A Hybrid Fault Detection and Isolation Strategy for Nonlinear Systems In Presence of Large Environmental Disturbances

Journal:	*IET Control Theory & Applications*
Manuscript ID:	CTA-2009-0294
Manuscript Type:	Regular Paper
Date Submitted by the Author:	11-Jun-2009
Complete List of Authors:	Nader, Meskin; Concordia University, Electrical and Computer Engineering Khorasani, K.; Concordia University, Dept of Electrical & Computer Eng'g Rabbath, Camille Alain; Defence R&D Canada, Precision Weapons
Keyword:	Fault/Change Detection, Nonlinear Systems, Hybrid Systems, Aerospace Applications

A Hybrid Fault Detection and Isolation Strategy for Nonlinear Systems In Presence of Large Environmental Disturbances

N. Meskin, K. Khorasani, and C. A. Rabbath

Abstract

In this paper, the problem of designing and developing a hybrid Fault Detection and Isolation (FDI) scheme for a nonlinear system that is subject to large environmental disturbances is investigated. In the proposed FDI algorithm, a hybrid architecture is introduced which is composed of a bank of residual generators and a Discrete-Event System (DES) fault diagnoser. A novel set of residuals is generated so that a DES fault diagnoser will robustly detect and isolate actuator faults in the system by incorporating an appropriate combination of residuals and their sequential features. Necessary and sufficient conditions for existence of a set of residuals that are used by the DES fault diagnoser is derived based on the nonlinear geometric FDI approach. Our proposed hybrid FDI algorithm is then applied to actuator fault detection and isolation of an Almost-Lighter-Than-Air-Vehicle (ALTAV). Simulation results presented demonstrate and validate the performance capabilities of our proposed hybrid FDI algorithm.

I. INTRODUCTION

One of the important issues in model-based FDI schemes is their robustness performance against environmental disturbances and modeling errors. One way to design robust FDI algorithms is to consider disturbance inputs as faults and use the developed FDI algorithms in [1],

N. Meskin and K. Khorasani are with the Department of Electrical and Computer Engineering, Concordia University, Montreal, Quebec, H3G 1M8 Canada (Email: {n_meskin,kash}@ece.concordia.ca).

C. A. Rabbath is with the Department of National Defence, Defence Research and Development Canada (DRDC), Valcartier, 2459 boul, Pie XI North, Quebec, Canada.

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

[2] for generating residuals that are decoupled from disturbance inputs. However, one may not always be able to consider disturbance inputs as faults since this will limit the number of faults that can be detected and isolated in the system. Another approach is to use the game theoretic or nonlinear H_∞ approaches to attenuate the effects of disturbances on the residuals. However, design of a robust nonlinear observer based on these approaches needs the solution to a complex set of partial differential equations [3], [4].

In this paper, a novel hybrid FDI algorithm for a nonlinear system that is subject to *large* environmental *disturbances* is developed. Many modern systems such as aircraft and balloons are expected to operate in harsh environments where large disturbances (wind gust) may be present. One of the main challenges in designing a robust FDI algorithm for these systems is to determine how to distinguish between large environmental disturbances and faults or failures. In this paper, we introduce a hybrid diagnosis approach to tackle this problem for actuator faults. Towards this end, a hybrid architecture for robust FDI is introduced that is composed of a bank of continuous-time residual generators and a DES fault diagnoser. First a set of residuals is generated for a family of fault signatures with a given isolability index (defined subsequently). Two threshold levels are assigned to the residuals. It is further assumed that the external disturbances can be categorized into two families, namely, the tolerable disturbance inputs and the large and unexpected disturbances. The first level of threshold is selected such that using the residuals the tolerable disturbance inputs do not generate any false alarms. Next, a complementary set of residuals is generated by considering the effects of disturbances on the first set of generated residuals. A DES fault diagnoser is then designed to invoke an appropriate combination of the residuals and their sequential features to not only detect and isolate faults and guarantee no false alarms but also to detect and identify the occurrence of *large* external *disturbances*.

It should be emphasized that our proposed FDI approach achieves simultaneous robust fault detection and isolation as well as large and unexpected disturbance detection without imposing any limitations on the total number of faults that can be detected and isolated. In contrast, in the previous FDI algorithms developed in [1], [2], [5], the residuals are decoupled from the disturbance inputs. However, the number of output measurements may not be sufficient with respect to the number of faults and disturbances, and therefore one may not be able to achieve disturbance decoupling as well as fault detection and isolation properties simultaneously.

Our proposed hybrid FDI algorithm is finally applied to actuators fault detection and isolation problem in an Almost-Lighter-Than-Air-Vehicle (ALTAV) system. The ALTAVs use buoyancy to float in the air complemented by the use of four motors to generate sufficient lift forces. The Quanser ALTAV [6], [7] system provides a platform to demonstrate and validate fault diagnosis algorithms for a fleet of unmanned aerial vehicles. The ALTAV system that is used for simulation studies in this paper (as well as in real world experiments), has six degrees of freedom, in which translational and rotational motions are described by six variables, and four control inputs are available corresponding to four motors on the vehicle. The presence of both single and multiple simultaneous faults in the vehicle's four input channels are shown to be detected and isolated by using our proposed FDI method. Moreover, it is shown that no false alarms are generated due to wind disturbances and changes in the buoyant force of the ALTAV system. Preliminary results of our proposed FDI scheme for the ALTAV system are presented in [8].

The remainder of this paper is organized as follows. In Section II, the nonlinear geometric fault detection and isolation (FDI) approach of [1] is briefly reviewed and the notion of the structured fault detection and isolation for nonlinear systems is introduced. Our hybrid FDI algorithm for a nonlinear system that is subject to large disturbances is developed and presented in Section III. The proposed FDI algorithm is then applied to a nonlinear ALTAV system in Section IV. Simulation results corresponding to different fault scenarios are provided in Section V. Conclusions and future work are presented in Section VI.

The following notation is used throughout the paper. For any positive integer k, $\mathbf{k}$ denotes the finite set $\{1, 2, \cdots, k\}$. For a given set $\mathbf{n}$, a *combination* is an un-ordered collection of the elements of $\mathbf{n}$ and is a subset of $\mathbf{n}$. The order of the elements in a combination is not important and the elements cannot be repeated. $C(n, k)$ denotes a number of k combinations (k-subset) of $\mathbf{n}$ which is equal to $\frac{n!}{k!(n-k)!}$, and T^*X denotes the co-tangent space of the manifold X and $\bar{\mathcal{L}}$ denotes the involutive closure of the distribution $\mathcal{L}$.

II. Structured Fault Detection and Isolation for Nonlinear Systems

Consider a general class of nonlinear systems that is described by the following model

$$\dot{x} = f(x) + g(x)u + \sum_{i=1}^{k} l_i(x)m_i$$
$$y = h(x) \tag{1}$$

with the state x defined in a neighborhood $\mathcal{X}$ of the origin in $\mathbb{R}^n$; the input is denoted by $u \in \mathbb{R}^m$; the output is denoted by $y \in \mathbb{R}^q$; the fault modes are denoted by $m_i \in \mathbb{R}^{k_i}$, $l_i(x)$'s are the fault signatures, $f(x)$, $g(x)$ and $l_i(x)$'s are smooth vector fields, $h(x)$ is a nonlinear smooth mapping, and $f(0) = 0, h(0) = 0$. It is assumed that $span\{l_i^1(x), ..., l_i^{k_i}(x)\}, i \in \mathbf{k}$ is nonsingular where l_i^j denotes the j-th column of l_i. It should be emphasized that the fault modes m_i can be both time-dependent and state dependent.

The Structured Fault Detection and Isolation Problem (SFDIP) as introduced in [9] for linear systems is defined formally as design of a dynamic residual generator that takes the observables $u(t)$ and $y(t)$ as inputs and generates a set of ξ residuals $r_j(t), j \in \Xi = \{1, ..., \xi\}$ with the following properties: **a)** when no failure is present, all the residuals $r_j(t)$ decay asymptotically to zero, and **b)** for each fault signal $m_i(t)$, the residuals $r_j(t)$, $j \in \Omega_i \subset \Xi$, are affected by $m_i(t)$, and the other residuals $r_\alpha(t)$, $\alpha \in \Xi - \Omega_i$, are decoupled from this fault.

The prespecified family of the *coding sets* $\Omega_i \subseteq \Xi, i \in \mathbf{k}$ should be chosen such that by knowing which $r_j(t)$ is zero and which ones are not, one can uniquely identify the fault. The resulting residual set which has the corresponding required sensitivity to specific faults and insensitivity to others is known as the *structured residual set* [10]. For detecting all possible faults in the system, no coding set should be empty. The minimum requirement for fault isolation is that all the coding sets be distinct. Coding sets satisfying the above two requirements are defined as *weakly isolating*. The weakly isolating coding sets $\Omega_i, i \in \mathbf{k}$ is defined as being *strongly isolating* if for each $i, j \in \mathbf{k}$, $i \neq j$, $\Omega_i \not\subseteq \Omega_j$. A strongly isolating coding set prevents incorrect fault detection when some of the residuals in Ω_i do not exceed the respective thresholds while the others do. For the given coding sets $\Omega_i, i \in \mathbf{k}$, the finite set $\Gamma_j \subset \mathbf{k}, j \in \Xi$ is defined as the collection of all $i \in \mathbf{k}$ for which the i-th failure mode affects the j-th residual, i.e. $\Gamma_j = \{i \in \mathbf{k} | j \in \Omega_i\}$.

In the nonlinear fundamental problem in residual generation (*I*NFPRG) introduced in [1], the family of the coding sets was chosen as $\Omega_i = \{i\}$. This family of coding sets is also called a *dedicated residual set* [11]. In this coding scheme, one needs to design a set of filters which generates k residuals $r_i(t), i \in \mathbf{k}$ such that the fault in the i-th component l_i can only affect the residual $r_i(t)$ and no other residuals $r_j(t) (i \neq j)$. With this coding scheme one can detect and isolate multiple faults in all channels.

The solvability conditions for the *I*NFPRG was obtained in [1]. Let for a given distribution $\mathcal{L}$, the largest conditioned invariant distribution which contains $\mathcal{L}$ be denoted by $\Sigma_*^{\mathcal{L}}$ and the largest codistribution contained in $\mathcal{L}^\perp$ as o.c.a.$((\Sigma_*^{\mathcal{L}})^\perp)$. The *l*NFPRG has then a solution only if there exist observability codistributions $\Pi_i^* =$ o.c.a.$((\Sigma_*^{\mathcal{L}_i})^\perp)$ such that $(span\{l_i\})^\perp + \Pi_i^* = T^*X$ where $\mathcal{L}_i = \text{span}\{l_1(x), ..., l_{i-1}(x), l_{i+1}(x), ..., l_m(x)\}$. If the observability codistribution Π_i^* exists, one can find a coordinate transformation such that the subsystem of the new system in the new local coordinates, denoted by the z_1-subsystem [1], is only affected by $m_i(t)$ and is decoupled from others. However, the existence of the observability codistribution Π_i^* is not sufficient to guarantee that a state observer can be built for the z_1-subsystem. To guarantee the existence of a state observer, extra assumptions are needed (Assumption III in [1]). We are now in a position to state our first result.

Theorem 2.1: For a given family of the coding sets, the SFDIP problem has a solution only if $\text{span}\{l_i\} \nsubseteq [\Pi_j^*]^\perp,\ i \in \Gamma_j$ where $\Pi_j^* =$ o.c.a.$((\Sigma_*^{\mathcal{L}_{\Gamma_j}})^\perp)$ and $\mathcal{L}_{\Gamma_j} = \text{span}\{l_i(x), i \notin \Gamma_j\},\ j \in \Xi$.

Proof: According to [1], the SFDIP problem can be solved as ξ separate *l*NFPRG problems. Each residual $r_j(t), j \in \Xi$ can be generated by applying the *l*NFPRG results to the following model

$$\dot{x}(t) = f(x) + g(x)u(t) + \bar{l}_1(x)\bar{m}_1(t) + \bar{l}_2(x)\bar{m}_2(t)$$
$$y(t) = h(x)$$

where $\bar{l}_1(x) = \{l_i(x) | i \in \Gamma_j\}$, $\bar{l}_2(x) = \{l_i(x) | i \in \mathbf{k} - \Gamma_j\}$, $\bar{m}_1 = \{m_i | i \in \Gamma_j\}$ and $\bar{m}_2 = \{m_i | i \in \mathbf{k} - \Gamma_j\}$. This completes the proof of the theorem. ∎

It is clear that similar extra assumptions as in [1] are required for the design of state observers as the residual signal generators in SFDIP. A family of fault signatures that satisfies the *l*NFPRG conditions above where $\Omega_i = \{i\}$ is said to be *strongly detectable*. It follows that a necessary condition for existence of a solution to the *l*NFPRG is that $\text{Rank}\{l_1(x), l_2(x)\ , ..., l_k(x)\} = \sum_{i=1}^k k_i,\ \forall x \in \mathcal{X}$ which implies that there should be no dependency among the fault signatures. Recently in [12], a new coding set is introduced for the family of fault signatures that are not *strongly detectable*. It is clear that for a family of fault signatures that is not strongly detectable, one <u>cannot</u> detect and isolate multiple faults in all channels. To formalize our results, the following isolability index is introduced next.

Definition 1: For system (1) with a family of fault signatures $l_i(x), i \in \mathbf{k}$, the *isolability index* μ is defined as the maximum value of multiple simultaneous faults that can be detected and isolated.

It is clear that the weakly isolating coding sets Ω_i's that can be used for detecting and isolating the occurrence of up to μ multiple faults should have the following property that for each two different $1 \le l, h \le \mu$ combinations $l_{i_1}(x), ..., l_{i_l}(x)$ and $l_{j_1}(x), ..., l_{j_h}(x)$ of L_i's,

$$\Omega_{i_1 i_2 \dots i_l} \neq \Omega_{j_1 j_2 \dots j_h} \tag{2}$$

where for each l combination $l_{i_1}, ..., l_{i_l}$ of l_i's, $\Omega_{i_1 i_2 \dots i_l} = \bigcup_{j=i_1}^{i_l} \Omega_j$. Moreover, in order to prevent false fault isolation, it is desirable to have strongly isolating coding sets $\Omega_{i_1 i_2 \dots i_l}$ as defined below.

***Definition** 2:* The coding sets that satisfy the condition (2) are said to be strongly isolating with index μ if for each two different $1 \le l \le \mu$ combination $l_{i_1}, ..., l_{i_l}$ and $l_{j_1}, ..., l_{j_l}$ of l_i's, $\Omega_{i_1 i_2 \dots i_l} \not\subseteq \Omega_{j_1 j_2 \dots j_l}$ and $\Omega_{i_1 i_2 \dots i_l} \not\supseteq \Omega_{j_1 j_2 \dots j_l}$. Moreover, if the SFDIP problem for a given family of fault signatures has a solution for a strongly isolating coding set with index μ, then we call the isolability index of that family as the strongly isolability index μ.

***Lemma** 2.2:* The strong isolability index μ of a given family of fault signatures is either $\mu = k$ or $\mu < k - 1$.

Proof: Let $\Omega_i, i \in \mathbf{k}$ be strongly isolating with index $\mu = k - 1$. Consider that concurrent faults have occurred in all fault signatures. Since Ω_i's are weakly isolating (none of them is empty), all residuals will be affected by these concurrent faults. Moreover, since the strong isolability of fault signatures is μ, it is clear that for each $k-1$ combination $l_{i_1}(x), ..., l_{i_{k-1}}(x)$ of l_i's, we have $\Omega_{i_1 i_2 \dots i_{k-1}} \neq \Omega_{1,\dots,k} = \bigcup_{j=1}^{k} \Omega_j$. Therefore, one can also detect if there exist concurrent faults in all channels. Moreover, by assumption one can detect and isolate up to $k - 1$ concurrent faults. Consequently, we have $\mu = k$. ■

It should be emphasized that not every coding set satisfying condition (2) is strongly isolating with index μ. For instance, consider the coding sets $\Omega_1 = \{1, 2\}$, $\Omega_2 = \{3, 4\}$ and $\Omega_3 = \{2, 3\}$. It can easily be verified that these coding sets satisfy the condition (2) with $\mu = 2$ but they are not strongly isolating with index 2. Indeed it is clear that $\Omega_{2,3} \subset \Omega_{1,2}$. Since strong isolability index is more desirable and it prevents incorrect detection and isolation, we will focus on strong isolability index. The next theorem illustrates how one can construct coding sets that have the strong isolability index $\mu < k - 1$.

***Theorem** 2.3:* Let $\Gamma_j, j \in \Xi$ be defined as the $k - \mu$ combinations of the set $\mathbf{k}$. The corresponding sets $\Omega_i, i \in \mathbf{k}$ defined as $\Omega_i = \{j \in \Xi | i \in \Gamma_j\}$ are then strongly isolating with index

μ.

Proof: Consider two different $1 \leq l, h \leq \mu$ combinations $i_1, ..., i_l$ and $j_1, ..., j_h$ of the set $\mathbf{k}$. In order to show that equation (2) holds it is sufficient to show that the complement sets $\Xi - \Omega_{i_1 i_2 \ldots i_l}$ and $\Xi - \Omega_{j_1 j_2 \ldots j_h}$ are not equal where

$$\Xi - \Omega_{i_1 i_2 \ldots i_l} = \{j \in \Xi | i_k \notin \Gamma_j, \ \forall i_k \in \{i_1, ..., i_l\}\} \tag{3}$$

Assume that $l \leq h$. Since two combinations $i_1, ..., i_l$ and $j_1, ..., j_h$ are different, there exists $j_t \in \{j_1, ..., j_h\}$ such that $j_t \in \mathbf{k} - \{i_1, i_2, ..., i_l\}$. Since the sets $\Gamma_j, j \in \Xi$ are defined as $k - \mu$ combinations of the set $\mathbf{k}$ and $l \leq \mu$, there exists a combination Γ_j such that $j_t \in \Gamma_j$ and $i_k \notin \Gamma_j, \ \forall i_k \in \{i_1, ..., i_l\}$, therefore $j \notin \Xi - \Omega_{j_1 j_2 \ldots j_h}$ and $j \in \Xi - \Omega_{i_1 i_2 \ldots i_l}$ which shows that equation (3) holds. The combination Γ_j can be found by first selecting j_t and then selecting $k - \mu - 1$ elements from the set $\mathbf{k} - \{i_1, i_2, ..., i_l, j_t\}$. It is clear that since $l \leq \mu$, then $|\mathbf{k} - \{i_1, i_2, ..., i_l\}| \geq k - \mu$ and one can find the combination Γ_j. Similarly it can be shown that the coding sets Ω_i's satisfies conditions in Definition 2, and hence are strongly isolating.

In order to show that μ is the maximum number of combinations that satisfy equation (2), it should be noted that $|\Xi - \Omega_{i_1 i_2 \ldots i_l}| = C(k - l, k - \mu)$, therefore for $l > \mu$, the set $\Xi - \Omega_{i_1 i_2 \ldots i_l}$ is empty and for any different l combinations $i_1, ..., i_l$ and $j_1, ..., j_l$, we have $\Omega_{i_1 i_2 \ldots i_l} = \Omega_{j_1 j_2 \ldots j_l}$. ■

Theorem 2.4: A necessary condition for the SFDIP problem for the nonlinear system (1) to have a solution for the coding sets introduced in Theorem 2.3 and a given family of fault signatures is that for each $\mu + 1$ combination $l_{i_1}(x), ..., l_{i_{\mu+1}}(x)$ of $l_i(x)$'s, the dimension of distribution $\Delta = \text{span}[l_{i_1}(x), ..., l_{i_{\mu+1}}(x)]$ is $v_i = \sum_{j=1}^{\mu+1} k_{i_j}$.

Proof: If there exists a $\mu + 1$ combination $l_{i_1}(x), ..., l_{i_{\mu+1}}(x)$ of $l_i(x)$'s such that the dimension of distribution $\Delta = \text{span}[l_{i_1}(x), ..., l_{i_{\mu+1}}(x)]$ is less than $v_i = \sum_{j=1}^{\mu+1} k_{i_j}$, then there exists $x \in \mathcal{X}$ such that $l_{i_{\mu+1}}(x) \subset \Delta_i = \text{span}\{l_{i_1}(x), ..., l_{i_\mu}(x)\}$. Due to the fact that the sets Γ_j are defined in Theorem 2.3 as the $k - \mu$ combinations of the set $\mathbf{k}$, one of the sets Γ_j is equal to $\mathbf{k} - \{i_1, i_2, ..., i_\mu\}$ and $\text{span}\{l_{i_{\mu+1}}\} \subset (o.c.a.((\Sigma_*^{\Delta_i})^\perp))^\perp$. ■

The above necessary condition provides a test to determine the possible values of the isolability index for a family of fault signatures. In the next section, based on our introduced strongly isolating coding set with index μ, a hybrid FDI scheme for nonlinear systems is developed that is subjected to *both* large and unexpected disturbances as well as actuator faults where the family of fault signatures is *not* necessarily strongly detectable.

III. HYBRID NONLINEAR FDI APPROACH

Consider the following nonlinear system

$$\dot{x} = f(x) + g(x)u + \sum_{i=1}^{k} l_i(x)m_i + \sum_{l=1}^{P} p_l(x)\omega_l$$
$$y = h(x) + v \qquad (4)$$

where $\omega_l \in \mathbb{R}^{P_l}$ denotes the disturbance inputs, v represents the measurement noise, and $l_i(x)$ represents the actuator fault signatures. It is assumed that $\omega_l, v \in \mathfrak{L}^p[0,\infty]$ for some $1 \leq p \leq \infty$ where $\mathfrak{L}^p[0,\infty]$ denotes the space of $\mathfrak{L}^p$ norm bounded signals, i.e. $||\omega||_p < \infty$.

Assumption 1: The disturbance inputs are categorized into two types, namely tolerable disturbance signals $\mathfrak{D}_1 = \{\omega \in \mathfrak{L}^p[0,\infty] \mid ||\omega||_p < \delta_1\}$ and large and unexpected disturbance signals $\mathfrak{D}_2 = \{\omega \in \mathfrak{L}^p[0,\infty] \mid \delta_1 < ||\omega||_p < \delta_2\}$, where $\delta_1 \ll \delta_2$.

As an example for the ALTAV system that is introduced and described in details in Section IV, the wind disturbance forces (W) can be categorized into two types, namely the regular tolerable wind disturbances that satisfy $W \leq 0.5$ $(Newton)$ and the large unexpected wind gust disturbances that satisfy $0.5 \ll W < 5$ $(Newton)$.

Assumption 2: A given actuator fault and the unexpected large disturbances have not occurred simultaneously and there exists a sufficient time interval between the occurrence of a fault and the disturbances.

Our goal in this paper is to solve the problem of designing a hybrid fault diagnoser (HFD) in order to detect and isolate each fault m_i while guaranteeing that the fault diagnoser remains robust with respect to both types of disturbances described in Assumption 1. In other words, no false alarms should be generated due to disturbances. The hybrid fault diagnoser is composed of two modules, namely, a low-level bank of residual generators and a high-level discrete-event system (DES) diagnoser. The bank of continuous-time residual generators produces first a set of residuals based on the nonlinear geometric FDI approach. It then compares, using an evaluation function, each residual to its corresponding threshold value, from which a set of residual logic units is generated. Two levels of thresholds are needed for certain residuals (this will be discussed in more detail subsequently). The DES diagnoser module is a finite-state automaton that takes the residual logic units as inputs and estimates the current state of the system. For designing such a DES diagnoser, the combined nonlinear plant and the bank of residual generators is modeled

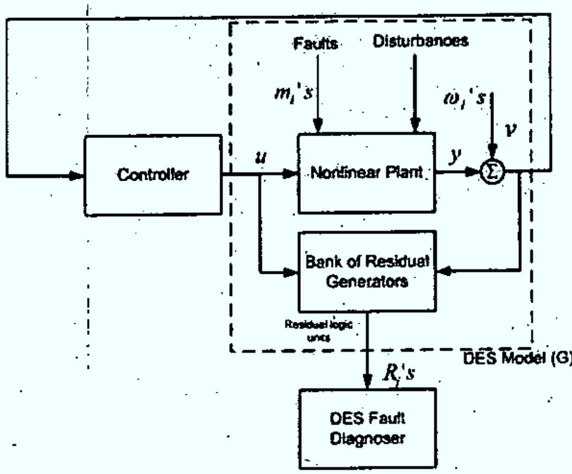

Fig. 1. General architecture of our proposed hybrid diagnoser.

as a finite state Moore automaton (G). The general architecture of our proposed hybrid fault diagnoser is shown in Figure 1.

One possible approach to design a robust FDI algorithm for the nonlinear system (4) is to generate a set of residuals as in [1] where each residual is affected by only one fault and is decoupled from all other faults and all the disturbances. If such a set of residuals exist, then one can robustly detect and isolate faults despite the presence of disturbances. Under this scenario, there will be no need to have a hybrid structure for the fault diagnoser. However, due to availability of limited number of output measurements in practically most realistic situations in comparison to the potentially large number of faults and disturbances, our proposed hybrid fault diagnoser becomes the only available methodology for a general class of nonlinear systems.

In the next section, the procedure for designing a hybrid fault diagnoser that is composed of a bank of residual generators and a DES diagnoser is described in detail.

A. Bank of Continuous-Time Residual Generators

In this section, a systematic approach is proposed to design a set of residual generators that provides the required information for the DES diagnoser. Towards this end, two sets of residuals are developed. The first set is generated according to the coding set that is introduced in Section II for a family of fault signatures with a given isolability index. The hybrid fault diagnoser (HFD) that is developed below is guaranteed to remain robust with respect to both tolerable disturbance inputs ($\omega_l \in \mathfrak{D}_1$) and measurement noise (v) by selecting appropriate threshold values associated with the residuals. To ensure that the HFD is also robust to large disturbance inputs ($\omega_l \in \mathfrak{D}_2$), a second set of complementary residuals is generated so that the DES diagnoser by utilizing the entire two sets of residuals will robustly detect and isolate a fault.

In the following, we assume that the strongly isolability index of l_i's is $\mu \le k$ where as shown in Lemma 2.2, either $\mu = k$ or $\mu < k - 1$. Therefore, the SFDIP problem has a solution for the strongly isolating coding set Ω_i, and a set of $\xi = C(k, \mu)$ residuals $r_j, j \in \Xi$ can be generated. Let us denote $\mathfrak{R}_1 = \{r_j, j \in \Xi\}$. Let Λ_j denote the set of disturbance signatures ω_l's that affect the residual r_j, i.e. $\Lambda_j = \{l \in \mathbf{P} | \text{ span}\{p_l\} \not\subseteq (\Pi_j^*)^\perp\},\ j \in \Xi$ where Π_j^* is defined in Theorem 2.1.

Assume that one can generate a set of complementary residuals $\mathfrak{R}_2 = \{r_{\xi+j}, j \in \Xi\}$ such that $r_{\xi+j}$ is decoupled from the disturbance inputs specified by Λ_j but is affected by all the faults $m_i, i \in \Gamma_j$ and possibly other fault modes. The residuals $r_j \in \mathfrak{R}_2$ can be generated only if there exist the observability codistributions $\Pi_{\xi+j}^* = o.c.a.((\Sigma_*^{\mathcal{L}_{\xi+j}})^\perp), j \in \Xi$ such that $\text{span}\{l_i\} \not\subseteq [\Pi_{\xi+j}^*]^\perp,\ j \in \Xi$ for all $i \in \Gamma_j$ and $\mathcal{L}_{\xi+j} = \text{span}\{p_l(x), l \in \Lambda_j\},\ j \in \Xi$. It should be mentioned that for a system where $\Lambda_j = \Lambda, j \in \Xi$, i.e. the set of disturbances that affects all the residuals $r_i \in \mathfrak{R}_1$ are the same, only a single extra residual $r_{\xi+1}$ is sufficient for designing our hybrid FDI scheme.

For each disturbance input $\omega_l \in \mathbf{P}$ and fault mode $m_i, i \in \mathbf{k}$, the coding sets Ω_l^p and Ω_i^f are defined respectively as

$$\begin{aligned} \Omega_l^p &= \{j \in \{1, ..., 2\xi\} | \text{span}\{p_l\} \not\subseteq (\Pi_j^*)^\perp\} \\ \Omega_i^f &= \Omega_i \cup \Upsilon_i^f \end{aligned} \tag{5}$$

where $\Upsilon_i^f = \{j \in \{\xi + 1, ..., 2\xi\} | \text{span}\{l_i\} \not\subseteq (\Pi_j^*)^\perp\}\}$. In other words, the sets Ω_l^p and Ω_i^f are the index set of those residuals $r_j \in \mathfrak{R}_1 \cup \mathfrak{R}_2$ that are affected by ω_l and m_i, respectively. Figure 2 shows an incidence matrix for a system with three fault signatures and two disturbance inputs where a 1 in the $(i, j)^{th}$ entry indicates that the residual r_j is affected by fault or disturbance, where a 0 indicates that the residual is decoupled from that fault or disturbance, and where an X indicates that the value 1 or 0 is indifferent in the proposed FDI approach. All the sets that are used in this work (Ω_i's, Ω_i^f's, Ω_l^p's, Λ_j's and Υ_i^f) are identified and shown in Figure 2.

Assumption 3: Let $l \notin \cup_{j=1}^k \Lambda_j$ for some disturbance input ω_l, then $\Omega_l^p = \emptyset$.

	f_1	f_2	f_3	ω_1	ω_2
r_1	1	1	0	1	0
r_2	1	0	1	1	1
r_3	0	1	1	0	1
r_4	1	1	X	0	X
r_5	1	X	1	X	0
r_6	X	1	1	0	0

Fig. 2. An incidence matrix.

The disturbances which satisfy Assumption 3 have no effect on the residuals, and therefore the hybrid diagnoser does not need to be robust to them. In other words, the generated set of residuals are already decoupled from these disturbances and no further invoking of the DES diagnoser is required.

In the following example, we demonstrate how to generate the above set of residuals for a given nonlinear system.

Example 1: Consider a nonlinear system that has 3 fault signatures and one disturbance input as governed by the following dynamics

$$\dot{x}_1 = -x_1x_2 + m_1 + exp(x_2)m_2 + 2m_3 + \omega_1$$

$$\dot{x}_2 = -x_1^2 - 2\frac{x_2}{x_1}m_1 + m_2 + 0.5m_3 - 0.2\omega_1$$

with the output measurement $y = [x_1, x_2]'$. It is clear that the above family of fault signatures does not satisfy the necessary condition of the *l*NFPRG, and hence it is not strongly detectable. Therefore, according to Lemma 2.2, the strong isolability index satisfies $\mu < 2$. Now we show that the strong isolability index for the above fault signatures is 1, i.e. $\mu = 1$. First, we generate the coding sets that are required for the family of fault signatures with $\mu = 1$. Towards this end, the sets $\Gamma_j, j = 1, 2, 3$ are selected as 2 combinations of the set $\{1, 2, 3\}$, namely $\Gamma_1 = \{1, 2\}$, $\Gamma_2 = \{1, 3\}$ and $\Gamma_3 = \{2, 3\}$. The corresponding coding sets Ω_i, $i = 1, 2, 3$ are given by $\Omega_1 = \{1, 2\}$, $\Omega_2 = \{1, 3\}$ and $\Omega_3 = \{2, 3\}$ and the number of residuals is $\xi = C(3, 1) = 3$. Our next step involves checking the solvability conditions for the SFDIP problem. According to Theorem 2.1, one needs first to obtain the unobservability codistributions $\Pi_j^*, j = 1, 2, 3$. These codistributions are found by using the algorithm that is presented in [1] and are given as

$\Pi_1^* = \text{span}\{d(x_1 - 4x_2)\}$, $\Pi_2^* = \text{span}\{d(x_1 - exp(x_2))\}$ and $\Pi_3^* = \text{span}\{d(x_1^2 x_2)\}$.

It can be verified that the necessary conditions of Theorem 2.1 are satisfied, and hence the isolability index for the above family of fault signatures is 1. We are now ready to design the residual generators. Towards this end, the z_1-subsystem for generating the residuals $r_j, j = 1, 2, 3$ should be found from the unobservability codistributions $\Pi_j^*, i = 1, 2, 3$. As an illustration, the z_1-subsystem for generating the residual r_1 can be obtained as follows

$$r_1 : \begin{cases} \dot{z}_1 = -2\frac{z_1^2}{y_2} - y_2^4 + (2\frac{z_1}{y_2}exp(\frac{z_1}{y_2^2}) + y_2^2)m_2 + (4\frac{z_1}{y_2} + 0.5y_2^2)m_3 + (2\frac{z_1}{y_2} - 0.2y_2^2)\omega_1 \\ y_1 = z_1 = x_1 - 4x_2, \quad y_2 = x_2 \end{cases}$$

It follows that $\Lambda_j = \Lambda = \{1\}$ (the disturbance input ω_1 affects all the residuals $r_j,\ j = 1, 2, 3$) and only one extra residual is required. To generate this residual, one needs to find Π_4^* that is given by $\Pi_4^* = \text{span}\{d(x_1 + 5x_2)\}$. Consequently, the coding sets Ω_1^p and $\Omega_i^f,\ i = 1, 2, 3$ are determined as follows: $\Omega_1^p = \{1, 2, 3\}$, $\Omega_1^f = \{1, 2, 4\}$, $\Omega_2^f = \{1, 3, 4\}$, and $\Omega_3^f = \{2, 3, 4\}$.

It should be noted that since the above family of fault signatures is not strongly detectable, the method proposed in [1] cannot be applied to this system. Moreover, as a comparison with some methods in the literature that consider disturbances as faults [1], [2], [5], if the disturbance input ω_1 is treated as the fourth fault, the isolability index for the new family of fault signatures (four faults) is 1, implying that one still cannot detect the concurrent occurrence of a fault and a disturbance. However, as will be shown subsequently, our proposed hybrid FDI algorithm enables one to detect a single fault in the system despite the fact that a large disturbance input is applied through ω_1.

Corresponding to each residual $r_j \in \mathfrak{R}_1 \cup \mathfrak{R}_2$, an evaluation function is now assigned. Various evaluation functions have been introduced in the literature [13]. For the residuals $r_j \in \mathfrak{R}_1$, two different thresholds are needed as $J_{th_j}^{\beta} = \sup_{v \in \mathfrak{L}_p, \omega \in \mathfrak{D}_\beta, m_i = 0, i \in k}(J_{r_j})\ j \in \Xi, \beta = 1, 2$. In determining the first threshold, only tolerable disturbance inputs ($\omega_l \in \mathfrak{D}_1$) are considered. However, the second threshold incorporates all the possible disturbance inputs. In other words, the supremum that arises in determining the threshold values $J_{th_j}^1$ and $J_{th_j}^2$ can be obtained from evaluation of J_{r_j} corresponding to and during the healthy operation or simulation of the system by considering the worst case effects of the disturbances ω_l in $\mathfrak{D}_1$ and $\mathfrak{D}_2$, respectively.

It should be noted that one may choose to only consider the threshold level that is given by $J_{th_j}^2$ as the worst case scenario associated with large disturbances. In this case, no false alarms will be generated due to this type of disturbances. However, this may lead to selection of higher threshold values that would unnecessarily reduce the sensitivity of the FDI algorithm to low severity faults. As will be shown subsequently, by selecting two threshold levels and considering the temporal and sequential characteristics of the residuals, one can not only enhance the fault sensitivity characteristics but also design a robust FDI algorithm.

The threshold values for the residuals $r_j \in \mathfrak{R}_2$ are selected according to

$$J^1_{th_j} = \sup_{v \in \mathfrak{L}_p, \omega_l \in \mathfrak{D}_2, i \in \Omega^p_l, m_i = 0, i \in \mathbf{k}} (J_{r_j}), \; j \in \{\xi + 1, ..., 2\xi\}$$

For a system such as in Example 1 and the ALTAV system that is discussed in Section IV, where the residuals $r_j \in \mathfrak{R}_2$ are affected by a few or even no disturbance input channels, one can select lower threshold values for these residuals. In other words, the residuals $r_j \in \mathfrak{R}_2$ are generally less sensitive to the disturbance inputs than the residuals $r_j \in \mathfrak{R}_1$. It should be emphasized that for systems where $\Lambda_j = \Lambda, j \in \Xi$, the residual $r_{\xi+1}$ is decoupled from all disturbance inputs, and hence the threshold values for these residuals are definitely less than the ones for $r_j, j \in \Xi$.

For each residual $r_j \in \mathfrak{R}_1$ defined at a given point in time t, we can choose the corresponding two threshold logic units $R^1_j(t)$ and $R^2_j(t)$ according to

$$R^\beta_j(t) = \begin{cases} 1 & \text{if } J_{r_j}(t) > J^\beta_{th_j} \\ 0 & \text{otherwise} \end{cases}, j \in \Xi, \beta = 1, 2 \tag{6}$$

Similarly, for each residual $r_j(t) \in \mathfrak{R}_2$, the threshold logic unit is assigned as follows

$$R^1_j(t) = \begin{cases} 1 & \text{if } J_{r_j}(t) > J^1_{th_j} \\ 0 & \text{otherwise} \end{cases}, j \in \{\xi + 1, ..., 2\xi\} \tag{7}$$

The definition below describes the classification of faults into three separate classes in view of the threshold logic unit $R^1_j(t)$ that was defined above.

***Definition** 3:* The fault scenarios considered for the nonlinear system (4) are categorized into the following three classes, namely, high severity faults, low severity faults, and non-detectable faults. Their specific characteristics are as follows: (1) the high severity faults correspond to faults that will affect the residual logic units $R^1_j, j \in \{1, ..., 2\xi\}$, (2) the low severity faults correspond to faults that will affect only $R^1_j, j \in \{\xi+1, ..., 2\xi\}$, and (3) the non-detectable faults correspond to faults that do not affect any of the residual logic units $R^1_j, j \in \{1, ..., 2\xi\}$.

B. The DES Fault Diagnoser

For sake of simplicity and without loss of generality, let us assume that multiple faults in two actuators are possible. Furthermore, let us consider the scenario where only concurrent occurrence of one fault and one large disturbance is allowed. This assumption will limit the number of all possible operational states of the DES system. However, our proposed algorithm is easily expandable to more general cases, but due to space limitations is not addressed here.

First, the nonlinear system along with a bank of residual generators is modeled as a finite state Moore automaton [14] that is specified according to $G = (S, \Sigma, \delta, s_0, Y, \lambda)$, where S, Σ, Y are the finite state, event and output sets; s_0 is the initial state, $\delta : S \times \Sigma \to 2^S$ is the transition function, and $\lambda : S \to Y$ is the output map (2^S denotes the power set of S). For the nonlinear system (4), the state set is given by $S = \{s_0, s_1, ..., s_k, s_{1,2}, ..., s_{k-1,k}, s_D, s_{1,D}, ..., s_{k,D}\}$, where the state s_0 corresponds to the normal operational mode of the system (i.e. no fault and no large disturbance input exist), the states s_i, $i \in \mathbf{k}$ correspond to faults in the i-th component, the states $s_{i,j}$, $i, j \in \mathbf{k}, i \neq j$ correspond to multiple faults in the i-th and j-th components, the state s_D corresponds to occurrence of a large disturbance input, and the states $s_{i,D}$ correspond to a concurrent fault in the i-th component and a large disturbance input.

The event set is denoted by $\Sigma = \{\mathcal{F}_1^o, ..., \mathcal{F}_k^o, \mathcal{F}_1^r, ..., \mathcal{F}_k^r, \mathcal{D}^o, \mathcal{D}^r\}$, where the events $\mathcal{F}_i^o$ and $\mathcal{F}_i^r, i \in \mathbf{k}$ correspond to the occurrence and removal of a fault in the i-th actuator, respectively and the event $\mathcal{D}^o$ corresponds to the occurrence of a large disturbance in one of the ω_l, $l \in \mathbf{P}$ channels, and $\mathcal{D}^r$ corresponds to the removal of a disturbance from all the channels. The output set is denoted by $Y = \{(R_1^1, ..., R_{2\xi}^1, R_1^2, ..., R_\xi^2) \in \mathbb{B}^\kappa\}$, where $\mathbb{B} = \{0, 1\}$ and κ can be either $2\xi + 1$ or 3ξ depending on the property of Λ_j. Based on the above definitions, the transition function δ is now defined formally as $\delta(s_0, \mathcal{D}^o) = s_D$, $\delta(s_D, \mathcal{D}^r) = s_0$, $\delta(s_D, \mathcal{F}_i^o) = s_{i,D}$, $\delta(s_0, \mathcal{F}_i^o) = s_i$, $i \in \mathbf{k}$ $\delta(s_i, \mathcal{F}_j^o) = s_{i,j}$, $i, j \in \mathbf{k}, i \neq j$, $\delta(s_i, \mathcal{D}^o) = s_{i,D}$, $\delta(s_i, \mathcal{F}_i^r) = s_0$, $i \in \mathbf{k}$, $\delta(s_{i,j}, \mathcal{F}_i^r) = s_j$, $\delta(s_{i,j}, \mathcal{F}_j^r) = s_i$, $i, j \in \mathbf{k}, i \neq j$ $\delta(s_{i,D}, \mathcal{F}_i^r) = s_D$ and $\delta(s_{i,D}, \mathcal{D}^r) = s_i$. As an illustration, Figure 3 shows the corresponding transition function of the nonlinear system that was considered in Example 1. It should be noted that since for this system the isolability index is $\mu = 1$, multiple fault states are not applicable. As shown in Figure 3, the DES model of the nonlinear system in Example 1 has eight states, namely the normal operational state s_0, three faulty states $s_i, i = 1, 2, 3$, three concurrent fault and large disturbance states $s_{i,D}, i = 1, 2, 3$,

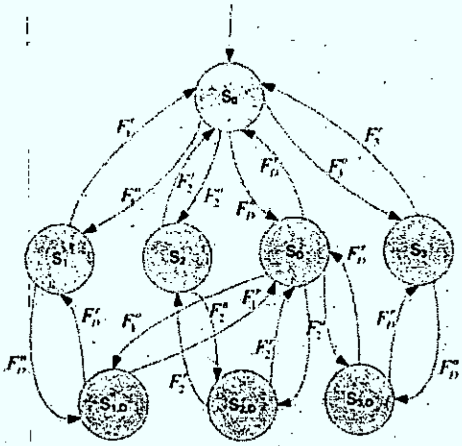

Fig. 3. The transition function corresponding to Example 1.

and the large disturbance input s_D. The event set and the output set for this system are given by $\Sigma = \{\mathcal{F}_1^o, \mathcal{F}_2^o, \mathcal{F}_3^o, \mathcal{F}_1^r, \mathcal{F}_2^r, \mathcal{F}_3^r, \mathcal{D}^o, \mathcal{D}^r\}$ and $Y = \{(R_1^1, ..., R_4^1, R_1^2, ..., R_3^2) \in \mathbb{B}^7\}$, respectively.

The output map λ depends on the severity of a fault and the threshold values of the residuals. As mentioned in the previous section, the threshold values for the residuals $r_j \in \mathfrak{R}_2$ are usually lower than those of $r_j \in \mathfrak{R}_1$. Therefore, there could be a low severity fault scenario where the residual logic unit $R_{\xi+j}^1$ becomes one while R_j^1 is zero. In defining the output map λ, such scenarios are also incorporated. Table I shows the corresponding output map λ. Consequently, some states may have different outputs that would depend on the severity of the fault and disturbances. Moreover, non-detectable fault scenarios (refer to Definition 3) are not observable from residual logic units, and therefore they cannot be detected and isolated. These types of faults are not considered in λ. In other words, no event is assigned to such faults.

The objective of the DES diagnoser is to use the output sequence of the system (residual logic units) as inputs and to generate an estimate of the state of the system. In this work, a DES diagnoser is modeled as a finite state automaton $H = (S_H, I_H, \delta_H, z_0, Y_H, \lambda_H)$, where S_H, I_H, Y_H denote the finite state, input and output sets; z_0 is the initial state of the diagnoser, $\delta_H : S_H \times I_H \rightarrow S_H$ denotes the transition function and λ_H is the output map. In order to eliminate any possible ambiguity in the DES model (G) output, two additional states with respect to the state set of G are considered for H, namely $S_H = \{S, s_F, s_{F,D}\}$, where s_F corresponds to the faulty state where one cannot isolate the faulty channel and $s_{F,D}$ which corresponds to

TABLE I

OUTPUT MAP OF THE PLANT

	Output map λ
s_0	$(0, ..., 0)$
s_D	$\{(R_1^1, ..., R_\xi^2) \in Y \mid \exists l \in \mathbf{P}, \forall j \in \Omega_l^p, R_j^1 = 1\}$
s_i	$\{(R_1^1, ..., R_\xi^2) \in Y \mid \exists \beta \in \{1,2\}, j \in \Omega_i^f,\ R_j^\beta = 1\}$
$s_{i,j}$	$\{(R_1^1, ..., R_\xi^2) \in Y \mid \exists \beta \in \{1,2\}, l \in \Omega_i^f \cup \Omega_j^f, R_l^\beta = 1\}$
$s_{i,D}$	$\{(R_1^1, ..., R_\xi^2) \in Y \mid \exists \beta \in \{1,2\}, j \in \Omega_i^f,\ R_j^\beta = 1\} \cup$ $\{(R_1^1, ..., R_\xi^2) \in Y \mid \exists l \in \mathbf{P}, \forall j \in \Omega_l^p, R_j^1 = 1\}$

the concurrent occurrence of a fault and a large disturbance in the system when a fault may not be isolated. The input set for the diagnoser is an output set of G (set Y). The output set is the same as the state set of the diagnoser ($Y_H = S_H$) and the output map $\lambda_H : S_H \rightarrow Y_H$ is an identity map.

The main step that is left is the design of a transition map δ_H. First, we consider the case when the system is in a normal operational mode s_0 and try to find the transition function corresponding to this mode. Based on Assumption 2, three transitions are possible in the normal operation, namely transition to the state s_i which corresponds to the occurrence of a fault in the i-th actuator (event $\mathcal{F}_i^o$), transition to the state s_D which corresponds to the occurrence of a large disturbance in one of the input disturbance channels (event $\mathcal{D}^o$), and finally the transition to the fault mode s_F which corresponds to the occurrence of a low severity fault in one of the actuators that may not be isolable.

Lemma 3.1 below shows that the hybrid fault diagnoser can easily distinguish the effects of a fault and a disturbance by using the coding sets Ω_i^f and Ω_l^p, and therefore the sets Ω_i^f and Ω_l^p can be used for the transition to states s_i and s_D, respectively.

***Lemma** 3.1:* **a)** The coding sets Ω_l^p and Ω_i^f are distinct, i.e. $\Omega_l^p \neq \Omega_i^f, l \in \mathbf{P}, i \in \mathbf{k}$, and **b)** The coding sets Ω_i^f and $\Omega_j^f, i \neq j$ are distinct, i.e. $\Omega_i^f \neq \Omega_j^f, i, j \in \mathbf{k},\ i \neq j$.

Proof: a) First we consider the disturbances $\omega_l,\ l \in \mathbf{P}$ such that $l \in \Lambda_j$ for some $j \in \Xi$ (ω_l affects at least one of the residuals $r_j \in \Re_1$). Since the residual $r_{\xi+j}$ is decoupled from ω_l and is affected by all the faults $m_i, i \in \Gamma_j$, we have $\xi + j \notin \Omega_l^p$ and $\xi + j \in \Omega_i^f,\ i \in \Gamma_j$. Hence, we have $\Omega_l^p \neq \Omega_i^f,\ i \in \Gamma_j$. Moreover, for all $m_i,\ i \in \mathbf{k}$'s such that $i \notin \Gamma_j$, we have $j \in \Omega_l^p$ and

$j \notin \Omega_i^f$; hence $\Omega_l^p \neq \Omega_i^f$, $i \notin \Gamma_j$. Therefore, $\Omega_l^p \neq \Omega_i^f, i \in \mathbf{k}$. Next, we consider the disturbances ω_l, $l \in \mathbf{P}$ such that $l \notin \cup_{j=1}^{\xi}\Lambda_j$, i.e. disturbance inputs that do not affect any of the residuals $r_j, j \in \Xi$. Therefore, we have $j \notin \Omega_l^p, \forall j \in \Xi$. However, for any $i \in \mathbf{k}$, there exists at least one residual $r_j \in \mathfrak{R}_1$ such that $j \in \Omega_i^f$; hence $\Omega_l^p \neq \Omega_i^f, i \in \mathbf{k}$.

b) Given the procedure in Section II for generating the residuals r_i, $i \in \Xi$, we conclude that $\Omega_i \neq \Omega_j$, $i, j \in \mathbf{k}$, $i \neq j$. Let us define a new set Υ_i^f according to $\Upsilon_i^f = \Omega_i^f \cap \{\xi+1, ..., 2\xi\}$, $i \in \mathbf{k}$. Consequently, we can write $\Omega_i^f = \Omega_i \cup \Upsilon_i^f, i \in \mathbf{k}$. Since $\Omega_i \cap \{\xi+1, ..., 2\xi\} = 0$, $i \in \mathbf{k}$, it follows that $\Omega_i^f \neq \Omega_j^f$, $i, j \in \mathbf{k}$, $i \neq j$. This completes the proof of the lemma. ■

The only remaining case of interest is when the occurrence of a low severity fault (refer to Definition 3) in the i-th actuator will lead to changes in only $R_{\xi+i}^1$. The next lemma shows that the occurrence of a low severity fault can be distinguished from the occurrence of large disturbance inputs.

***Lemma** 3.2:* The coding sets Ω_l^p and Υ_i^f are distinct.

Proof: For the disturbance inputs $\omega_l \in \mathbf{P}$ such that $l \in \Lambda_j$ for some $j \in \Xi$, the proof follows along the same lines as that in the proof of part a) of Lemma 3.1. According to Assumption 3, for the disturbances that do not affect any of the residuals $r_j \in \mathfrak{R}_1$, i.e. $l \in \mathbf{P}$ such that $l \notin \cup_{i=1}^{\xi}\Lambda_i$, we have $\Omega_l^p = \emptyset$. But $\xi + i \in \Upsilon_i^f$, and hence $\Omega_l^p \neq \Upsilon_i^f$. ■

To summarize, our proposed hybrid fault diagnoser can *detect* the occurrence of a fault since $\Omega_l^p \neq \Upsilon_i^f$. However, we may have $\Upsilon_i^f = \Upsilon_j^f$ for some $i, j \in \mathbf{k}$, and therefore the fault cannot be *isolated*. In this case, the state of the fault diagnoser will change to s_F.

The next step is now to consider scenarios when initially a large disturbance is applied to the system followed by a fault that is concurrently present in one of the system actuators. Therefore, it is assumed that the system has a transition from the normal operation state s_0 to the disturbance state s_D where we define a set $\mathcal{D} = \{1 \leq j \leq \xi | R_j^1 = 1\}$. In this state, the second threshold logic units R_i^2 are used for all the residuals $r_j, j \in \mathcal{D}$. It is assumed that the effects of the fault is not nullified by a large disturbance input, which is quite a reasonable consideration for practically all situations.

Now, let us consider a scenario where a fault is detected in the i-th actuator and the state of the fault diagnoser is s_i. Generally, we should investigate three possible cases, namely 1) the removal of a detected fault, 2) the occurrence of a second fault in the j-th actuator, and 3) the occurrence of a disturbance in $\omega_l, l \in \mathbf{P}$. Actually, the main challenge here is to distinguish between cases 2 and 3, since the removal of a fault can be easily detected when all the threshold logic units become zero. The necessary condition for distinguishing between cases 2 and 3 is governed by

$$\Omega_i^f \cup \Omega_j^f \neq \Omega_i^f \cup \Omega_l^p,\ i, j \in \mathbf{k}, ; l \in \mathbf{P} \tag{8}$$

The next lemma provides the sufficient condition for satisfying the condition (8).

***Lemma** 3.3:* If the number of residuals $r_i \in \mathfrak{R}_1$ that are affected by each disturbance input is more than $|\Omega_i \cup \Omega_j| = \xi - C(k-2, k-\mu)$, i.e. $|\Omega_l^p \cap \Xi| > \xi - C(k-2, k-\mu), \forall l \in \mathbf{P}$, then the condition (8) is satisfied for all the disturbance inputs $l \in \mathbf{P}$ as well as fault modes $m_i, m_j, i \neq j$.

Proof: If $|\Omega_l^p \cap \Xi| > \xi - C(k-2, k-\mu)$, then for any two fault modes $m_i, m_j, i, j \in \mathbf{k}, i \neq j$, there exists at least one residual $r_\alpha \in \mathfrak{R}_1$ such that $r_\alpha \in \Omega_l^p$ and $r_\alpha \notin \Omega_i^f \cup \Omega_j^f$, and therefore it follows that $\Omega_i^f \cup \Omega_j^f \neq \Omega_i^f \cup \Omega_l^p$. This complete the proof of the lemma. ■

It can be easily verified that the system where $\Lambda_i = \Lambda, i \in \mathbf{k}$ satisfies the above sufficient condition if $\mu > 1$ since $|\Omega_l^p \cap \Xi| = \xi$ and $|\Omega_i^f \cup \Omega_j^f| < \xi$.

***Remark** 1:* In the situation where $\Omega_i^f \cup \Omega_j^f \subset \Omega_i^f \cup \Omega_l^p$, one could potentially have a false alarm associated with the second fault while a large disturbance input is present. To remedy this problem, the DES diagnoser will declare the detection of the second fault after a specific waiting-time interval τ_0, if all the residual threshold logics specified by $\Omega_i^f \cup \Omega_j^f$ are at 1 while the remaining residual threshold logic units specified by $\{\Omega_i^f \cup \Omega_j^f\} - \{\Omega_i^f \cup \Omega_l^p\}$ remain at zero.

Tables II and III summarize all the transitions of the DES diagnoser. By specifying these transitions, the design of our proposed hybrid DES diagnoser is now completed.

***Example 1** (Cont.)* According to the coding sets that were obtained for the nonlinear system in Example 1, the DES diagnoser can be designed as follows: the state set is specified by $S_H = \{s_0, s_1, s_2, s_3, s_D, s_F, s_{1,D}, s_{2,D}, s_{3,D}\}$, the input set is defined by $I_H = \{R_1^1, R_2^1, R_3^1, R_4^1, R_1^2, R_2^2, R_3^2\}$, and the transition map λ_H is given in Table IV. Therefore, the design of our proposed hybrid diagnoser for the nonlinear system in Example 1 is now completed. In the next section, our proposed FDI algorithm will be applied to the ATLAV system.

TABLE II

TRANSITION FUNCTION OF THE STATES s_0, s_D AND $s_i, i \in \mathbf{K}$

Current State	Input $(R_1^1, ..., R_{2\xi}^1, R_1^2, ..., R_\xi^2)$	Next state	Corresponding event in G
s_0	$\bigwedge_{j \in \Omega_i^f} R_j^1 = 1$	$s_i, i \in \mathbf{k}$	$\mathcal{F}_i^o$
s_0	$\exists l \in \mathbf{k}$ such that $\bigwedge_{j \in \Upsilon_l^f} R_j^1 = 1$	s_F	$\mathcal{F}_i^o \in \{\mathcal{F}_1^o, ..., \mathcal{F}_k^o\}$
s_0	$\exists l \in \mathbf{P}$ such that $\bigwedge_{j \in \Omega_l^p} R_j^1 = 1$	s_D	$\mathcal{D}_i^o$
s_D	all inputs become zero	s_0	$\mathcal{D}^r$
s_D	$\bigwedge_{j \in \Omega_i^f \cap \mathcal{D}} R_j^2 \bigwedge_{l \in \Upsilon_i^f} R_l^1 = 1$	$s_{i,D}$	$\mathcal{F}_i^o$
s_D	$\exists l \in \mathbf{k}$ such that $\bigwedge_{j \in \Upsilon_l^f} R_j^1 = 1$	$s_{F,D}$	$\mathcal{F}_i^o \in \{\mathcal{F}_1^o, ..., \mathcal{F}_k^o\}$
s_i	all inputs become zero	s_0	$\mathcal{F}_i^r$
s_i	$\bigwedge_{l \in \Omega_i^f \cup \Omega_j^f} R_1^1 = 1$ for the time interval τ_0	$s_{i,j}$	$\mathcal{F}_j^r$
s_i	$\exists l$ such that $\bigwedge_{j \in \Omega_i^f \cup \Omega_l^p} R_j^1 = 1$	$s_{i,D}$	$\mathcal{D}^o$

IV. Hybrid FDI Design for the Almost-Lighter-Than-Air-Vehicle (ALTAV) System

Example 1 worked out in the previous section belonged to a class of nonlinear systems with not strongly detectable family of fault signatures. In this section, we consider the application of our proposed FDI methodology to an ALTAV system where the actuator fault signatures are strongly detectable. The ALTAV system considered in this paper is a six degrees of freedom unmanned aerial vehicle (refer to [15]). The states/variables describing the motion of the system are x, y, z, θ, γ and ϕ. These states correspond to the translation in the x, y and z directions and rotations about the z, y and x axes (heading, pitch and roll angles) in the local horizontal/local vertical frame, respectively. It is assumed that these states and their first order derivatives are available for measurement.

TABLE III

TRANSITION FUNCTION OF THE STATES s_F, $s_{F,D}$, $s_{i,D}$ AND $s_{i,j}$

Current State	Input $(R_1^1, ..., R_{2\xi}^1, R_1^2, ..., R_\xi^2)$	Next state	Corresponding event in G
s_F	$\bigwedge_{j\in\Omega_i^f} R_j^1 = 1$ for the time interval τ_0	s_i	$\mathcal{F}_i^o$
s_F	$\exists l \in \mathbf{P}$ such that $\bigwedge_{j\in\Omega_l^p} R_j^1 = 1$	$s_{F,D}$	$\mathcal{D}^o$
$s_{F,D}$	$\bigwedge_{j\in\Omega_i^f\cap D} R_j^2 \bigwedge_{l\in\Upsilon_i^f} R_l^1 = 1$	$s_{i,D}$	$\mathcal{F}_i^o$
$s_{F,D}$	$\exists l \in \mathbf{k}$ such that $\bigwedge_{j\in\Upsilon_l^f} R_j^1 = 1$	s_F	$\mathcal{D}^r$
$s_{F,D}$	$\exists l \in \mathbf{P}$, $i \in \mathbf{k}$ such that $\bigwedge_{j\in\Omega_l^p} R_j^1 = 1$	s_D	$\mathcal{F}_i^r \in \{\mathcal{F}_1^o, ..., \mathcal{F}_k^o\}$
$s_{i,D}$	$\exists l \in \mathbf{P}$ such that $\bigwedge_{j\in\Omega_l^p} R_j^1 = 1$	s_D	$\mathcal{F}_i^r \in \{\mathcal{F}_1^o, ..., \mathcal{F}_k^o\}$
$s_{i,D}$	$\bigwedge_{j\in\Omega_i^f} R_j^1 = 1$	s_i	$\mathcal{D}^r$
$s_{i,j}$	$\bigwedge_{l\in\Omega_i^f} R_l^1 = 1$	s_i	$\mathcal{F}_j^r$
$s_{i,j}$	$\bigwedge_{l\in\Omega_j^f} R_l^1 = 1$	s_j	$\mathcal{F}_i^r$

The dynamics of the ALTAV system is governed by the following equations [6]

$$
\begin{aligned}
M\ddot{x} &= \sum_{i=1}^{4} F_i sin(\gamma) - C_x\dot{x} + W_x \\
M\ddot{y} &= \sum_{i=1}^{4} F_i sin(\phi) - C_y\dot{y} + W_y \\
M\ddot{z} &= -\sum_{i=1}^{4} F_i cos(\gamma)cos(\phi) - F_B + Mg - C_z\dot{z} \\
J_\theta\ddot{\theta} &= (F_1 l - F_2 l + F_3 l - F_4 l)sin(\rho) - C_\theta\dot{\theta} \\
J_\gamma\ddot{\gamma} &= (F_1 l - F_3 l) - F_B L_B sin(\gamma) - C_\gamma\dot{\gamma} \\
J_\phi\ddot{\phi} &= -(F_2 l - F_4 l) - F_B L_B sin(\phi) - C_\phi\dot{\phi}
\end{aligned} \tag{9}
$$

where the four input forces $F_i, i = 1, ..., 4$ are produced by the propellers which are controlled through four vectoring brushless DC motors subject to the constraints $0 \leq F_i \leq F_i^{max}$, C_x, C_y, C_z denote the drag coefficients, M denotes the mass, J denotes the moment of inertia, l denotes the perpendicular distance between the motors and vehicle center of gravity, F_B denotes the Buoyant force, W_x, W_y, W_z denote the wind disturbances, and ρ denotes the angular offset from vertical of the motor thrust vectors.

Common actuator faults that are considered here may include [16]: (i) freezing or lock in-place

(LIP) fault, (ii) float fault, (iii) hard-over fault (HOF), and (iv) loss of effectiveness (LOE) fault. In case of the LIP fault, the actuator states freezes at a particular value and will not respond to subsequent commands. HOF is characterized by the actuator moving to its upper or lower saturation limits regardless of the commanded signal. The actuator transient response time is bounded by its rate limits. Float fault occurs when the actuator floats with zero output and does not contribute to the control authority. Loss of effectiveness is characterized and represented by lowering the actuator gain with respect to its nominal value.

A bank of residual generators are first designed for the four input channels of the ALTAV system. The state space representation of the ALTAV system is rewritten as follows

$$\dot{X} = f(X) + \sum_{i=1}^{4} g_i(X)F_i + \sum_{j=1}^{3} p_j(X)\omega_j$$
$$Y = X + v \tag{10}$$

where $F_1, ..., F_4$ are the input force control channels; $X^T = [x \ y \ z \ \dot{x} \ \dot{y} \ \dot{z} \ \theta \ \gamma \ \phi \ \dot{\theta} \ \dot{\gamma} \ \dot{\phi}]$, ω_1 and ω_2 represent the wind disturbances in the x and the y directions, respectively, ω_3 represents a change in the buoyant force F_B, $X = \{X_i\}_{i=1}^{12}$ and $Y = \{Y_i\}_{i=1}^{12}$.

First, we need to generate residuals $r_i, i = 1, ..., 4$ such that each residual r_i is only affected by F_i and is decoupled from all other faults $F_j, j \neq i$. Towards this end, the largest observability codistributions $\Pi_i^* = o.c.a.((\sum^{\mathcal{L}_i})^{\perp})$ should be found where $\mathcal{L}_1 = span\{g_2(X), g_3(X), g_4(X)\}$, $\mathcal{L}_2 = span\{g_1(X), g_3(X), g_4(X)\}$, $\mathcal{L}_3 = span\{g_1(X), g_2(X), g_4(X)\}$, and $\mathcal{L}_4 = span\{g_1(X), g_2(X), g_3(X)\}$, such that $span\{g_i(X)\} \not\subset (\Pi_i^*)^{\perp}$, $i = 1, ..., 4$.

For the ALTAV system since we have assumed full state measurements $X_i, i = 1, ..., 12$ and $\bar{\mathcal{L}}_i = \mathcal{L}_i$, we conclude that $\Pi_i^* = \mathcal{L}_i^{\perp}$. It can be easily shown that $\Pi_1^* = \text{span}\{dX_1, dX_2, dX_3, dX_7, dX_8, dX_9, dz_{11}, dz_{12}, dz_{13}\}$, where $z_{11} = 2J_\gamma sin(\rho) sin(X_8)\ X_{11} + J_\theta sin(X_8)X_{10} + lM sin(\rho)X_4$, $z_{12} = 2J_\gamma sin(\rho) sin(X_9)X_{11} + J_\theta sin(X_9)X_{10} + lM sin(\rho)X_5$, and $z_{13} = 2J_\gamma sin(\rho)\ cos(X_8) cos(X_9)X_{11} + J_\theta cos(X_8) cos(X_9)X_{10} - lM sin(\rho)X_6$. Given that we have full state measurements each of the three states z_{11}, z_{12} and z_{13} can be used for generating the residual r_1 such that it is only affected by F_1 and is decoupled from $F_j, j \neq 1$. It should be noted that other state candidates, i.e. X_i, $i = 1, 2, 3, 7, 8, 9$ are not affected by F_1, and hence cannot be selected for generating the residual r_1. It is evident that each of the states z_{11}, z_{12} and z_{13} are affected by one disturbance input (W_x, W_y and F_B, respectively).

Therefore, by selecting only one of the states for residual generation, the residual becomes decoupled from all the other disturbance inputs. Moreover, the full state measurement assumption can be relaxed since from states X_4, X_5, X_6 only one is needed for generating the residual r_1. This redundancy in generating the residuals from different measurements can be used whenever one considers the presence of a fault in the sensors (this is beyond the scope of the current work). In the following we only use the measurement X_4 for generating the residuals and the following set of states can be found such that $z_i, i = 1, ..., 4$ is affected by F_i and is decoupled from the other input channels $F_j, j \neq i$, namely

$$z_1 = 2J_\gamma sin(\rho)sin(X_8)X_{11} + J_\theta sin(X_8)X_{10} + lM sin(\rho)X_4$$
$$z_2 = -2J_\phi sin(\rho)sin(X_8)X_{12} - J_\theta sin(X_8)X_{10} + lM sin(\rho)X_4$$
$$z_3 = -2J_\gamma sin(\rho)sin(X_8)X_{11} + J_\theta sin(X_8)X_{10} + lM sin(\rho)X_4$$
$$z_4 = 2J_\phi sin(\rho)sin(X_8)X_{12} - J_\theta sin(X_8)X_{10} + lM sin(\rho)X_4$$

It can be checked that $\Lambda_i = \{p_1, p_3\}, i = 1, ..., 4$, and one needs only to generate one extra residual that is decoupled from ω_1 and ω_3. Towards this end, the largest observability codistribution $\Pi_5^* = o.c.a.((\sum_*^{\mathcal{L}_5})^\perp)$ should be found where $\mathcal{L}_5 = \{p_1, p_3\}$ such that $span\{g_i(X)\} \not\subset (\Pi_5^*)^\perp$, $i = 1, ..., 4$. For the ALTAV model, we have $\Pi_5^* = \mathcal{L}_5^\perp$. Based on Π_5^* the following set of states can be found that are decoupled from p_1 and p_3 and are affected by all control inputs F_i's, namely $z_5 = X_{10}$ and $z_6 = X_5$. However, only one of the above states is sufficient and in order to satisfy Assumption 3, we can only select z_5 for this purpose, since $\Omega_3^p = \{r_6\}$, where r_6 corresponds to the residual that is generated by the observer of the state z_6. The coding sets for the fault channels $F_1, ..., F_4$ and the disturbance inputs ω_1 and ω_3 are as follows: $\Omega_1^f = \{1, 5\}$, $\Omega_2^f = \{2, 5\}$, $\Omega_3^f = \{3, 5\}$, $\Omega_4^f = \{4, 5\}$, and $\Omega_1^p = \Omega_3^p = \{1, 2, 3, 4\}$. Moreover, it is clear that the sufficient condition in Lemma 3.3 is also satisfied for the ALTAV system.

It should be emphasized that for generating the residuals that are decoupled from the disturbance inputs W_x, W_y and F_B, the following observability codistributions should be obtained, namely, $\Pi_i^* = o.c.a.((\sum_*^{\mathcal{L}_i})^\perp)$, where $\mathcal{L}_i = \text{span}\{\mathcal{L}_i(x), p_1(x), p_2(x), p_3(x)\}$. It can be verified that $span\{g_i(X)\} \subset (\Pi_i^*)^\perp$, $i = 1, ..., 4$, and therefore fault detection and isolation is not feasible. However, based on our proposed approach, we can accomplish both fault detection and isolation among the actuator faults as well as robustness with respect to the disturbance

TABLE IV

TRANSITION FUNCTION OF EXAMPLE 1

Current State	Input $(R_1^1, ..., R_4^1, R_1^2, ..., R_3^2)$	Next state
s_0	$R_1^1 \bigwedge R_2^1 \bigwedge R_4^1 = 1$	s_1
s_0	$R_1^1 \bigwedge R_3^1 \bigwedge R_4^1 = 1$	s_2
s_0	$R_2^1 \bigwedge R_3^1 \bigwedge R_4^1 = 1$	s_3
s_0	$R_1^1 \bigwedge R_2^1 \bigwedge R_3^1 = 1$	s_D
s_0	$R_4^1 = 1$	s_F
s_i	all zero	s_0
s_D	all zero	s_0
s_D	$R_1^2 \bigwedge R_2^2 \bigwedge R_4^1 = 1$	$s_{1,D}$
s_D	$R_1^2 \bigwedge R_3^2 \bigwedge R_4^1 = 1$	$s_{2,D}$
s_D	$R_2^2 \bigwedge R_3^2 \bigwedge R_4^1 = 1$	$s_{3,D}$
s_F	all zero	s_0
s_F	$R_1^1 \bigwedge R_2^1 \bigwedge R_4^1 = 1$	s_1
s_F	$R_1^1 \bigwedge R_3^1 \bigwedge R_4^1 = 1$	s_2
s_F	$R_2^1 \bigwedge R_3^1 \bigwedge R_4^1 = 1$	s_3
s_F	$R_1^1 \bigwedge R_2^1 \bigwedge R_3^1 \bigwedge R_4^1 = 1$	$s_{F,D}$

inputs.

Once the residuals $r_j(t), j = 1, ..., 5$ are constructed, the next step is to determine the threshold value J_{th_j} and the evaluation function $J_{r_j}(t)$. In this paper, the following evaluation functions are selected $J_{r_j}(t) = \int_{t-T_0}^{t} r_j^T(t) r_j(t) dt,\ j = 1, ..., 5$, where T_0 is the length of the evaluation window. The main advantage of these evaluation functions is that one can also detect intermittent faults easily. The residual logic units $R_j^1, j = 1, ..., 5$ and $R_j^2, j = 1, ..., 4$ are selected according to equations (6) and (7), respectively, where the corresponding threshold values are found as discussed in Section III. It should be noted that the supremum that arises in determining the threshold values can be estimated from simulations by considering the worst case effects of the measurement noise and input disturbances on the residuals.

It is interesting to note that the trivial evaluation functions $J_{r_j}(t) = r_j(t)$ are not applicable to the ALTAV system since according to our extensive simulation studies (refer to Section V, Figure 6) it turns out that oscillations are present in the residuals $r_j, i = j, ..., 4$ when we have simultaneously a fault in one of the input channels F_j and the state γ happens to be also varying about zero. Under these circumstances the corresponding residuals will also behave similar to that of γ, and therefore cannot be used to conduct fault detection.

The final step is to design a DES fault diagnoser H. The state set of H is defined as $S_H = \{s_0, ..., s_4, s_{1,2}, ..., s_{3,4}, s_{1,D}, ..., s_{4,D}, s_F, s_{F,D}\}$, where cardinality of S is 23. The input set of the diagnoser is $I = \{R_1^1, ..., R_5^1, R_1^2, ...R_4^2\}$, and the output set is equal to S_H. The transition function λ_H can be found by following the results that are given in Section III. This derivation is not included here due to space limitations.

V. Simulation Results

In this section, simulation results of our proposed hybrid FDI scheme as applied to the nonlinear ALTAV system are presented. Various actuator faults are considered in the four input channels of the ALTAV system. In a surveillance-type maneuvering mission, the ALTAV initiates its motion from a given coordinate and follows a rectangular path in the *x-y* plane, and then changes its altitude and follows the same pattern in this altitude. The output measurement noise and tolerable disturbance inputs $\mathfrak{D}_1$ that are considered in the simulation results below are as follows: uniform random variable $\pm$ 1 degree for output measurements γ and ϕ, uniform random variable $\pm$ 0.1 m/s for measurement $\dot{x}$, uniform random variable $\pm$ 0.5 degree/s for measurements $\dot{\theta}$, $\dot{\gamma}$ and $\dot{\phi}$, uniform random variable $\pm$ 0.5 Newton for disturbance inputs W_x and W_y, and uniform random variable $\pm$ 2 Newton for ΔF_B. Since large changes in the buoyant force F_B do not produce any changes in the residuals, only the wind disturbance in the x-direction needs to be considered for simulations (the wind disturbance in the y-direction is unobservable from the residuals), i.e. $\mathfrak{D}_2 = \{W_x | 0.5 \ll W_x < 5\ (Newton)\}$. By considering the worst case scenario of the residuals corresponding to the healthy mode of the ALTAV system subject to the measurement noise and tolerable input disturbances $\mathfrak{D}_1$, the threshold values of $J_{th_j}^1 = 6e-4, J_{th_i}^2 = 4.5e-3,\ j = 1, ..., 4$ and $J_{th_5}^1 = 3e-5$ and the evaluation windows of $T_0 = 5$ seconds and $T_0 = 10$ seconds are selected for the residuals $r_1, ..., r_4$ and r_5, respectively. It should be pointed out that since the residual r_5 is decoupled from all the disturbance inputs, one can select a lower threshold value for it.

Figure 4 shows the residual evaluation functions corresponding to a permanent float fault in the input channel F_1 at $t = 100$ seconds. A concurrent wind disturbance gust that is represented by a rectangular pulse of a constant amplitude 3 (Newton) in the x-direction between $t = 80$ and

$t = 120$ seconds is also applied to the ALTAV system in this simulation. Figure 5 depicts the state of the DES fault diagnoser. As shown in this figure, the diagnoser state first changes to s_D at $t = 83$ seconds after the occurrence of the large wind disturbance in the x-direction with no false alarm generated. Later when a fault in the input channel F_1 is injected, the diagnoser state first switches to $s_{F,D}$ at $t = 101.3$ seconds and then after about 2 seconds it switches to state $s_{1,D}$ at $t = 103$ seconds. Consequently, we can conclude that the diagnoser can perfectly detect and isolate the fault despite the presence of a *large* concurrent disturbance. Finally, after the disturbance is removed at $t = 120$ seconds, the diagnoser switches to the state s_1 at time $t = 123$ seconds. It should be emphasized that if one *only* uses the first 4 residuals $r_1, ..., r_4$, not only a *false alarm* will be generated due to the wind disturbance but also the actual fault at $t = 100$ *cannot* be detected and isolated. However, by using our proposed hybrid FDI methodology, we are able to distinguish the occurrence of a fault as well as large wind disturbance in the x-direction ($\omega_1 \in \mathfrak{D}_2$) by designing only one additional residual.

Figure 6 shows the residuals r_1 and r_2 corresponding to the above fault scenario. As stated in the previous section it should be now evident from this figure as to why one cannot directly evaluate the residual signals using their thresholds, i.e. $J_{r_j} = r_j$, since due to the dynamics of the ALTAV system after the occurrence of a fault, the residuals tends to oscillate in and out of the threshold bounds.

Figure 7 depicts the residual evaluation functions associated with a permanent hard over fault (HOF) in the input channel F_2 that is applied at $t = 100$ seconds, and Figure 8 shows the corresponding fault diagnoser state. A wind disturbance gust that is represented by a rectangular pulse of a constant amplitude 3 (Newton) in the x-direction is also injected between $t = 50$ and $t = 80$ seconds in the simulations. As seen from Figure 8, the diagnoser first detects the fault at $t = 100.2$ seconds and also isolates the fault at $t = 107.5$ seconds. Moreover, no false alarm is generated due to the presence of the disturbance input. As shown in Figure 7, the residual evaluation function J_{r_2} does not exceed the second threshold values $J^2_{th_j}$. Consequently, if one only uses a conventional FDI method and chooses the threshold values by considering the entire disturbance set, i.e. $\mathfrak{D}_2$, then the hard over fault cannot be detected and isolated. However, by using our proposed approach, this fault can easily be detected and then isolated despite the presence of a large wind disturbance.

The last scenario we consider corresponds to presence of multiple faults in the ALTAV

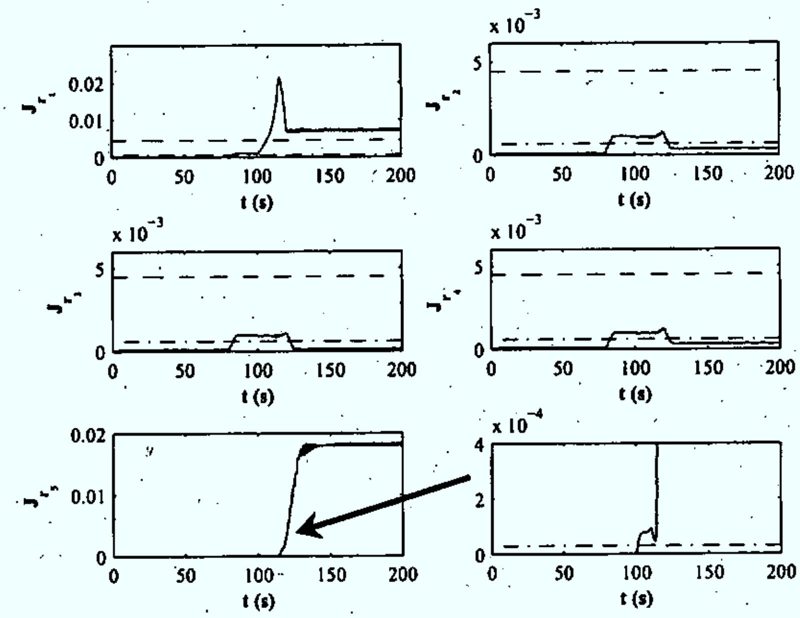

Fig. 4. Residual evaluation functions corresponding to a float fault in F_1 actuator (the dashed dots correspond to the threshold values $J^1_{th_i} = 6e-4, i = 1, \dots, 4$ and $J^1_{th_5} = 3e-5$, the dashed lines correspond to the threshold value $J^2_{th_i} = 4.5e-3$).

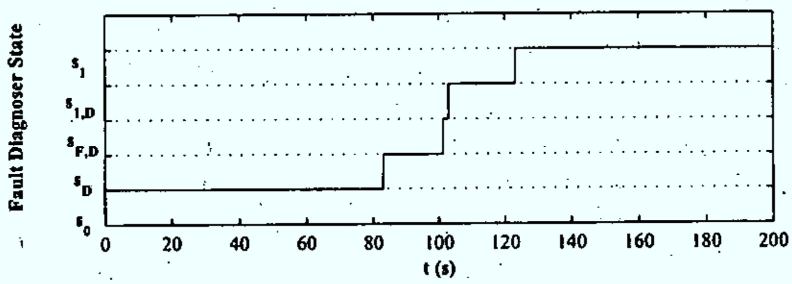

Fig. 5. Fault diagnoser state corresponding to a float fault in F_1 actuator.

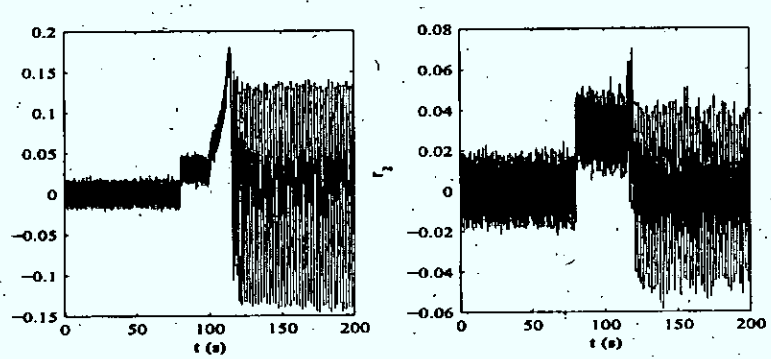

Fig. 6. Residuals corresponding to a float fault in F_1 actuator.

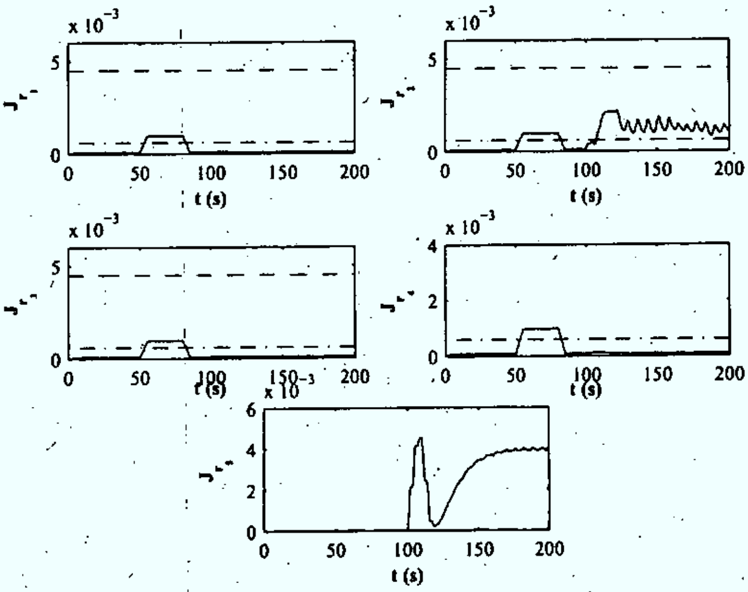

Fig. 7. Residual evaluation functions corresponding to a hard over fault in F_2 actuator (the dashed dots correspond to the threshold values $J^1_{th_i} = 6e-4, i = 1, \dots, 4$ and $J^1_{th_5} = 3e-5$, the dashed lines correspond to the threshold value $J^2_{th_i} = 4.5e-3$).

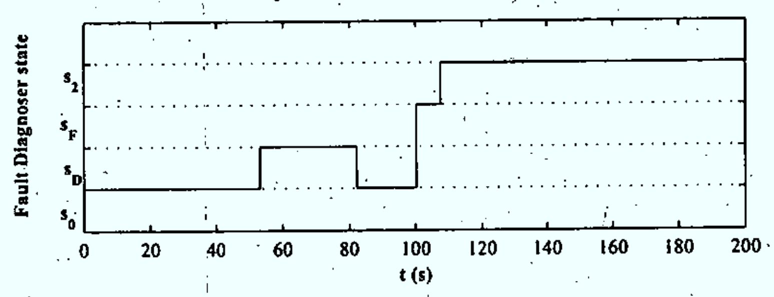

Fig. 8. Fault diagnoser state corresponding to a hard over fault in F_2 actuator.

actuators. For the generated residuals, we have $\Omega_i^f \cup \Omega_j^f \subset \Omega_i^f \cup \Omega_1^p$. Therefore, according to Remark 1, a waiting time interval of $\tau_0 = 1$ second is considered for detecting the second fault. Figures 9 and 10 show the corresponding residual evaluation functions and the fault diagnoser, respectively, to an intermittent float fault in the input channel F_1 that is applied between $t = 100$ and $t = 150$ seconds, a permanent 50% loss of effectiveness fault in the input channel F_4 that is applied at $t = 120$ seconds, and a wind gust disturbance that is represented by a rectangular pulse of a constant amplitude 3 (Newton) that is injected in the x-direction between $t = 50$

and $t = 80$ seconds. According to these figures one does clearly detect and isolate faults in F_1 and F_4 at $t = 104$ and $t = 121$ seconds, respectively. It is worth mentioning that according to Definition 3, a hard over and a float fault are categorized as high severity faults and a 50% loss of effectiveness fault is considered as a low severity fault.

VI. Conclusions

A novel hybrid fault detection and isolation scheme is proposed for a nonlinear system that is subject to large disturbances. The proposed scheme consists of two modules, namely, a bank of residual generators and a discrete-event system (DES)-based fault diagnoser. The notions of strongly and not strongly detectable fault signatures for a nonlinear system are introduced. A new coding set for not strongly detectable fault signatures is then developed. A novel set of complementary residuals is proposed and constructed for not strongly detectable fault signatures based on the nonlinear geometric approach. A DES diagnoser is developed which uses the residuals and their temporal behavior to robustly detect and isolate the faulty channels. Our proposed hybrid FDI methodology is applied to the problem of actuator fault detection and isolation for an almost-lighter-than-air-vehicle (ALTAV) system. Simulation results clearly illustrate and demonstrate the effectiveness and advantages of our proposed approach in detecting and isolating four common fault types in the input channels/actuators of the ALTAV system.

Acknowledgement

The authors would like to acknowledge the support received from Quanser Inc. [6], [15] for the mathematical model of the ALTAV system.

References

[1] C. D. Persis and A. Isidori, "A geometric approach to nonlinear fault detection and isolation," *IEEE Transactions on Automatic Control*, vol. 46, no. 6, pp. 853–865, 2001.

[2] R. Seliger and P. M. Frank, "Fault diagnosis by disturbance decoupled nonlinear observer," *Proceedings of IEEE Conference on Decision and Control*, pp. 2248–2253, 1991.

[3] A. J. Krener, "Necessary and sufficient conditions for nonlinear worst case (H_∞) control and estimation," *Journal of Mathematical Systems, Estimation and Control*, vol. 4, no. 4, pp. 1–25, 1994.

[4] C. D. Persis and A. Isidori, "On the design of fault detection filters with game-theoretic-optimal sensitivity," *International Journal of Robust and Nonlinear Control*, vol. 12, pp. 729–747, 2002.

[5] D. Berdjag, C. Christophe, and V. Cocquempot, "Nonlinear model decomposition for fault detection and isolation system design," *Proc. of 45th IEEE Conference on Decision and Control*, pp. 3321–3326, 2006.

[6] E. Earon, "Almost-lighter-than-air-vehicle fleet simulation," *Technical Report, V. 0.9, Quanser Inc., Toronto, Canada*, 2005.

[7] N. Lechevin, C. A. Rabbath, and E. Earon, "Towards decentralized fault detection in uav formations," *Proceeding of the American Control Conference*, pp. 5759–5764, 2007.

[8] N. Meskin, T. Jiang, E. Sobhani, K. Khorasani, and C. A. Rabbath, "A nonlinear geometric fault detection and isolation approach for almost-lighter-than-air-vehicles," *Proceedings of IEEE Multi-Conference on Systems and Control*, pp. 1073–1078, 2007.

[9] M. A. Massoumnia, G. C. Verghese, and A. S. Willsky, "Failure detection and identification," *IEEE Transactions on Automatic Control*, vol. 34, no. 3, pp. 316–321, 1989.

[10] J. Gertler, "Analytical redundacy methods in failure detection and isolation," *Proceeding of IFAC Fault Detection, Supervision and Safety for Technical Processes*, pp. 9–21, 1991.

[11] J. Chen and R. J. Patton, *Robust model-based fault diagnosis for dynamic systems*. Boston/Dordrecht/London: Kluwer Academic Publishers, 1999.

[12] N. Meskin and K. Khorasani, "Fault detection and isolation in a redundant reaction wheels configuration of a satellite," *Proceeding of IEEE International Conference on Systems, Man, and Cybernetics*, pp. 3153–3158, 2007.

[13] S. X. Ding, P. Zhang, P. M. Frank, and E. L. Ding, "Threshold calculation using LMI-technique and its integarion in the design of fault detection systems," *Proceeding of the* 42th *Conference on Decision and Control*, pp. 469–474, 2003.

[14] S. Hashtrudizad, R. H. Kwong, and W. M. Wonham, "Fault diagnosis in discrete-event systems: Framework and model reduction," *IEEE Transactions on Automatic Control*, vol. 48, no. 7, pp. 1199–1212, 2003.

[15] E. Earon, "ALTAV MK II information," *Pre-release specification, Quanser Inc., Toronto, Canada*, 2007.

[16] J. D. Boskovic, S. E. Bergstrom, and R. K. Mehra, "Retrofit reconfigurable flight control in the presence of control effector damage," *Proceeding of American Control Conference*, pp. 2652–2657, 2005.

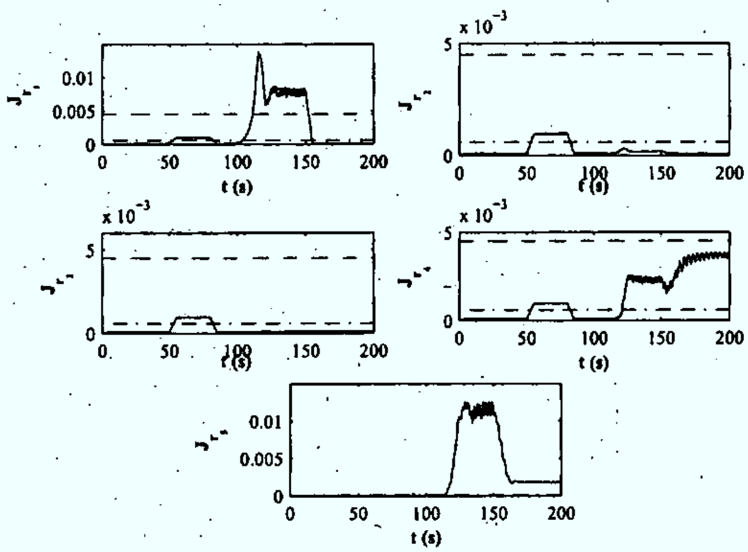

Fig. 9. Residual evaluation functions corresponding to multiple faults in F_1 and F_4 actuators (the dashed dot corresponds to the threshold values $J^1_{th_i} = 6e-4, i = 1, \ldots, 4$ and $J^1_{th_5} = 3e-5$, the dashed lines correspond to the threshold value $J^2_{th_i} = 4.5e-3$).

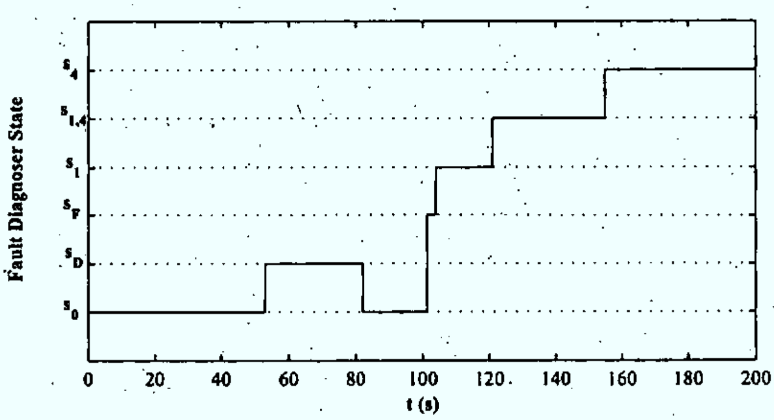

Fig. 10. Fault diagnoser state corresponding to multiple faults in F_1 and F_4 actuators.