Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics
San Antonio, TX, USA - October 2009

# Diagnosis of Hybrid Systems: Part 1- Diagnosability

R. Mohammadi, S. Hashtrudi-Zad and K. Khorasani
Department of Electrical and Computer Engineering,
Concordia University
Montréal, QC, Canada, H3G 1M8
E-mail: a_mohamm,shz,kash@ece.concordia.ca

***Abstract*—In this paper, we investigate fault diagnosis and diagnosability in hybrid systems modeled by hybrid automata. Generally, in hybrid systems, there are discrete sensors generating discrete outputs available at the discrete-event system representation of the system and continuous sensors generating continuous outputs available at the continuous dynamics. We assume that there is a bank of residual generators (using continuous sensors) designed for the continuous dynamics of the system. We present a hybrid diagnosis approach in which faults are diagnosed by integrating the information generated by the residual generators and the information at the discrete-event system representation of the system. We investigate the diagnosability of faults in the hybrid diagnosis framework.**

***Index Terms*—Fault diagnosis, hybrid systems, finite-state automata, diagnosability.**

## I. INTRODUCTION

Fault diagnosis based on discrete event or continuous dynamics models have been studied extensively in the literature. For example, one may refer to the diagnosis approaches based on the Finite-State Automata (FSA) models [3], [10] in the Discrete-Event System (DES) literature, and diagnosis approaches based on analytical redundancy (refer to survey [2] and the references therein) in the continuous-variable literature.

Fault diagnosis in hybrid systems has been a subject of research. A number of diagnosis approaches have been developed for hybrid systems that are mostly based on discrete and/or temporal abstractions of continuous dynamics. (See for example, [6], [9] and [12].) Diagnosability of faults in hybrid systems has also been investigated in the literature. However, little work is available. In [11], diagnosability in hybrid systems is studied using a timed automaton abstraction of the hybrid system.

In general, there are two types of sensors in a hybrid system, namely, discrete sensors that generate discrete outputs such as level sensors used for measuring different levels of a liquid in a tank, and continuous sensors that generate continuous outputs such as a sensor continuously measuring the temperature of a room. In [7], we developed a hybrid automaton model for a gas turbine engine and studied fault diagnosis in the engine. We showed that there are cases in which some faults are not diagnosable either by using DES model (information provided by discrete sensors) alone or by using the continuous methods based on residual generation (using continuous sensors) alone. However, these faults can be diagnosed if the information provided by the residual generators are integrated with the output of the discrete sensors. In [7], we developed a systematic method for constructing an *extended DES model* containing the information at the DES level of the engine as well as the diagnosis information provided by the residual generators. Based on the extended DES model, we constructed a hybrid diagnoser for the engine.

In this paper, we review our hybrid diagnosis method and investigate the diagnosability of failure modes in our framework. We introduce a notion of diagnosability in hybrid automata and show that a failure mode is diagnosable in a hybrid automaton if it is diagnosable in the extended DES model. In [8], we study the problem of residual generator selection in hybrid automata. We also investigate fault diagnosis for the cases that some residual generators generate incorrect output.

Since residual generators in our work use all the information available about the continuous dynamics of the system and the outputs of continuous sensors, we do not lose a major amount of information available at the continuous level due to the abstraction. Our hybrid diagnosis approach produces a less conservative diagnosis and therefore, it can detect and isolate faults faster compared with the diagnosis approaches in the literature that are based on abstracted models.

The remainder of the paper is organized as follows. In Sec. II, the motivation of our hybrid diagnosis approach is demonstrated by an example. In Sec. III, the modeling of hybrid automata that are subject to faults is described. In Sec. IV, our diagnosis approach in hybrid automata is reviewed. Diagnosability in our framework is discussed in Sec. V. We present the conclusions and the planed future work in Sec. VI.

## II. MOTIVATION

Consider the system in Fig. 1. The system consists of a single-spool gas turbine engine and its fuel supply system and nozzle actuator. Here, we briefly describe the system. The details of modeling and fault diagnosis in the gas turbine engine is provided in [7]. The air is taken to the engine through the intake duct and compressed with the compressor. Then, fuel is added to the air, and the mixture is burned in the combustion chamber. The high-pressure and high-temperature

This work is supported in part by a Strategic Projects grant from the Natural Sciences and Engineering Research Council of Canada (NSERC).



978-1-4244-2794-9/09/$25.00 ©2009 IEEE

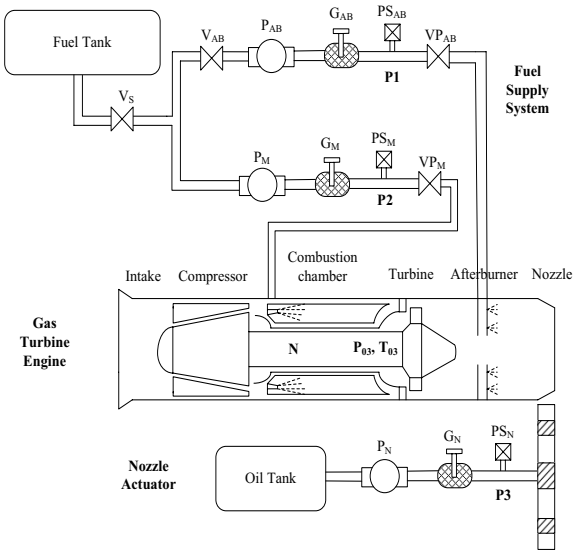



Fig. 1. A gas turbine engine and its fuel supply system and nozzle actuator.

gases turn the turbine. Then the gases are reheated using the afterburner and expanded through the nozzle to produce thrust. The fuel supply system has two branches: one controlling the fuel mass flow rate entering the combustion chamber and the other controlling the fuel entering the afterburner. The pumps $P_M$ and $P_{AB}$ are in charge of pumping the fuel to the engine. The governors $G_M$ and $G_{AB}$ are servo-valves that control the mass flow rate of the fuel passing through them. The valves $V_S$ and $V_{AB}$ are solenoid shut-off valves. The pressurizing valves $VP_M$ and $VP_{AB}$ ensure that the fuel entering the engine has a high pressure for efficient atomization. The area of the nozzle is variable and changes with a hydraulic actuator consisting of the pump $P_N$ and the governor $G_N$. There are three discrete sensors $PS_{AB}$, $PS_M$ and $PS_N$ installed in the fuel supply system and the nozzle actuator, generating "low" and "high" measurements for pressures at $P_1$, $P_2$ and $P_3$. Continuous sensors are installed in the engine to measure the turbine inlet temperature $T_{03}$, the turbine inlet pressure $p_{03}$ and the shaft speed $N$. It can be verified that the effects of the afterburner fuel mass flow rate and the nozzle area on the continuous sensors are similar. Therefore, the failure modes in the components of the afterburner fuel supply system cannot be distinguished from the failure modes in the nozzle actuator using the readings of the continuous sensors only. Moreover, discrete sensors cannot sense the small deterioration of the components. For example, consider the faults "small loss-of-effectiveness of $G_M$" and "stuck-closed of $V_S$". Suppose a small loss-of-effectiveness fault in $G_M$ occurs. This fault cannot be detected using discrete sensors alone. Also, it can be verified that using residual generators, this fault cannot be distinguished from stuck-closed in $V_S$. However, integrating the information coming from the discrete sensors and the information provided by the residual generators, the fault in $G_M$ can be isolated.

This example demonstrates the advantages of integrating the information at the DES level and the readings of the continuous sensors for fault diagnosis.

## III. MODELING OF HYBRID AUTOMATA

First, a formal definition of hybrid automata in our work which is a modified form of the definition in [4] is presented.

*Definition 1:* A **hybrid automaton** is defined to be a 14-tuple $H = (Q, \mathcal{X}, \mathcal{U}, \mathcal{Y}, FT, Init, S, \Sigma, T, G, \rho, D, \lambda, q_0)$, where $Q$ is the set of finite discrete states; $\mathcal{X} \subseteq \mathbb{R}^n$, $\mathcal{U} \subseteq \mathbb{R}^p$ and $\mathcal{Y} \subseteq \mathbb{R}^r$ are vector spaces of continuous state, control input and output, respectively; $FT$ is the set of $m$ fault types $f^1, \cdots, f^m$ with $f^i(t) \in \mathbb{R}$ for $1 \leq i \leq m$; $Init \subseteq \mathcal{X}$ is the set of initial continuous states; $S = \{S_q \mid q \in Q\}$ is the set of dynamic models defining the continuous dynamics of the system; $\Sigma$ is a set of symbols representing the discrete events labeling the transitions among discrete states; $T \subseteq Q \times \Sigma \times Q$ is the set of discrete transitions; $G : T \times \mathcal{X} \times \mathcal{U} \longrightarrow \{True, False\}$ is the set of guard conditions; $\rho : T \times \mathcal{X} \longrightarrow \mathcal{X}$ is a reset map; $D$ is the set of discrete output symbols; $\lambda : Q \longrightarrow D$ is the discrete output map and $q_0$ is the initial discrete state. ■

In the above definition of hybrid automata, a discrete event is associated with any transition between two discrete states. It can be seen from Def. 1 that the tuple $(Q, \Sigma, T, D, \lambda, q_0)$ defines a Moore FSA representing a DES level abstraction of the system. We denote this tuple by $H_{abs}$ and refer to it as the **DES abstraction** of $H$. We assume that $\Sigma = \Sigma_o \dot{\bigcup} \Sigma_{uo}$, where $\Sigma_o$ represents the observable event set and $\Sigma_{uo}$ consists of unobservable events. In the following, we explain fault modeling of hybrid automata.

In this work, we assume that the dynamics of the system at each discrete state can be represented by $S_q := \begin{cases} \dot{x} = E_q(x,u) + G_q(f) \\ y = M_q(x,u) \end{cases}$, where $E_q$ and $M_q$ define the state flow and the output map of the continuous dynamics at $q$, respectively, and $f$ is a subset of fault types present in the system. Two discrete states $q_1$ and $q_2$ are called **EM-similar** if $E_{q_1}(x,u) = E_{q_2}(x,u)$ and $M_{q_1}(x,u) = M_{q_2}(x,u)$ (for every $x$, $u$). Assume that there are $d$ distinct pairs $(E, M)$ for the continuous dynamics of the system. The discrete state set of the system can be partitioned based on the $(E, M)$ pairs: $Q = Q^{EM_1} \dot{\bigcup} \cdots \dot{\bigcup} Q^{EM_d}$.

The system can be in the normal mode of operation or in a failure mode corresponding to a fault. In our work, faults are represented by **fault types**. Each fault type corresponds to one or more **failure modes** in a component of the system. Initially, the system is in the normal mode of operation and fault types have zero values. When a fault occurs in the system, the value of the corresponding fault type becomes nonzero and the system enters the failure mode corresponding to that fault. A fault type $f$ is called **active** in a discrete state $q$ if $f(t)$ is nonzero in $q$ for all the times that the system is in $q$. For example, consider a solenoid valve, where the flow rate passing through the valve, $x$ is related to the input voltage $u$ by a dynamical relation. The valve has three failure modes:

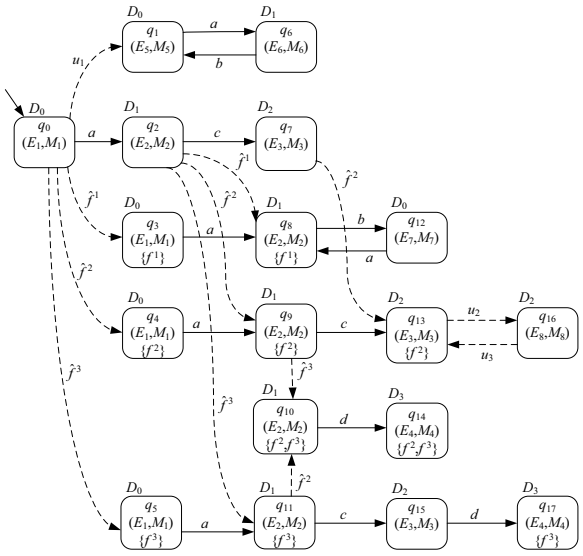



Fig. 2. The DES abstraction of a hybrid automaton with three failure modes.

stuck-closed, stuck-open and a 10% loss-of-effectiveness. The failure modes in the valve can be represented by an additive fault type $f_v(t)$. Each failure mode can be specified with a specific function assigned to $f_v$. For instance, the stuck-closed fault can be specified by $f_v = -u$, the stuck-open fault can be specified by $f_v = u_{max} - u$, where $u_{max}$ is the maximum magnitude of the input, and a 10% loss-of-effectiveness fault can be represented by $f_v = -0.1u$.

Assume that there are $\hat{m}$ ($\hat{m} \geq m$) failure modes corresponding to the $m$ fault types of the system. Let $F^j$ be a failure mode corresponding to the fault type $f^i$ ($1 \leq i \leq m\}$). We say $F^j$ occurs at time $t_0$ if $f^i(t) = 0$ for $t < t_0$ and for $t \geq t_0$, $f^i(t)$ takes values corresponding to $F^j$. The occurrence of a failure mode $F^j$ is modeled by an unobservable **fault event** denoted by $\hat{f}^j$ at the DES level. Fig. 2 shows the DES abstraction of a hybrid automaton $H$ with three fault types $f^1$, $f^2$ and $f^3$ and the corresponding failure modes $F^1$, $F^2$ and $F^3$, respectively. The occurrence of the failure modes $F^1$, $F^2$ and $F^3$ are modeled by the events $\hat{f}^1$, $\hat{f}^2$ and $\hat{f}^3$, respectively. Unobservable events are shown by dashed lines.

In this work, we assume that faults are **permanent**. It should be noted that fault types are not necessarily active in all the discrete states of their corresponding failure mode. For example, $f^1$ is not active in $q_{12}$. This typically happens when the system is in a mode of operation in which a faulty component is not used or is off.

Let $\mathcal{K}$ denote the **condition set**. The system can be in the normal condition $(N)$ or a condition corresponding to a combination of failure modes. The discrete state set can be partitioned according to the condition of the system: $Q = Q_N \dot{\bigcup} (Q_{F^1} \dot{\bigcup} \cdots \dot{\bigcup} Q_{F^{\hat{m}}}) \dot{\bigcup} (Q_{F^{1,2}} \dot{\bigcup} \cdots \dot{\bigcup} Q_{F^{\hat{m}-1,\hat{m}}}) \dot{\bigcup} \cdots \dot{\bigcup} Q_{F^{1,\cdots,\hat{m}}}$. For example, in the system of Fig. 2, $\mathcal{K} = \{N, F^1, F^2, F^3, F^{2,3}\}$, where $F^{2,3}$ corresponds to the case where both failure modes $F^2$ and $F^3$ have occurred. Here, $Q_{F^1} = \{q_3, q_8, q_{12}\}$ and $Q_{F^{2,3}} = \{q_{10}, q_{14}\}$.

The function $active : Q \longrightarrow 2^{FT}$ yields the fault types active in a discrete state: $active(q) = \{f \mid f \in FT$ and $f$ is active in $q\}$. The mapping $active$ can also be extended to subsets of $Q$ as follows. For $\bar{Q} \subseteq Q$, $active(\bar{Q}) = \bigcup_{q \in \bar{Q}} active(q)$. The inverse function $active^{-1} : 2^{FT} \longrightarrow 2^Q$ maps a set of fault types in $FT$ to the set of discrete states of $Q$ in which the fault types are active. For example, in the system of Fig. 2, $active^{-1}(\{f^1\}) = \{q_3, q_8\}$. Let $\Sigma_f \subseteq \Sigma_{uo}$ denote the set of fault events. Function $\kappa : Q \to \mathcal{K}$ denotes the **condition map** of the system, and is defined such that for every $q \in Q$ , $\kappa(q)$ is the condition of the system at the discrete state $q$. The definition of $\kappa$ can be extended to the subsets of $Q$: $\kappa(z) = \{\kappa(q) \mid q \in z\}$, for any $z \subseteq Q$.

Let $\mathcal{F} = \mathcal{K} - \{N\}$ denote the set of **faulty conditions**. Also, let $\mathcal{F}^i$ be the set of faulty conditions in which the failure mode $F^i$ is present, and $Q_{\mathcal{F}^i} = \bigcup_{c \in \mathcal{F}^i} Q_c$. For example, in the system of Fig. 2, $Q_{\mathcal{F}^2} = Q_{F^2} \bigcup Q_{F^{2,3}} = \{q_4, q_9, q_{10}, q_{13}, q_{14}, q_{16}\}$.

Fault diagnosis in our work is to determine the condition of the system by detecting and isolating failure modes in a bounded time after the occurrence of a fault. In the next section, we describe our hybrid diagnosis methodology.

## IV. FAULT DIAGNOSIS IN HYBRID AUTOMATA

Fault diagnosis in our work is achieved at both the DES and the continuous levels. We assume that there is a bank of residual generators (isolators) designed based on the continuous dynamics to isolate fault types at the continuous level. Each residual generator takes the continuous input and output of the system and produces a residual. In the remainder of the paper, we refer to residual generators as **isolators**.

We develop a method for constructing a hybrid diagnoser that integrates the information generated by the isolators and the information available at the DES level (outputs of discrete sensors) to diagnose failures. Fig. 3 shows the schematic of our hybrid diagnosis methodology. First, a DES abstraction of each isolator is constructed which generates discretized version of residual signals. The DES model of the isolators is then integrated with the DES abstraction of the system to construct an **extended DES abstraction (EDESA)**. The hybrid diagnoser is a diagnoser designed based on the EDESA.

We follow the following four steps to construct the EDESA: 1) Each isolator in the system is modeled by a DES; 2) The DES abstraction model of the system ($H_{abs}$) is modified (by adding appropriate selfloop transitions) to make the transitions in the DES models of isolators (step 1) consistent and synchronous with the system transitions; 3) We impose certain assumptions on the order of occurrence of isolator events and specific system events. These assumptions are enforced by DES. This will be discussed in more detail subsequently; and 4) The EDESA will be constructed by integrating the DES models of the isolators, modified DES abstraction of the system and the DES model enforcing the assumptions (step 3) using the synchronous product operation.

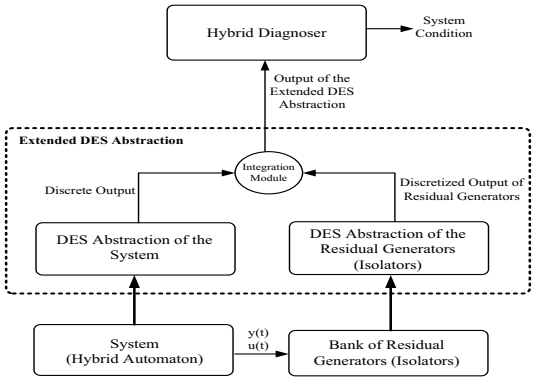



Fig. 3. The schematic of the hybrid diagnosis approach.

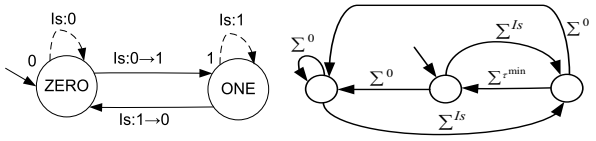
**Modeling of Isolators -**We design a set of isolators based on the continuous dynamics of each EM-similar partition. The necessary and sufficient conditions for the existence of residual generators for isolating faults in linear and nonlinear systems have been studied in [5] and [1], respectively.

For simplicity, we assume that the isolators are initialized to zero. Let $Q^{EM}$ be a set of EM-similar discrete states, $FT^{Q^{EM}}$ be the set of fault types of $Q^{EM}$ and $\Phi \subseteq FT^{Q^{EM}}$. An isolator which is designed for $Q^{EM}$ to be sensitive to the fault types of $\Phi$ and insensitive to the fault types of $FT^{Q^{EM}} - \Phi$ is denoted by $Is^{Q^{EM}}(\Phi)$. We assume that the isolator $Is^{Q^{EM}}(\Phi)$ generates a nonzero residual for all inputs $u \in \mathcal{U}$ after the transient response due to the mismatch of the initial conditions of the $Is^{Q^{EM}}(\Phi)$ and the system dies out if the system is not evolving in one of the discrete states of $Q^{EM}$. This is not a very limiting assumption because the continuous dynamics of the system in discrete states of $Q^{EM}$ is different from the continuous dynamics of the system in any other discrete state, and therefore, it is unlikely that the isolator designed based on the dynamics of $Q^{EM}$ generates a zero residual while the system is not evolving in one of the discrete states of $Q^{EM}$.

Let $\epsilon_\Phi^{Q^{EM}} \geq 0$ be a threshold chosen to evaluate the residual $r_\Phi^{Q^{EM}}(t)$ generated by the isolator $Is^{Q^{EM}}(\Phi)$. Also, let $W = active^{-1}(\Phi) \bigcap Q^{EM}$. The isolator $Is^{Q^{EM}}(\Phi)$ must satisfy the following two properties after its transient response due to the mismatch of its initial conditions and the system dies out, namely, 1) $||r_\Phi^{Q^{EM}}(t)|| < \epsilon_\Phi^{Q^{EM}}$ if the system is in one of the discrete states of $Q^{EM} - W$; 2) $||r_\Phi^{Q^{EM}}(t)|| \geq \epsilon_\Phi^{Q^{EM}}$ if the system is in one of the discrete states of $(Q - Q^{EM}) \bigcup W$.

We assume that there is a signal processing unit that takes a residual and generates a "zero" value if it is below the threshold and generates a "one" value if it is equal to or above the threshold. The binary output of the signal processing unit allows one to model the isolator by a DES.

**Modeling the Isolators with DES -** Every isolator in our work can be modeled as a finite state Moore automaton with two states ZERO and ONE. Let $\overline{Is}$ be the FSA model of $Is$. Fig. 4(a) shows the FSA model of the isolator $Is$. In Fig. 4(a), the events '$Is : 0 \rightarrow 1$' and '$Is : 1 \rightarrow 0$' label the transitions from the state ZERO to ONE and from the state ONE to ZERO, respectively. The unobservable events '$Is : 0$' and '$Is : 1$' are fictitious events added for design consistency. These selfloop transitions (transitions from one discrete state to itself) are unobservable and do not change the output. Assume there are $b$ ($b \geq 0$) isolators designed for the system, and let $\mathbf{IS}_{tot} = \{Is_1, \cdots, Is_b\}$ be the set of isolators. Also, let $\Sigma^{Is_i} = \{Is_i : 0 \rightarrow 1, Is_i : 1 \rightarrow 0, Is_i : 0, Is_i : 1\}$ for $1 \leq i \leq b$.




(a) $\overline{Is}$ (b) $ASM_{Is}$

Fig. 4. The finite-state automata $\overline{Is}$ and $ASM_{Is}$.

**Consistency Between the System and the Isolator DES Models -** While the system is in any $q \in Q^{EM}$, the isolators designed for the discrete states $q \in Q - Q^{EM}$ can only have transitions from ZERO to ONE or stay at ONE (if already at ONE). Assume that the system enters the discrete state $q \in Q^{EM}$. While the system is in $q$, an isolator $Is^{Q^{EM}}(\Phi)$ has a transition from ONE to ZERO or stays at ZERO if none of the fault types of $\Phi$ is active in $q$. Otherwise, it has a transition from ZERO to ONE or stays at ONE. The DES model of the system $H_{abs}$ is modified to enforce these consistency requirements by adding appropriate selfloop transitions to $H_{abs}$. The new FSA is denoted by $\hat{H}_{abs}$. (The procedure of constructing $\hat{H}_{abs}$ is not shown here due to space limitation.)

**Enforcing Assumptions by DES Models -** In general, there are two types of transitions in a hybrid automaton, namely, transitions with a purely DES nature such as "open" command generated by a supervisory controller to open a valve, and autonomous transitions whose occurrence depends on the continuous dynamics such as turning off of an automatic heater when the temperature reaches a certain value. In many hybrid systems, due to practical considerations such as stability issues, it is usually assumed that when the system enters a discrete state, certain transitions defined at that state do not occur instantaneously.

In order to take into account the above issues, we assume that certain transitions in the system can occur only if the system has stayed in the source state of those transitions for at least a $\tau^{min}$. In this work, $\tau^{min}$ denotes the worst-case (maximum) time that is required for the transient response due to the mismatch in initial conditions of the residual generators and the system dies out. Based on this assumption, we partition the event set into $\Sigma = \Sigma^{\tau^{min}} \bigcup \Sigma^0$, where $\Sigma^{\tau^{min}}$ is the set of events labeling the transitions that can occur only if the system has stayed in the source of these transitions for at least $\tau^{min}$, and $\Sigma^0$ is the set of all other events. This assumption is enforced as follows: one event of every isolator must occur before any event of $\Sigma^{\tau^{min}}$ occurs. The FSA $ASM_{Is}$, as shown in Fig. 4(b), enforces this assumption for the isolator $Is$.

**Constructing the EDESA of the Hybrid Automata -** Let $\overline{\mathbf{IS}}_{tot} = \{\overline{Is}_1, \cdots, \overline{Is}_b\}$ be the set of FSA modeling the isolators. The EDESA of $H$, denoted by $\tilde{H}$, is an FSA defined as $\tilde{H} = (\tilde{Q}, \tilde{\Sigma}, \tilde{T}, \tilde{D}, \tilde{\lambda}, \tilde{q}_0)$ and is constructed by integrating $\hat{H}_{abs}$, the FSA modeling the isolators and the FSA enforcing the ordering assumption: $\tilde{H} = \overline{Is}||\hat{H}_{abs}||ASM$, where $\overline{Is} = \overline{Is}_1||\cdots||\overline{Is}_b$ and $ASM = ASM_{Is_1}||\cdots||ASM_{Is_b}$. Here, the notation '||' denotes the synchronous product.

The diagnoser designed for $\tilde{H}$ and denoted by $DG(\tilde{H})$ is a DES diagnoser (as described in [3]) which uses the discrete outputs of EDESA for diagnosis and is defined to be a finite-state Moore automaton $DG(\tilde{H}) = (\tilde{Z}\bigcup\{\tilde{\underline{z}}_0\}, \tilde{D}, \tilde{\delta}, \tilde{z}_0, \tilde{\mathcal{C}}, \tilde{\kappa})$, where $\tilde{Z}\bigcup\{\tilde{\underline{z}}_0\}$, $\tilde{D}$ and $\tilde{\mathcal{C}} \subseteq 2^{\mathcal{K}} - \{\emptyset\}$ are the state, event and output sets; $\tilde{\underline{z}}_0 := (\tilde{z}_0, 0)$ is the initial set with $\tilde{z}_0 \in 2^{\tilde{Q}} - \{\emptyset\}$; $\tilde{Z} \subseteq 2^{\tilde{Q}} - \{\emptyset\}$, and $\tilde{\delta} : \tilde{Z}\bigcup\{\tilde{\underline{z}}_0\} \times \tilde{D} \rightarrow \tilde{Z}$ represents the transition function; $\tilde{\kappa} : \tilde{Z}\bigcup\{\tilde{\underline{z}}_0\} \rightarrow \tilde{\mathcal{C}}$ denotes the output map. Given the state estimate $\tilde{z}_n$ and upon observing $\tilde{d}_{n+1}$, the state estimate is updated according to: $\tilde{z}_1 = \tilde{z}_0 \bigcap \tilde{\lambda}^{-1}(\{\tilde{d}_1\})$ $(n = 0)$ and $\tilde{z}_{n+1} = \tilde{\delta}(\tilde{z}_n, \tilde{d}_{n+1})$ $(n \geq 1)$.

## V. DIAGNOSABILITY OF FAILURE MODES

In this section, we investigate diagnosability of failure modes of $H$. We will show that for verifying the diagnosability of a failure mode of $H$, it is sufficient to verify the diagnosability of that failure mode in the EDESA of $H$ and the isolators designed for $H$.

We assume that $Q = Q^{inf}\dot{\bigcup}Q^{fin}$, where $Q^{fin}$ is the set of states in which the system never stays longer than a finite time $\tau^{max}$, and $Q^{inf}$ is the set of states in which the system remain indefinitely. Similarly, $\tilde{Q} : \tilde{Q} = \tilde{Q}^{inf}\dot{\bigcup}\tilde{Q}^{fin}$. The value of $\tau^{max}$ can be calculated by using the dynamics of the system at the discrete states and the dynamics of the guard conditions. In this paper, we assume that $\tau^{max}$ is given.

We add an unobservable selfloop transition labeled with a fictitious event to every discrete state of $Q^{inf}$ which has an outgoing transition to another state. By doing this, we allow transitions to occur at these states without changing the state of the system, and thus, model EDESA getting stuck in a state.

*Definition 2:* We call a failure mode $F^i$ **$\Pi$-diagnosable** if it is always possible to detect after a bounded number of events $\Pi$ generated in the system (following the occurrence of the failure mode and initialization of the diagnoser) whether the system has entered and stayed in the set $Q_{\mathcal{F}^i}$. ■

Generally, the constraints for diagnosability analysis in DES is expressed in terms of the number of events generated in the system. However, in hybrid automata, the notion of time is included in the model. Therefore, it is desirable to develop diagnosability results with respect to time requirements. In order to discuss diagnosability of failure modes with time constraints, we describe the notion of *execution* in hybrid automata. First, we define a hybrid time set.

A **hybrid time set** [4] is a finite or infinite sequence of intervals $\tau = \{I_i\}_{i=0}^{\tilde{N}}$ such that if $\tilde{N}$ is finite then 1) $I_i = [\tau_i, \tau_i']$ for all $0 \leq i < \tilde{N}$ with $\tau_0 < \tau_0' = \tau_1 < \tau_1' \leq \cdots < \tau_{\tilde{N}-1} < \tau_{\tilde{N}-1}'$; 2) $I_{\tilde{N}} = [\tau_{\tilde{N}}, \tau_{\tilde{N}}')$; If $\tilde{N} = \infty$, then $I_i = [\tau_i, \tau_i']$ for all $0 \leq i \leq \tilde{N}$ with $\tau_0 < \tau_0' = \tau_1 < \tau_1' \leq \cdots < \tau_{\tilde{N}-1} < \tau_{\tilde{N}-1}'$. The $\tau_i$ are the times at which discrete transitions take place. $|\tau| = \tilde{N}+1$ is the number of intervals. For a hybrid time set $\tau = \{I_i\}_{i=0}^{\tilde{N}}$, we define $< \tau >$ as the set $\{0, 1, \cdots, \tilde{N}\}$ if $\tilde{N}$ is finite, and $\{0, 1, \cdots\}$ if $\tilde{N} = \infty$.

An **execution** [4] of a hybrid automaton is a tuple $e = (\tau^e, q^e, x^e)$, where $\tau^e = \{I_i^e\}_{i=0}^{\tilde{N}^e}$ is a hybrid time set with time intervals $I_i^e = [\tau_i^e, \tau_i'^e]$ for all $0 \leq i \leq \tilde{N}^e$; $q^e :< \tau^e > \rightarrow Q$ is a map such that $q^e(0) = q_0$; $x^e = \{x_i^e : i \in < \tau^e >\}$ is a set of differentiable maps $x_i^e : I_i^e \rightarrow \mathcal{X}$, such that 1) $x_0^e(0) \in Init$; 2) for all $t \in [\tau_i, \tau_i')$, $\dot{x^e}_i(t) = E_{q^e(i)}(x_i^e(t), u_i^e(t)) + G_{q^e(i)}(f_{1,i}^e(t), \cdots, f_{m,i}^e(t))$, where $u_i^e : I_i^e \rightarrow \mathcal{U}$ and $f_{j,i}^e : I_i \rightarrow \mathbb{R}$ (for $1 \leq j \leq m$) are the maps which give the input signal and the signal of active fault types in interval $I_i^e$, respectively; 3) if $\tilde{N}^e$ is finite, for all $i \in < \tau > \backslash\{\tilde{N}^e\}$, there exists $\sigma \in \Sigma :\ d = (q^e(i), \sigma, q^e(i+1)) \in T,\ G(d, x_i^e(\tau_i')) = \{True\}$ and $x_{i+1}^e(\tau_{i+1}) = \rho(d, x_i^e(\tau_i'))$; 4) if $\tilde{N} = \infty$, for all $i \in < \tau >$, there exists $\sigma \in \Sigma :\ d = (q^e(i), \sigma, q^e(i+1)) \in T,\ G(d, x_i^e(\tau_i')) = \{True\}$ and $x_{i+1}^e(\tau_{i+1}) = \rho(d, x_i^e(\tau_i'))$.

The maps $q^e$ and $x^e$ describe the evolution of the discrete states $q$ and the continuous state $x$, respectively. They satisfy the discrete and the continuous dynamics and their interactions (initial state, guard conditions and reset maps) in the system.

Let $\mathcal{E}$ be the **set of all executions** of $H$. For any execution $e \in \mathcal{E}$, we have $|e| = |\tau^e|$. In this paper, we assume that all hybrid executions are defined for all $t \geq 0$. In other words, we study *non-blocking* hybrid automata. We do not have Zeno executions in our framework, therefore, the executions are infinite, i.e., $\Sigma_{k=0}^{|e|}(\tau_k'^e - \tau_k^e) = \infty$. However the hybrid time sets may be finite or infinite. Let $q \in Q$ be a discrete state.

Let $e \in \mathcal{E}$ be an execution. **The continuous output signal** $y^e$ for execution $e$ is the set of maps $y^e = \{y_i^e : i \in < \tau^e >\}$ with $y_i^e : I_i^e \rightarrow \mathcal{Y}$, such that for all $t \in [\tau_i^e, \tau_i'^e)$, $y_i^e(t) = M_{q^e(i)}(x_i^e(t), u_i^e(t))$

Let $t_i \in I_i^e$ and $t_j \in I_j^e$ with $i < j$. The continuous state trajectory from time $t_i$ to $t_j$ for execution $e$ is denoted by $x^e|_{t_i}^{t_j}$: $x^e|_{t_i}^{t_j} = \{x_i^e(t) \mid t_i \leq t \leq \tau_i'^e, x_{i+1}^e, \cdots, x_{j-1}^e, x_j^e(t) \mid \tau_j^e \leq t \leq t_j\}$. Similarly, $y^e|_{t_i}^{t_j}$ denotes the output signals from time $t_i$ to $t_j$ for execution $e$. The map $\mu : \mathcal{E} \longrightarrow D^*$ associates a sequence of discrete output to each execution $e$ as: $\mu(e) = \lambda(q^e(0))\lambda(q^e(1))\cdots\lambda(q^e(|e|))$. We denote by $\mu(e)|_{t_i}^{t_j}$. The sequence of the discrete outputs associated with $e$ from time $t_i$ to time $t_j$: $\mu(e)|_{t_i}^{t_j} = \lambda(q^e(i))\lambda(q^e(i+1))\cdots\lambda(q^e(j))$ such that $t_i \in I_i^e$ and $t_j \in I_j^e$. We omit all discrete outputs $\lambda(q^e(j))$ such that $\lambda(q^e(j)) = \lambda(q^e(j+1))$ from $\mu(e)$ and denote the new sequence by $\hat{\mu}(e)$. For instance, if $\mu(e) = aab$, then $\hat{\mu}(e) = ab$. The map $\hat{\mu}(e)$ shows only the output changes that are used for diagnosis. The map $\hat{\mu}(e)|_{t_i}^{t_j}$ will be similarly constructed from $\mu(e)|_{t_i}^{t_j}$.

An execution $e \in \mathcal{E}$ is called an **$\mathbf{F^i}$-faulty execution** if there exists $0 \leq k_i \leq |e|$ such that for all $k < k_i$, $q^e(k) \notin Q_{\mathcal{F}^i}$ and $q^e(k_i) \in Q_{\mathcal{F}^i}$. Let $t_{F^i}^e$ be the time that $F^i$-faulty execution $e$ enters $Q_{\mathcal{F}^i}$. Since the occurrence of each failure mode is modeled by an unobservable transition, execution $e$ enters $Q_{\mathcal{F}^i}$ at time $t_{F^i}^e = \tau_{k_i}^e$. Let $\mathcal{E}^{F^i}$ be the set of all $F^i$-

faulty executions. For diagnosability analysis, we assume that the failure modes are permanent. Failure mode $F^i$ is permanent if for any $e \in \mathcal{E}^{F^i}$ such that $q^e(k_i) \in Q_{\mathcal{F}^i}$, then $q^e(k) \in Q_{\mathcal{F}^i}$ for all $k_i \leq k \leq |e|$.

Let $\Delta \geq 0$ be a positive real number. We call a failure mode $F^i$ $\Delta$-diagnosable if it is always possible to detect, with a delay no longer than $\Delta$ following the occurrence of $F^i$, whether the system has visited the set $Q_{\mathcal{F}^i}$ (by using the sequence of discrete outputs and continuous output signal of the system.

*Definition 3:* Assume that a permanent failure mode $F^i$ occurs at $t = t_0 \geq 0$ and the diagnosis starts at $t_d \geq 0$. Also let $t_m = max(t_0, t_d)$. The failure mode $F^i$ is **$\Delta$-diagnosable** in $H$ if for all $e \in \mathcal{E}^{F^i}$ and $e' \in \mathcal{E} - \mathcal{E}^{F^i}$, $\hat{\mu}(e)|_{t_m}^{(t_m+\Delta)} \neq \hat{\mu}(e')|_{t_m}^{(t_m+\Delta)}$ or $\left[\begin{array}{c} u^e \\ y^e \end{array}\right] \Big| \begin{array}{l} t_m + \Delta \\ t_m \end{array} \neq \left[\begin{array}{c} u^{e'} \\ y^{e'} \end{array}\right] \Big| \begin{array}{l} t_m + \Delta \\ t_m \end{array}$ [1]. ■

*Proposition 1:* If a failure mode $F^i$ is not $\Delta$-diagnosable in $H$, $F^i$ is not $\Delta'$-diagnosable in $H$ for all $\Delta' \leq \Delta$.

**Proof -** The proof is omitted due to space limitation. ■

*Theorem 1:* Assume that the diagnoser of $\tilde{H}$ is initialized with $\tilde{z}_0 = \tilde{Q}$. A permanent failure mode $F^i$ is $\Delta$-diagnosable in $H$ if $F^i$ is $\Pi$-diagnosable in $\tilde{H}$ for some $\Pi \leq [\frac{\Delta}{\tau^{max}}]$. ■

**Proof -** By contradiction, we prove that if $F^i$ is not $\Delta$-diagnosable (for a $\Delta \geq 0$) in $H$, there exists no $\Pi \leq [\frac{\Delta}{\tau^{max}}]$ such that $F^i$ is $\Pi$-diagnosable in $\tilde{H}$.

Assume that the failure mode $F^i$ corresponding to fault type $f^i$ is not $\Delta$-diagnosable in $H$. Thus, there exist $e \in \mathcal{E}^{F^i}$ and $e' \in \mathcal{E} - \mathcal{E}^{F^i}$ such that both executions $e$ and $e'$ will generate the same sequence of discrete outputs and identical continuous input and output signals from $t_m$ to $t_m + \Delta$, i.e., $\hat{\mu}(e)|_{t_m}^{(t_m+\Delta)} = \hat{\mu}(e')|_{t_m}^{(t_m+\Delta)}$ and $u^e|_{t_m}^{t_m+\Delta} = u^{e'}|_{t_m}^{t_m+\Delta}$ and $y^e|_{t_m}^{t_m+\Delta} = y^{e'}|_{t_m}^{t_m+\Delta}$. Therefore, any isolator $Is \in \mathbf{IS}_{tot}$ that takes the continuous input and output of the system generates identical outputs for $e$ and $e'$ from $t_m$ to $t_m + \Delta$. Thus, the FSA modeling $Is$ will generate identical discrete outputs and events for $e$ and $e'$ from $t_m$ to $t_m+\Delta$. Let $0 \leq i \leq j \leq |e|$ such that $t_m \in I_i^e$ and $(t_m + \Delta) \in I_j^e$. Also let $0 \leq i' \leq j' \leq |e'|$ such that $t_m \in I_{i'}^{e'}$ and $(t_m + \Delta) \in I_{j'}^{e'}$. The output sequence generated by $\tilde{H}$ consists of the system discrete outputs and outputs generated by isolators between system outputs. Hence, the output sequence generated by $\tilde{H}$ from $t_m$ to $t_m + \Delta$ will be identical for both executions $e$ and $e'$. Let $q^e(i)$ and $q^{e'}(i')$ denote the initial discrete states of $\tilde{H}$ on $e$ and $e'$, respectively. Also let $q^e(j)$ and $q^{e'}(j')$ denote the final discrete states of $\tilde{H}$ on $e$ and $e'$, respectively. If the diagnoser for $\tilde{H}$ is started at $t_d = t_m$, then $q^e(i), q^{e'}(i') \in \tilde{z}_0$, and since the output sequences of $\tilde{H}$ on $e$ and $e'$ are the same, then $q^e(j), q^{e'}(j') \in \tilde{z}(t_m + \Delta)$, where $\tilde{z}(t_m + \Delta)$ is the state estimate provided by the diagnoser at $t_m+\Delta$. Thus, $\tilde{z}(t_m+\Delta)$ is $F^i$-uncertain. If all the discrete states from $q^e(i)$ to $q^e(j)$ are not in $Q^{inf}$, then during $e$, at least $\frac{\Delta}{\tau^{max}}$ events must have been generated by $\tilde{H}$. If one or more of discrete states from $q^e(i)$ to $q^e(j)$ is in $Q^{inf}$, considering the fictitious selfloops for states in $Q^{inf}$, then the sequence from $q^e(i)$ to $q^e(j)$ can be considered to have an arbitrary large number of events. Since the final diagnoser state is $F^i$-uncertain, then $F^i$ is not $\Pi$-diagnosable for any $\Pi \leq [\frac{\Delta}{\tau^{max}}]$. ■

*Proposition 2:* Let $b$ be the number of isolators designed for the system. Also let $|Q|$ be the cardinality of $Q$. The complexity of verifying the diagnosability of the failure mode $F^i$ in $\tilde{H}$ is $\mathcal{O}(2^{4b}|Q|^4)$.

**Proof -** The proof is omitted due to space limitation. ■

## VI. CONCLUSIONS AND FUTURE WORK

A hybrid diagnosis methodology is presented in this paper for systems modeled by hybrid automata, and diagnosability of failure modes is investigated within the diagnosis framework. It is assume that a bank of residual generators is designed based on the continuous dynamics of the system. A systematic approach is developed for integrating the diagnosis information provided by the residual generators and the discrete-event abstraction of the system to build an Extended Discrete-Event System Abstraction (EDESA). Then, a diagnoser is constructed for the EDESA. The diagnosability of failure modes in the EDESA is studied and a notion of diagnosability in hybrid automata is introduced. It is shown that a failure mode is diagnosable in a hybrid automaton if it is diagnosable in the EDESA. Extending the diagnosis approach so that the diagnosability of the EDESA becomes necessary for the diagnosability of a hybrid automaton is the subject of ongoing research.

[1] We say $u^e|_{t_2}^{t_1} \neq u^{e'}|_{t_2}^{t_1}$ if the set $\{t \mid t_1 \leq t \leq t_2 \text{ and } t \in I_i^e \text{ and } t \in t_j^{e'} : u_i^e(t) = u_j^{e'}(t)\}$ is of measure zero.

## REFERENCES


[1] C. De Persis and A. Isidori, "A geometric approach to nonlinear fault detection and isolation," *IEEE Trans. on Automat. Contr.*, vol. 46, no. 6, pp. 853 - 865, 2001.

[2] R. J. Patton, P. M. Frank and R. N. Clark, "Issues of fault diagnosis for dynamic systems," *Springer*, 2000.

[3] S. Hashtrudi Zad, R.H. Kwong and W.M. Wonham, "Fault diagnosis in discrete-event systems: Framework and model reduction," *IEEE Trans. on Automat. Contr.*, vol. 48, no. 7, pp. 1199-1212, 2003.

[4] K. H. Johansson, J. Lygeros, S.N. Simic, J. Zhang, and S. Sastry, "Dynamical properties of hybrid automata," *IEEE Trans. on Automat. Contr.*, vol. 48, no. 1, pp. 2-17, 2003.

[5] M. A. Massoumnia, G. C. Verghese, and A. S. Willsky, "Fault detection and identification," *IEEE Trans. on Automat. Contr.*, vol. AC-34, no. 3, pp. 316-321, 1989.

[6] S. McIlraith, G. Biswas, D. Clancy and V. Gupta, "Hybrid systems diagnosis," *Hybrid Systems: Computation and Control, vol. 1790 of LNCS*, pp. 282-295, Springer-Verlag, 2000.

[7] R. Mohammadi, S. Hashtrudi-Zad, and K. Khorasani, "Hybrid fault diagnosis: Application to a gas turbine engine," Proc. of the *Turbo Expo 2009*, Orlando, FL, USA, 11 pages, 2009.

[8] R. Mohammadi, S. Hashtrudi-Zad, and K. Khorasani, "Diagnosis of hybrid systems: Part 2- Residual generator selection and diagnosis in the presence of unreliable residual generators," Proc. of *the IEEE Conf. on Sys., Man and Cyber.*, San Antonio, TX, USA, 2009.

[9] S. Narasimhan, "Model-based diagnosis of hybrid systems", Ph.D. dissertation, EECS Dept, Vanderbilt University, Nashville, TN, 2002.

[10] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Diagnosability of discrete-event systems," *IEEE Trans. on Automat. Contr.*, vol. 40, no. 9, pp. 1555-1575, 1995.

[11] S. Tripakis, "Fault diagnosis for timed automata," *Proc. of the Intl. Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems, vol. 2469 of LNCS*, pp. 205-224, Springer-Verlag, 2002.

[12] F. Zhao, X. Koutsoukos, H. Haussecker, J. Reich, and P. Cheung, "Monitoring and Fault Diagnosis of Hybrid Systems," *IEEE Trans. on Syst., Man, and Cyber. - Part B*, vol. 35, no. 6, pp. 1225-1240, 2005.