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

Diagnosis of Hybrid Systems: Part 2- Residual Generator Selection and Diagnosis in the Presence of Unreliable Residual Generators

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*—We have presented a framework in [6] for fault diagnosis of hybrid systems modeled by hybrid automata and investigated the diagnosability of failure modes in hybrid automata. In this framework, we assume that there is a bank of residual generators designed for the continuous dynamics of the system. We have developed 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. In this paper, we study the problem of residual generator selection in hybrid automata. Moreover, we investigate fault diagnosis of hybrid systems in the presence of unreliable residual generators generating false alarms or false silence signals.**

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

I. INTRODUCTION

In general, there are two types of sensors in a hybrid system, namely, discrete sensors that generate discrete outputs which are available at the Discrete-Event System (DES) representation of the system, and continuous sensors that generate continuous outputs which are available at the continuous dynamics. In [5], we developed a hybrid automaton model for a gas turbine engine and studied fault diagnosis in the engine. We showed that there are cases that some faults are not diagnosable 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 is integrated with the output of the discrete sensors.

We assume that a bank of residual generators (using continuous sensors) designed for the continuous dynamics of the system is available. In [5], we developed a systematic method for constructing an extended DES model containing the information at the DES level of the system as well as the diagnosis information provided by the residual generators. Based on the extended DES model, we construct a hybrid diagnoser for hybrid automata. In [6], we reviewed our hybrid diagnosis method and investigated the diagnosability of failure modes in our hybrid diagnosis framework. It is shown that a failure mode is diagnosable in a hybrid automaton if it is diagnosable in the extended DES model.

In this paper, we study the problem of residual generator selection in hybrid automata and develop a generic algorithm for computing a minimal set of residual generators for attaining the diagnosability of failure modes. We develop necessary and sufficient conditions for residual generator selection in a hybrid automaton so that a failure mode becomes diagnosable in the extended DES model of the hybrid system and residual generators. The problem of residual generator selection studied for hybrid automata can be considered as the counterpart of the sensor selection problem discussed in [1] and [7] for purely DES.

Moreover, we investigate fault diagnosis of hybrid systems in the presence of unreliable residual generators generating false alarms or false silence signals.

The remainder of the paper is organized as follows. In Sec. II, we briefly present our diagnosis framework and review the notations used in this paper. We investigate the problem of residual generator selection in Sec. III. Fault diagnosis in the presence of unreliable isolators is studied in Sec. IV. We present the conclusions in Sec. V.

II. PRELIMINARIES

In this section, we briefly overview our hybrid diagnosis framework. The details of the hybrid diagnosis approach can be found in [5], [6].

A. Failure Modeling

A **hybrid automaton** with faulty behavior in our work 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; Σ is a set of symbols representing the discrete events labeling the transitions among discrete

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

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.

A discrete event is associated with any transition between two discrete states. We refer to the tuple $H_{abs} = (Q, \Sigma, T, D, \lambda, q_0)$ as the **DES abstraction** of H. We assume that $\Sigma = \Sigma_o \bigcup \Sigma_{uo}$, where Σ_o represents the observable event set and Σ_{uo} consists of unobservable events.

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. 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. 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.

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. This typically happens when a faulty component is not used or is off in a given mode of operation. 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: $Q = Q_N \bigcup (Q_{F^1} \bigcup \cdots \bigcup Q_{F^{\hat{m}}}) \bigcup (Q_{F^{1,2}} \bigcup \cdots \bigcup Q_{F^{\hat{m}-1,\hat{m}}}) \bigcup \cdots \bigcup Q_{F^{1,\cdots,\hat{m}}}$.

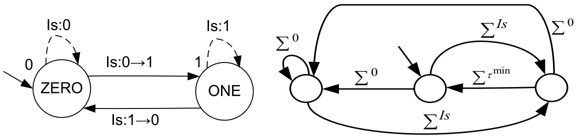
Let $\mathcal{F} = \mathcal{K} - \{N\}$ denote the set of **faulty conditions**. Also, let $\mathcal{F}^i$ be the set of faulty conditions in which the failure mode F^i is present, $\overline{\mathcal{F}^i} = \mathcal{F} - \mathcal{F}^i$, $Q_{\mathcal{F}^i} = \bigcup\limits_{c \in \mathcal{F}^i} Q_c$ and $Q_{N,\overline{\mathcal{F}^i}} = Q - Q_{\mathcal{F}^i}$.

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 a state set $\bar{Q} \subseteq Q$ as follows. $active(\bar{Q}) = \bigcup\limits_{q \in \bar{Q}} active(q)$. 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.

We assume that $Q = Q^{inf} \bigcup Q^{fin}$, where Q^{fin} is the set of discrete states in which the system never stays longer than a finite time τ^{max}, and Q^{inf} is the set of discrete states in which the system remain indefinitely.

B. Fault Diagnosis in Hybrid Automata

We assume that a bank of residual generators (using continuous sensors) designed for the continuous dynamics of the system is available. The residual generator used for fault diagnosis in our work are referred to as **isolators**.



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

Fig. 1. The finite-state automata $\overline{Is}$ and ASM_{Is}.

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). A set of isolators is designed based on the continuous dynamics of each partition. The solvability conditions for the existence of residual generators for isolating faults in linear and nonlinear systems have been studied in [4] and [2], 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 designed for Q^{EM} to be sensitive to fault types of Φ 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}.

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. 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 not 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 "zero" if it is below the threshold and generates "one" if it is equal to or above the threshold. The binary output of the signal processing unit allows us to model an isolator with a DES. Let $\overline{Is}$ be the FSA model of Is. Fig. 1(a) shows the FSA model of the isolator Is. In order to make the transitions of isolators consistent with the transition system of the system, we modify the DES model of the system H_{abs}. We add appropriate selfloop transitions to H_{abs} and denote the new FSA by $\hat{H}_{abs}$. 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, and $\Sigma^{Is_i} = \{Is_i : 0 \rightarrow 1, Is_i : 1 \rightarrow 0, Is_i : 0, Is_i : 1\}$ for $1 \leq i \leq b$.

Let τ^{min} denote the time required that the transient response due to the mismatch of the initial conditions of residual generators and the system dies out. We assume that certain transitions in the system can occur only if the system has stayed in their source state for at least τ^{min}. Based on this assumptions, 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 their source state for at least τ^{min}, and Σ^0 is the set of 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. 1(b), enforces this assumption for the isolator Is.

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 or parallel composition.

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 $DG(\tilde{H}) = (\tilde{Z} \bigcup \{\underline{\tilde{z}}_0\}, \tilde{D}, \tilde{\delta}, \tilde{z}_0, \tilde{\mathcal{C}}, \tilde{\kappa})$, where $\tilde{Z} \bigcup \{\underline{\tilde{z}}_0\}$, $\tilde{D}$ and $\tilde{\mathcal{C}} \subseteq 2^{\mathcal{K}} - \{\emptyset\}$ are the state, event and output sets of $DG(\tilde{H})$; $\underline{\tilde{z}}_0 := (\tilde{z}_0, 0)$ is the initial set with $\tilde{z}_0 \in 2^{\tilde{Q}} - \{\emptyset\}$; $\tilde{Z} \subseteq 2^{\tilde{Q}} - \{\emptyset\}$, and $\tilde{\delta} : \tilde{Z} \bigcup \{\underline{\tilde{z}}_0\} \times \tilde{D} \to \tilde{Z}$ represents the transition function; $\tilde{\kappa} : \tilde{Z} \bigcup \{\underline{\tilde{z}}_0\} \to \tilde{\mathcal{C}}$ denotes the output map. Given 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 $\tilde{z}_{n+1} = \tilde{\delta}(\tilde{z}_n, \tilde{d}_{n+1})$ $(n \geq 1)$. In the following, we study the problem of isolator selection in hybrid automata.

III. ISOLATOR SELECTION

Assuming failure diagnosability, some of the isolators may provide redundant information and therefore, they may be not necessary for fault diagnosis. Thus, we want to investigate the problem of selecting a minimal set of isolators to ensure the diagnosability of failure modes in the system. For a set of isolators $\mathbf{IS} \subseteq \mathbf{IS}_{tot}$, let $\tilde{H}(\mathbf{IS})$ denote the EDESA constructed based on the system H and isolators of $\mathbf{IS}$. Also let $\mathbf{SIS}^{F^i}$ be the set of isolator sets for which a failure mode F^i is diagnosable in the EDESA of the system and isolators $\tilde{H}$. We develop a *buttom-up, top-down* algorithm for determining a minimal set $\mathbf{IS}^{F^i}_{min} \subseteq \mathbf{IS}_{tot}$ such that F^i is diagnosable in $\tilde{H}(\mathbf{IS}^{F^i}_{min})$. In this algorithm, diagnosability of a failure mode is initially investigated based on the DES abstraction model. If the information gathered from the discrete outputs of the system is not sufficient for diagnosis of a failure mode, appropriate isolators are selected to make that failure mode diagnosable in the hybrid system.

Let Q^{EM} be a set of EM-similar discrete states, $FT^{Q^{EM}}$ be the set of fault types present in Q^{EM}. Isolator $Is^{Q^{EM}}(\Phi)$ generates zero output only if the system is in a discrete state of Q^{EM} where no fault type of Φ is active. Therefore, the output generated by an isolator can be considered as a function of the discrete state of the system. We associate a binary function with any isolator $Is^{Q^{EM}}$ designed for Q^{EM} as follows:

$$\Gamma^{Is^{Q^{EM}}(\phi)}(q) = \begin{cases} 1 \text{ if } q \notin Q^{EM} \\ 1 \text{ if } q \in Q^{EM} \text{ and } active(q) \bigcap \phi \neq 0 \\ 0 \text{ if } q \in Q^{EM} \text{ and } active(q) \bigcap \phi = 0 \end{cases}$$

Let $\mathbf{IS} = \{Is^1, \cdots, Is^l\} \subseteq \mathbf{IS}_{tot}$ be a set of isolators that can be designed for the system. Function Γ associated with a set of isolators $\mathbf{IS}$ is defined as follows: $\Gamma^{\mathbf{IS}}(q) = (\Gamma^{Is^1}(q) \times \cdots \times \Gamma^{Is^l}(q))$. Two discrete states are called distinguishable if using the outputs of the isolators, one can identify which of the discrete states the system is evolving in.

Definition 1: Two discrete states $q, q' \in Q$ are called **distinguishable** from each other if there exists an isolator $Is \in \mathbf{IS}_{tot}$ such that $\Gamma^{Is}(q) \neq \Gamma^{Is}(q')$. ■

Let $P, P' \subseteq Q$ be two discrete state sets. We say P and P' are distinguishable from each other if for any $q \in P$ and $q' \in P'$, q and q' are distinguishable from each other. Let $\mathbf{IS} \subseteq \mathbf{IS}_{tot}$ be the set of isolators such that P and P' are distinguishable from each other using the outputs of the isolators of $\mathbf{IS}$. Isolator set $\mathbf{IS}$ is called a $\mathbf{P|P'}$**-distinguisher**. Let $\mathbf{SDS}(P|P')$ denote the set of all $P|P'$-distinguishers.

Definition 2: Let $\mathbf{IS} \in \mathbf{SDS}(P|P')$. $\mathbf{IS}$ is called a **minimal** $\mathbf{P|P'}$**-distinguisher** if none of the proper subsets of $\mathbf{IS}$ is a $P|P'$-distinguisher. ■

Lemma 1: Let $P, P \subseteq Q$ be two sets of discrete states. Also let $V \subseteq P$ and $V' \subseteq P'$. If $\mathbf{IS} \in \mathbf{SDS}(P|P')$, then $\mathbf{IS} \in \mathbf{SDS}(V|V')$.

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

Theorem 1: Let $P, P' \subseteq Q$.

$$\mathbf{SDS}(P|P') = \bigcap_{q \in P} \bigcap_{q' \in P'} \mathbf{SDS}(\{q\}|\{q'\})$$

Proof - Suppose $\mathbf{IS} \in \mathbf{SDS}(P|P')$. According to Lemma 1, we have $\mathbf{IS} \in \mathbf{SDS}(\{q\}|\{q'\})$ for any $q \in P$ and $q' \in P'$. Therefore, $\mathbf{IS} \in \bigcap_{q \in P} \bigcap_{q' \in P'} \mathbf{SDS}(\{q\}|\{q'\})$. Now, let $\mathbf{IS} \in \bigcap_{q \in P} \bigcap_{q' \in P'} \mathbf{SDS}(\{q\}|\{q'\})$. This means that for any $q \in P$ and $q' \in P'$, $\Gamma^{\mathbf{IS}}(q) \neq \Gamma^{\mathbf{IS}}(q')$ and by Definition 1, $\mathbf{IS} \in \mathbf{SDS}(\{q\}|\{q'\})$. Therefore, $\mathbf{IS} \in \mathbf{SDS}(P|P')$. As a result, $\mathbf{SDS}(P|P') = \bigcap_{q \in P} \bigcap_{q' \in P'} \mathbf{SDS}(\{q\}|\{q'\})$. ■

We observe that if $P \bigcap P' \neq \emptyset$, then $\mathbf{SDS}(P|P') = \emptyset$.

Let $H_{abs,\mathcal{F}^i}$ and $H_{abs,N,\overline{\mathcal{F}^i}}$ denote the sub-generators of H_{abs} corresponding to the states of $Q_{\mathcal{F}^i}$ and $Q - Q_{\mathcal{F}^i}$, respectively. Also, let $L_o(H_{abs,\mathcal{F}^i}, q)$ and $L_o(H_{abs,N,\overline{\mathcal{F}^i}}, q')$ be the output language generated from q in the sub-generators $H_{abs,\mathcal{F}^i}$ and $H_{abs,N,\overline{\mathcal{F}^i}}$, respectively.

Let $q \in Q_{\mathcal{F}^i}$. State set $Amb(q)$ denotes the set of discrete states in $Q - Q_{\mathcal{F}^i}$ from which the system can generate an infinite output sequence identical to one generated from q: $Amb(q) = \{q' | q' \in Q - Q_{\mathcal{F}^i}$ and $\{s | s \in L_o(H_{abs,N,\overline{\mathcal{F}^i}}, q') \bigcap L_o(H_{abs,\mathcal{F}^i}, q), |s| \geq |Q|^2\} \neq \emptyset\}$.

Theorem 2: Assume that $\tilde{z}_0 = \tilde{Q}$. For an isolator set $\mathbf{IS}$, a permanent failure mode F^i will be diagnosable in $\tilde{H}(\mathbf{IS})$ if and only if:

1) For any $q \in Q_{\mathcal{F}^i}$ such that $q \in Q^{inf}$, if $\lambda^{-1}(\lambda(q)) \bigcap (Q - Q_{\mathcal{F}^i}) \neq \emptyset$, then $\mathbf{IS} \in \mathbf{SDS}(\{q\} | \lambda^{-1}(\lambda(q)) \bigcap (Q - Q_{\mathcal{F}^i}))$;

2) For any cycle of discrete states $Q^c_{\mathcal{F}^i}$ in $Q_{\mathcal{F}^i}$ consisting of states having the same discrete output in H_{abs}, say d, if $\lambda^{-1}(d) \bigcap (Q - Q_{\mathcal{F}^i}) \neq \emptyset$, then there exists $Q_1 \subseteq Q^c_{\mathcal{F}^i}$ such that for any $q_j \in Q_1$ there exists $Q_j \subseteq \lambda^{-1}(d) \bigcap (Q - Q_{\mathcal{F}^i})$ and $\mathbf{IS} \in \mathbf{SDS}(\{q_j\}|Q_j)$ and $\bigcup_{j=1}^{|Q_1|} Q_j = \lambda^{-1}(d) \bigcap (Q - Q_{\mathcal{F}^i})$;

3) For any cycle of discrete states $Q^c_{\mathcal{F}^i}$ in $Q_{\mathcal{F}^i}$, if there exists a cycle of discrete states $Q^c_{N,\overline{\mathcal{F}^i}} \subseteq Q - Q_{\mathcal{F}^i}$ generating the same unbounded discrete output sequence in H_{abs}, then there exist $q \in Q^c_{\mathcal{F}^i}$ and $q' \in Q^c_{N,\overline{\mathcal{F}^i}}$ and $q' \in Amb(q)$ such that $\mathbf{IS} \in \mathbf{SDS}(\{q\}|\{q'\})$.

Proof: (If part)- Conditions (1) guarantees that after F^i occurs, if the system remains indefinitely in a discrete state $q \in Q^{inf}$, the isolator set $\mathbf{IS}$ generates new output symbols so that q can be distinguished from any $q' \in Q - Q_{\mathcal{F}^i}$ having the same discrete output as q. The output generated by the isolators in the isolator set $\mathbf{IS}$ (integrated with those of discrete sensors) will be F^i-indicative. Conditions (2) guarantees that after F^i occurs, if the system remains in a cycle of discrete states with similar discrete outputs, the isolator set $\mathbf{IS}$ can distinguish any $q' \in Q - Q_{\mathcal{F}^i}$ having the same discrete output from some state of that cycle. Therefore, as the system evolves in the cycle, outputs of the isolator set $\mathbf{IS}$ isolate F^i. Condition (3) guarantees that after F^i occurs, if the system enters a cycle of discrete states $Q^c_{\mathcal{F}^i}$ generating an unbounded sequence of outputs that can be also generated by a cycle of discrete states $Q^c_{N,\overline{\mathcal{F}^i}}$ in $Q - Q_{\mathcal{F}^i}$, then there exists a discrete state $q \in Q^c_{\mathcal{F}^i}$ such that the isolator set $\mathbf{IS}$ can distinguish q from one $q' \in Amb(q)$. When the system is in $Q^c_{\mathcal{F}^i}$, the sequence of discrete outputs generated by the isolator set will be different from those generated in $Q^c_{N,\overline{\mathcal{F}^i}}$. Hence, faulty behavior $\mathcal{F}^i$ will be isolated.

(Only if part) Suppose either conditions (1) or (2) does not hold. After F^i occurs, the system may stay indefinitely in one discrete state $q \in Q^{inf}$ or a cycle of faulty discrete states whose discrete output is not F^i-indicative. If the diagnoser is initialized after this last output and the isolator set $\mathbf{IS}$ does not generate F^i-indicative outputs, then F^i will be undiagnosable in $\tilde{H}$. Condition (3) can be also proven to be necessary by using a similar discussion. ■

In the following, by using the results of Theorem 2, we develop a procedure to compute a set of isolators that makes a failure mode F^i diagnosable. The output of the procedure is a minimal isolator set $\mathbf{IS}^{F^i}_{min}$ that makes F^i diagnosable in $\tilde{H}(\mathbf{IS})$. First we develop a bottom-up algorithm to compute a set $\mathbf{IS}^{F^i}$ that makes F^i diagnosable in $\tilde{H}(\mathbf{IS})$. The set $\mathbf{IS}^{F^i}$ may not be minimal. Thus, by using the top-down algorithm, we can calculate a minimal isolator set.

Initially, $\mathbf{IS}^{F^i} = \emptyset$. First, we add enough isolators to $\mathbf{IS}^{F^i}$ to satisfy condition (1) in Theorem 2. For any states $q \in Q_{\mathcal{F}^i} \bigcap Q^{inf}$ and $q' \in Q - Q_{\mathcal{F}^i}$ such that $\lambda(q) = \lambda(q')$, we compute a $q|q'$-distinguisher. If $q|q'$-distinguisher does not exists, F^i remains undiagnosable in $\tilde{H}(\mathbf{IS})$ for any $\mathbf{IS} \subseteq \mathbf{IS}_{tot}$. If $q|q'$-distinguisher exists, we add it to $\mathbf{IS}^{F^i}$.

Secondly, we add enough isolators to $\mathbf{IS}^{F^i}$ to satisfy condition (2) in Theorem 2. Let $Q^c_{\mathcal{F}^i} \subseteq Q_{\mathcal{F}^i}$ be a set of discrete state having the same output and make a cycle in $Q_{\mathcal{F}^i}$, and $\lambda(Q^c_{\mathcal{F}^i})$ is not F^i-indicative. Also let $Q^C_{\mathcal{F}^i}$ be the set of all these sets. For any $Q^c_{\mathcal{F}^i} \in Q^C_{\mathcal{F}^i}$, we compute a set of isolators to distinguish one of the states $q \in Q^c_{\mathcal{F}^i}$ from a state $q' \in Q - Q_{\mathcal{F}^i}$ having the same output. If a $q|q'$-distinguisher exists, we add this set to $\mathbf{IS}^{F^i}$. If there exists a cycle $Q^c_{\mathcal{F}^i}$ such that for all $q \in Q^c_{\mathcal{F}^i}$ no $q|q'$-distinguisher exists, F^i remains undiagnosable.

Thirdly, we add enough isolators to $\mathbf{IS}^{F^i}$ to satisfy condition (3) in Theorem 2. Let $Q^o_{\mathcal{F}^i} \subseteq Q_{\mathcal{F}^i}$ be a set of discrete states that make a cycle in $Q_{\mathcal{F}^i}$ and there exists $q' \in Q - Q_{\mathcal{F}^i}$ such that $q' \in Amb(q)$ for some $q \in Q^o_{\mathcal{F}^i}$. Also let $Q^O_{\mathcal{F}^i}$ be the set of all these state sets. We compute a set of isolators to distinguish one of the states $q \in Q^o_{\mathcal{F}^i}$ from the state $q' \in Amb(q)$. If a $q|q'$-distinguisher exists, we add this set to $\mathbf{IS}^{F^i}$. If there exists a cycle $Q^o_{\mathcal{F}^i}$ such that for all $q \in Q^o_{\mathcal{F}^i}$ no $q|q'$-distinguisher exists, F^i remains undiagnosable. Finally, by using a top-down algorithm, we compute a minimal set $\mathbf{IS}^{F^i}_{min}$.

Let $Q^o_{N,\overline{\mathcal{F}^i}} \subseteq Q - Q_{\mathcal{F}^i}$ be a set of discrete states that make a cycle in $Q - Q_{\mathcal{F}^i}$ and there exists $q \in Q_{\mathcal{F}^i}$ such that $q' \in Amb(q)$ for some $q' \in Q^o_{N,\overline{\mathcal{F}^i}}$, and let $Q^O_{N,\overline{\mathcal{F}^i}}$ be the set of all these state sets. We are now in a position to formally present our procedure.

```
Procedure: Given sets $Q^C_{\mathcal{F}^i}$, $Q^O_{\mathcal{F}^i}$ and $Q^O_{N,\overline{\mathcal{F}^i}}$
    Call Initialization
    Call VerifyCon1
    Call VerifyCon2
    Call VerifyCon3
    Call Top_downProc
End (Procedure)
Procedure Initialization
    $\mathbf{IS}^{F^i}_{Min} = \emptyset$, $\mathbf{IS}^{F^i} = \emptyset$
End (Procedure Initialization)
Procedure VerifyCon1
    For all $q' \in Q - Q_{\mathcal{F}^i}$
        For all $q \in Q_{\mathcal{F}^i}$
            If $\lambda(q) = \lambda(q')$ and $q \in Q^{inf}$
                Compute $\mathbf{SDS}(\{q\}|\{q'\})$
                If $\mathbf{SDS}(\{q\}|\{q'\}) = \emptyset$
                    $F^i$ is not diagnosable
                    End of Procedure
                END (If)
                $\mathbf{IS}^{F^i} = \mathbf{IS}^{F^i} \bigcup \mathbf{IS}$ for one $\mathbf{IS} \in \mathbf{SDS}(\{q\}|\{q'\})$
            END (If)
        End (For)
    End (For)
End (Procedure VerifyCon1)
Procedure VerifyCon2
    For all $q' \in Q - Q_{\mathcal{F}^i}$
        $Q(q') = \{Q^c_{\mathcal{F}^i} \mid Q^c_{\mathcal{F}^i} \in Q^C_{\mathcal{F}^i}$ and $\lambda(q') = \lambda(Q^c_{\mathcal{F}^i})\}$
        For all $q \in Q_{\mathcal{F}^i}$
            If $\lambda(q) = \lambda(q')$ and $q \in Q^c_{\mathcal{F}^i}$ for some $Q^c_{\mathcal{F}^i} \in Q^C_{\mathcal{F}^i}$
                Compute $\mathbf{SDS}(\{q\}|\{q'\})$
                $\mathbf{IS}^{F^i} = \mathbf{IS}^{F^i} \bigcup \mathbf{IS}$ for one $\mathbf{IS} \in \mathbf{SDS}(\{q\}|\{q'\})$
                $Q(q') = Q(q') - \{Q^c_{\mathcal{F}^i} \mid Q^c_{\mathcal{F}^i} \in Q^C_{\mathcal{F}^i}$ and $q \in Q^c_{\mathcal{F}^i}\}$
            End (If)
        End (For)
        If $Q(q') \neq \emptyset$
            $F^i$ is not diagnosable
            End of Procedure
        END (If)
    End (For)
```

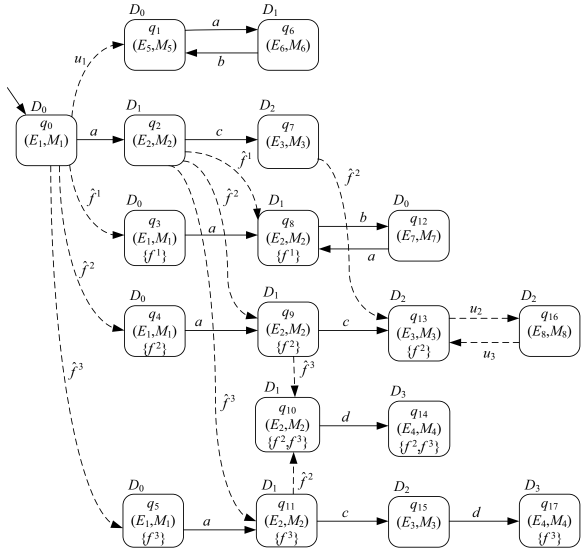


Fig. 2. The DES abstraction of a hybrid automaton with three failure modes.

```
End (Procedure VerifyCon2)
Procedure VerifyCon3
    For all $q' \in Q - Q_{\mathcal{F}^i}$
        For all $q \in Q_{\mathcal{F}^i}$
            If $\lambda(q) = \lambda(q')$ and $q' \in Amb(q)$ and
            $\{Q^o_{N,\overline{\mathcal{F}^i}} \mid Q^o_{N,\overline{\mathcal{F}^i}} \in Q^O_{N,\overline{\mathcal{F}^i}}$ and $q' \in Q^o_{N,\overline{\mathcal{F}^i}}\} \neq \emptyset$
                Compute $\mathbf{SDS}(\{q\}|\{q'\})$
                $\mathbf{IS}^{F^i} = \mathbf{IS}^{F^i} \bigcup \mathbf{IS}$ for one $\mathbf{IS} \in \mathbf{SDS}(\{q\}|\{q'\})$
                $Q^O_{N,\overline{\mathcal{F}^i}} = Q^O_{N,\overline{\mathcal{F}^i}} - \{Q^o_{N,\overline{\mathcal{F}^i}} \mid q' \in Q^o_{N,\overline{\mathcal{F}^i}}\}$
            End (If)
        End (For)
    End (For)
    If $Q^O_{N,\overline{\mathcal{F}^i}} \neq \emptyset$
        $F^i$ is not diagnosable
        End of Procedure
    END (If)
End (Procedure VerifyCon3)
Procedure Top_downProc
    For all $Is \in \mathbf{IS}^{F^i}$
        $\mathbf{IS}^{F^i} = \mathbf{IS}^{F^i} - \{Is\}$
        Check the conditions of Theorem 2 for $\tilde{H}(\mathbf{IS}^{F^i})$
        If $\mathbf{IS}^{F^i} \notin \mathbf{SIS}^{F^i}$ (conditions of Theorem 2 fail)
            $\mathbf{IS}^{F^i} = \mathbf{IS}^{F^i} \bigcup \{Is\}$
        End (If)
    End (For)
    $\mathbf{IS}^{F^i}_{min} = \mathbf{IS}^{F^i}$
End (Procedure Top_downProc)
```

Example: 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 transitions labeled with the events $\hat{f}^1$, $\hat{f}^2$ and $\hat{f}^3$, respectively. Unobservable events are shown with dashed lines. Suppose $Q^{inf} = \{q_{14}, q_{17}\}$ and $\mathbf{IS}_{tot} = \{Is^{Q^{E_1M_1}}(\{f^1, f^3\})$, $Is^{Q^{E_1M_1}}(\{f^1, f^2, f^3\})$, $Is^{Q^{E_2M_2}}(\{f^3\})$, $Is^{Q^{E_2M_2}}(\{f^1, f^2\})$, $Is^{Q^{E_2M_2}}(\{f^2, f^3\})$, $Is^{Q^{E_2M_2}}(\{f^1, f^2, f^3\})$, $Is^{Q^{E_3M_3}}(\{f^2\})$, $Is^{Q^{E_4M_4}}(\{f^2\})$, $Is^{Q^{E_4M_4}}(\{f^3\})$, $Is^{Q^{E_4M_4}}(\{f^2, f^3\})\}$. The set of discrete outputs of the system is: $D = \{D_0, D_1, D_2, D_3\}$. Let z_0 be the initial state of the diagnoser designed for H_{abs}. Assuming $z_0 = Q$, none of the failure modes are diagnosable using the diagnoser designed for H_{abs}.

In order to make F^1 diagnosable, we need to use isolators that make changes in the output sequence generated by the system when the system enters the cycle of states q_8 and q_{12} to distinguish the failure mode F^1 from the normal condition. Thus we need a $q_8|q_6$-distinguisher or a $q_{12}|q_1$-distinguisher to make F^1 diagnosable. We can verify that $\mathbf{SDS}(\{q_8\}|\{q_6\}) = \{\{Is^{Q^{E_2M_2}}(\{f^2, f^3\})\}$, $\{Is^{Q^{E_2M_2}}(\{f^3\})\}, \{Is^{Q^{E_2M_2}}(\{f^2, f^3\}), Is^{Q^{E_2M_2}}(\{f^3\})\}\}$ and $\mathbf{SDS}(\{q_{12}\}|\{q_1\}) = \emptyset$. Therefore, $\mathbf{SIS}^{F^1} = \mathbf{SDS}(\{q_8\}|\{q_6\})$, and $\mathbf{IS}^{F^1}_{min} = \{Is^{Q^{E_2M_2}}(\{f^3\})\}$. For making F^2 diagnosable, we need a $q_{13}|\{q_7, q_{15}\}$-distinguisher. We can verify that $\mathbf{SDS}(\{q_{13}\}|\{q_7, q_{15}\}) = \mathbf{SDS}(\{q_{13}\}|\{q_7\}) \bigcap \mathbf{SDS}(\{q_{13}\}|\{q_{15}\}) = \{\{Is^{Q^{E_3M_3}}(\{f^2\})\}\}$. Moreover, $q_{14} \in Q^{inf}$ but the system generates the same output when only F^3 has occurred and the system is in q_{17}. We can verify that $\mathbf{SDS}(\{q_{14}\}|\{q_{17}\}) = \{\{Is^{Q^{E_4M_4}}(\{f^2\})\}\}$. Therefore, $\mathbf{IS}^{F^2}_{min} = \mathbf{SIS}^{F^2} = \{\{Is^{Q^{E_3M_3}}(\{f^2\}), Is^{Q^{E_4M_4}}(\{f^2\})\}\}$. For making F^3 diagnosable, we need to use $q_{14}|q_{17}$-distinguisher. As explained above, the isolator $Is^{Q^{E_4M_4}}(\{f^2\})$ can distinguish q_{14} from q_{17}. Therefore, $\mathbf{SIS}^{F^3}_{min} = \mathbf{SIS}^{F^3} = \{\{Is^{Q^{E_4M_4}}(\{f^2\})\}\}$. ■

IV. Fault Diagnosis in the Presence of Unreliable Isolators

So far, we have assumed that isolators function without error. However, in practice, isolators may generate incorrect output (error). In some cases, when the residual should be zero, due to noise and modeling uncertainty, a nonzero residual close to the threshold may be generated which triggers a false alarm. Some times even in the presence of failures, the residual does not reach the threshold because of the interference by noise or modeling uncertainty. In this work, we assume that the generation of incorrect output by the isolators is intermittent implying that an isolator may generate incorrect output every now and then.

A. Problem Formulation

Given a set of b unreliable isolators $\mathbf{IS}_{tot} = \{Is_1, \cdots, Is_b\}$ designed for the system, and assuming that at any given time up to $k_{sim} \leq b$ isolators may generate incorrect output simultaneously, we want to investigate if there are sufficient redundant information from isolators and discrete sensors to make a failure mode F diagnosable in the EDESA of the system and isolators.

In the following, we develop a systematic approach for fault diagnosis in the presence of unreliable isolators. In this approach, we first modify the model of an isolator to take into account potential isolator errors. Then, we construct the EDESA for the system and isolators. Diagnosability of the failure modes will be verified in the EDESA of the hybrid system and isolators similar to that described in [6].

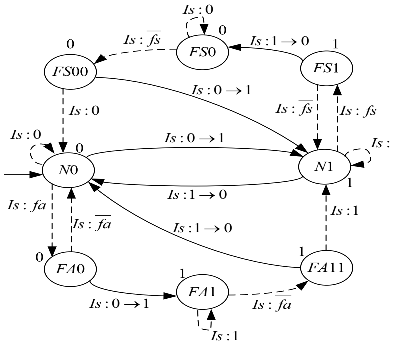


Fig. 3. A finite state automaton modeling an unreliable isolator.

B. Modeling Unreliable Isolators

In general, an isolator may generate incorrect output in two cases: 1) The isolator must produce zero (no fault) but it produces one (fault present). In this case, the output of the isolator is called a **false alarm**; 2) The isolator must produce one (fault present) but it produces zero (no fault). In this case, the output of the isolator is called a **false silence**.

We modify the model of a residual generator to include these two types of errors. Let Is be an unreliable isolator. Fig. 3 shows the FSA modeling Is with unreliable behavior. The isolator has three modes of operation: normal, false alarm and false silence. The generation of incorrect output by the isolator is modeled by the occurrence of unobservable events. The unobservable event '$Is : fa$' labels the transition from normal to false alarm mode, and the unobservable event '$Is : fs$' labels the transition from normal to false silence mode. Isolator errors are assumed intermittent. Therefore, the isolator may have a transition from false alarm mode or false silence mode to normal. Both of these transitions are assumed unobservable. The transition of the isolator from false alarm mode to normal mode is labeled by the unobservable event '$Is : \overline{fa}$', and the transition of the isolator from false alarm mode to normal mode is labeled by the unobservable event '$Is : \overline{fs}$'.

Let Σ^{Is_i} be the event set of the FSA model of the isolator Is_i for $1 \leq i \leq b$: $\Sigma^{Is_i} = \{Is_i : 0 \rightarrow 1, Is_i : 1 \rightarrow 0, Is_i : 0, Is_i : 1, Is_i : fa, Is_i : \overline{fa}, Is_i : fs, Is_i : \overline{fs}\}$. Also, let $\Sigma_N^{Is_i} = \{Is_i : 0 \rightarrow 1, Is_i : 1 \rightarrow 0, Is_i : 0, Is_i : 1\}$, $\Sigma_{ur}^{Is_i} = \{Is_i : fa, Is_i : fs\}$ and $\Sigma_{\overline{ur}}^{Is_i} = \{Is_i : \overline{fa}, Is_i : \overline{fs}\}$. We define $\Sigma_{ur}^{\mathbf{IS}_{tot}}$ and $\Sigma_{\overline{ur}}^{\mathbf{IS}_{tot}}$ as follows: $\Sigma_{ur}^{\mathbf{IS}_{tot}} = \bigcup\limits_{Is_i \in \mathbf{IS}_{tot}} \Sigma_{ur}^{Is_i}$, $\Sigma_{\overline{ur}}^{\mathbf{IS}_{tot}} = \bigcup\limits_{Is_i \in \mathbf{IS}_{tot}} \Sigma_{\overline{ur}}^{Is_i}$.

C. Constructing the EDESA of the System and Isolators in the Presence of Unreliable Isolators

The assumption that at any given time up to $k_{sim} \leq s$ isolators may generate incorrect output simultaneously can be enforced by an FSA denoted by $ASM_{k_{sim}}$. Fig. 4 shows the FSA enforcing this assumption for the case that $k_{sim} = 3$.

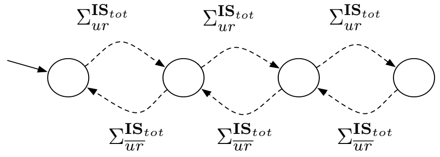

$\Sigma_{ur}^{\mathbf{IS}_{tot}}$
$\Sigma_{ur}^{\mathbf{IS}_{tot}}$
$\Sigma_{ur}^{\mathbf{IS}_{tot}}$
$\Sigma_{\overline{ur}}^{\mathbf{IS}_{tot}}$
$\Sigma_{\overline{ur}}^{\mathbf{IS}_{tot}}$
$\Sigma_{\overline{ur}}^{\mathbf{IS}_{tot}}$

Fig. 4. Finite state automaton $ASM_{k_{sim}}$ for the case that $k_{sim} = 3$.

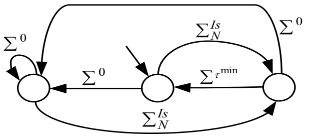


Fig. 5. Finite state automaton ASM_{Is}^{ur}.

The FSA ASM_{Is}^{ur}, as shown in Fig. 5, enforces the assumption that one event of Is (not considering events introduced for modeling isolator errors, i.e, $Is : fa$, $Is : \overline{fa}$, $Is : fs$ and $Is : \overline{fs}$) must occur before any event of $\Sigma^{\tau^{min}}$ occurs.

Let $\overline{IS} = \overline{Is}_1 || \cdots || \overline{Is}_b$. The EDESA of the hybrid system and isolators, denoted by $\tilde{H}$, is an FSA which is constructed as: $\tilde{H} = H_{abs} || \overline{IS} || ASM_{k_{sim}} || ASM^{ur}$, where $ASM^{ur} = ASM_{Is_1}^{ur} || \cdots || ASM_{Is_b}^{ur}$.

A DES diagnoser is designed for the EDESA of the hybrid system and isolators based on the method described in [3]. Diagnosability of the failure modes will be verified in the EDESA similar to the approach in [6].

V. CONCLUSIONS

In this paper, the problem of residual generator selection in hybrid automata is investigated. Necessary and sufficient conditions for residual generator selections have been provided and a procedure has been developed to determine a minimal set of residual generators so that a failure mode becomes diagnosable in the extended DES model of the hybrid system and the set of residual generators. Furthermore, diagnosis of hybrid automata is studied in the case that some residual generators generate incorrect data as false alarm and false silence signals.

REFERENCES

[1] L. Aguirre-Salas, "Sensor selection for observability in interpreted petri nets: a genetic approach," *Proc. of the 42nd IEEE Conference on Decision and Control*, Maui, Hawaii USA, vol. 6, pp. 3760-3765, 2003.

[2] 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.

[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] 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.

[5] 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.

[6] R. Mohammadi, S. Hashtrudi-Zad, and K. Khorasani, "Diagnosis of hybrid systems: Part 1- Diagnosability," Proc. of *the IEEE Conf. on Sys., Man and Cyber.*, San Antonio, TX, USA, 2009.

[7] J. Pan and S. Hashtrudi-Zad, "Diagnosability analysis and sensor selection in discrete event systems with permanent failures," *Proc. of IEEE Conf. on Aut. Sci. and Eng.*, Scottsdale, AZ, USA, pp. 869-874, 2007.