Fault Model Identification with Petri Nets

Maria Paola Cabasino (*), Alessandro Giua (*),

Christoforos N. Hadjicostis (**), Carla Seatzu (*)

(*) Department of Electrical and Electronic Engineering, University of Cagliari,
Piazza D'Armi, 09123 Cagliari, Italy. Email: {cabasino,giua,seatzu)}@diee.unica.it

(**) Coordinated Science Laboratory and Department of Electrical and Computer Engineering,
University of Illinois at Urbana-Champaign, IL 61801-2307, USA. E-mail: chadjic@uiuc.edu

Abstract

Most of the fault identification problems in the Discrete Event Systems literature assume knowledge of the structure of the net system, including the nature (and behavior) of the possible faults. In this paper we deal with this problem within the framework of Petri nets by removing the requirement that the nature (and behavior) of the fault is known. In particular, we devise a way to identify the structure of the faulty transitions of the system given its language. Then, we generalize this procedure to unobservable faults, in which case the structure of the faulty system needs to be recognized from the knowledge of the structure of the fault-free system, and the projection of the faulty system language on the set of non-faulty events, that are assumed to be observable.

Published as:

M.P. Cabasino, A. Giua, C.N. Hadjicostis, C. Seatzu, "Fault model identification with Petri nets," *9th Int. Workshop on Discrete Event Systems* (Gteborg, Sweden), pp. 455-461, May 2008.

This work was supported in part by the International Curriculum Option on Hybrid Control for Complex, Distributed and Heterogeneous Embedded Systems (http://www.piaggio.ccii.unipi.it/ICO/).

I. INTRODUCTION

Fault detection and diagnosis of discrete event systems is a research area that has received a lot of attention in the last years and has been motivated by the practical need of ensuring the correct and safe functioning of large complex systems. Several original theoretical approaches have been proposed [1], [4], [6], [7], [9], [10] to solve this problem.

In this paper we deal with the problem of fault identification in Petri nets. The proposed approach starts from earlier results by some of us [2], [5] where, given the language of a Petri net system, we identify the Petri net structure and its initial marking by solving an integer programming problem.

Here we suppose to know the fault-free system and our goal is to identify the structure of the faulty system, namely the additional transitions that contribute to the faulty behavior. We consider two different cases. First, we assume that the language of the faulty system is completely known. In such a case the problem reduces to an identification problem that can be solved using the approach in [2]. The only difference is the addition of appropriate constraints that enforce the (known) structure of the fault-free system. Second, we consider faults that are unobservable, which implies that identification should only be based on the projection of the faulty system language on the set of non-faulty (observable) events.

As an example, consider the fault-free net system in Fig. 1.(a), whose language is $\mathcal{L} = \{\varepsilon\} \cup \{(t_1t_2)^n \mid n \geq 0\} \cup \{(t_1t_2)^n t_1 \mid n \geq 0\}$. Assume that a fault f may occur, and that the observable language of the system with faults is $\mathcal{L}^F = \{\varepsilon\} \cup \{((t_1 + \varepsilon)\ t_2)^n \mid n \geq 0\} \cup \{(t_1t_2)^n t_1 \mid n \geq 0\}$. We have to identify a net system that coincides with the net system in Fig. 1.(a) if the fault transition and its connected arcs are removed, and whose language projected on $\{t_1, t_2\}$ is equal to $\mathcal{L}^F$. Clearly, a solution to this is given by the net system in Fig. 1.(b); however, this is not the only possible solution. Thus, we have to associate an appropriate performance index to select one solution within the set of admissible ones.

II. BACKGROUND ON PETRI NETS

In this section we recall the formalism used in the paper. For more details on Petri nets we refer the reader to [8].

A *Place/Transition net* (P/T net) is a structure $N = (P, T, Pre, Post)$, where P is a set of m places; T is a set of n transitions; $Pre:\ P \times T\ \rightarrow \mathbb{N}$ and $Post:\ P \times T\ \rightarrow \mathbb{N}$ are the pre– and

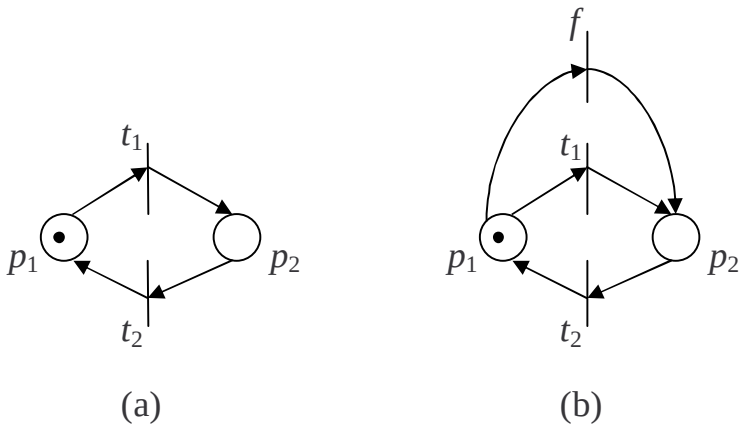

Fig. 1. A motivational example.

$post$– incidence functions that specify the arcs; $C = Post - Pre$ is the incidence matrix. The *preset* and *postset* of a node $X \in P \cup T$ are denoted ${}^\bullet X$ and $X^\bullet$ while ${}^\bullet X^\bullet = {}^\bullet X \cup X^\bullet$.

A *marking* is a vector $M : P \to \mathbb{N}$ that assigns to each place of a P/T net a nonnegative integer number of tokens, represented by black dots. We use $M(p)$ to denote the marking of place p. A P/T *system* or *net system* $\langle N, M_0 \rangle$ is a net N with an initial marking M_0.

A transition t is enabled at M iff $M \geq Pre(\cdot\,, t)$ and may fire yielding the marking $M' = M + C(\cdot\,, t)$. We write $M\ [\sigma\rangle$ to denote that the sequence of transitions $\sigma = t_{j_1} \cdots t_{j_k}$ is enabled at M, and we write $M\ [\sigma\rangle\ M'$ to denote that the firing of σ yields M'. We denote the length of the firing sequence σ by $|\sigma|$.

Given a sequence $\sigma \in T^*$, we call $\pi : T^* \to \mathbb{N}^n$ the function that associates to σ a vector $y \in \mathbb{N}^n$, named the *firing vector* of σ. In particular, $y = \pi(\sigma)$ is such that $y(t) = k$ if the transition t is contained k times in σ.

A marking M is *reachable* in $\langle N, M_0 \rangle$ iff there exists a firing sequence σ such that $M_0\ [\sigma\rangle\ M$. The set of all markings reachable from M_0 defines the *reachability set* of $\langle N, M_0 \rangle$ and is denoted by $R(N, M_0)$.

Given a Petri net system $\langle N, M_0 \rangle$ we define its language as the set of its firing sequences $L(N, M_0) = \{\sigma \in T^* \ \mid \ M_0[\sigma\rangle\}$. We also define the set of firing sequences of length less than or equal to $k \in \mathbb{N}$ as: $L_k(N, M_0) = \{\sigma \in L(N, M_0) \ \mid \ |\sigma| \leq k\}$.

III. PETRI NET IDENTIFICATION

In this section we briefly recall the identification procedure we presented in [2].

***Problem** 1:* Let $\mathcal{L} \subset T^*$ be a finite prefix-closed language[1], and

$$k = \max_{\sigma \in \mathcal{L}} |\sigma|$$

be the length of the longest string in $\mathcal{L}$. Given that the set of places P has cardinality m, we want to identify the structure of a net $N = (P, T, Pre, Post)$ and an initial marking M_0 such that

$$L_k(N, M_0) = \mathcal{L}.$$

The unknowns we want to determine are the elements of the two matrices $Pre,\ Post \in \mathbb{N}^{m \times n}$ and the elements of the vector $M_0 \in \mathbb{N}^m$. ■

A solution to the above identification problem can be computed thanks to the following theorem, that provides a linear algebraic characterization of the place/transition nets N with m places and n transitions such that $L_k(N, M_0) = \mathcal{L}$.

***Theorem** 2:* [2] A net system $\langle N, M_0 \rangle$ is a solution of the identification problem (1) if and only if it satisfies the following set of linear algebraic constraints:

$$\mathcal{G}_m(\mathcal{E}, \mathcal{D}) \triangleq \begin{cases} M_0 + Post \cdot \vec{\sigma} - Pre \cdot (\vec{\sigma} + \vec{t_j}) \geq \vec{0} \\ \qquad\qquad \forall (\sigma, t_j) \in \mathcal{E} \quad (a) \\ -KS_{\sigma,j} + M_0 + Post \cdot \vec{\sigma} \\ \qquad -Pre \cdot (\vec{\sigma} + \vec{t_j}) \leq -\vec{1}_m \\ \qquad\qquad \forall (\sigma, t_j) \in \mathcal{D} \quad (b) \\ \vec{1}^{\,T} S_{\sigma,j} \leq m - 1 \qquad \forall (\sigma, t_j) \in \mathcal{D} (c) \\ M_0 \in \mathbb{N}^m \qquad (d) \\ Pre, Post \in \mathbb{N}^{m \times n} \qquad (e) \\ S_{\sigma,j} \in \{0,1\}^m \qquad (f) \end{cases} \tag{1}$$

where

$$\mathcal{E} = \{(\sigma, t_j) \mid \sigma \in \mathcal{L}, |\sigma| < k, \sigma t_j \in \mathcal{L}\}, \tag{2}$$

$$\mathcal{D} = \{(\sigma, t_j) \mid \sigma \in \mathcal{L}, |\sigma| < k, \sigma t_j \notin \mathcal{L}\}, \tag{3}$$

[1]A language $\mathcal{L}$ is said to be *prefix-closed* if for any string $\sigma \in \mathcal{L}$, all prefixes of σ are in $\mathcal{L}$.

and K is a very large constant. ■

Constraints (a) are the *enabling constraints*, i.e., a transition t_j is enabled at $M_0 + (Post - Pre) \cdot \vec{\sigma}$ if and only if $M_0 + (Post - Pre) \cdot \vec{\sigma} \geq Pre \cdot \vec{t}_j$.

Constraints (b) and (c) are the *disabling constraints*: if a transition t_j is disabled at $M_0 + (Post - Pre) \cdot \vec{\sigma}$ then there exists at least one place $p \in P$ such that

$$M_0(p) + (Post(p, \cdot) - Pre(p, \cdot)) \cdot \vec{\sigma} \leq Pre(p, \cdot) \cdot \vec{t}_j - 1. \tag{4}$$

Indeed, by constraint (c) at least one entry of $S(\sigma, t_j)$ is null, thus eq. (4) holds for at least one $p \in P$. On the contrary, no constraint is given for the other places which correspond to a non null entry of $S(\sigma, t_j)$, because in this case constraint (b) is redundant.

In general, the solution of the set (1) is not unique, thus there exists more than one Petri net system $\langle N, M_0 \rangle$ such that

$$L_k(N, M_0) = \mathcal{L}.$$

To select a unique Petri net among these systems, we choose a given performance index and, solving an appropriate IPP (Integer Programming Problem), we determine a Petri net system that minimizes the considered performance index[2]. In particular, if $f(M_0, Pre, Post)$ is the considered performance index, an identification problem can be formally stated as follows.

***Problem** 3:* [2] Let us consider the identification problem (1) and let $f(M_0, Pre, Post)$ be a given performance index. The solution to the identification problem (1) that minimizes $f(M_0, Pre, Post)$ can be computed by solving the following IPP

$$\begin{cases} \min & f(M_0, Pre, Post) \\ \text{s.t.} & \mathcal{G}_m(\mathcal{E}, \mathcal{D}). \end{cases} \tag{5}$$

■

Of particular interest are those objective functions that are linear in the unknowns, so that the problem to solve is a linear integer programming problem [2]. A typical choice is the following

$$f(M_0, Pre, Post) = \vec{1}_m^T \cdot M_0 + \vec{1}_m^T \cdot (Pre + Post) \cdot \vec{1}_n$$

which corresponds to minimizing the number of tokens in the initial marking and minimizing the number of arcs (weighted by their individual weights).

[2]Clearly, also in this case the solution may not be unique.

IV. Problem Statements

Assume that a net system $\langle N, M_0\rangle$ generating a nominal (i.e., *fault-free*) language $\mathcal{L}$ is given and let $N = (P, T, Pre, Post)$ be its net structure. We consider a *faulty* net system $\langle N^F, M_0\rangle$, where $N^F = (P, T^F, Pre^F, Post^F)$, with the same number of places and the same initial marking as the nominal one. However, its set of transitions is $T^F = T \cup T_f$, where $T_f = \{f_1, \cdots, f_q\}$ is the set of faulty transitions. Furthermore we make the following assumption.

Assumption (A1): The pre and post incidence matrices of the faulty net are

$$Pre^F = \left[\begin{array}{cccc} Pre & Pre^{f_1} & \cdots & Pre^{f_q} \end{array}\right],$$
$$Post^F = \left[\begin{array}{cccc} Post & Post^{f_1} & \cdots & Post^{f_q} \end{array}\right],$$

where Pre^{f_i} (resp., $Post^{f_i}$) is the $m \times 1$ Pre (resp., Post) incidence matrix of transition f_i. ■

According to this assumption, the faulty net retains the structure of the nominal one but includes a number of additional faulty transitions.

We consider two different problem statements: in the first one the occurrence of fault transitions is observable, whereas in the second one faults are unobservable.

A. Case I: Faults are Known

***Problem** 4:* Let us consider a fault-free net system $\langle N, M_0\rangle$. Let $\mathcal{L}^F$ be a finite prefix-closed language over alphabet $T^F = T \cup T_f$, where $T_f = \{f_1, \ldots, f_q\}$, and such that all strings in $\mathcal{L}^F$ have length less than or equal to k.

We want to identify a faulty net system $\langle N^F, M_0\rangle$, satisfying (A1) and such that $L_k(N^F, M_0) = \mathcal{L}^F$. ■

In simple terms, here we are assuming that the number of faults and their effect on the net behavior (i.e., the language of the resulting system) are known. Our goal is that of identifying the structure of the system with faults, namely the weights of the arcs incident on fault transitions f_1, …, f_q, under the constraint that the structure of the fault-free system is kept intact.

The next result characterizes the existence of a solution for this problem.

***Proposition** 5:* Given a fault-free system $\langle N, M_0\rangle$, let $\mathcal{L} = L_k(N, M_0) \subset T^*$.

A necessary condition for the existence of a solution to Problem 4 is that $\mathcal{L}^F \subset (T^F)^*$ satisfies $\mathcal{L} = \mathcal{L}^F \cap T^*$, i.e., all words that are firable in the faulty system and consist of fault-free transitions can also be fired in the fault-free system.

Proof: Consider a word $w \in T^*$. According to assumption (A1), this word is firable in $\langle N, M_0\rangle$ if and only if it is also firable in $\langle N^F, M_0\rangle$. □

B. Case II: Faults are Unobservable

***Problem** 6:* Let us consider a fault-free net system $\langle N, M_0\rangle$. Let $\mathcal{L}^F$ be a finite prefix-closed language over T whose strings have length less than or equal to k.

Let $\Lambda(\mathcal{L}^F)$ be the set of languages over T^F whose projection[3] over T is equal to $\mathcal{L}^F$, i.e.

$$\Lambda(\mathcal{L}^F) = \{\mathcal{L} \subset (T^F)^* \ : \ P(\mathcal{L}) = \mathcal{L}^F\}.$$

We want to identify a faulty net system $\langle N^F, M_0\rangle$ satisfying (A1) and such that $L_k(N^F, M_0) \in \Lambda(\mathcal{L}^F)$. ■

In simple terms, here we are assuming that faults are *unobservable* events. Our goal is to identify the structure of the faulty system, based on the knowledge of its observable language, namely the projection of its firing sequences over the set of observable transitions T.

Our next result characterizes the existence of a solution for this problem.

***Proposition** 7:* Given a fault-free system $\langle N, M_0\rangle$, let $\mathcal{L} = L_k(N, M_0) \subset T^*$.

A necessary condition for the existence of a solution to Problem 6 is that $\mathcal{L} \subseteq \mathcal{L}^F$.

Proof: Assumption (A1) guarantees that all sequences firable in $\langle N, M_0\rangle$ can also be fired in $\langle N^F, M_0\rangle$. Thus Problem 6 is well-posed only if $\mathcal{L}^F$ contains all the sequences in $\mathcal{L}$. □

As a final remark, note that in Case II we can only identify faults generating strings whose observable projection is not contained in the language of the nominal system. The following example clarifies this.

***Example** 8:* Let us consider the net system in Fig. 2, where $T = \{t_1\}$ and $T_f = \{f\}$. Here $\mathcal{L} = \mathcal{L}^F = \{\varepsilon, t_1\}$, i.e., the nominal language coincides with the observable language of the faulty system. This means that after the firing of fault transition f no anomalous string will be observed, thus this fault cannot be identified. ■

[3]We define the *projection operator* $P : (T^F)^* \to T^*$ *recursively as follows: (i)* $P(t_j) = t_j \ \ \forall t_j \in T$*; (ii)* $P(f_i) = \varepsilon \ \forall f_i \in T_f$*; (iii)* $P(\sigma t_j) = P(\sigma)P(t_j) \ \ \forall \sigma \in (T^F)^*, t_j \in T^F$.

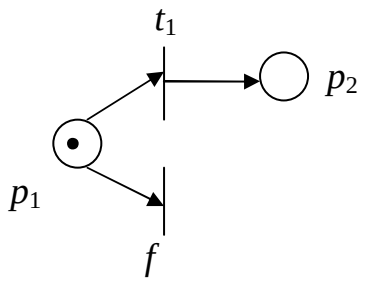

Fig. 2. A Petri net where $\mathcal{L} = \mathcal{L}^F = \{\varepsilon, t_1\}$.

V. Fault Identification in Case I

In this section we show how Problem 4 can be easily solved using our results in [2], that have been summarized in Section III. The idea is that of providing an algebraic characterization of the set of admissible faulty systems. Then, the identification problem is formulated in terms of a linear IPP.

***Proposition** 9:* Let us consider Problem 4, and let

$$g(Pre^{f_1}, \ldots, Pre^{f_q}, Post^{f_1}, \ldots, Post^{f_q}) = \sum_{i=1}^{m}\sum_{j=1}^{q}\left[b_{i,j}Pre^{f_j}(p_i) + c_{i,j}Post^{f_j}(p_i)\right]$$

be a given linear performance index, where $b_{i,j}$, $c_{i,j} \in \mathbb{R}_0^+$.

A solution of Problem 4 that is optimal with respect to $g(Pre^{f_1}, \ldots, Pre^{f_q}, Post^{f_1}, \ldots, Post^{f_q})$ can be computed by solving the following IPP

$$\begin{cases} \min & g(Pre^{f_1}, \ldots, Pre^{f_q}, Post^{f_1}, \ldots, Post^{f_q}) \\ \text{s.t.} & \mathcal{G}_m(\bar{\mathcal{E}}^F, \bar{\mathcal{D}}^F) \\ & M_0 \ is \ given \end{cases} \tag{6}$$

where

$$\bar{\mathcal{E}}^F = \{(\sigma, t_j) \mid \sigma \in \mathcal{L}^F, |\sigma| < k, \sigma t_j \in \mathcal{L}^F \setminus \mathcal{L}\} \tag{7}$$

and

$$\begin{aligned} \bar{\mathcal{D}}^F = & \{(\sigma, t_j) \mid \sigma \in \mathcal{L}^F \setminus \mathcal{L}, |\sigma| < k, t_j \in T, \sigma t_j \notin \mathcal{L}^F\} \\ & \cup \\ & \{(\sigma, t_j) \mid \sigma \in \mathcal{L}^F, |\sigma| < k, t_j \in T_f, \sigma t_j \notin \mathcal{L}^F\} \end{aligned} \tag{8}$$

Proof: Follows from Theorem 2 and the fact that we have to impose the enabling and disabling constraints only for those sequences that contain fault transitions. In fact, by assumption (A1) all sequences that are enabled in the fault-free net are also enabled in the faulty system. □

***Example** 10:* Let us consider the token passing communication system represented in Figure 3(a), where p_1, p_2, p_3 represent three different agents.

The nominal language of this system is $\mathcal{L} = \{\varepsilon, t_1, t_3, t_1t_2, t_3t_4, t_1t_2t_1, t_1t_2t_3, t_3t_4t_3, t_3t_4t_1, t_1t_2t_1t_2, t_1t_2t_3t_4, t_3t_4t_3t_4, t_3t_4t_1t_2\}$.

Assume we can detect four different types of events denoting faults: f_1, f_2, f_3 and f_4. Monitoring several identical instances of this communication system the following set of strings have been observed: $\mathcal{L}^F = \{\varepsilon, f_1, t_1, t_3, t_1t_2, t_1f_2,\ t_1f_4, t_3t_4, t_3f_3, t_1t_2t_1, t_1t_2t_3, t_1t_2f_1, t_1f_4f_3, t_1f_4t_4, t_3t_4t_3, t_3t_4t_1, t_3t_4f_1, t_1t_2t_1t_2, t_1t_2t_1f_2, t_1t_2t_1f_4, t_1t_2t_3t_4, t_1t_2t_3f_3,\ t_1f_4t_4f_1,\ t_1f_4t_4t_1,\ t_1f_4t_4t_3,\ t_3t_4t_3t_4,\ t_3t_4t_3f_3,\ t_3t_4t_1f_$ $t_3t_4t_1t_2, t_3t_4t_1f_2\}$ thus $k = 4$. Assume that we want to determine the Petri net system that minimizes the arc weights incident on the fault transitions such that $L_k(N^F, M_0) = \mathcal{L}^F$. This requires the solution of a linear IPP of the form (6) where

$$\begin{aligned}\bar{\mathcal{E}}^F = \{&(\varepsilon, f_1), (t_1, f_2), (t_1, f_4), (t_3, f_3), (t_1t_2, f_1),\\ &(t_1f_4, f_3), (t_1f_4, t_4), (t_3t_4, f_1), (t_1t_2t_1, f_2),\\ &(t_1t_2t_1, f_4), (t_1t_2t_3, f_3), (t_1f_4t_4, f_1), (t_1f_4t_4, t_1),\\ &(t_1f_4t_4, t_3), (t_3t_4t_3, f_3), (t_3t_4t_1, f_4), (t_3t_4t_1, f_2)\},\end{aligned}$$

and

$$\begin{aligned}\bar{\mathcal{D}}^F = \{&(\varepsilon, f_2), (\varepsilon, f_3), (\varepsilon, f_4), (f_1, t_1), (f_1, t_2), (f_1, t_3),\\ &(f_1, t_4), (f_1, f_1), (f_1, f_2), (f_1, f_3), (f_1, f_4), (t_1, f_1),\\ &(t_1, f_3), (t_3, f_1), (t_3, f_2), (t_3, f_4), (t_1t_2, f_2),\\ &(t_1t_2, f_3), (t_1t_2, f_4), (t_1f_4, f_1), (t_1f_4, f_2),\\ &(t_1f_4, f_4), (t_1f_4, t_1), (t_1f_4, t_2), (t_1f_4, t_3),\\ &(t_3t_4, f_2), (t_3t_4, f_3), (t_3t_4, f_4), (t_1t_2t_1, f_1),\\ &(t_1t_2t_1, f_3), (t_1t_2t_3, f_1), (t_1t_2t_3, f_2), (t_1t_2t_3, f_4),\\ &(t_1f_4t_4, t_2), (t_1f_4t_4, t_4), (t_1f_4t_4, f_2), (t_1f_4t_4, f_3),\\ &(t_1f_4t_4, f_4), (t_3t_4t_3, f_1), (t_3t_4t_3, f_2), (t_3t_4t_3, f_4),\\ &(t_3t_4t_1, f_1), (t_3t_4t_1, f_3)\}.\end{aligned}$$

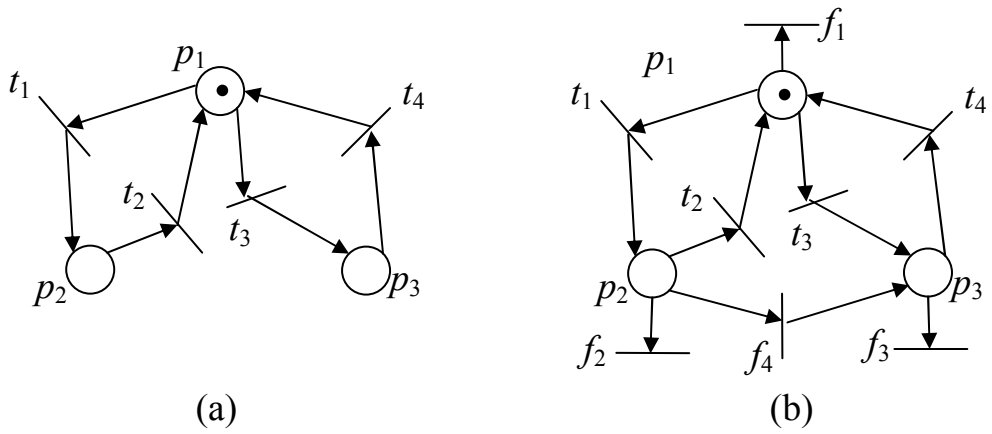

Fig. 3. (a) The faulty-free net system and (b) the faulty net system identified in Example 10.

We find the faulty net system in Fig. 3(b). By inspection of the faulty net, one can associate the following meaning to the faults: f_1 (resp., f_2, f_3) corresponds to a token loss for agent 1 (resp., 2, 3); f_4 corresponds to a token passage from 2 to 3. ■

VI. Fault Identification in Case II

In this section we consider Problem 6, and make the following additional assumptions.

Assumption (A2): The net contains a single fault, i.e., $q = 1$ thus $T_f = \{f\}$. ■

Assumption (A3): Transition t_f is loop-free, i.e., ${}^\bullet t_f \cap t_f^\bullet = \emptyset$. ■

The idea is to use these assumptions to provide an algebraic characterization of the set of admissible faulty systems. In particular, we show that if an upper bound is given on the number of times the fault transition may fire, then the characterization is linear and the identification problem can be written as a linear IPP.

Note that Assumption (A1) restricts the structure of the faulty Petri net to only include one additional faulty transition; it does not restrict the number of times this faulty transition can fire.

A. Preliminary Results

***Definition** 11:* Let $\mathcal{L}$ be the prefix-closed language of a fault-free net system, and $\mathcal{L}^F$ be the prefix-closed language of the faulty net system we want to identify.

We define the following sets:

$$\mathcal{E} = \{(\sigma, t_j) \mid \sigma \in \mathcal{L}, |\sigma| < k, \sigma t_j \in \mathcal{L}\}, \tag{9}$$

$$\mathcal{E}^F = \{(\sigma, t_j) \mid \sigma \in \mathcal{L}^F, |\sigma| < k, t_j \in T, \sigma t_j \in \mathcal{L}^F\}, \tag{10}$$

$$\tilde{\mathcal{E}}^F = \mathcal{E}^F \setminus \mathcal{E} \tag{11}$$

$$\tilde{\mathcal{D}}^F = \{(\sigma, t_j) \mid \sigma \in \mathcal{L}^F, |\sigma| < k, t_j \in T, \sigma t_j \notin \mathcal{L}^F\}. \tag{12}$$

■

***Proposition** 12:* Consider a pair $(\sigma, t_j) \in \tilde{\mathcal{E}}^F$. Under assumptions (A2) and (A3), the net $\langle N^F, M_0\rangle$ generates a word $(\sigma t_j)^F \in P^{-1}(\sigma t_j)$ such that[4] $|(\sigma t_j)^F|_{t_f} = \alpha_{\sigma,j}$, iff the following conditions are both verified:

(a) The net $\langle N^F, M_0\rangle$ generates a word $\sigma^F \in P^{-1}(\sigma)$ with $|\sigma^F|_{t_f} = \alpha_\sigma$.

(b) There exists an integer $\alpha_{\sigma,j}$ such that

$$\begin{cases} M_0 + \alpha_{\sigma,j}(Post^f - Pre^f) + C \cdot \vec{\sigma} \geq Pre(\cdot, t_j) \\ \alpha_{\sigma,j} \geq \alpha_\sigma \end{cases} \tag{13}$$

Proof. (*If* part) If the net $\langle N^F, M_0\rangle$ generates a word whose projection is σt_j, then there exists a firing sequence

$$M_0[\sigma^F\rangle M[t_f^l\rangle M'[t_j\rangle,$$

where $\sigma^F \in P^{-1}(\sigma)$ and $l \geq 0$ additional occurrences of the unobservable transition t_f may be necessary to enable transition t_j after σ^F has fired. Let $|\sigma^F|_{t_f} = \alpha_\sigma$; then according to the state equation it holds

$$\begin{aligned} M' &= M_0 + C \cdot \vec{\sigma} + \alpha_\sigma \cdot (Post^f - Pre^f) \\ &\quad + l \cdot (Post^f - Pre^f) \\ &= M_0 + C \cdot \vec{\sigma} + \alpha_{\sigma,j} \cdot (Post^f - Pre^f) \end{aligned}$$

with $\alpha_{\sigma,j} = \alpha_\sigma + l$ and, since M' enables t_j, we obtain (13).

(*Only if* part) Assume condition (a) is verified so that there exists a marking M such that $M_0[\sigma^F\rangle M$. This allows us to rewrite (13) as

$$\begin{cases} M + l \cdot (Post^f - Pre^f) \geq Pre(\cdot, t_j) \\ l \geq 0 \end{cases}$$

[4]We denote $|\sigma|_t$ the number of occurrences of transition t in sequence σ.

where $l = \alpha_{\sigma,j} - \alpha_\sigma$. Consider now the subnet obtained from N by removing all transitions except t_f with initial marking M. By assumption (A3) the net is acyclic, hence the fact that equation

$$M + l \cdot (Post^f - Pre^f) \geq Pre(\cdot, t_j) \geq \vec{0}$$

is satisfied implies that there exists a marking M' such that $M[t_f^l\rangle M'$ [3]. This means that a sequence $(\sigma t_j)^F \in P^{-1}(\sigma t_j)$ is firable in the faulty net with $|(\sigma t_j)^F|_{t_f} = \alpha_{\sigma,j} = \alpha_\sigma + l$. □

***Proposition** 13:* Consider a pair $(\sigma, t_j) \in \tilde{\mathcal{D}}^F$ and let $\bar{\gamma}_\sigma$ be the minimum number of fault transition firings necessary to enable σ, i.e.,

$$\bar{\gamma}_\sigma = \min_{\sigma^F \in P^{-1}(\sigma)} |\sigma^F|_{t_f}. \tag{14}$$

Under assumptions (A2) and (A3) the net $\langle N^F, M_0\rangle$ disables a transition t_j after all sequences $\sigma^F \in P^{-1}(\sigma)$ that are enabled at M_0, iff $\forall\ \gamma \in \mathbb{N}$, with $\gamma \geq \bar{\gamma}_\sigma$, it holds

$$M_0 + C \cdot \vec{\sigma} + \gamma \cdot (Post^f - Pre^f) \ngeq Pre(\cdot, t_j). \tag{15}$$

Proof. Let us show the *if* part. As well known, a transition t is not enabled at a marking $M' \in R(N, M_0)$ iff $M' \ngeq Pre(\cdot, t)$.

Now, if t_j is not enabled after the firing of all sequences $\sigma^F \in P^{-1}(\sigma)$ at M_0, then $\forall\ \gamma^F = |\sigma^F|_{t_f}$ it should be

$$M_0 + C \cdot \vec{\sigma} + \gamma^F \cdot (Post^f - Pre^f) \ngeq Pre(\cdot, t_j),$$

or, equivalently, equation (15) should be verified for all $\gamma \geq \bar{\gamma}_\sigma$, where $\bar{\gamma}_\sigma$ is defined as in equation (14).

Let us prove the *only if* part. Since the net is acyclic, the state equation gives conditions that are necessary and sufficient for the reachability (and for non-reachability as well). Thus, if equation (15) is satisfied for all $\gamma \geq \bar{\gamma}_\sigma$, then it means that for any marking M such that $M_0[\sigma^F\rangle M$ it is $M \ngeq Pre(\cdot, t_j)$. □

B. IPP Formulation

***Proposition** 14:* Let us consider Problem 6 under assumptions (A1) to (A3), and let

$$g(Pre^f, Post^f) = \sum_{i=1}^{m} \left[b_i Pre^f(p_i) + c_i Post^f(p_i)\right]$$

be a given linear performance index, where b_i, $c_i \in \mathbb{R}_0^+$.

A solution that is optimal with respect to $g(Pre^f, Post^f)$ can be computed by solving the following nonlinear IPP

$$\begin{cases} \min & g(Pre^f, Post^f) \\ \text{s.t.} & \mathcal{G}_m^f(\tilde{\mathcal{E}}^F, \tilde{\mathcal{D}}^F) \\ & M_0 \; is \; given \end{cases} \tag{16}$$

where

$$\mathcal{G}_m^f(\tilde{\mathcal{E}}^F, \tilde{\mathcal{D}}^F) \triangleq$$

$$\begin{cases} \left.\begin{array}{l} M_0 + \alpha_{\sigma,j} \cdot (Post^f - Pre^f) \\ \qquad\qquad +C \cdot \vec{\sigma} \geq Pre(\cdot, t_j) \\ \alpha_{\sigma,j} \in \mathbb{N} \\ \forall \; (\sigma, t_j) \in \tilde{\mathcal{E}}^F \end{array}\right\} (a) \\ \\ \left.\begin{array}{l} -KS_{\sigma,j}^f + M_0 + C \cdot \vec{\sigma} \\ \quad +\gamma \cdot (Post^f - Pre^f) - Pre(\cdot, t_j) \leq -\vec{1}_m \\ \vec{1}^{\,T} S_{\sigma,j}^f \leq m - 1 \\ S_{\sigma,j}^f \in \{0,1\}^m \\ \forall (\sigma, t_j) \in \tilde{\mathcal{D}}^F \\ \forall \gamma \in \mathbb{N} \end{array}\right\} (b) \\ \\ \left.\begin{array}{l} Pre^f(p_i) - z_{1,i} \cdot K \leq 0 \\ Post^f(p_i) - z_{2,i} \cdot K \leq 0 \\ z_{1,i} + z_{2,i} = 1, \quad i = 1, \ldots, m \end{array}\right\} (c) \end{cases} \tag{17}$$

with K (as usual) being a very large constant.

Proof: We first prove that, under assumptions (A1) to (A3), a net system $\langle N^F, M_0 \rangle$ is such that $P(L_k(N^F, M_0)) = \mathcal{L}^F$ if and only if it satisfies the set of algebraic constraints (17).

Constraints (a) are *enabling constraints* relative to those sequences that can only be observed when the fault occurs. They trivially follow from Proposition 12.

Constraints (b) are *disabling constraints* relative to those sequences that are not enabled even

if the fault occurs. They follow from Proposition 13 and their equivalence to constraints

$$\begin{cases} M_0 + C \cdot \vec{\sigma} + \gamma \cdot (Post^f - Pre^f) \not\geq Pre(\cdot, t_j) \\ \forall (\sigma, t_j) \in \tilde{\mathcal{D}}^F \\ \forall \gamma \in \mathbb{N} \end{cases}$$

To prove the equivalence between the two sets of constraints we first observe that, if t_j is not enabled at $M_0 + C \cdot \vec{\sigma} + \gamma \cdot (Post^f - Pre^f)$, then there exists at least one place $p \in P$ such that

$$\begin{aligned} M_0(p) + C(p, \cdot) \cdot \vec{\sigma} + \gamma \cdot (Post^f(p) - Pre^f(p)) \\ \leq Pre(p, t_j) - 1. \end{aligned} \tag{18}$$

This holds for all p such that $S^f_{\sigma,j}(p) = 0$. But, being $\vec{1}^T S^f_{\sigma,j} \leq m - 1$, this occurs for at least one place $p \in P$.

Finally, we observe that assuming $\gamma \in \mathbb{N}$ in (b) rather than $\gamma \geq \bar{\gamma}_\sigma$ (see equation (15)), introduces no spurious markings. In fact, by definition of $\bar{\gamma}_\sigma$, constraints (b) are redundant for all $\gamma \in [0, \bar{\gamma}_\sigma)$.

Constraints (c) force transition t_f to be loop-free. In fact, they imply that if $Pre^f(p_i) > 0$, then $Post^f(p_i) = 0$, and viz. □

***Remark** 15:* In Problem 6 we assumed that all sequences that are not in $\mathcal{L}^F$ are not observable, namely there exists no sequence of fault transitions that can enable them. In several practical applications it could be of interest to slightly modify the problem statement by assuming that no information can be deduced if a given sequence is not observed (it may be possible that no fault sequence is able to make it firable, but it can also be possible that such faults have not yet occurred even if their firing would have enabled it). In such a case a solution to the identification problem can still be computed by solving the IPP (16), provided that the disabling constraints (b) are removed from the set (17).

■

C. Constraints Linearization

Proposition 14 provides a systematic approach to solve Problem 6 under assumptions (A1) to (A3). However, some of the constraints that are necessary to characterize the set of admissible solutions are nonlinear.

The nonlinearity can be removed by assigning an upper bound Γ on the number of times the fault transition t_f may fire[5].

In particular, constraint (a) for the generic couple $(\sigma, t_j) \in \tilde{\mathcal{E}}^F$ can be translated into an OR constraint that can be written as a set of $\Gamma + 1$ linear constraints

$$\begin{cases} M_0 + Post^f - Pre^f + C \cdot \vec{\sigma} \\ \qquad\qquad -Pre(\cdot, t_j) \geq z^1_{\sigma,j} \cdot \vec{K} \\ M_0 + 2 \cdot (Post^f - Pre^f) + C \cdot \vec{\sigma} \\ \qquad\qquad -Pre(\cdot, t_j) \geq z^2_{\sigma,j} \cdot \vec{K} \\ \quad \vdots \\ \\ M_0 + \Gamma \cdot (Post^f - Pre^f) + C \cdot \vec{\sigma} \\ \qquad\qquad -Pre(\cdot, t_j) \geq z^\Gamma_{\sigma,j} \cdot \vec{K} \\ z^1_{\sigma,j} + z^2_{\sigma,j} + \ldots z^\Gamma_{\sigma,j} = \Gamma - 1 \\ z^1_{\sigma,j}, z^2_{\sigma,j}, \ldots, z^\Gamma_{\sigma,j} \in \{0, 1\} \end{cases}$$

where, as usual, K is a very large constant [2], and $\vec{K} = K \cdot \vec{1}_m$.

Similarly, if $\gamma \leq \Gamma$, the nonlinear inequality in (b) translates into an AND constraint that can be written as a set of Γ linear constraints

$$\begin{cases} -KS^f_{\sigma,j} + M_0 + C \cdot \vec{\sigma} + Post^f - Pre^f \\ \qquad\qquad -Pre(\cdot, t_j) \leq -\vec{1}_m \\ -KS^f_{\sigma,j} + M_0 + C \cdot \vec{\sigma} + 2 \cdot (Post^f - Pre^f) \\ \qquad\qquad -Pre(\cdot, t_j) \leq -\vec{1}_m \\ \quad \vdots \\ \\ -KS^f_{\sigma,j} + M_0 + C \cdot \vec{\sigma} + \Gamma \cdot (Post^f - Pre^f) \\ \qquad\qquad -Pre(\cdot, t_j) \leq -\vec{1}_m \end{cases}$$

[5]Note that a tradeoff should be made while choosing Γ. In fact, a large value of Γ makes the linearization less restrictive but results in a higher computational complexity. We assume here that a tentative value of Γ is initially taken, and it is then increased if the resulting set of linear constraints is infeasible.

D. Complexity of the Identification Procedure

We now discuss the complexity of the IPP we must solve to identify the faulty system. This complexity is given in terms of the number of constraints and the number of unknowns. Note however that it is well known that an IPP is an NP-hard problem itself.

Let n be the cardinality of T, k the length of the longest string in $\mathcal{L}$, and ν_r (ν'_r), for $r = 0, \ldots, k$, the number of strings in $\mathcal{L}^F \setminus \mathcal{L}$ ($\mathcal{L}^F$) of length r.

Then the nonlinear constraint set (17) contains

- $m \sum_{r=1}^{k} \nu_r$ constraints of type (a),
- $(m+1) \sum_{r=0}^{k-1} (n \cdot \nu'_r - \nu'_{r+1})$ constraints of type (b),
- $3 \cdot m$ constraints of type (c).

When linearized, the number of constraints (a) and (b) becomes equal to

$$m \cdot (\Gamma + 1) \sum_{r=1}^{k} \nu_r$$

and

$$(m \cdot \Gamma + 1) \sum_{r=0}^{k-1} (n \cdot \nu'_r - \nu'_{r+1})$$

respectively.

The total number of unknowns in the nonlinear IPP is

$$u_{nl} = 2m + \sum_{r=1}^{k} \nu_r \cdot + m \sum_{r=0}^{k-1} (n \cdot \nu'_r - \nu'_{r+1}) + 2m,$$

where the right-side terms are due respectively to the number of pre and post-incidence arcs, the integer variables $\alpha_{\sigma,j}$ in (a), the binary vectors $S^f_{\sigma,j}$ in (b), and the binary variables $z_{i,1}$ and $z_{i,2}$ in (c).

The total number of unknowns in the linear IPP is

$$u_l = 2m + \Gamma \cdot \sum_{r=1}^{k} \nu_r + m \sum_{r=0}^{k-1} (n \cdot \nu'_r - \nu'_{r+1}) + 2m.$$

Note that given values of k and n, it is possible to find a worst case bound for $\rho = \sum_{r=0}^{k-1} (n \cdot \nu'_r - \nu'_{r+1})$. In fact, it holds:

$$\begin{aligned} \rho &= \textstyle\sum_{r=0}^{k-1} (n \cdot \nu'_r - \nu'_{r+1}) \\ &= n \cdot \nu'_0 + (n-1) \cdot \left(\textstyle\sum_{r=1}^{k-1} \nu'_r \right) - \nu'_k \\ &= n + (n-1) \cdot \left(\textstyle\sum_{r=1}^{k-1} \nu'_r \right) - \nu'_k. \end{aligned}$$

This expression is maximized if we assume $\nu'_k = 0$ while all other ν'_r take the largest possible value, i.e., $\nu'_r = n^r$. Hence, we have

$$\rho \leq n + (n-1) \cdot (n + \cdots + n^{k-1}) = n^k,$$

so that the total number of unknowns in the nonlinear IPP in the worst case is

$$u_{\mathrm{nl_{MAX}}} \leq 4m + \textstyle\sum_{r=1}^{k} n^r + m \cdot n^k = \mathcal{O}(m\ n^k),$$

and the total number of unknowns in the linear IPP in the worst case is

$$u_{\mathrm{l_{MAX}}} \leq 4m + \Gamma \cdot \textstyle\sum_{r=1}^{k} n^r + m \cdot n^k = \mathcal{O}(m\ \Gamma\ n^k),$$

i.e., this problem has exponential complexity with respect to k.

E. Numerical Examples

In this section we present two examples. First, we provide an example of the procedure previously presented and then we show the problem of acyclicity and then the necessity of the assumption (A3).

***Example** 16:* Let us consider the net in Fig. 4(a) and the two languages $\mathcal{L} = \{\varepsilon, t_1, t_1t_1, t_1t_1t_2\}$ and $\mathcal{L}^F = \{\varepsilon, t_1, t_2, t_1t_1, t_2t_1, t_2t_2, t_1t_1t_2, t_2t_1t_1, t_2t_2t_1, t_2t_2t_2\}$ thus $k = 3$. Assume that we want to determine the Petri net system that minimizes the arc weights associated with the fault transition such that $P(L_k(N^F, M_0)) \in \Lambda(\mathcal{L}^F)$. This requires the solution of a linearized IPP of the form (17) where

$$\mathcal{E} = \{(\varepsilon, t_1), (t_1, t_1), (t_1t_1, t_2)\},$$

$$\begin{aligned}\mathcal{E}^F \;=\; & \{(\varepsilon, t_1), (\varepsilon, t_2), (t_1, t_1), (t_2, t_1), (t_2, t_2), (t_1t_1, t_2),\\ & (t_2t_1, t_1), (t_2t_2, t_1), (t_2t_2, t_2)\},\end{aligned}$$

$$\begin{aligned}\tilde{\mathcal{E}}^F \;=\; & \{(\varepsilon, t_2), (t_2, t_1), (t_2, t_2), (t_2t_1, t_1), (t_2t_2, t_1),\\ & (t_2t_2, t_2)\},\end{aligned}$$

and

$$\tilde{\mathcal{D}}^F = \{(t_1, t_2), (t_1t_1, t_1), (t_2t_1, t_2)\}.$$

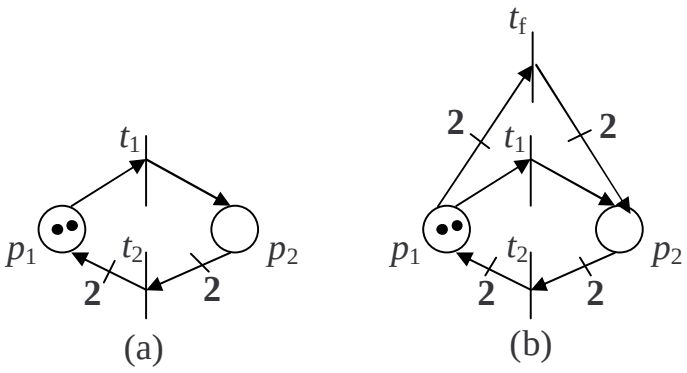

Fig. 4. (a) The faulty-free net system and (b) the faulty net system identified in Example 16.

For $\Gamma = 1$ and $\Gamma = 2$ we get no feasible solution, while for $\Gamma = 3$ we find the faulty net system in Fig. 4(b), where $Pre^f = [2\ 0]^T$ and $Post^f = [0\ 2]^T$. ■

***Example** 17:* Let us consider the net in Fig. 5(a) and the two languages $\mathcal{L} = \{\varepsilon, t_1, t_1t_1, t_1t_1t_2\}$ and $\mathcal{L}^F = \{\varepsilon, t_1, t_1t_1, t_1t_2, t_1t_1t_2, t_1t_2t_1\}$, thus $k = 3$. We note that a solution for these two languages exists and it is represented by the faulty net system in Fig. 5(b), but if we apply the identification procedure proposed we obtain that no integer solution is found, even if the constraints relative to the acyclicity of the fault transition, i.e., the constraints (c) in (17), are removed. Since our constraints are based on the incidence matrix, the two nets shown in Fig. 5(b) and Fig. 5(c) are equivalent as far as our procedure is concerned. The problem is that for the net in Fig. 5(c) the disabling constraint on the couple (ε, t_2) is not verified, since transition t_2 can be enabled at M_0 after t_f has fired twice. ■

VII. Conclusions

We have presented an approach for the identification of faults on a system modeled by Petri nets based on the knowledge of the nominal system and of the faulty behavior. If the faults are not observable, the presented approach requires two assumptions to hold: (A2) there exists a single faulty transition, and furthermore (A3) this transition must be loop-free. It may be possible to relax assumption (A2) and take into account the case of more than one faulty transition: this extension is rather straightforward but significantly increases the computational complexity during the phase of constraint linearization.

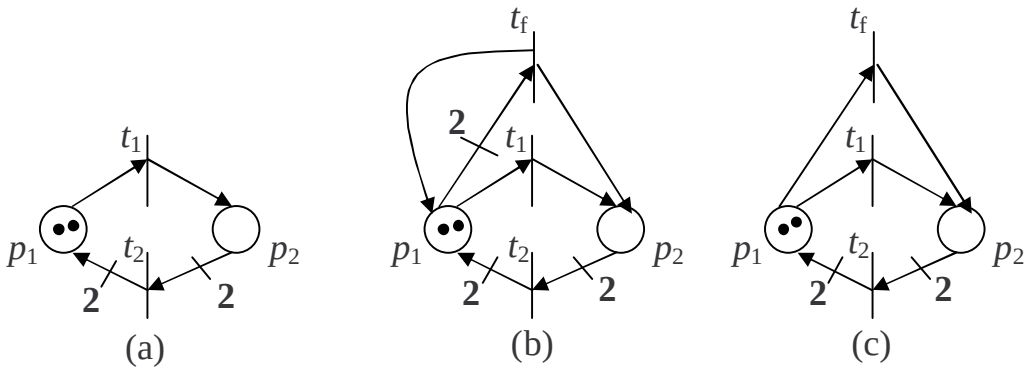

Fig. 5. (a) The faulty-free net system of Example 17, (b) the faulty net system where t_f is not loop-free, (c) the equivalent net of the one represented in (b).

REFERENCES

[1] R.K. Boel and J.H. van Schuppen. Decentralized failure diagnosis for discrete-event systems with costly communication between diagnosers. In *Proc. WODES'02: 6th Work. on Discrete Event Systems (Zaragoza Spain)*, pages 175–181, October 2002.

[2] M.P. Cabasino, A. Giua, and C. Seatzu. Identification of Petri nets from knowledge of their language. *Discrete Events Dynamic Systems*, 17(4):447–474, 2007.

[3] D. Corona, A. Giua, and C. Seatzu. Marking estimation of Petri nets with silent transitions. *IEEE Trans. Automatic Control*, 52(9):1695–1699, September 2007.

[4] R. Debouk, S. Lafortune, and D. Teneketzis. Coordinated decentralized protocols for failure diagnosis of discrete-event systems. *Discrete Events Dynamic Systems*, 20:33–79, 2000.

[5] A. Giua and C. Seatzu. Identification of free-labeled Petri nets via integer programming. In *Proc. IEEE 44rd Int. Conf. on Decision and Control (Seville, Spain)*, pages 7639–7644, December 2005.

[6] S. Jiang and R. Kumar. Failure diagnosis of discrete-event systems with linear-time temporal logic specifications. *IEEE Trans. Automatic Control*, 49(6):934–945, June 2004.

[7] J. Lunze and J. Schroder. Sensor and actuator fault diagnosis of systems with discrete inputs and outputs. *IEEE Trans. Systems, Man and Cybernetics, Part B*, 34(3):1096–1107, April 2004.

[8] T. Murata. Petri nets: properties, analysis and applications. *Proceedings of the IEEE*, 77(4):541–580, 1989.

[9] M. Sampath and S. Lafortune. Active diagnosis of discrete-event systems. *IEEE Trans. Automatic Control*, 43:908–929, 1998.

[10] S. Hashtrudi Zad, R.H. Kwong, and W.M. Wonham. Fault diagnosis in discrete-event systems: framework and model reduction. *IEEE Trans. Automatic Control*, 48(7):1199–1212, July 2003.