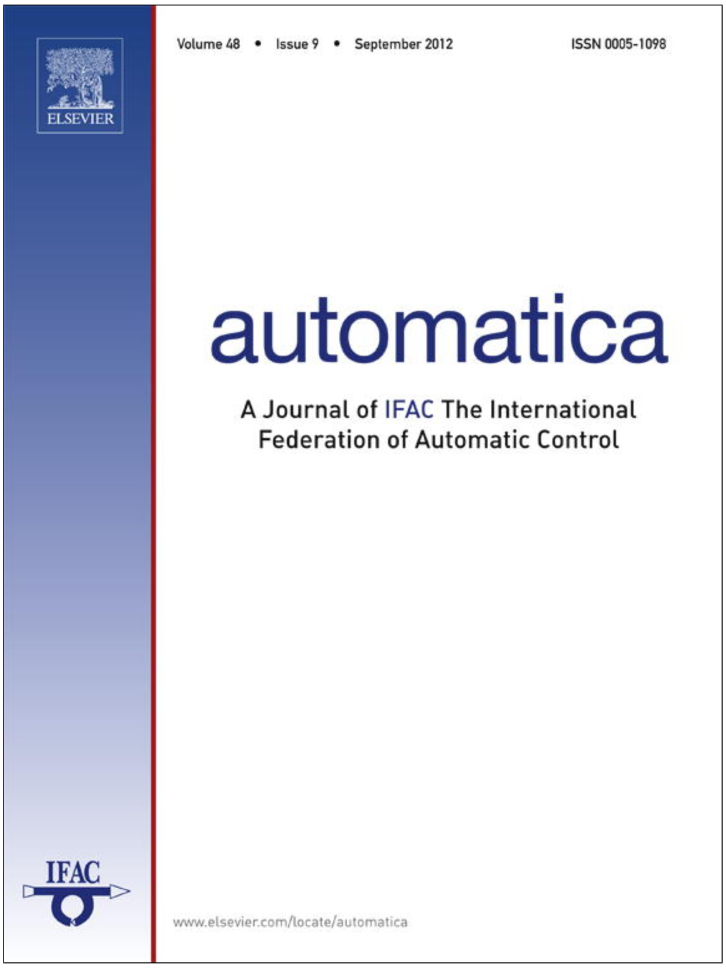

Volume 48 • Issue 9 • September 2012 ISSN 0005-1098

automatica

A Journal of IFAC The International Federation of Automatic Control

www.elsevier.com/locate/automatica

Automatica 48 (2012) 2047–2058

Contents lists available at SciVerse ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

On $\mathcal{K}$-diagnosability of Petri nets via integer linear programming[☆]

F. Basile[a], P. Chiacchio[a], G. De Tommasi[b,1]

[a] Dipartimento di Ingegneria Elettronica ed Ingegneria Informatica, Università degli Studi di Salerno, Salerno, Italy

[b] Dipartimento di Informatica e Sistemistica, Università degli Studi di Napoli Federico II, Napoli, Italy

ARTICLE INFO

Article history:
Received 29 December 2010
Received in revised form
11 January 2012
Accepted 12 April 2012
Available online 11 July 2012

Keywords:
Diagnosability
Discrete event systems
Petri nets
Integer linear programming

ABSTRACT

This paper deals with the problem of diagnosability of a fault after the firing of a finite number events (i.e., $\mathcal{K}$-diagnosability). This problem corresponds to diagnosability of a fault within a finite *delay* in the context of discrete event systems. The main contribution of this paper is a necessary and sufficient condition for $\mathcal{K}$-diagnosability of bounded nets. The proposed approach exploits the mathematical representation of Petri nets and the Integer Linear Programming optimization tool. In particular no specific assumptions are made on the structure of the net induced by the unobservable transitions, since the proposed approach permits to detect also the undiagnosability due to the presence of *unobservable cycles*.

1. Introduction

The fault diagnosis is crucial for the safety of both systems and operators in industry. Fault diagnosis has received a lot of attention in the discrete event systems (DES) community since the early 90s (Sampath, Sengupta, Lafortune, Sinnamohideen, & Teneketzis, 1995). Diagnosability of DES deals with the possibility of detecting, within a finite delay, the occurrences of *unobservable* fault events using the record of observed events. Fault detection consists of online monitoring the system using the record of observed events to timely provide the set of faults that could have happened.

The formal definition of diagnosability has been given in the framework of finite state automata and regular languages (Sampath et al., 1995; Zad, Kwong, & Wonham, 2005). Necessary and sufficient conditions for diagnosability of DES modeled as automata have been given in Sampath et al. (1995). The diagnosability test is based on another automaton called *diagnoser* which gives, after each observed event, a set of faults that could have happened (Sampath et al., 1995), or a set of fault states that the system could have reached (Zad et al., 2005). The *diagnoser approach* has been used to extend the diagnosability concept to stochastic automata (Lunze & Schröder, 2001), and to the decentralized case (Debouk, Lafortune, & Teneketzis, 2000). The concept of diagnosability itself has been also extended in Paoli and Lafortune (2005).

The problem of diagnosability has been recently tackled within the Petri nets (PNs) framework. PNs have a twofold representation: graphical and mathematical. The mathematical representation of PNs allows use of standard tools, such as Integer Linear Programming, to solve DES diagnosis problems. The graphical nature helps to recognize if a model belongs to a certain net subclass. If this is the case, efficient algorithms that exploit the peculiarity of a given subclass can be devised. Furthermore, the local state representation often helps in reducing both computational complexity and memory requirements when solving the diagnosis problem. Indeed, the building of a diagnoser requires the exploration of the state space, whose number of nodes grows exponentially with respect to the net size.

Although a number of results are now available for fault detection when DESs are modeled as PNs, only few of them are available for diagnosability. Two approaches are mainly adopted when PNs are used:

(1) the first consists in computing a graph from a net system; diagnosability test and/or online fault detection are then performed by using this graph;
(2) the second provides algorithms which perform the diagnosability test and/or online fault detection working directly on the net model. In this case the mathematical representation of PNs is exploited.

As for approach (1), in Ushio, Onishi, and Okuda (1998) the concept of diagnosability is formulated for PN systems, and a diagnoser-based approach is used to check this property assuming that the

[☆] The material in this paper was partially presented at the 10th International Workshop on Discrete Event Systems (WODES'10), August 30–September 1, 2010, Berlin, Germany. This paper was recommended for publication in revised form by Associate Editor Jan Komenda under the direction of Editor Ian R. Petersen.

E-mail addresses: fbasile@unisa.it (F. Basile), pchiacchio@unisa.it (P. Chiacchio), detommas@unina.it (G. De Tommasi).

[1] Tel.: +39 0817683853; fax: +39 0817683816.

0005-1098/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.automatica.2012.06.039

net marking is observable, all transitions are not observable, and the faults are associated to transitions. in this case the diagnoser turns to be equal to the reachability graph of the PN system with some additions. A sufficient condition for diagnosability of unbounded PNs is also presented. In Chung (2005) Chung presents a similar approach adding the assumption that some transitions are observable.

In Cabasino, Giua, and Seatzu (2009b) two graphs are presented, the *modified basis reachability graph* (MBRG) and the *basis reachability diagnoser* (BRD), assuming that the net marking is not observable. This approach is derived from the one proposed by the same authors in Cabasino, Giua, and Seatzu (2010) for fault detection, and it recalls the idea of reduced observer for fault detection proposed by Boel et al. in Boel and Jiroveanu (2004). Both the approaches proposed in Boel and Jiroveanu (2004) and Cabasino et al. (2010) require the PN model to be bounded. Although in most of the cases these two graphs are in general smaller than the reachability graph, the procedure proposed to build the MBRG can require a number of steps equal to the cardinality of the reachability set. Furthermore, the proposed diagnosability test requires to check the existence of cycles in the BRD, which, in the worst case, is a task with exponential complexity in time (Sampath, Sengupta, Lafortune, Sinnamohideen, & Teneketzis, 1996; Zad, Kwong, & Wonham, 2003).

Similarly, in Jiroveanu and Boel (2010) a automata called *ROF-automaton*, which may have state space that is significantly smaller than the reachability graph, is proposed to check diagnosability of bounded nets without unobservable cycles.

In their recent work (Cabasino, Giua, Lafortune, & Seatzu, 2009a), Cabasino et al. have also presented a necessary and sufficient condition for unbounded nets, which is based on the analysis of a net, called *verifier net*, that is built from the initial system. As in Cabasino et al. (2009b), the proposed approach for unbounded nets requires to search for the existence of cycles in the coverability graph of the verifier net, which is computationally demanding. Furthermore, the authors claim that when applicable the approach proposed in Cabasino et al. (2009b) may be preferable to the one in Cabasino et al. (2009a), because it also allows to solve the diagnosis problem within the same framework.

Different papers deal also with approach (2). In particular, using the assumption that the net marking and the transitions set are partially observable, and investigating the relation between diagnosability and the properties of the T-invariants of the net, a sufficient condition for diagnosability based on linear programming is proposed in Wen, Li, and Jeng (2005). In Trevino, Ruiz-Beltran, Rivera-Rangel, and Lopez-Mellado (2007) a sufficient condition has also been presented for safe and strongly connected PNs with an output function that associates an output vector to each net marking (interpreted PNs). Two sufficient conditions have been presented by the authors in Basile, Chiacchio, and De Tommasi (2008): the first is for undiagnosability of a fault transition t_f, while the second is for diagnosability of t_f. Such conditions use the concept of g-marking introduced for online fault detection in Basile, Chiacchio, and De Tommasi (2009a).

For the sake of completeness, different approaches to the fault diagnosis of DES modeled by PNs have been proposed in Lefebvre and Delherm (2007) and Wu and Hadjicostis (2005). In both cases it is assumed that the net marking is partially (Lefebvre & Delherm, 2007) or completely (Wu & Hadjicostis, 2005) observable, even if unobservable events (transitions) are admitted. However, they do not explicitly address the problem of diagnosability.

1.1. Contribution of the paper

This paper addresses the problem of $\mathcal{K}$-diagnosability of a fault in a DES modeled as a Petri net. This problem corresponds to the diagnosability of a fault within a finite *delay* (i.e., in $\mathcal{K}$ steps). The main result of this paper is a necessary and sufficient condition for $\mathcal{K}$-diagnosability of bounded nets. The proposed approach exploits the mathematical representation of Petri nets and the Integer Linear Programming (ILP) standard optimization tool, which has been recently used in Basile et al. (2009a), Basile, Chiacchio, and De Tommasi (2009b) and Dotoli, Fanti, and Mangini (2009) to successfully solve the fault detection problem.

The concept of $\mathcal{K}$-diagnosability has been originally formulated in Sampath et al. (1995) in the context of fault detection with automata. By definition, if a fault transition is diagnosable then there exists a minimum value $\bar{\mathcal{K}}$ such that it is also $\bar{\mathcal{K}}$-diagnosable. In the automata context, given an integer $\mathcal{K}$, $\mathcal{K}$-diagnosability can be checked by means a path search on the diagnoser (see Sampath et al., 1995, Corollary 1); furthermore the related concept of k-diagnoser has been recently adopted also to study the sensor minimization problem (Cassez, Tripakis, & Altisen, 2007). Although the concept of $\mathcal{K}$-diagnosability has been firstly extended to PNs by Cabasino et al. (2009a), the present paper is one of the few that deal with this subject within the PNs context without relying on a diagnoser-based approach.

The idea developed in this work is to characterize every sequence u, that enables a fault f from the initial marking, and every sequence v that continues the system evolution after the fault occurrence, in terms of two sets of firing count vectors satisfying a set of linear constraints. A second set of linear constraints is used to characterize, in terms of firing count vectors, the sequences of unobservable transitions which enable, and thus explain, the firing of the projection of u and v over the set of observable transitions. These two sets of constraints allow us to formulate the diagnosability of f as an integer linear programming problem.

As the conclusion of this section we would like to point out the main features of the proposed approach and some differences between this work and Cabasino et al. (2009a,b), which are the ones strictly related to the present work, and which give necessary and sufficient conditions for diagnosability of both bounded and unbounded nets. In particular, the proposed approach:

(1) uses a standard tool to check diagnosability, preventing the computation of a graph;
(2) does not require any specific assumption on the structure of the net induced by the unobservable transitions, while this net is supposed to be acyclic in Cabasino et al. (2009a,b); in literature such an assumption is usually exploited in order to being able to build the *diagnoser*, which is then used to check diagnosability. The proposed approach does not rely on a diagnoser, since it solves ILPs in order to detect the undiagnosability. In particular, the considered constraints include the state equation and the transition enabling conditions. Thanks to these constraints it is possible to avoid the spurious solutions obtained when only the state equation is used and when there are *unobservable cycles*;
(3) allows to check *practical* diagnosability, specifying a *quantitative* bound for the number of events in the continuation of u, i.e., it specifies an upper bound for the number of events that are needed to detect a fault. Given an integer $\mathcal{K}$, we provide a set of conditions that need to be satisfied if all the possible faults are diagnosable at most after $\mathcal{K}$ firings after their occurrence. This practical diagnosability permits to verify if the fault can be detected within a specified maximum time delay. If the maximum interleaving between two firings is given, and if it is required to detect the fault within a maximum delay, that implies the fault detection to be performed within a maximum number of firings, which is the design parameter $\mathcal{K}$. Hence the concept of $\mathcal{K}$-diagnosability is useful during the design phase, in order to check if the designed system fulfills the constraints in terms of maximum time needed to detect the faults;

(4) the proposed necessary and sufficient condition for $\mathcal{K}$-diagnosability can be applied only to bounded net systems;
(5) allows to solve both the diagnosability problem and fault detection within the same framework, i.e., exploiting the mathematical representation of PNs and ILP optimization tools, similarly to what has been done in Cabasino et al. (2009b) and Cabasino et al. (2010);
(6) as far as the computational complexity is concerned, its main drawback is that the characterization of a fireable sequence in terms of firing count vectors may require, in the worst case, a number of firing count vectors equal to the sequence length. However, a similar computational effort is needed to check the existence of cycles in the graphs as proposed in Cabasino et al. (2009a,b);
(7) making use of firing count vectors instead of explicit estimation of the reachability set, our approach is particularly suited when PNs concurrency is exploited to model DES behavior. In such a case it is possible to reduce the number of required firing count vectors and hence the computational effort.

The present work is organized as follows. Section 2 introduces basic PNs notation and the definition of diagnosability and $\mathcal{K}$-diagnosability. A necessary and sufficient condition to check $\mathcal{K}$-diagnosability of a fault transition in a bounded unlabeled net is provided in Section 3. This result is then extended to labeled nets in Section 4. The effectiveness of the proposed results is shown through the examples in Section 5. Eventually, some conclusive remarks are given in Section 6.

2. Preliminaries

The Petri nets basics, together with some additional notations are introduced at the beginning of this section. The definition of diagnosability in the field of Petri nets is then recalled. For a complete review on Petri nets the reader can refer to Hruz and Zhou (2007) and Murata (1989).

2.1. Background and notation

A *Place/Transition* net (P/T net) is a 4-tuple $N = (P, T, \mathbf{Pre}, \mathbf{Post})$, where P is a set of m places (represented by circles), T is a set of n transitions (represented by empty boxes and each one associated to an event), $\mathbf{Pre} : P \times T \mapsto \mathbb{N}$ ($\mathbf{Post} : P \times T \mapsto \mathbb{N}$) is the *pre-* (*post-*) *incidence* matrix. $\mathbf{Pre}(p, t) = w$ ($\mathbf{Post}(p, t) = w$) means that there is an arc with weight w from p to t (from t to p); $\mathbf{C} = \mathbf{Post} - \mathbf{Pre}$ is the incidence matrix. The symbols ${}^\bullet p$ (${}^\bullet t$) and $p^\bullet$ ($t^\bullet$) are used for the *pre-set* and *post-set* of a place $p \in P$ (transition $t \in T$), respectively, e.g.

$$ {}^\bullet t = \left\{p \in P \mid \mathbf{Pre}(p, t) \neq 0\right\}. $$

A *marking* is a function $\boldsymbol{m} : P \mapsto \mathbb{N}$ that assigns to each place of a net a nonnegative integer number of tokens, drawn as black dots. It is useful to represent the marking of a net with a vector $\boldsymbol{m} \in \mathbb{N}^m$. A *net system* $S = \langle N, \boldsymbol{m}_0\rangle$ is a net N with an initial marking $\boldsymbol{m}_0$. A transition t is enabled at $\boldsymbol{m}$ *if and only if* $\boldsymbol{m} \geq \mathbf{Pre}(\cdot, t)$ and this is denoted as $\boldsymbol{m}[t\rangle$. An enabled transition t may fire, yielding the marking $\boldsymbol{m}' = \boldsymbol{m} + \mathbf{C}(\cdot, t)$, and this is denoted as $\boldsymbol{m}[t\rangle \boldsymbol{m}'$. If a transition is not enabled at $\boldsymbol{m}$ it is denoted as $\boldsymbol{m}\neg[t\rangle$.

A *firing sequence* from $\boldsymbol{m}$ is a sequence of transitions $\sigma = t_1t_2 \dots t_k$ such that $\boldsymbol{m}[t_1\rangle \boldsymbol{m}_1[t_2\rangle \boldsymbol{m}_2 \dots [t_k\rangle \boldsymbol{m}_k$, and this is denoted as $\boldsymbol{m}[\sigma\rangle \boldsymbol{m}_k$. The notations $\boldsymbol{m}[\sigma\rangle$ and $\boldsymbol{m}\neg[\sigma\rangle$ denote an enabled and a disabled sequence under a marking $\boldsymbol{m}$, respectively. Furthermore, $t_i \in \sigma$ denotes that the transition t_i belongs to the sequence σ. The length of a sequence σ is denoted by $|\sigma|$. Furthermore, given $\bar{T} \subseteq T$, $\bar{T}^*$ denotes the Kleene closure of $\bar{T}$, that is $\bar{T}^*$ is the set of all finite sequence of elements of $\bar{T}$, including the empty sequence ν. The empty sequence ν is such that $\sigma\nu = \nu\sigma = \sigma$ and $|\nu| = 0$ (more details can be found in Cassandras & Lafortune, 1999, p. 55).

A marking $\boldsymbol{m}'$ is said to be *reachable* from $\boldsymbol{m}_0$ *iff* there exists a sequence σ such that $\boldsymbol{m}_0[\sigma\rangle \boldsymbol{m}'$. $R(N, \boldsymbol{m}_0)$ denotes the set of reachable markings of the net system $\langle N, \boldsymbol{m}_0\rangle$.

The function $\boldsymbol{\sigma} : T \mapsto \mathbb{N}$, where $\boldsymbol{\sigma}(t)$ represents the number of occurrences of t in σ, is called the *firing count vector* of the firing sequence σ. As has been done for the marking of a net, the firing count vector is often denoted as a vector $\boldsymbol{\sigma} \in \mathbb{N}^n$. The notation $\boldsymbol{\sigma} = \pi(\sigma)$ is used to denote that $\boldsymbol{\sigma}$ is the firing count vector of σ. Given a sequence σ the 1-norm of the related firing count vector[2] $\boldsymbol{\sigma} = \pi(\sigma)$ is equal to the length of the sequence, i.e., $\|\boldsymbol{\sigma}\|_1 = |\sigma|$.

If $\boldsymbol{m}_0[\sigma\rangle \boldsymbol{m}$, then it is possible to write the vector equation

$$ \boldsymbol{m} = \boldsymbol{m}_0 + \mathbf{C} \cdot \boldsymbol{\sigma}, \tag{1} $$

which is called the *state equation* of the net system.

Because of its *spurious solutions* (see García Vallés, 1999), the fulfilling of the state equation (1) is only necessary to determine if $\boldsymbol{m}$ is reachable from $\boldsymbol{m}_0$ after the firing of $\boldsymbol{\sigma}$, i.e., to check if $\boldsymbol{m} \in R\big(N, \boldsymbol{m}_0\big)$. Indeed, for a generic net, given a sequence σ, the fact that $\boldsymbol{\sigma} = \pi(\sigma)$ satisfies the state equation gives only a necessary condition to establish if σ is an enabled sequence. The next classical result gives a necessary and sufficient condition that must be fulfilled by every sequence with finite length which is enabled under the marking $\boldsymbol{m}$.

Lemma 1 (García Vallés, 1999)**.** *There exists a set of ρ integer vectors $\boldsymbol{s}_1, \dots, \boldsymbol{s}_\rho$ with $\rho \leq |\sigma|$ such that the following linear constraints are fulfilled*

$$ \begin{cases} \boldsymbol{m} \geq \mathbf{Pre} \cdot \boldsymbol{s}_1 \\ \boldsymbol{m} + \mathbf{C} \cdot \boldsymbol{s}_1 \geq \mathbf{Pre} \cdot \boldsymbol{s}_2 \\ \dots \\ \boldsymbol{m} + \mathbf{C} \cdot \displaystyle\sum_{i=1}^{\rho-1} \boldsymbol{s}_i \geq \mathbf{Pre} \cdot \boldsymbol{s}_\rho \\ \displaystyle\sum_{i=1}^{\rho} \boldsymbol{s}_i = \pi(\sigma) \end{cases} \tag{2} $$

iff *there exists at least one sequence σ, which is enabled under the marking $\boldsymbol{m}$ and such that $\pi(\sigma) = \boldsymbol{\sigma}$.* □

Definition 1 (*Reachability Graph and Live Ergodic Components* Góra, 1992; Teruel & Silva, 1993)**.** Given a net system $\langle N, \boldsymbol{m}_0\rangle$ and its reachability set $R(N, \boldsymbol{m}_0)$, the reachability graph is a labeled directed graph $RG(N, \boldsymbol{m}_0) = (V, E, l)$ with $l : E \mapsto T$ given by:

- $V = R(N, \boldsymbol{m}_0)$;
- $\big((\boldsymbol{m}, \boldsymbol{m}') \in E \wedge l(\boldsymbol{m}, \boldsymbol{m}') = t\big) \Leftrightarrow \boldsymbol{m}[t\rangle \boldsymbol{m}'$.

Given the reachability graph of a net system, let us denote with U a subset of nodes $U \subseteq R(N, \boldsymbol{m}_0)$, and with $U^\bullet = \big\{\boldsymbol{m}' \in R(N, \boldsymbol{m}_0) \mid (\boldsymbol{m}, \boldsymbol{m}') \in E, \boldsymbol{m} \in U\big\}$.

The set succ(U) of successors of U is the minimal set such that $U^\bullet \subseteq$ succ(U) and succ$(U)^\bullet \subseteq$ succ(U). The subgraph of (V, E, l) induced by U is defined by

$$ G(U) = \Big(U, (U \times U) \cap E, l|_{(U\times U)\cap E}\Big), $$

where $l|_{(U\times U)\cap E}$ denotes the restriction of l to the subset $(U \times U) \cap E$.

The set of labels of $G(U)$ is denoted with $l(U)$. The subset of nodes U is said to be an ergodic component if and only if $(U = \{v\} \wedge v^\bullet = \emptyset)$ or $(G(U)$ is strongly connected $\wedge\ U =$ succ$(U))$. Ergodic components of the first kind are also called deadlocks, while those of the second kind are called active ergodic components or, when $l(U) = T$, live ergodic components.

[2] Given a vector $\boldsymbol{\sigma}$, the 1-norm $\|\boldsymbol{\sigma}\|_1$ is equal to the sum of the absolute values of the vector elements.

A net system $S = \langle N, \boldsymbol{m}_0 \rangle$ is said to be *bounded* if the number of tokens in each place does not exceed a finite number k for any marking in $R\big(N, \boldsymbol{m}_0\big)$, otherwise it is said to be *unbounded*.

Definition 2 (*T-Invariants*)**.** Given a net N, a vector $\boldsymbol{y} \in \mathbb{N}^n$ is called *T-invariant* if

$$\boldsymbol{C} \cdot \boldsymbol{y} = \boldsymbol{0}.$$

Given a T-invariant $\boldsymbol{y}$, the set of transitions corresponding to nonzero entries of $\boldsymbol{y}$ is called the *support* of $\boldsymbol{y}$, and is denoted with $\mathrm{SUP}(\boldsymbol{y})$. The support is said to be minimal if no proper nonempty subset of the support is also a support. As defined in Murata (1989), a T-invariant $\boldsymbol{y}$ is said to be minimal if there is no other T-invariant $\boldsymbol{y}'$ such that $\boldsymbol{y}'(t) \leq \boldsymbol{y}(t)$ for all t. Given a minimal support of a T-invariant, there is a unique minimal T-invariant corresponding to the minimal support; such an invariant is called a *minimal support T-invariant*. We denote the set of minimal support T-invariants of N as $\mathcal{T}(N)$.

It should be noted that T-invariants define potential cycles in the reachability set $R\,(N, \boldsymbol{m}_0)$.

Given a P/T net N, the set $\mathcal{T}(N)$ can be computed by means of the algorithm proposed in Silva, Teruel, and Colom (1992), which is based on simple computations on the incidence matrix $\boldsymbol{C}$, that are scaling and summing of matrix rows. It should be noticed that, in general, the number of T-invariants grows exponentially with n.

Definition 3 (*Consistency*)**.** A net N is *consistent* if there exists a vector $\boldsymbol{y} \in \mathbb{N}^n$, such that $\boldsymbol{y} > \boldsymbol{0}$ and $\boldsymbol{C} \cdot \boldsymbol{y} = \boldsymbol{0}$.

Remark 1. A net is consistent if and only if it is covered by T-invariants, that is for all $t \in T$ there exists a T-invariant $\boldsymbol{y}$ such that $t \in \mathrm{SUP}(\boldsymbol{y})$. □

Definition 4 (*Reversible Net System*)**.** A net system S is said to be *reversible* if for each marking $\boldsymbol{m} \in R\,(N, \boldsymbol{m}_0)$, $\boldsymbol{m}_0$ is reachable from $\boldsymbol{m}$.

If a net system $\langle N, \boldsymbol{m}_0 \rangle$ is reversible it does not imply the net N to be consistent. However, if the net system is reversible there exists at least one T-invariant.

The following results hold.

Theorem 5 (Murata, 1989)**.** *Given a live and bounded net system $S = \langle N, \boldsymbol{m}_0 \rangle$ the corresponding net N is consistent. As a consequence, a bounded live net is covered by T-invariants (see Remark 1).*

The set T can be partitioned into the two disjoint sets of *observable* (represented by empty boxes) and *unobservable* transitions (represented by filled boxes), named respectively T_o and T_{uo} with $\mathrm{card}(T_{uo}) = n_{uo} \leq n$, where $\mathrm{card}(T_{uo})$ denotes the cardinality of T_{uo}. Fault events $t \in T_f$ are supposed to be unobservable, i.e., $T_f \subseteq T_{uo}$, with $\mathrm{card}(T_f) = n_f \leq n_{uo}$.

Given a firing count vector $\boldsymbol{\sigma} \in \mathbb{N}^n$, in this paper we are often interested in considering only the firings of either the observable or the unobservable transitions. For this reason we introduce the following notations:

$$\boldsymbol{\sigma}_{|T_o} \in \mathbb{N}^n, \quad \text{with } \boldsymbol{\sigma}_{|T_o}(t) = \begin{cases} \boldsymbol{\sigma}(t) & \text{if } t \in T_o \\ 0 & \text{if } t \notin T_o \end{cases}$$

$$\boldsymbol{\sigma}_{|T_{uo}} \in \mathbb{N}^n, \quad \text{with } \boldsymbol{\sigma}_{|T_{uo}}(t) = \begin{cases} \boldsymbol{\sigma}(t) & \text{if } t \in T_{uo} \\ 0 & \text{if } t \notin T_{uo}. \end{cases}$$

It is straightforward that given a firing count vector $\boldsymbol{\sigma}$ it holds that $\boldsymbol{\sigma} = \boldsymbol{\sigma}_{|T_o} + \boldsymbol{\sigma}_{|T_{uo}}$.

Example 1. Let us consider the net shown in Fig. 1, with $T_o = \big\{t_1, t_4, t_5\big\}$ and $T_{uo} = \big\{t_2, t_3\big\}$. Given the firing count vector $\boldsymbol{\sigma} = \big[2\,0\,2\,0\,1\big]^T$ one has $\boldsymbol{\sigma}_{|T_o} = \big[2\,0\,0\,0\,1\big]^T$ and $\boldsymbol{\sigma}_{|T_{uo}} = \big[0\,0\,2\,0\,0\big]^T$. □

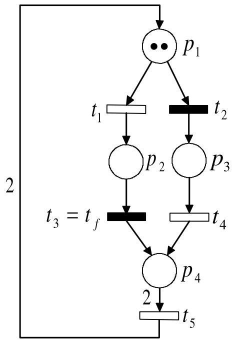

Fig. 1. Example net.

We now introduce the following definition of *unobservable explanations* of a given sequence σ enabled from the initial marking $\boldsymbol{m}_0$, which is related to the one given in Basile et al. (2009a).

Definition 6 (*Unobservable Explanation*)**.** Consider a net system $S = \langle N, \boldsymbol{m}_0 \rangle$ and a sequence $\sigma \in T^*$ such that $\boldsymbol{m}_0[\sigma\rangle$ and

$$\sigma = \sigma_{uo}^1 t_o^1 \sigma_{uo}^2 t_o^2 \cdots \sigma_{uo}^k t_o^k,$$

with $\sigma_{uo}^i \in T_{uo}^*$ and $t_o^i \in T_o,\ i = 1, \ldots, k$. The following set

$$\Sigma(N, \sigma) \triangleq \Big\{ \bar{\sigma} \in T_{uo}^* \mid \bar{\sigma} = \bar{\sigma}_{uo}^1 \bar{\sigma}_{uo}^2 \cdots \bar{\sigma}_{uo}^{k+1} \text{ and } \boldsymbol{m}_0[\bar{\sigma}_{uo}^1 t_o^1 \bar{\sigma}_{uo}^2 t_o^2 \cdots \bar{\sigma}_{uo}^k t_o^k \bar{\sigma}_{uo}^{k+1}\rangle \Big\},$$

contains the unobservable explanations of σ, and

$$\boldsymbol{\Sigma}(N, \sigma) \triangleq \Big\{ \bar{\boldsymbol{\sigma}} \in \mathbb{N}^n \text{ s.t. } \bar{\sigma} \in \Sigma(N, \sigma) \text{ and } \bar{\boldsymbol{\sigma}} = \pi(\bar{\sigma}) \Big\},$$

is the corresponding set of firing count vectors.

In simple words, the unobservable explanations of σ are all the sequences of unobservable transitions that can explain the firing of the observable transitions in σ. The notation $\Sigma(N, \sigma)$ makes clear the dependence of the unobservable explanations on the net structure.

Example 2. Given the net shown in Fig. 1, let

$$\sigma = t_1 t_2 t_4,$$

with $\boldsymbol{m}_0[\sigma\rangle$. Taking into account that the following sequences

$$\bar{\sigma}_1 = t_2 t_1 t_4, \qquad \bar{\sigma}_2 = t_1 t_3 t_2 t_4, \qquad \bar{\sigma}_3 = t_1 t_2 t_3 t_4,$$
$$\bar{\sigma}_4 = t_1 t_2 t_4 t_3, \qquad \bar{\sigma}_5 = t_2 t_1 t_3 t_4, \qquad \bar{\sigma}_6 = t_2 t_1 t_4 t_3,$$

are all enabled starting from $\boldsymbol{m}_0$, it follows that the set of unobservable explanations of σ is

$$\Sigma(N, \sigma) = \{t_2, t_3 t_2, t_2 t_3\},$$

and

$$\boldsymbol{\Sigma}(N, \sigma) = \Big\{ [0\,1\,0\,0\,0]^T, [0\,1\,1\,0\,0]^T \Big\}. \quad \square$$

2.2. Diagnosability and $\mathcal{K}$-diagnosability

The assumption stated below will be exploited throughout the paper in order to assure that after a fault occurrence the net does not enter a deadlock, which could prevent the diagnosis of the fault itself. To this purpose, liveness of the net system is commonly assumed when dealing with the diagnosability of DES; however we prefer to rely on the following and less conservative assumption, as has been done in Cabasino et al. (2009a,b).

Assumption 1. The net system $S = \langle N, \boldsymbol{m}_0 \rangle$ does not enter a deadlock after firing any fault transition. □

Let us now extend to the Petri nets the classical definition of diagnosability for DES given in the seminal work Sampath et al. (1995). Without loss of generality we will focus our attention on the diagnosability of a single fault t_f, rather than on diagnosability of class of faults.

Consider a net system $\langle N, \boldsymbol{m}_0\rangle$ with $T = T_{uo} \cup T_o$, and $T_f \subseteq T_{uo}$. Let L be the live and prefix-close language generated by $\langle N, \boldsymbol{m}_0\rangle$. We denote by L/σ the post-language of L after the sequence of transitions σ, i.e.

$$L/\sigma = \{v \in T^* \text{ s.t. } \sigma v \in L\}.$$

A sequence $v \in L/\sigma$ is called *continuation* of σ.

Denoting by $\Pr : T^* \mapsto T_o^*$ the natural projection which "erases" the unobservable transitions in a sequence σ, it is also possible to define the inverse projection operator extended to the language L as follows (see also Cassandras & Lafortune, 1999, p. 58)

$$\Pr_L^{-1}(r) = \{\sigma \in L \text{ s.t. } \Pr(\sigma) = r\}.$$

The following definition of diagnosability can be now given.

Definition 7 (*Diagnosable Fault*). A fault transition $t_f \in T_f$ is said to be diagnosable if

$\exists\, h \in \mathbb{N}$ such that

$\forall\, \sigma = ut_f$ with $t_f \notin u$, and $\forall\, v \in L/\sigma$ with $|v| \geq h$,

it is

$r \in \Pr_L^{-1}(\Pr(\sigma v)) \Rightarrow t_f \in r$. □

The above definition of diagnosability of a fault can be explained as follows. Let $\sigma = ut_f$ be any sequence generated by the system that ends in a failure event t_f, and let v be any sufficiently long continuation of σ. Diagnosability of t_f implies that along every continuation v of σ it is possible to detect the occurrence of the fault with a finite delay.

Given a fault t_f and a positive integer $\mathcal{K}$, it is now possible to give the following definition of $\mathcal{K}$-diagnosable fault t_f, which turns out to be a *practical* notion of diagnosability.

Definition 8 ($\mathcal{K}$*-Diagnosable Fault*). Given $t_f \in T_f$ and $\mathcal{K} \in \mathbb{N}$, t_f is said to be $\mathcal{K}$-diagnosable if

$\forall\, \sigma = ut_f$ with $t_f \notin u$ and $\forall\, v \in L/\sigma$ such that $|v| \geq \mathcal{K}$,

it is

$$r \in \Pr_L^{-1}(\Pr(\sigma v)) \Rightarrow t_f \in r. \quad \square \tag{3}$$

If $\sigma = ut_f$ is any sequence generated by the system that ends in a failure event t_f, then $\mathcal{K}$-diagnosability of t_f implies that it is possible to detect its occurrence within a finite delay, specifically after the firing of at most $\mathcal{K}$ transitions after its occurrence. Indeed, given an integer $\mathcal{K}$, condition (3) must be satisfied for all the continuations v of σ which contain at least $\mathcal{K}$ transitions. The definition of $\mathcal{K}$-diagnosability follows straightforwardly from the original definition given in Sampath et al. (1995).

It is worth noticing that while diagnosability requires the existence of an upper bound for the continuation of σ, $\mathcal{K}$-diagnosability specifies a *quantitative* bound for the number of events in the continuation of σ. It turns out that with $\mathcal{K}$-diagnosability it is possible to specify an upper bound for the number of events that are needed to detect a fault. In this sense we claim that $\mathcal{K}$-diagnosability is a *practical* diagnosability.

Indeed, given an integer $\mathcal{K}$, $\mathcal{K}$-diagnosability of a fault always implies its diagnosability, while the converse is not necessarily true. However, by definition, it follows that if a fault transition is diagnosable then there exists an integer $\bar{\mathcal{K}}$ such that it is also $\bar{\mathcal{K}}$-diagnosable.

Example 3. For the net in Fig. 1 let $t_3 \in T_f$ and consider the sequence $\sigma = t_1t_3$, i.e., σ is a sequence that ends with the fault transition t_3. Given the definition of $\mathcal{K}$-diagnosability, it turns out that t_3 is not 2-diagnosable. Indeed $v = t_2t_4$ belongs to the post-language L/σ with

$$\Pr(t_1t_3t_2t_4) = t_1t_4,$$

and $t_1t_2t_4 \in \Pr_L^{-1}(\Pr(\sigma v))$, with $t_3 \notin t_1t_2t_4$. Hence there exists one sequence σ that ends with t_3 and one sequence $v \in L/\sigma$ with $|v| = 2$, such that

$$r \in \Pr^{-1}(\Pr(\sigma v)) \nRightarrow t_3 \in r,$$

which, by definition, implies that t_3 cannot be 2-diagnosable. Exploiting similar arguments and by exhaustively searching for all possibilities, it follows that t_3 is 3-diagnosable. □

3. $\mathcal{K}$-diagnosability of unlabeled nets

The main result presented in this section is a necessary and sufficient condition for $\mathcal{K}$-diagnosability of a fault in unlabeled and bounded net systems. The proposed result is provided as the solution of an ILP problem. Before presenting the main contribution, we first informally discuss the adopted approach.

In order to check either the diagnosability or the $\mathcal{K}$-diagnosability of the fault transition t_f, we first need to characterize all markings reachable from $\boldsymbol{m}_0$ that enable t_f, and which are reached by the firing of a sequence that does not contain t_f. In the following we denote the set of these markings as

$$\mathcal{M}(t_f) = \left\{\boldsymbol{m} \in \mathbb{N}^m \mid \Big(\boldsymbol{m}_0[u\rangle\boldsymbol{m}\Big) \bigwedge \Big(t_f \notin u\Big) \bigwedge \Big(\boldsymbol{m}[t_f\rangle\Big)\right\}$$

where $\bigwedge$ denotes the logical *and* operator. Furthermore, given a marking $\boldsymbol{m} \in \mathcal{M}(t_f)$, in order to check $\mathcal{K}$-diagnosability of t_f we need to characterize all the possible continuations of the sequence ut_f holding at least $\mathcal{K}$ firings. In particular, we are interested in the sequences that belong to the set

$$\mathcal{S}(t_f, \mathcal{K}) = \left\{\sigma \in T^* \mid \Big(\sigma = ut_fv\Big) \bigwedge \Big(\boldsymbol{m}_0[\sigma\rangle\Big) \bigwedge \Big(\boldsymbol{m}_0[u\rangle\boldsymbol{m}\Big) \bigwedge \Big(\boldsymbol{m} \in \mathcal{M}(t_f)\Big) \bigwedge \Big(|v| \geq \mathcal{K}\Big)\right\}.$$

Once we have obtained the sequences in $\mathcal{S}(t_f, \mathcal{K})$, it is sufficient to check if the fault t_f belongs to all their unobservable explanations (see Definition 6): if this is the case then t_f is $\mathcal{K}$-diagnosable, otherwise it is not.

It is important to remark that the proposed approach relies on the characterization of the two sets $\mathcal{M}(t_f)$ and $\mathcal{S}(t_f, \mathcal{K})$ by means of linear constraints, as it will be shown in Section 3.1. Hence the explicit computation of these sets is not required.

Although the definition of the enabling markings set $\mathcal{M}(t_f)$ may resemble the definition of border forbidden states set given in Dideban and Alla (2008), the two concepts are different. Indeed, a border forbidden state is a forbidden marking that is adjacent to a legal marking in the reachability graph of a net. This concept is used to reduce the number of constraints, and hence the number of control places, when dealing with supervisory control. Given a fault t_f, the enabling markings set $\mathcal{M}(t_f)$ holds all the markings that enable t_f and are reached without its firing. In this paper we consider the set $\mathcal{M}(t_f)$ since it holds the firing count vectors leading to these markings starting from $\boldsymbol{m}_0$.

3.1. Preliminary results

Exploiting Lemma 1, it is now possible to introduce the following two lemmas that will be then exploited to state the main result of this section.

Lemma 2. *Consider a net system $S = \langle N, \boldsymbol{m}_0\rangle$ a transition $t \in T$ and a positive integer $\mathcal{K}$. There exists at least one sequence $\sigma = ut\upsilon$, with $\boldsymbol{v} = \pi(\upsilon)$, such that conditions*

$$\boldsymbol{m}_0[\sigma\rangle \tag{4a}$$

$$t \notin u \tag{4b}$$

$$\|\boldsymbol{v}\|_1 \geq \mathcal{K} \tag{4c}$$

are satisfied if and only if *there exist an integer $\mathcal{J}$ and $\mathcal{J} + \mathcal{K}$ vectors $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{\mathcal{J}}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{\mathcal{K}} \in \mathbb{N}^n$ that fulfill the following set of constraints denoted by $\mathcal{F}\big(\boldsymbol{m}_0, t, \mathcal{J}, \mathcal{K}\big)$*

$$\begin{cases}
\boldsymbol{m}_0 \geq \mathbf{Pre} \cdot \boldsymbol{u}_1 & \\
\boldsymbol{m}_0 + \boldsymbol{C} \cdot \boldsymbol{u}_1 \geq \mathbf{Pre} \cdot \boldsymbol{u}_2 & \\
\ldots & \text{(a)} \\
\boldsymbol{m}_0 + \boldsymbol{C} \cdot \displaystyle\sum_{i=1}^{\mathcal{J}-1} \boldsymbol{u}_i \geq \mathbf{Pre} \cdot \boldsymbol{u}_{\mathcal{J}} & \\
\boldsymbol{m}_0 + \boldsymbol{C} \cdot \displaystyle\sum_{i=1}^{\mathcal{J}} \boldsymbol{u}_i \geq \mathbf{Pre}\big(\cdot, t\big) & \text{(b)} \\
\boldsymbol{m}_0 + \boldsymbol{C} \cdot \displaystyle\sum_{i=1}^{\mathcal{J}} \boldsymbol{u}_i + \boldsymbol{C}\big(\cdot, t\big) \geq \mathbf{Pre} \cdot \boldsymbol{v}_1 & \\
\boldsymbol{m}_0 + \boldsymbol{C} \cdot \displaystyle\sum_{i=1}^{\mathcal{J}} \boldsymbol{u}_i + \boldsymbol{C}\big(\cdot, t\big) + \boldsymbol{C} \cdot \boldsymbol{v}_1 \geq \mathbf{Pre} \cdot \boldsymbol{v}_2 & \\
\ldots & \text{(c)} \\
\boldsymbol{m}_0 + \boldsymbol{C} \cdot \displaystyle\sum_{i=1}^{\mathcal{J}} \boldsymbol{u}_i + \boldsymbol{C}\big(\cdot, t\big) + \boldsymbol{C} \cdot \displaystyle\sum_{j=1}^{\mathcal{K}-1} \boldsymbol{v}_j \geq \mathbf{Pre} \cdot \boldsymbol{v}_{\mathcal{K}} & \\
\displaystyle\sum_{i=1}^{\mathcal{J}} \boldsymbol{u}(t) = 0 & \text{(d)} \\
\left\| \displaystyle\sum_{j=1}^{\mathcal{K}} \boldsymbol{v}_j \right\|_1 \geq \mathcal{K}. & \text{(e)}
\end{cases} \tag{5}$$

Proof. The proof readily follows from Lemma 1 by noting that constraints (5)(a), (b), and (d) are fulfilled if and only if there exist at least one sequence ut that is enabled from $\boldsymbol{m}_0$ and which satisfies condition (4b). Similarly, the continuation υ of ut satisfies (4c) if and only if constraints (5)(c) and (e) are fulfilled. □

Given a fault transition t_f, the set of constraints $\mathcal{F}\big(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\big)$ fully characterize the two sets $\mathcal{M}(t_f)$ and $\mathcal{S}(t_f, \mathcal{K})$. Indeed, constraints (5)(a), (b), and (d) imply that

$$\boldsymbol{m} = \boldsymbol{m}_0 + \boldsymbol{C} \cdot \sum_{i=1}^{\mathcal{J}} \boldsymbol{u}_i$$

belongs to $\mathcal{M}(t_f)$, and the firing count vector

$$\boldsymbol{u} = \sum_{i=1}^{\mathcal{J}} \boldsymbol{u}_i$$

corresponds to at least one sequence enabled from $\boldsymbol{m}_0$, which does not contain the fault t_f, and whose firing enables t_f.

Similarly, if the firing count vectors $\boldsymbol{u}_i$ and $\boldsymbol{v}_j$ fulfill the constraints (5)(c) and (e), then there is at least one sequence $\sigma = ut_f\upsilon$ that belongs to $\mathcal{S}(t_f, \mathcal{K})$, with $\pi(u) = \sum_{i=1}^{\mathcal{J}} \boldsymbol{u}_i$, and $\pi(\upsilon) = \sum_{j=1}^{\mathcal{K}} \boldsymbol{v}_j$.

Remark 2. It is important to note that constraints $\mathcal{F}\big(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\big)$ depend on the integer $\mathcal{J}$. The value of $\mathcal{J}$ implicitly defines the maximum length of the sequence u that yields a generic marking in $\mathcal{M}(t_f)$. Given a value $\mathcal{J}$, there may exist at least one marking $\widetilde{\boldsymbol{m}} \in \mathcal{M}(t_f)$ that does not satisfy (5). Nevertheless, $\widetilde{\boldsymbol{m}}$ could enable t_f, and starting from $\widetilde{\boldsymbol{m}}$ the fault may be undiagnosable in $\mathcal{K}$ steps.

It turns out that it is important to estimate the minimum value $\mathcal{J}_{\min}$ that permits to fully describe the set $\mathcal{M}(t_f)$. Furthermore, for unbounded net systems, $\mathcal{J}_{\min}$ could not exist. For this reason, in Section 3.2 we will assume that the net system is bounded in order to state a necessary and sufficient condition for $\mathcal{K}$-diagnosability.

In general the computation of $\mathcal{J}_{\min}$ is not an easy task, even in the case of bounded net systems. In the worst case an overestimation of $\mathcal{J}_{\min}$ is given by $\text{card}\Big(R\big(N, \boldsymbol{m}_0\big)\Big) - 1$.

Two results are presented next. The former can be exploited to estimate an upper bound for $\mathcal{J}_{\min}$, while the latter permits to check if, for a given integer $\mathcal{J}$ it holds $\mathcal{J} \geq \mathcal{J}_{\min}$, as it will be shown in Section 5. □

Theorem 9. *Given a live and bounded net system $\mathcal{S} = \langle N, \boldsymbol{m}_0\rangle$ an upper bound for $\mathcal{J}_{\min}$ is given by*

$$\mathcal{J}_{\min} \leq 2 \cdot \|\boldsymbol{m}_0\|_1 \cdot \left\| \sum_{\boldsymbol{y} \in \mathcal{T}(N)} \boldsymbol{y} \right\|_1 . \tag{6}$$

Proof. We first suppose the net system $\mathcal{S}$ is reversible, and we will remove this additional assumption later in this proof.

Since we are interested in an upper bound for $\mathcal{J}_{\min}$, we suppose that concurrence cannot be exploited; hence only a single transition is enabled under each reachable marking.

The main idea exploited in this proof is to *follow* each token belonging to $\boldsymbol{m}_0$ along the *longest* possible trajectory in the state space. Denote with $\widehat{\sigma} = t^1 t^2 \cdots t^k$ such a *longest* sequence, with $\widehat{\boldsymbol{\sigma}} = \pi(\widehat{\sigma})$, and

$$\boldsymbol{m}_0[t^1\rangle \boldsymbol{m}_1[t^2\rangle \boldsymbol{m}_2 \cdots \boldsymbol{m}_{k-1}[t^k\rangle \widehat{\boldsymbol{m}},$$

where the markings $\boldsymbol{m}_0, \boldsymbol{m}_1, \boldsymbol{m}_{k-1}, \widehat{\boldsymbol{m}}$ are all different, and k is the biggest as possible. It turns out that $\widehat{\boldsymbol{m}}$ is the *farthest* marking that can be reached from $\boldsymbol{m}_0$ by firing the maximum number of transitions and without reaching two times the same intermediate marking.

Liveness of $\mathcal{S}$ implies that N can be covered by the single T-invariant given by (see Remark 1)

$$\widehat{\boldsymbol{y}} = \sum_{\boldsymbol{y} \in \mathcal{T}(N)} \boldsymbol{y}.$$

We now show that $\widehat{\boldsymbol{\sigma}} \lneq \widehat{\boldsymbol{y}}$. First note that $\widehat{\boldsymbol{\sigma}}$ cannot be equal to $\widehat{\boldsymbol{y}}$ otherwise $\widehat{\boldsymbol{m}} = \boldsymbol{m}_0$. Suppose now, *ad absurdum*, that

$$\exists\, t \in T \quad \text{s.t.}\ \widehat{\boldsymbol{\sigma}}(t) > \widehat{\boldsymbol{y}}(t).$$

Since the net system is reversible, by definition there exists a transition t' whose firing after $\widehat{\sigma}$ yields the marking $\boldsymbol{m}_0$. It readily follows that the corresponding firing count vector $\pi(\widehat{\sigma}t')$, corresponds to a T-invariant and it would have at least one component greater than $\widehat{\boldsymbol{y}}$, which is not possible. Hence $\widehat{\boldsymbol{\sigma}} \lneq \widehat{\boldsymbol{y}}$, and since we have assumed that concurrency cannot be exploited, it follows that an upper bound for the number of transitions that need to be fired in order to bring all the tokens from the initial marking to the *farthest* one is given by

$$\|\boldsymbol{m}_0\|_1 \cdot \|\widehat{\boldsymbol{y}}\|_1 = \|\boldsymbol{m}_0\|_1 \cdot \left\| \sum_{\boldsymbol{y} \in \mathcal{T}(N)} \boldsymbol{y} \right\|_1 . \tag{7}$$

Let now remove the reversibility assumption. If the net system is not reversible, in the reachability graph there is at least one live ergodic component (see Definition 1). Let us denote with $\tilde{\sigma} \in T^*$, and $\tilde{\boldsymbol{\sigma}} = \pi(\tilde{\sigma})$ the *longest* possible sequence that *follows* a single token from $\boldsymbol{m}_0$ to a marking $\widetilde{\boldsymbol{m}}$ belonging to a live ergodic component. The sequence $\tilde{\sigma}$ and the marking $\widetilde{\boldsymbol{m}}$ are such that $\boldsymbol{m}_0[\tilde{\sigma}\rangle\widetilde{\boldsymbol{m}}$ and

$$\nexists\, \tilde{\sigma}' \in T^* \quad \text{s.t. } \tilde{\boldsymbol{\sigma}}' \lneq \tilde{\boldsymbol{\sigma}} \wedge \boldsymbol{m}_0[\tilde{\sigma}'\rangle\widetilde{\boldsymbol{m}},$$

with $\tilde{\boldsymbol{\sigma}}' = \pi(\tilde{\sigma}')$.

Suppose, *ad absurdum*, that

$$\exists\, t \in T \quad \text{s.t. } \tilde{\boldsymbol{\sigma}}(t) > \hat{\boldsymbol{y}}(t). \tag{8}$$

After the firing of $\tilde{\sigma}$ the net reaches $\widetilde{\boldsymbol{m}}$; since the net is supposed to be live, starting from $\widetilde{\boldsymbol{m}}$ the sequence corresponding to $\hat{\boldsymbol{y}}$ can fire infinitely. If (8) holds then the number of firings of t needed to reach again $\widetilde{\boldsymbol{m}}$ starting from $\widetilde{\boldsymbol{m}}$ is smaller in the sequence corresponding to $\hat{\boldsymbol{y}}$ rather than in $\tilde{\sigma}$.

It follows that there should be at least one transition t^* in $\tilde{\sigma}$ whose firing reduces the number of tokens. Since the net is live and $\hat{\boldsymbol{y}}$ covers the net, t^* can fire infinitely from $\widetilde{\boldsymbol{m}}$, making it possible to reduce the number of tokens. However, since the net is bounded, this implies that the net is not live, which contradicts the liveness assumption. Hence, it is

$$\tilde{\boldsymbol{\sigma}} \lneq \hat{\boldsymbol{y}}.$$

Exploiting the same arguments as in the case of reversible net, it follows that an upper bound for the number of transitions that need to be fired in order to bring all the tokens from the initial marking to $\widetilde{\boldsymbol{m}}$ is given by (7); hence, for nonreversible live and bounded nets the upper bound for $J_{\min}$ is given by (6). □

The following feasibility problem exploits Theorem 9 and PNs concurrency to check if a given $\mathcal{J} \in \mathbb{N} \geq \mathcal{J}_{\min}$.

Feasibility problem 1. *Given a live and bounded net system* $S = \langle N, \boldsymbol{m}_0\rangle$ *and* $\mathcal{J} \in \mathbb{N}$, *let*

$$\widehat{\boldsymbol{y}} = \sum_{\boldsymbol{y} \in \mathcal{T}(N)} \boldsymbol{y}.$$

If the following set of integer inequalities

$$\boldsymbol{m}_0 \geq \mathbf{Pre} \cdot \boldsymbol{u}_1 \tag{9a}$$

$$\boldsymbol{m}_0 + \boldsymbol{C} \cdot \boldsymbol{u}_1 \geq \mathbf{Pre} \cdot \boldsymbol{u}_2 \tag{9b}$$

$$\dots$$

$$\boldsymbol{m}_0 + \boldsymbol{C} \cdot \sum_{i=1}^{\mathcal{J}-1} \boldsymbol{u}_i \geq \mathbf{Pre} \cdot \boldsymbol{u}_{\mathcal{J}} \tag{9c}$$

$$\sum_{i=1}^{\mathcal{J}} \boldsymbol{u}_i \geq 2 \cdot \|\boldsymbol{m}_0\|_1 \cdot \hat{\boldsymbol{y}} \tag{9d}$$

admits a solution $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_{\mathcal{J}} \in \mathbb{N}^n$, *then* $\mathcal{J} \geq \mathcal{J}_{\min}$.

Remark 3. The dependency of $\mathcal{J}_{\min}$ from $\|\boldsymbol{m}_0\|_1$ is a consequence of the dependency on the cardinality of the reachability set. In the worst case, $\mathcal{J}_{\min}$ may increase exponentially with respect to the number of tokens in $\boldsymbol{m}_0$. However, the Feasibility problem 1 allows to exploit the net concurrency as shown in Example 7. □

Given a sequence σ and the firing count vector $\boldsymbol{b}$ corresponding to the observable transitions in σ, the next lemma introduces a set of linear constraints that must be fulfilled by a set of firing count vectors corresponding to the unobservable explanations of $\boldsymbol{b}$. This result will be exploited in Section 3.2 to compute the firing count vectors corresponding to the unobservable explanations of the sequences that fulfill constraints (5); these firing count vectors are then used to perform the $\mathcal{K}$-diagnosability test.

Lemma 3. *Consider a net system* $S = \langle N, \boldsymbol{m}_0\rangle$ *and a sequence* σ *enabled under the initial marking* $\boldsymbol{m}_0$. *The sequence* σ *is such that*

$$\pi\Big(\Pr(\sigma)\Big) = \boldsymbol{b},$$

if and only if there exist 2ρ *vectors* $\boldsymbol{s}_1, \dots, \boldsymbol{s}_\rho, \boldsymbol{\epsilon}_1, \dots, \boldsymbol{\epsilon}_\rho \in \mathbb{N}^n$, *with* $\rho \leq \|\sigma\|$, *that fulfill the following set of constraints denoted by* $\mathcal{E}\big(\boldsymbol{m}_0, \boldsymbol{b}\big)$

$$\begin{cases} \boldsymbol{m}_0 + \boldsymbol{C} \cdot \boldsymbol{\epsilon}_{1|T_{uo}} \geq \mathbf{Pre} \cdot \boldsymbol{s}_{1|T_o} \\ \boldsymbol{m}_0 + \boldsymbol{C} \cdot \sum_{i=1}^{2} \boldsymbol{\epsilon}_{i|T_{uo}} + \boldsymbol{C} \cdot \boldsymbol{s}_{1|T_o} \geq \mathbf{Pre} \cdot \boldsymbol{s}_{2|T_o} \\ \dots & \text{(a)} \\ \boldsymbol{m}_0 + \boldsymbol{C} \cdot \sum_{i=1}^{\rho} \boldsymbol{\epsilon}_{i|T_{uo}} + \boldsymbol{C} \cdot \sum_{j=1}^{\rho-1} \boldsymbol{s}_{j|T_o} \geq \mathbf{Pre} \cdot \boldsymbol{s}_{\rho|T_o} \\ \boldsymbol{m}_0 \geq \mathbf{Pre} \cdot \boldsymbol{\epsilon}_{1|T_{uo}} \\ \boldsymbol{m}_0 + \boldsymbol{C} \cdot \left(\boldsymbol{\epsilon}_{1|T_{uo}} + \boldsymbol{s}_{1|T_o}\right) \geq \mathbf{Pre} \cdot \boldsymbol{\epsilon}_{2|T_{uo}} \\ \dots & \text{(b)} \\ \boldsymbol{m}_0 + \boldsymbol{C} \cdot \sum_{i=1}^{\rho-1} \left(\boldsymbol{\epsilon}_{i|T_{uo}} + \boldsymbol{s}_{i|T_o}\right) \geq \mathbf{Pre} \cdot \boldsymbol{\epsilon}_{\rho|T_{uo}} \\ \sum_{i=1}^{\rho} \boldsymbol{s}_{i|T_o} = \boldsymbol{b}. & \text{(c)} \end{cases} \tag{10}$$

Proof. The proof readily follows from Lemma 1 when the transitions set is partitioned in the observable and unobservable transitions subsets. □

3.2. Main result

Now it is possible to exploit both Lemmas 2 and 3 to state the main contribution of this section.

Let first introduce a sufficient condition for $\mathcal{K}$-undiagnosability which holds for both bounded and unbounded unlabeled net systems.

Theorem 10. *Given a net system* $S = \langle N, \boldsymbol{m}_0\rangle$ *a fault transition* t_f, *and a positive integer* $\mathcal{K}$, *if there exist at least one* $\mathcal{J} \in \mathbb{N}$, $\mathcal{J} > 0$ *and* $3\big(\mathcal{J} + \mathcal{K}\big)$ *vectors* $\boldsymbol{u}_1, \dots, \boldsymbol{u}_{\mathcal{J}}, \boldsymbol{v}_1, \dots, \boldsymbol{v}_{\mathcal{K}}, \boldsymbol{\epsilon}_1, \dots, \boldsymbol{\epsilon}_{\mathcal{J}+\mathcal{K}}, \boldsymbol{s}_1, \dots, \boldsymbol{s}_{\mathcal{J}+\mathcal{K}} \in \mathbb{N}^n$ *such that*

$$\min_{\text{s.t. } \mathcal{D}\left(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\right)} \sum_{r=1}^{\mathcal{J}+\mathcal{K}} \boldsymbol{\epsilon}_r(t_f) = 0,$$

where the set of constraints $\mathcal{D}\big(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\big)$ *is equal to*

$$\mathcal{D}\big(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\big) : \begin{cases} \mathcal{F}\big(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\big) & \text{(a)} \\ \mathcal{E}\left(\boldsymbol{m}_0, \sum_{i=1}^{\mathcal{J}} \boldsymbol{u}_{i|T_o} + \sum_{j=1}^{\mathcal{K}} \boldsymbol{v}_{j|T_o}\right) & \text{(b)} \\ \boldsymbol{s}_{1|T_o} = \boldsymbol{u}_{1|T_o} \\ \dots \\ \boldsymbol{s}_{\mathcal{J}|T_o} = \boldsymbol{u}_{\mathcal{J}|T_o} \\ \boldsymbol{s}_{\mathcal{J}+1|T_o} = \boldsymbol{v}_{1|T_o} & \text{(c)} \\ \dots \\ \boldsymbol{s}_{\mathcal{J}+\mathcal{K}|T_o} = \boldsymbol{v}_{\mathcal{K}|T_o} \end{cases} \tag{11}$$

then t_f *is* $\mathcal{K}$*-undiagnosable.*

Proof. From Lemmas 2 and 3, it follows that if there is at least one positive integer $\mathcal{J}$ and a set of vectors $\boldsymbol{\epsilon}_1, \dots, \boldsymbol{\epsilon}_{\mathcal{J}+\mathcal{K}}$ such that constraints (11) are fulfilled, then $\sum_{r=1}^{\mathcal{J}+\mathcal{K}} \boldsymbol{\epsilon}_r$ represents the unobservable explanation of a sequence $\sigma = ut_f v$ with $t_f \notin u$.

If one has

$$\min_{\text{s.t. } \mathcal{D}\left(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\right)} \sum_{r=1}^{\mathcal{J}+\mathcal{K}} \boldsymbol{\epsilon}_r(t_f) = 0,$$

then it means that there is at least one continuation v of ut_f such that $\|v\| \geq \mathcal{K}$ and such that the unobservable explanation of $\Pr(ut_f v)$ does not include the fault t_f. Hence t_f is $\mathcal{K}$-undiagnosable. □

The additional constraints (11)(c) in $\mathcal{D}\left(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\right)$ are congruence conditions used to link the constraints $\mathcal{F}\left(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\right)$, which return the firing count vectors of the sequences $\sigma = ut_f v$, to the constraints $\mathcal{E}\left(\boldsymbol{m}_0, \sum_{i=1}^{\mathcal{J}} \boldsymbol{u}_{i|T_o} + \sum_{j=1}^{\mathcal{K}} \boldsymbol{v}_{j|T_o}\right)$, which return the firing count vectors of the unobservable explanations of σ. Indeed, constraints (11)(c) imply the fulfilling of condition (10)(c) in $\mathcal{E}\left(\boldsymbol{m}_0, \sum_{i=1}^{\mathcal{J}} \boldsymbol{u}_{i|T_o} + \sum_{j=1}^{\mathcal{K}} \boldsymbol{v}_{j|T_o}\right)$.

The following theorem is the main contribution of this section and it states a necessary and sufficient condition for $\mathcal{K}$-diagnosability of unlabeled and bounded net systems.

Theorem 11. *Consider a bounded net system $S = \langle N, \boldsymbol{m}_0\rangle$ and a fault transition t_f, let $\mathcal{J}$ be a positive integer such that $\mathcal{J} \geq \mathcal{J}_{\min}$. Given a positive integer $\mathcal{K}$, t_f is $\mathcal{K}$-diagnosable* if and only if *there exist $3\left(\mathcal{J} + \mathcal{K}\right)$ vectors $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{\mathcal{J}}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{\mathcal{K}}, \boldsymbol{\epsilon}_1, \ldots, \boldsymbol{\epsilon}_{\mathcal{J}+\mathcal{K}}, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{\mathcal{J}+\mathcal{K}} \in \mathbb{N}^n$ such that*

$$\min_{\text{s.t. } \mathcal{D}\left(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\right)} \sum_{r=1}^{\mathcal{J}+\mathcal{K}} \boldsymbol{\epsilon}_r(t_f) \neq 0.$$

Proof (*If*). From Lemmas 2 and 3, it follows that if a set of vectors $\boldsymbol{\epsilon}_1, \ldots, \boldsymbol{\epsilon}_{\mathcal{J}+\mathcal{K}}$ fulfill constraints (11), then $\sum_{r=1}^{\mathcal{J}+\mathcal{K}} \boldsymbol{\epsilon}_r$ is the firing count vector corresponding to an unobservable explanation of a sequence $\sigma = ut_f v$ with $t_f \notin u$.

Since it is $\mathcal{J} \geq \mathcal{J}_{\min}$, then the constraints (5) describe the whole set $\mathcal{M}(t_f)$. Note that the net system is assumed to be bounded, implying the existence of the integer $\mathcal{J}_{\min}$ (see Remark 2). It follows that, if

$$\min_{\text{s.t. } \mathcal{D}\left(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\right)} \sum_{r=1}^{\mathcal{J}+\mathcal{K}} \boldsymbol{\epsilon}_r(t_f) \neq 0,$$

then the fault t_f belongs to all the unobservable explanations of all the faulty sequences $\sigma = ut_f v$, such that the postfix after the fault t_f contains at least $\mathcal{K}$ transitions after t_f. Hence if $\min_{\text{s.t. } \mathcal{D}\left(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\right)} \sum_{r=1}^{\mathcal{J}+\mathcal{K}} \boldsymbol{\epsilon}_r(t_f) \neq 0$ then t_f is $\mathcal{K}$-diagnosable.

(only if) Let suppose t_f $\mathcal{K}$-diagnosable. It follows that, by definition, t_f belongs to all the unobservable explanations of all the sequences $ut_f v$ such that $t_f \notin u$ and $\|v\| \geq \mathcal{K}$.

Let now suppose, *ad absurdum* that

$$\min_{\text{s.t. } \mathcal{D}\left(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\right)} \sum_{r=1}^{\mathcal{J}+\mathcal{K}} \boldsymbol{\epsilon}_r(t_f) = 0,$$

then there should exist at least one unobservable explanation of a faulty sequence $ut_f v$, such that $\|v\| \geq \mathcal{K}$ and that does not contain t_f. This implies that t_f is not $\mathcal{K}$-diagnosable, which contradicts the initial hypothesis. □

Note that in Theorem 10 it is not required that $\mathcal{J} \geq \mathcal{J}_{\min}$ (see Remark 2), since to check $\mathcal{K}$-undiagnosability of a fault it suffices that there is at least one unobservable explanation of a faulty sequence $ut_f v$, with $\|v\| \geq \mathcal{K}$, that does not hold the fault t_f. Whereas, in Theorem 11 it is required that $\mathcal{J} \geq \mathcal{J}_{\min}$, since in order to state a necessary and sufficient condition for $\mathcal{K}$-diagnosability of a fault, the ILP problem

$$\min_{\text{s.t. } \mathcal{D}\left(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\right)} \sum_{r=1}^{\mathcal{J}+\mathcal{K}} \boldsymbol{\epsilon}_r(t_f)$$

must be solved over all the possible sequences $ut_f v$ with $u \in \mathcal{M}(t_f)$.

In the case of bounded and live net systems, the diagnosability can be verified by checking the $\mathcal{K}$-diagnosability and letting $\mathcal{K} = \text{card}\left(R\left(N, \boldsymbol{m}_0\right)\right)$. Although this is a possible approach to check diagnosability, it may lead to an unacceptable increase of the computational burden, as soon as the cardinality of the reachability set becomes considerable. Furthermore, being $\mathcal{K}$-diagnosable for a large value of $\mathcal{K}$ could mean to be *practically undiagnosable*, that is when the cardinality of the reachability set is high, it is practically required to be $\mathcal{K}$-diagnosable for $\mathcal{K} \lll \text{card}\left(R\left(N, \boldsymbol{m}_0\right)\right)$. Given a diagnosable transition, the minimum $\bar{\mathcal{K}}$ such that the transition is $\bar{\mathcal{K}}$-diagnosable can be computed exploiting Theorem 11 by means of a binary search on $\mathcal{K}$, starting from $\mathcal{K} = \text{card}\left(R\left(N, \boldsymbol{m}_0\right)\right)/2$.

Assumption 1 guarantees that the ILP problems in Theorems 10 and 11 are always feasible. If Assumption 1 is not fulfilled it means that either the given fault is not enabled under the initial marking, or that the system enters a deadlock before the occurred fault can be detected. In the latest case the fault is not diagnosable.

We now briefly discuss the complexity of the proposed approach to check $\mathcal{K}$-diagnosability of a fault transition for a given integer $\mathcal{K}$. In the following the complexity is given in terms of number of unknowns and constraints of the ILP problem to be solved. However, it should be noticed that it is well known that the ILP problem is an NP-hard problem itself.

Let us first assume that the integer $\mathcal{J}$ is given; it readily follows that the number of unknowns in $\mathcal{F}\left(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\right)$ is equal to

$$\#\text{unknowns}_{\mathcal{F}} = (\mathcal{J} + \mathcal{K}) \cdot n,$$

while the correspondent number of constraints is

$$\#\text{constraints}_{\mathcal{F}} = (\mathcal{J} + \mathcal{K} + 2) \cdot m + 1.$$

When dealing with the set of constraints $\mathcal{E}(\cdot, \cdot, \cdot)$ it should be noticed that the unknowns in each $\boldsymbol{\epsilon}_i$ vector are the n_{uo} components related to the unobservable transitions, while in each $\boldsymbol{s}_i$ vector the unknowns are the $n - n_{uo}$ observable components. Moreover, thanks to the constraints (11)(c), the latest unknowns are fictitious, thus

$$\#\text{unknowns}_{\mathcal{E}} = (\mathcal{J} + \mathcal{K}) \cdot n_{uo},$$

and

$$\#\text{constraints}_{\mathcal{E}} = [2 \cdot (\mathcal{J} + \mathcal{K}) + 1] \cdot m.$$

It turns out that the overall number of unknowns is

$$\#\text{unknowns} = (\mathcal{J} + \mathcal{K}) \cdot (n + n_{uo}) < 2n\mathcal{J} + 2n\mathcal{K},$$

while the total number of constraints is

$$\#\text{constraints} = 3m\mathcal{J} + 3m\mathcal{K} + 3m + 1.$$

Hence both the number of unknowns and the number of constraints grow linearly with respect to $\mathcal{K}$ and $\mathcal{J}$. Furthermore, if $\mathcal{J}$ is given, the number of constraints and unknowns increases linearly with the net size, and is independent from the initial marking.

However, if the net size changes, then $\mathcal{J}$ may be changed in order to check the necessary and sufficient condition stated in Theorem 11. From Theorem 9 it is

$$\mathcal{J}_{\min} \leq 2 \cdot \|\boldsymbol{m}_0\|_1 \cdot \left\| \sum_{\boldsymbol{y} \in \mathcal{T}(N)} \boldsymbol{y} \right\|_1 .$$

Taking into account that the number of T-invariants is bounded by[3] (see Silva et al., 1992)

$$\binom{n}{\left\lceil \frac{n}{2} \right\rceil},$$

and that $\mathcal{J}_{\min}$ depends also on the initial marking (see Remark 3), it turns out that, in the worst case, the complexity grows exponentially with respect to the net size. This result is in accordance to the fact that $\mathcal{J}$ is related to the reachability set of a net.

[3] $\lceil x \rceil$ denotes the ceiling of x, i.e., the smallest integer not less than x.

4. $\mathcal{K}$-diagnosability of labeled net

In this section we extend the result previously introduced to the case of labeled nets. Let consider the following definition of labeled P/T net, that allows us to associate events to the net transitions.

Definition 12 (*Labeled P/T Net System*). A *labeled P/T* net system is the 3-ple $G = \langle N, \boldsymbol{m}_0, \lambda\rangle$, where N is a standard P/T net, $\boldsymbol{m}_0$ is the initial marking, and

$$\lambda : T \mapsto E \cup \{\varepsilon\}$$

is the *labeling function* which assigns to each transition $t \in T$ either an event from the set E or the *silent event* ε. In particular, it is $\lambda(t) = \varepsilon$ if $t \in T_{uo}$, while $\lambda(t) \neq \varepsilon$ if $t \in T_o$. □

In the following we will assume $\mathrm{card}(E) = e$, and we also denote with

$$T^{\alpha_i} = \left\{t \in T \mid \lambda(t) = \alpha_i\right\},$$

the set of transitions associated with the same event $\alpha_i \in E$. Moreover, we denote as w the word of events associated with a sequence σ such that $w = \lambda(\sigma)$, assuming the usual extension of the labeling function $\lambda : T^* \mapsto E^*$. Given a word w we will denote with $|w|$ its length, and with $|w|_{\alpha_i}$ the number of occurrences of the event α_i in w.

In labeled nets two or more transitions can share the same event α, and this additional source of nondeterminism may affect diagnosability.

Before introducing the necessary and sufficient condition for the $\mathcal{K}$-diagnosability of bounded labeled net, let us consider the following extension of Lemma 3 to the case of labeled net. In particular, given a sequence σ and its corresponding observed word w, the next lemma introduces a necessary condition that must be fulfilled by a set of firing count vectors that correspond to the unobservable explanations of $\boldsymbol{b} = \pi\left(\Pr(\sigma)\right)$.

Lemma 4. *Consider a labeled net system $G = \langle N, \boldsymbol{m}_0, \lambda\rangle$ and a sequence σ enabled under the initial marking $\boldsymbol{m}_0$. If the sequence σ is such that*

$$\lambda(\sigma) = w,$$

*then there exist 2ρ vectors $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_\rho$, $\boldsymbol{\epsilon}_1, \ldots, \boldsymbol{\epsilon}_\rho \in \mathbb{N}^n$, with $\rho \leq |\sigma|$, that fulfill the following set of constraints denoted by $\mathcal{LE}\big(\boldsymbol{m}_0, |w|_{\alpha_1}, \ldots,$
$|w|_{\alpha_e}\big)$*

$$\begin{cases} \boldsymbol{m}_0 + \mathbf{C}\cdot\boldsymbol{\epsilon}_{1|T_{uo}} \geq \mathbf{Pre}\cdot\boldsymbol{s}_{1_{|T_o}} & \\ \boldsymbol{m}_0 + \mathbf{C}\cdot\displaystyle\sum_{i=1}^{2}\boldsymbol{\epsilon}_{i_{|T_{uo}}} + \mathbf{C}\cdot\boldsymbol{s}_{1_{|T_o}} \geq \mathbf{Pre}\cdot\boldsymbol{s}_{2_{|T_o}} & \\ \ldots & \text{(a)} \\ \boldsymbol{m}_0 + \mathbf{C}\cdot\displaystyle\sum_{i=1}^{\rho}\boldsymbol{\epsilon}_{i_{|T_{uo}}} + \mathbf{C}\cdot\sum_{j=1}^{\rho-1}\boldsymbol{s}_{j_{|T_o}} \geq \mathbf{Pre}\cdot\boldsymbol{s}_{\rho_{|T_o}} & \\ \boldsymbol{m}_0 \geq \mathbf{Pre}\cdot\boldsymbol{\epsilon}_{1_{|T_{uo}}} & \\ \boldsymbol{m}_0 + \mathbf{C}\cdot\left(\boldsymbol{\epsilon}_{1_{|T_{uo}}} + \boldsymbol{s}_{1_{|T_o}}\right) \geq \mathbf{Pre}\cdot\boldsymbol{\epsilon}_{2_{|T_{uo}}} & \\ \ldots & \text{(b)} \\ \boldsymbol{m}_0 + \mathbf{C}\cdot\displaystyle\sum_{i=1}^{\rho-1}\left(\boldsymbol{\epsilon}_{i_{|T_{uo}}} + \boldsymbol{s}_{i_{|T_o}}\right) \geq \mathbf{Pre}\cdot\boldsymbol{\epsilon}_{\rho_{|T_{uo}}} & \\ \displaystyle\sum_{t_j\in T^{\alpha_l}}\sum_{i=1}^{\rho}\boldsymbol{s}_i(t_j) = |w|_{\alpha_l}, \quad l = 1, \ldots, e. & \text{(c)} \end{cases} \tag{12}$$

Proof. Noting that (12)(c) is a congruence relation between transitions having the same label, the proof follows by exploiting similar arguments as in the proof of Lemma 3. □

Remark 4. It is worth noticing that Lemma 4 states only a necessary condition. Although the enabling of the unobservable explanations of σ is checked by means of (12)(a) and (b), the constraint (12)(c) cannot assure that a solution of $\mathcal{LE}\big(\boldsymbol{m}_0, |w|_{\alpha_1}, \ldots, |w|_{\alpha_e}\big)$ leads to the same observed word w. Indeed, the congruence with the observed word is not guaranteed by (12)(c), since it considers the sum over all the firing count vectors. □

It is now possible to state the following results, which can be proved by exploiting Lemma 4 and similar arguments as in Theorems 10 and 11.

Theorem 13. *Given a labeled net system $G = \langle N, \boldsymbol{m}_0, \lambda\rangle$ a fault transition t_f, and a positive integer $\mathcal{K}$, if there exists at least one $\mathcal{J} \in \mathbb{N}, \mathcal{J} > 0$ and $3\big(\mathcal{J} + \mathcal{K}\big)$ vectors $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\mathcal{J}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_\mathcal{K}$, $\boldsymbol{\epsilon}_1, \ldots, \boldsymbol{\epsilon}_{\mathcal{J}+\mathcal{K}}, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{\mathcal{J}+\mathcal{K}} \in \mathbb{N}^n$ such that*

$$\min_{\text{s.t. } \mathcal{LD}\left(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\right)} \sum_{r=1}^{\mathcal{J}+\mathcal{K}} \boldsymbol{\epsilon}_r(t_f) = 0,$$

where the set of constraints $\mathcal{LD}\big(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\big)$ is equal to (13), then t_f is $\mathcal{K}$-undiagnosable.

$$\begin{cases} \mathcal{F}\left(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\right) & \text{(a)} \\ \mathcal{LE}\left(\boldsymbol{m}_0, \displaystyle\sum_{t_l\in T^{\alpha 1}}\left(\sum_{i=1}^{\mathcal{J}}\boldsymbol{u}_i(t_l) + \sum_{j=1}^{\mathcal{K}}\boldsymbol{v}_j(t_l)\right), \ldots,\right. & \\ \qquad \left.\displaystyle\sum_{t_l\in T^{\alpha e}}\left(\sum_{i=1}^{\mathcal{J}}\boldsymbol{u}_i(t_l) + \sum_{j=1}^{\mathcal{K}}\boldsymbol{v}_j(t_l)\right)\right) & \text{(b)} \\ \displaystyle\sum_{t_j\in T^{\alpha_l}}\boldsymbol{s}_1(t_j) = \sum_{t_j\in T^{\alpha_l}}\boldsymbol{u}_1(t_j), \quad l = 1, \ldots, e & \\ \ldots & \\ \displaystyle\sum_{t_j\in T^{\alpha_l}}\boldsymbol{s}_\mathcal{J}(t_j) = \sum_{t_j\in T^{\alpha_l}}\boldsymbol{u}_\mathcal{J}(t_j), \quad l = 1, \ldots, e & \\ \displaystyle\sum_{t_j\in T^{\alpha_l}}\boldsymbol{s}_{\mathcal{J}+1}(t_j) = \sum_{t_j\in T^{\alpha_l}}\boldsymbol{v}_1(t_j), \quad l = 1, \ldots, e & \text{(c)} \\ \ldots & \\ \displaystyle\sum_{t_j\in T^{\alpha_l}}\boldsymbol{s}_{\mathcal{J}+\mathcal{K}}(t_j) = \sum_{t_j\in T^{\alpha_l}}\boldsymbol{v}_\mathcal{K}(t_j), \quad l = 1, \ldots, e. & \end{cases} \tag{13}$$

In Theorem 13 the additional constraints (13)(c) in $\mathcal{LD}\big(\boldsymbol{m}_0, t_f,$ $\mathcal{J}, \mathcal{K}\big)$ are congruence conditions used to link the constraints $\mathcal{F}\big(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\big)$, which return the firing count vectors of the sequences $\sigma = ut_f v$, to the constraints

$$\mathcal{LE}\left(\boldsymbol{m}_0, \sum_{t_l\in T^{\alpha 1}}\left(\sum_{i=1}^{\mathcal{J}}\boldsymbol{u}_i(t_l) + \sum_{j=1}^{\mathcal{K}}\boldsymbol{v}_j(t_l)\right), \ldots\right),$$

which return the firing count vectors of the unobservable explanations of σ.

These additional constraints allows to check the congruence with the observed word on each single firing count vector corresponding to the unobservable explanations of σ (see Remark 4).

Theorem 14. *Consider a labeled and bounded net system $G = \langle N,$ $\boldsymbol{m}_0, \lambda\rangle$ and a fault transition t_f, let $\mathcal{J}$ be a positive integer such that $\mathcal{J} \geq \mathcal{J}_{\min}$. Given a positive integer $\mathcal{K}$, t_f is $\mathcal{K}$-diagnosable iff there exist $3\big(\mathcal{J} + \mathcal{K}\big)$ vectors $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\mathcal{J}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_\mathcal{K}, \boldsymbol{\epsilon}_1, \ldots,$ $\boldsymbol{\epsilon}_{\mathcal{J}+\mathcal{K}}, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{\mathcal{J}+\mathcal{K}} \in \mathbb{N}^n$ such that*

$$\min_{\text{s.t. } \mathcal{LD}\left(\boldsymbol{m}_0, t_f, \mathcal{J}, \mathcal{K}\right)} \sum_{r=1}^{\mathcal{J}+\mathcal{K}} \boldsymbol{\epsilon}_r(t_f) \neq 0.$$

When bounded labeled nets are considered, thanks to the congruence conditions (13)(c), the use of Lemma 4 leads to a necessary and sufficient condition for $\mathcal{K}$-diagnosability. Indeed, the fulfilling of constraints (13)(c) imply the fulfilling of (12)(c), while the converse is not necessarily true.

5. Examples

In this section we illustrate the effectiveness of the proposed approach by means of four examples. The programming problems have been solved by using the GNU linear programming kit GPLK (GLPK, 2008).

Example 4. Let consider the net in Fig. 1, with $t_3 \in T_f$ and $\boldsymbol{m}_0 = \left[2\,0\,0\,0\right]^T$. It is straightforward to note that for this net the set $\mathcal{M}(t_3)$ can be characterized by using at most two firing count vectors, hence we set $\mathcal{J} = \mathcal{J}_{\min} = 2$. If we choose $\mathcal{K} = 2$ then

$$\min_{\text{s.t. } \mathcal{D}\left(\boldsymbol{m}_0, t_3, 2, 2\right)} \sum_{r=1}^{4} \boldsymbol{\epsilon}_r(t_3) = 0,$$

since t_3 is not 2-diagnosable, as discussed in Example 3.

Setting $\mathcal{K}$ equal to 3 it results

$$\min_{\text{s.t. } \mathcal{D}\left(\boldsymbol{m}_0, t_3, 2, 3\right)} \sum_{r=1}^{5} \boldsymbol{\epsilon}_r(t_3) = 1,$$

hence t_3 is 3-diagnosable. □

Example 5. Let us consider the unbounded labeled net system shown in Fig. 2, with $t_2 \in T_f$, $\boldsymbol{m}_0 = \left[1\,0\,0\,0\right]^T$ and

$$T^a = \left\{t_1\right\} \qquad T^b = \left\{t_4, t_6\right\}$$
$$T^c = \left\{t_7\right\} \qquad T^d = \left\{t_5\right\}.$$

In Cabasino et al. (2009a) it has been shown that t_2 is undiagnosable. Adopting the approach proposed in Section 4, for any $\mathcal{K} \in \mathbb{N}$ choosing $\mathcal{J} = \mathcal{K}$ it results

$$\min_{\text{s.t. } \mathcal{L}\mathcal{D}\left(\boldsymbol{m}_0, t_2, \mathcal{K}, \mathcal{K}\right)} \sum_{r=1}^{2\mathcal{K}} \boldsymbol{\epsilon}_r(t_2) = 0, \quad \forall \mathcal{K} \in \mathbb{N}.$$

Exploiting Theorem 13, it follows that t_2 is undiagnosable. Indeed, as it has been shown in Cabasino et al. (2009a), for any choice of $\mathcal{K}$, the sequence ut_2, with $u = t_1^{\mathcal{K}}$, does not allow to diagnose the fault after the firing of $\mathcal{K}$ transitions after its occurrence. For the same reason we have chosen $\mathcal{J} = \mathcal{K}$. □

Example 6. Let us consider the bounded labeled net system in Fig. 3, with $t_3 \in T_f$, $\boldsymbol{m}_0 = \left[3\,0\,0\,0\,0\right]^T$ and $T^a = \left\{t_1, t_4\right\}$. In this case it is easy to show that two firing count vectors $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$ are sufficient to characterize the set $\mathcal{M}(t_3)$, hence $\mathcal{J}$ is set equal to 2. Given this choice of $\mathcal{J}$, it results

$$\min_{\text{s.t. } \mathcal{L}\mathcal{D}\left(\boldsymbol{m}_0, t_3, 2, 7\right)} \sum_{r=1}^{9} \boldsymbol{\epsilon}_r(t_3) = 0,$$

and

$$\min_{\text{s.t. } \mathcal{L}\mathcal{D}\left(\boldsymbol{m}_0, t_3, 2, 8\right)} \sum_{r=1}^{10} \boldsymbol{\epsilon}_r(t_3) = 1.$$

Since the net system is bounded, in this case it is possible to exploit Theorem 14, hence it readily follows that the fault t_3 is not 7-diagnosable, while it is 8-diagnosable. □

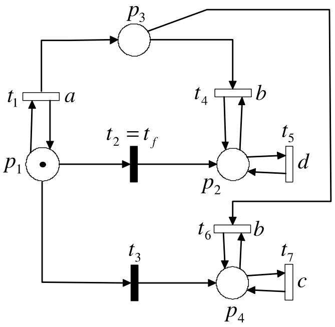

Fig. 2. Labeled net system of Example 5. The fault transition t_2 is undiagnosable.

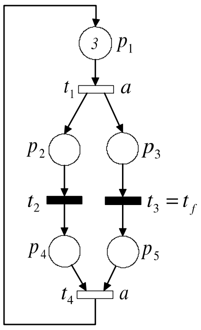

Fig. 3. Labeled net system of Example 6. The fault transition t_3 is 8-diagnosable.

Example 7. Let consider the net in Fig. 4 with

$$\boldsymbol{m}_0 = \left[2\,0\,2\,0\,0\,2\right]^T.$$

The fault transition t_6 is undiagnosable, since after its firing, the sequence $t_1t_2t_4$ can fire infinitely. Hence t_6 is $\mathcal{K}$-undiagnosable for every possible choice of $\mathcal{K} \in \mathbb{N}$.

In order to apply the Theorem 11 we estimate $\mathcal{J}_{\min}$ exploiting the Feasibility problem 1.

First, the minimal support T-invariants have been computed by using the Netlab software (Netlab, 2011)

$$\boldsymbol{y}_1 = [1\,1\,0\,1\,0\,0]^T, \qquad \boldsymbol{y}_2 = [0\,1\,1\,0\,1\,1]^T.$$

Then, taking into account that the net system in Fig. 4 is reversible, Theorem 9 gives the following upper bound for $\mathcal{J}_{\min}$

$$\mathcal{J}_{\min} \leq \|\boldsymbol{m}_0\|_1 \cdot \|\boldsymbol{y}_1 + \boldsymbol{y}_2\|_1 = 6 \cdot 7 = 42.$$

Furthermore, with $\mathcal{J} = 12$ it is possible to solve the Feasibility problem 1 modifying the inequality (9d) as

$$\sum_{i=1}^{\mathcal{J}} \boldsymbol{u}_i \geq \|\boldsymbol{m}_0\|_1 \cdot \hat{\boldsymbol{y}}.$$

The cardinality of $R(N, \boldsymbol{m}_0)$ has been computed with Netlab and it is equal to 60. Given $\mathcal{J} = 12$ it is possible to solve the Feasibility problem 1 also when

$$\boldsymbol{m}_0 = \left[2\,0\,3\,0\,0\,3\right]^T,$$

which corresponds to a cardinality of $R(n, \boldsymbol{m}_0)$ equal to 140.

Hence given $\mathcal{J} = 12$ and for every possible choice of $\mathcal{K}$ the ILP problem in Theorem 11 returns

$$\min_{\text{s.t. } \mathcal{D}\left(\boldsymbol{m}_0, t_6, 12, \mathcal{K}\right)} \sum_{r=1}^{\mathcal{K}+12} \boldsymbol{\epsilon}_r(t_6) = 0. \quad \square$$

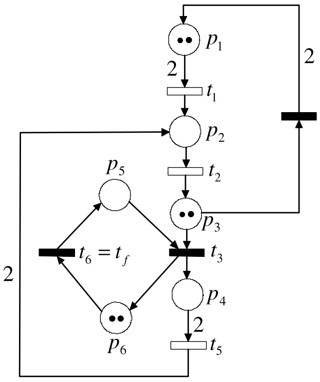

Fig. 4. Net system of Example 7. The fault transition t_6 is undiagnosable.

6. Concluding remarks

A necessary and sufficient condition to check $\mathcal{K}$-diagnosability of a fault transition in a bounded PNs has been provided in this paper for both unlabeled and labeled systems. The concept of $\mathcal{K}$-diagnosability corresponds to the diagnosability within a finite delay. The main results are expressed in terms of ILP problems, that can be easily solved by using off-the-shelf tools. The proposed approach does not require any specific assumption on the structure of the net induced by the unobservable transitions, and it allows to cast the diagnosability problem in the same framework adopted for fault diagnosis in Basile et al. (2009a) and Dotoli et al. (2009). Furthermore, the proposed approach does not require neither any explicit estimation of the reachability set, nor any search of paths in graphs.

Acknowledgments

This research has been partially supported by Italian Ministry of Education, University and Research—Research Project of National Interest "ROCOCO" (PRIN 2009) and by *Programma FARO* (Finanziamento per l'Avvio di Ricerche Originali) in the framework of the *LATINO Project: Un sistema innovativo di LocAlizzazione e Tracciamento di INdividui per l'Ottimizzazione di percorsi in ambienti indoor.*

References

Basile, F., Chiacchio, P., & De Tommasi, G. (2008). Sufficient conditions for diagnosability of Petri nets. In *Proc. of the 9th international workshop on discrete event systems*, WODES'08. Göteborg, Sweden. May (pp. 436–442).

Basile, F., Chiacchio, P., & De Tommasi, G. (2009a). An efficient approach for online diagnosis of discrete event systems. *IEEE Transactions on Automatic Control*, *54*(4), 748–759.

Basile, F., Chiacchio, P., & De Tommasi, G. (2009b). Online diagnosis of discrete events systems based on Petri nets and integer linear programming. In *Proc. 2nd IFAC workshop on dependable control of discrete systems*, DCDS'09. Bari, Italy. June (pp. 111–116).

Boel, R. K., & Jiroveanu, G. (2004). Contextual distributed diagnosis for very large systems. In *16th int. symp. on mathematical theory of networks and systems*. Leuven, Belgium. July.

Cabasino, M. P., Giua, A., Lafortune, S., & Seatzu, C. (2009a). Diagnosability analysis of unbounded Petri nets. In *Proc. of the 48th IEEE conf. on decision and control*. Shangai, China. December (pp. 1267–1272).

Cabasino, M. P., Giua, A., & Seatzu, C. (2009b). Diagnosability analysis of bounded Petri nets. In *Proc. of the 48th IEEE conf. on decision and control*. Shangai, China. December (pp. 1254–1260).

Cabasino, M. P., Giua, A., & Seatzu, C. (2010). Fault detection for discrete event systems using Petri nets with unobservable transitions. *Automatica*, *46*(9), 1531–1539.

Cassandras, C. G., & Lafortune, S. (1999). *Introduction to discrete event systems*. Springer.

Cassez, F., Tripakis, S., & Altisen, K. (2007). Sensor minimization problems with static or dynamic observers for fault diagnosis. In *7th Int. conf. application of concurrency to system design*. Bratislava, Slovak Republic. July.

Chung, S. L. (2005). Diagnosing PN-based models with partial observable transitions. *International Journal of Computer Integrated Manufacturing*, *18*(2–3), 158–169.

Debouk, R., Lafortune, S., & Teneketzis, D. (2000). Coordinated decentralized protocols for failure diagnosis of discrete event systems. *Discrete Event Dynamic Systems*, *10*(1), 33–86.

Dideban, A., & Alla, H. (2008). Reduction of constraints for controller synthesis based on safe Petri nets. *Automatica*, *44*(7), 1697–1706.

Dotoli, M., Fanti, M. P., & Mangini, A. M. (2009). Fault detection of discrete event systems by Petri nets and integer linear programming. *Automatica*, *45*(11), 2665–2672.

García Vallés, F. (1999). Contributions to the structural and symbolic analysis of place/transition nets with applications to flexible manufacturing systems and asynchronous circuits. *Ph.D. Thesis*. Universidad de Zaragoza.

GLPK, (2008). GNU linear programming kit. http://www.gnu.org/software/glpk/.

Góra, P. (1992). Graph theoretic bound on number of A.C.I.M. for random transformation. *Proceedings of the American Mathematical Society*, *116*(2), 401–410.

Hruz, B., & Zhou, M. C. (2007). *Modeling and control of discrete event dynamic systems*. London, UK: Springer.

Jiroveanu, G., & Boel, R. K. (2010). The diagnosability of Petri net models using minimal explanations. *IEEE Transactions on Automatic Control*, *55*(7), 1663–1668.

Lefebvre, D., & Delherm, C. (2007). Diagnosis of DES with Petri net models. *IEEE Transactions on Automation Science and Engineering*, *4*(1), 114–118.

Lunze, J., & Schröder, J. (2001). State observation and diagnosis of discrete-event systems described by stochastic automata. *Discrete Event Dynamic Systems*, *11*(4), 319–369.

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

Netlab, (2011). http://www.irt.rwth-aachen.de/en/fuer-studierende/downloads/petri-net-tool-netlab/.

Paoli, A., & Lafortune, S. (2005). Safe diagnosability for fault-tolerant supervision of discrete-event systems. *Automatica*, *41*(8), 1335–1347.

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

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

Silva, M., Teruel, E., & Colom, J. M. (1992). Linear algebraic and linear programming techniques for the analysis of place/transition net systems. In *Lectures notes in computer science*: *Vol. 616* (pp. 309–373). Springer-Verlag.

Teruel, E., & Silva, M. (1993). Liveness and home states in equal conflict systems. In *Proceedings of the 14th international conference on application and theory of Petri nets* (pp. 415–432). London, UK: Springer-Verlag.

Trevino, A. R., Ruiz-Beltran, E., Rivera-Rangel, I., & Lopez-Mellado, E. (2007). Online fault diagnosis of discrete event systems. A Petri net-based approach. *IEEE Transactions on Automation Science and Engineering*, *4*(1), 31–39.

Ushio, T., Onishi, L., & Okuda, K. (1998). Fault detection based on Petri net models with faulty behaviors. In *Proc. of the 1998 IEEE conf. on systems, man, and cybernetics*. San Diego, CA, USA. October (pp. 113–118).

Wen, Y., Li, C., & Jeng, M. (2005). A polynomial algorithm for checking diagnosability of Petri nets. In *Proc. of the 2005 IEEE conf. on systems, man, and cybernetics*, SMC'05. Vol. 3. October (pp. 2542–2547).

Wu, Y., & Hadjicostis, C. N. (2005). Algebraic approaches for fault identification in discrete-event systems. *IEEE Transactions on Automatic Control*, *50*(12), 2048–2053.

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

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

Francesco Basile was born in Naples, Italy, in 1971. He received the Laurea degree in Electronic Engineering in 1995 and the Ph.D. degree in Electronic and Computer Engineering in 1999 from the University of Naples. In 1999 he was a visiting researcher for six months at the Departamento de Ingenieria Informatica y Systems of the University of Saragoza, Spain. He is currently assistant professor of Automatic Control at the Dipartimento di Ingegneria dell'Informazione e Ingegneria Elettrica of the University of Salerno, Italy. He has published more than 70 papers in international journals and conferences. He is a member of the editorial board of IEEE Transactions on Control Systems Technology and International Journal of Robotics and Automation and of IEEE Control System Society Conference Editorial Board. His current research interest are: modeling and control of discrete event systems, automated manufacturing and robotics. He has been an IEEE Senior member since November 2011.

Pasquale Chiacchio was born in Naples, Italy, on September 7, 1963. He received the Laurea (5 years) degree in Electronic Engineering and the Research Doctorate (3 years) degree in Electronic and Computer Engineering from the University of Naples in 1987 and 1992. He is Professor of Automatic Control in the Department of Electronic and Computer Engineering, University of Salerno. His main research interests include robotics and modeling and control of discrete event systems. In the robotics field, he has been working on robot control and identification, inverse kinematic problems, control of redundant manipulators, control of cooperative manipulators. In the discrete event systems field, he has been working on supervisory control based on monitors, optimal supervisory control and formal specification for supervisory systems. The results have been published in the main journals of the sector and have been accompanied by intense experimental activity. He has coauthored 5 national books, 35 international journal papers, 86 international conference papers and book chapters. He has been the coordinator of the Research Program of National Interest (PRIN 2007) "Control themes in hyperflexible robotic workcells" and he is at the moment coordinator of the Research Program of National Interest (PRIN 2009) "ROCOCO Cooperative and collaborative robotics". He is a senior member of the Institute of Electrical and Electronic Engineers (IEEE) and a member of the Italian Society of Control Researchers. In December 2011 was nominated for the Knight of the Order of Merit of Italy.

Gianmaria De Tommasi was born in Milan, Italy, in 1975. He received the Laurea degree (summa cum laude) in Electronic Engineering from the University of Naples Federico II in 2001. Since 2002 he has been with the Department of Computer and Systems Engineering of the University of Naples Federico II, where he received the Research Doctorate degree in Computer and Automatic Engineering in 2005, and where he is currently an Assistant Professor. Since 2002 he has been a visiting researcher at the JET tokamak (UK), where he has participated in various projects connected to the JET plasma current and shape control system. Since 2009, he has also participated in the modeling activities for the Central Safety System and Central Interlock System at the ITER Organization (France). Recently he has been Project Leader of an international project at JET named Current Limit Avoidance Implementation (2010–11), aimed at developing and implementing an intelligent control system to avoid reaching the current limits during tokamak operations. He is Senior Member of the IEEE. His current research interests include control of nuclear fusion devices, fault detection for discrete event systems, identification of discrete event systems modeled with Petri nets, and stability of hybrid systems. He has published more than 100 journal and conference papers on these topics.