Solving Diagnosability of Hybrid Systems via Abstraction and Discrete Event Techniques

Alban Grastien, Louise Travé-Massuyès, Vicenç Puig

▶ **To cite this version:**

Alban Grastien, Louise Travé-Massuyès, Vicenç Puig. Solving Diagnosability of Hybrid Systems via Abstraction and Discrete Event Techniques. 20th IFAC World Congress, Jul 2017, Toulouse, France. pp.5023-5028, 10.1016/j.ifacol.2017.08.911 . hal-02004402

HAL Id: hal-02004402
https://hal.science/hal-02004402

Submitted on 16 Apr 2019

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.

Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 50-1 (2017) 5023–5028

Solving Diagnosability of Hybrid Systems via Abstraction and Discrete Event Techniques

Alban Grastien * **Louise Travé-Massuyès** ** **Vicenç Puig** ***

* *Data61, Decision Science Program; and the ANU, Artificial Intelligence Group, (e-mail: alban.grastien@data61.csiro.au)*
** *LAAS-CNRS, Université de Toulouse, France, (e-mail: louise@laas.fr)*
*** *SAC Group, Universitat Politècnica de Catalunya,Barcelona,Spain, (e-mail: vicenc.puig@upc.edu)*

Abstract: This paper addresses the problem of determining the diagnosability of hybrid systems by abstracting hybrid models to a discrete event setting. From the continuous model the abstraction only remembers two pieces of information: indiscernability between modes (when they are guaranteed to generate different observations) and ephemerality (when the system cannot stay forever in a given set of modes). Then, we use standard discrete event system diagnosability algorithms. The second contribution is an iterative approach to diagnosability that starts from the most abstract discrete event model of the hybrid system. If it is diagnosable, that means that the hybrid system is diagnosable. If it is not, the counterexample generated by the diagnosability procedure is analysed to refine the DES. If no refinement is found, then it can not be proved that the hybrid system is diagnosable. Otherwise, the refinement is included in the abstract DES model and the diagnosability procedure continues.

© 2017, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved.

Keywords: Diagnosability, Hybrid systems, discrete event systems, Invariant sets.

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 observations of the system. Diagnosability has been studied for continuous systems and for discrete event systems (DES) separately. In case of continuous systems, it is formulated in terms of fault detectability and isolability from a structural point of view as in Blanke and Kinnaert (2016) or accounting for the characteristics of model uncertainties and noises impacting the system (Basseville et al., 2001). In the case of DES, the first diagnosability definition was proposed in Sampath et al. (1995) together with the necessary and sufficient conditions for diagnosability based on the Sampath's diagnoser, a finite state machine built from the system model. Diagnosability of hybrid systems was addressed later, benefiting from the works existing in both the continuous systems and the DES fields. Bayoudh and Travé-Massuyès (2014) exemplifies how these works can be merged for hybrid systems represented by hybrid automata. The discrete states of the hybrid automaton represent the operation modes of the system for which different continuous dynamics are specified via a set of differential equations involving continuous variables. 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, also known as *discernibility*. Different mode signatures are then translated into a set of so-called signature-events associated to mode transitions resulting in 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 in a discrete event framework. Other related works can be mentioned. For instance, the approach of Daigle et al. (2008) is similar to Bayoudh and Travé-Massuyès (2014) and Cocquempot et al. (2004) bases the analysis on continuous dynamics only and is hence limited to discernibility. Vento et al. (2015) extends the work of Bayoudh and Travé-Massuyès (2014) by proposing an incremental diagnosis framework in which discernibility remains implicit.

This paper addresses the problem of determining the diagnosability of hybrid systems with a different point of view. Instead of enriching the DES with full information arising from continuous dynamics (e.g. signature-events that require to determine all mode signatures as in Bayoudh and Travé-Massuyès (2014)), it proposes to abstract hybrid models to a discrete event setting and check diagnosability in an incremental way. The proposed approach starts by generating the most abstract DES model of the hybrid system and checking diagnosability of this DES model. If it is diagnosable, that means that the hybrid system is diagnosable. While if it is not, we search for a refinement that contradicts a counterexample generated by the diagnosability procedure. If no refinement is found, then it can not be proved that the hybrid system is diagnosable. Otherwise, the refinement is included in the abstract DES model and the diagnosability procedure continues. This approach uses just the necessary information about continuous dynamics, in an "on request" manner, hence potentially saving quite a lot of computation.

The structure of the paper is as follows: Section 2 presents the preliminaries regarding diagnosability. Section 3 describes the hybrid systems that we consider and the DES setting used for diagnosability. Section 4 shows how the hybrid system can be abstracted to a DES and the properties involved in their refinment. Section 5 presents how to test diagnosability of a hybrid system incrementally and illustrates the method with an application example presented in Section 6.

2405-8963 © 2017, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved.
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2017.08.911

2. PRELIMINARIES ON DIAGNOSABILITY

We start by providing a definition of diagnosability based on models. Next we quickly discuss how abstract models can be used to test diagnosability.

2.1 Model-Based Diagnosability

We call "model", hereafter denoted M, the implicit representation of a set of "system behaviours" (both faulty and nominal), where a system behaviour, denoted $\sigma \in M$, represents the evolution of the system state during a (finite or infinite) time window. The model is assumed to be prefix-closed (if a behaviour is possible, its prefixes are possible) and live (all behaviours have a future). We also assume a single fault, although the generalization to multiple fault is straightforward. We write $M[N]$ and $M[F]$ the subsets of nominal and faulty behaviours of M.

A model M is equipped with an observation function obs_M that indicates what can be observed when a specified behaviour takes place: $o \in obs_M(\sigma)$ is one of the possible system observations for the behaviour $\sigma \in M$. It is assumed that the observation function satisfies natural assumptions such as the fact that if σ' has a prefix σ, then every observation $o' \in obs_M(\sigma')$ has a prefix $o \in obs_M(\sigma)$. To simplify notations, we drop the references to the model and simply write $obs(\sigma)$ when not ambiguous.

Model-Based Diagnosis is the problem of deciding whether the observations generated by the system betray a nominal or a faulty behaviour. Specifically, given a model M, given an unknown behaviour $\hat{\sigma} \in M$, given the observation $\hat{o} \in obs(\hat{\sigma})$, the model-based diagnosis is defined as follows:

$$\Delta(\hat{o}) = \{\delta \in \{N,F\} \mid \exists \sigma \in M[\delta].\ \hat{o} \in obs(\sigma)\},$$

i.e., the hypotheses (N or F) for which there exists a behaviour consistent with the observations. Under the usual assumptions that the diagnosis model is complete (all possible system behaviours are in M and all possible observations of every behaviour σ are in $obs(\sigma)$) the diagnosis is guaranteed to be correct: $\hat{\delta} \in \Delta(\hat{o})$.

Diagnosability is the property that if a fault occurs on the system, then this fault will eventually be diagnosed. Because we limit ourselves to a single fault, this implies that the diagnosis will eventually be $\Delta = \{F\}$.

We use the notation $\sigma \sqsubseteq \sigma'$ to specify that σ is a prefix of σ', and $\sigma \sqsubseteq_d \sigma'$ to specify that the time window of σ' is at least d units of time longer than that of σ.

Definition 1. The model M is *diagnosable* if the following property holds:

$$\forall \sigma \in M[F].\ \exists d \in \mathbf{N}.\ \forall \sigma' \in M.\ \sigma \sqsubseteq_d \sigma' \Rightarrow \forall o' \in obs(\sigma').\ \Delta(o') = \{F\}.$$

In words, this definition states that for any faulty behaviour σ, after waiting for a sufficiently long time (d, leading to extended behaviour σ' and observation o'), the diagnosis is unambiguously F.

2.2 Abstraction and Diagnosability

Abstraction plays an important role in this work. The idea of abstraction is to remove some information included in the model in order to make the task of diagnosis, or diagnosability, computationally simpler or even decidable.

A model M' is an *abstraction* of M if the former allows for more behaviours than the latter:

$$M' \supseteq M \ \wedge\ (\forall \sigma \in M.\ obs_{M'}(\sigma) \supseteq obs_M(\sigma)).$$

M is then called a *refinement* of M'.

Abstraction can help prove diagnosability through the following lemma.

Lemma 1. Let M' be an abstraction of M. If M' is diagnosable, then M is also diagnosable.

This lemma can be easily proved by noting that the condition for diagnosability (Definition 1) is easier to satisfy for the refined models. Notice that Lemma 1 does not tell us much about diagnosability of M if M' is not diagnosable.

3. HYBRID SYSTEMS AND DES ABSTRACTION

We first introduce the definition of hybrid systems that we are considering in this paper. We then move to the discrete event model. We review some results about verifying diagnosability of DES. Finally, we show how the hybrid system can be abstracted to a DES.

3.1 Hybrid Systems

In this paper, we consider uncertain hybrid systems that can be represented by uncertain hybrid automata (Lunze and Lamnabhi-Lagarrigue, 2009) :

$$M = (Q, T, \zeta, C, (q_0, x_0)) \tag{1}$$

where:

- Q is the set of discrete system states, i.e. modes. Each state $q \in Q$, represents a mode of operation of the system.
- $T \subseteq Q \times Q$ is the set of *transitions*. A transition $t(q_i, q_j)$ may be guarded by a condition given as a set of equations $\mathscr{G}(t(q_i,q_j)) = g_{ij}(x, \theta_g) = 0$, θ_g being a constant parameter vector. The transition happens when the state $x(t)$ hits the guard g_{ij}. A reset map $\mathscr{R}_{ij}$, possibly equal to the identity, is specified.
- ζ is the set of continuous variables, functions of time t, including state, input, and output variables as defined below. Input/output variables form the set of observable, i.e. measured, continuous variables denoted by ζ_{OBS}.
- $C = \{C_q\}$ is the set of system constraints linking continuous variables in mode q:

$$\begin{cases} \dot{x}(t) = f_q(x(t,p), u(t), p) \\ y(t) = g_q(x(t,p), p) \\ x(t_0) = x_0 \end{cases} \qquad t_0 \le t \le T \tag{2}$$

  where :
  - $x(t) \in \mathbb{R}^{n_x}$, $u(t) \in \mathbb{R}^{n_u}$, and $y(t) \in \mathbb{R}^{n_y}$ denote the vectors of state, input, and output variable at time t, respectively,
  - the functions f_q and g_q are real and analytic on $D_x \subseteq \mathbb{R}^{n_x}$, where D_x is the definition domain of $x(t)$ such that $x(t) \in D_x$ for every $t \in [t_0,\ T]$ and T is a finite or infinite time bound,
  - $p \in P \subseteq \mathbb{R}^p$ is the vector of parameters and $x(t_0) = x_0 \in X_0 \subseteq \mathbb{R}^{n_x}$ is the initial continuous state.
- (Q_0, x_0) is the initial condition of the hybrid system, where $Q_0 \subseteq Q$ is the initial mode.

Transitions from one mode to another change the continuous dynamics driving the behavior of the system.

3.2 Discrete Event Systems

A DES is a discrete state, event driven system where the state evolution depends on the occurrence of asynchronous discrete events. For consistency with hybrid systems, these states are here referred to as "modes".

Compared to hybrid systems, DES have discrete observations. Contrary to the standard literature (Sampath et al. (1995); Lamperti and Zanella (2003); Pencolé and Cordier (2005)) we assume that the observations are state-based, but this choice is purely for convenience: there is no fundamental difference between state-based and event-based observations. We assume a constant set I of *indicators* which are observable properties about the current system mode—when the property holds in the mode, we say that the indicator is satisfied. In a given mode, an indicator could be always satisfied, never satisfied, or sometimes satisfied.

Definition 2. A *discrete event system* is a tuple $D = \langle Q, T, q_o, L, Eph\rangle$ where Q is a set of *modes* with $q_o \in Q$ the *initial mode*, $T \subseteq Q \times Q$ is the set of *transitions*, $L : Q \times I \to \{0, 1, -1\}$ is the *indicator function*, and $Eph \subseteq 2^Q$ is a collection of *ephemeral sets*.

A behaviour on the DES is a sequence of modes $q_0 \to \ldots \to q_k$ such that $q_0 = q_o$ and all $\langle q_{i-1}, q_i\rangle$ are transitions. For every mode $q \in Q$ and every indicator $indi \in I$, $L(q, indi) = 1$ (resp. $L(q, indi) = -1$) specifies that the indicator is always (resp. never) satisfied in this mode. We define $I^{>0}(q) = \{indi \in I \mid L(q, indi) > 0\}$ as the list of indicators that are always satisfied in mode q and $I^{\geq 0}(q) = \{indi \in I \mid L(q, indi) \geq 0\}$ the list of indicators that are always or sometimes satisfied. Then an observation θ in mode q is the list of indicators satisfied in this mode and is such that:

$$I^{>0}(q) \subseteq \theta \subseteq I^{\geq 0}(q).$$

Notice that at different times the observation of the same mode may vary (but it always satisfies the subset constraint above). An observation of $q_0 \to \ldots \to q_k$ is then a sequence $o = \theta_0, \ldots, \theta_k$ where each θ_i is an observation of q_i.

We now explain the last parameter of the DES definition. A DES is event driven, meaning that the mode of the system may remain the same over time. This is allowed via an explicit transition $\langle q, q\rangle \in T$ for all $q \in Q$. There are however modes in which one cannot stay forever. For example, in a situation where a container is being filled at a non-trivial rate, the system mode will eventually change (as e.g. the container will become full, or it will start leaking). We model this with a notion of *ephemerality*. Formally for any infinite sequence $q_0 \to q_1 \to \ldots$ let us denote Q_∞ the set of modes that appear infinitely often; then this set of modes cannot appear in Eph:

$$Q_\infty \notin Eph.$$

This property is similar to that of *fairness* frequently used in model checking but also in diagnosis (Biswas et al., 2010).

3.3 Diagnosability of DES

Diagnosability of DES is a well-studied problem. It was introduced by Sampath et al. (1995) and polynomial algorithms were developed in parallel by Yoo and Lafortune (2002) and Jiang et al. (2001). These papers assume event-based observations, but state-based observations can be considered too. Similarly it is possible to include fairness conditions (Grastien, 2009).

The standard way to solve diagnosability of DES is to search for two infinite behaviours in the model, a faulty one and a nominal one, and that are observation-similar. This search is implemented by constructing the twin plant (defined below) and searching for reachable fair cycles, i.e., cycles that do not remain in ephemeral sets of modes. We assume that the modes are partitioned into nominal modes Q_N and faulty modes Q_F (when faults are defined as events, we assume that every mode remembers whether a faulty event occurred).

Definition 3. Given the DES $D = \langle Q, T, q_o, L, Eph\rangle$ the *twin plant* is the state machine $\langle \mathfrak{Q}, \mathfrak{T}, \mathfrak{q}_o, \mathfrak{E}\rangle$ where:

- $\mathfrak{Q} = \{\langle q_1, q_2\rangle \in Q \times Q \mid \forall indi \in I \{L(q_1, indi), L(q_2, indi)\} \neq \{-1, 1\}\}$,
- $\mathfrak{T} = \{\langle\langle q_1, q_2\rangle, \langle q_1', q_2'\rangle\rangle \in \mathfrak{Q} \times \mathfrak{Q} \mid \langle q_1, q_1'\rangle \in T \wedge \langle q_2, q_2'\rangle \in T\}$,
- $\mathfrak{q}_o = \langle q_o, q_o\rangle$, and
- $\mathfrak{E} = \{\mathfrak{Q}' \subseteq \mathfrak{Q} \mid \exists X \in Eph \text{ where } X = \{q \mid \langle q, q'\rangle \in \mathfrak{Q}'\}\}$.

The first item in Definition 3 simply indicates that the twin plant only includes states $\mathfrak{q} = \langle q_1, q_2\rangle$ such that the two modes q_1 and q_2 do not disagree on any indicator. Indeed if $\{L(q_1, indi), L(q_2, indi)\} = \{-1, 1\}$ then the indicator is always satisfied in one mode and always unsatisfied in the other mode.

Note that the indicators do not appear in the twin plant as they are only relevant to define its states $\mathfrak{Q}$. Notice also that the ephemerality relation on the twin plant is defined only on the first element of the twin plant: a set of states $\mathfrak{Q}'$ of the twin plant is ephemeral iff the set X of modes that are mentioned in the states of $\mathfrak{Q}'$ (as first element of the pair) is ephemeral. Accordingly given a cycle $\mathfrak{q}_1 \to \ldots \to \mathfrak{q}_i$ (i.e., such that $\mathfrak{q}_1 = \mathfrak{q}_i$), we say that this cycle is *fair* iff $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_i\} \notin \mathfrak{E}$.

Proposition 1. (Grastien (2009)) Let $\mathfrak{A} = (Q_F \times Q_N) \cap \mathfrak{Q}$ be the set of *ambiguous states* of the twin plant. The DES is diagnosable iff the twin plant does not contain any fair cycle of ambiguous states that can be reached from its initial state.

The cycle $\mathfrak{c} = \mathfrak{q}_1 \to \ldots \to \mathfrak{q}_j$ mentioned in Proposition 1 (where $\mathfrak{q}_i = \langle q_i, q_i'\rangle$ for each index i) is called the *counterexample*. It represents a possible faulty system behaviour (namely $q_1 \to q_2 \to \ldots$) that can be mistaken for a nominal behaviour (namely $q_1' \to q_2' \to \ldots$). We write $\mathfrak{Q}^\infty(c)$ the list of (twin plant) states that appear in the cycle.

4. DIAGNOSABILITY OF HYBRID SYSTEMS WITH DES METHODS

In this section we reduce the problem of diagnosability of hybrid systems to the problem of diagnosability of DES. To this end we define D_M^∞, a DES abstraction of the hybrid system M. All the continuous dynamics of the hybrid system are embedded in the indicators (cf. Section 4.1) and ephemerality (cf. Section 4.2) relations of the DES. Then from Lemma 1 diagnosability of D_M^∞ implies diagnosability of the hybrid system. Again, nondiagnosability of D_M^∞ leaves open the question of diagnosability of the hybrid system.

4.1 Residuals, discernibility and the indicator function

Discernibility of a pair of modes can be verified from the *residuals* attached to the modes (Bayoudh and Travé-Massuyès (2014) Vento et al. (2015)). Residuals are consistency indicators used by the FDI community to check the measurements against

the continuous dynamics of every mode. There are several approaches for obtaining residual generators (Blanke and Kinnaert, 2016) (as e.g., using structural methods, or decoupling unknown variables), all of them based on the elimination of the unknown variables $x(t)$. The elimination process produces testable relations that only depend on variables that can be determined from measured variables, i.e. input and output variables $u(t)$ and $y(t)$ and their derivatives up to some order n gathered in the vectors $\bar{y}^{(n)}(t)$ and $\bar{y}^{(n)}(t)$. Thus, in the ideal case (no noise and uncertainty) [1], as long as the hybrid system is actually in mode q and there is no fault, the residual $r(\bar{y}^{(n)}(t), \bar{u}^{(n)}(t))$ (in vector form) satisfies

$$r(\bar{y}^{(n)}(t), \bar{u}^{(n)}(t)) = 0 \tag{3}$$

Otherwise, the residual $r(\bar{y}^{(n)}(t), \bar{u}^{(n)}(t))$ (or r for short) is different from zero indicating that measurements are inconsistent with the continuous dynamics of mode q.

In this paper, discernibility is not explicit. It is represented in the first item of Definition 3 of the twin plant. But the set of indicators I is built from the residuals generated for every mode. An indicator $indi \in I$ is associated to the residual vectors obtained for every mode. Denote by r_q the residual vector for mode q. Then, from the properties of residuals, we have:

- $L(q, indi) = 1$ because r_q evaluates to zero when the system is in mode q (unknown faults are not considered in this paper),
- $L(q', indi) = 1$ when r_q also evaluates to zero in $q' \neq q$,
- $L(q', indi) = -1$ when r_q never evaluates to zero in q',
- $L(q', indi) = 0$ when r_q sometimes evaluates to zero in q'.

4.2 Checking ephemerality

Ephemerality is a notion that, as far as we are aware, has never been introduced before. Ephemerality means that the system cannot stay forever in a given set of modes. We believe that ephemerality is a problem that will require further investigation, but we propose two methods to check it:

- by running a hybrid *reachability* procedure from all possible initial states. This method is applicable to a set of modes,
- by computing the *positive invariant set*, i.e. the attractor state region where the continuous dynamics drive the state and where the state stays forever. As far as we know, this method is applicable to one mode only.

The advantage of the invariant set theory is that it provides the theoretical attractor set. However it only gives "static" information, i.e. we know that the system converges towards this set. On the contrary, reachability analysis provides the atteignable set during transient behavior but it requires a sufficiently long run (whose minimal temporal bound is unknown) to obtain the invariant set.

Ephemerality via reachability – In this paper, we are concerned by – possibly nonlinear – uncertain hybrid systems as given by (1). For these systems, continuous dynamics, guard sets and reset functions are defined by nonlinear functions and all uncertainties are considered bounded. At some instant t, the hybrid state $(Q_t, x(t))$ is uncertain, which means that Q_t and $x(t)$ are set-valued, i.e. $Q_t \subseteq Q$ and $x(t) = x_t \subseteq \mathbb{R}^{n_x}$. Q_t is the set of "active" modes at time t, i.e. the modes in which the system may operate at t, and x_t is the set of possible states at t given an uncertain initial hybrid state at time t_0. In a given mode, the continuous state trajectory takes the form of a "flow-pipe" which defines the bounds of the continuous state in time. When a flow-pipe of non-zero size reaches a mode guard condition, there is a non-empty set of instants during which the constraints are satisfied, leading to a continuum of switching times.

Running a hybrid reachability procedure for a set of modes $Q^* \subseteq Q$ permits to envision all the hybrid states reachable by the hybrid system from the initial hybrid state $(Q_0, x_0) = (Q^*, X^*)$, where X^* is the set of possible continuous states associated to Q^*. This can obviously be used to assess that the system cannot stay forever in Q^*, proving ephemerality [2]. Several methods have been developed recently for the explicit computation of reachable sets. In this paper, we have used the method and associated software presented in Maïga et al. (2016) that can be decomposed in three algorithmic steps: 1) compute the reachable set, 2) compute the discrete transitions, and 3) enclose the multiple trajectories resulting from an uncertain transition.

Ephemerality via set-invariance – Another way of checking ephemerality is based on the use of set-invariance based on the positive invariant set concept (Seron et al. (2012); Blanchini (1999)). The computation of these sets can be performed beforehand and depends on known system's dynamics and bounds on input signals and disturbances/uncertainties.

Definition 4. The set $\mathscr{S} \subset \mathbb{R}^n$ is said to be *positively invariant* w.r.t. the continuous dynamics of a mode q of the hybrid system (2) if every solution trajectory $x(t)$ with initial condition $x(0) \in \mathscr{S}$ is globally defined and such that $x(t) \in \mathscr{S}$ for $t > 0$.

The application of the set-invariance approach to prove that one mode q is ephemeral comes back to check whether all the states in the minimal robust positive invariance (mRPI) set of a mode satisfy the guard [3]. If ephemerality must be proved for a set of modes, reachability analysis is preferred.

5. INCREMENTAL DIAGNOSABILITY

5.1 Introduction

Computing precisely D_M^∞ can be very expensive, and we also want to identify which indicators are useful in ensuring diagnosability. For this reason we show how to test diagnosability incrementally, i.e. by starting with abstract L and Eph parameters and incrementally refining them until diagnosability has been shown, or an irrefutable counterexample is produced.

5.2 Description of the Approach

Our approach is summarized in Algorithm 1. We start with a hybrid system model M. From this model we generate the most abstract DES model D_M^0. We check diagnosability of the current abstract model. If it is diagnosable, then we found an abstraction that allows us to diagnose precisely the system.

[1] In case of noise or uncertainty the residual consistency is checked with statistical or set-membership methods Blanke and Kinnaert (2016)

[2] Note that reachability analysis can also be used to check discernibility. Indeed, if reachability analysis is run for two modes starting with all their possible initial continuous states, if the flow-pipes separate at some point in time, it means that these modes are discernible.

[3] Set-invariance can also be used to check discernibility. Indeed, two modes that have mRPI sets that do not intersect are discernible.

Algorithm 1 Incremental Diagnosability

Input: hybrid system model M
$A := D^0_M$
Repeat
  if A is diagnosable (using the Twin Plant method and Lemma 1)
    return diagnosable (with abstraction A)
  let c be a counterexample for A
  if there is a refinement of A that contradicts c
    apply refinement to A
  else
    return could not prove diagnosability

If the current model is not diagnosable, then we analyse the counterexample generated by the diagnosability procedure and search for a refinement of L or *Eph* that contradicts the counterexample. If no refinement is found, then we cannot prove that the system is diagnosable. If a refinement is found, then it is included to the abstract model and we test diagnosability of this new model again. Given that the amount of information in D^∞_M is finite it is easy to demonstrate the following theorem.

Theorem 2. If D^∞_M is diagnosable and the search for refinements contradicting counterexamples is complete, then Algorithm 1 always returns an abstraction of D^∞_M that is diagnosable.

6. APPLICATION EXAMPLE

To illustrate the proposed approach, consider the model of a heating system of Figure 1. The system starts in mode $N1$ and navigates between $N1$, $N2$, and $N3$. The value of state variable x representing temperature increases in $N1$ and $N2$, albeit at a different speed, and decreases in $N3$. Notice that the system can transition freely between $N1$ and $N2$ but it has to transition to $N3$ if the temperature becomes greater to 80. A fault leads to a similar situation where the increase/decrease in the state are modified and the models become uncertain. Observations y are the state x and its derivative $\dot{x} = \dot{y}$.

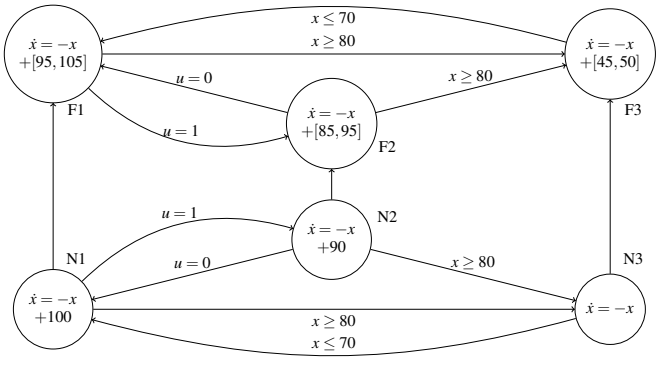

Fig. 1. The System Model

Residuals (cf. Section 4.1) are equations involving observable quantities that evaluate to zero in some modes. A set of primary residuals for this model can be generated as follows:

$$\begin{array}{ll} r_{N1} = \dot{y} + y - 100 & r_{F1} = \dot{y} + y - [95,105] \\ r_{N2} = \dot{y} + y - 90 & r_{F2} = \dot{y} + y - [85,95] \\ r_{N3} = \dot{y} + y & r_{F3} = \dot{y} + y - [45,50] \end{array} \quad (4)$$

From these residuals, the set I of indicators introduced in Definition 2 can be obtained as explained in Section 4.1. Taking into account the dynamic models associated to the modes of the hybrid system of Figure 1, the corresponding invariance sets can be computed as follows:

$$\begin{array}{ll} \mathscr{S}_{N1} = 100 & \mathscr{S}_{F1} = [95,105] \\ \mathscr{S}_{N2} = 90 & \mathscr{S}_{F2} = [85,95] \\ \mathscr{S}_{N3} = 1 & \mathscr{S}_{F3} = [45,50] \end{array} \quad (5)$$

Analyzing the position of these invariant sets with respect to the mode's guards, we can assess ephemerability. Moreover, these invariant sets can also be used to evaluate the residuals associated to the set I of indicators that allow distinguishing in which mode q the hybrid system is operating. In particular, as e.g., residual r_{N1} is zero and consequently the associated indicator is $I_{N1} = 1$ when the system reaches the invariant set $\mathscr{S}_{N1}$ according to Section 4.1. A similar reasoning applies for residuals r_{N2} and r_{N2}. In case of residuals r_{F1} to r_{F3}, they do not evaluate to zero even if the hybrid system is in some of the associated modes F_1 and F_2 because of model uncertainty, being the corresponding indicator $I_{N1} = -1$. Thus, invariant sets can be used in an analogous manner as residuals to generate the indicators I introduced in Section 4.1. The diagnosability procedure includes two components: a "discrete component", which generates "counterexamples" (that negate diagnosability) and a "continuous component", which tries to invalidate the counterexamples. The algorithm starts with an abstraction of the model where all the continuous aspects are ignored (loops are added on each mode). Each call to the continuous component refines the model. Here is part of the execution of the procedure on this example:

[CE1] The discrete component computes the following counterexample: if the system takes the following infinite faulty behaviour $\sigma_f = N1 \to F1\ (\to F1)^\infty$, this behaviour cannot be distinguished from $\sigma_N = N1 \to N1\ (\to N1)^\infty$.

This counterexample can be eliminated if we demonstrate that the infinite faulty behaviour is impossible (ephemerality, i.e., if the system cannot stay in mode $F1$ forever) or that the two behaviours can be distinguished (i.e., if $N1$ can always be distinguished from $F1$). In this instance we see that $\{F1\}$ is ephemeral. Proof of ephemerality is simply obtained from the invariant set of F_1: $\mathscr{S}_{F1} = [95,105]$. For F_1, all the possible continuous state initial conditions are $x_0 = [0,80[$, hence the system must cross the guard $x \ge 80$ to converge to the invariant set. The same result can be obtained by running hybrid reachability starting with $x_0 = [0,80[$ as shown on Fig. 2.

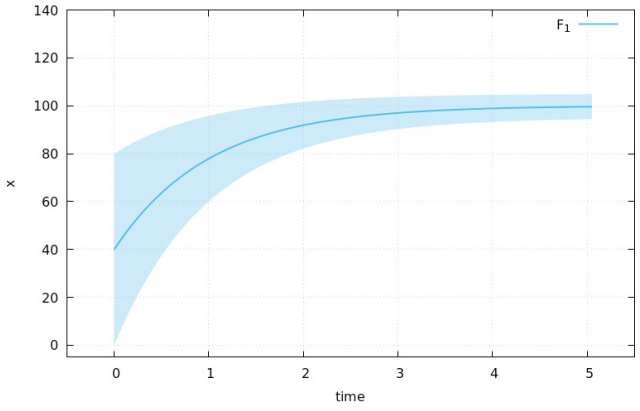

Fig. 2. Reachability analysis for F1 starting with all possible initial states $x_0 = [0,80[$

[CE2] Now the discrete component is not allowed to generate a counterexample with a faulty loop that contains only $F1$

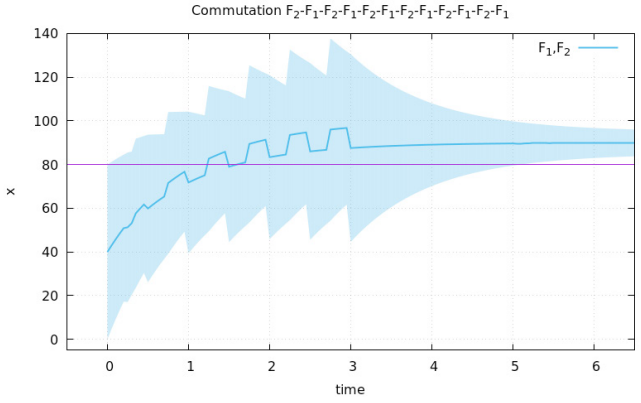

Fig. 3. Reachability analysis for the set of modes {F1, F2} starting with all possible initial states $x_0 = [0, 80[$ and 11 transitions

or only $F2$, but the faulty loop may consists in $\{F1, F2\}$. New counterexample:

- $\sigma_f = N1 \rightarrow F1 \rightarrow F2\ (\rightarrow F1 \rightarrow F2)^\infty$,
- $\sigma_N = N1 \rightarrow N1 \rightarrow N1\ (\rightarrow N1 \rightarrow N1)^\infty$.

But $\{F1, F2\}$ is ephemeral. For a set of modes, proof of ephemerality is obtained by hybrid reachability. Possible initial states are $([0, 80[, F_1)$ and $([0, 80[, F_2)$. For any transition sequence triggered by $u(t)$, the system behavior converges towards the invariant set of the last mode. Fig. 3 shows an 11 transitions scenario ending with mode F_2.

[CE3] New counterexample:

- $\sigma_f = N1 \rightarrow F1 \rightarrow F2 \rightarrow F3\ (\rightarrow F1 \rightarrow F2 \rightarrow F3)^\infty$,
- $\sigma_N = N1 \rightarrow N1 \rightarrow N1 \rightarrow N1\ (\rightarrow N1 \rightarrow N1 \rightarrow N1)^\infty$.

Ephemerality does not allow to reject this counterexample. Therefore, we need to check whether $N1$ can always be distinguished from $F1$, whether $N1$ can always be distinguished from $F2$, and whether $N1$ can always be distinguished from $F3$. According to Equation (5), $F2$ and $F3$ can be distinguished from $N1$ since the corresponding invariant sets do not intersect, but not $F1$ because in this case the intersection is not empty. This means that the residuals r_{F2} and r_{F3} can be used for distinguishing from $N1$. But this is not the case of residual r_{F1}.

[CE4] We generate a new counterexample that cannot have the faulty behaviour in mode $F2$ while the nominal behaviour is in mode $N1$:

- $\sigma_f = N1 \rightarrow F1 \rightarrow F2 \rightarrow F3\ (\rightarrow F1 \rightarrow F2 \rightarrow F3)^\infty$,
- $\sigma_N = N1 \rightarrow N1 \rightarrow N2 \rightarrow N1\ (\rightarrow N1 \rightarrow N2 \rightarrow N1)^\infty$.

But $F3$ can be distinguished from $N1$ because the corresponding invariant sets do not intersect according to (5), or equivalently, the residuals r_{F3} and r_{N1} can be used for distinguishing between these two modes. The diagnosability algorithm continues and eventually fails at producing a counterexample, meaning that the system is diagnosable. By analysing this diagnosability proof, we notice that we need to distinguish the following pairs of modes: $(F3, N1)$, $(F3, N2)$, $(F3, N3)$, and $(F2, N1)$. However, we do not need any other distinguishability check. For instance, we do not need to distinguish $N1$ from $N2$.

7. CONCLUSIONS

This paper has addressed the problem of determining the diagnosability of hybrid systems by abstracting hybrid models to a discrete event setting. The abstracted model only remembers two pieces of information: distinguishability between modes (when they are guaranteed to generate different observations) and ephemerality (when the system cannot stay forever in a given set of modes). Then, standard DES diagnosability algorithms are applied to the abstracted model. An iterative approach to diagnosability is proposed that starts with the most abstract DES model and iteratively calls for refinements until diagnosability is proved or there are no more refinements available. The proposed approach has been illustrated with an academic example that clearly shows how the different techniques used interplay.

REFERENCES

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

Bayoudh, M. and Travé-Massuyès, L. (2014). Diagnosability analysis of hybrid systems cast in a discrete-event framework. *Discrete Event Dynamic Systems*, 24(3), 309–338.

Biswas, S., Sarkar, D., Mukhopadhyay, S., and Patra, A. (2010). Fairness of transitions in diagnosability of discrete event systems. *Journal of Discrete Event Dynamical Systems (JDEDS)*, 20, 349–376.

Blanchini, F. (1999). Set invariance in control. *Automatica*, 35(11), 1747 – 1767.

Blanke, M. and Kinnaert, M. (2016). *Diagnosis and Fault-tolerant control*. Springer.

Cocquempot, V., Mezyani, T., and Staroswiecki M, M. (2004). Fault detection and isolation for hybrid systems using structured parity residuals. In *Asian Control Conference*, 1204–1212.

Daigle, M., Koutsoukos, X., and Biswas, G. (2008). An event-based approach to hybrid systems diagnosability. In *Nineteenth International Workshop on Principles of Diagnosis (DX-08)*, 47–54.

Grastien, A. (2009). Symbolic testing of diagnosability. In *20th International Workshop on Principles of Diagnosis (DX-09)*, 131–138.

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

Lamperti, G. and Zanella, M. (2003). *Diagnosis of active systems*. Kluwer Academic Publishers.

Lunze, J. and Lamnabhi-Lagarrigue, F. (eds.) (2009). *Handbook of Hybrid Systems Control : Theory, Tools, Applications*. Cambridge University Press, Cambridge, UK, New York.

Maïga, M., Ramdani, N., Travé-Massuyès, L., and Combastel, C. (2016). A comprehensive method for reachability analysis of uncertain nonlinear hybrid systems. *Automatic Control, IEEE Transactions on*. doi: 10.1109/TAC.2015.2491740.

Pencolé, Y. and Cordier, M.O. (2005). A formal framework for the decentralised diagnosis of large scale discrete event systems and its application to telecommunication networks. *Artificial Intelligence (AIJ)*, 164(1–2), 121–170.

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., and Teneketzis, D. (1995). Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control (TAC)*, 40(9), 1555–1575.

Seron, M.M., Dona, J.A.D., and Olaru, S. (2012). Fault tolerant control allowing sensor healthy-to-faulty and faulty-to-healthy transitions. *IEEE Transactions on Automatic Control*, 57(7), 1657–1669.

Vento, J., Travé-Massuyès, L., Puig, V., and Sarrate, R. (2015). An incremental hybrid system diagnoser automaton enhanced by discrenibility properties. *IEEE Transactions on Systems, Man, and Cybernetics (TSMC)*, 45(5), 788–804.

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