Diagnosability in Switched Linear Systems

Lizette Rubio- Gómez[1], David Gómez-Gutiérrez[1], Antonio Ramírez-Treviño[1], Javier Ruiz-León[1] and Guillermo Ramírez-Prado[2]
[1]Centro de Investigaciones y de Estudios Avanzados del IPN Unidad Guadalajara, México.
[2]Universidad Autónoma de Aguascalientes, México.

1. Introduction

This work is concerned with fault detection of Switched Linear Systems (*SLS*) and the design of asymptotic diagnosers for this class of systems. In the approach herein addressed a system can evolve from a normal behavior to a faulty behavior selected from an a priori known set of possible faulty behaviors. The faulty or normal behaviors are represented by a family of Linear Systems (*LS*) and an Interpreted Petri Net (*IPN*) is used to represent the way in which the normal and faulty behaviors are visited. Moreover, there could exist several *LS* representing the system normal behavior in some operation points. Notice that several real systems can be represented with this model, for instance power systems can be represented by a family of *LS*, one for each operation point and one for each fault.

In *LS* there are works dealing with continuous fault diagnosis. In (Massoumnia et al., 1989) a residue is used to show when a fault f_i can be detected in the system. Fault f_i can be seen on the output of a residual model for fault f_i. However the number of faults that may be detected is restricted to the range of the output matrix. In (Gertler et al., 2002) the design of residual diagnosers is proposed.

The diagnosability in Discrete Event Systems (*DES*) has been addressed using Finite Automata (*FA*) (Sampath et al 1995), where a *DES* is diagnosable if there is no F_i indeterminate cycles. Some extensions have been made to previous work, as (Hashtrudi-Zad et al., 2003), where the diagnoser and the system are allowed to start in different initial conditions. Diagnosability in *DES* has been also addressed using Petri Nets (*PN*) (Hadjicostis et al., 1999), (Hadjicostis et al., 2000) where a fault is detected if a conservative marking law is not fulfilled. In (Ramirez et al., 2007) a fault is detected when a siphon is unmarked, leading to a deadlock in the whole *PN*.

In (Fourlas et al., 2005) and (Fourlas 2009) the problem of fault diagnosability in hybrid system was addressed. That approach detects and isolates faults using the event sequences and associating to each faulty event a guard that can be taken from the continuous variables or discrete labels. The way in which continuous variables are chosen, however, is not mentioned.

This work is focused in fault diagnosis of systems where the set of potential faults can be a priori known. However the occurrence of them in real time needs to be detected and isolated. A normal assumption followed in this work is that the faults are fired from certain system states, i.e. they cannot occur everywhere. For instance, a motor can be broken if it is working.

In the present work the diagnosability is addressed combining the residue generation, distinguishability and indeterminate cycles. Fault rises are represented by the firing of some *PN* transitions, herein named faulty transitions. Thus the *SLS* jump from one *LS* representing a normal behavior to another *LS* representing a faulty behavior by the firing of faulty transitions. Thus the fault detection and isolation could be carried out by detecting or computing the firing of such faulty transitions. In order to do such task, the knowledge of both, continuous and discrete parts of the input-output *SLS* information, are used.

In particular, the firing of a faulty transition can be detected if it is event detectable. This concept was derived for *IPN* (Ramirez et al., 2007), now this concept is extended to *SLS* in the three following ways.

If the faults are detectable in the sense introduced in (Massoumnia et al., 1989) then a set of residue generators, one generator per fault, can be built. Thus, when the output of generator representing fault f_i is different from zero, then that transition t_{f_i} (representing fault f_i) was fired for sure, i.e. the fault and the firing of a faulty transition was detected and isolated.

If the *LS* Σ_a evolving before the firing of a faulty transition t_{f_i} is distinguishable from the *LS* Σ_b evolving after the firing of t_{f_i} then the firing of t_{f_i} can be detected and isolated by computing which *LS* systems is evolving, either Σ_a or Σ_b.

If the firing of a faulty transition cannot be detected because it is not event detectable, the faults are not detectable as in (Massoumnia et al., 1989) and distinguishability does not hold, then the not firing of a faulty transition can be detected if the firing of transitions representing the *SLS* normal behavior is detected.

This paper is organized as follows. In Section 2 the background of *LS*, and *IPN* are presented, as well as the *SLS* definition and diagnosability in *SLS*. In Section 3 the characterization of diagnosability using the concepts of distinguishability and event detectable is presented. The diagnoser design is presented in Section 4, and an illustrative example is reported in Section 5. The last section presents the conclusions and future work.

2. Preliminaries

Through this work, *SLS* are represented by the tuple $\langle \mathcal{F}, (Q, M_0) \rangle$, where $\mathcal{F}$ is a family of continuous *LS* and (Q, M_0) is an *IPN*. Next two subsections are devoted to briefly present these dynamical systems. An interested reader can consult (Chen, 1970; Wonham, 1979) for *LS*, and (Desel and Esparza, 1995; Rivera-Rangel, 2005) for Petri nets and interpreted Petri nets. Afterwards, the formal definition of *SLS* is presented.

2.1 Linear systems

Definition 2.1 A Linear System *(LS)* is described by for all t≥0

$$\Sigma \begin{cases} \dot{x}(\tau) = Ax(\tau) + Bu(\tau), \quad x(\tau_0) = x_0 \\ y(\tau) = Cx(\tau) \end{cases} \tag{2.1}$$

where $x \in \mathbb{R}^n$ is the state vector, $u \in \mathbb{R}^p$ is the system input vector, $y \in \mathbb{R}^q$ is the system output vector, and A, B, and C are, respectively, $n \times n$, $n \times p$ and $q \times n$ constant matrices. The state space of the dynamical equation (2.1) is $\mathcal{X}$.

Through this work, equation (2.1) will be referred as the *LS* $\Sigma(A, B, C)$ or simply system Σ.

Definition 2.2 A *LS*, $\Sigma(\mathrm{A,B,C})$, is said to be observable at τ_0 if there exists a finite $\tau_1 > \tau_0$ such that for any state x_0 at time τ_0, the knowledge of the input $u[\tau_0, \tau_1]$ and the output $y[\tau_0, \tau_1]$ over the time interval $[\tau_0, \tau_1]$ suffices to determine the state x_0. Otherwise, the dynamic equation $\Sigma(\mathrm{A,B,C})$ is said to be unobservable at τ_0.

Theorem 2.3 Let $\Sigma(\mathrm{A,B,C})$ be a *LS*. Then $\Sigma(\mathrm{A,B,C})$ is observable if and only if the unobservable subspace $\mathcal{N} \subseteq \mathcal{X}$ of $\Sigma(\mathrm{A,B,C})$ is the trivial subspace 0, i.e. for all t≥0

$$\mathcal{N} = \cap_{i=1}^{n} \ker\left(CA^{i-1}\right) = 0 \qquad (2.2)$$

or equivalently, if and only if it does not exist a nontrivial subspace $\mathcal{V} \subseteq \mathcal{X}$, such that $\mathcal{V} \subseteq \ker C$ and $\mathcal{V}$ is A-invariant (i.e. $A\mathcal{V} \subseteq \mathcal{V}$).

Proof. The proof is presented in (Wonham, 1979). ■

2.2 Petri nets and Interpreted Petri nets

Definition 2.4 A Petri net system or Petri net $\mathrm{N} = (\mathrm{G}, \mathrm{M}_0)$ is a bipartite digraph where $\mathrm{G} = (\mathrm{P, T, F})$ and:

- $P = \{p_1, p_2, \ldots\}$ is a finite set of vertices called places,
- $T = \{t_1, t_2, \ldots\}$ is a finite set of vertices called transitions,
- F is a relation on $P \cup T$ such that $F \cap (P \times P) = F \cap (T \times T) = \emptyset$.
- M_0 is the initial token distribution or initial marking, where a marking $M: P \to \mathbb{Z}^+$ is the number of tokens associated to each place, this is usually expressed as a vector of dimension equal to $|P|$.

The incidence matrix of G is $\mathcal{C} = [c_{ij}]$ such that

$$c_{ij} = \begin{cases} 0 & \text{if} \quad (p_i, t_j) \notin F \text{ and} (t_j, p_i) \notin F \text{ or} \\ & \qquad (p_i, t_j) \in F \text{ and } (t_j, p_i) \in F \\ -1 & \text{if} \quad (p_i, t_j) \in F \text{ and} (t_j, p_i) \notin F \\ 1 & \text{if} \quad (p_i, t_j) \notin F \text{ and } (t_j, p_i) \in F. \end{cases}$$

In a *PN* system, a marking M enables a transition t_j if it marks every place p_i such that $(p_i, t_j) \in F$; if t_j is enabled at M_k then the transition t_j can be fired reaching a new marking M_{k+1} (written as $M_k \overset{t_j}{\to} M_{k+1}$).

In a *PN*, $\sigma = t_1 t_2 \ldots t_k$ is a firing transition sequence leading from M to M_k (written as $M \overset{\sigma}{\to} M_k$) if $M \overset{t_1}{\to} M_1 \overset{t_2}{\to} \cdots \overset{t_k}{\to} M_k$. A marking M_k is said to be reachable from M if $M \overset{\sigma}{\to} M_k$ for some firing transition sequence σ. The reachability set of a *PN* is the set of all possible markings reached from M, this set is denoted by $R(G, M)$.

A Petri net (G, M_0) is live if, for every $M \in R(G, M_0)$ and every $t \in T$ there exists a marking $M' \in R(G, M)$ which enables t; it is cyclic if M_0 is reachable from every $M \in R(G, M_0)$ and it is binary if for every marking $M_k \in R(G, M_0)$ and every place $p_i \in P$ $M_k(p_i) \leq 1$.

As mentioned before, *IPN* are used to capture the discrete nature of *SLS*, this extension allows to associate input and output signals to *PN* models. These nets are defined as follows.

Definition 2.5 An interpreted Petri net *(IPN)* is the pair $(\mathrm{Q}, \mathrm{M}_0)$ with $\mathrm{Q} = (\mathrm{G}, \xi, \Gamma, \lambda, \varphi)$ where:

- (G, M_0) is a *PN* system.
- $\xi = \{\alpha_1, \alpha_2, \ldots\}$ is a finite set of input symbols.

• $\Gamma = \{\gamma_1, \gamma_2, ...\}$ is a finite set of output symbols.

• $\lambda: T \rightarrow \xi \cup \{\varepsilon\}$ is a labeling function of transitions with the following constraint: $\forall t_j, t_k \in T,\ j \neq k,\ \lambda(t_j) \neq \varepsilon, \lambda(t_k) \neq \varepsilon$ if there exists p_i such that $(p_i, t_j) \in F$ and $(p_i, t_k) \in F$ then $\lambda(t_j) \neq \lambda(t_k)$, where $\lambda(t) = \varepsilon$ represents a silent transition and ε is an internal system event.

There exists an output relation $\varphi \subset P \times \Gamma$ associating to each place a set of output symbols, where $(p_i, \gamma_j) \in \varphi$ if the output symbol γ_j is generated as an output when the place p_i is marked. The relation φ can be represented in a matricial form, where $\varphi_{ij} = 1$ if $(p_i, \gamma_j) \in \varphi$ and $\varphi_{ij} = 0$ otherwise.

If $\lambda(t_j) = \alpha_i \neq \varepsilon$ and the symbol α_i is present as an input when t_j is enabled, then t_j must fire. If $\lambda(t_j) = \varepsilon$ and t_j is enabled then t_j can be fired. The transition t_i is said to be manipulated if $\lambda(t_i) \neq \varepsilon$. Otherwise it is non manipulated.

The reachability set of (Q, M_0) is denoted as $R(Q, M_0)$ and is defined in a similar way as $R(G, M_0)$. Notice that $R(Q, M_0) \subseteq R(G, M_0)$ since the labeling function λ may force two transitions equally labeled to fired simultaneously in the *IPN*.

Definition 2.6 Let $M_i \overset{t_{i+1}}{\rightarrow} M_{i+1} \overset{t_{i+2}}{\rightarrow} \cdots \overset{t_l}{\rightarrow} M_l$ be a marking sequence. The input-output sequence $\omega = (\alpha_0, y_0) \cdots (\alpha_k, y_k)$ generated by $M_i \cdots M_l$ is defined inductively as follows:

• $\alpha_0 = \varepsilon$ and $y_0 = \varphi M_i$.

• If $\alpha_n = \lambda(t_j)$ and $y_n = \varphi M_j$ then $\alpha_{n+1} = \lambda(t_k)$ and $y_{n+1} = \varphi M_k$ if $\varphi M_k \neq \varphi M_j$ and there is no $M_{\hat{k}}$ occurring after M_j and before M_k such that $\varphi M_{\hat{k}} \neq \varphi M_j$ and $\varphi M_{\hat{k}} \neq \varphi M_k$.

Note that, if $\varphi M_i = \varphi M_{i+1}$ then the input-output sequence generated by $M_i M_{i+1}$ is the same as the one generated by M_i or M_{i+1}, say $\omega = (\varepsilon, \varphi M_i)$.

The marking sequences set corresponding to ω is defined as for all t≥0

$$S_\omega = \{M_i \cdots M_k | M_i \cdots M_k \text{ generates the input} - \text{output sequence } \omega\} \qquad (2.3)$$

2.3 Switched linear system

Definition 2.7 A Switched Linear System *(SLS)* is the tupla $SLS = \{F, N\}$, where F is a family of Linear Systems (*LS*) $\{\Sigma_1, \Sigma_2 ..., \Sigma_s\}$ and N is an Interpreted Petri Net *(IPN)*, where the following considerations are fulfilled:

- The interpreted Petri net N is live, binary and cyclic.
- $\Phi: P \rightarrow F \cup \{\mu\}$ is a function associating to each place a LS or μ, $\Phi(\mathrm{p_i}) = \mu$ indicates that p_i has not associated LS, where the following constraint is fulfilled: $\forall t_j \in T\ \sum_{p_i \in {}^\bullet t_j} \dim \Phi(p_i) = \sum_{p_k \in t_j^\bullet} \dim \Phi(p_k)$
- $\forall t_j$ such that $\{p_1, \dots, p_q\} \in {}^\bullet t_j$ and $\{p_q, \dots, p_g\} \in t_j^\bullet$ is defined $\delta_{t_j}: \mathbb{R}^n \rightarrow \mathbb{R}^n$ with $\delta_{t_j}\left(\begin{bmatrix} \overline{x_1}(\tau_k{}^-) \\ \vdots \\ \overline{x_q}(\tau_k{}^-) \end{bmatrix}\right) = \begin{bmatrix} \overline{x_q}(\tau_k) \\ \vdots \\ \overline{x_g}(\tau_k) \end{bmatrix}$, where $\overline{x_\iota}$ has the same dimension than $\Phi(p_i)$, $p_i \in {}^\bullet t_j$ and $\overline{x_\iota}$ has the same dimension then $\Phi(p_i)$, $p_i \in t_j^\bullet$. The final state at time τ_k when t_j is fired, $\overline{x_\iota}(\tau_k)$ is the initial condition of $\Phi(p_i)$.

- If the output symbol γ_j, where $(p_i, \gamma_j) \in \varphi$ appears more than one time, then it must be associated to places of the same P-component.
- The dwell time in a state M_k is finite and different from zero.

Definition 2.8 Let $\{F, N\}$ be a *SLS*. The *SLS* is named a Complete *SLS* if the system faults are included in the model in the following way. A faulty transition t_{f_i} and a faulty place p_{f_i} are added to the *IPN* in order to represent each fault f_i that the *SLS* model must capture. The place p_j of the *SLS* where the system can evolve from a normal behavior into a faulty behavior, where fault f_i is present, must be connected through an arc from p_j to t_{f_i} and also an arc from t_{f_i} to p_{f_i} must be added. The set F is recomputed as $F' = F \cup \{\Phi(p_{f_1}), \ldots, \Phi(p_{f_k})\}$.
Remark 2.9 Through this work, F, P *and* T are decomposed as $F = F_N \cup F_F$, $P = P_N \cup P_F$ and $T = T_N \cup T_F$ in a *Complete SLS* $\{F, N\}$, where $F_N, P_N,$ *and* T_N are elements of the *SLS* and $F_F, P_F,$ *and* T_F are the faulty elements added to the *Complete SLS* to include the faulty behavior in the *SLS.*
Definition 2.10 Let $\{F, N\}$ be a *Complete SLS* and $T_F = \{t_{f_1}, \ldots, t_{f_k}\}$ the set of faulty transitions. A place $p_k \in {}^{\blacksquare}T_F$ is named a risk place and a transition $t_i \in T - T_F$ where $t_i \in p_k{}^{\blacksquare}$ is named a post-risk transition.

2.4 Example

Example 2.11 Consider the *SLS* where the discrete part is represented by the *IPN* depicted below

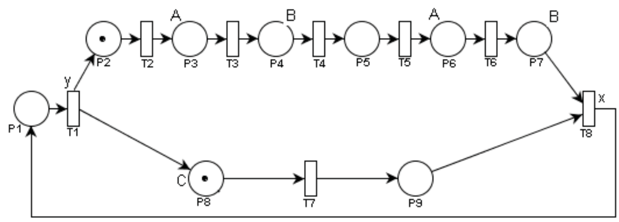

Fig. 1. Normal behavior of the *SLS.*

The *LS* associated to each place are presented in the next table:

P	$\Phi(P_N) = \Sigma(A,B,C)$		
p_1	$A_1 = \begin{bmatrix} -2 & 0 & 1 & 0 \\ -2 & 3 & 1 & 0 \\ 0 & -3 & 2 & -1 \\ -3 & 2 & 1 & 1 \end{bmatrix}$	$B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$	$C_1 = \begin{bmatrix} -1 & 0 & 2 & 1 \\ 1 & 0 & -1 & 0 \end{bmatrix}$
p_2	$A_2 = \begin{bmatrix} -2 & -1 \\ 3 & -5 \end{bmatrix}$	$B_2 = \begin{bmatrix} -3 \\ 1 \end{bmatrix}$	$C_2 = [1 \quad 3]$
p_3	$A_3 = \begin{bmatrix} -7 & -3 \\ 2 & -2 \end{bmatrix}$	$B_3 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$C_3 = [7 \quad 15]$
p_4	$A_4 = \begin{bmatrix} -3 & 0 \\ 3 & -4 \end{bmatrix}$	$B_4 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$C_4 = [0 \quad 1]$
p_5	$A_5 = \begin{bmatrix} -3 & 3 \\ 0 & -4 \end{bmatrix}$	$B_5 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$	$C_5 = [2 \quad -1]$
p_6	$A_6 = \begin{bmatrix} -5 & -4 \\ 2 & 1 \end{bmatrix}$	$B_6 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$C_6 = [15 \quad 12]$
p_7	$A_7 = \begin{bmatrix} -5 & 2 \\ -1 & -2 \end{bmatrix}$	$B_7 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$C_7 = [1 \quad 0]$
p_8	$A_8 = \begin{bmatrix} -1 & 3 \\ 0 & -2 \end{bmatrix}$	$B_8 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$C_8 = [2 \quad -9]$
p_9	$A_9 = \begin{bmatrix} -6 & 1 \\ -3 & -2 \end{bmatrix}$	$B_9 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$	$C_9 = [1 \quad 1]$

Table 1. Linear Systems associated to *IPN* places.

Notice that the *LS* evolving when the place p_1 is marked is of dimension four with two inputs and two outputs, when the transition t_1 is fired the *LS* associated to the places p_2 and p_8 evolves independently from each other, each one of dimension two with a single input and a single output, this situation may be interpreted as a decoupled of two machines cooperating with each other, in a similar way the firing of transition t_8 represents that two machines are cooperating in such a way that their dynamics couple together.
Then the faulty behavior $F_F = \{p_{10}, p_{11}\}$ is added according to the proposed model. The resulting *Complete SLS* model with both behaviors is represented in next figure.

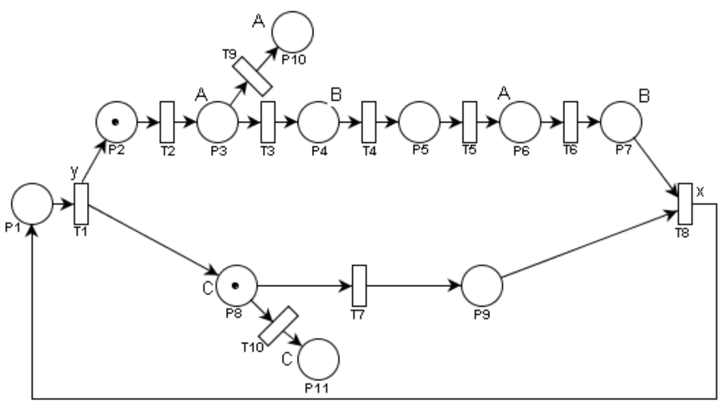

Fig. 2. Normal and faulty behavior of the *SLS*

The post-risk transitions are t_3 and t_7, while $T_F = \{t_9, t_{10}\}$. The faults $\Phi(p_{10})$ and $\Phi(p_{11})$ have the following information associated:

P	$\Phi(P_F) = \Sigma(A,B,C)$		
p_{10}	$A_{10} = \begin{bmatrix} -2 & 0 \\ 2 & -5 \end{bmatrix}$	$B_{10} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$C_{10} = [1 \quad 0]$
p_{11}	$A_{11} = \begin{bmatrix} -3 & -1 \\ 3 & -7 \end{bmatrix}$	$B_{11} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$	$C_{11} = [-3 \quad -1]$

Table 2. Linear Systems associated to *IPN* places.

3. Characterization of diagnosable *Complete SLS*

The characterization of diagnosability in *SLS* is based on the observation of the firing transition sequence containing a faulty transition. However, since the marking of some places cannot be observed from the output information, then an output information sequence could be generated by several possible firing transition sequences, some of them containing the faulty transition.

The diagnosability characterization is then reduced to compute the actual fired transition sequence in a finite number of fired transitions when a faulty transition is fired. Notice that the firing of a faulty transition is equivalent to that post risk transitions cannot be fired. Thus the idea behind this work is to detect if post risk transitions can be fired (the *SLS* is normaly evolving) or not (the *SLS* is in a fault behavior).

In order to ensure that the detection of the firing of post risk transitions is computed in a finite number of transition fires, the concept of relative distance between transitions is presented. Although the computation of this distance seems to be an *NP* complete problem, the finiteness of this distance can be computed efficently for the *IPN* used in the *SLS*.

3.1 Relative Distance Concepts

Definition 3.1 The relative distance between any pair of transitions $t_i, t_j \in T$, $D(t_i, t_j)$, in the *IPN*, is the maximum number that t_i can be fired when a token is held in the place $^\bullet t_j$. The maximum relative distance between any pair of transitions $t_i, t_j \in T$ is $D_H(t_i, t_j) = \max(D(t_i, t_j), D(t_j, t_i))$.

Notice that in live, cyclic and binary *IPN* the finiteness of this distance can be computed easily. For instance, the *IPN* of the *SLS* in Example 2.12 is covered by P-components, and these P-components become siphons when faulty transitions are added. Thus the firing of a faulty transition unmarks a P-component, thus all transitions of the P-component cannot fire anymore, thus the maximum relative distance between any pair of transitions of the P-component is finite. The next proposition states that when all T-Components share transitions with a P-component, if the P-component becomes unmarked, then the *IPN* is no longer live.

Proposition 3.2 Let $\{F, N\}$ be a *SLS* and $\{F', N'\}$ be a Complete *SLS*, where all T-Components of the *IPN* in the SLS share transitions with a P-component containing a risk place (p_i). If the faulty transition connected to the risk place is fired, then after a finite number of transition firing the *IPN* is no longer live (or blocked).

Proof. Since the *IPN* of the *SLS* is live and binary, then it is covered by P-Components (Dessel et al., 1995). When the faulty transition is added, the places of the P-Component become a siphon, thus the firing of the faulty transition unmarks the siphon. Since siphons cannot be marked again, then all transition in the P-Component cannot be fired. Moreover, since all T-Component share transitions with the P-Component, and every T-Component needs to fire all its transitions to be live, then eventually the transitions of the T-Component cannot be fired, since they need the firing of the transitions in the P-component. ■

Corollary 3.3 Let $\{F, N\}$ be a *SLS* and $\{F', N'\}$ be a Complete *SLS*, where all T-Components of the *IPN* in the *SLS* share transitions with any P-component containing a risk place (p_i). Then $t_i, t_j \in T$ is $D_H(t_i, t_j) < \infty$, where t_i is the post risk transition $t_i \in {}^{\blacksquare}p_i$.

Since the firing of any sequence contains transition $t_i \in {}^{\blacksquare}p_i$ then the idea is to add a "marker" to transition $t_i \in {}^{\blacksquare}p_i$ in such a way that the firing (or not firing) of this transition can be observed from the *SLS* output. The firing of such transition can be detected using the *LS* input output information based on distinguishability property or the *IPN* input output information, based en event detectability property. Next subsection formalizes these ideas.

3.2 Distinguishability Concepts

Definition 3.4 The linear systems $\Sigma_i(A_i, B_i, C_i)$, $\Sigma_j(A_j, B_j, C_j)$ are said to be distinguishable from each other if the knowledge of the input $u[t_0, t_1]$ and the output $y[t_0, t_1]$ over the finite time interval $[t_0, t_1]$ suffices to determine which *LS* is evolving.

Notation 3.5 Let $\Sigma_i(A_i, B_i, C_i)$, and $\Sigma_j(A_j, B_j, C_j)$ be two $SISO$ linear systems, then the linear system $\bar{\Sigma}\{\bar{A}, \bar{B}, \bar{C}\}$ denotes the extended LS form with the matrices for all t≥0

$$\bar{A} = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}$$
$$\bar{B} = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} \qquad (3.1)$$
$$\bar{C} = [C_1 \quad -C_2].$$

Lemma 3.6 Let $\Sigma_1(A_1, B_1, C_1)$, $\Sigma_2(A_2, B_2, C_2)$ be two $SISO$ LS where $A_1 \in \mathbb{R}^{n \times n}$ and $A_2 \in \mathbb{R}^{m \times m}$. Then the linear systems $\Sigma_1(A_1, B_1, C_1)$ and $\Sigma_2(A_2, B_2, C_2)$ are distinguishable from each other if and only if the only solution to the equation for all t≥0

$$\bar{C}e^{\bar{A}t}\left[x_0 + \int_0^t e^{-\bar{A}\tau}\bar{B}u(\tau)d\tau\right] = 0 \qquad (3.2)$$

is $x_0 = 0$ and $u(t) = 0$.

Proof. If the linear systems $\Sigma_1(A_1, B_1, C_1)$ and $\Sigma_2(A_2, B_2, C_2)$ are indistinguishable from each other then there exists an input $u(t)$ such that the same output $y(t)$ is produced by both systems when $u(t)$ is applied, i.e. for two different initial conditions x_0^1, x_0^2 it holds that for all t≥0:

$$y(t) = C_1 e^{A_1 t}\left[x_0^1 + \int_0^t e^{-A_1\tau}B_1 u(\tau)d\tau\right] \qquad (3.3)$$

and

$$y(t) = C_2 e^{A_2 t}\left[x_0^2 + \int_0^t e^{-A_2\tau}B_2 u(\tau)d\tau\right] \qquad (3.4)$$

then combining equations (3.3) and (3.4):

$$C_1 e^{A_1 t}\left[x_0^1 + \int_0^t e^{-A_1\tau}B_1 u(\tau)d\tau\right] = C_2 e^{A_2 t}\left[x_0^2 + \int_0^t e^{-A_2\tau}B_2 u(\tau)d\tau\right] \qquad (3.5)$$

this equation can be written as

$$C_1 e^{A_1 t}x_0^1 - C_2 e^{A_2 t}x_0^2 = \int_0^t \left[-C_1 e^{-A_1(t-\tau)}B_1 + C_2 e^{-A_2(t-\tau)}B_2\right]u(\tau)d\tau. \qquad (3.6)$$

Now, since (3.6) is equivalent to:

$$\begin{aligned} &[C_1 \quad -C_2]\begin{bmatrix} e^{A_1 t} & 0 \\ 0 & e^{A_2 t}\end{bmatrix}\begin{bmatrix} x_0^1 \\ x_0^2 \end{bmatrix} = \\ &-\int_0^t [C_1 \quad -C_2]\begin{bmatrix} e^{A_1(t-\tau)} & 0 \\ 0 & e^{A_2(t-\tau)}\end{bmatrix}\begin{bmatrix} B_1 \\ B_2 \end{bmatrix} u(\tau)d\tau \end{aligned} \tag{3.7}$$

Equation (3.7) can be written in terms of the matrices (3.1), with $x_0 = [x_0^1 \quad x_0^2]^T$, then

$$\bar{C}e^{\bar{A}t}\left[x_0 + \int_0^t e^{-\bar{A}\tau}\bar{B}u(\tau)d\tau\right] = 0. \tag{3.8}$$

Since $\Sigma_1(A_1, B_1, C_1)$ is indistinguishable from $\Sigma_2(A_2, B_2, C_2)$, thus there exist solutions $x_0 \neq 0$ and $u(t) \neq 0$ to Equation (3.8). The converse is also true, then $\Sigma_1(A_1, B_1, C_1)$ and $\Sigma_2(A_2, B_2, C_2)$ are indistinguishable from each other if and only if the only solution to Equation (3.8) is $x_0 = 0$ and $u(t) = 0$. ■

Theorem 3.7 Let $\Sigma_i(A_i, B_i, C_i)$, $\Sigma_j(A_j, B_j, C_j)$ be two *SISO* linear systems, where the matrices $A_i \in \mathbb{R}^{n\times n}$ and $A_j \in \mathbb{R}^{m\times m}$. Then the linear systems $\Sigma_1(A_1, B_1, C_1)$, $\Sigma_2(A_2, B_2, C_2)$ are distinguishable from each other if and only if the extended *LS* $\Sigma_{i,j}(A_{i,j}, B_{i,j}, C_{i,j})$ has no system zeros.

The proof follows from Lemma 3.6 ■

3.3 Distinguisher Design

The distinguisher proposed in this work is presented in Figure 3. It is capable of compute which *LS* is evolving from a set of possible evolving and distinguishable from each other set of *LS*. This figure shows that the diagnoser is composed of an observer, a set of simulation models of all possible evolving *LS* and a decision block.

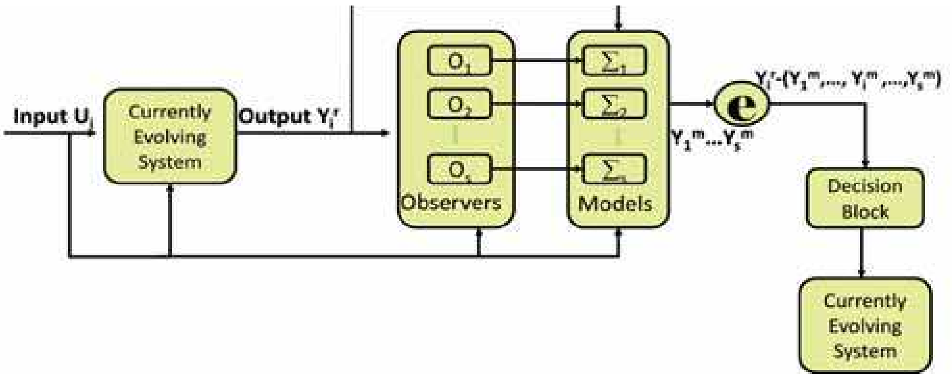

Fig. 3. Distinguishability architecture.

The distinguisher works as follows. The input and output of the current evolving *LS* are introduced to all Luenberger observers of the set of possible evolving *LS*. Notice that one of the Luenberger observers is the observer of the current evolving *LS*, thus at least this observer will compute the current *LS* state. The state estimated by each observer O_i is given as initial condition to the corresponding *LS* model Σ_i and a simulation starts. Since all the *LS* are distinguishable from each others, then the output of just one system will be equal to the current *LS* output. Thus the decision block isolates the model corresponding to the current *LS* evolving.

3.3 Event Detectability

Definition 3.8 An *IPN* given by (Q, M_0) is event-detectable if any transition firing can be uniquely determined by the knowledge of the input given to (Q, M_0) and output signals that it produces.

The following Lemma provides a structural characterization of the IPN exhibiting event-detectability.

Lemma 3.9 A live *IPN* given by $(Q, \mathcal{M}_0)$ is event-detectable if

1. $\forall \mathbf{t}_i, \mathbf{t}_j \in T$ such that $\lambda(\mathbf{t}_i) = \lambda(\mathbf{t}_j)$ or $\lambda(\mathbf{t}_i) = \varepsilon$ it holds that $\varphi\mathcal{C}(\bullet, \mathbf{t}_i) \neq \varphi\mathcal{C}(\bullet, \mathbf{t}_j)$

and

2. $\forall \mathbf{t}_k \in T$ it holds that $\varphi\mathcal{C}(\bullet, \mathbf{t}_k) \neq 0$.

The proof is presented in (Rivera et al., 2005). ■

Lemma 3.10 A transition $t_k \in T$ in the IPN N of the SLS is event-detectable if:

$$1. \quad \left\{ \begin{array}{c} \varphi C(\bullet, t_k) \neq 0 \text{ or} \\ \begin{bmatrix} \Phi(p_i') & & \\ & \ddots & \\ & & \Phi(p_j') \end{bmatrix} \mathit{is\ distinguishable\ from} \begin{bmatrix} \Phi(p_k'') & & \\ & \ddots & \\ & & \Phi(p_l'') \end{bmatrix} \\ \mathit{where}\ p_r' \in {}^{\blacksquare}t_k\ \mathit{and}\ p_r'' \in t_k^{\blacksquare} \end{array} \right.$$

and

$$2. \quad \left\{ \begin{array}{c} \forall t_i \in T \text{ such that } \varphi C(\bullet, t_k) = \varphi C(\bullet, t_i) \text{ fulfills that} \\ \left\{ \begin{bmatrix} \Phi(p_i') & & \\ & \ddots & \\ & & \Phi(p_j') \end{bmatrix} \mathit{is\ distinguishable\ from} \begin{bmatrix} \Phi(p_k'') & & \\ & \ddots & \\ & & \Phi(p_l'') \end{bmatrix} \right. \\ \mathit{where}\ p_r' \in t_k^{\blacksquare}\ \mathit{and}\ p_r'' \in t_i^{\blacksquare} \end{array} \right.$$

Proof: In order to uniquely determine the firing of any transition, their firing must be detected (part 1), i.e. if $\varphi C(\bullet, t_k) \neq 0$ then the firing of t_k is detected using the discrete inputs-outputs information change $y_k - y_{k-1} = \varphi C(\bullet, t_k) \neq 0$, otherwise if the

$$\begin{bmatrix} \Phi(p_i') & & \\ & \ddots & \\ & & \Phi(p_j') \end{bmatrix} \mathit{is\ distinguishable\ from} \begin{bmatrix} \Phi(p_k'') & & \\ & \ddots & \\ & & \Phi(p_l'') \end{bmatrix}$$

then by using continuous information it can be determined the firing of t_k .

The change that every firing produces in the output is unique (part 2). Since two transitions producing the same discrete input-output information, $\varphi C(\bullet, t_k) = \varphi C(\bullet, t_i)$ belongs to the same P-Component (because the places of P-components can have the same output symbol), then the property of distinguishability between the LS associated with $t_k^{\blacksquare}$ and the LS associated with $t_i^{\blacksquare}$ can be tested.

Since part 2 states that both systems are distinguishable from each other, then it can be determined if the places of $t_k^{\blacksquare}$ or the places of $t_i^{\blacksquare}$ are marked and consequently conclude which transition has been fired.

3.4 Diagnosability characterization

Detecting and isolating a fault in *LS* and *IPN* has been widely addressed in the literature. The results are identical in both cases for additive faults. A residue generator can be built in such a way that the subspace generated by the input can be twisted and placed into the kernel of the output map while the fault resides out of the kernel of the output map. These residue generators (Massoumnia et al., 1989; Hadjicostis et al., 1999; Ramirez et al. 2007) must be built and can be used to detect faults when it is possible. However, there could be cases when the faults cannot be isolated by the residue generators, but still can be isolated, as the following theorem states.

Theorem 3.11 Let $\{F, N\}$ be a *SLS* and $\{F', N'\}$ be its Complete *SLS* where every fault f_i all T-Components of the *IPN* in the *SLS* share transitions with the P-component containing the risk place $p_i \in {}^{\blacksquare}t_{f_i}$. If the pre risk t_{ri}, post risk t_i, and faulty t_{f_i} transitions of every fault f_i fulfill that:

1. $\forall t_j \in T$ is $D_H(t_i, t_j) < \infty$,
2. t_{ri} and t_i are event detectable or t_{f_i} is event detectable

then the *SLS* is diagnosable.

Proof. Since $\forall t_j \in T$ is $D_H(t_i, t_j) < \infty$, then the firing of t_i appears in all finite transition firing sequences. In order to fire t_i, the risk place p_i must be marked. At this marking the fault f_i (represented by the firing of t_{f_i}) could occur.

Notice that the moment when place p_i is marked is detected since t_{ri} is event detectable. Eventually either, the transition t_i will be fired and detected (since $D_H(t_i, t_j) < \infty$ and t_i is event detectable) and there is no fault in the *SLS*, or the *IPN* will be blocked. Since $\lambda(t_i) \neq \varepsilon$ then the symbol $\lambda(t_i)$ could be given to the *IPN*, if the firing of t_i is detected, then there is no fault in the *SLS*, otherwise, the *SLS* is in a fault state, moreover, the fault f_i occurred into the *SLS*.

4. Diagnoser design

The scheme used to detect and isolate faults when the system is working on-line is presented in Figure 4. Its funcionality is as follows, when the inputs manipulable and not manipulable are applied to the system, the event-detectability implies that generate an output change in the *IPN* model which contains the normal and faulty behavior, the diagnoser model is binary too and only contains the event detectability normal behavior. The transition $t_k \in {}^{\blacksquare}p_k$, where p_k is a risk place in the *SLS*, is event detectable. When no fault is presented in the *SLS* the error between the *IPN* model and the diagnoser model will be zero. Now, if a fault occurs and the *IPN* is event-detectable then the error between the diagnoser and the *Complete SLS* will be different from zero. If a transition is confused and it is necessary to verify which *LS* is evolving, i.e. which place is marked, then the distinguishable diagnoser is used. The later diagnoser gives the requiered event detectability; when the difference is not zero, it implies that a fault occurs in the *Complete SLS*.

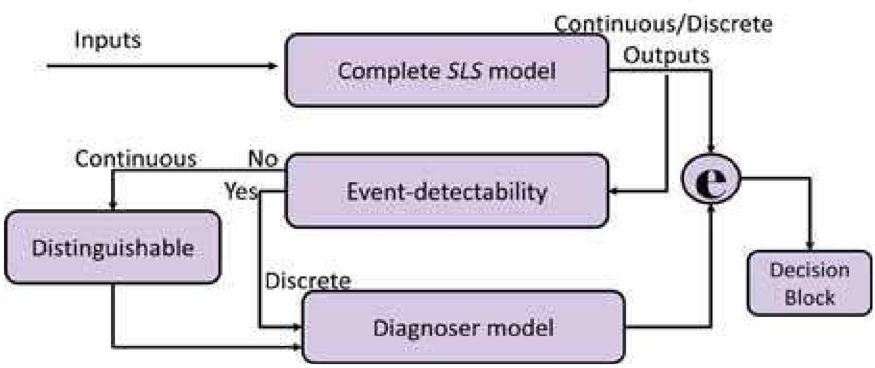

Fig. 4. Diagnoser scheme

5. Illustrative example

Example 5.1 Consider the *SLS* of Example 2.11 where the normal and faulty behavior is depicted. Notice that the *IPN* is not input-output diagnosable using only the discrete information because when the system turns on and A appears, it is not possible to know which one is and in consequence if a fault occurs. The relative distance between the post-risk transition and the others in the *IPN* is finite. The *IPN* system has two places with the same symbol A. As both *LS* associated to $\Phi(P_3)$ and $\Phi(P_6)$ are distinguishable, if in the *IPN* A is detected, the distinguishable design immediately starts its operation and the currently evolving system will be detected. If the place p_6 is marked cannot occurs a fault. If the risk place p_3 is marked and as the relative distance is finite, t_3 must be fired, when no change in the *IPN* is detected implies that the fault $\Phi(P_{10})$ occurs in the system.
To diagnose the fault $\Phi(P_{11})$ the *IPN* gives enough information to know that the system arrives to a risk place, as the *LS* marked with the same symbol C in the *IPN* are distinguishable, this means that $\Phi(P_8)$ is distinguishable from $\Phi(P_{11})$, i. e. the extended system:

$$\bar{A} = \begin{bmatrix} -1 & 3 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -3 & -1 \\ 0 & 0 & 3 & -7 \end{bmatrix}; \; \bar{B} = \begin{bmatrix} 1 \\ 1 \\ 2 \\ 1 \end{bmatrix} \; and \; \bar{C} = \begin{bmatrix} 2 & -9 & -3 & -1 \end{bmatrix}$$

is observable, controllable and does not have transmission zeros. It is easy to see if a fault occurs using the distinguishable design.

6. Conclusions

This chapter addresses the diagnosability problem in *SLS* represented by a family of linear systems and an interpreted Petri net. It shows that although the results of diagnosability in *IPN* and *LS* can be used, the class of *SLS* that can be analyzed include those where neither the *SLS* nor the *IPN* are diagnosable.

The main idea behind of diagnosability is that the occurrence of a fault can be detected in the output because if the use of residue generator, distinguishability or the expected normal behavior is not carried out. These three ideas are introduced into the *IPN* as the solely concept of event detectability, thus when faulty, pre and post risk transitions are event detectable and the relative distance of post risk transition and other transitions is finite then the *SLS* is diagnosable.

The advantages of the proposed method are that the diagnosability characterization is structural and polynomial, the diagnoser converges to the fault in finite time and the *SLS* model captures the fact that several systems can work coupled or uncoupled, depending on the operation circumstances.

7. Acknowledgment

This work was supported by the National Council of Science and Technology of Mexico (CONACYT), Project No. 107195.

8. References

C. T. Chen, (1970) Linear System Theory and Design. Holt, Rinehart and Winston.

J. Desel and J. Esparza. (1995) Free Choice Petri Nets. Cambridge University Press.

G. K. Fourlas, K. J. Kyriakopoulos and N. J. Krikelis (2005) Fault Diagnosis of Hybrid Systems, in Proceedings IEEE international symposium on intelligent control, p.p. 832-837

George K. Fourlas (2009) Multiple Faults Diagnosability of Hybrid Systems. , in Proceedings of the 17th Mediterraneean Conference on Control & Automation, pp. 365-370

J. Gertler, M. Staroswiecki and S. Mengbing, (2002) Direct design of structured residuals for fault diagnosis in linear systems, in American Control Conference, vol. 6, pp. 4519-4524.

D. Gomez-Gutierrez, G. Ramirez-Prado, A. Ramirez-Trevino, and J. Ruiz-Leon. (2008) Joint state-mode observer design for switched linear systems, in IEEE International Conference on Emerging Technologies and Factory Automation, pp. 1408-1415.

C. N. Hadjicostis and G. Verghese. (2000) Power Systems Monitoring Using Petri Net Embeddings. IEE Proceedings C: Generation, Transmition, Distribution, vol. 147, no. 5, pp. 299-303.

C. N. Hadjicostis and G. Verghese. (1999) Structured Redundancy for Fault Tolerance in State-Space models and Petri Nets. Kybernetica, vol. 35, no. 1, pp. 39-55.

S. Hashtrudi-Zad, 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

M. Massoumnia, G. C. Verghese and A. S. Willsky, (1989) Failure Detection and Identication", in IEEE Trans. Autom. Control, vol. 34, no. 3 pp. 316-321.

A. Ramírez-Treviño, E. Ruiz-Beltrán, I. Rivera-Rangel and E. López-Mellado, (2007) On-line fault diagnosis of Discrete Event Systems. A Petri Net Based Approach, in IEEE Transactions on Science and Engineering. Vol. 1 No. 4, January 2007. pp 31-39.

I. Rivera-Rangel, A. Ramirez-Treviño, L.I. Aguirre-Salas, and J. Ruiz-León. (2005) Geometrical characterization of Observability in Interpreted Petri Nets. Kybernetika, 41, 553-574.

M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen and D. Teneketzis, (1995) Diagnosability of discrete event systems, in IEEE Transactions on Automatic and Control, vol. 4, no. 9, pp. 1555-1575.

W. M. Wonham, (1979) Linear Multivariable Control: A Geometric Approach. Springer-Verlag.

Petri Nets Applications

Edited by Pawel Pawlewski

ISBN 978-953-307-047-6
Hard cover, 752 pages
Publisher InTech
Published online 01, February, 2010
Published in print edition February, 2010

Petri Nets are graphical and mathematical tool used in many different science domains. Their characteristic features are the intuitive graphical modeling language and advanced formal analysis method. The concurrence of performed actions is the natural phenomenon due to which Petri Nets are perceived as mathematical tool for modeling concurrent systems. The nets whose model was extended with the time model can be applied in modeling real-time systems. Petri Nets were introduced in the doctoral dissertation by K.A. Petri, titled "„Kommunikation mit Automaten" and published in 1962 by University of Bonn. During more than 40 years of development of this theory, many different classes were formed and the scope of applications was extended. Depending on particular needs, the net definition was changed and adjusted to the considered problem. The unusual "flexibility" of this theory makes it possible to introduce all these modifications. Owing to varied currently known net classes, it is relatively easy to find a proper class for the specific application. The present monograph shows the whole spectrum of Petri Nets applications, from classic applications (to which the theory is specially dedicated) like computer science and control systems, through fault diagnosis, manufacturing, power systems, traffic systems, transport and down to Web applications. At the same time, the publication describes the diversity of investigations performed with use of Petri Nets in science centers all over the world.