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

1. INTRODUCTION

Faults are physical conditions that cause a device or a component to fail to perform in a required manner (e.g., a short-circuit, an intermittent connection, a valve stuck-closed, etc.). Fault analysis consists in
monitoring the system behaviour, determining the occurrence of any fault and identifying its type or origin.

Automatic fault detection and diagnosis is a research area that received a lot of attention in the last years not only within the framework of time-driven systems, but also in the case of Discrete Event Systems (DES). In the related literature the fault detection and diagnosis of DES is addressed by several model-based approaches in which the diagnosis is based on the specification of the system dynamics (f.e., Lefebvre and Delherm 2007, Sampath et al. 1995, Hashtrudi Zad et al. 2003). These papers are all based on the use of automata models and lead to the construction of a diagnoser automaton. More precisely, the diagnoser is built from the system model and is used to perform on-line the monitoring of the DES for fault diagnosis purposes. Moreover, diagnosers can also be used to analyze the diagnosability properties of the system, i.e., to check whether it is possible to detect, observing a word of finite length, the occurrences of the unobservable events associated to faults.

Although automata models are suitable for describing DES, the use of Petri Nets (PN) offers significant advantages because of their twofold representation: graphical and mathematical. Moreover, recent research focuses on overcoming the main drawback of the automata approaches: avoiding the enumeration of the system states and the consequent state explosion.

Among the pioneering works dealing with PN for fault detection, we recall the approach of Srinivasan and Jafari (1993) that employ time PN to model the DES controller and backfiring transitions to determine whether a given state is invalid. Later on, time PN have been employed by Ghazel et al. (2005) to propose a monitoring approach for DES with unobservable events and to represent the a priori known behaviour of the system and track on-line its state to identify the events that occur. Moreover, using time constraints, Dotoli et al. (2008b) present a novel event-based approach for DES on-line monitoring, ensuring timely and accurate detection of system failures and avoiding the state enumeration. Timed Petri nets with guarded transitions and timing analysis are used in (Jiroveanu and Boel 2006) that propose an algorithm for fault detection and diagnosis suitable to large systems.

An alternative approach to avoid complexity is proposed by Hadjicostis and Veghese (1999) that use PN models to introduce redundancy into the system and additional P-invariants to detect and isolate faulty markings. Prock (1991) proposes an on-line technique for fault detection that is based on monitoring the number of tokens residing into P-invariants: when the number of tokens inside P-invariants changes, then the error is detected.

In some approaches that use PN for fault detection, the system state is assumed partially observable. In particular, Wu and Hadjicostis (2005) use redundancy to enable fault detection and identification by algebraic decoding techniques. They consider two types of faults: place faults that corrupt the net marking and transition faults that cause an incorrect update of the marking after an event occurrence. Although this
approach is general, the net marking has to be periodically observable even if unobservable events occur. Analogously, Lefebvre and Delherm (2007) investigate the determination of the set of places that must be observed for the exact and immediate estimation of fault occurrences. Ramirez-Trevino et al. (2007) employ interpreted PN to model the system behaviour that includes both events and states that are partially observable. Based on the interpreted PN model derived from an on-line methodology, a scheme utilizing a solution of a programming problem is proposed for on-line diagnosis.

Several recently presented papers are based on the assumption that no places are observable. Among these papers we consider compiled and interpreted diagnosers (Benveniste et al. 2003). In the compiled diagnosers the diagnoser construction can be performed off-line (Genc and Lafortune 2003, Genc and Lafortune 2007, Giua and Seatzu 2005, Cabasino et al. 2007 and Jiroveanu et al. 2008), while in the interpreted diagnosers, the diagnoser computes on-line the faults or the fault states (Benveniste et al. 2003, Basile et al. 2008). In particular, Genc and Lafortune (2003) extend, in the context of PN models, the diagnoser approach originally proposed in (Sampath et al. 1995). The diagnoser has the same graphical structure as the PN modelling the DES and finds all the states that are consistent with the sequence of observable events. Even if the diagnoser is used for on-line fault detection, we remark that it is built off-line by enumerating at each observation all the states the DES can be in and by associating to each state the fault information. Hence, the state explosion is not avoided when the diagnoser is applied in a centralized way. An improvement is obtained in Genc and Lafortune (2007) where the system is modelled as a collection of PN modules coupled through common places and the diagnosis is based on a modular approach that performs the on-line distributed diagnosis of faults in each module. The diagnosis approach by Giua and Seatzu (2005) avoids an exhaustive enumeration of the DES states by introducing the notion of basis markings and justifications that allow characterizing the set of markings that are consistent with the actual observation, and the set of unobservable transitions whose firing enables it. A similar approach is proposed in (Jiroveanu et al. 2008), where the diagnoser is based on a backward analysis on the net structure. The improvement with respect to the method of Giua and Seatzu (2005) is that the approach of Jiroveanu et al. (2008) can be applied to a larger class of PN describing the unobservable behaviour of the system. The main advantage of compiled diagnosers is that they can be built off-line. Nevertheless, even if an exhaustive enumeration of the states in some cases can be avoided, a large memory may be required.

An improvement in this respect is given by the interpreted diagnosers of Benveniste et al. (2003) and Basile et al. (2008). In particular, Benveniste et al. (2003) use a net unfolding approach for designing an on-line asynchronous diagnoser. The state explosion is avoided but the on-line computational effort can be high due to the on-line construction of the PN structures by means of the unfolding. In Basile et al. (2008) the diagnoser is built on-line by defining and solving some Integer Linear Programming (ILP)
problems that detect the fault occurrences. Moreover, an off-line analysis of the PN structure reduces the computational effort of the ILP problem but requires the redesign and the redefinition of the diagnoser when the system structure changes.

In order to avoid the redesign and the redefinition of the diagnoser when the structure of the system varies, this paper proposes an on-line fault detection strategy in a PN framework. More precisely, assuming that the structure of the PN model and the initial marking are known, faults are modelled by unobservable transitions and additional unobservable transitions may be associated with the system legal behaviour. The diagnoser 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 ILP problems are defined and provide eventually a sequence of unobservable transitions containing the faults that may have occurred. The proposed fault detection technique is general since no assumption is imposed on the reachable state set that can be unlimited, and only few properties must be fulfilled by the structure of the PN modelling the system fault behaviour. Even if ILP is a standard mathematical tool and an accepted methodology to solve problems in DES modelled by PN (e.g., we recall the contributions by Dotoli et al. 2008a, Basile et al. 2008, Cabasino et al. 2007), no polynomial algorithm for it is known to exist, so the on-line computational effort of the proposed algorithm can be high. To overcome this drawback, we provide some results showing that if the unobservable subnet enjoys suitable properties, the algorithm solution may be obtained with low computational complexity because each basic solution of the Linear Programming (LP) relaxation of the defined ILP problems is an integer-valued solution.

Comparing the proposed approach with the interpreted diagnosis techniques of Benveniste et al. (2003) and Basile et al. (2008), the computational complexity of our diagnosis algorithm is still a concern if we wish to provide a reasonably efficient method suitable for on-line use with large systems. However, our algorithm does not require off-line calculations based on the structure of the considered PN system. In this way, the approach turns out to be more easily applicable than the two mentioned techniques to situations in which the system structure may change.

The remainder of the paper is structured as follows. Section 2 provides basic definitions and notations that are needed in the paper. Section 3 defines the fault detection problem and characterizes the diagnoser. Moreover, Section 4 specifies the on-line fault detection algorithm and shows that in some cases the proposed algorithm enables an efficient solution (the related proofs are reported in the Appendix). Finally, Section 5 draws the conclusions.

2. BASIC DEFINITIONS AND NOTATIONS

This section recalls some basic definitions on PN (Peterson, 1981).
Definition 1: A PN is a bipartite graph described by the four-tuple \( PN=(P, T, \text{Pre}, \text{Post}) \), where \( P \) is a set of places with cardinality \( m \), \( T \) is a set of transitions with cardinality \( n \), \( \text{Pre} : P \times T \to \mathbb{N} \) and \( \text{Post} : P \times T \to \mathbb{N} \) 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 \( \text{Pre}(p,t) \) (\( \text{Post}(p,t) \)) 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 \( C=\text{Post}-\text{Pre} \) is the \( m \times n \) incidence matrix of the net \( PN \).

For the pre- and post-sets we use the dot notation, e.g., \( \bullet t=\{p \in P : \text{Pre}(p,t)>0\} \).

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

A transition \( t_j \in T \) is enabled at a marking \( M \) if and only if (iff) for each \( p \in \bullet t_j \), it holds:

\[
M(p) \geq \text{Pre}(p,t_j)
\]  

and we write \( M[t_j] \) to denote that \( t_j \in T \) is enabled at marking \( M \). When fired, \( t_j \) produces a new marking \( M' \), denoted by \( M[t_j]M' \) that is computed by the PN state equation:

\[
M'=M+C \; \bar{i}_j,
\]  

where \( \bar{i}_j \) is the \( n \)-dimensional firing vector corresponding to the \( j \)-th canonical basis vector.

Let \( \sigma=t_{h_1}t_{h_2}...t_{h_k} \) be a sequence of transitions (or firing sequence) and let \( k=|\sigma| \) be its length, given by the number of transitions that \( \sigma \) contains. If a transition \( t \in T \) appears in the sequence \( \sigma \), we write \( t \in \sigma \). Moreover, the notation \( M[\sigma] \) indicates that the sequence \( \sigma \) is enabled at \( M \) and \( M[\sigma]M' \) indicates that the enabled sequence \( \sigma \) may fire at \( M \) yielding \( M' \). We also denote \( \vec{\sigma} : T \to \mathbb{N}^n \) the firing vector associated with a sequence \( \sigma \), i.e., \( \vec{\sigma}(t)=q \) if transition \( t \) is contained \( q \) times in \( \sigma \). A marking \( M \) is said reachable from \( \langle PN,M_0 \rangle \) iff there exists a firing sequence \( \sigma \) such that \( M_0[\sigma]M \). The set of all markings reachable from \( M_0 \) defines the reachability set of \( \langle PN,M_0 \rangle \) and is denoted by \( R(PN,M_0)=\{M \exists \ \sigma : M_0[\sigma]M \} \).
**Definition 2:** A PN system \( \langle PN, M_0 \rangle \) is said **bounded** if there exists \( k \in \mathbb{R} \) such that the number of tokens in each place does not exceed the finite number \( k \) for any marking reachable from \( M_0 \), i.e., \( M(p) \leq k \) for each \( p \in P \) and for each \( M \in R(PN, M_0) \).

**Definition 3:** A net is said **backward conflict-free** if for each \( t_i, t_j \in T \) with \( t_i \neq t_j \) it holds \( t_i \bullet \cap t_j \bullet = \emptyset \), i.e., all transitions have no output common place.

**Definition 4:** A net \( PN=\langle P, T, \text{Pre}, \text{Post} \rangle \) is said a **State Machine** (SM) if for each \( t \in T \) it holds \( \text{Card}(\bullet t) = \text{Card}(t \bullet) = 1 \), i.e., for each transition \( t \in T \) there exists only one arc going from \( t \) and only one arc going to \( t \). Note that the symbol \( \text{Card}(.) \) stands for “Cardinality of the set (.).”

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 \( y \) satisfies equation \( M_0 + Cy \geq 0 \), there exists a firing sequence \( \sigma \) fireable from \( M_0 \) and such that the firing vector associated to \( \sigma \) is \( y \).

(ii) A marking \( M \) is reachable from \( M_0 \) iff there exists a non negative integer solution \( y \) satisfying the state equation \( M = M_0 + Cy \).

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 \( PN=\langle P, T, \text{Pre}, \text{Post} \rangle \) is used to model the DES, the system events are associated with transitions.

**Definition 5:** Given a PN, the function \( \lambda: T \rightarrow E \cup \{ \varepsilon \} \) is the transition labelling function that assigns to each transition \( t \in T \) either a symbol \( e_i \in E \) or the empty string \( \varepsilon \).

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 \( \lambda \) 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 6: Given a net $PN=(P, T, Pre, Post)$ and a subset $T_\Lambda \subseteq T$ of its transitions, we define the $T_\Lambda$-induced subnet of $PN$ as the new net $PN_\Lambda=(P, T_\Lambda, Pre_\Lambda, Post_\Lambda)$ where $Pre_\Lambda$ and $Post_\Lambda$ are the restrictions of $Pre$ and $Post$ to $T_\Lambda$. In other words, the net $PN_\Lambda$ is obtained from $PN$ removing all transitions in $T\setminus T_\Lambda$. We also write $PN_\Lambda \triangleleft T_\Lambda \angle PN$.

In the following we consider the subnet $PN_u \triangleleft T_u \angle PN$ and we denote by $C_u=Post_u-Pre_u$ the restriction of the incidence matrix $C=Post-Pre$ to $T_u$.

3. THE FAULT DETECTION PROBLEM

3.1 Description of the DES Fault Behaviour

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

Let $\Delta_f=\{f_1, \ldots, f_F\}$ 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 $T_f=\{\tau_1, \tau_2, \ldots, \tau_F\} \subseteq T_u$, since an observable fault transition is trivially diagnosed. Consequently, denoting by $T_{nf}=\{\tau_{F+1}, \tau_{F+2}, \ldots, \tau_{F+K}\} \subseteq T_u$ the set of $K$ 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 $i\in \{1, \ldots, F\}$ occurs when the corresponding fault transition $\tau_i\in T_f$ fires. Obviously, the observable transitions are $n-K-F=O$ in number. We note that in this work we do not consider the time-varying faults, such as the so-called evolving faults, i.e., faults having one character initially and changing to a different state subsequently, which can occur in power systems, as well as in some computing and electronic systems (Shanthi and Parthasarathi 2003).

We denote as $w$ the word of events associated with the sequence $\sigma\in T^*$ with $w=\lambda(\sigma)$, using the extended form of the transition labelling function $\lambda: T^* \rightarrow E^*$ in the usual manner, i.e., if $\sigma=t_{b_1}t_{b_2}\ldots t_{b_k}$ then it holds $\lambda(\sigma)=\lambda(t_{b_1})\lambda(t_{b_2})\ldots\lambda(t_{b_k})$. Note that the length of a sequence $\sigma$ is greater than or equal to the corresponding word $w$ (i.e., $|\sigma|\geq|w|$). In fact, if $\sigma$ contains $q$ transitions labelled by $\varepsilon$, then $|\sigma|=q+|w|$. In addition, we denote by $\sigma_o\in \sigma$ ($\sigma_o\in \sigma$) the subsequence of $\sigma$ composed by the unobservable (observable) transitions and by $\overline{\sigma}_o: T_o \rightarrow \mathbb{N}^{K+F}$ ($\overline{\sigma}_o: T_o \rightarrow \mathbb{N}^O$) the corresponding firing vector. Analogously, we denote by $\overline{\sigma}_f (\overline{\sigma}_{nf}) \in \sigma_o$ the subsequence of $\sigma_o$ composed by the fault (no fault) transitions and by $\overline{\sigma}_f (\overline{\sigma}_{nf})$ the corresponding firing vectors. By the assumption $E=T_o$, it holds $\sigma_o=w$. Note that in the sequel
we denote the firing vector \( \tilde{\sigma} = \begin{bmatrix} \sigma_o \\ \sigma_u \end{bmatrix} \).

The following definitions are introduced for the diagnoser specification.

**Definition 7.** Given the initial marking \( M_0 \in \mathbb{N}^n \) and a sequence \( \sigma_o \) of observable transitions such that \( M_0[\sigma_o] \), we define \( \Sigma(M_0, \sigma_o) = \{ \sigma \in T^* \mid M_0[\sigma] \text{ and } \sigma_o \in \sigma \} \) the set of interpretations of \( \sigma_o \) at \( M_0 \).

In other words, \( \Sigma(M_0, \sigma_o) \) is the set of sequences containing the observable sequence \( \sigma_o \) and the unobservable sequences whose firing at \( M_0 \) is consistent with \( \sigma_o \).

**Definition 8.** Given the initial marking \( M_0 \in \mathbb{N}^n \) and an observable sequence \( \sigma_o \), we define the set of interpretations of \( \sigma_o \) at \( M_0 \) containing fault \( f_k \) as: \( \Sigma(M_0, \sigma_o, f_k) = \{ \sigma \in \Sigma(M_0, \sigma_o) \mid \tau_k \in \sigma \} \).

### 3.2 Main Assumptions and Diagnoser Definition

In this paper we deal with the problem of specifying a diagnoser that detects at each observed DES event whether the system behaviour is normal or a fault may have occurred.

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

A1) a net \( PN=(P, T, Pre, Post) \) modelling the DES and the initial marking \( M_0 \) are known;

A2) the labels associated to the firing of transitions in \( T_o = E \) can be observed;

A3) the subnet \( PN_u \angle_{\tau^+_u} PN \) is acyclic.

In particular, A1 and A2 are assumptions that exhibit the level of the system knowledge. Moreover, assumption A3 leads to a hypothesis commonly adopted in the field of fault detection: cycles of non-observable events are not admissible (Sampath et al. 1995).

The inputs of the diagnoser are the initial marking \( M_0 \) and the observed word \( w \in L \), where \( L \) is the language of the DES. Assuming that \( w = \lambda(\sigma) \), the sequence \( \sigma = \sigma_{u_1} t_{\alpha_1} \sigma_{u_2} t_{\alpha_2} \ldots \sigma_{u_h} t_{\alpha_h} \) with \( h \geq 1 \) denotes the sequence of observable and unobservable transitions corresponding to the word \( w \). More precisely, \( \sigma_o = t_{\alpha_1} t_{\alpha_2} \ldots t_{\alpha_h} = w \) with \( t_{\alpha_i} \in T_o \) for \( i = 1, \ldots, h \) is the observable subsequence of \( \sigma \) and each \( \sigma_{u_i} \in T_u^* \) is the sequence of unobservable transitions that have occurred before transition \( t_{\alpha_i} \) for \( i = 1, \ldots, h \) and after transition \( t_{\alpha_{i-1}} \) for \( i = 2, \ldots, h \).
Definition 9: A **diagnoser** is a function $\Phi : \mathbb{N}^m \times T_o^* \rightarrow \Delta \cup \{N\}$ that associates to each initial marking $M_0 \in \mathbb{N}^m$ and to each observation $w \in T_o^*$ the following sets:

- $\Phi(M_0, w) = \{N\}$ if $\forall f_k \in \Delta_f$ it holds $\Sigma(M_0, \sigma_o, f_k) = \emptyset$;
- $\Phi(M_0, w) = \{f_k \in \Delta_f | \Sigma(M_0, \sigma_o, f_k) \neq \emptyset \}$ with $\sigma_o = w$;
- $\Phi(M_0, w) = \emptyset$.

i.e., 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;

i.e., the behaviour of the system is **faulty** during the observed word $w$. In such a case the diagnoser provides the possible faults $f_k \in \Delta_f$ that may be contained in a sequence consistent with the observation;

- $\Phi(M_0, w) = \emptyset$.

i.e., the behaviour of the system is **ambiguous**, because two cases are possible: i) fault $f_k \in \Delta_f$ may have occurred during the observed word $w$, ii) the behaviour of the system may be normal.

Definition 10: The diagnosis of a PN system $\langle PN, M_0 \rangle$ is said **unambiguous** if $\forall w \in T_o^*$ there exists a diagnoser $\Phi$ that verifies one of the following two mutually exclusive conditions:

1) $\Phi(M_0, w) = \{N\}$;
2) for each $f_k \in \Phi(M_0, w)$ and for each $\sigma \in \Sigma(M_0, \sigma_o)$ it holds $\sigma \in \Sigma(M_0, \sigma_o, f_k)$.

In other words, the diagnosis of a PN system $\langle PN, M_0 \rangle$ is unambiguous 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 fireable 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 $t_1$ and $\tau_2$, respectively. Let us also assume that the system is in the initial marking $M_0 = [1 \ 1 \ 0 \ 0 \ 0 \ 0]^T$ and word $w=t_1$ is observed. Hence, while transition $t_1$ may have fired before $t_1$, $\tau_2$ may not have fired before $t_1$ (see Fig. 1). We infer $(\tau_1t_1) \in \Sigma(M_0, t_1, f_1)$ and $\Sigma(M_0, t_1, f_2) = \emptyset$, i.e., fault $f_1$ ($f_2$) is (not) consistent with the observation. Hence, $\Phi(M_0, t_1) = \{f_1, N\}$ is obtained by the diagnoser, i.e., fault $f_1$ may have occurred but the DES behaviour may also be normal.

Now, assume that at marking $M_0$ word $w=t_1t_2$ is observed. With reference to Fig. 1, we deduce that, in order for $t_2$ to fire, $\tau_3$ must have fired, so that $t_1$ cannot have fired. On the other hand, the firing of $t_2$
excludes the possibility that $\tau_2$ has fired. Hence, we infer $\Sigma(M_0, t_1, t_2, f_k) = \emptyset$ for $k=1,2$. Therefore, the diagnoser provides $\Phi(M_0, (t_1, t_2)) = \{N\}$, i.e., neither fault $f_1$ nor $f_2$ have occurred during the observed sequence and the behaviour is normal.

Fig. 1. The PN of Example 1.

4. THE ON-LINE DIAGNOSER SPECIFICATION

4.1 Main Results

Given a DES with language $L$ and a PN system $\langle PN, M_0 \rangle$ modelling the DES and satisfying A1-A3, this section proposes a procedure that specifies a diagnoser $\Phi$ that works on-line. More precisely the following propositions allow us to specify the diagnoser and to characterize the behaviour of the system as normal, faulty or ambiguous. In particular, for each initial marking $M_0 \in \mathbb{N}^m$, at the occurrence of an observed word $w \in L$, Proposition 1 provides a linear algebraic characterization of each sequence $\sigma \in T^*$ whose firing at $M_0$ is consistent with the observed sequence $\sigma_o = w$.

Proposition 1: Consider a DES with language $L$ and a PN system $\langle PN, M_0 \rangle$ modelling the DES and satisfying A1-A3. Given a word $w \in L$ denoted by $w = \sigma_0 = t_{\alpha_1} t_{\alpha_2} ... t_{\alpha_h}$, a sequence $\sigma = \sigma_{u_1} t_{\alpha_1} ... \sigma_{u_h} t_{\alpha_h}$ with $|\sigma_{u_i}| \geq 0$ for $i=1, ..., h$ is such that $\sigma \in \Sigma(M_0, \sigma_o)$ iff there exist $h$ firing vectors $\bar{\sigma}_{u_1}, ..., \bar{\sigma}_{u_i}, ..., \bar{\sigma}_{u_h}$ that satisfy the following set of linear constraints:

$$\zeta(w, M_0, Post, Pre) = \begin{cases} 
    \bar{\sigma}_{u_i} \in \mathbb{N}^{F+K}, & \text{for } i=1, ..., h \\
    C_u \sum_{i=1}^{k} \bar{\sigma}_{u_i} \geq Pre t_{\alpha_k} - M_0 - C \sum_{i=1}^{k-1} t_{\alpha_i} & \text{for } k=1, ..., h.
\end{cases}$$

Proof:
(Only if) Assume that \( \sigma \in \Sigma(M_0, \sigma_0) \) such that \( \sigma = \sigma_{u_1} t_{\alpha_1} \cdots \sigma_{u_h} t_{\alpha_h} \) and \( M_0[\sigma_{u_1} t_{\alpha_1}] M_1 \cdots M_{h-1}[\sigma_{u_h} t_{\alpha_h}] M_h \), where \( M_i \) is the marking reached after transition \( t_{\alpha_i} \) fires for \( i = 1, \ldots, h \). The corresponding firing vectors \( \bar{\sigma}_{u_1}, \ldots, \bar{\sigma}_{u_i}, \ldots, \bar{\sigma}_{u_h} \) trivially verify constraints (3a).

By the enabling condition (1) we infer:
\[
M_{i-1} + C_{u} \bar{\sigma}_{u_i} \geq \text{Pre} \bar{t}_{\alpha_i} \quad \text{for } i = 1, \ldots, h .
\] (4)

Moreover, by the state equation (2), the firing vectors \( \bar{\sigma}_{u_1}, \ldots, \bar{\sigma}_{u_i}, \ldots, \bar{\sigma}_{u_h} \) satisfy the constraints:
\[
M_{i-1} + C_{u} \bar{\sigma}_{u_i} + \bar{C} \bar{t}_{\alpha_i} = M_i \quad \text{for } i = 1, \ldots, h .
\] (5)

By writing (4) and (5) for each \( i = 1, \ldots, h \) and recursively eliminating all the intermediate markings \( M_i \) for \( i = 1, \ldots, h \) from the obtained equations, it is easy to show that it holds
\[ C_{u} \sum_{i=1}^{k} \bar{\sigma}_{u_i} \geq \text{Pre} \bar{t}_{\alpha_k} - M_0 - C \sum_{i=1}^{k-1} \bar{t}_{\alpha_i} \quad \text{for } k = 1, \ldots, h , \]
where by A1 Pre, \( M_0 \) and \( C \) are known terms.

(If) If there exist some firing vectors \( \bar{\sigma}_{u_1}, \ldots, \bar{\sigma}_{u_i}, \ldots, \bar{\sigma}_{u_h} \) that satisfy the set of constraints \( \xi(w, M_0, \text{Post, Pre}) \), then there exists a sequence of markings \( M_1, \ldots, M_{h-1}, M_h \) that satisfies (4) and (5).

By Theorem 1, there exists a sequence \( \sigma = \sigma_{u_1} t_{\alpha_1} \cdots \sigma_{u_h} t_{\alpha_h} \) that is enabled at \( M_0 \) and may fire yielding the evolution \( M_0[\sigma_{u_1} t_{\alpha_1}] M_1 \cdots M_{h-1}[\sigma_{u_h} t_{\alpha_h}] M_h \). Hence, \( \sigma \in \Sigma(M_0, \sigma_0) \).

In general, the solution of the set of constraints (3) is not unique. In order to check whether a fault \( f_\theta \in \Delta_f \) may have occurred when word \( w \in L \) is observed, we have to select a possible solution of (3) containing transition \( \tau_\theta \in T_f \). The following proposition proves that such a solution can be obtained by solving the ILP Problem 1 (ILPP 1) and if it admits a solution then the DES behaviour is normal during the observation \( w \) as enlightened by Corollary 1.

**Proposition 2:** Consider a DES with language \( L \) and a PN system \( \langle PN, M_0 \rangle \) modelling the DES and satisfying A1-A3. Given an observed word \( w \in L \) denoted by \( w = \sigma_o = t_{\alpha_1} t_{\alpha_2} \cdots t_{\alpha_h} \), let us define the following ILP problem ILPP 1:

\[
\text{ILPP 1:} \quad \text{max } \varphi_1(\bar{\sigma}_{u_1}, \bar{\sigma}_{u_2}, \ldots, \bar{\sigma}_{u_h}) = \sum_{i=1}^{h} \bar{\sigma}_{u_i}(\tau_\theta) \\
\text{s.t. } \xi(w, M_0, \text{Post, Pre}).
\]

If for \( \tau_\theta \in T_f \) ILPP 1 admits a solution \( \bar{\sigma}^*_{u_1}, \bar{\sigma}^*_{u_2}, \ldots, \bar{\sigma}^*_{u_h} \) and \( \varphi_1(\bar{\sigma}^*_{u_1}, \bar{\sigma}^*_{u_2}, \ldots, \bar{\sigma}^*_{u_h}) = \varphi_1^{\max} > 0 \), then
it holds $\sigma = \sigma_{u_1}t_{\alpha_1}\ldots\sigma_{u_h}t_{\alpha_h} \in \Sigma(M_0, \sigma_o, f_\theta)$.

**Proof:** Assume that vectors $\overline{\sigma}^*_{u_1}, \overline{\sigma}^*_{u_2}, \ldots, \overline{\sigma}^*_{u_h}$ are a solution of ILPP 1 and $\phi_1(\overline{\sigma}^*_{u_1}, \overline{\sigma}^*_{u_2}, \ldots, \overline{\sigma}^*_{u_h}) = \phi_1^{\text{max}} > 0$. Hence, we infer that $\overline{\sigma}^*_{u_i}(\tau_\theta) \geq 1$ for some $i \in \{1, \ldots, h\}$. By Proposition 1 there exists a sequence $\sigma = \sigma_{u_1}t_{\alpha_1}\ldots\sigma_{u_h}t_{\alpha_h}$ such that $\sigma \in \Sigma(M_0, \sigma_o)$ and $\tau_\theta \in \sigma_{u_i} \in \sigma$. Consequently, $\sigma = \sigma_{u_1}t_{\alpha_1}\ldots\sigma_{u_h}t_{\alpha_h} \in \Sigma(M_0, \sigma_o, f_\theta)$. $\square$

**Corollary 1:** Consider a DES with language $L$ and a PN system $\langle PN, M_0 \rangle$ modelling the DES and satisfying A1-A3. Given an observed word $w \in L$ denoted by $w = \sigma_o = t_{\alpha_1}t_{\alpha_2}\ldots t_{\alpha_h}$, if for each $\tau_\theta \in \Delta_f$ the ILPP 1 admits a solution $\overline{\sigma}^*_{u_1}, \overline{\sigma}^*_{u_2}, \ldots, \overline{\sigma}^*_{u_h}$ with $\phi_1(\overline{\sigma}^*_{u_1}, \overline{\sigma}^*_{u_2}, \ldots, \overline{\sigma}^*_{u_h}) = \phi_1^{\text{max}} = 0$, then the DES behaviour is normal during the observation $w$.

**Proof.** Let us assume that for each $f_\theta \in \Delta_f$ the ILPP 1 solution $\overline{\sigma}^*_{u_1}, \overline{\sigma}^*_{u_2}, \ldots, \overline{\sigma}^*_{u_h}$ is such that $\phi_1(\overline{\sigma}^*_{u_1}, \overline{\sigma}^*_{u_2}, \ldots, \overline{\sigma}^*_{u_h}) = \phi_1^{\text{max}} = 0$. Hence, two situations may occur.

(i) For each $f_\theta \in \Delta_f$ the ILPP 1 solution is $\overline{\sigma}^*_{u_i} = \emptyset$ for $i = 1, \ldots, h$: there exists no firing sequence containing a transition $\tau_k \in \Delta_f$ that is consistent with the observation. Hence, it holds $\Sigma(M_0, \sigma_o) = \emptyset$ and the system behavior is normal during the observed word $w$.

(ii) For some $f_\theta \in \Delta_f$ the ILPP 1 solution is such that $\overline{\sigma}^*_{u_i} \neq \emptyset$ for some $i \in \{1, \ldots, h\}$ and $\Sigma(M_0, \sigma_o) = \emptyset$. However, since $\phi_1(\overline{\sigma}^*_{u_1}, \overline{\sigma}^*_{u_2}, \ldots, \overline{\sigma}^*_{u_h}) = \phi_1^{\text{max}} = 0$, then for each $\sigma_{u_i} \in \sigma \in \Sigma(M_0, \sigma_o)$ it holds $\sigma_{u_i} \in T_{nf}^*$. Hence, the system behaviour is normal. In other words, in such a case some transition $\tau_k \in T_{nf}$ may have fired, but this does not correspond to the occurrence of a fault. $\square$

The following proposition allows us to detect if the behaviour of the system may be normal.

**Proposition 3:** Consider a DES with language $L$ and a PN system $\langle PN, M_\theta \rangle$ modelling the DES and satisfying A1-A3. Let us consider a word $w \in L$ denoted by $w = \sigma_o = t_{\alpha_1}t_{\alpha_2}\ldots t_{\alpha_h}$ and the following ILP problem ILPP 2:
ILPP 2

$$\min \varphi_2(\tilde{\sigma}, \tilde{\sigma}_2, ..., \tilde{\sigma}_h) = \vec{1}_F^T \sum_{i=1}^h \tilde{\sigma}_i$$

s.t. $\xi(w, M_0, Post, Pre)$

where $\vec{1}_F$ is the column vector of dimension $F$ with each element being 1 and $\sigma_i \in \sigma_{u_i}$ for $i=1,...,h$.

If ILPP 2 admits a solution $\tilde{\sigma}_1, \tilde{\sigma}_2, ..., \tilde{\sigma}_h$ and $\varphi_2(\tilde{\sigma}_1, \tilde{\sigma}_2, ..., \tilde{\sigma}_h) = \varphi_2^{\min} = 0$, then the behaviour of the system may be normal.

**Proof:** Assume that vectors $\tilde{\sigma}_1, \tilde{\sigma}_2, ..., \tilde{\sigma}_h$ are solution of ILPP 2. If $\varphi_2(\tilde{\sigma}_1, \tilde{\sigma}_2, ..., \tilde{\sigma}_h) = \varphi_2^{\min} = 0$ then by Proposition 1 there exists a sequence $\sigma = \sigma_{u_1}t_{\alpha_1}...\sigma_{u_h}t_{\alpha_h} \in \Sigma(M_0, \sigma_o)$ such that $M_0[\sigma_{u_1}t_{\alpha_1}]M_1...M_{h-1}[\sigma_{u_h}t_{\alpha_h}]M_h$ with $|\sigma_i| = 0$ for $i=1,...,h$. Consequently, the system behaviour during the occurrence of $w$ at $M_0$ may be normal.

### 4.2 The Fault Detection Algorithm

The on-line diagnostor function $\Phi$ can be specified by the fault detection algorithm in Fig. 2 that is described in the following.

The inputs of the diagnostor are the initial marking $M_0$, the PN structure (i.e., $PN=(P, T, Pre, Post)$) and the observable events of the DES. Step 2 initializes the algorithm variables and step 3 waits until a new event $e$ is observed. Assuming that the word $w$ has been observed with $|w|=h$, by the labelling function $\lambda$ we obtain $w = \lambda(\sigma)$ and $\sigma_o = t_{\alpha_1}t_{\alpha_2}...t_{\alpha_h} = w \in \Sigma$ with $t_{\alpha_i} \in T_o$ for $i=1,...,h$. Moreover, the algorithm defines the vector $\vec{\varphi}_1^{\max}$ of dimension $F$ that is devoted to store the maximum values of the objective function of ILPP 1 for each $f_{\theta} \in \Delta_f$.

Step 4 of the algorithm defines and solves ILPP 1 for each $f_{\theta} \in \Delta_f$ and records the values of the corresponding objective function in $\vec{\varphi}_1^{\max}(0)$. If ILPP 1 admits a solution $\tilde{\sigma}_1, \tilde{\sigma}_2, ..., \tilde{\sigma}_h$ for $f_{\theta}$ and $\varphi_1(\tilde{\sigma}_1, \tilde{\sigma}_2, ..., \tilde{\sigma}_h) = \varphi_1^{\max} > 0$, then by Proposition 2 it holds $\sigma = \sigma_{u_1}t_{\alpha_1}...\sigma_{u_h}t_{\alpha_h} \in \Sigma(M_0, \sigma_o, f_{\theta})$ and the algorithm sets $\Phi(M_0,w) = \Phi(M_0,w) \cup \{f_{\theta}\}$.

Step 5 checks whether the system behaviour is normal: if $\vec{\varphi}_1^{\max} = \vec{0}$, then by Corollary 1 the system behaviour is normal and the algorithm sets $\Phi(M_0,w) = N$. In such a case the algorithm returns to wait for a new event (step 3).
Finally, the algorithm checks whether $\Sigma(M_0, \sigma_o)$ may contain a sequence of silent not faulty transitions. Hence, ILPP 2 is defined (Step 6). By Proposition 3, if ILPP 2 admits a solution $\tilde{\sigma}^*u_1, \tilde{\sigma}^*u_2, \ldots, \tilde{\sigma}^*u_h$ and $\phi_1(\tilde{\sigma}^*u_1, \tilde{\sigma}^*u_2, \ldots, \tilde{\sigma}^*u_h) = \phi_1^{\min} = 0$, then the algorithm sets $\Phi(M_0, w) = \Phi(M_0, w) \cup \{N\}$, i.e., the behaviour in ambiguous because step 6 is executed only if it results $\Phi(M_0, w) \neq \emptyset$.

1. Input: $M_0$, $PN=(P, T, Pre, Post)$, $\lambda$, $T_o$, $T_u$, $T_f$, $T_{nf}$
   Output: $\Phi$
2. Initializing the algorithm variables.
   \[ w = \epsilon, h = 0, \tilde{\sigma}_o \in \mathbb{N}^0, \sigma_o = 0 \]
3. Recording the events.
   Wait until a new event $e$ is observed.
   \[ e := \lambda(t); w = wt; h = h + 1, \Phi(M_0, w) = \emptyset, \tilde{\sigma}_o(t) = \sigma_o(t) + 1; \quad \phi_1^{\max} = 0 \]
4. Solving the ILPP 1
   for $\theta = 1$ to $F$
   \[ \text{Determine } z_1 = \max \phi(\tilde{\sigma}_{u_1}, \tilde{\sigma}_{u_2}, \ldots, \tilde{\sigma}_{u_h}) \text{ s.t. } \zeta(w, M_0, Post, Pre) \]
   \[ \phi_1^{\max}(\theta) = z_1 \]
   If $\phi_1^{\max}(\theta) > 0$ then set $\Phi(M_0, w) = \Phi(M_0, w) \cup \{f_\theta\}$
   end for
5. Checking if the behaviour can be normal.
   if $\phi_1^{\max} = 0$ then $\Phi(M_0, w) = \{N\}$ go to 7 else go to 6
6. Solving the ILPP 2.
   \[ \text{Determine } z_2 = \min \phi(\tilde{\sigma}_{u_1}, \tilde{\sigma}_{u_2}, \ldots, \tilde{\sigma}_{u_h}) \text{ s.t. } \zeta(w, M_0, Post, Pre) \]
   If $z_2 = 0$ then set $\Phi(M_0, w) = \Phi(M_0, w) \cup \{N\}$.
7. Returning to the condition of recording the events.
   goto 3.

Fig. 2 The fault detection algorithm specifying the diagnoser function.

Remark 1. As enlightened in Section 2, this paper does not consider PN systems in which transitions may share the same label and are associated to the same event. Indeed, in such a case the computational effort required by the introduced algorithm increases since the loop of step 4 should be performed for each transition sharing the detected event label.
Example 2: Consider the net in Fig. 1 and described in Example 1 and assume that the word \( w = t_1t_2t_3t_4t_5 \) is observed at the initial marking \( M_0 = [1 1 0 0 0 0]^T \). The algorithm in Fig. 2 provides the following results: 
\[
\Phi(M_0, t_1) = \{f_1, N\}, \quad \Phi(M_0, t_2t_3) = \{N\}, \quad \Phi(M_0, t_1t_4) = \{N\}, \quad \Phi(M_0, t_1t_2t_3) = \{f_1, N\}, \quad \Phi(M_0, t_1t_2t_3t_4) = \{f_1f_2\}.
\]
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 \( t_k \in T_f \) and consistent with the observation. An uncertain situation is detected after word \( w = t_1t_2t_3t_4 \) because either fault \( f_1 \) may have occurred or the system behaviour may be normal. However, when \( w = t_1t_2t_3t_4t_5 \) is observed the diagnoser decides that the two faults \( f_1 \) and \( f_2 \) have occurred because the two provided minimal interpretations contain both \( t_1 \) and \( t_2 \). For example, the sequence \( \sigma = t_1t_2t_3t_4t_5t_1t_2t_3 \) may have occurred.

For this example, decisions after each observed event are taken by the diagnoser in 0.074 seconds in the worst case using a PC equipped with a 1.73 GHz processor, 1 GB RAM and the GLPK solver (GLPK Reference Manual).

4.3 Complexity Reduction of the Fault Detection Algorithm

This section presents some cases in which the ILP problems defined and solved by the proposed fault detection algorithm exhibit some peculiarities that enable an efficient solution. Indeed, we remark that even if ILP is a standard mathematical tool and an accepted methodology to solve problems in DES (Dotoli et al. 2008a, Basile et al. 2008, Cabasino et al. 2007), the on-line computational effort of the proposed algorithm increases with the number of observed transitions. To overcome this drawback, we show that if the unobservable subnet enjoys suitable properties, the solution of the algorithm may be obtained with low computational complexity. In particular, the following result enlightens a case in which the defined ILP problems admit at most one solution.

**Theorem 2.** Let \( \langle PN, M_0 \rangle \) be a PN system modeling the DES. If the subnet \( PN_u \perp_{T_u} PN \) is acyclic and backward conflict-free, then the diagnosis of the PN system \( \langle PN, M_0 \rangle \) performed by Algorithm 1 is unambiguous.

**Proof.** The proof follows from the results reported in (Giua and Seatzu 2005) in which it is proven that if
the $P_{Nu} \angle_{Tu} PN$ is acyclic and backward conflict-free, then it holds $\text{Card}(\Sigma(M_\emptyset, \sigma_o)) \leq 1$ for each $\sigma_o \in T_0^*$. Consequently, by Propositions 1, 2 and 3 and by Definitions 9 and 10 the diagnosis of the PN system $<PN, M_\emptyset>$ performed by the diagnoser $\Phi$ is unambiguous.

**Remark 2.** If the hypotheses of Theorem 2 hold, then there is at most one sequence of observable and unobservable transitions satisfying (3). Hence, a method to determine the solution is simply to solve (3).

In order to reduce the computational complexity of the proposed fault detection algorithm, the following result states that if the subnet $P_{Nu} \angle_{Tu} PN$ enjoys suitable properties, then each basic solution of the LP relaxations of ILPP 1 and ILPP 2 is an integer-valued solution.

**Theorem 3.** Let $<PN, M_\emptyset>$ be a PN system modeling the DES. If the subnet $P_{Nu} \angle_{Tu} PN$ is an acyclic SM and $<PN, M_\emptyset>$ is bounded, then each basic solution of the LP relaxations of ILPP 1 and ILPP 2 is an integer-valued solution.

*The proof is reported in the Appendix.*

Theorem 3 points out that if the unobservable subnet is an acyclic SM, then the solution of each ILP problem formulated by the fault detection algorithm can be obtained as a solution of LP problems which are of polynomial complexity.

### 4.4 Computational remarks and comparisons

In this section we present a comparison between the proposed fault detection procedure and the relevant methods presented in the related literature. The ILP problems solved by the fault detection algorithm in Fig. 2 are at most $F+1$ in number, where $F$ is the cardinality of the set of faults that may occur in the system. To evaluate the computational effort required by the proposed algorithm, we recall that the primary determinants of the computational difficulty of an ILP problem are the number of integer variables. It is easy to infer that in the worst case the unknowns of each ILP problem are $h(m+F+K)$ in number, where $h \geq 1$ denotes the length of the word $w$ and $K$ is the cardinality of the set of silent transitions that do not correspond to faults. In practice, our experience shows that in the examined cases, of size comparable with those presented in the literature, 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 Reference Manual).

Concerning the comparison with (Cabasino et al. 2007) we enlighten that their fault detection procedure involves $F \times \text{Card}(\mathcal{M}(w))$ ILP problems, where $\mathcal{M}(w)$ is the set including the basis markings and the relative firing vectors for the observed word $w$. We note that the basis marking is the marking reached firing $w$ interleaved with an observable justification $\sigma_i$, hence the number of elements of $\mathcal{M}(w)$ may be very large.

Similar considerations apply to the approach proposed by Basile et al. (2008) that presents an on-line algorithm solving at each observed transition some ILP problems for each fault transition and for each so-called $g$-marking estimation, i.e., a marking having some negative components because silent transitions have occurred.

Summing up, both the above recalled fault detection algorithms require solving at each observation several ILP problems. In neither cases an estimate of the number of solved ILP problems is provided, nor an upper bound for it. Conversely, our approach requires solving at most $F+1$ ILP problems at each observed word.

Another relevant issue of our approach concerning the computational complexity is that the presented algorithm is reduced to polynomial complexity in the special case in which the subnet $\text{PN}_u \angle_{\text{PN}}$ is an acyclic SM and the PN system $\langle \text{PN}, M_0 \rangle$ is bounded. This result extends a similar property of Basile et al. (2008).

It could be interesting to compare the proposed approach with the one of Genc and Lafortune (2003). In particular, the PN structure is the input of the diagnosers both in our approach and in (Genc and Lafortune 2003). However, as we point out in the introduction, the diagnoser proposed by Genc and Lafortune (2003) is “compiled” and does not avoid the state explosion problem. Indeed, it is built off-line by enumerating all the markings consistent with the observed word and each state has to be characterized with the corresponding fault information. Obviously, the structure of the diagnoser strictly depends on the DES structure and has to be completely redefined if the DES changes. The advantages of our approach is avoiding the state explosion and building the diagnoser as an “interpreted” diagnoser with the absence of the off-line computations. Hence, it can be applied to different DES by simply updating the structure of the PN system in input to the procedure. Nevertheless, the authors believe that the computational effort could be reduced by suitable off-line evaluations, as proposed for example by Basile et al. (2008). However, such an off-line computation could be complex and time consuming. Hence, in our approach we choose to avoid such a kind of computation presenting a fault detection strategy that can be performed completely on-line.
5. CONCLUSIONS

The paper addresses the fault detection problem of Discrete Event Systems (DES) and proposes an on-line diagnoser in a Petri Net (PN) framework. A procedure observes and stores the sequence of system events and decides on-line whether the system behaviour is normal or some faults may have occurred. To this aim, some Integer Linear Programming (ILP) problems are defined by an algorithm that provides, at each observed event, the possible occurred faults or certifies the system normal behaviour. In order to cope with the computational complexity of the algorithm, sufficient conditions are provided guaranteeing that the continuous relaxation of the ILP problems provides an integer solution. In this way the proposed algorithm turns out to exhibit polynomial complexity.

With respect to the approaches proposed in the related literature, the proposed method is concerned with the computational complexity of the diagnosis algorithm in order to provide a reasonably efficient method suitable for on-line use with large systems. However, the algorithm does not require off-line calculations based on the structure of the considered PN system. In this way, the proposed fault detection technique can be more easily applicable to situations in which the system structure may change than other approaches in the related literature.

Further improvements in the efficiency of the proposed method could be obtained if we assume that after an event sequence occurrence the reached marking is known or univocally determined. In this situation, an incremental solution approach could be devised, taking as the input to the algorithm the reached marking. However, identifying the conditions necessary to univocally determine the reached marking is expected to require a significant amount of effort to be specified and developed. Hence, this issue will be tackled in a successive work.

Another line for future research will focus on the problem of diagnosability, i.e., determine if it is possible to reconstruct the occurrence of fault events observing words of finite length. This problem was extensively studied within the framework of automata, whereas very few results have been presented in the PN area, so that diagnosability still is an open problem. The idea presented in the paper could provide some hints to face the diagnosability problem with PN approaches, too.

APPENDIX

A general ILPP is \( \text{z}_{\text{IP}} = \max \{ cx \mid \text{s.t. } Ax \leq b, x \in \mathbb{N}^m \} \) (Nemhauser and Wolsey 1988). The basic solution of the LP relaxation of an ILPP is related to some properties of the coefficient matrix \( A \). The following definitions and propositions are recalled in order to prove Theorem 3.

**Definition A1**: An \( m \times n \) integral matrix \( A \) is said Totally Unimodular (TU) if the determinant of each
square sub-matrix of $A$ is equal to 0, 1 or -1.

**Proposition A1** (Nemhauser and Wolsey 1988). Let $A$ be a (0,1,-1) matrix with no more than two nonzero elements in each column. If each column $j$ that contains two nonzero elements is such that $\sum_i A(i,j)=0$, then $A$ is TU.

**Proposition A2** (Nemhauser and Wolsey 1988). If $A$ is TU, $b$, $b'$, $d$ and $d'$ are integral and $P(b,b',d,d')=\{x \in \mathbb{R}^n : b' \leq Ax \leq b, d' \leq x \leq d\}$ is not empty, then $P(b,b',d,d')$ is an integral polyhedron.

Now, the following results characterize the unobservable behaviour of a bounded PN system in which the subnet $PN_u \angle TuPN$ induced by the set of unobservable transition set $T_u$ is acyclic.

**Theorem A1.** (Cabasino 2005) Consider a PN system $\langle PN, M_0 \rangle$ and the subnet $PN_u \angle TuPN$ induced by the set of unobservable transition set $T_u$. If $\langle PN, M_0 \rangle$ is bounded and $PN_u \angle TuPN$ is acyclic, then there exists a positive integral number $b_{max}$ such that $\forall M \in R(\langle PN, M_0 \rangle), \forall \sigma_u \in T_u^* : M[\sigma_u] \geq 0 \leq \sum_i u^G_{\sigma} |u(\sigma) - b_{\sigma} \tau| \leq b_{max}$ for $i=1,\ldots,h$.

In other words, Theorem A1 states that if $\langle PN, M_0 \rangle$ is bounded and $PN_u \angle TuPN$ is acyclic, then the length of the unobservable firing sequences is bounded by an integer $b_{max}$ and can not be infinite.

Now, the following lemmas are introduced in order to prove that the hypotheses of Proposition A2 are verified if $PN_u \angle TuPN$ is an acyclic MG and $\langle PN, M_0 \rangle$ is bounded.

**Lemma A1.** Consider a DES with language $L$. Let $\langle PN, M_0 \rangle$ be a bounded PN system modelling the DES and satisfying A1-A3. Given a word $w \in L$ denoted by $w=\sigma_o = t_{\alpha_1} t_{\alpha_2} \cdots t_{\alpha_h}$, the set of linear constraints $\xi(w, M_0, Post, Pre)$ admits at least a solution $\bar{\sigma}_{u_1}, \ldots, \bar{\sigma}_{u_i}, \ldots, \bar{\sigma}_{u_h}$ such that $0 \leq \sum_{j=1}^{F+K} \bar{\sigma}_{u_i} \tau_j \leq b_{\max}$ for $i=1,\ldots,h$.

**Proof:** If it holds $M_0[t_{\alpha_1}]M_1 \cdots M_{h-1}[t_{\alpha_h}]M_h$ then $\sigma=\sigma_o = t_{\alpha_1} t_{\alpha_2} \cdots t_{\alpha_h}$ and vectors $\bar{\sigma}_{u_i}=0$ for $i=1,\ldots,h$ satisfy the set of constraints (3). On the other hand, if there exists a sequence $\sigma=\sigma_{u_1} t_{\alpha_1} \cdots \sigma_{u_h} t_{\alpha_h}$ that is enabled at $M_0$, then by Theorem A1 it holds $|\sigma_{u_i}| \leq b_{max}$ for $i=1,\ldots,h$. Consequently, we infer
\[ 0 \leq \sum_{j=1}^{F+K} \bar{\sigma}_{ui}(\tau_j) \leq b_{\text{max}} \text{ for } i=1,\ldots,h. \]

Now we consider the set of inequality constraints (3). It can be turned into a set of equations by subtracting to each \( k \)-th constraint a surplus variable vector \( z_k \in \mathbb{N}^m \) with \( k=1,\ldots,h \). Denoting

\[
\text{Pre} \ t_{\alpha_k} \cdot M_0 \cdot C \sum_{i=1}^{k-1} t_{\alpha_i} = b_k \text{ for } k=1,\ldots,h,
\]

the constraint set \( \xi(w, M_0, \text{Post, Pre}) \) can be rewritten by the following equations:

\[
\bar{\xi}_1(w, M_0, \text{Post, Pre}) = \left\{ \begin{array}{c}
\bar{\sigma}_{ui} \in \mathbb{N}^{F+K}, \quad z_i \in \mathbb{N}^m, \text{ for } i=1,\ldots,h \\
C_u \begin{bmatrix} 0 & 0 \ldots & 0 & -I_m & 0 & 0 \ldots & 0 \\
0 & C_u \ldots & 0 & 0 & I_m & -I_m \ldots & 0 \\
0 & 0 & C_u \ldots & 0 & 0 & I_m & -I_m \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & C_u & 0 & 0 \ldots & 0 \ldots & 0 & -I_m \\
\end{bmatrix}
\end{array} \right\}
\]

where \( I_m \) is the identity matrix of dimension \( m \).

Denoting \( A = \begin{bmatrix} C_u & 0 & 0 & \ldots & 0 & -I_m & 0 & 0 & \ldots & 0 \\
0 & C_u & 0 & \ldots & 0 & I_m & -I_m & 0 & \ldots & 0 \\
0 & 0 & C_u & \ldots & 0 & 0 & I_m & -I_m \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & C_u & 0 & 0 \ldots & 0 \ldots & 0 & -I_m \\
\end{bmatrix} \), \( x = \begin{bmatrix} \bar{\sigma}_{ui} \\
\bar{\sigma}_{u2} \\
\bar{\sigma}_{u3} \\
\bar{\sigma}_{uh} \\
z_1 \\
z_2 \\
z_3 \\
z_h \\
\end{bmatrix} \) and \( B = \begin{bmatrix} b_1 \\
b_2 - b_1 \\
b_3 - b_2 \\
\ldots \\
b_h - b_{h-1} \\
\end{bmatrix} \),

we prove the following Lemma that characterizes the solutions of the constraints set \( \xi_1(w, M_0, \text{Post, Pre}) \).

**Lemma A2:** Consider a DES with language \( L \) and a bounded PN system \( \langle PN, M_0 \rangle \) modelling the DES and satisfying A1-A3. If the constraint matrix \( A \) of \( \xi_1(w, M_0, \text{Post, Pre}) \) is TU, then the set of solutions \( x \in \mathbb{N}^{2(F+H)} \) of (6) is an integral polyhedron.
Proof: $B$ is integral because it is obtained by sub-vectors that are differences of integral vectors. Hence we can assume $b=b'=B$. By Lemma A1 the firing vectors $\tilde{\sigma}_{u_1}, \ldots, \tilde{\sigma}_{u_i}, \ldots, \tilde{\sigma}_{u_h}$ are such that

$$0 \leq \sum_{j=1}^{F+K} \tilde{\sigma}_{u_i}(r_j) \leq b_{\text{max}}$$

for $i=1,\ldots,h$. Consequently, it holds $\tilde{\sigma}_{u_i} \leq \tilde{b}_{\text{max}}$ were $\tilde{b}_{\text{max}}$ is equal to a column vector of dimensions $(F+K)$ with each element being $b_{\text{max}}$. On the other hand, the surplus variables are

$$z_k \leq kC_\mu \tilde{b}_{\text{max}} - b_k$$

for $k=1,\ldots,h$. Hence, we choose $d' = 0$ and $d = \begin{bmatrix} d_1 \\ d_2 \end{bmatrix}$ with $d_1 = \tilde{b}_{\text{max}}$ and $d_2 = kC_\mu \tilde{b}_{\text{max}}$. Since by Lemma A1 the set $P(B, B, 0, d) = \{x \in \mathbb{R}^{F+H+m} : Ax = B, 0 \leq x \leq d\}$ is nonempty, then by Proposition A2 the set $P(B, B, 0, d)$ is an integral polyhedron.

Having established the previous results, we can now prove Theorem 3:

Proof of Theorem 3
Since $C_\mu$ is an incidence matrix of a SM and matrices $I_{F+K}$ are identity matrices, $A$ is a $(0,1,-1)$ matrix with no more than two nonzero elements in each column. Moreover, by the properties of SM and the matrix inspection, if a column has two nonzero elements, then such elements have opposite sign. Hence, each column $j$ that contains two nonzero elements is such that $\sum_i A(i,j)=0$. Thus $A$ is TU and by Lemma A2, a basic solution of the LP relaxation of ILPP 1 and ILPP 2 is an integer-valued solution.

REFERENCES
M. P. Cabasino (2005), Diagnosi di un sistema ad eventi discreti mediante automi e reti di Petri, Graduate Thesis (in Italian), University of Cagliari.


