Fault diagnosis of discrete event systems using Petri nets

Carla Seatzu

***Abstract*— This talk focuses on on-line fault diagnosis of discrete event systems based on Petri nets. In particular a diagnosis approach based on the notion of basis markings and justifications is discussed. This concept allows us to represent the reachability space in a compact manner, i.e., it requires to enumerate only a subset of the reachability space. Arbitrary labeled Petri nets are considered as the reference model. Some results on diagnosability analysis are finally recalled.**

I. Introduction

Failure detection and isolation in industrial systems is a subject that has received a lot of attention in the past few decades. A failure is defined to be any deviation of a system from its normal or intended behavior. Diagnosis is the process of detecting an abnormality in the system behavior and isolating the cause or the source of this abnormality.

The first contributions in the discrete event systems framework have been proposed in the context of automata by Sampath *et al.* [1], [2] who proposed an approach to failure diagnosis where the system is modeled as a nondeterministic automaton in which failures are treated as unobservable events.

More recently, Petri net (PN) models have been used in the context of diagnosis [3], [4], [5], [6]. Indeed, the use of PNs offers significant advantages because of their twofold representation: graphical and mathematical. Moreover, the intrinsically distributed nature of PNs where the notion of state (i.e., marking) and action (i.e., transition) is local reduces the computational complexity involved in solving a diagnosis problem.

In this talk we recall an approach we proposed in [7], that is a generalization of [8]. The main difference between the diagnosis approach presented here and the approaches cited above is the concept of basis marking. This concept allows us to represent the reachability space in a compact manner, i.e., it requires to enumerate only a subset of the reachability space. In particular, we deal with arbitrary labeled PNs where there is an association between sensors and observable events, while no sensor is available for certain activities — such as faults or other unobservable but regular transitions — due to budget constraints or technology limitations. It is assumed that several different transitions might share the same sensor in order to reduce cost or power consumption. If two transitions are simultaneously enabled and one of them fires, it is impossible to distinguish which one has fired, thus they are called *undistinguishable*. The diagnosis approach here presented is based on the definition of four diagnosis states modeling different degrees of alarm and it applies to all systems whose unobservable subnet is acyclic.

Note that the approach here presented, as most of the approaches dealing with diagnosis of discrete event systems, assumes that the faulty behavior is completely known, thus a fault model is available.

The last part of the talk is devoted to briefly recall some results on diagnosability analysis that may also be applied to unbounded nets.

C. Seatzu is with the Department of Electrical and Electronic Engineering, University of Cagliari, Piazza D'Armi, 09123 Cagliari, Italy. E-mail:seatzu@diee.unica.it.

II. Background on labeled Petri nets

A *Place/Transition net* (P/T net) is a structure $N = (P, T, Pre, Post)$, where P is a set of m places; T is a set of n transitions; $Pre: P \times T \to \mathbb{N}$ and $Post: P \times T \to \mathbb{N}$ are the pre– and $post$– incidence functions that specify the arcs; $C = Post - Pre$ is the incidence matrix.

A *marking* is a vector $M: P \to \mathbb{N}$ that assigns to each place of a P/T net a nonnegative integer number of tokens, represented by black dots. The marking of place p is denoted as $M(p)$. A P/T *system* or *net system* $\langle N, M_0 \rangle$ is a net N with an initial marking M_0. A transition t is enabled at M iff $M \geq Pre(\cdot, t)$ and may fire yielding the marking $M' = M + C(\cdot, t)$. One writes $M\ [\sigma\rangle$ to denote that the sequence of transitions $\sigma = t_{j_1} \cdots t_{j_k}$ is enabled at M, and $M\ [\sigma\rangle\ M'$ to denote that the firing of σ yields M'. One writes $t \in \sigma$ to denote that a transition t is contained in σ.

The set of all sequences that are enabled at the initial marking M_0 is denoted $L(N, M_0)$, i.e., $L(N, M_0) = \{\sigma \in T^* \mid M_0[\sigma\rangle\}$.

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

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

A PN having no directed circuits is called *acyclic*. A net system $\langle N, M_0 \rangle$ is *bounded* if there exists a positive constant k such that, for $M \in R(N, M_0)$, $M(p) \leq k$.

The association between sensors and transitions can be captured by a *labeling function* $\mathcal{L}: T \to L \cup \{\varepsilon\}$ assigns to each transition $t \in T$ either a symbol from a given alphabet L or the empty string ε.

The set of transitions whose label is ε is denoted as T_u, i.e., $T_u = \{t \in T \mid \mathcal{L}(t) = \varepsilon\}$. Transitions in T_u are called *unobservable* or *silent*. T_o denotes the set of transitions labeled with a symbol in L. Transitions in T_o are called *observable* because when they fire their label can be

observed. Note that we assume that the same label $l \in L$ can be associated to more than one transition. In particular, two transitions $t_1, t_2 \in T_o$ are called *undistinguishable* if they share the same label, i.e., $\mathcal{L}(t_1) = \mathcal{L}(t_2)$. The set of transitions sharing the same label l are denoted as T_l.

In the following let C_u (C_o) be the restriction of the incidence matrix to T_u (T_o) and n_u and n_o, respectively, be the cardinality of the above sets. Moreover, given a sequence $\sigma \in T^*$, $P_u(\sigma)$, resp., $P_o(\sigma)$, denotes the projection of σ over T_u, resp., T_o.

The word w of events associated to sequence σ is $w = P_o(\sigma)$.

***Definition** 2.1:* [7] Let $\langle N, M_0\rangle$ be a labeled net system with labeling function $\mathcal{L} : T \to L \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in L^*$ be an observed word. Let $\mathcal{S}(w) = \{\sigma \in L(N, M_0) \mid P_o(\sigma) = w\}$ be the set of firing sequences *consistent* with $w \in L^*$, and $\mathcal{C}(w) = \{M \in \mathbb{N}^m \mid \exists \sigma \in T^* : P_o(\sigma) = w \wedge M_0[\sigma\rangle M\}$ be the set of reachable markings *consistent* with $w \in L^*$. ■

In plain words, given an observation w, $\mathcal{S}(w)$ is the set of sequences that may have fired, while $\mathcal{C}(w)$ is the set of markings in which the system may actually be.

***Example** 2.2:* Consider the PN in Fig. 1. Assume $T_o = \{t_1, t_2, t_3, t_4, t_5, t_6, t_7\}$ and $T_u = \{\varepsilon_8, \varepsilon_9, \varepsilon_{10}, \varepsilon_{11}, \varepsilon_{12}, \varepsilon_{13}\}$, where for a better understanding unobservable transitions have been denoted ε_i rather than t_i. The labeling function is defined as follows: $\mathcal{L}(t_1) = a$, $\mathcal{L}(t_2) = \mathcal{L}(t_3) = b$, $\mathcal{L}(t_4) = \mathcal{L}(t_5) = c$, $\mathcal{L}(t_6) = \mathcal{L}(t_7) = d$.

First consider $w = ab$. The set of firing sequences that is consistent with w is $\mathcal{S}(w) = \{t_1t_2, t_1t_2\varepsilon_8, t_1t_2\varepsilon_8\varepsilon_9, t_1t_2\varepsilon_8\varepsilon_9\varepsilon_{10}, t_1t_2\varepsilon_8\varepsilon_{11}\}$, and the set of markings consistent with w is $\mathcal{C}(w) = \{[0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T, [0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T, [0\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0]^T, [0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T, [0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0]^T\}$.

If $w = acd$ is considered the set of firing sequences that are consistent with w is $\mathcal{S}(w) = \{t_1t_5t_6, t_1t_5\varepsilon_{12}\varepsilon_{13}t_7\}$, and the set of markings consistent with w is $\mathcal{C}(w) = \{[0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T\}$. Thus two different firing sequences may have fired (the second one also involving silent transitions), but they both lead to the same marking. ■

***Definition** 2.3:* Given a net $N = (P, T, Pre, Post)$, and a subset $T' \subseteq T$ of its transitions, let us define the *$T'-$induced subnet of* N as the new net $N' = (P, T', Pre', Post')$ where $Pre', Post'$ are the restrictions of $Pre, Post$ to T'. The net N' can be thought as obtained from N removing all transitions in $T \setminus T'$. Let us also write $N' \prec_{T'} N$. ■

III. Characterization of the set of consistent markings

A. Minimal explanations and minimal e-vectors

***Definition** 3.1:* [8] Given a marking M and an observable transition $t \in T_o$, let $\Sigma(M, t) = \{\sigma \in T_u^* \mid M[\sigma\rangle M',\ M' \geq Pre(\cdot, t)\}$ be the set of *explanations* of t at M, and let $Y(M, t) = \pi(\Sigma(M, t))$ be the *e-vectors* (or *explanation vectors*), i.e., firing vectors associated to the explanations. ■

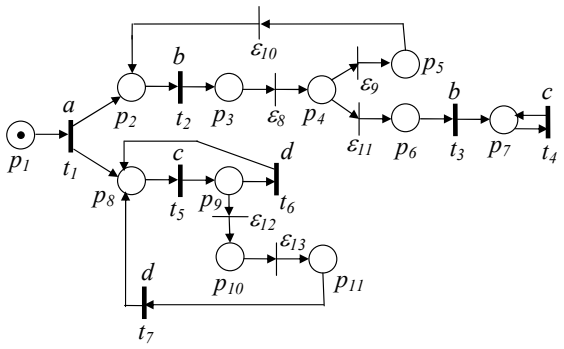

Fig. 1. The PN system considered in Sections II to IV.

Thus $\Sigma(M, t)$ is the set of unobservable sequences whose firing at M enables t. Among the above sequences select those whose firing vector is minimal. The firing vector of these sequences are called *minimal e-vectors*.

***Definition** 3.2:* [8] Given a marking M and a transition $t \in T_o$, let us define

$$\Sigma_{\min}(M, t) = \{\sigma \in \Sigma(M, t) \mid \nexists\, \sigma' \in \Sigma(M, t) : \pi(\sigma') \lneqq \pi(\sigma)\}$$

the set of *minimal explanations* of t at M, and let us define $Y_{\min}(M, t) = \pi(\Sigma_{\min}(M, t))$ the corresponding set of *minimal e-vectors*. ■

***Example** 3.3:* Consider the PN in Fig. 1 previously introduced in Example 2.2. It holds that $\Sigma(M_0, t_1) = \{\varepsilon\}$. Then $\Sigma(M_0, t_2) = \emptyset$. Finally, let $M = [\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ ]^T$, it holds that $\Sigma(M, t_5) = \{\varepsilon, \varepsilon_8, \varepsilon_8\varepsilon_9, \varepsilon_8\varepsilon_{11}, \varepsilon_8\varepsilon_9\varepsilon_{10}\}$, while $\Sigma_{min}(M, t_5) = \{\varepsilon\}$. It follows that $Y(M, t_5) = \{[0\ 0\ 0\ 0\ 0\ 0]^T,\ [1\ 0\ 0\ 0\ 0\ 0]^T,\ [1\ 1\ 0\ 0\ 0\ 0]^T,\ [1\ 0\ 0\ 1\ 0\ 0]^T,\ [1\ 1\ 1\ 0\ 0\ 0]^T\}$, and $Y_{min}(M, t_5) = \{[0\ 0\ 0\ 0\ 0\ 0]^T\}$. ■

B. Basis markings and j-vectors

***Definition** 3.4:* [7] Let $\langle N, M_0\rangle$ be a net system with labeling function $\mathcal{L} : T \to L \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in L^*$ be a given observation. Let

$$\begin{aligned}\hat{\mathcal{J}}(w) \quad = \{\ &(\sigma_o, \sigma_u),\ \sigma_o \in T_o^*,\ \mathcal{L}(\sigma_o) = w,\ \sigma_u \in T_u^* \mid \\ &[\exists \sigma \in \mathcal{S}(w) : \sigma_o = P_o(\sigma),\ \sigma_u = P_u(\sigma)] \wedge \\ &[\nexists \sigma' \in \mathcal{S}(w) : \sigma_o = P_o(\sigma'),\ \sigma'_u = P_u(\sigma') \wedge \\ &\qquad \pi(\sigma'_u) \lneqq \pi(\sigma_u)]\}\end{aligned}$$

be the set of pairs (sequence $\sigma_o \in T_o^*$ with $\mathcal{L}(\sigma_o) = w$, corresponding *justification* of w). ■

In simple words, $\hat{\mathcal{J}}(w)$ is the set of pairs whose first element is the sequence $\sigma_o \in T_o^*$ labeled w and whose second element is the corresponding sequence of unobservable transitions interleaved with σ_o whose firing enables σ_o and whose firing vector is minimal. The firing vectors of these sequences are called *j-vectors*.

***Example** 3.5:* Consider the PN in Fig. 1 previously introduced in Example 2.2. It is $\hat{\mathcal{J}}(ab) = \{(t_1t_2, \varepsilon)\}$ and $\hat{\mathcal{J}}(acd) = \{(t_1t_5t_6, \varepsilon), (t_1t_5t_7, \varepsilon_{12}\varepsilon_{13})\}$. ■

The main difference among minimal explanations and justifications is that the first ones are functions of a generic marking M and transition t, while justifications are functions of the initial marking M_0 and w. Moreover, as shown in [7], in the case of acyclic unobservable subnets, justifications can be computed recursively summing up minimal explanations.

***Definition** 3.6:* [7] Let $\langle N, M_0\rangle$ be a net system with labeling function $\mathcal{L} : T \to L \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let w be a given observation and $(\sigma_o, \sigma_u) \in \hat{\mathcal{J}}(w)$ be a generic pair (sequence of observable transitions labeled w; corresponding justification). The marking $M_b = M_0 + C_u \cdot y + C_o \cdot y'$, where $y = \pi(\sigma_u)$ and $y' = \pi(\sigma_o)$, i.e., the marking reached firing σ_o interleaved with the justification σ_u, is called *basis marking* and y is called its *j-vector* (or *justification-vector*). ■

Obviously, because in general more than one justification exists for a word w (the set $\hat{\mathcal{J}}(w)$ is generally not a singleton), the basis marking may be not unique as well.

***Definition** 3.7:* [7] Let $\langle N, M_0\rangle$ be a net system with labeling function $\mathcal{L} : T \to L \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in L^*$ be an observed word. Let

$$\mathcal{M}(w) = \{(M, y) \mid (\exists \sigma \in \mathcal{S}(w) \ : \ M_0[\sigma\rangle M) \wedge (\exists (\sigma_o, \sigma_u) \in \hat{\mathcal{J}}(w) \ : \ \sigma_o = P_o(\sigma), \ \sigma_u = P_u(\sigma), \ y = \pi(\sigma_u))\}$$

be the set of pairs (basis marking, relative j-vector) that are *consistent* with $w \in L^*$. ■

Note that the set $\mathcal{M}(w)$ does not keep into account the sequences of observable transitions that may have actually fired. It only keeps track of the basis markings that can be reached and of the firing vectors relative to sequences of unobservable transitions that have fired to reach them. Indeed, this is the information really significant when performing diagnosis. The notion of $\mathcal{M}(w)$ is fundamental to provide a recursive way to compute the set of minimal explanations. Under the assumption of acyclicity of the unobservable subnet, the set $\mathcal{M}(w)$ can be easily constructed following a simple algorithm in [7].

***Definition** 3.8:* [7] Let $\langle N, M_0\rangle$ be a net system where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Assume that the unobservable subnet is acyclic. Let $w \in T_o^*$ be an observed word. Let

$$\mathcal{M}_{basis}(w) = \{M \in \mathbb{N}^m \mid \exists y \in \mathbb{N}^{n_u} \text{ and } (M, y) \in \mathcal{M}(w)\}$$

be the set of basis markings at w. Moreover, denote as $\mathcal{M}_{basis} = \bigcup_{w \in T_o^*} \mathcal{M}_{basis}(w)$ the set of all basis markings for any observation w. ■

Note that if the net system is bounded then the set $\mathcal{M}_{basis}$ is *finite* being the set of basis markings a subset of the reachability set.

***Theorem** 3.9:* [7] Consider a net system $\langle N, M_0\rangle$ whose unobservable subnet is acyclic. For any $w \in L^*$ it holds that

$$\mathcal{C}(w) = \{M \in \mathbb{N}^m \mid M = M_b + C_u \cdot y \ : y \geq \vec{0} \text{ and } M_b \in \mathcal{M}_{basis}(w)\}.$$

The above result shows that the set $\mathcal{C}(w)$ can be characterized in linear algebraic terms given the set $\mathcal{M}_{basis}(w)$, thus not requiring exhaustive enumeration. This is the main advantage of the approach here presented.

IV. On-line diagnosis using Petri nets

Assume that the set of unobservable transitions is partitioned into two subsets, namely $T_u = T_f \cup T_{reg}$ where T_f includes all fault transitions (modeling anomalous or fault behavior), while T_{reg} includes all transitions relative to unobservable but regular events. The set T_f is further partitioned into r different subsets T_f^i, where $i = 1, \ldots, r$, that model the different fault classes. Usually, fault transitions that belong to the same fault class are transitions that represent similar physical faulty behavior.

***Definition** 4.1:* [7] A *diagnoser* is a function $\Delta : L^* \times \{T_f^1, T_f^2, \ldots, T_f^r\} \to \{0, 1, 2, 3\}$ that associates to each observation $w \in L^*$ and to each fault class T_f^i, $i = 1, \ldots, r$, a *diagnosis state*.

• $\Delta(w, T_f^i) = 0$ if for all $\sigma \in \mathcal{S}(w)$ and for all $t_f \in T_f^i$ it holds $t_f \notin \sigma$.

In such a case the ith fault cannot have occurred, because none of the firing sequences consistent with the observation contains fault transitions of class i.

• $\Delta(w, T_f^i) = 1$ if:

(i) there exist $\sigma \in \mathcal{S}(w)$ and $t_f \in T_f^i$ such that $t_f \in \sigma$ but

(ii) for all $(\sigma_o, \sigma_u) \in \hat{\mathcal{J}}(w)$ and for all $t_f \in T_f^i$ it holds that $t_f \notin \sigma_u$.

In such a case a fault transition of class i may have occurred but is not contained in any justification of w.

• $\Delta(w, T_f^i) = 2$ if there exist $(\sigma_o, \sigma_u), (\sigma_o', \sigma_u') \in \hat{\mathcal{J}}(w)$ such that

(i) there exists $t_f \in T_f^i$ such that $t_f \in \sigma_u$;

(ii) for all $t_f \in T_f^i$, $t_f \notin \sigma_u'$.

In such a case a fault transition of class i is contained in one (but not in all) justification of w.

• $\Delta(w, T_f^i) = 3$ if for all $\sigma \in \mathcal{S}(w)$ there exists $t_f \in T_f^i$ such that $t_f \in \sigma$.

In such a case the ith fault must have occurred, because all firable sequences consistent with the observation contain at least one fault in T_f^i. ■

***Example** 4.2:* Consider the PN in Fig. 1 previously introduced in Example 2.2. Let $T_f = \{\varepsilon_{11}, \varepsilon_{12}\}$. Assume that the two fault transitions belong to different fault classes, i.e., $T_f^1 = \{\varepsilon_{11}\}$ and $T_f^2 = \{\varepsilon_{12}\}$.

Let us observe $w = a$. Then $\Delta(w, T_f^1) = \Delta(w, T_f^2) = 0$, being $\hat{\mathcal{J}}(w) = \{(t_1, \varepsilon)\}$ and $\mathcal{S}(w) = \{t_1\}$. In simple words no fault of both fault classes may have occurred.

Let us observe $w = ab$. Then $\Delta(w, T_f^1) = 1$ and $\Delta(w, T_f^2) = 0$, being $\hat{\mathcal{J}}(w) = \{(t_1t_2, \varepsilon)\}$ and $\mathcal{S}(w) = \{t_1t_2, t_1t_2\varepsilon_8, t_1t_2\varepsilon_8\varepsilon_9, t_1t_2\varepsilon_8\varepsilon_9\varepsilon_{10}, t_1t_2\varepsilon_8\varepsilon_{11}\}$. This means that a fault of the first fault class may have occurred (firing the sequence $t_1t_2\varepsilon_8\varepsilon_{11}$) but it is not contained in any

justification of ab, while no fault of the second fault class can have occurred.

Now, consider $w = abb$. In this case $\Delta(w, T_f^1) = 2$ and $\Delta(w, T_f^2) = 0$, being $\hat{\mathcal{J}}(w) = \{(t_1t_2t_2, \varepsilon_8\varepsilon_9\varepsilon_{10}), (t_1t_2t_3, \varepsilon_8\varepsilon_{11})\}$ and $\mathcal{S}(w)$=$\{t_1t_2\varepsilon_8\varepsilon_9\varepsilon_{10}t_2, t_1t_2\varepsilon_8\varepsilon_9\varepsilon_{10}t_2\varepsilon_8, t_1t_2\varepsilon_8\varepsilon_9\varepsilon_{10}t_2\varepsilon_8\varepsilon_9, t_1t_2\varepsilon_8\varepsilon_9\varepsilon_{10}t_2\varepsilon_8\varepsilon_9\varepsilon_{10}, t_1t_2\varepsilon_8\varepsilon_9\varepsilon_{10}t_2\varepsilon_8\varepsilon_{11}, t_1t_2\varepsilon_8\varepsilon_{11}t_3\}$. This means that no fault of the second fault class can have occurred, while a fault of the first fault class may have occurred since one justification does not contain ε_{11} and one justification contains it.

Finally, consider $w = abbccc$. In this case $\Delta(w, T_f^1) = 3$ and $\Delta(w, T_f^2) = 1$. In fact since $\hat{\mathcal{J}}(w) = \{(t_1t_2t_3t_5t_4t_4, \varepsilon_8\varepsilon_{11}), (t_1t_2t_3t_4t_5t_4, \varepsilon_8\varepsilon_{11}), (t_1t_2t_3t_4t_4t_5, \varepsilon_8\varepsilon_{11}), (t_1t_2t_3t_4t_4t_4, \varepsilon_8\varepsilon_{11})\}$ a fault of the first fault class must have occurred, while a fault of the second fault class may have occurred (e.g. $t_1t_2\varepsilon_8\varepsilon_{11}t_3t_4t_4t_5\varepsilon_{12}$) but it is not contained in any justification of w. ■

***Proposition** 4.3:* [7] Consider an observed word $w \in L^*$.

- $\Delta(w, T_f^i) \in \{0, 1\}$ iff for all $(M, y) \in \mathcal{M}(w)$ and for all $t_f \in T_f^i$ it holds $y(t_f) = 0$.
- $\Delta(w, T_f^i) = 2$ iff there exist $(M, y) \in \mathcal{M}(w)$ and $(M', y') \in \mathcal{M}(w)$ such that:

(i) there exists $t_f \in T_f^i$ such that $y(t_f) > 0$,
(ii) for all $t_f \in T_f^i$, $y'(t_f) = 0$.

- $\Delta(w, T_f^i) = 3$ iff for all $(M, y) \in \mathcal{M}(w)$ there exists $t_f \in T_f^i$ such that $y(t_f) > 0$.

In [7] it has been shown that it is possible to distinguish between diagnosis states 0 and 1 by simply checking if a given constraint set is feasible or not.

***Remark** 4.4:* As proved in [7], if the considered net system is bounded, the most burdensome part of the procedure can be moved off-line defining a graph called *Basis Reachability Graph* (BRG). The BRG is a deterministic graph that has as many nodes as the number of possible basis markings, thus it is always finite being the set of basis markings a subset of the set of reachable markings. ■

V. Diagnosability analysis

In the diagnosis framework two different problems can be solved: the problem of diagnosis and the problem of diagnosability. As explained in detail in the above sections, solving a problem of diagnosis means that to each observed string of events is associated a diagnosis state, such as "normal" or "faulty" or "uncertain". Solving a problem of diagnosability is equivalent to determine if the system is diagnosable, i.e., to determine if, once a fault has occurred, the system can detect its occurrence in a finite number of steps. We addressed this problem in two different settings, depending on the boundedness of the net system. In particular, in [9] we proposed a solution that only applies to bounded nets, where the major feature is to allow to perform, using the same framework, both diagnosis and diagnosibility analysis.

Moreover, in [10] we proposed an approach that also applies to unbounded PNs. In particular in [10] we dealt with two different notions of diagnosability: diagnosability and diagnosability in K steps. Diagnosability in K steps is stronger than diagnosability and implies not only that the system is diagnosable, i.e., when the fault occurs we are able to detect it in a finite number of transition firings, but also that if the fault occurs we are able to detect it in at most K steps. We gave necessary and sufficient conditions for both notions of diagnosability and we presented a test to study both diagnosability and K-diagnosability based on the analysis of the coverability graph of a special PN, called *Verifier Net*, that is built starting from the initial system. Moreover, we gave a procedure to compute the bound K in the case of K-diagnosable systems. Then, we showed how sufficient conditions on diagnosability can be computed using linear programming techniques.

To the best of our knowledge, this is the first time that necessary and sufficient conditions for diagnosability and K-diagnosability of labeled unbounded Petri nets are presented.

VI. Conclusion and future work

In this talk an on-line approach for fault diagnosis of discrete event systems based on labeled Petri nets has been discussed. Some results on diagnosability analysis have also been recalled, that also apply to unbounded nets.

Several are the future lines of research in this framework. One of the most important is the relaxation of the assumption that the fault model is perfectly known, as well as the initial state of the system. Moreover, it is interesting to investigate how the problems of on-line fault diagnosis and diagnosability analysis can take advantage from information coming timing associated with transitions. Finally, due to the complexity of current systems, it is important to develop efficient distributed and/or decentralized approaches.

References

[1] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Diagnosability of discrete-event systems," *IEEE Trans. on Automatic Control*, vol. 40 (9), pp. 1555–1575, 1995.

[2] ——, "Failure diagnosis using discrete-event models," *IEEE Trans. Control Systems Technology*, vol. 4, no. 2, pp. 105–124, 1996.

[3] S. Genc and S. Lafortune, "Distributed diagnosis of place-bordered Petri nets," *IEEE Trans. on Automation Science and Engineering*, vol. 4, no. 2, pp. 206–219, 2007.

[4] A. Benveniste, E. Fabre, S. Haar, and C. Jard, "Diagnosis of asynchronous discrete event systems: A net unfolding approach," *IEEE Trans. on Automatic Control*, vol. 48, no. 5, pp. 714–727, 2003.

[5] F. Basile, P. Chiacchio, and G. D. Tommasi, "An efficient approach for online diagnosis of discrete event systems," *IEEE Trans. on Automatic Control*, vol. 54, no. 4, pp. 748–759, 2009.

[6] M. Dotoli, M. P. Fanti, A. Mangini, and W. Ukovich, "On-line fault detection in discrete event systems by Petri nets and integer linear programming," *Automatica*, vol. 45, no. 11, pp. 2665–2672, 2009.

[7] M. Cabasino, A. Giua, M. Pocci, and C. Seatzu, "Discrete event diagnosis using labeled Petri nets. An application to manufacturing systems," *Control Engineering Practice*, 2011, (in press, published on-line with DOI 10.1016/j.conengprac.2010.12.010).

[8] M. Cabasino, A. Giua, and C. Seatzu, "Fault detection for discrete event systems using Petri nets with unobservable transitions," *Automatica*, vol. 46, no. 9, pp. 1531–1539, 2010.

[9] ——, "Diagnosability of discrete event systems using labeled Petri nets," *IEEE Trans. on Automation Science and Engineering*, vol. 11, no. 1, pp. 144–153, 2014.

[10] M. Cabasino, A. Giua, S. Lafortune, and C. Seatzu, "A new approach for diagnosability analysis of Petri nets using Verifier Nets," *IEEE Trans. on Automatic Control*, vol. 57, no. 12, pp. 3104–3117, 2012.