \{q \in \bar{Q}, \exists(q', \sigma) \in \bar{Q} \times \bar{\Sigma}_o \mid \bar{T}(q', \sigma) = q\}$ denotes the set of observable states. We define the label propagation function $LP : \bar{Q}_o \times \Delta \times \bar{\Sigma}^* \to \Delta$. Given $q \in \bar{Q}_o, l \in \Delta$ and $s \in L_o(S, q)$, LP propagates the label l over s, starting from q and following the dynamics of S, i.e. according to $L(S, q)$:

$$LP(q, l, s) = \begin{cases} \emptyset \text{ if } l = \emptyset \text{ and } \forall i, f_i \notin s \\ \{F_i | F_i \in l\} \cup \{F_i | f_i \in s\} \text{ otherwise} \end{cases}$$

The diagnoser of the abstract system is a deterministic finite state machine $Diag(B_A(S)) = (Q_D, \Sigma_D, T_D, q_{D_0})$ built from the behavior automaton where:

- $q_{D_0} = \{(q_0, \emptyset)\}$ is the initial state of the diagnoser (we assume that the system S starts in a normal mode),
- $\Sigma_D = \bar{\Sigma}_o$ is the set of all observable events of the system,
- $Q_D \subseteq 2^{\bar{Q}_o \times \Delta}$ is the set of states of the diagnoser (states reachable from q_{D_0} under T_D). The states of the diagnoser provide the set of diagnosis candidates as a set of couples whose first element refers to the state of the behavior automaton $B_A(S)$ and the second

[8] The same symbol is used for faults and their corresponding labels.

is a label providing the set of faults on the path leading to this state. In other words, an element $q_D \in Q_D$ is a set of the form $q_D = \{(q_1, l_1), (q_2, l_2), ..., (q_n, l_n)\}$, where $q_i \in \bar{Q}_o$ and $l_i \in \Delta$.

– $T_D \subseteq Q_D \times \bar{\Sigma}_o \rightarrow Q_D$ is the partial transition function of the diagnoser defined as follows:

$$T_D(q_D, \sigma) = \bigcup_{\substack{(q,l)\in q_D \\ s\in L_\sigma(S,q)}} \{(\bar{\mathcal{T}}(q, s), LP(q, l, s))\}$$

where $\bar{\mathcal{T}}(q, s)$ is the recursive application of $\bar{T}$ along the string s as defined in section 3.

It is well-known that the construction of the diagnoser is of exponential complexity in the number of states and number of fault labels of the initial automaton. However, in contrast to standard DES models, our hybrid formalism limits the number of discrete states to the operating modes of the system. The combinatorial problem introduced by discretizing variables is hence avoided and the number of discrete states is hence drastically reduced, which makes the problem much more tractable.

Example 5 Let us consider the behavior automaton of figure 2. The diagnoser of the abstract system is built as explained above and provided in figure 3. The events associated to transitions of the diagnoser are all the observable events of the original system. The states of the diagnoser provide the diagnosis information in terms of possible states of the behavior automaton and its associated faults.

Starting with the normal state "N", assume that we observe the string of observable events $Ro_{12}.o_1.Ro_{23}$, then the diagnosis is given by the pair $(q'F1, \{F1\})$, which means that the system is in state $q'F1$ and that the fault $F1$ has occured. If Ro_{24} is observed instead of Ro_{23}, then the diagnosis is different and equal to $(q'F2, \{F2\})$. Without signature-events, the observed string would be reduced to the event o_1 and the diagnosis could not disambiguate the two diagnoser states $(q'F1, \{F1\})$ and $(q'F2, \{F2\})$, as it can be seen on the diagnoser of the underlying DES $M = (Q, \Sigma, T, q_0)$ given in figure 4. This illustrates clearly how signature-events coming from the continuous dynamics can refine the diagnosis.

6 Diagnosability of the hybrid system

The diagnosability of a system depends on the observable manifestations of the different faulty situations. In other words, the occurrence of any fault event must be detectable on a bounded time window. In the case of hybrid systems, observable manifestations consist in the continuous evolutions reported by the sensors and in the observable discrete events. In our case, continuous dynamics are abstracted in term of a set of signature-events, some of which are observable. Diagnosability can hence be analyzed from the abstract language $L(S)$ defined in the previous sections.

6.1 Properties of the hybrid language

Let us consider the abstract language $L(S) \subseteq \bar{\Sigma}^*$. As presented before, this language interlinks in a specific way discrete events from Σ and events issued from the abstraction of the continuous dynamics Σ^{Sig}. $L(S)$ has the property below illustrated in figure 5.

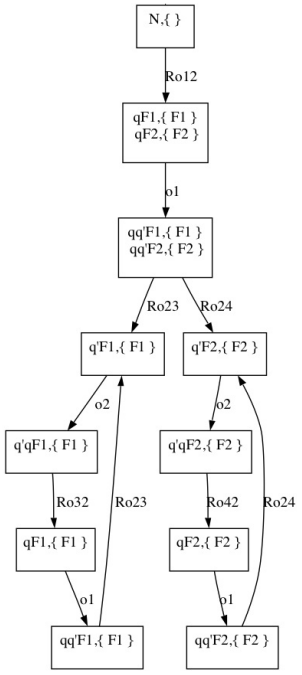

Fig. 3 The diagnoser $Diag(B_A(S))$ for the running example

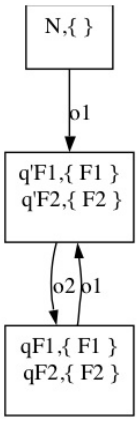

Fig. 4 The diagnoser of $M = (Q, \Sigma, T, q_0)$

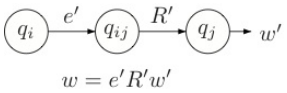

Fig. 5 Property of the abstract language

Property 1 $\forall w \in L(S), w = e'.R'.w'$, where $e' \in \Sigma, R' \in \Sigma^{Sig}, w' \in L(S)$.

This property is true by construction (cf. section 4.2). It is useful later to prove the conditions for diagnosability of the hybrid system.

6.2 Hybrid system diagnosability definition

Definition 8 A fault F is diagnosable if the occurrence of the associated fault event f can always be detected from the system observations with a finite delay i.e. thanks to a finite sequence of observable discrete events and the continuous variable measurements gathered on a bounded time window. The hybrid system is said to be diagnosable if and only if all the anticipated faults are diagnosable.

According to Sampath et al (1995), this definition can be interpreted formally as follows.

Definition 9 The hybrid system is diagnosable if $\forall f$, $\exists n \in \mathbb{N}$ such that $\forall s_F t \in L(S)$, such that s_F ends with the occurrence of f, and $t \in L(S)$ is a continuation of s_F:

$$||t|| \geq n \Rightarrow (\forall w \in L(S) : P_{\bar{\Sigma}_o}(w) = P_{\bar{\Sigma}_o}(s_F t) \Rightarrow f \in w)$$

where $P_{\bar{\Sigma}_o}$ is the projection operator on the set of observable events of $\bar{\Sigma}$ i.e. $\bar{\Sigma}_o = \Sigma_o \cup \Sigma_o^{Sig}$.

Let us notice that definition 9 characterizes *mode* diagnosability. Travé-Massuyès et al (2006) indeed showed that it naturally extends to multiple faults, hence to modes. From now on, diagnosability is understood as mode diagnosability.

6.3 Sufficient conditions for hybrid diagnosability

Two sufficient conditions for the diagnosability of the hybrid system $S = (\zeta, Q, \Sigma, T, C, (\zeta_0, q_0))$ based on the diagnosability of the underlying DES $M = (Q, \Sigma, T, q_0)$ on one hand, and on the diagnosability of the multimode system $\Xi = (\zeta, Q, C, \zeta_0)$ on the other hand, are stated and proved. Given that diagnosability is improved by the addition of observations, these results are quite obvious and easily proved.

6.3.1 The sufficient condition based on discrete event observations

Theorem 1 *The hybrid system $S = (\zeta, Q, \Sigma, T, C, (\zeta_0, q_0))$ is diagnosable if its underlying DES $M = (Q, \Sigma, T, q_0)$ is diagnosable.*

Proof Consider a hybrid system $S = (\zeta, Q, \Sigma, T, C, (\zeta_0, q_0))$ such that the underlying DES $M = (Q, \Sigma, T, q_0)$ is diagnosable. Let us consider a fault $f \in \Sigma_F$ and $s_F t \in L(S)$ such that $s_F \in L(S)$ ends with the occurrence of f and $t \in \bar{\Sigma}^*$ is a continuation of s_F as shown in figure 6.
Let us define $s'_F = P_\Sigma(s_F)$ and $t' = P_\Sigma(t)$, where P_Σ is the projection on the set of discrete events Σ. We have $s'_F \in L(M)$ that ends with $f \in \Sigma_{uo} \subseteq \Sigma$ and $t' \in \Sigma^*$ is a continuation of s'_F. Since $M = (Q, \Sigma, T, q_0)$ is diagnosable then there exists an integer n' such that: $||t'|| \geq n' \Rightarrow \forall w' \in L(M), (P_{\Sigma_o}(w') = P_{\Sigma_o}(s'_F t') \Rightarrow f \in w')$ (stated by the diagnosability definition of DES (Sampath et al (1995)).
Let us consider the integer $n = 2n' + 1$, then from Property 1 we have $||t|| \geq n \Rightarrow ||t'|| \geq n'$ $\forall w \in L(S)$ such that $P_{\bar{\Sigma}_o}(w) = P_{\bar{\Sigma}_o}(s_F t)$, and $w' = P_\Sigma(w)$, then :
$P_{\bar{\Sigma}_o}(w) = P_{\bar{\Sigma}_o}(s_F t) \Rightarrow P_{\Sigma_o}(w') = P_{\Sigma_o}(s'_F t') \Rightarrow f \in w'$ thus $f \in w$ and consequently the hybrid system S is diagnosable.

■

The above result provides a sufficient condition for hybrid diagnosability that is based on the observation of the discrete events only, i.e. the underlying DES $M = (Q, \Sigma, T, q_0)$ must be diagnosable. Let's outline that in practice this condition is rarely satisfied because the states of $M = (Q, \Sigma, T, q_0)$ do not have the same semantics as the states of a standard discrete-event model. Whereas a standard discrete-event model would include explicitly the events that occur after the occurrence of a fault, $M = (Q, \Sigma, T, q_0)$ does not generally include this information which is rather captured by the contiuous models associated to the system modes.

$$\underbrace{e_1 \rightarrow R_1 \rightarrow ... \rightarrow e_n \rightarrow R_n \rightarrow f}_{s_F} \rightarrow \underbrace{R_{n+1} \rightarrow e_{n+1} \rightarrow ...}_{t}$$

$$\underbrace{e_1 \rightarrow ... \rightarrow e_n \rightarrow f}_{s'_F} \rightarrow \underbrace{e_{n+1} \rightarrow ...}_{t'}$$

Fig. 6 A fault trajectory of the abstract system, where $e_i \in \Sigma$ and $R_i \in \Sigma^{Sig}, i = 1, \ldots, n+1$, and its projection into the discrete-event set Σ

6.3.2 The sufficient condition based on continuous variable observations

Theorem 2 *The hybrid system $S = (\zeta, Q, \Sigma, T, C, (\zeta_0, q_0))$ is diagnosable if the underlying multimode system $\Xi = (\zeta, Q, C, \zeta_0)$ is diagnosable.*

Proof Consider a hybrid system $S = (\zeta, Q, \Sigma, T, C, (\zeta_0, q_0))$, such that the underlying multimode system $\Xi = (\zeta, Q, C, \zeta_0)$ is diagnosable. Given a fault $f \in \Sigma_F$ and $s_F t \in L(S)$ such that $s_F \in L(S)$ ends with the occurrence of f as shown in figure 7, let $q_c(q_f)$ be the mode of the system before (after) the occurrence of the fault event f.
Since the underlying multimode system is diagnosable then $\forall q_i \neq q_j, Sig(q_i) \neq Sig(q_j)$, therefore $\Sigma_{uo}^{Sig} = \emptyset$ and in addition, all the observable events $R_{o_{ij}}$ are different. Let $t \in \bar{\Sigma}^*$ be a continuation of s_F such that $||t|| \geq 1$. $\forall w \in L(S)$ such that $P_{\bar{\Sigma}_o}(w) = P_{\bar{\Sigma}_o}(s_F t)$, Property 1 guarantees that $P_{\bar{\Sigma}_o}(s_F t) = P_{\bar{\Sigma}_o}(s_F) R_{o_{cf}} w'$ (where $w' \in \bar{\Sigma}_o^*$). The observation of the event $R_{o_{cf}}$ means that the system has transited from the current mode q_c to the faulty mode q_f, thus $f \in w$. Hence, the hybrid system S is diagnosable.

■

$$\underbrace{e_1 \rightarrow R_1 \rightarrow ... \rightarrow e_n \rightarrow R_n \rightarrow f}_{s_F} \rightarrow \underbrace{R_{o_{cf}} \rightarrow e_{n+1} \rightarrow ...}_{t}$$

Fig. 7 A fault trajectory of the abstract system

Corollary 1 *If all pairs of modes (q_i, q_j), $i \neq j$, of the hybrid system are diagnosable then the hybrid system is diagnosable.*

Proof The proof follows directly from definition 6 and theorem 2.

■

Theorem 2 provides a sufficient condition based on the diagnosability of the different modes of the hybrid system from the observation of their continuous dynamics.

6.4 Necessary and sufficient condition

This section shows that both continuous and discrete-event observations are required to achieve a necessary and sufficient condition for hybrid diagnosability. This condition is obtained on the diagnoser of the abstract system as an extension of the diagnosability condition for DES of (Sampath et al (1995)).

Consider $Diag(B_A(S)) = (Q_D, \Sigma_D, T_D, q_{D_0})$, the diagnoser of the abstract system and $\Delta_f = \{F_1, F_2, ..., F_n\}$, the set of fault labels.

Definition 10 Uncertain state
Given a diagnoser state $q_D \in Q_D$, q_D is F_i-uncertain if F_i belongs to at least one label of q_D but not all. Formally, a state $q_D \in Q_D$ is F_i-uncertain if $\exists (q, l), (q', l') \in q_D$, such that $F_i \in l$ and $F_i \notin l'$.

Definition 11 Indeterminate cycle
An F_i-indeterminate cycle $\mathcal{C}_{F_i}$ in $Diag(B_A(S))$ is a cycle composed of F_i-uncertain states for which there exist:

1. a corresponding cycle (of observable events) in $B_A(S)$ involving only states that carry F_i in their labels in $\mathcal{C}_{F_i}$
2. a corresponding cycle in $B_A(S)$ involving only states that do not carry F_i in their labels in $\mathcal{C}_{F_i}$.

Proposition 2 *The hybrid system $S = (\zeta, Q, \Sigma, T, C, (\zeta_0, q_0))$ is diagnosable, i.e. the abstract language $L(S)$ is diagnosable, if and only if there is no F_i-indeterminate cycle in the diagnoser $Diag(B_A(S))$ for all F_i.*

Proof This result is a direct extension of the diagnosability condition of Sampath et al (1995). Sampath et al (1995) proved that a language L is diagnosable if and only if there is no F_i-indeterminate cycle in its diagnoser, for all F_i. This condition, applied to the abstract language $L(S)$, provides proposition 2 and guarantees that the hybrid system is diagnosable because the abstraction in terms of signature-events preserves mode diagnosability.

■

Example 6 Let us come back to the running example of figure 1 and analyse the diagnoser that was given in figure 3. This diagnoser does not contain any indeterminate cycles. Then, according to the sufficient and necessary condition of Proposition 2, we conclude that the hybrid system is diagnosable.

It is interesting to notice that none of the two sufficient conditions for diagnosability given by theorem 1 and theorem 2 hold, i.e.:

- the underlying multimode system is not diagnosable, which was shown in section 3.1. In particular faults F_1 and F_2 are not diagnosable from the continuous observations.
- the underlying DES is not diagnosable due to the presence of the indeterminate cycle (o_1, o_2), involving the uncertain states $\{(qF1, \{F_1\}), (qF2, \{F_2\})\}$ and $\{(q'F1, \{F_1\}), (q'F2, \{F_2\})\}$, in its diagnoser (cf. figure 4). Again, faults F_1 and F_2 are not diagnosable.

Hence, the necessary and sufficient condition is required to decide about the diagnosability of the hybrid system. Faults F_1 and F_2 are diagnosable for the hybrid system.

7 Discussion

The diagnosability definition that we use is inspired by the discrete-event system definition, hence it is event-based in the sense that it is stated in terms of fault events and guarantees that a fault event is detected after a time delay represented by an integer n as expressed in definition 9. The time delay is given as the number of observable events (from $\bar{\Sigma}_o$) required to detect the fault occurrence. It is a consequence of the discrete-event dynamics, and captures the number of mode changes in the behavior automaton $B_A(S)$ needed before fault detection. Because of the transitory modes of Q_t, the number of mode changes in the original hybrid system S is less than n. If the system modes are diagnosable from continuous observations, i.e. from their signatures, $1 \leq n \leq 2$ for all fault types F_i. Indeed, considering a transition between a normal mode q_c and a faulty mode q_f, the signature-event $R_{o_{cf}}$ induced by the signature change allows us to detect the fault as explained in the proof of theorem 2.
The proposed hybrid diagnosability condition does not account for *fair* transitions, as recently suggested by Biswas et al (2010). Fair transitions are transitions that are inevitably fired when the system is in their source mode, due to the continuous dynamics of the hybrid system. Obviously, these transitions may allow the system to exit an indeterminate cycle, relaxing the hybrid diagnosability condition. We believe that our approach could be adapted to account for fair transitions, however it should be noticed that the knowledge required to be able to assess fairness may be quite difficult to acquire, particularly in the case of nonlinear continuous dynamics.

8 Case study: the AOCS (Attitude and Orbit Control System)

The Attitude and Orbit Control System (AOCS) of a spacecraft aims to stabilize the satellite attitude in the presence of disturbances by pointing the axes of the spacecraft in the directions required for its mission (cf. figure 9). The satellite attitude is determined using measurements incoming from sensors and appropriate control torques that are exerted by actuators (thrusters, reaction wheels, ...).

In this case study, we tackle the diagnosability of the propulsion system (c.f. figure 8), the satellite attitude being measured by means of gyroscopic sensors and the attitude maneuver performed by firing the thruster **T** [9]. The thruster propellant supply is achieved by activating valve V_1. A redundant valve V_2 is used in case of failure of valve V_1. Commands ON_{V_2} and OFF_{V_2} open and close valve V_2, respectively.

The nominal modes considered in this study are denoted PH, CA and FA, and represent the thruster PreHeating, the Coarse Acquisition and the Fine Acquisition modes, respectively. In the CA mode, the attitude maneuver calls for the whole thruster power whereas in mode FA only 10% is required. Transitions between modes CA and FA are controlled by remote commands TC_1 and TC_2. Commands are observable by definition.

Our focus is on actuator faults concerning the equipments that are represented by a continuous model and on faults manifesting on the discrete dynamics like a fault on the discrete controller. Faults are represented by specific faulty modes and by means of fault events that lead to these faulty modes.
For this case study, two faults on the thruster **T** and one on the valve V_1 are considered by means of fault events f_1 (thruster 50% stuck), f_2 ((thruster 100% stuck) and f_3 (valve

[9] Redundant thrusters are not considered here, for sake of simplicity.

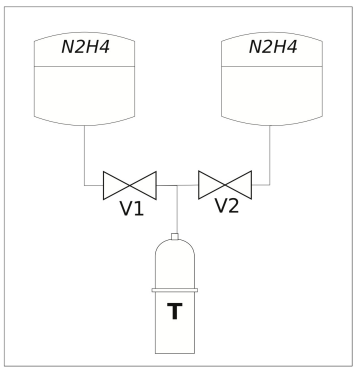

Fig. 8 The propulsion system

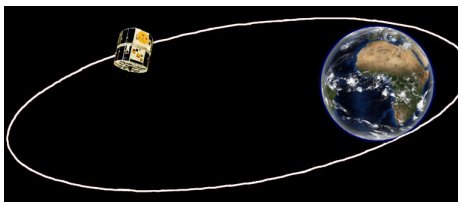

Fig. 9 Orbiting spacecraft

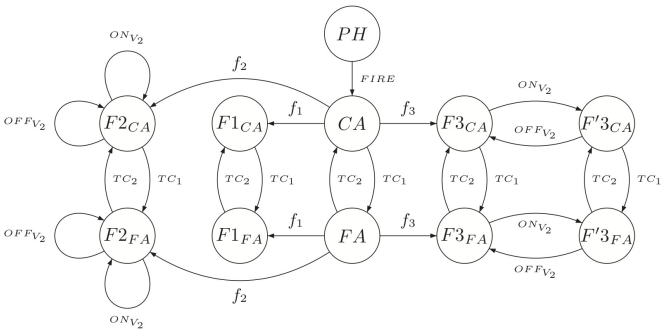

Fig. 10 Underlying DES and modes of the Attitude and Orbit Control System (AOCS)

V_1 blocked) that lead to faulty modes $F1_{CA}$, $F1_{FA}$, $F2_{CA}$, $F2_{FA}$, and $F3_{CA}$, $F3_{FA}$, respectively. Notice that each fault can occur both in modes CA and FA. $F3'_{CA}$ and $F3'_{FA}$ are reachable from $F3_{CA}$ and $F3_{FA}$ respectively, by opening valve V_2. Table 1 presents the nominal and faulty system modes of the AOCS. The mode transitions are described by the mode automaton provided in figure 10.

The continuous behaviors in both nominal and faulty modes are given in the state-space representation form (7), where the tuples ($\tilde{A}$, $\tilde{B}$, $\tilde{C}$, $\tilde{D}$) are specified in the last column of

table 1 for each mode [10].

$$\begin{cases} \dot{x}(t) = \tilde{A}x(t) + \tilde{B}u(t) \\ y(t) = \tilde{C}x(t) + \tilde{D} \end{cases} \tag{7}$$

Modes	Valve $V1$	Valve $V2$	Thruster	State-space model ($\tilde{A}$, $\tilde{B}$, $\tilde{C}$, $\tilde{D}$)
PH	on	off	ok	$(A, B_{0\%}, C, D)$
CA	on	off	ok	$(A, B_{100\%}, C, D)$
FA	on	off	ok	$(A, B_{10\%}, C, D)$
$F1_{CA}$	on	off	50% stuck	$(A, B_{50\%}, C, D)$
$F2_{CA}$	on	off	100% stuck	$(A, B_{0\%}, C, D)$
$F3_{CA}$	$blocked$	off	ok	$(A, B_{0\%}, C, D)$
$F'3_{CA}$	$blocked$	on	ok	$(A, B_{100\%}, C, D)$
$F1_{FA}$	off	off	50% stuck	$(A, B_{10\%}, C, D)$
$F2_{FA}$	off	off	100% stuck	$(A, B_{0\%}, C, D)$
$F3_{FA}$	$blocked$	off	ok	$(A, B_{0\%}, C, D)$
$F'3_{FA}$	$blocked$	on	ok	$(A, B_{10\%}, C, D)$

Table 1 The considered modes of the AOCS

We have:

$$A = \begin{bmatrix} 0\ 0\ 0 & 1 & 0 & 0 \\ 0\ 0\ 0 & 0 & 1 & 0 \\ 0\ 0\ 0 & 0 & 0 & 1 \\ 0\ 0\ 0 & 0 & 0 & \omega_0(\frac{I_Y - I_X}{I_Z} - 1) \\ 0\ 0\ 0 & 0 & 0 & 0 \\ 0\ 0\ 0 & \omega_0(\frac{I_Z - I_Y}{I_X} + 1) & 0 & 0 \end{bmatrix}, C = \begin{bmatrix} -\omega_0\ 0\ 0 & 0\ 0\ 1 \\ 0\ 0\ 0 & 0\ 1\ 0 \\ 0\ 0\ \omega_0 & 1\ 0\ 0 \end{bmatrix}, D = \begin{bmatrix} 0 \\ -\omega_0 \\ 0 \end{bmatrix}$$

$$B_{100\%} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ \frac{-I_W}{I_Z} & 0 & 0 \\ 0 & \frac{-I_W}{I_Y} & 0 \\ 0 & 0 & \frac{-I_W}{I_X} \end{bmatrix}, B_{50\%} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ \frac{-I_W}{2I_Z} & 0 & 0 \\ 0 & \frac{-I_W}{2I_Y} & 0 \\ 0 & 0 & \frac{-I_W}{2I_X} \end{bmatrix},$$

$$B_{10\%} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ \frac{-I_W}{10I_Z} & 0 & 0 \\ 0 & \frac{-I_W}{10I_Y} & 0 \\ 0 & 0 & \frac{-I_W}{10I_X} \end{bmatrix}, B_{0\%} = \begin{bmatrix} 0\ 0\ 0 \\ 0\ 0\ 0 \\ 0\ 0\ 0 \\ 0\ 0\ 0 \\ 0\ 0\ 0 \\ 0\ 0\ 0 \end{bmatrix}$$

[10] Faults affecting satellite inertia and gyroscopic sensors could also be represented by means of suitable dynamics and observation matrices A and C, respectively.

8.1 Diagnosability analysis

In this section we focus on the diagnosablity analysis of the hybrid system. At the continuous level, the ARRs are obtained from the continuous model of each mode by means of the parity space approach and lead to the theoretical mode signatures provided in table 2.

$\{PH, F2_{CA}, F2_{FA}, F3_{FA}, F3_{CA}\}$	$\{CA, F'3_{CA}\}$	$\{FA, F1_{FA}, F'3_{FA}\}$	$\{F1_{CA}\}$
$Sig_1 = \begin{bmatrix}0\\0\\0\\0\\0\\1\\1\\1\\1\\1\end{bmatrix}$	$Sig_2 = \begin{bmatrix}1\\1\\1\\1\\1\\0\\0\\1\\1\\1\end{bmatrix}$	$Sig_3 = \begin{bmatrix}1\\1\\1\\1\\1\\1\\1\\0\\0\\1\end{bmatrix}$	$Sig_4 = \begin{bmatrix}1\\1\\1\\1\\1\\1\\1\\1\\1\\0\end{bmatrix}$

Table 2 The mode signatures of the AOCS

The mode sets $\{PH, F2_{CA}, F2_{FA}, F3_{FA}, F3_{CA}\}$, $\{CA, F'3_{CA}\}$ and $\{FA, F1_{FA}, F'3_{FA}\}$ are not diagnosable from the continuous observations because they share the same mode signature as shown by table 2.
The underlying DES is not diagnosable either: in particular, faults F_1 and F_3 are not diagnosable because of the presence of an uncertain cycle $(TC_1TC_2)^*$ in the corresponding diagnoser.
Consequently, the diagnosability of the hybrid system cannot be decided by means of one of the two sufficient criteria. However, the hybrid system is diagnosable, which can be explained as follows.
In mode CA, the whole thruster power is required, so blockages with different levels are distinguishable. Hence fault $F1$ is diagnosable from faults $F2$, and $F3$. However, faults F_2 (thruster 100% stuck) and F_3 (valve V_1 blocked) are not diagnosable, but by activating the redundant valve V_2 (command ON_{V_2}), these two faults (modes $F2_{CA}$ and $F'3_{CA}$) can be discriminated. Similarly, in mode FA, $F2$ and $F3$ are not diagnosable but the same action as above (command ON_{V_2}) makes these two faults distinguishable. In addition, $F1$ is indistinguishable from normal, but switching to mode CA with command TC_2 brings back the system to the CA mode in which $F1$ can be distinguished from normal.
The diagnoser of the abstract system which accounts for the hybrid model is given in figure 11. The transient state between two states X and Y is noted $X^{\rightarrow Y}$. None of the cycles of the diagnoser are indeterminate cycles, which confirms the diagnosability of the propulsion system explained above.

9 Conclusion

This paper contributes with a theoretical framework to analyze the diagnosability of hybrid systems. First it is assumed that they are observed through continuous variables only and reduce to what we call a multimode system. Second discrete event observations are also

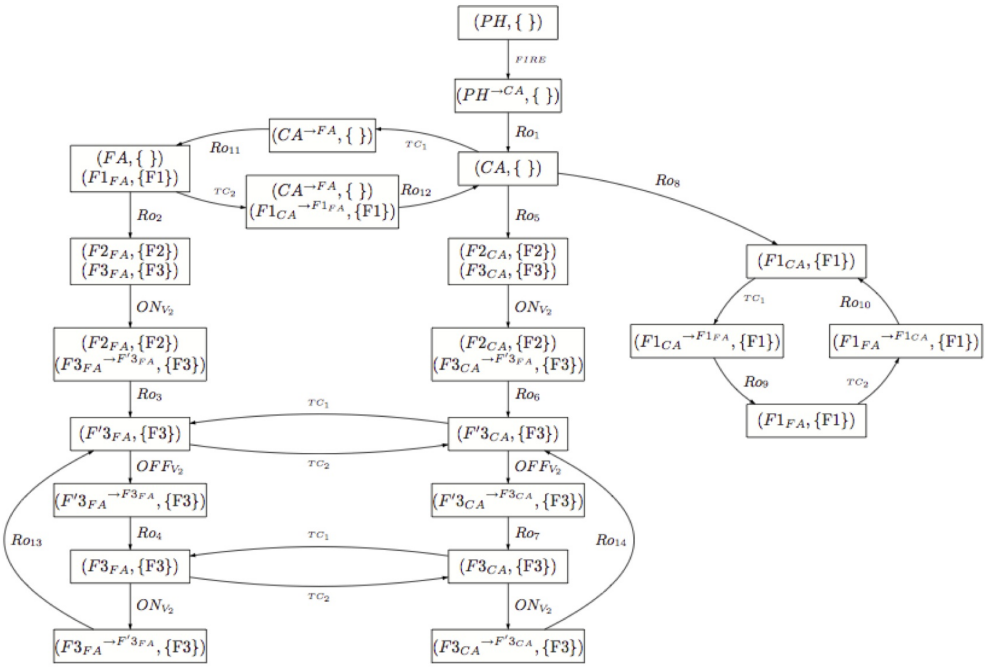

Fig. 11 The propulsion system hybrid diagnoser

assumed to be available. The new concepts of mirror, reflexive and mode signatures are introduced. Based on these concepts, a characterization of the diagnosability for multimode systems is proposed. Then, hybrid diagnosability is defined based on an abstract language over the alphabet of discrete events and additional events that capture the continuous dynamics.

By proposing an abstraction of the continuous dynamics in terms of discrete events that preserves mode diagnosability, a general framework for analyzing hybrid systems diagnosability is proposed, that builds upon existing work on DES and continuous systems diagnosability. Two sufficient conditions for diagnosability based on continuous variable measurements on one hand and on the event observations on the other hand are given, as well as a necessary and sufficient condition.

From a technical point of view, our proposal may suffer from the complexity of the diagnoser approach, which is exponential in the number of states of the behavior automaton and number of fault labels. However, the formalism that we use to represent hybrid systems is not a standard DES model as it proceeds of an aggregation in terms of modes. This results in behavior automata with a tractable number of states. An alternative to the diagnoser approach would be the twin plants approach (Jiang et al (2001b); Yoo and Lafortune (2002a)) which has polynomial time complexity. This does not solve however the problem of modeling multiple faults which results in an explosion of the state space to cover all combinations of faulty modes. This is a problem common to DES approaches. From a pragmatic point of view, it seems reasonable to adopt the single fault assumption or to model only the most probable and critical combinations of faults. Note that the modeling can be made easier by

synchronizing the automata of the different components to obtain the underlying DES of the whole system as illustrated by Maiga et al (2012).

A related scalability issue is the number of ARRs, i.e. residuals, that must be generated. Although the generation is off-line, this can be avoided by generating the ARRs on the fly at run time, for modes that are successors of the current mode Bayoudh et al (2009b).

The diagnosability analysis framework and the on-line hybrid state tracking approach proposed by Bayoudh et al (2008b) lead to an approach for active diagnosis of hybrid systems guided by diagnosability properties (Bayoudh et al (2009a)). Future works will be based on these results and consider the problem of coupling the diagnosis and planning modules involved in an architecture for autonomy. The problem of deciding whether to initiate an active diagnosis session or to keep the execution of the current plan is of particular interest. Another problem is to decide how to interlink the actions required by active diagnosis and those of the on-going plan. Another direction of work is to cast the proposed approach into a distributed framework. Some progress along this line has been reported in Indra et al (2011).

Acknowledgements This work was supported by Thales Alenia Space France. We do thank Xavier Olive who was in charge of all correspondance.

References

Alur R, Henzinger TA, Lafferire G, Pappas GJ (2000) Discrete abstractions of hybrid systems. Proceeding of the IEEE 88(7):971–984

Armengol J, Bregon A, Escobet T, Gelso E, Krysander M, Nyberg M, Olive X, Pulido B, L Travé-Massuyès L (2009) Minimal structurally overdetermined sets for residual generation: A comparison of alternative approaches. In: Proceedings of the 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Barcelona, Spain, pp 227–232

Basseville M, Kinnaert M, Nyberg M (2001) On fault detectability and isolability. European Journal of Control 7(6):625–641

Bayoudh M, Travé-Massuyès L, Olive X (2008a) Coupling continuous and discrete event system techniques for hybrid systems diagnosability analysis. In: Proceedings of the 18th European Conference on Artificial Intelligence ECAI, Patras (Greece), pp 219–223

Bayoudh M, Travé-Massuyès L, Olive X (2008b) Hybrid systems diagnosis by coupling continuous and discrete event techniques. In: Proceedings of the 17th International Federation of Automatic Control, World Congress, IFAC-WC, Seoul (Korea), pp 7265–7270

Bayoudh M, Travé-Massuyès L, Olive X (2009a) Active diagnosis of hybrid systems guided by diagnosability properties. In: Proceedings of the 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes Safeprocess'09, Barcelona, Spain, pp 1498–1503

Bayoudh M, Travé-Massuyès L, Olive X (2009b) On-line analytic redundancy relations instantiation guided by component discrete-dynamics for a class of non-linear hybrid systems. In: Proceedings of the Decision and Control Conference CDC/CCC 2009., Shanghai (China), pp 6970 – 6975

Benazera E, Travé-Massuyès L (2009) Set-theoretic estimation of hybrid system configurations. IEEE Transactions on Systems, Man, and Cybernetics Part B, Cybernetics: a publication of the IEEE Systems, Man, and Cybernetics Society 39(5):1277–1291

Biswas G, Cordier M, Lunze J, Travé-Massuyès L, (Eds) MS (2004) Special Issue on Diagnosis of Complex Systems : Bridging the methodologies of the FDI and DX Communities. IEEE Transactions on Systems, Man, and Cybernetics, Part B 34(5)

Biswas S, Sarkar D, Mukhopadhyay S, Patra A (2006) Diagnosability analysis of real time hybrid systems. In: Proceedings of the IEEE International Conference on Industrial Technology ICIT'06, Mumbai, India, pp 104–109

Biswas S, Sarkar D, Mukhopadhyay S, Patra A (2010) Fairness of transitions in diagnosability of discrete event systems. Discrete Event Dynamic Systems 20:349–376

Brenan KE, Campbell SL, Petzold LR (1989) Numerical Solution of Initial-Value Problems in Differential-Algebric Equations. SIAM, Philadelphia

Chanthery E, Pencolé Y (2009) Monitoring and active diagnosis for discrete-event systems. In: 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Systems, Barcelona, Spain, pp 1545–1550

Chen J, Patton R (1994) A re-examination of the relationship between. parity space and observer- based approaches in fault diagnosis. In: In Proceedings of the IFAC Symposium on Fault Detection, Supervision and Safety of Technical Systems Safeprocess'94, Helsinki, Finland, pp 590–596

Chow E, Willsky A (1984) Analytical redundancy and the design of robust failure detection systems. IEEE Transactions on Automatic Control 29(7):603–614

Cocquempot V, Mezyani TE, Staroswiecki M (2004) Fault detection and isolation for hybrid systems using structured parity residuals. In: Proceedings of the IEEE/IFAC-ASCC: Asian Control Conference, Melbourne, Australia, vol 2, pp 1204–1212

Contant O, Lafortune S, Teneketzis D (2006) Diagnosability of discrete event systems with modular structure. Discrete Event Dynamic Systems 16(1):9–37

Daigle MJ, Koutsoukos D, Biswas G (2010a) An event-based approach to integrated parametric and discrete fault diagnosis in hybrid systems. Transactions of the Institute of Measurement and Control, Special Issue on Hybrid and Switched Systems 32(5):487–510

Daigle MJ, Roychoudhury I, Biswas G, Koutsoukos D, Patterson-Hine A, Poll S (2010b) A comprehensive diagnosis methodology for complex hybrid systems: A case study on spacecraft power distribution systems. IEEE Transactions of Systems, Man, and Cybernetics, Part A, Special Issue on Model-based Diagnosis: Facing Challenges in Real-world Applications 4(5):917–931

Fourlas G, Kyriakopoulos K, Krikelis N (2002) Diagnosability of hybrid systems. In: Proceedings of the 10th Mediterranean Conference on Control and Automation-MED2002, Lisbon, Portugal, pp 3994–3999

Frank P (1990) Fault diagnosis in dynamic systems using analytic and knowledge-based redundancy - a survey. Automatica 26(3):459–474

de Freitas N (2002) Rao-blackwellised particle filtering for fault diagnosis. In: Proceedings of the IEEE Aerospace Conference 2002, vol 4, pp 1767–1772

Frisk E, Krysander M, Aslund J (2009) Sensor placement for fault isolation in linear differential-algebraic systems. Automatica 45(2):364–371

Gertler J (1998) Fault Detection and Diagnosis in Engineering Systems. Marcel Deker

Henzinger T (1996) The theory of hybrid automata. In: Proceedings of the 11th Annual IEEE Symposium on Logic in Computer Science (LICS'96), New Brunswick, New Jersey, pp 278–292

Hofbaur M, Williams B (2004a) Hybrid estimation of complex systems. IEEE Transactions on Systems, Man, and Cybernetics - Part B 34(5):2178–2191

Hofbaur MW, Williams BC (2004b) Hybrid estimation of complex systems. IEEE Transactions on Systems, Man, and Cybernetics - Part B: Cybernetics 34(5):2178–2191

Indra S, Travé-Massuyès L, Chanthery E (2011) A decentralized fdi scheme for spacecraft: Bridging the gap between model based fdi research and practice. In: Proceedings of the 4th European Conference for Aerospace Sciences, Saint Petersburg, Russia

Jiang S, Huang Z, Chandra V, Kumar R (2001a) A polynomial time algorithm for diagnosability of discrete event systems. IEEE Transactions on Automatic Control 46(8):1318–1321

Jiang S, Huang Z, Chandra V, Kumar R (2001b) A polynomial time algorithm for diagnosability of discrete event systems. IEEE Transactions on Automatic Control 46(8):1318–1321

Kilic E (2008) Diagnosability of fuzzy discrete event systems. Information Sciences 178(3):858–870

Kinnaert M (2003) Fault diagnosis based on analytical models for linear and nonlinear systems-a tutorial. IFAC Symposium on Fault Detection, Supervision and Safety of Technical Systems, Washington DC, USA pp 37–49

Krysander M, Aslund J, Nyberg M (2008) An efficient algorithm for finding over-constrained sub-systems for construction of diagnostic tests. IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans 38(1):197 – 206

Liu F, Qiu D (2008) Safe diagnosability of stochastic discrete-event systems. IEEE Transactions on Automatic Control 53(5):1291–1296

Lunze J, Lamnabhi F (2009) Handbook of hybrid systems control: theory, tools, applications. Cambridge

Maiga M, Chanthery E, Travé-Massuyès L (2012) Hybrid system diagnosis: Test of the diagnoser hydiag on a benchmark of the international diagnostic competition dxc2011. In: Proceedings of the 8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes Safeprocess'12, Mexico city, Mexico

Melliti T, Dague P (2010) Generalizing diagnosability definition and checking for open systems: a Game structure approach. In: Proceedings of the 21st International Workshop on Principles of Diagnosis DX'10, Portland (OR), United States, pp 103–110

Narasimhan S, Biswas G (2002) An approach to model-based diagnosis of hybrid systems. In: Tomlin C, Greenstreet M (eds) Hybrid Systems: Computation and Control, HSCC 2002, Lecture Notes in Computer Science, vol 2289, Springer Verlag, pp 308–322

Nyberg M (2002) Criterions for detectability and strong detectability of faults in linear systems. International Journal of Control 75(7):490–501

Pencolé Y (2004) Diagnosability analysis of distributed discrete event systems. In: Proceedings of the 16th Eureopean Conference on Artificial Intelligence, ECAI'2004, Valencia, Spain, pp 43–47

Pencolé Y, Subias A (2009) A chronicle-based diagnosability approach for discrete timed-event systems: Application to web-services. Journal of Universal Computer Science 15(17):3246–3272

Pérez R, Escobet T, Travé-Massuyes L (2007) Fault diagnosability utilizing quasi-static and structural modelling. Matematical and Computer Modelling 45(5):606–616

Ploix S, Yassine AA, Flaus JM (2008) An improved algorithm for the design of testable subsystems. In: Proceedings of the 17th International Federation of Automatic Control, World Congress, IFAC-WC, Seoul (Korea), pp 7191–7196

Ramadge PJ, Wonham WM (1989) The control of discrete-event systems. Proceeding of the IEEE 77(1):81–98

Ribot P, Pencolé Y (2008) Design requirements for the diagnosability of distributed discrete event systems. In: Proc. 19th Intl. Workshop on Principles of Diagnosis (DX), Blue Mountains, Australia, pp 347–354

Sampath M, Sengputa R, Lafortune S, Sinnamohideen K, Teneketsis D (1995) Diagnosability of discrete-event systems. IEEE Transactions on Automatic Control 40:1555–1575

Sampath M, Lafortune S, Teneketzis D (1998) Active diagnosis of discrete-event systems. IEEE Transactions on Automatic Control 43(7):908 – 929

Sarrate R, Puig V, Escobet T, Rosich A (2007) Optimal sensor placement for model-based fault detection and isolation. 46th IEEE Conference on Decision and Control, New Orleans (LA), USA pp 2584 – 2589

Staroswiecki M (2002) Structural analysis for fault detection and isolation and for fault tolerant control, chapter in Encyclopedia of Life Support Systems. Fault Diagnosis and Fault Tolerant Control. Oxford, UK

Staroswiecki M, Comtet-Varga G (2001) Analytical redundancy relations for fault detection and isolation in algebraic dynamic systems. Automatica 37(5):687–699

Svard C, Nyberg M (2010) Residual generators for fault diagnosis using computation sequences with mixed causality applied to automotive systems. Trans Sys Man Cyber Part A 40(6):1310–1328

Thorsley D, Teneketzis D (2005) Diagnosability of stochastic discrete-event systems. IEEE Transactions on Automatic Control 50(4):476–492

Travé-Massuyès L, Cordier M, Pucel X (2006) Comparing diagnosability criterions in continuous systems and descrete events systems. In: Proceedings of the 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes Safeprocess'06, Beijing, P.R. China, pp 55–60

Travé-Massuyès L, Escobet T, Olive X (2006) Diagnosability analysis based on component-supported analytical redundancy relations. IEEE Transactions on Systems, Man and Cybernetics, Part A 36(6):1146–1160

Vento J, Puig V, Sarrate R (2010) Fault detection and isolation of hybrid system using diagnosers that combine discrete and continuous dynamics. In: Conference on Control and Fault Tolerant System, Nice, French, pp 6914–6919

Vento J, Puig V, Sarrate R, Travé-Massuyès L (2012) Fault detection and isolation of hybrid systems using diagnosers that reason on components. In: Proceedings of the 8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes Safeprocess'12, Mexico city, Mexico

Verma V, Gordon G, Simmons R, Thrun S (2004) Real-time fault diagnosis. IEEE Robotics and Automation Magazine 11(2):56–66

Yan Y, Ye L, Dague P (2010) Diagnosability for Patterns in Distributed Discrete Event Systems. In: 21st International Workshop on Principles of Diagnosis DX'10, Portland, OR États-Unis, pp 345–352

Yoo T, Lafortune S (2002a) Polynomial-time verification of diagnosability of partially-observed discrete-event systems. IEEE Trans on Automatic Control 47(9):1491–1495

Yoo TS, Lafortune S (2002b) Polynomial-time verification of diagnosability of partially observed discrete- event systems. IEEE Transactions on Automatic Control 47(9):1491–1495

Appendix

This appendix develops the parity space residual generation method for a mode q_i with a discrete time [11] linear state-space model obtained from (4) of the form :

$$\begin{cases} x_i(n+1) = A_i x_i(n) + B_i u(n) + E_{x_i}\epsilon(n) \\ \quad y(n) = C_i x_i(n) + D_i u(n) + E_{y_i}\epsilon(n) \end{cases} \tag{8}$$

$x_i(n)$, $u(n)$, $y(n)$ and $\epsilon(n)$ are the state, the input, the output and the noise vectors of dimensions n_{x_i}, n_u , n_y and n_ϵ respectively, considered at the sampling time n. A_i, B_i, C_i and D_i are constant dynamic, input, output and direct transmission matrices of appropriate dimensions. E_{x_i} and E_{y_i} are constant matrices of appropriate dimensions that capture the influence of the noise on state and output evolution, respectively.
Following the parity space approach, ARRs can be obtained by relating the inputs with the outputs over a time-window of $p_i + 1$ samples. Selecting p_i appropriately (typically $p_i \leq n_{x_i}$) allows us to eliminate any dependency upon the system state x_i. This procedure can be summarized as follows.
Given a vector V, let us denote by V^p the vector obtained by the concatenation of the vector values at every sampling instant $(n - p + k)$, $0 \leq k \leq p$, for a given p. Then $V^p(n) = [V^T(n-p), ..., V^T(n-p+k), ..., V^T(n)]^T$. By iterating state-evolution and observation equations (8), we obtain:

$$y^{p_i}(n) = O_i^{p_i} x_i(n-p_i) + L_i^{p_i}(A_i, B_i, C_i, D_i)u^{p_i} + L_i^{p_i}(A_i, E_{x_i}, C_i, E_{y_i})\epsilon^{p_i}(n) \tag{9}$$

with: $L_i^{p_i}(A_i, N, C_i, Q) = \begin{pmatrix} Q & 0 & ... & 0 \\ C_i N & Q & ... & ... \\ ... & ... & ... & 0 \\ C_i A_i^{(p_i-1)} N & ... & C_i N & Q \end{pmatrix}$ and $N \in \{B_i, E_{x_i}\}, Q \in \{D_i, E_{y_i}\}$

$$O_i^{p_i} = \begin{pmatrix} C_i \\ C_i A_i \\ ... \\ C_i A_i^{p_i} \end{pmatrix}$$

The state $x_i(n-p_i)$ in equation (9) can be eliminated through left-hand multiplication by an operator $\Omega_i^{p_i}$. We obtain ARRs that can be decomposed into a computational and an evaluation form denoted $\rho_{c_i}^{p_i}$ and $\rho_{e_i}^{p_i}$, respectively:

$$\rho_{c_i}^{p_i}(n) = \Omega_i^{p_i} y^{p_i}(n) - \Omega_i^{p_i} L_i^{p_i}(A_i, B_i, C_i, D_i)u^{p_i}(n) \tag{10}$$

$$\rho_{e_i}^{p_i}(n) = \Omega_i^{p_i} L^{p_i}(A_i, E_{x_i}, C_i, E_{y_i})\epsilon^{p_i}(n) \tag{11}$$

The Boolean-residual vector of mode q_i is denoted $R_{q_i} = [r_i^1, r_i^2, ..., r_i^{n_i}]^T$ and is obtained by checking whether $\rho_{c_i}^{p_i}(n) = \rho_{e_i}^{p_i}(n)$. Two cases are hence distinguished.

– noise-free hypothesis: $\rho_{e_i}^{p_i} = 0, \forall n \in \mathbb{N}$
A threshold vector is defined as $\alpha_i = [\alpha_i^1, ..., \alpha_i^{n_i}]^T$. The threshold values take into account the computation precision and the relative order of magnitude of the different variables.

$$r_i^j = \begin{cases} 0 \text{ if } \rho_{c_i}^{p_i}(n) \leq \alpha_i^j \\ 1 \text{ otherwise} \end{cases} \tag{12}$$

[11] Time is considered sampled to be closer to implementation.

– white-Gaussian-Noise hypothesis
We have $\epsilon(n) \sim N(0, \sigma^2)$, hence $\epsilon(n, n-p_i) \sim N(0, diag_{p_i+1}(\sigma^2))$, where σ^2 denotes the variance and $diag_{p_i+1}(\sigma^2)$ denotes the diagonal matrix of dimension p_i+1 in which the diagonal values are equal to σ^2. Consequently the probability density function of the evaluation form has a normal distribution:
$\rho_{e_i}^{p_i}(n) \sim N(0, \Omega_i^{p_i} L^{p_i}(A_i, E_{x_i}, C_i, E_{y_i}) diag(\sigma^2)(L^{p_i}(A_i, E_{x_i}, C_i, E_{y_i}))^T (\Omega_i^{p_i})^T)$

$$r_i^j = \begin{cases} 0 \text{ if } \rho_{c_i}^{p_i}(n) \sim \rho_{e_{ij}}^{p_i} \\ 1 \text{ otherwise} \end{cases} \tag{13}$$

where $\rho_{e_{ij}}^{p_i}$ denotes the j^{th} element of $\rho_{e_i}^{p_i}$.