A polynomial algorithm for diagnosability of fair discrete event systems

Pradeep Kumar Biswal and Santosh Biswas*

Department of Computer Science and Engineering, Indian Institute of Technology, Guwahati, India

(Received 26 July 2014; accepted 9 February 2015)

The discrete event system (DES) has been used for failure detection and diagnosis (FDD) of a wide range of systems. The major reason for resorting to the DES framework is the simplicity in modelling and the low complexity of the FDD algorithms. Pure DES models cannot directly capture systems with continuous dynamics. However, the DES paradigm surmounts the problem by partitioning the continuous state space and capturing each subspace as a discrete state. Conventional methods for FDD consist in constructing a diagnoser, the complexity of which is exponential in the number of system states. In the case of non-diagnosability, the diagnoser needs to be reconstructed after taking suitable measures such as increase in measurements, etc. The conventional schemes have two issues, namely, exponential complexity of diagnoser and erroneous diagnosability conclusions for fair systems. Several works address the first issue where checking diagnosability does not involve a diagnoser and has polynomial time complexity. Once a fault is diagnosable, a diagnoser is constructed for concurrent system monitoring. Regarding the second issue, the abstraction employed in DES modelling may obliterate the fairness property for systems having continuous dynamics, leading to erroneous inferences. Works addressing this issue have augmented fairness to the model and the diagnoser, and new diagnosability conditions have been proposed for fair systems. However, all the Fair DES diagnosability frameworks are based on diagnoser and hence have exponential complexity. In this paper, we propose a new DES diagnosability framework that suffices for fair systems but at the same time has polynomial complexity.

Keywords: fair discrete event systems; failure diagnosis; diagnosability; diagnoser

1. Introduction

Diagnosis of failures in large, complex systems is a crucial and involved task. The increasingly stringent requirements on performance and reliability of complex systems have necessitated the development of systematic methods for timely and accurate diagnosis of system failures. As a result, the failure diagnosis problem has been an area of recent research interest in the contexts of centralized systems (Bavishi and Chong, 1994; Lafortune, Teneketzis, Sampath, Sengupta, and Sinnamohideen, 2001; Lin and Wonham, 1988), decentralized systems (Debout, Lafortune, and Teneketzis, 1998), timed systems (Lamperti and Zanella, 1999; Zad, Kwong, and Wonham, 2005) and untimed systems (Sampath, Sengupta, Lafortune, Sinnamohideen, Teneketzis, 1995, 1996; Thorsley and Teneketzis, 2005; Zad, Kwong, and Wonham, 2003). In these works, the systems have been abstracted using discrete event system (DES) models. A DES model is characterized by a discrete state space and event-driven dynamics. A state-based DES model that captures both normal and failure conditions of a system comprises two categories of states, namely, the normal states and the failure states. Any failure state differs from a normal state in the value of a state variable (status variable) which cannot be measured.

A DES diagnosability analysis procedure takes as input any DES model with the measurable subset of the state variables and determines whether it is diagnosable (Sampath et al., 1995, 1996; Zad et al., 2003; Thorsley and Teneketzis, 2005). Typically, such a procedure consists in constructing a diagnoser, which is a kind of state estimator of the model. Then, it is checked whether the diagnoser can ascertain that the model is in a failure state within finite time of the concurrence of the failure. Some of such methods are discussed at length in Sampath et al. (1995) and Zad et al. (2003). The DES diagnosability analysis procedures, referred to above, suffer from two drawbacks.

First, in the worst case, the number of diagnoser states may be exponential in the number of system states. Hence, if a failure turns out to be non-diagnosable, then the diagnoser needs to be reconstructed after taking proper steps such as increasing the measurements. Thus, it is preferable that diagnosability be analysed using structures that are computationally simpler than a diagnoser. Construction of the diagnoser can be taken up only when the system is found to be diagnosable. Secondly, these procedures turn out to be inadequate for many systems which are fair. The transitions in the DES models corresponding to many real-life systems, such as those with continuous dynamics for
example, are fair. A transition is fair if it occurs infinitely often in all traces that visit the state from where the transition emanates, infinitely often. Many such systems, in which occurrences of a failure manifest themselves in finite time, are adjudged to be non-diagnosable by the diagnosability procedures mentioned above because fairness of transitions is not considered. In this paper, an example illustrates this fact.

To handle these two issues, several works have been reported in the literature. To address the first issue, procedures for diagnosability analysis have been reported in the literature for centralized systems (Jiang, Huang, Chandra, and Kumar, 2001; Tae-Yoo and Lafortune, 2002), decentralized systems (Moreira, Jesus, and Basilio, 2011) and fuzzy systems (Liu, 2014), which do not require the construction of a diagnoser. Instead, they construct a two-dimensional product model and check for a suitable condition over that model. The procedures accordingly have complexity polynomial in the number of system states.

The second issue has been handled in Thorsley and Teneketzis (2005) and Biswas, Sarkar, Mukhopadhyay, and Patra (2010), where the basic DES model was augmented with the concept of fairness. The classical DES frameworks declare a fault as non-diagnosable if there is a cycle through failure states which cannot be distinguished from a similar cycle through normal states. Thorsley and Teneketzis (2005) showed that the mere presence of such a cycle through faulty states to declare the failure non-diagnosable does not hold for many systems, for example, once having continuous dynamics. Thorsley et al. proposed a new DES paradigm where the classical DES model was augmented with probabilities of transitions. In the stochastic framework, failure is considered diagnosed when it is found that probability of the system traversing though failure states is higher than a threshold. Latter, Biswas et al. (2010) have proposed another DES paradigm to handle similar systems, where fairness was augmented to the classical DES model. The claim was, the abstraction employed in obtaining DES models from many systems, for example, those having continuous dynamics often obliterates the fairness property. The diagnosability condition in this case checks if there exists equivalent strongly connected components (SCCs) involving failure states and normal states. Comparing these works, it may be said that a transition having positive probability can be assumed to have fairness. In fact, the equivalence of the stochastic DES scheme (Thorsley and Teneketzis, 2005) and fair DES (FDES) scheme has been established in Biswas (2013). However, both these schemes which address fairness are based on diagnoser and hence exponential in the number of system states. To the best of our knowledge, no work has been reported for failure detection in the DES framework that suffices for fair systems and at the same time has polynomial time complexity.

The present paper aims at devising a polynomial time diagnosability testing procedure for FDES models. The major contributions of this paper are as follows:

- Identifying the issues in failure detection and diagnosis (FDD)-based DES frameworks having polynomial time complexity (Jiang et al., 2001; Tae-Yoo and Lafortune, 2002) when applied for fair systems. A brief discussion regarding these schemes and complexity analysis has been given. Following that, how wrong diagnosability inferences can be given if these techniques are applied on fair systems has been identified and demonstrated using a simple example.
- FDD schemes in DES frameworks have been enhanced to handle fair systems (Biswas et al., 2010; Thorsley and Teneketzis, 2005). A brief discussion is given in this paper regarding these schemes and how they handle fairness is highlighted. However, it is also demonstrated that these schemes involve exponential complexity with respect to the system states.
- To address the above situation, we developed an FDD framework for FDES models but involving only polynomial time complexity.
  - An algorithm has been proposed that takes in an FDES model and generates a strict composition with itself after eliminating the unmeasurable transition sequences.
  - A diagnosability condition has been proposed in the model obtained after composition, which ascertains if an FDES model is diagnosable under a given measurement limitation.
  - The correctness and completeness of the condition have been proved formally.
  - The complexity of the scheme, that is, generating the composition and checking the diagnosability condition have been analysed and shown to be polynomial with respect to the number of system states.
  - The entire theory has been illustrated using an example.

The paper is organized as follows. Section 2 presents the DES model, failure modelling, a formal definition of (DES) diagnosability and the polynomial time diagnosability analysis algorithm reported in Jiang et al. (2001) and Tae-Yoo and Lafortune (2002). In Section 3, an example has been used to illustrate that the DES diagnosability condition checked by this algorithm fails for many practical systems with continuous dynamics. In this section, we also present in brief the traditional diagnoser-based algorithm (Biswas et al., 2010; Thorsley and Teneketzis, 2005) for handling FDD of FDES models. We also discuss the computational complexity of the algorithm and highlight that it is exponential in number of system states.
FDES models are introduced next in Section 4. A new condition for FDES diagnosability analysis is introduced in the same section incorporating the property of fairness and the necessity and sufficiency of the condition are formally established. Then, we provide the computational complexity of checking this FDES diagnosability condition. The paper is concluded in Section 5.

2. DES models

A DES model $G$ is defined as

$$G = (V, X, \mathcal{A}, X_0),$$

where $V = \{v_1, v_2, \ldots, v_n\}$ is a finite set of discrete variables assuming values from some finite sets, called the domains of the variables. $X$ is a finite set of states and $X_0$ is a set of initial states. A state $x$ is a mapping of each variable to one of the elements of the domain of the variable. A transition $\tau \in \mathcal{A}$ from a state $x$ to another state $x^+$ is an ordered pair $(x, x^+)$, where $x$ is denoted as initial($\tau$) and $x^+$ is denoted as final($\tau$). We assume that any state of $G$ is reachable from some initial state.

A trace of a DES model $G$ is an infinite sequence of transitions of $G$ and denoted as $s^2 = (\tau_1, \tau_2, \ldots)$, where initial($\tau_1$) is an initial state in $X_0$ and the consecution property holds, that is, initial($\tau_{i+1}$) = final($\tau_i$), for $i \geq 1$. A finite prefix of a trace is referred to as a ‘finite trace’. Henceforth, we assume the consecution property for any ‘sequence of transitions’. For any trace $s = (\tau_1, \tau_2, \ldots)$, initial($s$) = initial($\tau_1$) and for a finite prefix $s^2 = (\tau_1, \tau_2, \ldots, \tau_j)$, final($\tau_j$) = final($s$). The set of all traces of $G$ and their finite prefixes are the language of $G$, denoted as $L(G)$. The set $L_f(G)$ denotes the subset of $L(G)$ comprising the finite prefixes of the members of $L(G)$. Naturally, $L(G) - L_f(G)$ is a subset of $\mathcal{A}^\infty$, where $\mathcal{A}^\infty$ is the set of all infinite sequences of $\mathcal{A}$; $L_f(G)$ is a subset of $\mathcal{A}^*$, the Kleene closure of $\mathcal{A}$. The post language of $G$ after a finite prefix $s$ of a trace, denoted as $L(G)/s$, is defined as

$$L(G)/s = \{t \in \mathcal{A}^\infty | st \in L(G)\}.$$  (2)

$L_f(G)/s \subseteq L(G)/s$ comprises finite prefixes of the traces of $L(G)/s$.

2.1. Models with measurement limitations

The set of variables are partitioned into two disjoint subsets, $V_m$ and $V_u$, of measurable and unmeasurable variables, respectively. Given such a partition, the transitions are partitioned into two sets, $\mathcal{A}_m$ and $\mathcal{A}_u$, of measurable and unmeasurable transitions, respectively, as follows.

DEFINITION 1 Measurable Transitions: A transition $\tau = (x, x^+)$ is said to be measurable if $x|_{V_u} \neq x^+|_{V_u}$, where $x|_{V_u}$ is the restriction of the function (defined by the state) $x$ to $V_m$. A transition which is not measurable is an unmeasurable transition.

DEFINITION 2 Two states $x$ and $y$ are said to be (measurement) equivalent, denoted as $x \equiv y$, if $x|_{V_u} = y|_{V_u}$.

DEFINITION 3 Two measurable transitions $\tau_1 = (x_1, x_1^+) = (x_2, x_2^+)$ are equivalent, denoted as $\tau_1 \equiv \tau_2$, if $x_1 = x_2$ and $x_1^+ = x_2^+$.

DEFINITION 4 A projection operator $P : \mathcal{A}^* \rightarrow \mathcal{A}_m^*$ can now be defined in the following manner:

$$P(\epsilon) = \epsilon, \text{ null string},$$

$$P(\tau) = \tau \text{ if } \tau \in \mathcal{A}_m^*,$$

$$P(\tau) = \epsilon \text{ if } \tau \in \mathcal{A}_u^*, (3)$$

The function $P$ erases the unmeasurable transitions from the argument finite trace. $P(s)$ is termed as the measurable finite trace corresponding to the finite trace $s$.

DEFINITION 5 Two finite traces $s$ and $s'$ are measurement equivalent if $P(s) = (\tau_1, \tau_2, \ldots, \tau_n)$, $P(s') = (\tau_1', \tau_2', \ldots, \tau_n')$ and $\tau_i \equiv \tau_i'$, $1 \leq i \leq n$.

We use the symbol $E$ to denote measurement equivalence of finite traces as well as that of transitions, with slight abuse of notation. The equivalence of finite traces $s$ and $s'$ implies that if measurable transitions are extracted from $s$ and $s'$ by the use of the operator $P$, then all the transitions are measurement equivalent.

The inverse projection operator $P^{-1} : \mathcal{A}_m^* \rightarrow \mathcal{A}^*$ is defined as

$$P^{-1}(s) = \{s' \in L_f(G)/s | ss' \in \mathcal{A}^\infty\}.$$  (4)

Thus, $P^{-1}(s)$ includes all possible sequences of transitions that are equivalent to the finite trace $s$. The projection function $P$, the inverse function $P^{-1}$ and the measurement equivalence $E$ of finite traces can be extended to traces in $\mathcal{A}^\infty$, in a natural way.

2.2. Failure diagnosis

Failure modelling: Each state $x$ is assigned a failure label by an unmeasurable status variable $C \in V$ with its domain $= \{N\} \cup 2^{F_1, F_2, \ldots, F_p}$, where $F_i$, $1 \leq i \leq p$, denotes permanent failure status and $N$ denotes normal status. For a normal state $x_N$, $x_N(C) = \{N\}$. The set of all normal states is denoted as $X_N$. Similarly, for a failure state (i.e. an $F_i$-state) $x_{F_i}$, $x_{F_i}(C) = \{F_i\}$. The set of all normal states is denoted as $X_N$. For a failure state $x_{F_i}$, $x_{F_i}(C) = \{N\}$. The set of all states $x$ s.t. $F_i \in x(C)$ is denoted as $X_{F_i}$. In the
sequel, a $G$-transition $(x, x^+)$ is called a normal ($F_i$) $G$-transition if $x, x^+ \in X_N(x_{F_i})$. A transition $(x, x^+)$, where $x(C) \neq x^+(C)$, is called a failure transition indicating the first occurrence of some failure in $x^+(C) - x(C)$.

Since failures are assumed to be permanent, there is no transition from any $x_{F_i}$ to any $x_N$ or any $x_{F_i}F_i$ to any $x_{F_i}$. Also, for a transition $(x, x^+)$, $x(C) \neq \{N\} \Rightarrow x(C) \subseteq x^+(C)$.

The following definition, proposed in Sampath et al. (1995), formalizes the notion of DES diagnosability of the failure $F_i$. Let $\Psi(X_{F_i}) = \{s \in L_f(G)\}$ the last transition of $s$ is measurable and final($s$) $\in X_{F_i}$.

**Definition 6** $F_i$-Diagnosability: A DES model $G$ is said to be $F_i$-diagnosable for the failure $F_i$ under a measurement limitation if the following holds $\exists n_{F_i} \in \mathbb{N}$ s.t. $[\forall s \in \Psi(X_{F_i}) \forall t \in L_f(G) / s(\{s \geq n_{F_i} \Rightarrow D\})]$, where the condition $D$ is $\forall u \in P^{-1}(P(st))$, final($u$) $\in X_{F_i}$.

The above definition means the following. Let $s$ be any finite prefix of a trace of $G$ that ends in an $F_i$-state and let $t$ be any sufficiently long continuation of $s$. Condition $D$ then requires that every sequence of transitions, measurement equivalent with $st$ (i.e. belonging to $P^{-1}(P(st))$), shall end into an $F_i$-state. This implies that, along every continuation $t$ of $s$, one can detect the occurrence of failure corresponding to $F_i$ within a finite delay, specifically in at most $n_{F_i}$ transitions of the system after $s$.

In the next subsection, we present in brief the polynomial time algorithm for diagnosability analysis of DES models as given in Jiang et al. (2001). The diagnosability result obtained by the scheme proposed in Tae-Yoo and Lafortune (2002) is equivalent to the one obtained by the technique proposed in Jiang et al. (2001). Both the algorithms are polynomial time in the number of system states and works on the DES framework but uses slightly different diagnosability analysis procedures. In this paper, we compare our technique with the algorithm proposed in Jiang et al. (2001).

The algorithm presented in Jiang et al. (2001) is based on an event-based DES framework first proposed in Sampath et al. (1995). In contrast, the algorithm proposed in our present work is based on the state-based framework similar to the one used in Zad et al. (2003). We present the algorithm proposed in Jiang et al. (2001) after adapting it for the state-based framework. The state-based DES framework has two advantages compared to event-based one, as identified in Zad et al. (2003) and discussed in brief as follows.

In the event-based framework, the problem of fault diagnosis is to use observations to detect if a failure event (unobservable) had occurred in the system since the start of diagnosis. In state-based frameworks, there is an additional assumption that the state set of the system can be partitioned according to the condition (failure status) of the system. The assumption has two benefits. First, instead of detecting failure events, for the purpose of fault diagnosis, the diagnoser determines the system condition. This is particularly useful in cases where the failure might have occurred before the start of diagnosis. Another benefit of the aforementioned assumption is that it simplifies the transition function of the diagnoser. Since the system condition is a function of state, after receiving a new observation (i.e. output symbol), updating the estimate of the systems state is enough to update the condition in the diagnoser. In this way, label propagation as done in event-based models can be avoided.

Therefore, in our present work, we use the state-based framework. As the works reported on polynomial time failure diagnosis schemes (Jiang et al., 2001; Tae-Yoo and Lafortune, 2002) are based on event-based frameworks, we recast them in terms of state-based framework.

### 2.3. A polynomial time algorithm for testing diagnosability of DES models

The algorithm for polynomial time diagnosability analysis (Jiang et al., 2001) is as follows.

**Algorithm 1**

**Input:** A DES Model $G$ with failures $F_i$, $1 \leq i \leq p$.

**Output:** Diagnosability of $G$ for a fault $F_i$ for some $i \in [1, p]$.

1. Obtain a new DES $G_n = \langle V, X_n, \xi_n, X_0 \rangle$ from $G = \langle V, X, \xi, X_0 \rangle$ as follows:
   
   (a) $X_n = \{x | x \in X_0 \text{ or } x \in X \text{ and there exists a measurable transition } t \in \xi \text{ such that final}(t) = x\}$,
   
   (b) $\xi_n = \{(x, x^+) | x, x^+ \in X_n \text{ and there exists a sequence } s \text{ of } G\text{-transitions of the form } s = (t_1, t_2, \ldots, t_k, \tau), \text{ where initial}(t_1) = x, \text{ final}(t) = x^+ \text{ and } P(s) = \{t\}, \text{ i.e. } t_1 \text{ through } t_k \text{ are unmeasurable transitions} \}$.

The language generated by $G_n$ is $L(G_n)$. It may be noted that $G_n$ can also be considered as a DES model but without any unmeasurable transition. Hence, all the definitions for DES model $G$ also holds for $G_n$.

2. Compute $G_d = (G_n || G_n)$, the strict composition of $G_n$ with itself as the ordered tuple $G_d = (V, X_d, \xi_d, X_0)$, where
   
   (a) $X_{d0}$ is the set of initial states of $G_d$ defined as $X_{d0} = \{(x_1, x_2) | x_1 \in X_2 \text{ and } x_1, x_2 \in X_0\}$,
   
   (b) $\xi_d$ is the set of transitions of $G_d$ defined by the following rules:
      
      (i) All unordered pairs of $G_n$-transitions of the form $(t_1, t_2)$ are members of $\xi_d$, where $t_1 = (x_1, x_2^1)$, $t_2 = (x_2, x_2^2)$, $(x_1, x_2) \in X_{d0}$ and $x^1 \in X_2^1$.
      
      (ii) All unordered pairs of $G_n$-transitions of the form $(t_1, t_2)$ are members of $\xi_d$, where
\( r_1 = (x_1, x_1^+) \), \( r_2 = (x_2, x_2^+) \), \( x_1^+ E x_2^+ \) and \( \exists (r_1, r_2) \in \mathcal{R}_d \) such that final \((r_1) = x_1 \) and final \((r_2) = x_2 \).

(c) \( X_d \) is the set of states of \( G_d \) defined by the following rules:

(i) All members of \( X_m \) are members of \( X_d \).

(ii) All unordered pairs of \( G_n \)-states of the form \((x_1, x_2)\) such that for some \((r_1, r_2) \in \mathcal{R}_d\), \( x_1 = \text{final}(r_1) \), \( x_2 = \text{final}(r_2) \) and (initial \((r_1)\), initial \((r_2)\)) \(\in X_d\).

Thus, a state of \( G_d \) comprises two measurement equivalent \( G_n \)-states \( x_1 \) and \( x_2 \) which are either initial \( G_n \)-states or are reachable from some pair of initial \( G_n \)-states through two measurement equivalent finite sequences of transitions of \( G_n \). A \( G_d \)-state \((x_1, x_2)\), where \( x_1 = x_2 \), is also possible.

(3) The \( F_i \)-diagnosability condition: There does not exist any cycle \( c_d \) of the form \((x_d, x_d, \ldots, x_d, x_d)\), where, for any \( j \), \( 1 \leq j \leq k \), \( x_d = (x_1, x_2) \), \( F_i \in x_1(C) \) and \( F_i \notin x_2(C) \). Such a cycle is called an ‘offending cycle’ for failure \( F_i \).

Henceforth, in this paper the states (transitions) of \( G \), \( G_n \) and \( G_d \) would be termed as \( G \)-states (transitions), \( G_n \)-states (transitions) and \( G_d \)-states (transitions), respectively.

DEFINITION 7 \( N \)-\( G_d \)-state: A \( G_d \)-state \( x_d \) of the form \((x_1, x_2)\), where \( x_1(C) = x_2(C) = N \) is called an \( N \)-\( G_d \)-state.

\( F_i \)-\( G_d \)-state: A \( G_d \)-state of the form \((x_1, x_2)\), where \( F_i \in x_1(C) \) or \( F_i \notin x_2(C) \) is called an \( F_i \)-\( G_d \)-state.

DEFINITION 8 \( F_i \)-certain-\( G_d \)-state: A \( G_d \)-state of the form \((x_1, x_2)\) where \( F_i \in x_1(C) \) and \( F_i \notin x_2(C) \) is called an \( F_i \)-certain-\( G_d \)-state.

DEFINITION 9 \( F_i \)-uncertain-\( G_d \)-state: A \( G_d \)-state of the form \((x_1, x_2)\) where \( F_i \in x_1(C) \) and \( F_i \notin x_2(C) \) is called an \( F_i \)-uncertain-\( G_d \)-state.

It may be noted that an offending cycle for failure \( F_i \) is a cycle in \( G_d \) with only \( F_i \)-uncertain-\( G_d \)-states.

PROPERTY 1 If \( s_n \) is any trace in \( L(G_n) \), then there exists a trace \( s \) in \( L(G) \) such that \( s = P^{-1}(s_n) \). Roughly speaking, if only the measurable transitions of any trace \( s \) of \( G \) are considered in juxtaposition, then we can find a corresponding trace \( s_n \) of \( G_n \).

PROPERTY 2 For any trace \( s_n = (x_{n_1}, x_{n_1}, \ldots, x_{n_l}) \) of \( G_n \), where \( x_{n_i} \in X_0 \) and \( x_{n_i} \in X_n \), \( 1 \leq i \leq l \), the following holds:

1. \( x_{n_i}(C) = x_{n_{i+1}}(C) = \ldots = x_{n_l}(C) \), as the states form a cycle and any failure is permanent.
2. There exists a trace \( s \) of \( L(G) \) of the form \((s_1, s_2, \ldots, s_l)\) such that \( P(s) = (x_{n_1}, x_{n_1}, \ldots, x_{n_l}) \) and \( P(t) = (x_{n_1}, x_{n_{i+1}}, \ldots, x_{n_{j-1}}, x_{n_l}, x_{n_i}) \).

PROPERTY 3 For any path \( s_d = (x_{d_1}, x_{d_2}, \ldots, x_{d_l}, x_{d_k}) \) of \( G_d \), where \( x_{d_i} \in X_0 \) is of the form \((x_{n_1}, x_{n_2}) \) and \( 1 \leq i \leq l \), \( x_{d_0} \in X_d \) is of the form \((x_1, x_2) \), there are two measurement equivalent traces of \( L(G_n) \) corresponding to \( s_d \) as follows:

\((1)\) \( s^1_n = (x_{n_1}^1, x_{n_1}^1, \ldots, x_{n_i}^1, x_{n_i}^2, x_{n_i}^1, \ldots, x_{n_l}^1) \),

\((2)\) \( s^2_n = (x_{n_1}^2, x_{n_1}^2, \ldots, x_{n_i}^2, x_{n_i}^1, x_{n_i}^2, \ldots, x_{n_l}^2) \).

Two traces \( s^1_n \) and \( s^2_n \) may be the same \( G_n \)-trace also. If the \( G_d \)-cycle \((x_{d_1}, \ldots, x_{d_l}, x_{d_0}) = c_d \) is an offending cycle for any failure \( F_i \), then each of the \( G_d \)-state of \( c_d \) comprises one \( F_i \)-\( G_n \)-state and one non-\( F_i \)-\( G_n \)-state. In that case \( s^1_n \) and \( s^2_n \) are two different, but measurement equivalent, \( G_n \)-traces.

THEOREM 1 A DES model is \( F_i \)-diagnosable iff there is no offending cycle for failure \( F_i \) in \( G_d \).

An intuitive proof is presented for completeness; for details the reader may refer to Jiang et al. (2001). From Property 3, the existence of an offending cycle for failure \( F_i \) in \( G_d \) implies that there are at least two different, but measurement equivalent, syntactic cycles in \( G_n \) (corresponding to the offending cycle for \( F_i \)). By Property 2, there are two \( G \)-cycles, one comprising only non-\( F_i \)-states and the other comprising \( F_i \)-states. These cycles can be reached by measurement equivalent \( G \) traces (from a state in \( X_0 \)). This renders the DES model \( F_i \)-non-diagnosable because, at each point in the cycle, there exists uncertainty regarding the occurrence of \( F_i \) and the system may not exit from such a cycle. Therefore, \( F_i \) may not be diagnosed in finite time. For detailed proof and the complexity analysis, the reader is referred to Jiang et al. (2001).

Since the modified diagnosability analysis algorithm (for FDES models) presented in this paper also needs the computation of \( G_n \) and \( G_d \), we now determine the complexity of these two steps of Algorithm 1.

Complexity of Algorithm 1: Let the number of \( G \)-states be \( n \); the number of \( G \)-transitions \( t \) is \( O(n^2) \).

Step 1 Construction of \( X_0 \) in \( G_n \) involves searching all the \( G \)-states which is \( O(n) \). Construction of \( X_n = X_0 \) involves \( O(n^2 \cdot t) \) steps because there are \( n^2 \) state pairs and studying reachability of each of them involves \( O(t) \) steps. Hence, generation of \( G_n \) requires \( O(n + n^2 \cdot t) = O(n^2 \cdot t) = O(n^2 \cdot n^2) = O(n^6) \) steps.

Step 2 Generating \( G_d \) from \( G_n \) requires

(i) Construction of \( X_d \) by rule 2(a);

(ii) Construction of \( G_d \)-transitions emanating from each member \( (x_1, x_2) \) of \( X_d \) by rule 2(b)(i) and adding the successor pair \( (x^1_1, x^2_2) \) as non-initial \( G_d \)-state to \( X_d \).
(iii) Construction of $G_d$-transitions emanating from each member $\langle x_1, x_2 \rangle$ of $X_d - X_{d0}$ (non-initial $G_d$-states) by rule 2(b)(i) and adding the successor pair $(x_1', x_2')$ as non-initial $G_d$-state to $X_d$.

Step (i) is $O(n^2)$ and steps (ii) and (iii) together are $O(r^2) = O(n^4)$ because no transition pair of $G_n$ needs to be checked more than once. The non-initial $G_d$-states are generated hand-in-hand with the $G_d$-transitions as discussed above and thus do not require additional complexity. Hence, generation of $G_d$ from $G_n$ requires $O(n^4)$ steps.

Step 3 The complexity of checking the presence of any offending cycle for a failure $F_i$ is of the $O(n^4)$, explained as follows (Jiang et al., 2001). First, only $G_d$ states of type $x_d = (x_1, x_2)$, such that $F_i \in x_1(C)$ and $F_i \notin x_2(C)$ are retained. In other words, $G_d$ states $x_d = (x_1, x_4)$, such that $F_i \in x_1(C)$ and $F_i \notin x_4(C)$ are deleted. Also, transitions that emanate from or lead to $G_d$ states which are deleted are also eliminated. In the resultant $G_d$, if there is a cycle then it is an offending cycle for the failure $F_i$. The complexity of checking the presence of a cycle in a directed graph can be done using depth first search and involves complexity of the $O(|V| + |E|)$, where $|V|$ is the number of states and $|E|$ is the number of edges in the graph. As the number of states and transitions in $G_d$ are $n^2$ and $n^4$, respectively, in the worst case checking of offending cycle involves complexity of the $O(n^2 + n^4) = O(n^4)$.

The complexity of Algorithm 1 is $O(n^4 + n^4 + n^4) = O(n^4)$, that is, polynomial in the number of system states.

The algorithm above works with DES models where fairness of transitions is not ensured. In a system with all transitions fair, if there is an offending cycle with some transitions leading out of the cycle, then that cycle cannot execute infinitely at a stretch. Thus, the above theorem does not hold for such systems. In the next section, we depict a situation involving a failure which is diagnosable because of fairness of transitions but the corresponding $G_d$ contains an offending cycle for the failure $F_i$. Then, we preset in brief the traditional diagnoser-based scheme (Thorsley and Teneketzis, 2005) that solves the failure diagnosis problem in FDES models. There we highlight how the scheme addresses the fairness issue and how the complexity is exponential in a number of system states.

3. DES diagnosability for a fair system

3.1. DES diagnosability for the chemical reaction chamber

Let us consider a chemical reaction chamber where temperature ($T$) is maintained between 50°C and 70°C by switching a heater ON and OFF and pressure ($P$) is maintained between 80 and 90 cm of Hg by opening and closing a valve. A DES model having states $x_1$ through $x_8$ is shown in Figure 1(a). We consider only a heater stuck-off failure, designated as $F_1$. States $x_1$ to $x_4$ are normal and $x_5$ to $x_8$ are $F_1$-states. When the temperature falls below 50°C, a temperature controller changes $C_{H1}$ from 0 to 1 to put the heater ON. This is captured by transitions 1 and 5 in the normal condition and transitions 9 and 12 in the case of $F_1$. Similarly, when temperature reaches 70°C or more, the temperature controller changes $C_{H1}$ from 1 to 0 to put the heater OFF. This is captured by transitions 2 and 6 in the normal condition. It may be noted that in the case of failure $F_1$, the temperature does not rise and hence the corresponding transitions to put the heater OFF are absent. Similar control logic holds for the (normal) pressure control loop. The controller commands $C_{H1}$ (for the heater), $C_V$ (for the valve) and the signs of the rates $dP$ of $T$ and $dP$ of $P$ are measurable discrete variables. The following symbols are used to designate the states of the heater and the valve at various $G$ states: $H$: heater on, $H$: heater off, $H_S$: heater stuck-off, $H_v$: heater on, $V_G$: valve open, and $V_C$: valve closed.

The model $G_n$ for the system model $G$ is shown in Figure 1(b). In $G_n$, the two unmeasurable transitions of $G$, labelled as fault in Figure 1(a), are replaced by transitions numbered 15, 16, 17 and 18. The model $G_d$ is illustrated in Figure 1(c). Consider the cycle marked $c_d = \langle (x_1, x_5), (x_4, x_8) \rangle$ in Figure 1(c). $x_1(C) = N \neq x_5(C) = \{F_1\}$. Similarly, $x_4(C) = N \neq x_8(C) = \{F_1\}$. Hence, $c_d$ is an offending cycle for failure $F_1$. Hence, by the DES diagnosability condition reported in Jiang et al. (2001) and presented as Theorem 1 in the previous section, the failure is non-diagnosable.

The failure, however, is manifested in finite time. It may be noted that in the cycle $\langle x_5, x_8 \rangle$, the temperature keeps decreasing up to 50°C whereupon the cycle is exited. Consequently, the system reaches state $x_6$ or $x_7$ in finite time where failure can be detected because the corresponding normal states $x_5$ and $x_8$ have a different value for the measurable variable $dT$. More specifically, if the system is normal and the temperature falls below 50°C, the system reaches state $x_2$ (or $x_3$), where $C_{H1} = 1, C_V = 0, dP = -1$ and $dT = 1$ ($C_{H1} = 1, C_V = 1, dP = 1$ and $dT = 1$). In contrast, if the failure $F_1$ has occurred, then the system reaches state $x_6$ (or $x_7$) where $C_{H1} = 1, C_V = 0, dP = -1$ but $dT = -1$ ($C_{H1} = 1, C_V = 1, dP = 1$ but $dT = -1$). It may be noted that the difference is due to the fact that in the failure condition, even when $C_{H1} = 1$, the temperature keeps falling whereas it should be rising as in the normal condition. In short, the fact that the cycle $\langle x_5, x_8 \rangle$ cannot execute infinitely long results in manifestation of $F_1$ in finite time. This happens because the transition 9 from $x_5$ and the transition 12 from $x_8$ are fair.

This property is not apparent in the DES model because of the following reason.

The chemical reaction chamber is basically a hybrid system because it has, in addition to discrete variables $C_{H1}, C_V$, etc., continuous dynamics corresponding to temperature and pressure. The model illustrated in Figure 1(a) is a DES model where the enabling conditions
of the transitions and the continuous dynamics in the model states are abstracted out. It may be noted that with each model transition there is an implicit enabling condition that is a linear inequality over either of the continuous variables; for example, if the continuous variable $T$ (for temperature) were used explicitly, then the transitions 1, 5, 9, and 12 would have $T \leq 50^\circ C$ as the enabling condition. The enabling conditions are abstracted out in the DES model as we do not model (or measure) the continuous variables $T$ and $P$. Furthermore, in the DES model...
we retain *only the signs* of the rates of the continuous variables, e.g. $d_T = -1$ or $+1$ and not the accurate continuous dynamics of these (continuous) variables. Moreover, there is no special semantics associated with $d_T$ or $d_R$ unlike the rates used in the hybrid system model where the (absolute) rates are interpreted in terms of a ‘clock tick’ (i.e. say the rate of $T$ is $+5^\circ$C per unit time). As ‘clock tick’ is not modelled in DES, we cannot ascribe any semantics to the signs of the rates of the continuous variables to capture the accurate (continuous) dynamics. This abstraction of the continuous dynamics, in turn, abstracts out the fairness of transitions as indicated below.

Any system trace with the infinite suffix $\langle x_5, x_8, x_5, x_8, \ldots, \rangle$, which implies infinitely long execution of the cycle $\langle x_5, x_8 \rangle$, cannot happen in the system because the temperature keeps on decreasing without bound in such a suffix trace. The transitions $\langle x_5, x_6 \rangle$ and $\langle x_8, x_7 \rangle$ are unfair in the trace $\langle x_1, \ldots, x_5, x_8, x_5, x_8, \ldots \rangle$ as the trace visits the states $x_5$ and $x_8$ infinitely many times without taking these transitions infinitely often. We rule out such traces from the language generated by the DES models of the systems with (implicit) continuous dynamics (where all transitions are fair). In other words, fairness of transitions is explicitly imposed as an assumption of the DES models and we designate such models as FDES models. The following definitions are in order.

A transition $\tau = \langle x, x^+ \rangle$ is said to be *enabled* in a trace $s$ if $x$ is in $s$ and is said to be *taken* in $s$ if both $x$ and $x^+$ are in $s$.

**Definition 10 (Fair transitions:)** A transition $\tau = \langle x, x^+ \rangle$ is *fair* if there is no trace that visits $x$ indefinitely often without taking $\tau$ in it indefinitely often.

**Definition 11 (FDES Models)** A DES model in which all transitions are fair is called an FDES model.

The fairness assumption restricts the traces actually generated by $G$. Any sequence of transitions, constructed syntactically satisfying the confluence property, is not necessarily a member of $L(G)$. The assumption also implies that any cycle in $G$ having at least one transition out of the cycle can only be traversed a finite number of times consecutively.

### 3.2. Diagnoser-based FDD scheme for FDES models

*(Thorsley and Teneketzis, 2005)*

In this subsection we discuss in brief the traditional diagnoser-based FDD scheme proposed in Thorsley and Teneketzis (2005). The diagnosability condition to be checked for ascertaining if a fault is diagnosable in a fair system is called the $A$-diagnosability condition and comprises the following steps:

- Construct a logical diagnoser.
  The diagnoser is a directed graph $D = (Z, A)$, where $Z$ is the set of diagnoser states and $A$ is the set of diagnoser transitions. Each diagnoser state $z \in Z$ is an ordered set comprising a subset of equivalent $G$-states representing the uncertainty about the actual $G$-state and each diagnoser transition $a \in A$ is a set of equivalent $G$-transitions representing the uncertainty about the actual transition that occurs.

  - Associate probability matrix $\Phi_a$ with each diagnoser transition $a = (z, z^+)$. $\Phi_a$ represents probability of transitions from $G$-states in the diagnoser state $z$ to $G$ states in the diagnoser state $z^+$. If $z$ has $i$ $G$-states and $z^+$ has $j$ $G$-states, $\Phi_a$ is of dimension $i \times j$ ($i$ rows and $j$ columns). For a $G$-state $x_t \in z$ and another $G$-state $x_m \in z^+$, the probability of the transition $\tau \in a$ (from $x_t$ to $x_m$ in the model $G$) is represented by the $l$, $m$ element of $\Phi_a$ and denoted as $\Phi_{a_{lm}}$.

  - Find the recurrent and the non-recurrent $G$-states in the diagnoser states.

  A Markov matrix is generated from the diagnoser with the help of the probability matrices. Given each diagnoser state, it is determined if the $G$-states in the diagnoser state are recurrent or non-recurrent. A recurrent (non-recurrent) $G$-state if visited once, then the probability of visiting it again in finite number of transitions is 1 (0) and this condition holds indefinitely often.

  - Diagnosability condition (termed as $A$-diagnosability condition) check.

  If any $F_i$-uncertain diagnoser state contains a recurrent $F_i$-$G$-state, then fault is non-diagnosable, else diagnosable. The basic idea behind the condition is, if there is a recurrent $G$-state in any diagnoser state then that diagnoser state will be visited again and again with probability 1. If the diagnoser state under question is $F_i$-uncertain and the recurrent $G$-state is $F_j$-$G$-state, then $F_j$-certain diagnoser states will not be reached; this renders $F_i$ to be non-diagnosable. On the other hand, if all $F_i$-uncertain diagnoser states have non-recurrent $F_j$-$G$-states then $F_j$-certain diagnoser states will be reached in finite time after occurrence of failure $F_i$ with probability 1; this renders $F_i$ to be diagnosable. This condition can adequately handle FDES models.

  If there is a cycle of $F_j$-$G$-states with an outward transition then these $F_j$-$G$-states are non-recurrent. Therefore, even if these $F_j$-$G$-states are embedded in an $F_i$-uncertain diagnoser cycle, the fault is diagnosable because the $F_i$-uncertain diagnoser states (involved in the $F_i$-uncertain diagnoser cycle) do not have recurrent $F_j$-$G$-states.

Now we discuss the computational complexity of the $A$-diagnosability checking scheme.

**Computational complexity**

- If $n$ is the number of $G$-states then the number of diagnoser states can be $O(2^n) = n_d$. As each
diagnoser state comprises a subset of (measurement equivalent) G-states, so all possible diagnoser states is power set of G-states. Therefore, the complexity of constructing a diagnoser is \(O(2^n)\). The number of G-transitions can be \(O(n^2)\) denoted as \(t_d\) and diagnoser transitions can be \(O(n_d^2)\) denoted as \(t_d\).

- The probability transition matrices have dimensions of the \(O(n \times n)\) because each diagnoser state can have \(O(n)\) G-states. The value of any \(i, j\) element of such a matrix is the probability of the corresponding G-transition. The complexity of generating one matrix is \(O(n^2)\) because it involves considering probability values of all G-transitions in the worst case. Complexity of generating these matrices for all diagnoser transitions is \(O(n^2 \times t_d)\).
- From the Markov matrix, recurrent and non-recurrent G-states in the diagnoser states can be determined using the scheme proposed in Xie and Beerel (1998a) and involves a complexity \(O((n_d \times n)^2)\).
- \(A\)-diagnosability condition checking would involve verifying each \(F_i\)-uncertain diagnoser state and containment of any recurrent \(F_i\)-G-state; that is the worst case would involve a complexity \(O(n_d \times n)\).

Hence, the total complexity of \(A\)-diagnosability is \(O(2^n + (n^2 \times t_d) + ((n_d \times n)^2) + (n_d \times n))\). Substituting \(t_d\) with \(n_d^2\) we obtain the complexity of \(A\)-diagnosability as \(O(2^n + (n^2 \times n_d^2) + ((n_d \times n)^2) + (n_d \times n))\). As \(n_d = O(2^n)\), the complexity can be written as \(O(2^n + (n^2 \times 2^{2n}) + (2^n \times n^2) + (2^n \times n))\). Therefore, it can be concluded that the traditional diagnoser-based \(A\)-diagnosability scheme is exponential (i.e., \(O(2^n)\)) in number of G-states.

Note: We have represented the steps of \(A\)-diagnosability analysis and their computational complexity in an over simplified manner, just required to highlight the fairness handling capability and the exponential complexity. For a more complete analysis, the readers are referred to Thorsley and Teneketzis (2005) and Biswas et al. (2010).

### 4. A new polynomial time condition for FDES diagnosability

In this section, we propose a new condition for FDES diagnosability taking fairness of transitions into account. Henceforth, we use \(G\) to represent FDES models; whenever \(G\) is used for DES models, it would be denoted explicitly.

Before we formalize, the new condition certain definitions are introduced.

**Definition 12**: Recurrent States: A state (node) \(x\) in a directed graph \(G\) is said to be recurrent if any (infinite) trace \(s\) of \(G\) that visits \(x\) once, visits \(x\) infinitely often.

**Definition 13**: SCC of a Directed Graph: A maximal connected sub-graph of a directed graph \(G\) is called a connected component of \(G\). A connected component of a directed graph \(G\) is said to be an SCC, if for every pair \((x_1, x_2)\) of states in the component (subgraph), there is a path from \(x_1\) to \(x_2\) and vice-versa.

- The set of SCCs of \(G\) is denoted as \(C\). Any \(c \in C\) comprises a subset of \(G\)-states and such \(G\)-states are termed as \(G\)-states in the SCC \(c\). Similarly, \(G\)-transitions in \(c\) is given by the set \(\{\tau | \tau \in \Sigma \text{ and initial}(\tau), \text{final}(\tau) \in c\}\).

**Definition 14**: Maximal SCCs: Let a partial order \(\leq\) \((C \times C)\) be defined as: \(c_1 \leq c_2\), if some state in \(c_2\) is reachable from some state in \(c_1\).

- The set of maximal elements of the poset \(\langle C, \leq \rangle\) is denoted as \(C_{\text{max}}\). Clearly, from any \(c_{\text{max}} \in C_{\text{max}}\), there is no path to any other SCC. The SCCs in \(C_{\text{max}}\) are referred to as maximal SCCs.

It may be observed that in a directed graph corresponding to an FDES model, the states in any \(c \notin C_{\text{max}}\) are the non-recurrent states. This is because, if some state in \(c_{\text{max}} \in C_{\text{max}}\) is reached, then only the states in \(c_{\text{max}}\) can be visited infinitely often and a trace taken to reach \(c_{\text{max}}\) passes through the intermediate states that are never visited again after it reaches \(c_{\text{max}}\). The details on the relationship of recurrence of states with SCCs can be found in Nuutila and Soisalon-Soininen (1994) and Xie and Beerel (1998b).

**Definition 15**: \(F_i\)-Diagnosability for an FDES model: An FDES model \(G\) is said to be \(F_i\)-diagnosable for a failure \(F_i\) under a measurement limitation if the following holds \(\exists n \in \mathbb{N} \forall s \in \Psi(X_{Fi}) \exists \tau \in L_{Fi}(G) (s)(|t| \geq n \Rightarrow D))\), where \(D = \forall u \in P^{-1}[P(st)], \text{final}(u) \in X_{Fi}\).

It may be noted that the definition for \(F_i\)-Diagnosability for DES models (Definition 6) and that for \(F_i\)-Diagnosability for FDES models is the same except for the language \(L(G)\).

### 4.1. A condition for FDES diagnosability

As shown in Section 3, a failure may be diagnosable in spite of the presence of an offending cycle for the failure \((F_i)\) in \(G_d\) (Figure 1). If there is an outward transition from the \(F_i\)-\(G_d\)-cycle, then this cycle will not move infinitely long at a stretch. Furthermore, corresponding to this outward \(F_i\)-\(G_d\)-transition (from the \(F_i\)-\(G_d\)-cycle), if there is no measurement equivalent non-\(F_i\)-\(G_d\)-transition (from the non-\(F_i\)-\(G_d\)-cycle), then the failure is diagnosed in finite time. It may be noted that in the example of the chemical reaction chamber (shown in Figure 1(c)), corresponding to the \(F_i\)-offending cycle \((x_1, x_2, (x_4, x_7))\) the \(F_i\)-\(G_d\)-cycle is \((x_5, x_8)\) and the non-\(F_i\)-\(G_d\)-cycle is \((x_1, x_4)\). There are outward \(F_i\)-\(G_d\)-transitions from the \(F_i\)-\(G_d\)-cycle \((x_5, x_8)\), namely, 9 and 12; there is no measurement equivalent
non-$F_1$-$G_d$-transition corresponding to 9 and 12 emanating from the non-$F_1$-$G_n$-cycle $(x_1, x_4)$. Hence, the presence of this $F_1$-offending cycle does not hamper $F_1$-diagnosability. In contrast, the traces of an FDES model (e.g. $G_n$) may remain infinitely long only in the maximal SCCs (of $G_n$). Hence, to analyse failure diagnosability of $F_i$, we need to find SCCs in $G_n$ with $F_i$-uncertain states that has an embedded maximal SCC of $G_n$. This motivates the following definition.

**Definition 16** Terminal offending $F_i$-SCCs: An SCC $c_{d}$ of $G_d$ is said to be a terminal offending $F_i$-SCC, if it comprises $F_i$-uncertain $G_d$-states $(x_1^1, x_2^1), (x_1^2, x_2^2), \ldots, (x_1^n, x_2^n)$ such that there exists a maximal $G_n$-SCC $c_{n(n_{\text{max})}} = \{x_1^n, x_2^n, \ldots, x_4^n\}$, where $x_1^n, x_2^n$ are $F_i$-uncertain $G_d$-states.

The intuitive logic behind the equivalence of $F_i$-diagnosability of an FDES model with the absence of terminal offending $F_i$-SCC is as follows. A terminal offending $F_i$-SCC $c_{d}$ contains a (maximal) $F_i$-$G_n$-SCC having all transitions emanating from states of that $F_i$-$G_n$-SCC in some $G_d$-transitions of $c_{d}$. The states in $c_{d}$ are $F_i$-uncertain. Hence, corresponding to the $F_i$-$G_n$-SCC in question, there is another $G_n$-SCC of non-$F_i$ states and the transitions involved in the traces generated by traversing both these SCCs are measurement equivalent. Thus, as long as the system (after failure $F_i$) moves in the $F_i$-$G_n$-SCC the failure cannot be diagnosed. As the $F_i$-$G_n$-SCC is maximal, the system after failure may move in that $F_i$-$G_n$-SCC under question infinitely long (even in an FDES framework); so the failure will not be diagnosed in finite time.

The structure $G_d$ for the chemical reaction chamber example shown in Figure 1(c) has an $F_i$-uncertain SCC $c_{d}$, which is not a terminal offending $F_i$-SCC because the $F_i$-$G_n$-states $x_5$ and $x_8$ contained in $c_{d}$ do not belong to any $c_{n(n_{\text{max})}} \in C_{n(n_{\text{max})}} = \{x_5, x_8\}$. Hence, the failure is FDES-diagnosable in keeping with the intuitive discussion included in the last section.

Before we prove formally the equivalence of $F_i$-diagnosability of FDES models and the absence of a terminal offending $F_i$-SCC in $G_d$, we introduce the following properties that follow from the construction of $G_n$ and $G_d$.

**Property 4** For any $G_d$-SCC $c_{d} = \{x_1, \ldots, x_d\}$ there are two SCCs in $G_n$, not necessarily distinct, given by

1. $c_{n}^{1} = \{x_1^n, \ldots, x_k^n\} \cup X_1^n$, where $x_1^n \in x_1, 1 \leq i \leq k$, (i.e. these are states of $c_{n}^{1}$ that are in $c_{d}$) and $X_1^n$ is the subset of states of $c_{d}$ that are not in $c_{d}$.
2. $c_{n}^{2} = \{x_1^n, \ldots, x_k^n\} \cup X_2^n$, where $x_1^n \in x_1, 1 \leq i \leq k$, (i.e. these are states of $c_{n}^{2}$ that are in $c_{d}$) and $X_2^n$ is the subset of states of $c_{n}^{2}$ that are not in $c_{d}$, such that $x_1^n Ex_2^n, 1 \leq i \leq k$.

**Proof** The fact that the SCCs $c_{n}^{1}$ and $c_{n}^{2}$ may contain $G_{n}$-states which do not pair up as $c_{d}$ states follows from the following observation. There may be transitions emanating from a state in $\{x_1, \ldots, x_i\}$ and terminating in a state in $X_1^n$ for which there is no measurement equivalent transition emanating from a state in $\{x_1^n, \ldots, x_k^n\}$ and terminating in a state in $X_2^n$, or vice-versa.

This may be observed in the example of the chemical reaction shown in Figure 1(c). In the $G_d$-SCC $c_{d}$ of the example, $G_{n}$-SCC2 is embedded totally in $c_{d}$; however, only two states (namely, $x_1$ and $x_4$) of the $G_{n}$-SCC1 are contained in $c_{d}$ while other two states (namely, $x_2$ and $x_3$) are not. So, $X_1^n = \phi$ and $X_2^n = \{x_2, x_3\}$.

**Property 5** Let $s$ be a trace of $G$ such that $P(s) = (\tau_1, \ldots, \tau_l)$. There is a path in $G_d$ corresponding to $s$, namely $s_d = (\tau_1, \ldots, \tau_l)$, such that $\tau_i \in \tau_d, 1 \leq i \leq l$. It implies that each transition of $s_d$ contains a transition from $P(s)$ as one of its two members. If $s_d$ also corresponds to another sequence of $G$-transitions, $s'$ say, then $s'$ starts from an initial state of $G$ and is measurement equivalent with $s$.

The proof follows from the definition of $G_d$-transitions.

**Property 6** In any $G_d$-SCC $c_{d}$, $F_i$-ceratin $G_d$-states cannot coexist with $F_i$-uncertain $G_d$-states or $N$-$G_d$-states. The proof follows from the permanence of failures.

**Theorem 2** An FDES model is $F_i$-diagnosable iff there is no terminal offending $F_i$-SCC in $G_d$.

**Proof** ($\Rightarrow$): Let $G$ be $F_i$-diagnosable. Let there be a terminal offending $F_i$-SCC in $G_d$, namely $c_{d} = \{x_1, x_2, \ldots, x_d\}$. By Property 4, there are two SCCs of $G_n$ in $c_{d}$ namely, $c_{n}^{1}$ and $c_{n}^{2}$. From the definition of terminal offending $F_i$-SCC, as $F_i \in x_1^n (C)$ and $F_i \notin x_2^n (C)$ for $1 \leq j \leq k$, $c_{n}^{1}$ and $c_{n}^{2}$ are not the same. Also, $c_{n}^{1} \in C_{n(n_{\text{max})}}$ and has no transition that is contained in a $G_d$-transition that leads out of $c_{d}$. In other words, $c_{n}^{1}$ is completely embedded in $c_{d}$ and hence $X_1^n = \phi$. Furthermore, since all the model states are reachable, there is a $G$-trace that leads to a state in $c_{n}^{1}$ from an initial $G$-state. Obviously, final($s_1$) = $X_{F_i}$. All the extensions of this $G$-trace remain confined in $c_{n}^{1}$ because it is a maximal SCC; also, $X_{n} = \phi$. Hence, $\forall n_{F_i} \geq 1$, an extension of $s_1$ can be constructed as $s_1t_1$ which does not leave $c_{n}^{1}$. By Property 5, there is also a trace $u$ say, (which is measurement equivalent to $s_1t_1$, i.e., $u \in P^{-1}(P(s_1))$ for $c_{n}^{2}$ that comprises non-$F_i$-states and hence final($u$) $\notin X_{F_i}$. So $G$ is $F_i$-non-diagnosable. (Contradiction)

($\Leftarrow$): Let there be no terminal offending $F_i$-SCC in $G_d$. Let $G$ be $F_i$-nondiagnosable. Then by negating the
diagnosability Definition (15),

\[ \forall n_{F_i} \in \mathbb{N}, \exists s \in \Psi(F_{X_{F_i}}), \exists t \in L(G) / \]
\[ s[t] > n \land \exists u \in P^{-1}(P_{st}) \land \text{final}(u) \not\in X_{F_i}, \]

(5)

final(st) = final(t) ∈ X_{F_i} because final(s) ∈ X_{F_i} and F_i is permanent. By Property 5, there is a path s_d = (τ_1, ..., τ_t) in G_d corresponding to st. Since u ∈ P^{-1}(P_{st}), (i.e. u is measurement equivalent to st), s_d also corresponds to u. As s_d corresponds to st, where final(st) ∈ X_{F_i}, and to u, where final(u) ∉ X_{F_i}, s_d ends in an F_i-uncertain G_d state, say. Since (Equation (5)) holds for any n_{F_i} ∈ \mathbb{N}, t can be taken to be arbitrarily long so that the length of the G_n-path t is greater than the number of states in G_n. Hence, t is of the form t_1t_2 where t_2 is confined in a maximal G_n-SCC c_n, say. Furthermore, s_t and u are measurement equivalent traces; let u lead to u_2 such that u_2 is measurement equivalent to t_2. Thus, the G_n-states of t_2 are embedded entirely in some G_n'-SCC, c_d say, and the G_n-states of t_2 are also in c_d. As t_2 comprises F_i-G_n-states and t_2 comprises non-F_i-G_n-states, c_d is an F_i-uncertain G_d-SCC. As there is a maximal F_i-G_n-SCC c_n that is embedded in an F_i-uncertain G_d-SCC, from the definition of ‘terminal offending Fi-SCC’ (Definition 16), c_d is a terminal offending F_i-SCC in G_d. (Contradiction)

The diagnosability analysis algorithm that follows from Theorem 2 for the F_i-diagnosability analysis of FDES models (for a given failure F_i) is given below:

**ALGORITHM 2**

**Input:** An FDES Model G.

**Output:** Diagnosability of G for a fault F_i.

1. Obtain DES G_n = (V_{X_{F_i}}, X_{F_i}, X_n) from G = (V_{X_{F_i}}, X_{F_i}, X_0) (same as Step-1 of Algorithm 1).
2. Compute G_d (same as Step-2 of Algorithm 1).
3. Compute C_d, the set of SCCs of G_d.
4. Check if any c_d ∈ C_d is a terminal offending F_i-SCC. If there is one such SCC in G_d, then the system in non-diagnosable for failure F_i, otherwise, it is diagnosable for failure F_i.

**4.2. Complexity analysis**

**Complexity of Algorithm 2**

Both Step 1 and Step 2 are \( O(n^4) \) as discussed in Section 2.3.

Step 3 This step requires \( O(n^2 + r^2) = O(n^4) \), i.e. the time for finding the G_d-SCCs (Nuutila and Soisalon-Soininen, 1994).

Step 4 For each c_d ∈ C_d the following sub-steps are required to determine if c_d is a terminal offending F_i-G_n-SCC.

- Step 4(i) Check that one of the component G_n-states in any state of c_d is an F_i-state and the other is a non-F_i-state.
- Step 4(ii) Generate G_n'-SCCs and mark the maximal SCCs, i.e. construct \( C_{n(max)} \).
- Step 4(iii) Locate a maximal SCC \( c_{n(max)} \) ∈ \( C_{n(max)} \) such that all the F_i-states of G_n that are in any state of c_d are from the maximal SCC \( c_{n(max)} \).
- Step 4(iv): Check that none of the transitions of \( c_{n(max)} \) is in an outgoing transition from c_d.
- Step 4(i) through step 4(iv) are repeated for all G_d-SCCs.

Step 4(i) is \( O(n^2) \) as in the worst case, each G_d-SCC may have \( n^2 \) states and this step involves vising each state in c_d and checking the failure labels of the two component G_n-states. Step 4(ii) requires \( O(n + t + 1) \) steps as follows. Generating G_n-SCCs is \( O(n + t) \) and finding \( C_{n(max)} \) involves construction of the relational matrix \( R_{G} \) of \( (C_{n}, \leq) \) and identification of the rows of \( R_{G} \) having all elements as zeros except the diagonal elements. This can be done in \( O(t) \) time by examining the G_n-transitions. This is because, in the relational matrix of any partial order, the row corresponding to any maximal element has all zeros except in the diagonal element. Step 4(iii) requires checking the F_i-G_n-states in c_d vis-a-vis all the G_n-states in \( c_{n(max)} \); this involves \( (n^2) + (n \cdot n) = O(n^3) \) steps. This is because finding all the F_i-G_n-states that are in c_d requires checking the F_i-G_n-states in each of the states of c_d. Furthermore, checking if all the G_n-states in c_d are in \( c_{n(max)} \) requires checking the G_n-states in c_d vis-a-vis the G_n-states in \( c_{n(max)} \) and there can be \( O(n) \) maximal G_n-SCCs (i.e. \( |C_{n(max)}| = n \)). Step 4(iv) requires checking each G_n-transition of \( c_{n(max)} \) vis-a-vis the outgoing transitions of c_d, which in the worst case is \( O(t \cdot r) \). Complexity of step 4(i) through step 4(iv) is \( O((n^2) + (n + t + 1) + (n^3) + (t \cdot r)) = O(n^3 + n^2 + t + n^3 + t \cdot r) = O(3 \cdot O(n^3) = O(n^3)). \) As Step 4(i) through Step 4(iv) are to be repeated for all G_d-SCCs, detecting terminal offending F_i-SCC is \( O(n^2 \cdot n^2) = O(n^4) \) as in the worst case there may be \( O(n^2) \) G_d-SCCs (i.e. when each state of G_d is an SCC).

Thus, the overall complexity of Algorithm 2 is \( O(n^4 + n^4 + n^4 + n^8) = O(n^8) \). Without loss of generality, if we assume that all failures involve the same number of system states and transitions, then it may be shown that F_i-diagnosability analysis for FDES models is \( O(n^8/p) \). Therefore, when we repeat for all failures, the complexity figure is not increased. The detailed calculation is avoided for simplicity. Thus, the overall complexity of the scheme for FDES diagnosability analysis is polynomial in the number of system states.

As already discussed, the complexity of classical polynomial time algorithm (Algorithm 1) is \( O(n^4) \). Therefore, we can see that complexity of FDES polynomial time
diagnosability analysis is higher than that of classical polynomial time diagnosability analysis, however, the order is same. Therefore, we can conclude that incorporating fairness in the polynomial time diagnosability framework increases the complexity but maintains the order.

5. Conclusion

The DES framework has been found to be applicable for FDD of a wide range of systems, even including those having continuous dynamics. For such hybrid systems, DES paradigm partitions the continuous state space and captures each subspace as a discrete state. The DES framework facilitates simplistic modelling and failure analysis algorithms. Furthermore, it has been seen that most of the failures can be detected even if their effect is abstracted in terms of discrete state space. The first series of FDD algorithms were based on a diagnoser which is a state estimator of the system. It basically performs the following two functions—(i) diagnosability analysis, where certain conditions on the diagnoser are checked off line to determine if failure can be diagnosed within finite time of its occurrence and (ii) online fault diagnosis. The classical scheme suffers from two drawbacks, namely, (i) exponential complexity and (ii) improper diagnosis of fair systems having continuous dynamics. These two problems have been solved independently in the literature. In this paper, we have addressed both these problems together in an unified approach.

We have discussed in this paper how the DES framework has been enhanced to handle fair systems (Thorsley and Teneketzis, 2005; Biswas et al., 2010) by using the concept of recurrent and non-recurrent states. The major idea is to check the impact of only the recurrent states in diagnosability analysis. No system trace passes over the non-recurrent states after a finite time and hence they need not be used in diagnosability checking. Then, the computational complexity of these schemes has been derived and shown to be exponential with respect to the system states. We have also presented in this paper the schemes that have handled the complexity issue (Jiang et al., 2001; Tae-Yoo and Lafortune, 2002). These frameworks use a product automata, instead of diagnoser to derive the diagnosability results. As the use of diagnoser is avoided, these schemes have polynomial time complexity. However, the product automata cannot be used for online diagnosis. The motivation of still using these polynomial schemes is to first check diagnosability using a simple scheme. Only when diagnosability is assured a diagnoser can be constructed else, appropriate steps, such as increasing measurement points, improving sensor quality, etc. need to be taken. However, how wrong diagnosability inferences can be given if these polynomial schemes are applied on fair systems have been identified and demonstrated using a simple example in this paper.

To address the above situation we developed an FDD framework for FDES models but involving only polynomial time complexity. Given an FDES model, first unmeasurable transitions are eliminated. Then, an automaton is generated by strict composition of the resultant FDES model with itself. In that automaton, we check for ‘terminal offending SCCs’. Such SCCs are composed of $F_\tau$-uncertain states and may not exit in finite time because the corresponding system states are recurrent. Hence, the presence of such SCCs render a failure nondiagnosable. If no such SCCs are present, the fault is diagnosable. The working of the theory has been illustrated using the example of a simple chemical reaction chamber. Also, the scheme has been formally shown to be working properly by proving the correctness and completeness of the ‘terminal offending SCCs’ based condition.

The scheme proposed in this paper works for FDES where all transitions are fair. In general, however, a system may have some transitions fair and some unfair (Biswas et al., 2010). If the unfair and fair transitions are identified then there exits an algorithm (Biswas et al., 2006) that can transform the DES model with unfair and fair transitions to an equivalent DES model with only fair transitions (i.e. FDES model). This generalizes the given diagnosability algorithm for FDES models to general DES models with fair and unfair transitions provided unfair transitions are identified explicitly.

It is desirable that given any DES model, the unfair transitions be detected algorithmically. This work can be accomplished using symbolic model checking of the corresponding hybrid system models. Several computational tree logic model checkers have been reported in the literature for hybrid systems, namely, HyTech (Alur, Courcoubetis, Henzinger, and Ho, 1993), CheckMate (Chutinan and Krogh, 1999) and PHAVer (Frehse, 2005). To verify unfairness of a transition $\tau = (x, x')$, we need to verify symbolically that (i) there is a path where $x$ is visited infinitely often, and (ii) in that path, $e_\tau$ is not satisfied in future forever. All these techniques call for specifying the initial states/values of the continuous variables. However, it may be noted that this technique is incomplete for generalized classes of hybrid automata and partially decidable for linear hybrid systems (LHS) (Alur et al., 1993; Alur, Henzinger, and Ho, 1996). The details of symbolic model checking algorithms for LHS are discussed in Alur et al. (1993) and Alur et al. (1996).

Disclosure statement

No potential conflict of interest was reported by the authors.

Note

1. Two approaches (Thorsley and Teneketzis, 2005; Biswas et al., 2010) have solved the same problem in a slightly different manner. In this paper, we discuss the scheme proposed in Thorsley and Teneketzis (2005); equivalence between these schemes has been shown (Biswas, 2013).
References

Alur, R., Courcoubetis, C., Henzinger, T. A., & Ho, P.-H. (1993). Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems. In R. L. Grossman, A. Nerode, A. P. Ravn, & H. Rischel (Eds.), *Hybrid Systems, LNCS 736* (pp. 209–229). Heidelberg: Springer.

Alur, R., Henzinger, T. A., & Ho, P.-H. (1996). Automatic symbolic verification of embedded systems. *IEEE Transactions on Software Engineering, 22*, 181–201.

Bavishi, S., & Chong, E. (1994). Automated fault diagnosis using a discrete event systems framework. *IEEE International Symposium Intelligent Control*, 213–218.

Biswas, S. (2013). Equivalence of fair diagnosability and stochastic diagnosability of discrete event systems. *IEEE SMC, Manchester*, pp. 378–383.

Biswas, S., Karfa, C., Kanwar, H., Sarkar, D., Mukhopadhyay, S., & Patra, A. (2006). Fairness of transitions in diagnosability analysis of hybrid systems. *American Control Conference 2006, Minneapolis, MN*, pp. 2664–2669.

Biswas, S., Sarkar, D., Mukhopadhyay, S., & Patra, A. (2010). Fairness of transitions in diagnosability of discrete event systems. *Journal of Discrete Event Dynamic Systems: Theory and Applications, 20*(3), 349–376.

Chutinan, A., & Krogh, B. (1999). Verification of polyhedral-invariant hybrid automata using polygonal flow pipe approximations. *International Workshop on Hybrid Systems: Computation and Control*, 76–90.

Debouk, R., Lafortune, S., & Teneketzis, D. (1998). Coordinated decentralized protocols for failure diagnosis of discrete event systems. Proceeding of the 37th IEEE Conference on Decision and Control, Tampa, FL, pp. 3763–3768.

Frehse, G. (2005). Phaver: Algorithmic verification of hybrid systems past hytech. *International Workshop on Hybrid Systems: Computation and Control*, 258–273.

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

Lafortune, S., Teneketzis, D., Sampath, M., Sengupta, R., & Sinnamohideen, K. (2001). Failure diagnosis of dynamic systems: An approach based on discrete event systems. American Control Conference, Arlington, VA, pp. 2058–2071.

Lamperti, G., & Zanella, M. (1999). Diagnosis of discrete event systems integrating synchronous and asynchronous behavior. 9th International workshop on principles of diagnosis (pp. 129–139).

Lin, F., & Wonham., W. M. (1988). On observability of discrete event system. *Information Sciences, 44*, 173–198.

Liu, F. (2014). Polynomial-time verification of diagnosability of fuzzy discrete event systems. *Science China Information Sciences, 57*(6), 1–10.

Moreira, M. V., Jesus, T. C., & Basilio, J. C. (2011). Polynomial time verification of decentralized diagnosability of discrete event systems. *IEEE Transaction on Automation Control, 56*(7), 1679–1684.

Nuutila, E., & Soisalon-Soininen, E. (1994). On finding the strongly connected components in a directed graph. *Information Processing Letters, 49*, 9–14.

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

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., & Teneketzis, D. C. (1996). Failure diagnosis using discrete-event models. *IEEE Transaction on Control Systems Technology, 4*(2), 105–124.

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

Xie, A., & Beerel, P. A. (1998a). Efficient state classification of finite-state Markov chains. *IEEE Transaction on CAD Circuits System, 17*(12), 1334–1339.

Xie, A., & Beerel, P. A. (1998b). Efficient state classification of finite-state Markov chains. *IEEE Transaction on CAD of Circuits and Systems, 17*(12), 1334–1339.

Yoo, T.-S., & Lafortune, S. (2002). Polynomial time verification of diagnosability of partially observed discrete event systems. *IEEE T Automatic Control, 129–139.

Zad, S. H., Kwong, R. H., & Wonham, W. M. (2003). Fault diagnosis in discrete-event systems: Framework and model reduction. *IEEE Transaction on Automatic Control, 48*(7), 1199–1212.

Zad, S. H., Kwong, R. H., & Wonham, W. M. (2005). Fault diagnosis in discrete-event systems: Incorporating timing information. *IEEE Transaction on Automatic Control, 50*(7), 1010–1015.