Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

Fault Detection of Discrete Event Systems Using Petri Nets and Integer Linear Programming

Dotoli M., Fanti M.P.*, Mangini A.M.*****

** Electrical and Electronic Engineering Department, Polytechnic of Bari, Bari Italy (tel. +39-080-5963643, e-mail: fanti@deemail.poliba.it).*
***Electrical and Electronic Engineering Department, Polytechnic of Bari, Bari Italy (e-mail: dotoli@deemail.poliba.it).*
****Electrical and Electronic Engineering Department, Polytechnic of Bari, Bari Italy (e-mail: mangini@deemail.poliba.it).*

Abstract: The paper addresses the fault detection problem for discrete event systems on the basis of a Petri Net (PN) model. Assuming that the structure of the PN and the initial marking are known, faults are modelled by unobservable transitions. Moreover, we assume that there may be additional unobservable transitions that are associated with the system legal behaviour and that the marking reached after the firing of a transition is unknown. We propose a diagnoser that works on-line: it waits for the firing of an observable transition and employs an algorithm based on the definition of some integer linear programming problems to decide whether the system behaviour is normal or exhibits some possible faults.

1. INTRODUCTION

Faults are physical conditions that cause a device or a component to fail to perform in a required manner. A fault may cause failures, i.e., the termination of the ability of an item to perform a function. If a fault is detected early and removed, the failure may be avoided. Hence, automatic fault detection and diagnosis in Discrete Event Systems (DES) is a research area that received a lot of attention in the last years. The analysis of the fault detection and diagnosis of DES is based in the related literature on models that describe the expected behaviour of the system in the presence of faults (see the works by Sampath *et al.* 1995, 1998 for an overview of the literature). In (Sampath *et al.* 1995) the diagnoser is a finite state machine containing the system state estimate and the transition from a normal state to a fault state is triggered by an unobservable event. Moreover, Lunze and Schroder (2004) use a stochastic automaton and a diagnostic algorithm that detects the existence of a fault and isolates possible sensor or actuator faults or identifies plant faults. However, these approaches require the explicit determination of all the system states. In order to cope with the state explosion problem, Petri Net (PN) models have been used in the context of DES fault detection. Hadjicostis and Verghese (1999) consider faults in PN in the form of losses or duplications of tokens. Sahraoui *et al.* (1987) use PN to model the normal behaviour of systems and consider as faults the occurrence of events that do not match firing conditions properly. Benveniste *et al.* (2003) propose an approach to handle unbounded asynchrony in DES diagnosis using net unfolding. In addition, Prock (1991) presents a technique for on-line fault detection monitoring the number of tokens marking places belonging to p-invariants: when the number of tokens inside p-invariants changes then a fault is detected. Ushio et al. (1998) extend the necessary and sufficient condition for diagnosability to unbounded PN and introduce a method for the modification of coverability trees in order to detect failure transitions. Moreover, Giua and Seatzu (2005) construct a diagnoser using PN models and a deterministic automaton whose edges are labelled by the observable transitions and nodes are reachable from the initial state by a firing sequence of transitions. However, the drawback of this diagnoser approach is that it requires the computation of a new diagnoser if the system changes. In a recent paper, Ramirez-Trevino *et al.* (2007) propose an on-line approach for fault diagnosis of DES by the interpreted PN formalism.

This paper deals with the fault detection and diagnosis of DES on the basis of a PN model of the system. Assuming that the structure of the PN and the initial marking are known, faults are modelled by unobservable transitions. Moreover, we assume that there may exist additional unobservable transitions that are associated with the system legal behaviour. The proposed diagnoser works on-line: it waits for an observable event and an algorithm decides whether the system behaviour is normal or may exhibit some possible faults. To this aim, some Integer Linear Programming Problems (ILPP) are defined and provide eventually the minimal sequences of silent transitions containing the faults that may have occurred.

The proposed approach avoids the state explosion problem because it neither requires the complete knowledge of the state reachability set as in (Corona *et al.* 2004) nor that of the automaton states as in (Sampath *et al.* 1995). Moreover, it is a general technique since no assumption is imposed on the reachable state set that can be unlimited and few properties must be fulfilled by the structure of the PN modeling the system. In addition, the benefit of this approach compared with the fault detection methods proposed in the related literature is that it does not require the computation of a new diagnoser when the system changes or it is reconfigurated.

2. BASIC DEFINITIONS ON PETRI NETS

This section recalls some basic definitions on PN (Peterson, 1981).

Definition 1: A PN is a bipartite graph described by the four-tuple $PN=(P, T, \boldsymbol{Pre}, \boldsymbol{Post})$, where P is a set of places with cardinality m, T is a set of transitions with cardinality n, $\boldsymbol{Pre}$: $P\times T\rightarrow\mathbb{N}$ and $\boldsymbol{Post}$: $P\times T\rightarrow\mathbb{N}$ are the *pre-* and *post-incidence matrices* respectively, which specify the arcs connecting places and transitions. More precisely, for each $p\in P$ and $t\in T$ element $\boldsymbol{Pre}(p,t)$ ($\boldsymbol{Post}(p,t)$) is equal to a natural number indicating the arc multiplicity if an arc going from p to t (from t to p) exists, and it equals 0 otherwise. Note that $\mathbb{N}$ is the set of non-negative integers. Matrix $\boldsymbol{C}=\boldsymbol{Post}-\boldsymbol{Pre}$ is the $m\times n$ *incidence matrix* of the net

For the pre- and post-sets we use the dot notation, e.g., $\bullet t=\{p\in P: \boldsymbol{Pre}(p,t)>0\}$. A PN is said *pure* if for each $p\in P$ and $t\in T$ it holds $\boldsymbol{Pre}(p,t)\boldsymbol{Post}(p,t)=0$, i.e., p can not be simultaneously an input and output place of the same transition t.

The state of a PN is given by its current marking, which is a mapping $\boldsymbol{M}$: $P\rightarrow\mathbb{N}$, assigning to each place of the net a nonnegative number of tokens. A PN system $\langle PN,\boldsymbol{M_0}\rangle$ is a net PN with an initial marking $\boldsymbol{M_0}$.

A transition $t_j\in T$ is enabled at a marking $\boldsymbol{M}$ if and only if (iff) for each $p\in\bullet t_j$, it holds $\boldsymbol{M}(p)\geq\boldsymbol{Pre}(p,t_j)$ and we write $\boldsymbol{M}[t_j>$ to denote that $t_j\in T$ is enabled at marking $\boldsymbol{M}$. When fired, t_j produces a new marking $\boldsymbol{M'}$, denoted by $\boldsymbol{M}[t_j>\boldsymbol{M'}$ that is computed by the PN state equation $\boldsymbol{M'}=\boldsymbol{M}+\boldsymbol{C}\,\vec{t}_j$ where $\vec{t}_j$ is the n-dimensional firing vector corresponding to the j-th canonical basis vector.

Let $\sigma=t_{b_1},t_{b_2},...,t_{b_k}$ be a sequence of transitions (or firing sequence) and let $k=|\sigma|$ be its length, given by the number of transitions that σ contains. If a transition $t\in T$ appears in the sequence σ, we write $t\in\sigma$. Moreover, the notation $\boldsymbol{M}[\sigma\rangle\boldsymbol{M'}$ indicates that the sequence of the enabled transitions σ may fire at $\boldsymbol{M}$ yielding $\boldsymbol{M'}$. We also denote $\vec{\sigma}$: $T\rightarrow\mathbb{N}^n$ the firing vector associated with a sequence σ, i.e., $\vec{\sigma}(t)=q$ if transition t is contained q times in σ. A marking $\boldsymbol{M}$ is said reachable from $\langle PN,\boldsymbol{M_0}\rangle$ iff there exists a firing sequence σ such that $\boldsymbol{M}_0[\sigma\rangle\boldsymbol{M}$. The set of all markings reachable from $\boldsymbol{M}_0$ defines the reachability set of $\langle PN,\boldsymbol{M_0}\rangle$ and is denoted by $R(PN,\boldsymbol{M}_0)=\{\boldsymbol{M}|\exists\ \sigma : \boldsymbol{M}_0[\sigma\rangle\boldsymbol{M}\}$.

A PN having no oriented cycles is called *acyclic*. We recall the following result for this subclass of PN:

Theorem 1: (Corona *et al.* 2004) Let PN be an acyclic PN.

(i) If vector $\boldsymbol{y}$ satisfies equation $\boldsymbol{M_0}+\boldsymbol{Cy}\geq 0$ there exists a firing sequence σ firable from $\boldsymbol{M_0}$ and such that the firing vector associated to σ is $\boldsymbol{y}$.

(ii) A marking $\boldsymbol{M}$ is reachable from $\boldsymbol{M_0}$ iff there exists a non negative integer solution $\boldsymbol{y}$ satisfying the state equation $\boldsymbol{M}=\boldsymbol{M_0}+\boldsymbol{C}\,\boldsymbol{y}$.

A language may be a formal way describing the behaviour of a DES. The event set $E=\{e_i\}$ is viewed as an alphabet and $L\subset E^*$ is the set of all words (sequence of events) generated by the system, also called the DES language (Cassandras and Lafortune 1999).

If a PN $PN=(P, T, \boldsymbol{Pre}, \boldsymbol{Post})$ is used to model the DES, the system events are associated with transitions.

Definition 2: Given a PN, the function λ: $T\rightarrow E\cup\{\varepsilon\}$ is the transition labelling function that assigns to each transition $t\in T$ either a symbol $e_i\in E$ or the empty string ε.

We assume that the set of transitions is partitioned into $T=T_o\cup T_u$, where T_o represents the set of *observable* transitions and T_u represents the set of *unobservable* or *silent* transitions. Accordingly, the labelling function λ is defined as follows: if $t\in T_u$ then $\lambda(t)=\varepsilon$, if $t\in T_o$ then $\lambda(t)\neq\varepsilon$.

In this paper we assume that the same label $e_i\in E$ cannot be associated to more than one transition. Hence, the labelling function restricted to T_o is an isomorphism and with no loss of generality we assume $E=T_o$.

Definition 3: Given a net $PN=(P, T, \boldsymbol{Pre}, \boldsymbol{Post})$ and a subset $T_A\subseteq T$ of its transitions, we define the T_A-induced subnet of PN as the new net $PN_A=(P, T_A, \boldsymbol{Pre}_A, \boldsymbol{Post}_A)$ where $\boldsymbol{Pre}_A$ and $\boldsymbol{Post}_A$ are the restrictions of $\boldsymbol{Pre}$ and $\boldsymbol{Post}$ to T_A. In other words, the net PN_A is obtained from PN removing all transitions in $T\backslash T_A$. We also write $PN_A\angle_{TA}PN$.

In the following we consider the subnet $PN_u\angle_{Tu}PN$.

3. FAULT DETECTION PROBLEM STATEMENT

3.1 Basic Definitions

In this section we provide some further definitions necessary to introduce the fault detection problem for DES.

Let $\Delta_f=\{f_1,\dots f_F\}$ be the set of faults that may occur in the system and F the corresponding cardinality. Each $f_i\in\Delta_f$ is modelled by an unobservable fault transition $\tau_i\in T_f$ with $T_f=\{\tau_1, \tau_2,\dots, \tau_F\}\subseteq T_u$, since an observable fault transition is trivially diagnosed. Consequently, denoting by $T_{nf}=\{\tau_{F+1}, \tau_{F+2},\dots, \tau_{F+H}\}$ the set of H unobservable transitions that do not correspond to faults, it holds $T_u=T_f\cup T_{nf}$. We say that a fault f_i with $i\in\{1,\dots,F\}$ occurs when the corresponding fault transition $\tau_i\in T_f$ fires. Obviously, the observable transitions are n-H-F=O in number.

Moreover, we denote by w the word of events associated with the sequence $\sigma\in T^*$ with $w=\lambda(\sigma)$, using the extended form of the transition labelling function λ: $T^* \rightarrow E^*$ in the usual manner. Note that the length of a sequence σ is greater than or equal to the corresponding word w (i.e., $|\sigma|\geq|w|$). In fact, if σ contains q transitions labelled by ε, then $|\sigma|=q+|w|$. In addition, we denote by $\sigma_u\in\sigma$ ($\sigma_o\in\sigma$) the subsequence of σ composed by the unobservable (observable) transitions and by $\vec{\sigma}_u : T_u\rightarrow \mathbb{N}^{H+F}$ ($\vec{\sigma}_o : T_o\rightarrow \mathbb{N}^{O}$) the corresponding firing vector. Analogously, we denote by $\sigma_f\,(\sigma_{nf})\in\sigma_u$ the subsequence of σ_u composed by the fault (no fault) transitions and by $\vec{\sigma}_f$ ($\vec{\sigma}_{nf}$) the corresponding firing vectors. By the assumption $E=T_o$, it holds $\sigma_o=w$. Note that in the following we denote the firing vector $\vec{\sigma}=\begin{bmatrix}\vec{\sigma}_o\\ \vec{\sigma}_u\end{bmatrix}$.

The following definitions are necessary for the diagnoser specification.

Definition 4. Given the initial marking $\boldsymbol{M_0}\in \mathbb{N}^m$ and an observable sequence σ_o, we define

$\Sigma(\boldsymbol{M_0}, \sigma_o)=\{\sigma\in T^* \mid \boldsymbol{M_0}[\sigma\rangle, \sigma_o\in\sigma \text{ and } |\sigma|>|\sigma_o|\}$

the set of *interpretations* of σ_o at $\boldsymbol{M_0}$.

More precisely, $\Sigma(\boldsymbol{M_0}, \sigma_o)$ is the set of sequences containing the observable sequence σ_o and the unobservable sequences whose firing at $\boldsymbol{M_0}$ is consistent with the observed sequence σ_o.

Definition 5. Given the initial marking $\boldsymbol{M_0}\in \mathbb{N}^m$ and an observable sequence σ_o, we define the set of interpretations of σ_o at $\boldsymbol{M_0}$ containing the fault f_k as:

$\Sigma(\boldsymbol{M_0}, \sigma_o, f_k)=\{ \sigma\in\Sigma(\boldsymbol{M_0}, \sigma_o) \mid \tau_k\in\sigma \}$.

Among the above sequences, we want to select those whose firing vector is minimal, that we call *minimal interpretations*.

Definition 6. Given the initial marking $\boldsymbol{M_0}\in \mathbb{N}^m$ and an observable sequence σ_o, we define the set of minimal interpretations of σ_o at $\boldsymbol{M_0}$ containing the fault f_k:

$\Sigma_m(\boldsymbol{M_0}, \sigma_o, f_k)=\{ \sigma\in\Sigma(\boldsymbol{M_0}, \sigma_o, f_k) \mid \neg\exists\ \sigma'\in\Sigma(\boldsymbol{M_0}, \sigma_o, f_k)$ such that $|\sigma'|<|\sigma|\}$

and we denote $Y_m(\boldsymbol{M_0}, \sigma_o, f_k)=\{\vec{\sigma}\in \mathbb{N}^m \mid \sigma\in\Sigma_m(\boldsymbol{M_0}, \sigma_o, f_k)\}$ the corresponding set of firing vectors.

3.2 The Diagnoser Definition

In this paper we deal with the problem of detecting at each observed DES event whether the behaviour is normal or a fault may have occurred. Hence we address the specification of a *diagnoser*.

We assume the following properties hold for the system under investigation:

A1) the structure of the net *PN* modelling the DES is known and pure;
A2) the initial marking $\boldsymbol{M_0}$ is known;
A3) the labels associated to the firing of transitions in T_o can be observed;
A4) the subnet $PN_u\angle_{T_u}PN$ is acyclic.

In particular, assumption A1 imposes that each transition firing changes the token distribution of the net. Moreover, A2 and A3 are assumptions that exhibit the level of the system knowledge. Finally, assumption A4 is commonly adopted in the field of fault detection and it means that cycles of non-observable events are not admissible (Sampath *et al.* 1995).

The inputs of the diagnoser are the initial marking $\boldsymbol{M_0}$ and the observed word $w\in L$, where L is the language of the DES. Assuming that $w=\lambda(\sigma)$, the sequence $\sigma=\sigma_{u_1}t_{\alpha_1}\sigma_{u_2}t_{\alpha_2}...\sigma_{u_h}t_{\alpha_h}$ with $h\geq1$ denotes the sequence of observable and unobservable transitions corresponding to the word w. More precisely, $\sigma_o=t_{\alpha_1}t_{\alpha_2}...t_{\alpha_h}=w$ with $t_{\alpha_i}\in T_o$ for $i=1,\ldots,h$ is the observable subsequence of σ and each $\sigma_{u_i}\in T_u^*$ is the sequence of unobservable transitions that have occurred before transition t_{α_i} for i=1,…,h and after transition $t_{\alpha_{i-1}}$ for i=2,…,h.

Definition 7: A *diagnoser* is a function Φ that associates to each observed word $w\in T^*_o$ and to each initial marking $\boldsymbol{M_0}\in \mathbb{N}^m$ the following sets:

- $\Phi(\boldsymbol{M}_0,w)= N$

if the behaviour of the system is *normal* during the observed word w because there exists no firing sequence containing a transition $\tau_k\in T_f$ that is consistent with the observation.

- $\Phi(\boldsymbol{M}_0,w)=\{(f_k, \vec{\sigma}) \mid \Sigma(\boldsymbol{M_0}, \sigma_o, f_k)\neq\emptyset$ and $\vec{\sigma}\in Y_m(\boldsymbol{M_0}, \sigma_o, f_k)$ with $\sigma_o=w\}$

if fault $f_k\in\Delta_f$ may have occurred during the observed word w. In such a case $\forall f_k\in\Delta_f$ such that $\Sigma(\boldsymbol{M_0}, \sigma_o, f_k)\neq\emptyset$ the diagnoser provides the firing vector of a minimal interpretation of $\sigma_o=w$ containing fault f_k.

- $\Phi(\boldsymbol{M}_0,w)=\{(f_k, \vec{\sigma}) \mid \Sigma(\boldsymbol{M_0}, \sigma_o, f_k)\neq\emptyset$ and $\vec{\sigma}\in Y_m(\boldsymbol{M_0}, \sigma_o, f_k)$ with $\sigma_o=w\}\cup\{N\}$

if two cases may occur: i) some faults $f_k\in\Delta_f$ may have occurred during the observed word w, ii) the behaviour of the system may be normal.

Definition 8: A PN system <*PN*,$\boldsymbol{M_0}$> is said diagnosable if for each observed word $w\in T^*_o$ the diagnoser detects either a normal behaviour or a set of faults that must have occurred because they are contained in each firable sequence consistent with the observation.

Example 1: As an example, let us consider the net in Fig. 1. Assume that the set of observable transitions is $T_o=\{t_1, t_2, t_3\}$ and the set of unobservable transitions is $T_u=\{\tau_1,\ldots,\tau_4\}$, where faults f_1 and f_2 are associated to transitions τ_1 and τ_2, respectively. Let us also assume that the system is in the initial marking $\boldsymbol{M}_0=[1\ 1\ 0\ 0\ 0\ 0\ 0]^T$ and word $w=t_1=\sigma_o$ is observed. We infer $\Sigma_m(\boldsymbol{M_0}, t_1, f_1)=\{(\tau_1 t_1)\}$ and $\Sigma_m(\boldsymbol{M_0}, t_1, f_2)=\emptyset$.

Hence, $\Phi(\boldsymbol{M}_0,t_1)=\{(f_1, \vec{\sigma}=[1\ \ 0\ \ 0\ \mid\ 1\ \ 0\ \ 0\ \ 0]^T), N\}$ is obtained by the diagnoser, i.e., fault f_1 may have occurred but the behaviour may also be normal.

Now, assume that at marking $\boldsymbol{M}_0$ word $w=t_1t_2$ is observed. The sets of minimal interpretations of $\sigma_o=t_1t_2$ at $\boldsymbol{M}_0$ are $\Sigma_m(\boldsymbol{M}_0,t_1t_2,f_k)=\varnothing$ for k=1,2. Hence, the diagnoser provides $\Phi(\boldsymbol{M}_0,(t_1t_2))=N$, i.e., fault f_1 has not occurred during the observed sequence and the behaviour must be normal.

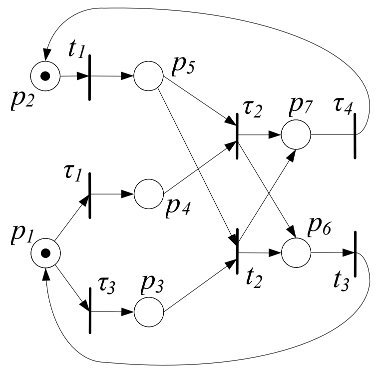

Fig. 1. *The PN of Example 1.*

4. THE DIAGNOSER SPECIFICATION

Given a DES with language L and a PN system $\langle PN,\boldsymbol{M}_0\rangle$ modelling the DES and satisfying A1-A4, this section proposes an algorithm that specifies on-line a *diagnoser* Φ for each initial marking $\boldsymbol{M}_0\in\mathbb{N}^m$ at the occurrence of an observed word $w\in L$. To show the algorithm properties, the following results are proven.

Proposition 1: Let us consider a DES with language L and a PN system $\langle PN,\boldsymbol{M}_0\rangle$ modelling the DES and satisfying A1-A4. Given an observation $w\in L$ denoted by $w=\sigma_o=t_{\alpha_1}t_{\alpha_2}...t_{\alpha_h}$, if there exists $f_k\in\Delta_f$ and a sequence $\sigma=\sigma_{u_1}t_{\alpha_1}...\sigma_{u_h}t_{\alpha_h}$ with $|\sigma_{u_i}|\geq 0$ such that $\sigma\in\Sigma_m(\boldsymbol{M}_0,\sigma_o,f_k)$, then the following ILPP 1 admits at least a solution.

$$\textit{ILPP 1: } \min\varphi(\vec{\sigma}_{u_1},\vec{\sigma}_{u_2},...,\vec{\sigma}_{u_h})=\vec{\mathbf{1}}^T_{F+H}\sum_{i=1}^{h}\vec{\sigma}_{u_i} \tag{1}$$

s.t. $\xi_1(w,\boldsymbol{M}_0,\boldsymbol{Post},\boldsymbol{Pre})=$

$$=\begin{cases}\boldsymbol{M}_i\in\mathbb{N}^m \text{ for } i=1,...,h & (2a)\\ \vec{\sigma}_{u_i}\in\mathbb{N}^{F+H}, \text{ for } i=1,...,h & (2b)\\ \boldsymbol{M}_{i\text{-}1}+\boldsymbol{C}_u\vec{\sigma}_{u_i}\geq 0 \text{ for } i=1,...,h & (2c)\\ \boldsymbol{M}_{i\text{-}1}+\boldsymbol{C}_u\vec{\sigma}_{u_i}\geq \boldsymbol{Pre}\,\vec{t}_{\alpha_i} \text{ for } i=1,...,h & (2d)\\ \boldsymbol{M}_{i\text{-}1}+\boldsymbol{C}_u\vec{\sigma}_{u_i}+\boldsymbol{C}\vec{t}_{\alpha_i}=\boldsymbol{M}_i \text{ for } i=1,...,h & (2e)\\ \vec{\mathbf{1}}^T_{F+H}\sum_{i=1}^{h}\vec{\sigma}_{f_i}\geq 1 & (2f)\end{cases}$$

where $\boldsymbol{M}_i$ is the marking reached after the t_{α_i} fire for i=1,…,h, $\vec{\mathbf{1}}_{F+H}$ is the vector of dimensions F+H with each element being 1 and $\sigma_{f_i}\in\sigma_{u_i}$ for i=1,…,h.

Proof: Let us assume that there exists a fault $f_k\in\Delta_f$ and a sequence $\sigma=\sigma_{u_1}t_{\alpha_1}...\sigma_{u_h}t_{\alpha_h}$ such that $\sigma\in\Sigma_m(\boldsymbol{M}_0,\sigma_o,f_k)$. Denoting the evolution of the net $\boldsymbol{M}_0[\sigma_{u_1}t_{\alpha_1}\rangle\boldsymbol{M}_1...\boldsymbol{M}_{h-1}[\sigma_{u_h}t_{\alpha_h}\rangle\boldsymbol{M}_h$, constraints (2a) and (2b) are obviously verified. Since the PN $PN_u\angle_{T_u}PN$ is acyclic, by Theorem 1 constraints (2c) are verified because they guarantee that there exists a firing sequence σ_{u_i} fireable from $\boldsymbol{M}_{i\text{-}1}$ and such that the firing vector associated to σ_{u_i} is $\vec{\sigma}_{u_i}$. By the hypotheses, at marking $\boldsymbol{M}_{i\text{-}1}$ the subsequence σ_{u_i} enables transition t_{α_i} for i=1,…,h, and (2d) is satisfied. Moreover, if t_{α_i} fires then marking $\boldsymbol{M}_i$ is reached and constraints (2e) are verified. Furthermore, since we assume that $\sigma\in\Sigma_m(\boldsymbol{M}_0,\sigma_o,f_k)$, there exists at least an unobservable subsequence $\sigma_{f_i}\in\sigma$ such that $|\sigma_{f_i}|\geq 1$. Consequently, constraint (2f) is verified. Hence, the ILPP 1 admits at least a solution and selects the firing vectors $\vec{\sigma}_{u_1}$, …, $\vec{\sigma}_{u_h}$ minimizing $\varphi(\vec{\sigma}_{u_1},\vec{\sigma}_{u_2},...,\vec{\sigma}_{u_h})$. □

Remark 1: By Proposition 1, if the ILPP 1 does not admit any solution then we can infer that no fault has occurred at $\boldsymbol{M}_0$ during the observed word $w\in T^*_o$.

Proposition 2: Let us consider a DES with language L and a PN system $\langle PN,\boldsymbol{M}_0\rangle$ modelling the DES and satisfying A1-A4. Given an observation $w\in L$ denoted by $w=\sigma_o=t_{\alpha_1}t_{\alpha_2}...t_{\alpha_h}$, the fault $f_\theta\in\Delta_f$ is contained in a fireable sequence consistent with the observation iff there exists a sequence of firing vectors $\vec{\sigma}_{u_1},...,\vec{\sigma}_{u_i},...,\vec{\sigma}_{u_h}$ that is a solution of the following ILPP 2.

$$\textit{ILPP 2: } \min\varphi(\vec{\sigma}_{u_1},\vec{\sigma}_{u_2},...,\vec{\sigma}_{u_h})=\vec{\mathbf{1}}^T_{F+H}\sum_{i=1}^{h}\vec{\sigma}_{u_i}$$

s.t. $\xi_2(w,\boldsymbol{M}_0,\boldsymbol{Post},\boldsymbol{Pre},\tau_\theta)=$

$$=\begin{cases}\boldsymbol{M}_i\in\mathbb{N}^m \text{ for } i=1,...,h & (3a)\\ \vec{\sigma}_{u_i}\in\mathbb{N}^{F+H} \text{ for } i=1,...,h & (3b)\\ \boldsymbol{M}_{i\text{-}1}+\boldsymbol{C}_u\vec{\sigma}_{u_i}\geq 0 \text{ for } i=1,...,h & (3c)\\ \boldsymbol{M}_{i\text{-}1}+\boldsymbol{C}_u\vec{\sigma}_{u_i}\geq \boldsymbol{Pre}\,\vec{t}_{\alpha_i} \text{ for } i=1,...,h & (3d)\\ \boldsymbol{M}_{i\text{-}1}+\boldsymbol{C}_u\vec{\sigma}_{u_i}+\boldsymbol{C}\vec{t}_{\alpha_i}=\boldsymbol{M}_i \text{ for } i=1,...,h & (3e)\\ \sum_{i=1}^{h}\vec{\sigma}_{u_i}(\tau_\theta)\geq 1 & (3f)\end{cases}$$

Proof (Only if:) Assume that fault $f_\theta\in\Delta_f$ may have occurred. Hence, there exists $\sigma\in\Sigma_m(\boldsymbol{M}_0,\sigma_o,f_\theta)$ such that $\sigma=\sigma_{u_1}t_{\alpha_1}...\sigma_{u_h}t_{\alpha_h}$ and $\boldsymbol{M}_0[\sigma_{u_1}t_{\alpha_1}\rangle\boldsymbol{M}_1...\boldsymbol{M}_{h-1}[\sigma_{u_h}t_{\alpha_h}\rangle\boldsymbol{M}_h$, where $|\sigma_{u_i}|\geq 0$ for i=1,…,h and for some $i\in\{1,…,h\}$ it holds

$\tau_\theta \in \sigma_{u_i}$. Constraint (3a) is trivially verified. Moreover, following the proof of Proposition 1, we show that for each σ_{u_i} for i=1,…,h the associated firing vectors $\vec{\sigma}_{u_i}$ satisfy (3b)-(3e). Since $\sigma \in \Sigma_m(\boldsymbol{M_0}, \sigma_o, f_\theta)$, there exists a sequence $\sigma_{u_i} \in \sigma$ such that $\tau_\theta \in \sigma_{u_i}$, i.e., $\vec{\sigma}_{u_i}(\tau_\theta) \geq 1$. Consequently, constraint (3f) is verified. This proves that the ILPP 2 admits a solution and selects the firing vectors $\vec{\sigma}_{u_1}, \ldots, \vec{\sigma}_{u_i}, \ldots, \vec{\sigma}_{u_h}$ minimizing $\varphi(\vec{\sigma}_{u_1}, \vec{\sigma}_{u_2}, \ldots, \vec{\sigma}_{u_h})$.

(*If*): If there exists a solution $\vec{\sigma}_{u_1}$, …, $\vec{\sigma}_{u_h}$ of the ILPP 2, by constraints (3a) - (3e) the sequence $\sigma = \sigma_{u_1} t_{\alpha_1} \ldots \sigma_{u_h} t_{\alpha_h}$ is enabled at $\boldsymbol{M_0}$ and may fire yielding the evolution $\boldsymbol{M}_0[\sigma_{u_1} t_{\alpha_1}\rangle \boldsymbol{M}_1 \ldots \boldsymbol{M}_{h-1}[\sigma_{u_h} t_{\alpha_h}\rangle \boldsymbol{M}_h$. Moreover, constraint (3f) imposes that at least a vector $\vec{\sigma}_{u_i}$ for some $i \in \{1,\ldots,h\}$ is such that $\vec{\sigma}_{u_i}(\tau_\theta) \geq 1$. Hence, it holds $\tau_\theta \in \sigma_{u_i} \in \sigma$. Consequently, fault $f_\theta \in \Delta_f$ may have occurred during the sequence σ_o firing. □

Remark 2: By Proposition 2, iff the ILPP 2 admits a solution $\vec{\sigma}_{u_1}, \ldots, \vec{\sigma}_{u_i}, \ldots, \vec{\sigma}_{u_h}$ and for some $i \in \{1,\ldots,h\}$ $\vec{\sigma}_{u_i}(\tau_\theta) \geq 1$, then there exists a sequence $\sigma = \sigma_{u_1} t_{\alpha_1} \ldots \sigma_{u_h} t_{\alpha_h}$ such that $\sigma \in \Sigma_m(\boldsymbol{M_0}, \sigma_o, f_\theta)$. Consequently, we infer that fault f_θ may have occurred at the occurrence of $w=\sigma_o$ at marking $\boldsymbol{M_0}$. However, even if the ILPP 2 admits a solution, it is possible that there exists a sequence $\sigma \in \Sigma(\boldsymbol{M_0}, \sigma_o)$ where each $\sigma_{u_i} \in \sigma$ is such that $\sigma_{u_i} \in T_{nf}^*$, i.e., each unobservable subsequence does not contain any fault transition. In such a case the behaviour of the system may also be normal. The following proposition allows us to detect such a situation.

Proposition 3: Let us consider a DES with language L and a PN system $\langle PN, \boldsymbol{M_0}\rangle$ modelling the DES and satisfying A1-A4. Given an observation $w \in L$ denoted by $w = \sigma_o = t_{\alpha_1} t_{\alpha_2} \ldots t_{\alpha_h}$, if the following ILPP admits a solution, then the behaviour of the system may be normal.

$$\text{ILPP 3} \min \varphi(\vec{\sigma}_{u_1}, \vec{\sigma}_{u_2}, \ldots, \vec{\sigma}_{u_h}) = \vec{\mathbf{1}}_{F+H}^T \sum_{i=1}^{h} \vec{\sigma}_{u_i}$$

$$\text{s.t. } \xi_3(w, \boldsymbol{M_0}, \boldsymbol{C_u}, \boldsymbol{Pre}) = \begin{cases} \boldsymbol{M}_i \in \mathbb{N}^m \text{ for } i=1,\ldots,h & \text{(4a)} \\ \vec{\sigma}_{u_i} \in \mathbb{N}^{F+H} & \text{(4b)} \\ \boldsymbol{M}_{i-1} + \boldsymbol{C}_u \vec{\sigma}_{u_i} \geq 0 \text{ for } i=1,\ldots,h & \text{(4c)} \\ \boldsymbol{M}_{i-1} + \boldsymbol{C}_u \vec{\sigma}_{u_i} \geq \boldsymbol{Pre}\, \vec{t}_{\alpha_i} \text{ for } i=1,\ldots,h & \text{(4d)} \\ \boldsymbol{M}_{i-1} + \boldsymbol{C}_u \vec{\sigma}_{u_i} + \boldsymbol{C}\vec{t}_{\alpha_i} = \boldsymbol{M}_i \text{ for } i=1,\ldots,h & \text{(4e)} \\ \vec{\mathbf{1}}_{F+H}^T \sum_{i=1}^{h} \vec{\sigma}_{f_i} = 0 & \text{(4f)} \end{cases}$$

where $\sigma_{f_i} \in \sigma_{u_i}$ for i=1,…,h.

Proof Let us assume that there exist h vectors $\vec{\sigma}_{u_1}, \vec{\sigma}_{u_2}, \ldots, \vec{\sigma}_{u_h}$ solution of the ILPP3. By constraints (4a) - (4e) there exists a sequence $\sigma = \sigma_{u_1} t_{\alpha_1} \ldots \sigma_{u_h} t_{\alpha_h}$ such that $\boldsymbol{M}_0[\sigma_{u_1} t_{\alpha_1}\rangle \boldsymbol{M}_1 \ldots \boldsymbol{M}_{h-1}[\sigma_{u_h} t_{\alpha_h}\rangle \boldsymbol{M}_h$. Since constraint (4f) imposes that $\vec{\sigma}_{f_i}=0$ for i=1,…,h, it holds $\sigma \in \Sigma(\boldsymbol{M_0}, \sigma_o)$ and σ does not contain fault transitions. Hence, the system behaviour during the occurrence of w at $\boldsymbol{M_0}$ may be normal. □

The algorithm shown in Fig. 2 and described in the following allows us to specify on-line the *diagnoser* function Φ.

The inputs of the diagnoser are the initial marking $\boldsymbol{M_0}$, the PN structure and the DES observed word w. Assuming that $|w|=h$, by the labelling function λ we obtain $w=\lambda(\sigma)$ and $\sigma_o = t_{\alpha_1} t_{\alpha_2} \ldots t_{\alpha_h} = w \in \sigma$ with $t_{\alpha_i} \in T_o$ for i=1,…,h. The algorithm defines the ILPP1: if the ILPP1 admits no solution then by Proposition 1 it is inferred $\Phi(\boldsymbol{M}_0,w)=N$ (step 4) and the algorithm goes to step 7. If the ILPP1 admits a solution, Step 5 defines an ILPP 2 for each $f_\theta \in \Delta_f$: if the ILPP 2 admits a solution $\vec{\sigma}$ for f_θ, then by Proposition 2 and Remark 2, it holds that $\vec{\sigma} \in Y_m(\boldsymbol{M_0}, \sigma_o, f_\theta)$ and the algorithm sets $\Phi(\boldsymbol{M}_0,w) = \Phi(\boldsymbol{M}_0,w) \cup \{(f_\theta, \vec{\sigma})\}$. Finally, the algorithm has to check whether $\Sigma(\boldsymbol{M_0}, \sigma_o)$ may contain a sequence of silent but not faulty transitions. Hence the ILPP3 is defined (Step 6). By Proposition 3, if the ILPP 3 admits a solution then the algorithm sets $\Phi(\boldsymbol{M}_0,w) = \Phi(\boldsymbol{M}_0,w) \cup \{N\}$, i.e., the behaviour may either be normal or may correspond to a fault.

Algorithm

1. Input: $\boldsymbol{M_0} \in \mathbb{N}^m$, $PN=(P, T, \boldsymbol{Pre}, \boldsymbol{Post})$, λ, T_o, T_u, T_f, T_{nf}
   Output: Φ
2. *Initializing the algorithm variables.*
   $w=\varepsilon$, , h=0, $\vec{\sigma}_o \in \mathbb{N}^O$, $\vec{\sigma}_o = \vec{\mathbf{0}}$
3. *Recording the events.*
   Wait until a new event *e* is observed.
   $e =: \lambda(t)$; $w=wt$; $h=h+1$, $\Phi(\boldsymbol{M}_0,w)=\varnothing$, $\vec{\sigma}_o(t) = \vec{\sigma}_o(t)+1$;
4. *Solving the ILPP 1*
   Solve $\min \varphi(\vec{\sigma}_{u_1}, \vec{\sigma}_{u_2}, \ldots, \vec{\sigma}_{u_h})$ s.t. $\xi_1(w, \boldsymbol{M_0}, \boldsymbol{Post}, \boldsymbol{Pre})$
   If the ILPP 1 admits no solution then set $\Phi(\boldsymbol{M}_0,w)=N$ **and goto 7**
5. *Solving the ILPP 2*
   for θ=1 **to** F
   Solve min $\varphi(\vec{\sigma}_{u_1}, \vec{\sigma}_{u_2}, \ldots, \vec{\sigma}_{u_h})$ s.t. $\xi_2(w, \boldsymbol{M_0}, \boldsymbol{Post}, \boldsymbol{Pre}, \tau_\theta)$
   If the ILPP 2 admits a solution $\vec{\sigma}_{u_1}, \vec{\sigma}_{u_2}, \ldots, \vec{\sigma}_{u_h}$ **then set**
   $\vec{\sigma}_u = \sum_{i=1}^{h} \vec{\sigma}_{u_i}$, $\vec{\sigma} = \begin{bmatrix} \vec{\sigma}_o \\ \vec{\sigma}_u \end{bmatrix}$, $\Phi(\boldsymbol{M}_0,w) = \Phi(\boldsymbol{M}_0,w) \cup \{(f_\theta, \vec{\sigma})\}$
   end for
6. *Solving the ILPP 3.*
   Solve min $\varphi(\vec{\sigma}_{u_1}, \vec{\sigma}_{u_2}, \ldots, \vec{\sigma}_{u_h})$ s.t. $\xi_3(w, \boldsymbol{M_0}, \boldsymbol{Post}, \boldsymbol{Pre})$
   If the ILPP 3 admits a solution then set $\Phi(\boldsymbol{M}_0,w) = \Phi(\boldsymbol{M}_0,w) \cup \{N\}$**.**
7. *Returning to the condition of recording the events.*
   goto 3.

Fig. 2 The algorithm specifying the diagnoser function.

The ILPP solved by the algorithm are at most F+2 in number. Hence, if the number of fault transitions is not very large, then the algorithm can be applied in real time. Moreover, to evaluate the computational complexity of the optimization problems, we recall that the primary determinants of the computational difficulty of an ILPP are the number of integer variables. It is easy to infer that in the worst case the unknowns of each ILPP are $h(m+F+H)$ in number. However, in the examined cases an optimal solution is obtained in a short time implementing and solving the ILP problems on a PC equipped with a standard solver of optimization problems, e.g. Gnu Linear Programming Kit (GLPK, see http://www.gnu.org/software/glpk/glpk.html).

5. AN EXAMPLE

This section presents an example that shows how the diagnoser and the proposed algorithm work and how the resulting diagnoser is able to characterize the system behaviour.

Example 2: Let us consider the net in Fig. 1 and described in Example 1. Let us observe the word $w=t_1t_2t_3t_1t_3$ at the initial marking $\boldsymbol{M}_0=[1\ 1\ 0\ 0\ 0\ 0\ 0]^T$. The algorithm in Fig. 2 provides the following results:

$$\Phi(\boldsymbol{M}_0,t_1)=\{(f_1,\vec{\sigma}=[1\ \ 0\ \ 0\ \ |\ \ 1\ \ 0\ \ 0\ \ 0]^T),N\},$$

$$\Phi(\boldsymbol{M}_0,t_1t_2)=N,\ \Phi(\boldsymbol{M}_0,t_1t_2t_3)=N,$$

$$\Phi(\boldsymbol{M}_0,t_1t_2t_3t_1)=\{(f_1,\vec{\sigma}=[2\ \ 1\ \ 1\ \ |\ \ 1\ \ 0\ \ 1\ \ 1]^T),N\},$$

$$\Phi(\boldsymbol{M}_0,t_1t_2t_3t_1t_3)=\{(f_1,\vec{\sigma}=[2\ \ 1\ \ 2\ \ |\ \ 1\ \ 1\ \ 1\ \ 1]^T),$$

$$(f_2,\vec{\sigma}=[2\ \ 1\ \ 2\ \ |\ \ 1\ \ 1\ \ 1\ \ 1]^T)\}$$

Hence, the diagnoser provides an ambiguous solution after the observation of $w=t_1$ because either fault f_1 may have occurred or the system behaviour may be normal. On the other hand, when $w=t_1t_2$ and $w=t_1t_2t_3$, the ambiguity is solved because in the two cases there exists no firing sequence containing a transition $\tau_k\in T_f$ and consistent with the observation. An uncertain situation is detected after word $w=t_1t_2t_3t_1$ because either fault f_1 may have occurred or the system behaviour may be normal. However, when $w=t_1t_2t_3t_1t_3$ is observed the diagnoser decides that the two faults f_1 and f_2 have occurred because the two provided minimal interpretations contain both τ_1 and τ_2. For example, the sequence $\sigma=t_1\tau_3t_2t_3\tau_4\tau_1t_1\tau_2t_3$ may have occurred.

Note that decisions after each event are taken by the diagnoser in 0.074 seconds in the worst case using a PC with a 1.73 GHz processor, 1 GB RAM and the GLPK solver.

6. CONCLUSIONS

The paper discusses the fault detection problem of Discrete Event Dynamical Systems (DES) proposing a diagnoser specified in real time by a procedure that is based on a Petri Net (PN) model of the system. The on-line procedure stores the observed sequence of DES events and the corresponding observable PN markings and decides whether the system behaviour is normal or some faults may have occurred. To this aim, some integer linear programming problems are defined by an algorithm that provides, at each observed event, the possible occurred faults or detects the system normal behaviour. We remark that integer linear programming is an accepted methodology to solve problems in discrete event systems. However, the computational complexity of the proposed identification algorithm increases with the number of places, of the silent transitions and of the observed transitions of the PN model. Hence, our future efforts will be devoted to use appropriate heuristics and methodologies to overcome such a drawback.

REFERENCES

Benveniste, A., E. Fabre, S. Haar and C. Jard (2003). Diagnosis of asynchronous discrete event systems: a net unfolding approach. *IEEE Trans. Automatic Control*, vol. 48, pp.714-727.

Cassandras, C. G. and S. Lafortune (1999). *An Introduction to Discrete Event Systems*, Kluwer, Boston, MA.

Corona D., A. Giua and C. Seatzu (2004). Marking estimation of Petri nets with silent transitions. *Proc. 43th IEEE. Conf. on Decision and Control and 2004 European Control Conf.*, Atlantis, The Bahamas.

Giua A. and C. Seatzu (2005). Fault detection for discrete event systems using Petri nets with unobservable transitions. *Proc. 44th IEEE. Conf. on Decision and Control and 2005 European Control Conf.*, Seville, Spain, pp. 6326-6328.

Hadjicostis, C. N. and G. C. Verghese (1999). Monitoring discrete event systems using Petri nets embeddings. *Proc. Application Theory Petri Nets*, pp.188-208.

Lunze, J. and J. Schroder (2004). Sensor and actuator fault diagnosis of systems with discrete inputs and outputs. *IEEE Trans. Systems, Man and Cybernetics, Part B*, vol. 34, pp. 1096-1107.

Peterson, J.L. (1981). *Petri Net Theory and the Modeling of Systems*. Prentice Hall, Englewood Cliffs, NJ, USA.

Prock, J. (1991). A new technique for fault detection using Petri nets. *Automatica*, vol. 27, pp. 239-245, 1991.

Ramirez-Trevino, A. E. Ruiz-Beltràn, I.Rivera-Rangel and E. Lopez-Mellado (2007). Online fault diagnosis of Discrete Event Systems. A Petri Net-Based Approach. *IEEE Trans. on Automation Science and Engineering*, vol. 4, no. 1, pp. 31-39.

Sahraoui, A., H. Atabakhche, M. Courvoisier and R. Valette (1987). Joining Petri nets and knowledge-based systems for monitoring purposes. in *Proc. IEEE Int. Conf. Robotics Automation*, pp. 1160–1165.

Sampath, M., R. Sengupta, S. Lafortune, K. Sinnamohideen and D. Teneketzis (1995). Diagnosability of discrete-event systems. *IEEE Trans. Automatic Control*, vol. 40, pp. 1555-1575.

Sampath, M., S. Lafortune and D. Teneketzis (1998). Active diagnosis of discrete-event systems. *IEEE Trans. Automatic Control*, vol. 43, pp. 908-929.

Ushio, U., L. Onishi and K. Okuda (1998). Fault detection based on Petri net models with faulty behaviours. *Proc. SMC'98, IEEE Int. Conf. on Systems, Man, and Cybernetics*, San Diego, CA, USA, pp. 113-118.