Diagnosability of fault patterns with labeled stochastic Petri nets

Dimitri Lefebvre, Christoforos Hadjicostis

(will be inserted by the editor)

Diagnosability of fault patterns with labeled stochastic Petri nets

Dimitri Lefebvre · **Christoforos N. Hadjicostis**

Received: date / Accepted: date

Abstract: This paper is about the diagnosability of fault patterns in timed stochastic discrete event systems. For this purpose, the diagnosability problem is formulated with labeled stochastic Petri net models and pure logical fault pattern nets. A particular composition of a labeled stochastic Petri net with a fault pattern net is proposed and is shown to characterize in an explicit way the fault patterns, including the timing and probabilistic aspects of the underlying system. Logical and probabilistic verifiers are derived, and used to establish a set of conditions to check not only the strong diagnosability property but also weaker notions of diagnosability.

Keywords: Labeled stochastic Petri nets, fault patterns, diagnosability, probabilistic verification.

1 Introduction

Petri nets (PNs) comprise an important modeling tool for discrete event systems in a variety of applications (ranging from manufacturing and process engineering to computer systems and network/traffic protocols [17], [23]). Apart from control design issues, PNs have been studied from the perspective of fault diagnosis during the last 50 years [25]. Following a series of works about diagnosability using automata [37], [21], researchers have considered similar problems formulated within the Petri net framework. One important advantage of PN models is the possibility to represent a large variety of systems thanks to synchronisation, concurrency and weighted arcs. Another advantage is the compactness of the PN models that results mainly from the token semantics. Compared to finite automata, PNs are also suitable to deal with some classes of infinite state systems and to solve diagnosis problems for non-regular languages.

In its most basic form, a direct translation of the fault diagnosis problem from finite-state automata to Petri nets implies the existence of a set of observable transitions, with some of them perhaps sharing the same label, and a set of silent transitions, some of which constitute faults whose occurrence needs to be inferred after a bounded number of observations. There exists a large literature devoted to diagnosis with PNs. Some methods consider that the marking of certain places and the firing of certain transitions are observable, and the subclass of partially observed Petri nets (POPNs) has been defined for that purpose [26], [42], [43], [45]. Other methods assume that the markings are silent and are based on a set of observable transitions, and the subclass of labeled Petri nets (LPN) has been defined for that purpose [3], [5], [9], [16], [29]. Both subclasses of models have been shown to be equivalent [36]. Consequently, in this paper we will consider only LPNs, which have a simpler formalism and more tractable notations.

Most of the existing works have been developed in the logical setting (and not in the timed / probabilistic setting considered in this paper) and / or address the diagnosis of simple faults (thus, they are not directly applicable for the

Dimitri Lefebvre
GREAH, Le Havre Normandy University,
75 rue Bellot,
76600 Le Havre, France.
E-mail: dimitri.lefebvre@univ-lehavre.fr

Christoforos N. Hadjicostis
Department of Electrical and Computer Engineering,
University of Cyprus,
75 Kallipoleos Av.,
Nicosia 1678, Cyprus.
E-mail: chadjic@ucy.ac.cy

follows. This paper considers the diagnosability of fault patterns [22], [18], [33], instead of the diagnosability of simple fault events. In addition, the diagnosability problem is formulated in a timed and probabilistic setting [38], [39], [6] with labeled stochastic Petri net models. In this paper, we show how the timed / probabilistic aspects improve the detectability and discernability of faulty behaviours in the long run compared to the usual logical characterisations. For this purpose, a particular composition of a labeled stochastic Petri net with a logical fault pattern net is proposed and shown to characterize in an explicit way the fault patterns, including the timing and probabilistic aspects of the system. This allows us to provide a set of necessary and sufficient conditions for the notions of strong diagnosability and tA diagnosability. Another advantage of the proposed method is the use of a diagnoser of reduced size instead of a full size state estimator. This reduction in size of the estimator is obtained by defining the type of output needed to return a diagnosis decision (with respect to the considered fault pattern). Consequently, the use of such a diagnoser of reduced size is interesting if one aims to use the diagnoser during the online operation of the system (e.g., to save on storage requirements). We propose also a sufficient condition for the weaker notion of tAA-diagnosability. This condition is based on a simple comparison of a set of elementary matrices that extract the timing and probabilistic aspects of each absorbing strongly connected component of the verifier and that are useful to separate identical logical behaviours in the long run. To conclude, the proposed model is compact, and gives an explicit understanding of the considered system and pattern.

The rest of the paper is structured as follows. Section 2 reviews related works whereas Section 3 is about the preliminaries: the basic definitions of a labeled stochastic PN and a logical fault pattern net are detailed. Section 4 is about the diagnosability of labeled stochastic PNs from the perspective of the fault patterns. In Section 5, conditions for strong and also weaker notions of diagnosability of the fault patterns are derived. Section 6 concludes the paper.

2 Related works

This section aims to provide an overview of the diagnosis methods for discrete event systems based on PN formalisms. Most of the existing approaches have been developed for logical nets (i.e., untimed and non-probabilistic models) where single fault events are modeled with some silent transitions and diagnosis is developed in a centralized perspective [48].

One method is based on explanations and basis markings [8]. An explanation of an observable transition is a (possibly empty) sequence of silent transitions that enable the firing of this observable transition. Assuming that there are no cycles of silent transitions, tracking of explanations is reduced to tracking of the firing vectors of such sequences (i.e., without needing to track the order in which firings take place in those sequences). Basis markings that correspond to the markings the explanations lead to, are consequently computed. Finally, a fault is detected and isolated when all minimal explanations include the firing of the considered transition. This procedure is based on matrix multiplications and the manipulation of integer constraint sets. In the case of bounded net systems, the basis reachability graph can be calculated off-line to provide fast on-line diagnosis. However, a very large memory size may be required for this graph. To the best of our knowledge, this method is restricted to simple logical faults and has not been extended to the time domain or to complex fault patterns.

The mathematical formalism of PNs also allows the use of Integer Linear Programming (ILP) to perform diagnosis and investigate diagnosability. Apart from a preliminary study about the structural properties of T-invariants [42], a series of works focused on the use of ILP to formulate conditions for diagnosability based on g-markings and interpreted diagnosers [3], [15]. In addition, the authors in [45] combine a redundancy-building method and ILP formulations for diagnosis issues. Just like the previous ones, this method is also restricted to simple logical faults; it has been extended to the time domain in [4] but seems difficult to adapt to complex fault patterns.

Interesting approaches have also been inspired from the twin-plant/verifier approaches initialy developed for automata. In particular, the authors in [9] have developed an approach for analyzing diagnosability of unbounded Petri nets on the basis of a net called ‘verifier net’ and the corresponding coverability graph. In fact, the verifier net is obtained by a (parallel) composition of the PN model and a copy that depicts only the normal behavior. The authors in [29] combine positive and negative basis reachability graphs in a dual verifier that is used for diagnosability verification. The approaches based on the design of a verifier net are quite similar to our work. The idea is to design first a verification structure and then to derive the condition for diagnosis and / or diagnosability in terms of this structure. Unfortunately, the previous approaches are restricted to logical nets and simple fault events.

Other works have also exploited the structure of Petri nets, but in different ways: net unfoldings that avoid having to reconstruct all possible reachable markings [5], distributed diagnosis that analyzes information in local modules

preted Petri nets [34]. Decidability and complexity issues are studied in [46]. The problem of combinatorial explosion in diagnosability problems has been considered in detail in [28] and some reduction rules have been proposed to reduce computational complexity. Again, it is worth noting that the previous approaches have not been extended in the timed / probabilistic domain and cannot handle complex fault patterns. The rest of this discussion focuses on the few contributions that have considered these aspects.

Unlike the previous works mentioned above, our interest focuses on the diagnosis of fault patterns. Patterns are used to model behaviors of interest [22] or even system specifications [10], and they are also suitable to model faulty behaviors. In the diagnosis framework, patterns are a way to extend the notion of fault events by introducing more complex behaviors (i.e., some specific ordering of events occurring in the system). An event of the pattern, when viewed independently from other events, might not necessarily be a fault event by itself; however, the occurrence of all events of the pattern in a specific order might trigger a fault condition. Consequently, patterns are suitable to study a wide range of diagnosis problems: simple fault events, multiple faults, fault repetitions and more generally any behavior of interest. In addition, using patterns has the advantage to separate explicitly the behavioral model of the system and the objectives of the diagnosis tasks. The difficulty with the diagnosis of fault patterns is that the problem can no longer be approached as a silent event detection problem but should instead be reformulated as a a state isolation problem in a more complex structure (compared to the system itself) or solved with a more complicated diagnosis function. This second option is exactly the proposition developed in [18] where the detection of fault patterns is solved according to a matching function. Unfortunately, such an approach holds only for strong (i.e., logical) diagnosability reserved for a specific subclass of labeled Petri nets - namely labeled prioritized Petri nets. Compared to that work, our proposed approach does not require the use of priority on the transitions and uses the timed / probabilistic setting to refine diagnosability conditions in the long run. In [33], the same authors replace the matching function by a pattern matching product that results in an augmented net. Thanks to a model-checking approach, they improve the computational complexity, but one should notice that the approach is restricted to safe nets and that the proposed approach fails to provide any formal proof of the diagnosability of a given system. Some other contributions (based on a similar composition of the system by the pattern of interest) have been considered for the diagnosability of fault patterns in the framework of automata [22], [44]. It is worth noting that the previous approaches have been developed for logical systems and do not take advantage of timing information.

Our contribution considers not only logical but also timed / probabilistic aspects, and is suitable to study weaker notions of diagnosability (i.e., tA and tAA-diagnosability) as discussed later in the paper. Only a few approches have been developed in a timed or / and probabilistic setting with methods based on stochastic PNs. In [36], even if timing and probabilistic aspects have not been included at the net level, the authors introduced the notion of a firing sequence likehood in pure labeled PNs. They evaluated a fault event belief that is defined as the proportion of fault sequences (with respect to all acceptable sequences) consistent with a sequence of logical observations. Similar to our approach, the authors in [1] address the problem in a timed probabilistic setting using safe stochastic PNs where faults are also simple events. They study alarm correlation by using the concurrence of events in order to separate and simplify state estimation in a faulty system, and also evaluate the likehood of faulty sequences. Although, this approach has introduced probabilities at the net level, it does not consider the diagnosability characterization. Moreover, this approach only applies to safe nets and for simple fault events. The diagnosis of simple fault events has been also studied with labeled timed PNs in [4].The authors define a modified state class graph that allows an exhaustive representation of the evolution of the timed system. The diagnosis problem is then solved by a linear programming approach in this graph. Different from stochastic PNs, time PNs associate a time interval to each transition and probabilities are not considered. Thanks to the timing information, it becomes possible to refine diagnosis by analysing the time when the events occur, but the approach is not suitable to refine diagnosability of stochastic PNs in the long run because it does not include any probabilistic aspect. In addition, the approach has not been extended to fault patterns. Note that similar problems have been studied with automata in order to discuss diagnosability in a timed deterministic setting. In [12], [7], diagnosability of fault events is considered for the deterministic timed automata introduced in [2].

Finally, some approaches have been proposed for the diagnosability of simple fault events in a timed / probabilistic setting with methods based on stochastic automata. In [39], diagnosability is considered for stochastic timed automata defined as continuous-time Markov models and the notions of A and AA diagnosability (previously studied by the author in [38] and [6] for stochastic untimed automata) are extended in the time domain. More specifically, the notions of $tA-$ and tAA-diagnosability are introduced and analyzed based on the structure of a suitable diagnoser. Our contribution is developed in the same context and extends the previous results in the following directions: (i) by replacing stochastic automata by stochastic PNs, the modeling aspects are improved to consider a larger class of systems (allowing for parallelism and synchronization); (ii) by considering fault patterns instead of simple fault events, the application of the

3 Preliminaries

3.1 Petri nets

Definition 1 *The structure of a Petri net model for a given discrete event system (DES) is defined as* $PN = (P^s, T^s, W^s_{PR}, W^s_{PO})$*, where* $P^s = \{p_1, ..., p_n\}$ *is a set of n places,* $T^s = \{t_1, ..., t_q\}$ *is a set of q transitions and* $W^s_{PR} \in \mathbb{N}^{n\times q}$ *and* $W^s_{PO} \in \mathbb{N}^{n\times q}$ *are respectively the pre- and post-incidence matrices (*$\mathbb{N}$ *is the set of non-negative integer numbers).*

Matrix $W^s = W^s_{PO} - W^s_{PR}$ is the incidence matrix and (PN, M^s_I) denotes a marked PN (or equivalently a PN system) with initial marking $M^s_I \in \mathbb{N}^n$. $M^s \in \mathbb{N}^n$ denotes the net marking vector and $M^s(p)$ is the marking of place p (the indices of the places are used in the next to refer to the position of the entries in a given marking vector or incidence matrix).

Let us define the preset of a given transition t (resp. a given place p) as the subset of places p' (resp. the subset of transitions t') such that $w^s_{PR}(p',t) > 0$ (resp. $w^s_{PO}(p,t') > 0$). Here $w^s_{PR}(p',t)$ and $w^s_{PO}(p,t')$ refer to the entries of matrices W^s_{PR} and W^s_{PO} corresponding to place p' or p and transition t or t' (the indices of the places and transitions are used in the next to refer to the rows and columns of entries in matrices). The preset of t (resp. p) is denoted as $^\bullet(t)$ (resp. $^\bullet(p)$). Similarly, the postset of a given transition t (resp. a given place p) is defined as the subset of places p' (resp. the subset of transitions t') such that $w^s_{PO}(p',t) > 0$ (resp. $w^s_{PR}(p,t') > 0$). The postset of t (resp. p) is denoted as $(t)^\bullet$ (resp. $(p)^\bullet$). By firing t, we obtain a new marking $M'^s = M^s + W^s(:,t)$, where $W^s(:,t)$ denotes the column of W^s corresponding to transition t. This fact can be denoted by $M^s[t\rangle M'^s$ and $T^s(M^s, M'^s) \subseteq T^s$ is defined as the subset of transitions t such that $M^s[t\rangle M'^s$ (t can fire from M^s only if $M^s - W^s_{PR}(:,t) \geq 0$). A firing sequence σ is a sequence of transitions that consecutively fire from a given M^s; one writes $M^s[\sigma\rangle M'^s$ and M'^s is said to be reachable from M^s. Such a firing sequence is written as $\sigma = t_{j_1} t_{j_2} \cdots t_{j_h}$, where $j_1, j_2, \ldots, j_h$ are the indices of the transitions. When σ fires from marking M^s, it is associated to the trajectory

$$(\sigma, M^s) = M^s(0)[t_{j_1}\rangle M^s(1)[t_{j_2}\rangle \cdots M^s(h-1)[t_{j_h}\rangle M^s(h), \tag{1}$$

where $M^s(0) = M^s$. We call $M^s(h)$ the final marking of (σ, M^s). In the next, K-bounded nets are considered (i.e., nets for which the marking of each place does not exceed K). In this case, the number of markings that are reachable from the initial marking M^s_I is finite, and is denoted by N^s. We use $R^s = \{M^s_1, M^s_2, M^s_3, ..., M^s_{N^s}\}$ to denote the set of all reachable markings from M^s_I. In addition, we use $\mathscr{L}(M^s_I)$ to refer to the set of firing sequences $\sigma \in (T^s)^*$ such that $M^s_I[\sigma\rangle$ ($(T^s)^*$ refers to the set of firing sequences of finite length (but arbitrarily long), composed of transitions in T^s). In a certain sense, $\mathscr{L}(M^s_I)$ can be viewed as the language of the net.

3.2 Labeled stochastic Petri nets

Stochastic Petri nets have been defined to deal with stochastic and timing aspects in DESs [31], [20].

Definition 2 *A stochastic Petri net (SPN) system is defined as* (PN, M^s_I, μ)*, where* (PN, M^s_I) *is a Petri net system and* $\mu \in (\mathbb{R}^+)^q$ *(where* $\mathbb{R}^+$ *is the set of strictly positive real numbers) is a firing rate vector. It is assumed that (i) the firing delays of all transitions are exponentially distributed with independent random variables; (ii) the time semantic is characterized by monoserver, race and resampling memory policies [20].*

In details, the firing delays of a given transition $t \in T^s$ are exponentially distributed with firing parameter $\mu(t) \in \mathbb{R}^+$ and measured in time units (TU). The monoserver[1] policy allows a single instance of firing of t at M^s if $M^s[t\rangle$). Race is used as a choice policy in case of conflict or concurrence: the transition that will fire next is the transition with the shortest firing delay. Finally, at each firing, the clocks of all enabled transitions are reset. Observe that other time semantics may also be defined [20].

Important characteristics about the transient and the steady state of the SPN behavior can be obtained from the analysis of a continuous time Markov model that can be obtained from the reachability graph of the net and represents the timing and probabilistic aspects of the marking variation [20]. Given a certain time $\tau \in \mathbb{R}^+$, the marking of the SPN (resp. of the place p) at τ will be referred to as $M^s(\tau)$ (resp. $M^s(p,\tau)$) and the probability that at τ the marking

[1] The monoserver policy can be explicitly incorporated at the PN structure level by adding a place in self-loop with each transition, such that its initial marking equals 1.

(resp. the marking of a certain place p) has a certain value α will be referred to as $Prob(M^s(\tau)=\alpha), \alpha \in \mathbb{N}^n$ (resp. $Prob(M^s(p,\tau)=\alpha), \alpha \in \mathbb{N}$. In addition, the matrix G^s of dimension $N^s \times N^s$ is the generator matrix of the underlying continuous time Markov process that is defined by

- for all $M^s, M'^s \in R^s$, $M^s \neq M'^s$, $G^s(M^s, M'^s) = \sum_{t \in T^s(M^s, M'^s)} \mu(t)$,
- for all $M^s \in R^s$, $G(M^s, M^s) = \sum_{M'^s \neq M^s} -G(M^s, M'^s)$.

A timed firing sequence σ_τ fired from some marking M^s is written as $\sigma_\tau = (t_{j_1}, \tau_1)\ (t_{j_2}, \tau_2) \cdots (t_{j_h}, \tau_h)$, where $j_1, j_2, \ldots, j_h$ are the indices of the transitions, $\tau_1, \tau_2, \ldots, \tau_h$ represent the firing instants, and $0 \leq \tau_1 \leq \tau_2 \leq \cdots \leq \tau_h$. Note that $\tau(\sigma_\tau) = \tau_h$ is the duration of σ_τ. Given σ_τ and a time $\tau \geq \tau_h$, the timed trajectory associated with σ_τ within $[0, \tau)$, starting at M^s is defined by

$$(\sigma_\tau, M^s, \tau) = M^s(0)[(t_{j_1}, \tau_1)\rangle M^s(1)[(t_{j_2}, \tau_2)\rangle \cdots M^s(h-1)[(t_{j_h}, \tau_h)\rangle M^s(h), \tag{2}$$

where $M^s(0) = M^s$. Observe that there is no firing within $[\tau_h, \tau)$.

Labeled Petri nets (LPNs) have been intensively used for diagnosis issues with Petri nets. We assume that the transitions of the net can be partitioned into two subsets: the subset of observable transitions T_o^s that deliver a label in a set of labels Q and the subset of silent transitions T_u^s that do not. The labeling function $L : T^s \to Q \cup \{\varepsilon\}$ is defined such that for each $t \in T_o^s$, $L(t) \in Q$ and for each $t \in T_u^s$, $L(t) = \varepsilon$, where ε stands for the empty string. There is no difficulty to extend L recursively to any firing sequence: $L : (T^s)^* \to Q^*$ such that $L(\varepsilon) = \varepsilon$ and $L(\sigma t) = L(\sigma)L(t)$.

Definition 3 *A labeled Petri net system $LPN = (PN, M_I^s, L)$ is a Petri net system (PN, M_I^s) where the firing of some transitions is observable according to the labeling function L.*

A labeling function in the time domain is also defined recursively by $L_\tau : (T^s \times \mathbb{R}^+)^* \to (Q \times \mathbb{R}^+)^*$ with (i) $L_\tau(\varepsilon) = \varepsilon$, (ii) $L_\tau((t_{j_h}, \tau_h)) = (L(t_{j_h}), \tau_h)$ if $t_{j_h} \in T_o^s$ and $(L_\tau((t_{j_h}, \tau_h)) = \varepsilon$ if $t_{j_h} \in T_u^s$, (iii) $L_\tau(\sigma_\tau(t_{j_h}, \tau_h)) = L_\tau(\sigma_\tau)(L(t_{j_h}), \tau_h)$ if $t_{j_h} \in T_o^s$ and $L_\tau(\sigma_\tau(t_{j_h}, \tau_h)) = L_\tau(\sigma_\tau)$ if $t_{j_h} \in T_u^s$. In addition, a mask function that erases the time stamps is defined by $H : (T^s \times \mathbb{R}^+)^* \to (T^s)^*$ with (i) $H(\varepsilon) = \varepsilon$, (ii) $H((t_{j_h}, \tau_h)) = t_{j_h}$, (iii) $H(\sigma_\tau(t_{j_h}, \tau_h)) = H(\sigma_\tau)t_{j_h}$. Observe that $L(H(\sigma_\tau)) = H(L_\tau(\sigma_\tau))$.

Definition 4 *A labeled stochastic Petri net system $LSPN = (PN, M_I^s, L, \mu)$ is a stochastic Petri net system (PN, M_I^s, μ) where the firing of some transitions is observable according to the labeling function L.*

To avoid unbounded silent firing sequences, consistent with a given finite sequence of observed labels σ_o, the silent part of the considered LSPN is assumed to be acyclic.

Example 1: Consider the example of the LSPN in Fig. 1 where $P^s = \{p_1, p_2, p_3, p_4, p_5\}$, $T^s = \{t_1, t_2, t_3, t_4, t_5, t_6\}$ and $M_I^s = (2,0,0,0,0)^T$. $Q = \{a, b, c\}$ is the set of labels and the labeling function is defined such that $L(t_2) = L(t_5) = a$, $L(t_3) = b$, $L(t_6) = c$, $L(t_1) = L(t_4) = \varepsilon$. In addition, a rate $\mu(t)$ is defined for each transition $t \in T^s$. For simplicity, these rates are all assumed to equal to 1. In Fig. 1, labels and rates are reported near the transitions.

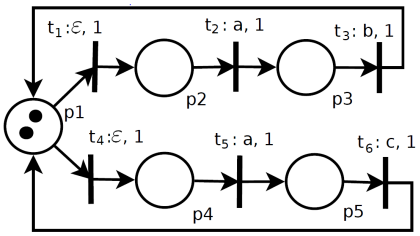

Fig. 1 An example of an LSPN model.

In the context of fault diagnosis, some particular sequences of transitions (eventually some individual transitions) are of interest because such sequences correspond to faulty behaviours of the considered systems [22], [44]. They will be referred to as *fault patterns* in the next.

Definition 5 *A fault pattern Σ_F of a given PN system (PN, M_I^s) is defined as a set (possibly of infinite cardinality) of firing sequences of finite length (but arbitrarily long): $\Sigma_F \subseteq \mathscr{L}(M_I^s)$.*

In this paper, the fault patterns are represented with a particular subclass of Petri net systems, namely *logical fault pattern nets* and a *synchronization function* that explains how the fault pattern net is connected with the LSPN.

Definition 6 *Given a K-bounded labeled stochastic Petri net system $LSPN = (P^s, T^s, W_{PR}^s, W_{PO}^s, M_I^s, L, \mu)$, and a subset $T_{sync} \subseteq T^s$ of r transitions, a logical fault pattern net is a pair (FPN, SF) such that FPN is a Petri net system $FPN = (P^F, T^F, W_{PR}^F, W_{PO}^F, M_I^F)$ and SF is a synchronization function having the following properties:*

- *$P^F = \{N_1, ..., N_m, F\}$ is a set of $m+1$ places where F is the single trapping place of the net: $(F)^\bullet = \emptyset$,*
- *T^F is a set of $m \times r$ transitions,*
- *$SF : T_{sync} \times (P^F \setminus \{F\}) \rightarrow T^F$ is a bijective function, i.e., SF associates each transition t' in T^F with a single pair $(t, p) \in T_{sync} \times (P^F \setminus \{F\})$,*
- *$(P^F, T^F, W_{PR}^F, W_{PO}^F, M_I^F)$ is a state graph: every transition has one incoming arc (i.e., $|^\bullet(t')| = 1$, $t' \in T^F$), and one outgoing arc (i.e., $|(t')^\bullet| = 1$, $t' \in T^F$), and all reachable markings have exactly one token,*
- *each place $p \in P^F \setminus \{F\}$ has exactly r outgoing arcs and r transitions in its postset such that $(p)^\bullet = \{SF(t,p),\ t \in T_{sync}\}$, ,*
- *M_I^F is such that $M_I^F(N_1) = 1$ and $M_I^F(p) = 0$ for all $p \in P^F \setminus \{N_1\}$.*

Observe that the transitions in set T_{sync} characterize the pattern of interest. The set $\{N_1, ..., N_m\}$ corresponds to the normal places of FPN, whereas F corresponds to the single fault place. There is no difficulty to extend the previous definition to nets that characterize multiple fault patterns by introducing a set of multiple fault places $\{F_1, F_2, ...\}$, but this will not be pursued further in the interest of simplicity.

Example 2: In Fig. 2, we consider several examples of logical fault pattern nets for the DES modeled with the LSPN in Fig. 1. For each transition $t' \in T^F$, the denomination within brackets $(t_{j,p})$ refers to the transition $t_j \in T_{sync}$ and to the place $p \in P^F \setminus \{F\}$ of the LSPN in Fig. 1 such that $t' = SF(t,p)$. Such denominations will be used later in a particular composition of the LSPN with the fault pattern net according to the synchronization function.

$(FPNa, SFa)$ in Fig. 2(a) is the fault pattern net corresponding to the situation where the transition t_1 of the LSPN in Fig. 1 is considered as a simple fault transition: N is the single normal place and F is the fault place. $T_{sync} = \{t_1\}$ and the synchronization function is defined by $SFa(t_1, N) = t_1'$. $(FPNa, SFa)$ aims to detect the set of sequences $\Sigma_{Fa} = \{(T^s \setminus \{t_1\})^* t_1 (T^s)^*\}$ in the LSPN.

(FPb, SFb) in Fig. 2(b) recognizes the repetition of the firings of t_1 at least twice during the system operation no matter how the system behaves between the two firings of t_1. Observe that the two transitions t_1' and t_2' of $FPNb$ correspond to the two successive firings of the same transition t_1 of the LSPN in Fig. 1. $N = \{N_1, N_2\}$ is the set of normal places and F is the fault place. $T_{sync} = \{t_1\}$ and the synchronization function is defined by $SFb(t_1, N_1) = t_1'$, and $SFb(t_1, N_2) = t_2'$ and leads to the denominations t_{1,N_1} for the first firing of t_1 and t_{1,N_2} for the second firing of the same transition. $(FPNb, SFb)$ aims to detect the set of sequences $\Sigma_{Fb} = \{(T^s \setminus \{t_1\})^* t_1 (T^s \setminus \{t_1\})^* t_1 (T^s)^*\}$ in the LSPN.

$(FPNc, SFc)$ in Fig. 2(c) recognizes the occurrence of either one of two possible fault transitions t_1 and t_4 in the LSPN in Fig. 1: N is the single normal place and F is the fault place. $T_{sync} = \{t_1, t_4\}$ and the synchronization function is defined by $SFc(t_1, N) = t_1'$, and $SFc(t_4, N) = t_2'$. $(FPNc, SFc)$ aims to detect the set of sequences $\Sigma_{Fc} = \{(T^s \setminus \{t_1, t_4\})^* t_1 (T^s)^*, (T^s \setminus \{t_1, t_4\})^* t_4 (T^s)^*\}$ in the LSPN. Note that $(FPNc, FSc)$ does not identify which fault has occurred (or which fault has occurred first). If one is interested in fault isolation, there is no difficulty to design two fault pattern nets, the first one with a place F_1 detecting that fault transition t_1 occurred first and the second one with a place F_2 detecting that fault transition t_4 occurred first.

$(FPNd, SFd)$ in Fig. 2(d) is sensitive to the occurrence of the firing sequences that contain both t_1 and t_4 in the LSPN in Fig. 1, regardless of the order in which the two transitions fire and how the system behaves between the firings of t_1 and t_4: $N = \{N_1, N_2, N_3\}$ is the set of normal places, F is the fault place, $T_{sync} = \{t_1, t_4\}$ and the synchronization function is defined by $SFd(t_1, N_1) = t_1'$, $SFd(t_4, N_3) = t_2'$, $SFd(t_1, N_3) = t_3'$, $SFd(t_4, N_1) = t_4'$, $SFd(t_1, N_2) = t_5'$ and $SFd(t_4, N_2) = t_6'$. $(FPNd,\ SFd)$ aims to detect the set of sequences $\Sigma_{Fd} = \{(T^s \setminus \{t_1, t_4\})^* t_1 (T^s \setminus \{t_1, t_4\})^* t_4\ (T^s)^*$, $(T^s \setminus \{t_1, t_4\})^* t_4 (T^s \setminus \{t_1, t_4\})^* t_1 (T^s)^*\}$ in the LSPN.

$(FPNe, SFe)$ in Fig. 2(e), with $N = \{N_1, N_2, N_3\}$ being the set of normal places and F being the fault place, is sensitive to more complex faulty behaviours in the LSPN in Fig. 1: the repetition of the firing of t_1 twice during the system

operation without experiencing the firing of t_4 more than once between the two successive firings of t_1 (but perhaps experiencing other transition firings). $T_{sync} = \{t_1, t_4\}$ and the synchronization function is defined by $SFe(t_1, N_1) = t'_1$, $SFe(t_1, N_3) = t'_2$, $SFe(t_4, N_3) = t'_3$, $SFe(t_4, N_1) = t'_4$, $SFe(t_4, N_2) = t'_5$ and $SFe(t_1, N_2) = t'_6$. $(FPNe, SFe)$ aims to detect the set of sequences $\Sigma_{Fe} = \{(T^s \setminus \{t_1, t_4\})^* t_1 (T^s \setminus \{t_1, t_4\})^* t_1 (T^s)^*,\ (T^s \setminus \{t_1, t_4\})^* t_1 (T^s \setminus \{t_1, t_4\})^* t_4 (T^s \setminus \{t_1, t_4\})^* t_1 (T^s)^*\}$ in the LSPN.

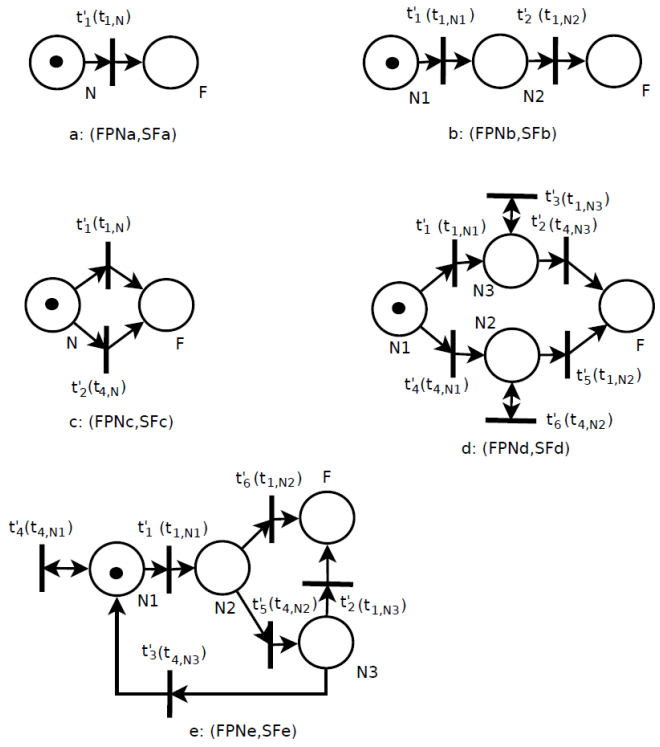

Fig. 2 Examples of logical fault pattern nets.

4 Diagnosability of LSPN

In order to study the diagnosability properties of a K-bounded LSPN with respect to a fault pattern, a three-step approach is proposed.

1. First, we define a particular composition of the LSPN with the fault pattern net (FPN, SF). This composition synchronizes some transitions of the LSPN with the transitions of FPN according to the synchronization function SF. We further prove that the resulting net, referred to as a *fault pattern stochastic net* (FPSN), is also a K-bounded LSPN that is able to track exactly the marking probabilities of the original system. The aim is to characterize the pattern of interest with the marking of the place F, i.e., determine whether the marking of the resulting FPSN satisfies $M(F) = 1$.
2. Second, we compute the logical observer of the FPSN by making abstraction of probabilistic and timing aspects. For this purpose, we propose to search for the reachability graph R of the FPSN and represent this graph as a labeled finite automaton A (ignoring the timing aspects) from which we can derive the logical observer using a standard method. This observer is a deterministic finite automaton. Observing that only an estimation of the marking of place F is needed to detect the occurrence of the fault pattern, a diagnoser of reduced size (compared to the logical observer) is computed thanks to a standard reduction method.
3. Third, we perform the parallel composition of A with the observer or diagnoser. On the one hand, we show that strong diagnosability and tA-diagnosability can be characterized according to structural properties of such a composition. On the other hand, we establish that tAA-diagnosability can be characterized according to probabilistic properties of the continous time Markov model that one can derive from the resulting composition.

In this section, we introduce a particular composition of the LSPN with the fault pattern net previously defined, according to the synchronisation function SF and refer to the result of this composition as a *fault pattern stochastic net* (FPSN). For short, we write $FPSN = (LSPN) \times_{SF} (FPN)$.

Let us refer to the r synchronisation transitions as $T_{sync} = \{t_{k_1}, ..., t_{k_r}\}$. As far as SF is a bijective function from $T_{sync} \times (P^F \setminus \{F\})$ to T^F, observe that SF defines a partition of the set T^F and one can write $T^F = T_1^F \cup ... \cup T_r^F$ with $T_h^F = \{t \in T^F$ such that $t = (t_{k_h}, p), p \in P^F - \{F\}\}$, $h = 1, ..., r$. Each subset $T_h^F \subseteq T^F$ is composed by exactly m transitions. For readability, and according to the notation already introduced in Fig. 2, let us refer to the transitions in T_h^F as $t_{k_h,N_1}, ..., t_{k_h,N_m}$. The FPSN is formally defined as follows.

Definition 7 *Consider a K-bounded labeled stochastic Petri net system* $LSPN = (P^s, T^s, W_{PR}^s, W_{PO}^s, M_I^s, L, \mu)$*, a subset* $T_{sync} \subseteq T^s$ *with r transitions, a fault pattern* Σ_F *represented by* (FPN, SF) *with* $FPN = (P^F, T^F, W_{PR}^F, W_{PO}^F, M_I^F)$ *with* $m+1$ *places and* $m \times r$ *transitions, and a given synchronisation function SF. The fault pattern stochastic net* $FPSN = (LSPN) \times_{SF} (FPN)$ *is the net defined by* $FPSN = (P, T, W_{PR}, W_{PO}, M_I, L, \mu)$ *with:*

- $P = P^s \cup P^F$ *a set of* $n + m + 1$ *places,*
- $T = T^s \cup T^F$ *a set of* $q + m \times r$ *transitions,*
- *the incidence matrices are defined by:*
  - $w_{PR}(p,t) = w_{PR}^s(p,t)$ *and* $w_{PO}(p,t) = w_{PO}^s(p,t)$ *for* $p \in P^s$ *and* $t \in T^s$*,*
  - $w_{PR}(p, t_{k_h,p}) = w_{PR}^F(p, t_{k_h,p})$*,* $w_{PO}(p, t_{k_h,p}) = w_{PO}^F(p, t_{k_h,p})$ *for* $p \in P^F$ *and* $t_{k_h,p} \in T_h^F$*,* $h = 1, ..., r$*,*
  - $w_{PR}(p', t_{k_h,p}) = w_{PR}^s(p', t_{k_h})$ *and* $w_{PO}(p', t_{k_h,p}) = w_{PO}^s(p', t_{k_h})$ *for* $p' \in P^s$ *and* $t_{k_h,p} \in T_h^F$*,* $h = 1, ..., r$*,*
  - $w_{PR}(p,t) = w_{PO}(p,t) = 0$ *for* $p \in P^F$ *and* $t \in T^s \setminus T_{sync}$*,*
  - $w_{PR}(F,t) = w_{PO}(F,t) = 1$ *for* $t \in T_{sync}$*,*
- *the firing rate of each transition* $t_{k_h,p} \in T_h^F$ *is defined by* $\mu(t_{k_h,p}) = \mu(t_{k_h})$ *(the firing rates of the transitions* $t \in T^s$ *being unchanged),*
- *the label of each transition* $t_{k_h,p} \in T_h^F$ *is defined by* $L(t_{k_h,p}) = L(t_{k_h})$ *(the labels of the transitions* $t \in T^s$ *being unchanged),*
- M_I *is the initial marking that satisfies* $M_I(N_1) = 1$*,* $M_I(p) = 0$*, for all* $p \in (P^F \setminus \{N_1\})$*, and* $M_I(p) = M_I^s(p)$ *for all* $p \in P^s$*.*

In the next, we will refer to the marking of a given FPSN as M, compared to the marking of the original LSPN that is referred to as M^s.The FPSN has the advantage of characterizing in an explicit way the fault pattern we are interested in. In particular, as stated in Lemma 1 below, it has a property of monotonicity with respect to the marking of the place F. Observe also that, for a given $h = 1, ..., r$, it is not possible for two transitions $t_{k_h,p}$ and $t_{k_h,p'}$ to be simultaneously enabled in the FPSN as long as the fault pattern net is a safe net.

Lemma 1: Given an FPSN and two given times $\tau, \tau' \in \mathbb{R}^+$, $\tau' \geq \tau$, then $M(F, \tau') = 1$ if $M(F, \tau) = 1$.

Proof : Observe that the place F is in the postset of the transitions $t_{k_h,p}$, $h = 1, .., r$, $p \in \{N_1, \cdots, N_m\}$. On the contrary, F is only in the preset of transitions t_{k_h}, $h = 1, .., r$, and there are selfloops between F and t_{k_h}. Consequently, the token is trapped in F and $M(F, \tau') = 1$ as far as $M(F, \tau) = 1$ and $\tau' \geq \tau$. □

Proposition 1: Given a K-bounded labeled stochastic Petri net system and a fault pattern Σ_F represented by (FPN, SF), then $FPSN = (LSPN) \times_{SF} (FPN)$ is also a K-bounded labeled stochastic net, and satisfies $Prob(M(p,\tau) = \alpha) = Prob(M^s(p,\tau) = \alpha)$, for all $p \in P^s$, $\alpha \in \mathbb{N}$ and $\tau \in \mathbb{R}^+$ (where $M(p,\tau)$ refers to the marking of place p at time τ in the FPSN).

Proof : First we prove that the net resulting from the composition of an LSPN with an FPN is a K-bounded net. Observe that the fault pattern net is a safe net (and consequently is 1-bounded). The set of places P^F is a P-invariant in the FPN and also in the FPSN, i.e., $M(N_1) + ... + M(N_m) + M(F) = 1$. Consequently, the places of the FPSN that belong to P^F are 1-bounded. Now, observe how the transitions in T^F are connected to the rest of the net: the P-invariants of the LSPN are conserved by the composition induced by the synchronization function SF and consequently the places of the FPSN that belong to P^s are K-bounded. To conclude, the FPSN is a K-bounded net.

Second, consider any place $p \in P^s$. Place p may have one or several subsets of $m+1$ synchronization transitions of the form $\{t_{k_h,N_1}, ..., t_{k_h,N_m}, t_{k_h}\}$ in its preset or in its postset. For a given $\tau \in \mathbb{R}^+$, no concurrent firing exists within the subset of transitions $\{t_{k_h,N_1}, ..., t_{k_h,N_m}, t_{k_h}\}$. As far as a monoserver policy is used, the probability that a token moves from a place $p \in P^s$ to another place $p' \in P^s$ is the same in the LSPN and the FPSN. Moreover, the distribution of the firing

delays for each transition $t \in T^s$ is the same in the LSPN and the FPSN, and the distribution of the firing delays for each transition $t_{k_h,p} \in T_h^F$, $p \in P^F$, is the same as the distribution of the firing delays of the transition $t_{k_h} \in T_{sync}$.We conclude that $Prob(M(p,\tau) = \alpha) = Prob(M^s(p,\tau) = \alpha)$ for any $p \in P^s$. □

Example 3: Consider the example of the LSPN in Fig. 1 and the fault pattern Σ_{Fb} represented by $(FPNb, SFb)$ in Fig. 2(b). The resulting FPSN is detailed in Fig. 3. This net is a labeled stochastic Petri net that is 2-bounded. The reachability set R of this net has 33 markings that are detailed in Table 1.The markings of the places N_1, N_2 and F correspond to the three last entries of vector M. One can notice that the place F of the FPSN provides explicit information about the occurrence of the fault pattern under interest. All markings M such that $M(F) = 1$ result from a firing sequence (originating from M_I) that includes at least two firings of transition t_1, whereas all markings M such that $M(F) = 0$ result from a firing sequence that includes zero or one firing of the transition t_1.

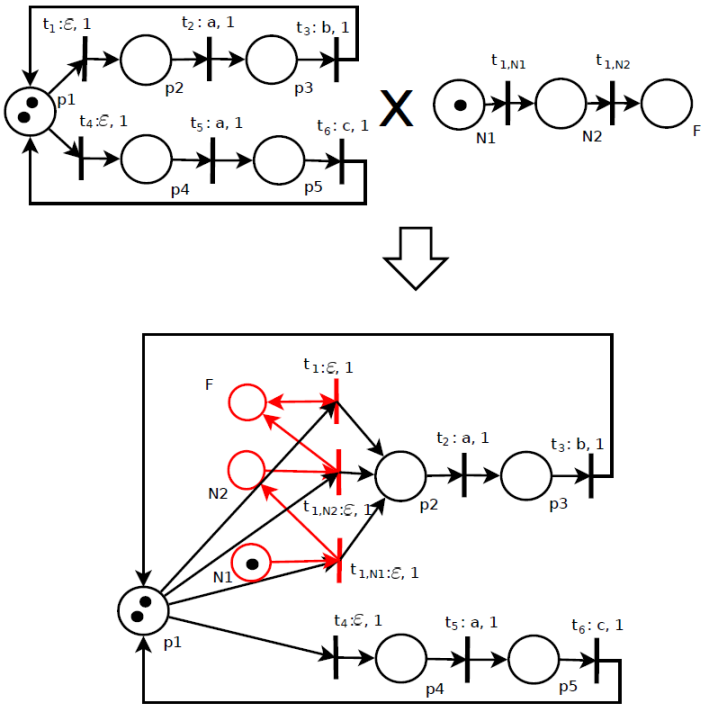

Fig. 3 FPSN obtained by composing the LSPN in Fig. 1 with the pattern Σ_{Fb}.

4.2 Logical observer and diagnoser design

To obtain a logical diagnoser of a given LSPN with respect to a fault pattern net Σ_F, we build first the FPSN and compute its reachability graph. The FPSN is a K-bounded net, consequently its reachability graph has a finite number of N_A markings. Making abstraction of the timing aspects, the reachability graph is associated to a labeled finite automaton $A = (X_A, T, \Delta_A, x_{A0}, L, Q \cup \{\varepsilon\})$ where X_A is the set of N_A states, each state being associated to a given marking; T is the set of transitions of the FPSN, and it is interpreted as the set of events; Δ_A is the transition relation such that $\Delta_A(M, q, M')$ is defined if there exists a transition $t \in T$ with $M[t\rangle M'$ and $L(t) = q$ with $q \in Q \cup \{\varepsilon\}$; x_{A0} corresponds to the initial marking M_0, and L and Q are respectively the labeling function and the set of labels. A is basically a non-deterministic automaton due to the labeling function that erases the labels of unobservable transitions and makes indiscernible the transitions that share the same label.

A standard approach (that transforms a non-deterministic automaton into a deterministic one) is used to compute the logical observer of A [11]. Each state of the resulting observer is a subset of markings in the reachability set R . The markings include not only the complete information about the system states but also the information about the occurrence of the fault pattern. In particular, $M(F) = 1$ indicates that the fault pattern has occurred. We propose also in this section a

$Fb\cdot$

M	Detail	M	Detail
M_0	$(2\,0\,0\,0\,0\,1\,0\,0)^T$	M_{17}	$(0\,0\,0\,0\,2\,1\,0\,0)^T$
M_1	$(1\,1\,0\,0\,0\,0\,1\,0)^T$	M_{18}	$(1\,0\,1\,0\,0\,0\,0\,1)^T$
M_2	$(1\,0\,0\,1\,0\,1\,0\,0)^T$	M_{19}	$(0\,1\,0\,1\,0\,0\,0\,1)^T$
M_3	$(0\,2\,0\,0\,0\,0\,0\,1)^T$	M_{20}	$(0\,0\,0\,2\,0\,0\,1\,0)^T$
M_4	$(1\,0\,1\,0\,0\,0\,1\,0)^T$	M_{21}	$(1\,0\,0\,0\,1\,0\,1\,0)^T$
M_5	$(0\,1\,0\,1\,0\,0\,1\,0)^T$	M_{22}	$(2\,0\,0\,0\,0\,0\,0\,1)^T$
M_6	$(0\,0\,0\,2\,0\,0\,1\,0)^T$	M_{23}	$(0\,0\,1\,1\,0\,0\,0\,1)^T$
M_7	$(1\,0\,0\,0\,1\,1\,0\,0)^T$	M_{24}	$(0\,1\,0\,0\,1\,0\,0\,1)^T$
M_8	$(0\,1\,1\,0\,0\,0\,0\,1)^T$	M_{25}	$(0\,0\,0\,1\,1\,0\,1\,0)^T$
M_9	$(2\,0\,0\,0\,0\,0\,1\,0)^T$	M_{26}	$(1\,0\,0\,1\,0\,0\,0\,1)^T$
M_{10}	$(0\,0\,1\,1\,0\,0\,1\,0)^T$	M_{27}	$(0\,0\,1\,0\,1\,0\,0\,1)^T$
M_{11}	$(0\,1\,0\,0\,1\,0\,1\,0)^T$	M_{28}	$(0\,0\,0\,0\,2\,0\,1\,0)^T$
M_{12}	$(0\,0\,0\,1\,1\,1\,0\,0)^T$	M_{29}	$(0\,0\,0\,2\,0\,0\,0\,1)^T$
M_{13}	$(0\,0\,2\,0\,0\,0\,0\,1)^T$	M_{30}	$(1\,0\,0\,0\,1\,0\,0\,1)^T$
M_{14}	$(1\,1\,0\,0\,0\,0\,0\,1)^T$	M_{31}	$(0\,0\,0\,1\,1\,0\,0\,1)^T$
M_{15}	$(1\,0\,0\,1\,0\,0\,1\,0)^T$	M_{32}	$(0\,0\,0\,0\,2\,0\,0\,1)^T$
M_{16}	$(0\,0\,1\,0\,1\,0\,1\,0)^T$		

logical diagnoser that is devoted to the estimation of $M(F)$. In most of the cases, the size of the diagnoser will be smaller than the size of the observer.

In order to define the *logical observer*, the following subsets of markings are introduced:

- for each marking $M \in R$, let $X(M,\varepsilon)$ be the set of markings reachable from M by firing zero or more silent transitions t (i.e., $L(t)=\varepsilon$);
- for each marking $M \in R$ and for each label $q \in Q$, let $X(M,q)$ be the set of markings that are reachable from M by firing exactly one transition t such that $L(t)=q$;
- for each marking $M \in R$ and for each label $q \in Q$, let $X_\varepsilon(M,q)$ be the set of markings that are reachable from any marking M in $X(M,q)$ by firing zero or more silent transitions.

Definition 8 *The logical observer for a given FPSN is defined as the triplet (OBS, Y_P, γ_P) where OBS is a deterministic finite automaton $OBS=(X,Q,\Delta_X,x_0)$ and $\gamma_P : X \to 2^{N_A}$ is an output function that associates each state $x \in X$ to the subset of markings in Y_P that is consistent with the observer state x:*

- *X is a set of states;*
- *$Y_P \subseteq 2^{N_A}$ is a set of marking subsets;*
- *Q is the set of observable labels;*
- *Δ_X is the transition function and γ_P is the output function that are defined for all $x \in X$ and $q \in Q$ by $\Delta_X(x,q)=x'$ and $\gamma_P(x')=\cup_{M\in\gamma_P(x)} X_\varepsilon(M,q)$ if $\cup_{M\in\gamma_P(x)} X_\varepsilon(M,q) \neq \emptyset$ (in such a case, there exists at least one combination of an observable transition t with $L(t)=q$, a silent firing sequence σ and two markings $M \in \gamma_P(x)$, $M' \in \gamma_P(x')$ such that $M[t\sigma\rangle M'$);*
- *x_0 is the observer initial state and $\gamma_P(x_0)=X(M,\varepsilon)$.*

Algorithm 1 details the computation of OBS, Y_P and γ_P. This algorithm searches iteratively the states of the observer. Each new state is temporarily saved in the list $UNEx$ and the algorithm ends when the list $UNEx$ is emptied. The final structure OBS has a complexity in space of $O(2^{N_A})$.

Algorithm 1: Logical observer *OBS* of the FPSN

Require: R, M_0, L, Q
Ensure: $X, \Delta_X, x_0, Y_P, \gamma_P$
1: $x \leftarrow 0, x_0 \leftarrow x, X \leftarrow \{x\}, UNEx \leftarrow \{x\}, k \leftarrow 0$
2: $\gamma_P(x) \leftarrow X(M_0, \varepsilon), Y_P \leftarrow \{\gamma_P(x)\}, \Delta_X \leftarrow \emptyset$
3: **while** $UNEx \neq \emptyset$ **do**
4: let x be the first element of $UNEx$
5: remove x from $UNEx$
6: **for** each label $q \in Q$ **do**
7: $z' \leftarrow \emptyset, y' \leftarrow \emptyset$
8: **for** each $M \in \gamma_P(x)$ **do**
9: $z' \leftarrow z' \cup X(M,q)$
10: **end for**
11: **for** each $M \in z'$ **do**
12: $y' \leftarrow y' \cup X(M, \varepsilon)$
13: **end for**
14: **if** $y' \notin Y_P$ **then**
15: $k \leftarrow k+1, x' \leftarrow k, \gamma_P(x') \leftarrow y'$
16: $X \leftarrow X \cup \{x'\}, Y_P \leftarrow Y_P \cup \{y'\}, UNEx \leftarrow UNEx \cup \{x'\}$
17: **else**
18: $x' \leftarrow k$
19: **end if**
20: $\Delta_X(x,q) \leftarrow x'$
21: **end for**
22: **end while**

The *diagnoser* for a given FPSN results from a simplification of the observer. For this purpose, we define the output function $\gamma_{PF} : X \to Y_F$ with $Y_F = \{\{0\},\{1\},\{0,1\}\}$ as:

- $\gamma_{PF}(x) = \{1\}$ if $M(F) = 1$ for all markings $M \in \gamma_P(x)$. In such a case, the fault pattern has certainly occurred thus far;
- $\gamma_{PF}(x) = \{0\}$ if $M(F) = 0$ for all markings $M \in \gamma_P(x)$. In such a case, the fault pattern did not occur thus far;
- $\gamma_{PF}(x) = \{0,1\}$ if $M(F) = 0$ for some markings $M \in \gamma_P(x)$ and $M(F) = 1$ for some other markings $M \in \gamma_P(x)$. In such a case, no conclusion can be stated for the occurrence of the fault.

The modified observer (OBS, Y_F, γ_{PF}) can be viewed as a Mealy machine [30], [35] (i.e., a deterministic finite state automaton with inputs and outputs) with outputs $\gamma_{PF}(x)$, $x \in X$. Consequently, using a standard reduction method [19], (OBS, Y_F, γ_{PF}) is simplified in the input / output sense such that the same sequence of input labels, produces the same sequence of outputs within Y_F. During the simplification process, some states of X are merged so that the total number of states after simplification is, in general, much smaller than the number of states in X .

Let us define the triplet $(DIAG, Y_F, \gamma_F)$ as the result of this simplification where $DIAG = (Y, Q, \Delta_Y, y_0)$ is a deterministic finite automaton with Y being the set of states; Q being the set of observable labels; the output function $\gamma_F : Y \to Y_F$ associating each state $y \in Y$, to the subset of possible markings for the place F; Δ_Y being the transition function such that $\Delta_Y(y,q) = y'$ implies that there exists an observable transition t and two markings $M, M' \in R$ with $M[t\rangle M'$, $M(F) \in \gamma_f(y)$, $M'(F) \in \gamma_f(y')$, and $L(t) = q \in Q$; and y_0 being the diagnoser initial state. $(DIAG, Y_F, \gamma_F)$ is a logical diagnoser because each state $y \in Y$ has an output that indicates explicitly if one can state that the fault pattern has occurred.

Example 4: Consider the example of the LSPN of Fig. 1 and the fault pattern Σ_{Fb} represented by $(FPNb, SFb)$ in Fig. 2(b). The FPSN in Fig. 3 is obtained. The logical observer (OBS, Y_P, γ_P), the transformation of (OBS, Y_P, γ_P) into (OBS, Y_F, γ_{PF}) and diagnoser $(DIAG, Y_F, \gamma_F)$ are respectively presented in Figs. 4, 5 and 6. The details of the states and outputs of (OBS, Y_P, γ_P) and $(DIAG, Y_F, \gamma_F)$ are reported in Table 2 (skip for now the last column of the table). For each reachable marking (see Table 1), the number of tokens in F-place is also reported in brackets in Table 2. Observe that the number of states of the diagnoser is much smaller than the number of states of the observer.

In the remainder of Section 3, we consider a labeled stochastic Petri net system $LSPN = (P^s, T^s, W^s_{PR}, W^s_{PO}, M^s_I, L, \mu)$ that is K-bounded and has a set of synchronization transitions $T_{sync} \subseteq T^s$. Σ_F is the fault pattern and (FPN, SF) with

Fig. 4 Logical observer (OBS, Y_P, γ_P) obtained for the LSPN in Fig. 1 with respect to the pattern Σ_{Fb}.

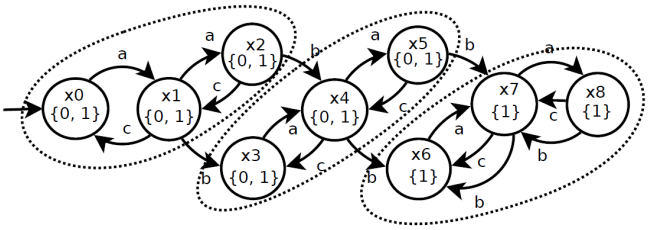

Fig. 5 Construction of (OBS, Y_F, γ_{PF}) from (OBS, Y_P, γ_P).

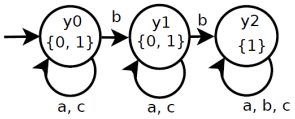

Fig. 6 Diagnoser $(DIAG, Y_F, \gamma_F)$ obtained for the LSPN in Fig. 1 with respect to the pattern Σ_{Fb}.

Table 2 States and outputs of the logical observer and diagnoser for the LSPN in Fig. 1 with respect to the pattern Σ_{Fb}.

x	$\gamma_P(x)$	y	$\gamma_F(y)$	F-certain
x_0	$\{M_0(0), M_1(0), M_2(0), M_3(1), M_5(0), M_6(0)\}$			
x_1	$\{M_4(0), M_7(0), M_8(1), M_{10}(0), M_{11}(0), M_{12}(0)\}$	y_0	$\{0,1\}$	uncertain
x_2	$\{M_{13}(1), M_{16}(0), M_{17}(0)\}$			
x_3	$\{M_3(1), M_9(0), M_{14}(1), M_{15}(0), M_{19}(1), M_{20}(0)\}$			
x_4	$\{M_8(1), M_{18}(1), M_{21}(0), M_{23}(1), M_{24}(1), M_{25}(0)\}$	y_1	$\{0,1\}$	uncertain
x_5	$\{M_{13}(1), M_{27}(1), M_{28}(0)\}$			
x_6	$\{M_3(1), M_{14}(1), M_{19}(1), M_{22}(1), M_{26}(1), M_{29}(1)\}$			
x_7	$\{M_8(1), M_{18}(1), M_{23}(1), M_{24}(1), M_{30}(1), M_{31}(1)\}$	y_2	$\{1\}$	F-certain
x_8	$\{M_{13}(1), M_{27}(1), M_{32}(1)\}$			

$FPN = (P^F, T^F, W^F_{PR}, W^F_{PO}, M^F_I)$ being the fault pattern net that represents Σ_F. $FPSN = (P, T, W_{PR}, W_{PO}, M_I, L, \mu)$ is the fault pattern stochastic net associated to the labeled finite automaton $A = (X_A, T, \Delta_A, x_{A0}, L, Q \cup \{\varepsilon\})$. (OBS, Y_P, γ_P) with $OBS = (X, E, \Delta_X, x_0)$ and $(DIAG, Y_F, \gamma_F)$ with $DIAG = (Y, E, \Delta_Y, y_0)$ are respectively the observer and diagnoser.

4.3 Strong diagnosability

Strong (i.e., logical) diagnosability requires that every occurrence of the fault pattern leads to observations distinct enough to enable identification of the fault pattern within a finite delay. A formal definition of strong diagnosability of fault patterns can be found in [44] for automata and in [18] for Petri nets according to the matching operator. In this work, we propose first a reformulation of the definition of diagnosability of fault patterns with LPN that gets rid of the matching operator.

Definition 9 *A given LSPN is said to be strongly diagnosable with respect to the fault pattern Σ_F if the following holds:*

$(\exists n > 0), (\forall \sigma_1 \in \Sigma_F$ *such that* $M_I^s[\sigma_1\rangle M^s), (\forall \sigma_2 \in (T^s)^*$ *such that* $M^s[\sigma_2\rangle)$
if $|\sigma_2| > n$ *then* $L^{-1}(L(\sigma_1\sigma_2)) \subseteq \Sigma_F$,

where L^{-1} *is defined for any sequence* σ *enabled at* M^s *by* $L^{-1}(L(\sigma)) = \{\sigma' \in (T^s)^*$ *such that* $M^s[\sigma'\rangle$ *and* $L(\sigma') = L(\sigma)\}$.

In order to evaluate the diagnosability of a given LSPN with respect to a given fault pattern in a logical setting, the proposed approach aims to do a parallel-like composition of the automaton A (obtained from the reachability graph of the FPSN) by its logical diagnoser, in order to compute a *fault pattern logical verifier*, denoted by $FPLV = A||DIAG$.

Definition 10 *The* fault pattern logical verifier *of an LSPN with respect to a given fault pattern* Σ_F *is defined as a deterministic finite automaton* $FPLV = (S, T, \Delta, s_0)$ *with*

- $S \subseteq X_A \times Y$;
- $\Delta(s,t) = s'$ *for all* $s = (M,y) \in S$, $s' = (M',y') \in S$, *if there exists* $t \in T$ *with* $\Delta_A(M,t) = M'$, $\Delta_Y(y,q) = y'$ *and* $L(t) = q$;
- $s_0 = (M_0, y_0)$.

The complexity in space of the FPLV is $O(N_A \times 2^{N_A})$. Observe that it is difficult to evaluate the gain in complexity resulting from the replacement of the full size observer by the reduced size diagnoser because of the incompletness of the modified observer (OBS, Y_F, γ_F) that is used for reduction purposes. In the worst case, no reduction is possible and the complexity of the diagnoser is similar to the one of the observer, i.e., $O(2^{N_A})$ in the worst case; however, in most of the cases, we expect that the diagnoser will be much smaller than the observer.

The output function Γ_F can be trivially defined for the FPLV from γ_F: for $s = (\bullet, y)$, $\Gamma_F(s) = \gamma_F(y)$. Consequently, an F*-certain* state $s \in S$, $s = (M,y)$ of the FPLV is equally characterized by $\gamma_F(y) = \{1\}$ or $\Gamma_F(s) = \{1\}$. To discuss strong diagnosability with respect to the FPLV, we introduce the notions of F-states and F-certain states.

Definition 11 *A marking* M *of the FPSN that satisfies* $M(F) = 1$ *is said to be an* F*-marking. In such a case, the fault pattern has occurred. In addition, a state of* X_A *that corresponds to an* F*-marking and a logical verifier state* $s = (M,y)$ *with* $y \in Y$ *such that* M *is an* F*-marking are also called* F*-states. Finally,* $s = (M,y)$ *is named an* F*-certain state if* $\gamma_F(y) = \{1\}$ *or equivalently* $\Gamma_F(s) = \{1\}$. *In such a case, from the observation of the diagnoser states captured thus far, one knows that the fault pattern has certainly occurred.*

We also extend the notions of F-states and F-certain states to the cycles of the verifier : a cycle is called an F-cycle if the states in the cycle are F-states. In addition, an F-cycle is F-certain if at least one of its states is F-certain. As stated in Lemma 2, the FPLV has a property of monotonicity with respect to F-states and F-certain states.

Lemma 2: Let $FPLV = (S, T, \Delta, s_0)$ be the fault pattern logical verifier of an LSPN with respect to the pattern Σ_F. Let $s \in S$ and $t \in T$. If s is an F-state and $\Delta(s,t) = s'$ then s' is also an F-state. In addition, if s is F-certain, then s' is also F-certain.

Proof : If s is an F-state , then $s = (M,y)$ with $M(F) = 1$. Observe that the place F is such that $w_{PR}(F,t) = w_{PO}(F,t) = 1$, for all $t \in T_{sync}$ and $w_{PR}(F,t) = w_{PO}(F,t) = 0$ otherwise. Consequently, the token is trapped in place F. In addition, as far as $M(F) = 1$, $M(N_1) = ... = M(N_m) = 0$ and no other token can enter F (because $\{N_1, ..., N_m, F\}$ is P-invariant in the FPSN and $M(N_1) + ... + M(N_m) + M(F) = 1$). Finaly, if $s' = (M',y')$ with $\Delta(s,t) = s'$, then $M'(F) = 1$ and s' is also an F-state.

If, in addition, s is F-certain, $\Gamma_F(s) = \{1\}$. With the same reasonning, if $s' = (M',y')$ with $\Delta(s,t) = s'$, then $\Gamma_F(s') = \{1\}$ and s' is F-certain. □

Proposition 2: A given LSPN is strongly diagnosable with respect to the pattern Σ_F if and only if all F-cycles of its FPLV are F-certain.

Proof : On the one hand, assume that all F-cycles of the FPLV are F-certain. Observe first, that, according to Lemma 2, all states of the cycles are necessarily F-certain. In addition, all states s' with reached via a sequence of transitions from a state s in an F-certain cycle are also F-certain and the system is strongly diagnosable. On the other hand, assume that an F-cycle exists in the FPLV that is not F-certain. Then, the cycle has no F-certain state and the system may experience an infinite repetition of this cycle. Such a system is not strongly diagnosable. □

To conclude, checking strong diagnosability of an LPN is the same as checking strong diagnosability of the underlying logical PN. However, it is worth noting that the proposed approach, developed in the next sections for weaker notions of diagnosability, also includes the information required for the verification of strong diagnosability. Observe that an alternative solution would be to evaluate the diagnosability directly on the diagnoser (by analysing its cycles). However, one objective of this paper is to propose a systematic and unified approach for different notions of diagnosability (not only strong diagnosability but also weaker notions that require timing and probabilistic aspects). To include such timing and probabilistic aspects in the analysis, it becomes necessary to keep track of the runs in the system, and for this reason an approach based on the parallel composition of the FPSN and its diagnoser is preferred.

Example 5: Consider again the LSPN system in Fig. 1 and the fault pattern Σ_{Fb} represented by $(FPNb, SFb)$. The diagnoser obtained in Fig. 6 has only one F-certain state (see Table 2). The FPLV that results from the parallel like product of A with the diagnoser $DIAG$ (detailed in Fig. 6), has 45 states, each one composed of a marking and a diagnoser state. The FPLV is composed by one absorbing strongly connected component C_1 of dimension 15 and a transient component of dimension 30. The transient has 6 cycles C_i, $i = 1,...,6$, that are detailed in Table 3. All cycles in the transient contain only uncertain states. Consequently, the system in Fig. 1 is not strongly diagnosable.

Table 3 Cycles of the FPLV for the LSPN in Fig. 1 with respect to the pattern Σ_{Fb}.

Cycle	Detail	F-certain
C_1	$\{(M_0,y_0),(M_2,y_0),(M_6,y_0),(M_7,y_0),(M_{12},y_0),(M_{17},y_0)\}$	uncertain
C_2	$\{(M_1,y_0),(M_5,y_0),(M_{11},y_0)\}$	uncertain
C_3	$\{(M_4,y_0),(M_{10},y_0),(M_{16},y_0)\}$	uncertain
C_4	$\{(M_9,y_1),(M_{15},y_1),(M_{20},y_1),(M_{21},y_1),(M_{25},y_1),(M_{28},y_1)\}$	uncertain
C_5	$\{(M_{14},y_1),(M_{19},y_1),(M_{24},y_1)\}$	uncertain
C_6	$\{(M_{18},y_1),(M_{23},y_1),(M_{27},y_1)\}$	uncertain
C_7	$\{(M_3,y_2),(M_8,y_2),(M_{13},y_2),(M_{14},y_2),(M_{18},y_2),(M_{19},y_2),...$	
	$...(M_{22},y_2),(M_{23},y_2),(M_{24},y_2),(M_{26},y_2),(M_{27},y_2),(M_{29},y_2),...$	F-certain
	$...(M_{30},y_2),(M_{31},y_2),(M_{32},y_2),\}$	

4.4 Conditional diagnosability

In order to compute the conditional diagnosability (conditioned on the fact that the fault pattern has occurred) as a probability, we model in this section the timing and probabilistic aspects with a continuous time Markov model.

Definition 12 *The fault pattern probabilistic verifier of an LSPN with respect to the pattern Σ_F is defined as $FPPV = (S, G, \Pi_0)$ where*

- $S \subseteq X_A \times Y$;
- G *is an* $|S| \times |S|$ *matrix such that*
  - *for all* $s = (M,y) \in S$, $s' = (M',y') \in S$, $s \neq s'$, $G(s,s') = \sum_{t \in T^s(M,M')} \mu(t)$,
  - *for all* $s = (M,y) \in S$, $G(s,s) = \sum_{s' \neq s} -G(s,s')$;
- Π_0 *is an initial distribution of the states such that* $\pi_{0,s_0} = 1$ *for* $s_0 = (M_0,y_0)$ *and* $\pi_{0,s} = 0$ *otherwise.*

Given a state $s \in S$ and a time $\tau \in \mathbb{R}^+$, $\pi_s(\tau,\Pi_0)$ is the probability of state s at τ assuming that the initial distribution of states is Π_0. In addition, the state probability vector $\Pi(\tau,\Pi_0)$ of S at τ is given as an $1 \times |S|$ vector. When there is no ambiguity about the initial probabilities Π_0, we will write in the next $\Pi(\tau)$ and $\pi_s(\tau)$ for notational simplicity.

Lemma 3: Let $FPPV = (S, G, \Pi_0)$ be the fault pattern probabilistic verifier of a given LSPN with respect to the pattern Σ_F. Let $s, s' \in S$ such that $G(s,s') > 0$. If s is an F-state, then s' is also an F-state. In addition, if s is F-certain then s' is also F-certain.

Proof : Observe that the FPPV and the FPLV have exactly the same set of states S and the same structure (the difference between the FPPV and the FPLV relies on the fact that the FPPV incorporates the timing and probabilistic information whereas the FPLV does not). Consequently, $G(s,s') > 0$ in the FPPV if and only if there exists $t \in T$ and

,

Proposition 3: The fault pattern probabilistic verifier $FPPV = (S, G, \Pi_0)$ obtained for an LSPN and the fault pattern Σ_F represented by (FPN, SF) is a continuous-time Markov model.

Proof : The FPPV is a CTMM by construction: (i) the initial probability vector Π_0 satisfies $\pi_{0,s_0} = 1$ for $s_0 = (M_0, y_0)$ and $\pi_{0,s} = 0$ otherwise. Obviously, $\sum_s \pi_{0,s} = 1$; (ii) matrix G is a generator matrix because $G(s,s') \geq 0$ for all $s, s' \in S$, $s' \neq s$, and $G(s,s) = \sum_{s' \neq s} -G(s,s')$. □

The complexity in space of the FPPV is the same as the one of the FPLV, i.e., $O(N_A \times 2^{N_A})$.

The graph of $FPPV$ is composed by a set $\mathscr{C}$ of one or more *absorbing strongly connected components*[2] (ASCCs) C_k, $k = 1, 2, \ldots, |\mathscr{C}|$. The rest of the graph corresponds to the transient T_R. Without any loss of generality, G can be re-arranged (by rearranging the indices of states) as in (3) below

$$G = \begin{pmatrix} G_{T_R,\,T_R} & G_{T_R,\,C_1} & \cdots & G_{T_R,\,C_{|\mathscr{C}|}} \\ 0 & G_{C_1,\,C_1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & G_{C_{|\mathscr{C}|},\,C_{|\mathscr{C}|}} \end{pmatrix}, \tag{3}$$

where the sub-matrices of G have appropriate dimensions. To simplify notation, we refer to the probabilities of the states of any subset X at time τ as $\Pi_X(\tau)$. In addition, for any subset of rows X and any subset of columns Y, we refer to the sub-matrix extracted from G with rows X and columns Y as to $G_{X,Y}$. The steady state probabilities satisfy [27]:

$$\begin{array}{rl} \Pi_{T_R}(\infty) & = (\mathbf{0})_{|T_R|}, \\ \Pi_{C_k}(\infty) \times G_{C_k,C_k} & = (\mathbf{0})_{|C_k|}, k = 1, 2, \ldots, |\mathscr{C}| \\ \Pi_{C_k}(\infty) \times (\mathbf{1})_{|C_k|} & = \Pi_{0,T_R} \times (-G_{T_R,T_R})^{-1} \times \\ & \quad G_{T_R,C_k} \times (\mathbf{1})_{|C_k|}, k = 1, 2, \ldots, |\mathscr{C}|, \end{array} \tag{4}$$

where $(\mathbf{0})_{|X|}$ (resp. $(\mathbf{1})_{|X|}$) is the column vector of size $|X|$ with all entries equal to 0 (resp. 1). The state probability vector $\Pi(\tau)$ is obtained by solving the Chapman-Kolmogorov equation related to the FPPV [32]:

$$\begin{array}{rl} \dfrac{d\Pi(\tau)}{d\tau} & = \Pi(\tau) \times G, \\ \Pi(0) & = \Pi_0. \end{array}$$

Let us define F_∞-states and F_∞-certain states as F-states and F-certain states that are recurrent, i.e., belong to an absorbing strongly component:

Definition 13 *A logical verifier state $s \in S$ is called an F_∞-state if s is an F-state and $s \in (\cup_{C \in \mathscr{C}} C)$. Similarly, s is called an F_∞-certain state if s is an Fcertain-state and $s \in (\cup_{C \in \mathscr{C}} C)$.*

The following two subsets B_F and C_F in S are also introduced:

$$\begin{array}{l} B_F = \{s \in (\cup_{C \in \mathscr{C}} C) \text{ with } s = (M, \bullet), M \in R \text{ such that } M(F) = 1\}, \\ C_F = \{s \in (\cup_{C \in \mathscr{C}} C) \text{ such that } \Gamma_F(s) = \{1\}\}. \end{array} \tag{5}$$

In simple words, B_F is the subset of F_∞-states of the FPLV and C_F is the subset of F_∞-certain states. Note that $C_F \subseteq B_F$. The sets B_F and C_F satisfy the following lemma.

Lemma 4: Let us consider $FPPV = (S, G, \Pi_0)$ of a given LSPN with respect to a pattern Σ_F. Each ASCC C_k, $k = 1, ..., |\mathscr{C}|$, satisfies the following two properties:

1. $C_k \cap B_F = \emptyset$ or $C_k \cap B_F = C_k$,
2. $C_k \cap C_F = \emptyset$ or $C_k \cap C_F = C_k$.

[2] C is an absorbing strongly connected component of a directed graph M if (1) for any nodes $S, S' \in C$, there exists a path from S to S'; (2) for any $C' \subseteq G$ with $C \subseteq C'$, C' does not satisfy condition (1); (3) for any nodes $S \in C$, $S' \in G$, then $S' \in C$ if a path exists from S to S'.

certain states is conserved when (i) considering only recurrent states; (ii) performing the parallel composition by the diagnoser. Given any absorbing strongly connected component C_k and any states $s, s' \in C_k$, there exists a sequence of transitions from s to s'. Consequenlty, s' is an F_∞-state (resp. an F_∞-certain state) if and only if s is an F_∞-state (resp. an F_∞-certain state). □

In simple words, Lemma 4 states that each ASCC of an FPPV is composed by states that (i) all result from sequences of transitions that all include the fault pattern (such ASCCs will be referred to as an F_∞-ASCCs), or all result from sequences of transitions that do not all include the fault pattern; (ii) are all F_∞-certain states (such ASCCs will be referred to as F_∞-certain ASCCs) or are all normal or uncertain states.

The steady-state conditional diagnosability $Diag(F,\infty|F)$ (i.e., conditional diagnosability in the long run) can be computed in a probabilistic setting as

$$Diag(F,\infty|F) = \frac{\sum_{s\in C_F} \pi_s(\infty)}{\sum_{s\in B_F} \pi_s(\infty)}. \tag{6}$$

4.5 Weaker notions of diagnosability for LSPN

Two weaker notions of diagnosability, namely *tA*-diagnosability and *tAA*-diagnosability have been introduced for timed automata in [39]. In this section, we give necessary and / or sufficient conditions for *tA*-diagnosability and *tAA*-diagnosability derived from the LSPN, the observer and the diagnoser.

To formally define these notions, let us consider a timed firing sequence σ_τ of h consecutive firings, the associated logical firing sequence $\sigma = H(\sigma_\tau)$, a time $\tau \in \mathbb{R}^+$ such that $\tau \geq \tau_h$ and a marking M such that $M[\sigma\rangle$. Let $\sigma_{o\tau} = L_\tau(\sigma_\tau)$ be the sequence of timed observations. We define the set of timed trajectories consistent with $\sigma_{o\tau}$ within $[0,\tau)$ as $L_\tau^{-1} = \{(\sigma_\tau, M, \tau) \in ((T^s \times \mathbb{R}^+)^* \times \mathbb{N}^n \times \mathbb{R}^+)$ such that $L_\tau(\sigma_\tau) = \sigma_{o\tau}$ and $\tau(\sigma_\tau) \leq \tau\}$. The concatenation of two timed trajectories that have the same time origin (σ_τ, M, τ) with $M[H(\sigma_\tau)\rangle M'$, $\sigma_\tau = (t(1),\tau_1)\ ...(t(h),\tau_h)$ and $(\sigma'_\tau, M', \tau')$ with $\sigma'_\tau = (t'(1),\tau'_1)\ ...(t'(h'),\tau'_{h'})$, $\tau' \geq \tau'_{h'} \geq \tau'_1 \geq \tau \geq \tau_h \geq \tau_1$ is also a time trajectory $(\sigma''_\tau, M, \tau')$ with $\sigma''_\tau = (t(1),\tau_1)\ ...(t(h),\tau_h)(t'(1),\tau'_1)\ ...(t'(h'),\tau'_{h'})$ within $[0,\tau')$.

Definition 14 *A given LSPN is said to be tA-diagnosable with respect to the fault pattern Σ_F if the following holds:*

$$\begin{array}{l}(\forall\alpha>0),(\exists\tau>0),(\forall(\sigma_{1\tau},M_l^s,\tau_1)\ with\ \sigma_{1\tau}\in(T^s\times\mathbb{R}^+)^*,M_l^s[H(\sigma_{1\tau})\rangle M^s,\\ (H(\sigma_{1\tau})\in\Sigma_F)),(\forall(\sigma_{2\tau},M^s,\tau_2)\ with\ \sigma_{2\tau}\in(T^s\times\mathbb{R}^+)^*,M^s[H(\sigma_{2\tau})\rangle,\tau_2\geq\tau),\\ Prob(D((\sigma_\tau,M_l^s,\tau_2))=0)<\alpha,\end{array}$$

where $(\sigma_\tau, M_l^s, \tau_2)$ is the concatenation of $(\sigma_{1\tau}, M_l^s, \tau_1)$ and $(\sigma_{2\tau}, M^s, \tau_2)$, and $D((\sigma_\tau, M_l^s, \tau_2)) = 1$ if $H(L_\tau^{-1}(L_\tau(\sigma_\tau))) \subseteq \Sigma_F$, otherwise $D((\sigma_\tau, M_l^s, \tau_2)) = 0$.

Definition 15 *A given LSPN is said to be tAA-diagnosable with respect to the fault pattern Σ_F if the following holds:*

$$\begin{array}{l}(\forall\alpha>0),(\forall\beta<1),(\exists\tau>0),(\forall(\sigma_{1\tau},M_l^s,\tau_1)\ with\ \sigma_{1\tau}\in(T^s\times\mathbb{R}^+)^*,M_l^s[H(\sigma_{1\tau})\rangle M^s,\\ (H(\sigma_{1\tau})\in\Sigma_F)),(\forall(\sigma_{2\tau},M^s,\tau_2)\ with\ \sigma_{2\tau}\in(T^s\times\mathbb{R}^+)^*,M^s[H(\sigma_{2\tau})\rangle,\tau_2\geq\tau),\\ Prob(D_\beta((\sigma_\tau,M_l^s,\tau_2))=0)<\alpha,\end{array}$$

where $(\sigma_\tau, M_l^s, \tau_2)$ is the concatenation of $(\sigma_{1\tau}, M_l^s, \tau_1)$ and $(\sigma_{2\tau}, M^s, \tau_2)$, and $D_\beta((\sigma_\tau, M_l^s, \tau_2)) = 1$ if $Prob(H(L_\tau^{-1}(L_\tau(\sigma_\tau))) \subseteq \Sigma_F) > \beta$, otherwise $D_\beta((\sigma_\tau, M_l^s, \tau_2)) = 0$.

Proposition 4 gives a necessary and sufficient condition for *tA*-diagnosability of the LSPN with respect to a given fault pattern Σ_F. To discuss *tA*-diagnosability one is interested in the absorbing strongly connected components of the FPPV. One advantage of the FPPV is that it describes in an explicit way both the F_∞-ASCCs and F_∞-certain ASCCs.

Proposition 4: A given LSPN is *tA*-diagnosable with respect to a given fault pattern Σ_F if and only if all F_∞-ASCCs in the FPPV are F_∞-certain.

Proof: To prove Proposition 4, observe that once the timing aspects are considered, the system cannot stay forever in a cycle that belongs to the transient part of the FPPV and must necessarily reach an ASCC in the long run (with increasing probability as we wait longer). In particular, if the system meets the fault pattern, then in its future behavior, it

with $\tau(\sigma_\tau)$ larger than a given time τ, the probability not to be in an F-certain state (and also in an F_∞-certain state) is less than an arbitrarily small value α. As far as all F_∞-ASCCs are F_∞-certain, the system will reach an F_∞-certain ASCC in the long run (sufficiency is proved). On the contrary, if there exists an F_∞-ASCC C that is not F_∞-certain, then the probability that the system reaches and stays in C is given by $\alpha(C) = \Pi_{0,T_R} \times (-G_{T_R,T_R})^{-1} \times G_{T_R,C} \times (\mathbf{1})_{|C|} > 0$ (see Eq. (4)). The condition of tA-diagnosability is no longer satisfied for $\alpha < \alpha(C)$.□

Note that an LSPN that is strongly diagnosable is also tA-diagnosable. In addition, Proposition 5 below is a corollary of Proposition 4.

Proposition 5: A given LSPN is tA-diagnosable with respect to a given fault pattern Σ_F if and only if condition (7) is satisfied.

$$\frac{\Pi_{C_F}(\infty) \times (\mathbf{1})_{|C_F|}}{\Pi_{B_F}(\infty) \times (\mathbf{1})_{|B_F|}} = 1. \tag{7}$$

Proof: To prove Proposition 5, one can use Proposition 4 and observe that all F_∞-ASCCs of the FPPV are F_∞-certain if and only if $Diag(F,\infty|F) = 1$. Then, replacing $Diag(F,\infty|F)$ by its analytical characterization (6) leads immediately to Eq. (7). □

Example 6: Consider again the LSPN system in Fig. 1 and the fault pattern Σ_{Fb} represented by $(FPNb, SFb)$. The structure and states of the FPPV are similar to the ones of the FPLV previously described: this continuous time Markov model has 45 states. It is composed by one absorbing strongly connected component C_1 of dimension 15 that is F_∞-certain (see Table 3) and a transient component of dimension 30. This system is tA-diagnosable with respect to the pattern Σ_{Fb}.

Now, consider, as another example, the LSPN system that results from the same system as the one in Fig. 1 with a labeling function defined as $L(t_2) = L(t_5) = a$, $L(t_3) = L(t_6) = b$, $L(t_1) = L(t_4) = \varepsilon$. The diagnoser of this LSPN has a single state that is uncertain and the FPPV of this system is a continuous time Markov model with 33 states. It is composed by one absorbing strongly connected component C_1 of dimension 15 and a transient component of dimension 18, both of them containing only uncertain states. Consequently, this system is not tA-diagnosable with respect to the pattern σ_{Fb}.

Proposition 6 below gives a sufficient condition for tAA-diagnosability of an LSPN with respect to a given pattern Σ_F. For this purpose, we need to define an extended fault pattern probabilistic verifier obtained from the logical observer (the complexity in space of the Ext-FPPV is also $O(N_A \times 2^{N_A})$). The motivation to pursue the analysis with the Ext-FPPV instead of the FPPV (that is based on the reduced size diagnoser) is that the Ext-FPPV tracks the set of markings that are consistent with the observations thus far. As we will see, in some particular cases, the refinement resulting from the use of the full size observer allows to separate pairs of ASCCs that cannot be separated using a reduced size diagnoser.

Definition 16 *The extended fault pattern probabilistic verifier of an LSPN with respect to a given fault pattern Σ_F is defined as $Ext-FPPV = (S', G', \Pi'_0)$ where*

- $S' \subseteq X_A \times X$;
- G' *is an* $|S'| \times |S'|$ *matrix such that*
  - *for all* $s = (M,x) \in S'$, $s' = (M',x') \in S'$, $s \neq s'$, $G'(s,s') = \sum_{t \in T^s(M,M')} \mu(t)$,
  - *for all* $s = (M,x) \in S'$, $G(s,s) = \sum_{s' \neq s} -G(s,s')$;
- Π'_0 *is an initial distribution of the states such that* $\pi'_{0,s} = 1$ *for* $s_0 = (M_0,x_0)$ *and* $\pi'_{0,s} = 0$ *otherwise.*

The extended fault pattern probabilistic verifier results from the parallel composition $A||OBS$ and is a continuous-time Markov model. Notation $\pi'_s(\tau,\Pi'_0)$ (or $\pi'_s(\tau)$ for simplicity) refers to the probability of state s at τ assuming that the initial distribution of states is Π'_0 and $\Pi'(\tau,\Pi'_0)$ (or $\Pi'_s(\tau)$ for simplicity) is the probability vector of dimension $1 \times |S'|$ of the Ext-FPPV.

Next, we focus on some average frequencies and probabilities in the Ext-FPPV after the system has reached a given F_∞-ASCC C_k that is uncertain (if such an ASCC does not exist, the system is tA-diagnosable and Proposition 4 or 5 can be used). The objective is similar to the one followed in [40] for logical stochastic systems: to track the occurrence of faults according to the probabilistic equivalence of the ASCCs. Equivalence of logical stochastic automata is a well-studied problem that can be decided in polynomial time [41], [24]. There are some important differences compared to [40]. First,

no need for such an additional model, because the complete behaviors and observations are already incorporated in the construction of the Ext-FPPV (according to the parallel composition with the logical observer). Second, the necessary and sufficient condition in [40] was proposed for logical stochastic systems and is too restrictive for timed stochastic systems. The properties of empirical conditional probabilities that are at the core of the method proposed in [40] fail to incorporate the additional information provided by the time elapsed between symbols. Thus, for timed behaviors, properties of average conditional frequencies (which take into account the average time between different observable symbols) should be considered. Third, the results in [40] concern automata whereas our contributions are formulated in the Petri net framework. The sufficient condition proposed in this paper is obviously weaker and more general than the sufficient condition proposed for *tAA*-diagnosability in [39].

The problem that is considered here is to separate, thanks to timing and probabilistic aspects, the observed behaviours in two ASCCs C and C' of the Ext-FPPV that have the same logical observable language (C being an F_∞-ASCC and C' being a non F_∞-ASCC). In particular, one can consider the repeated observations of the labels in the ASCCs C or C'. For a given state of the logical observer $x \in X$, the subset $S'(x) \subseteq S'$ is defined as the subset of FPPV states that correspond to x: $S'(x) = \{s \in S' \text{ such that } s = (\bullet, x)\}$ and $C(x) = S'(x) \cap C$. In addition, the following matrices are defined.

- $G'(\varepsilon, C(x))$ is the matrix of dimension $|C(x)| \times |C(x)|$ whose entries are defined for any states $s, s' \in C(x)$ as $G'_{s,s'}(\varepsilon, C(x)) = G'_{s,s'}$ if there exists a silent jump from s to s' or if $s = s'$, and $G'_{s,s'}(\varepsilon, C(x)) = 0$, otherwise. In simple words, $G'(\varepsilon, C(x))$ is obtained from matrix $G'_{C(x),C(x)}$ by removing all observable jumps.
- Given a label $q \in Q$, $G'(q, C(x))$ is the matrix of dimension $|C(x)| \times |C(\Delta_X(x,q))|$ (with $\Delta_X(x,q)$ being the successor of state x in *OBS* by a q-jump, i.e., a jump in *OBS* that delivers a label q) whose entries are defined for any pair of states $(s, s') \in C(x) \times C(\Delta_X(x,q))$ as $G'_{s,s'}(q, C(x)) = G'_{s,s'}$ if there is a q-jump from s to s', and $G'_{s,s'}(q, C(x)) = 0$, otherwise. In simple words, $G'(q, C(x))$ is the matrix of the q-transitions from $C(x)$ to $C(\Delta_X(x,q))$.

Then, we prove the following lemma that computes some elementary probabilities and frequencies, in particular: (i) the probability of the label q' conditioned on the previous observation q captured at the observer state x; (ii) the frequency of the label q conditioned on the observer state x.

Lemma 6: Assume that the system has reached a given ASCC C and consider two labels $q', q \in Q$ and a given observer state $x \in X$. The conditional probability $Prob(q'|x, q, C)$ that a q'-jump occurs after having observed a q-jump at x is given by

$$Prob(q'|x,q,C) = \frac{\Pi_{C(x)}(\infty) \times (-G'^{-1}(\varepsilon, C(x))) \times G'(q, C(x)) \times (-G'^{-1}(\varepsilon, C(x'))) \times G'(q', C(x')) \times (\mathbf{1})_{|C(x'')|}}{\Pi_{C(x)}(\infty) \times (-G'^{-1}(\varepsilon, C(x))) \times G'(q, C(x)) \times (\mathbf{1})_{|C(x')|}}, \quad (8)$$

where $\Pi_{C(x)}(\infty)$ is the average state distribution in $C(x)$, $x' = \Delta_X(x,q)$ and $x'' = \Delta_X(x', q')$. Similarly, the conditional frequency $Freq(q|x,C)$ of the label q at x is given by

$$Freq(q|x,C) = \frac{\Pi_{C(x)}(\infty) \times G'(q, C(x)) \times (\mathbf{1})_{|C(x')|}}{\Pi_C(\infty) \times (\mathbf{1})_{|C|}}. \quad (9)$$

Proof: To prove Eq. (8), let us first compute the conditional probability $Prob(q|x, \varepsilon, C)$ to observe the label q when one knows that the ASCC C has been reached and the observer state is x , i.e. the average probability to exit $C(x)$ by a q-jump. Such a probability depends on (i) the average state distribution within $C(x)$, (ii) the silent behaviours within $C(x)$ and (iii) the observable jumps that leave $C(x)$ and reach $C(\Delta_X(x,q))$ while generating a label q. In the long run, the average normalized[3] distribution $\Pi'_N(x, C)$ in $C(x)$ given by

$$\Pi'_N(x,C) = \frac{\Pi_{C(x)}(\infty)}{\Pi_{C(x)}(\infty) \times (\mathbf{1})_{|C(x)|}}.$$

In addition, the silent evolutions within $C(x)$ are characterized by the matrix $G'(\varepsilon, C(x))$ and the observable jumps that leave $C(x)$ by the q-transition rate matrix $G'(q, C(x))$. More details about the meaning of these terms can be found in [27]. Finally, $Prob(q|x, \varepsilon, C)$ is computed as

$$Prob(q|x,\varepsilon,C) = \Pi'_N(x,C) \times (-G'^{-1}(\varepsilon, C(x))) \times G'(q, C(x)) \times (\mathbf{1})_{|C(x')|}. \quad (10)$$

[3] A probability vector is normalized if the sum of its entries equals 1.

tion $\Pi'_N(x',C,q)$ immediately after entering in $C(x')$ from $C(x)$ with a q-jump:

$$\Pi'_N(x',C,q) = \frac{\Pi_{C(x)}(\infty) \times (-G'^{-1}(\varepsilon,C(x))) \times G'(q,C(x))}{\Pi_{C(x)}(\infty) \times (-G'^{-1}(\varepsilon,C(x))) \times G'(q,C(x)) \times (\mathbf{1})_{|C(x')|}}.$$

Again, the silent evolutions within $C(x')$ are characterized by the matrix $G'(\varepsilon,C(x'))$ and the observable jumps that leave $C(x')$ are characterized by the q'-transition rate matrix $G'(q', C(x'))$. Finally, we have

$$Prob(q'|x,q,C) = \Pi'_N(x',C,q) \times (-G'^{-1}(\varepsilon,C(x'))) \times G'(q',C(x')) \times (\mathbf{1})_{|C(x'')|},$$

that leads obviously to Eq. (8).

The reasonning to compute the conditional frequency $Freq(q|x,C)$ is quite similar. Observe that Eq. (9) can be rewritten as $Freq(q|x,C) = \Pi'_N(x,C) \times G'(q,C(x)) \times (\mathbf{1})_{|C(x')|}$, whereas $\Pi'_N(x,C) \times G'(q,C(x))$ corresponds to the average rate to leave each state within $C(x)$ by a q-jump. Consequently, Eq. (9) holds. □

For each ASCC $C \in \mathscr{C}$, the finite sets of elementary probabilities and frequencies of labels are defined:

- $\mathscr{P}_C = \{Prob(q'|x,q,C) | x \in X, q,q' \in Q\}$,
- $\mathscr{F}_C = \{Freq(q|x,C) | x \in X, q \in Q\}$.

These sets are used to compare the timing and probabilistic aspects of two ASCCs (including the more difficult case of identically structured ASCCs with same states, same transitions, and same symbols on the transitions, except for the fact that the time parameters in the second ASCC are different from the rates of the first one) as detailed in Proposition 6.

Proposition 6: A given LSPN, assumed not to be tA-diagnosable, is tAA-diagnosable with respect to the fault pattern Σ_F represented by (FPN, SF) if for any ASCCs C and C', C being an F_∞-ASCC, and C' not being an F_∞-ASCC, we have $(\mathscr{P}_C, \mathscr{F}_C) \neq (\mathscr{P}_{C'}, \mathscr{F}_{C'})$, i.e., there exist two labels $q,q' \in Q$ and a given $x \in X$ such that $Prob(q'|x,q,C) \neq Prob(q'|x,q,C')$ or $Freq(q|x,C) \neq Freq(q|x,C'))$.

Proof: To prove Proposition 6, first observe that if the system is not tA-diagnosable, there necessarily exists two F_∞-ASCC C and C', where the first ASCC is F_∞-certain and the second ASCC is not F_∞-certain. For simplicity, we will assume that $\mathscr{C} = \{C,C'\}$. This means that there exists a recurrent F-state that is uncertain: $s = (M,x)$ in C with $M(F) = 1$ and obviously $M \in \gamma_P(x)$. There exists also a marking $M' \neq M$ such that $M' \in \gamma_P(x)$ and $M'(F) = 0$ because s is uncertain. Consequently, there exists a recurrent state of the form $s' = (M',x)$ that is not an F_∞-state and belongs to another ASCC C' that is not an F_∞-ASCC. Basically the proof relies on the decomposition of conditioned frequencies and probabilities according to Eqs. (8) and (9).

To prove sufficiency, suppose that $(\mathscr{P}_C, \mathscr{F}_C) \neq (\mathscr{P}_{C'}, \mathscr{F}_{C'})$. Then, there exist two labels $q,q' \in Q$ and a given $x \in X$ such that we have either $Prob(q'|x,q,C) \neq Prob(q'|x,q,C')$ or $Freq(q|x,C) \neq Freq(q|x,C'))$. The timed observation of the repeated occurrences of q, q' and qq' in $C(x)$ during a time T as large as necessary, is enough to measure $\widehat{Freq}(q|x)$ and $\widehat{Prob}(q'|x,q)$ (without any assumption about the ASCC that the system has reached) with a given arbitrary precision. Then, by comparing $\widehat{Freq}(q|x)$ with $Freq(q|x,C)$ and $Freq(q|x,C')$ and by comparing also $\widehat{Prob}(q'|x,q)$ with $Prob(q'|x,q,C)$ and $Prob(q'|x,q,C')$, one can decide if the system stays in C or C' with a given probability β (see Definition 15). Consequently, the system is tAA-diagnosable. □

Example 7: Consider the example of the LSPN detailed on the top of Fig. 7. $Q = \{a,b\}$ is the set of labels and the labeling function is defined such that $L(t_2) = L(t_5) = a$, $L(t_3) = L(t_6) = b$, $L(t_1) = L(t_4) = \varepsilon$. The firing rates of the transitions are defined such that $\mu(t_1) = \mu(t_2) = \mu(t_4) = 1$ and $\mu(t_3) = 2$. Several values will be considered for $\mu(t_5)$ and $\mu(t_6)$ (see Table 5). In Fig. 7, labels and rates are reported near the transitions. The FPSN has 15 markings detailed in Table 4.

The diagnoser of this system is composed by a single state y_0 that is uncertain. Consequently, the system is obviously neither strongly diagnosable nor tA-diagnosable. In particular, one can observe that the FPPV obtained as the parallel like composition $FPPV = A||DIAG$ has three ASCC: $C_1 = \{(M_5,y_0),(M_9,y_0),(M_{10},y_0),(M_{13},y_0)\}$, $C_2 = \{(M_3,y_0),(M_8,y_0),(M_{12},y_0)\}$, $C_3 = \{(M_6,y_0),(M_{11},y_0),(M_{14},y_0)\}$. C_1 and C_3 are not F_∞-ASCC (when the system is trapped in one of these components, it will never experience the fault pattern) whereas C_2 is an F_∞-ASCC. The reason why C_1 and C_3 are not F_∞-ASCC while C_2 is an F_∞-ASCC can be found by looking at the markings in the three ASCCs, and more precisely on $M(F)$, i.e., the last element of the marking vector (see Table 4 for more details).

The logical observer of this system is composed by 6 states that are all uncertain: $x_0 = \{M_0,M_1,M_2,M_3,M_5,M_6\}$, $x_1 = \{M_4,M_7,M_8,M_9,M_{10},M_{11}\}$, $x_2 = \{M_{12},M_{13},M_{14}\}$, $x_3 = \{M_1,M_2,M_3,M_5,M_6\}$, $x_4 = \{M_8,M_9,M_{10},M_{11}\}$, $x_5 =$

$\{M_3, M_5, M_6\}$ (see Table 4). The Ext-FPPV is obtained as the parallel like composition $A||OBS$ and has a transient of 17 states and 3 ASCC: $C_1 = \{(M_5, x_5), (M_9, x_4), (M_{10}, x_4), (M_{13}, x_2)\}$, $C_2 = \{(M_3, x_5), (M_8, x_4), (M_{12}, x_2)\}$, $C_3 = \{(M_6, x_5), (M_{11}, x_4), (M_{14}, x_2)\}$. Again, C_1 and C_3 are non F_∞-ASCC whereas C_2 is an F_∞-ASCC. The average behaviour in the long run is characterized by the sets of elementary probabilities and frequencies in the Ext-FPPV. In this example, the elementary frequencies are enough to get a decision, and such frequencies are detailed in Table 5. For each value of the pair (μ_5, μ_6) and for each ASCC C_i, $i = 1, 2, 3$, the frequencies $Freq(q|x_k, C)$ are detailed by a matrix where each row corresponds to an observer state x_k, $k = 0, ..., 5$, and the two columns correspond to the two labels a and b. For example, in a first matrix computed for C_1 and $\mu_5 = \mu_6 = 1$, the occurrence frequency of label b is 0.67 when the observer state is x_2. In the second part of Table 5, the same was computed by using the diagnoser $(DIAG, Y_F, \gamma_F)$ instead of the observer (OBS, Y_P, γ_P).

- In the case $\mu_5 = \mu_6 = 1$, the frequencies of a and b in the F_∞-ASCC C_2 are different from the frequencies of the same labels in ASCC C_1 and C_3 and the system is tAA-diagnosable. Observe that if $(DIAG, Y_F, \gamma_F)$ is used instead of (OBS, Y_P, γ_P), the same conclusion is obtained.
- In the case $\mu_5 = 2$ and $\mu_6 = 1$, the conclusion is the same if (OBS, Y_P, γ_P) is used. In particular, if we consider the F_∞-ASCC C_2 and the non-F_∞-ASCC C_3, we observe that the elementary frequencies are different in C_2 and C_3, e.g., $Freq(a|x_4, C_2) \neq Freq(a|x_4, C_3)$. However, with the use of $(DIAG, Y_F, \gamma_F)$ instead of (OBS, Y_P, γ_P), one is no longer able to separate the behaviours in the ASCCs C_2 and C_3 by using the occurrence frequencies of a and b: $Freq(a|y_0, C_2) = Freq(a|y_0, C_3)$ and $Freq(b|y_0, C_2) = Freq(b|y_0, C_3)$.
- Finally, in the case $\mu_5 = 1$ and $\mu_6 = 2$, we cannot conclude that the system is tAA-diagnosable because all elementary frequencies in C_2 are identical to the elementary frequencies in C_3.

The same conclusions hold if the elementary probabilities are considered (such probabilities have not been reported in the example for brevity). This example illustrates a case where the full size observer is more precise than the reduced size diagnoser (in the sense that its use allows us to conclude that the system is not tAA- diagnosable whereas the use of the reduced size observer does not). To conclude, one can use a two-step approach using first the reduced size diagnoser and , if necessary, resorting to the full size observer . If there is a violation when using the reduced size diagnoser, the system is not tAA-diagnosable; similarly, if there is a violation when using the full size observer, again the system is not tAA-diagnosable. Some open questions remain that also relate to obtaining a necessary and sufficient condition for tAA-diagnosability. One question is to obtain a structure that allows us to discriminate between different ASCCs based only on elementary probabilities. Another question is to build a structure that is possibly more refined than the full size observer and allows us to discriminate between different ASCCs (based on elementary frequencies and probabilities) even when the full size observer cannot.

Table 4 Marking of the LSPN in Fig. 7 (bottom) with respect to the pattern Σ_{Fb}.

M	Detail	$M(F)$	ASCC	M	Detail	$M(F)$	ASCC
M_0	$(2\,0\,0\,0\,0\,1\,0\,0)^T$	0		M_8	$(0\,1\,1\,0\,0\,0\,0\,1)^T$	1	C_2
M_1	$(1\,1\,0\,0\,0\,0\,1\,0)^T$	0		M_9	$(0\,0\,1\,1\,0\,0\,1\,0)^T$	0	C_1
M_2	$(1\,0\,0\,1\,0\,1\,0\,0)^T$	0		M_{10}	$(0\,1\,0\,0\,1\,0\,1\,0)^T$	0	C_1
M_3	$(0\,2\,0\,0\,0\,0\,0\,1)^T$	1	C_2	M_{11}	$(0\,0\,0\,1\,1\,1\,0\,0)^T$	0	C_3
M_4	$(1\,0\,1\,0\,0\,0\,1\,0)^T$	0		M_{12}	$(0\,0\,2\,0\,0\,0\,0\,1)^T$	1	C_2
M_5	$(0\,1\,0\,1\,0\,0\,1\,0)^T$	0	C_1	M_{13}	$(0\,0\,1\,0\,1\,0\,1\,0)^T$	0	C_1
M_6	$(0\,0\,0\,2\,0\,1\,0\,0)^T$	0	C_3	M_{14}	$(0\,0\,0\,0\,2\,1\,0\,0)^T$	0	C_3
M_7	$(1\,0\,0\,0\,1\,1\,0\,0)^T$	0					

5 Conclusions and future work

To sum up the main contributions of the present work we would like to emphasize that we first propose a model-based fault diagnosis approach on labeled stochastic PNs that is able to track in an explicit way the occurrence of a given fault pattern for diagnosability analysis purposes. Then, based on the obtained model and on the design of a logical observer and a reduced size diagnoser, we revisit the diagnosability analysis of fault patterns in the framework of labeled Petri nets. The second proposition is to propose logical and probabilistic verifiers that are particularly interesting as they extend in a natural way already existing results, previously established for simple fault events. Necessary and sufficient conditions

Fig. 7 Example of an LSPN model that may be tAA-diagnosable but not tA-diagnosable with respect to the pattern Σ_{Fb} (top) and the resulting FPSN (bottom).

Table 5 Atomic frequencies $Freq(q|x_k, C_i)$ of the Ext-FPPV (top) and FPPV (bottom) for the LSPN in Fig. 7 (top left) with respect to the pattern Σ_{Fb}.

$ASCC$	$\mu_5 = 1, \mu_6 = 1$	$\mu_5 = 2, \mu_6 = 1$	$\mu_5 = 1, \mu_6 = 2$
C_1	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0.67 \\ 0 & 0 \\ 1.33 & 1 \\ 0.5 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0.67 \\ 0 & 0 \\ 1.33 & 1.33 \\ 0.67 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0.89 \\ 0 & 0 \\ 1.78 & 0.89 \\ 0.44 & 0 \end{pmatrix}$
C_2	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0.57 \\ 0 & 0 \\ 0.57 & 0.29 \\ 0.29 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0.57 \\ 0 & 0 \\ 0.57 & 0.29 \\ 0.29 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0.57 \\ 0 & 0 \\ 0.57 & 0.29 \\ 0.29 & 0 \end{pmatrix}$
C_3	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0.33 \\ 0 & 0 \\ 0.33 & 0.33 \\ 0.33 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0.29 \\ 0 & 0 \\ 0.29 & 0.57 \\ 0.57 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0.57 \\ 0 & 0 \\ 0.57 & 0.29 \\ 0.29 & 0 \end{pmatrix}$
C_1	$\begin{pmatrix} 1.83 & 1.67 \end{pmatrix}$	$\begin{pmatrix} 2.00 & 2.00 \end{pmatrix}$	$\begin{pmatrix} 2.22 & 1.78 \end{pmatrix}$
C_2	$\begin{pmatrix} 0.86 & 0.86 \end{pmatrix}$	$\begin{pmatrix} 0.86 & 0.86 \end{pmatrix}$	$\begin{pmatrix} 0.86 & 0.86 \end{pmatrix}$
C_3	$\begin{pmatrix} 0.67 & 0.67 \end{pmatrix}$	$\begin{pmatrix} 0.86 & 0.86 \end{pmatrix}$	$\begin{pmatrix} 0.86 & 0.86 \end{pmatrix}$

based on the timing notions of the original labeled stochastic PN.

Future research directions for our work will include the extension of diagnosis approaches to other classes of timed Petri nets, including PNs synchronised with input events and timed Petri nets with constant firing times or firing intervals. Addressing complexity issues related to pattern diagnosability, e.g., by using a diagnoser of reduced size or a pair verifier (as proposed in [47] and [21]). Another perspective is to replace the sufficient condition detailed in Proposition 6 by a necessary and sufficient condition. For this purpose, we aim to extend the set of computed frequencies and probabilities to a set of observation sequences that contain the minimal information required to separate, thanks to the timing and probabilistic aspects, the behaviours in two different absorbing strongly connected components that have the same observed logical language. We will also investigate other structures that may provide a necessary and sufficient condition by tracking the relevant information. In addition, an approach for the prognosis of fault patterns will be considered with a similar schema.

References

1. A. Aghasaryan, E. Fabre, A. Benveniste, R. Boubour and C. Jard, Fault detection and diagnosis in distributed systems: An approach by partially stochastic Petri nets. *Discrete Event Dynamic Systems: Theory and Applications*, vol. 82, no. 2, pp. 203–231, 1998.
2. R. Alur and D. L. Dill, A theory of timed automata. *Theoretical Computer Science*, vol. 126, pp. 183–235, 1994.
3. F. Basile, P. Chiacchio and G. De Tommasi, An efficient approach for online diagnosis of discrete event systems. *IEEE Transactions on Automatic Control*, vol. 54, no. 4, pp. 748–759, 2009.
4. F. Basile, M.P. Cabasino and C. Seatzu, State estimation and fault diagnosis of labeled time Petri net systems with unobservable transitions. *IEEE Transactions on Automatic Control*, vol. 60, no. 4, pp. 997–1009, 2015.
5. A. Benveniste, E. Fabre, S. Haar and C. Jard, Diagnosis of asynchronous discrete-event systems: A net unfolding approach. *IEEE Transactions on Automatic Control*, vol.48, no. 5, pp. 714–727, 2003.
6. N. Bertrand, S. Haddad and E. Lefaucheux, A Tale of Two Diagnoses in Probabilistic Systems. *Information and Computation*, Elsevier, vol. 269, pp.1–33, 2019.
7. P. Bouyer, F. Chevalier and D. D'Souza, Fault diagnosis using timed automata, in *Foundations of Software Science and Computational Structures* (Edt. V. Sassone), Springer Berlin Heidelberg, pp. 219–233, 2005.
8. M. P. Cabasino, A. Giua and C. Seatzu, Fault detection for DES using PN with unobservable transitions. *Automatica*, vol. 46, no.9, pp. 1531–1539, 2010.
9. M. P. Cabasino, A. Giua, S. Lafortune and C. Seatzu, A new approach for diagnosability analysis of Petri nets using verifier nets. *IEEE Transactions on Automatic Control*, vol. 57, no. 12, pp. 3104–3117, 2012.
10. F. G. Cabral and M. V. Moreira, Synchronous diagnosis of discrete-event systems. *IEEE Transactions on Automation Science and Engineering*, vol. 17, no. 2, pp. 921–932, 2020.
11. C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*, Springer, 2008.
12. F. Cassez and S. Tripakis, Fault diagnosis of timed systems, Roux, Olivier H. and Jard C (Eds.) *Communicating Embedded Systems – Software and Design* , ISTE Publishing Ltd. – JohnWiley & Sons, Ltd., 2009.
13. F. Cassez, Dynamic observers for fault diagnosis of timed systems, In Proc. of the 49th IEEE CDC, pp. 4359–4364, Atlanta, GA, USA, 2010.
14. Q. Chen, L. Yin, N. Wu, M. A. El-Meligy, M. A. F. Sharaf and Z. Li, Diagnosability of vector discrete-event systems using predicates. *IEEE Access*, vol. 7, pp. 147143–147155, 2019.
15. M. Dotoli, M. P. Fanti, A. M. 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.
16. S. Genc and S. Lafortune, Distributed diagnosis of place-bordered Petri nets. *IEEE Transactions on Automation Science and Engineering*, vol. 4, no. 2, pp. 206–219, 2007.
17. A. Giua and M. Silva, Petri nets and Automatic Control: A historical perspective. *Annual Reviews in Control*, vol. 45, no. 2, pp. 223–239, 2018.
18. H.E. Gougam, Y. Pencolé and A. Subias, Diagnosability analysis of patterns on bounded labeled prioritized Petri nets. *Discrete Event Dynamic Systems: Theory and Application*, vol. 27, no. 1, pp. 143–180, 2017.
19. S. Gören and F. J. Ferguson, On state reduction of incompletely specified finite state machines. *Comput. Electr. Eng.*, vol. 33, no. 1, pp. 58–69, 2007.
20. S. Haddad and P. Moreaux, Stochastic Petri Nets (Chapter 7), In *Petri Nets: Fundamental Models and Applications*, Wiley, 2009.
21. C. N. Hadjicostis, *Estimation and Inference in Discrete Event Systems: A Model-Based Approach with Finite Automata*, Springer Nature, 2020.
22. T. Jeron, H. Marchand, S. Pinchinat and M. O. Cordier, Supervision patterns in discrete event systems diagnosis. Proc. of the 8th Int. Workshop on Discrete Event Systems, pp. 262–268, Ann Harbor, Michigan, USA, 2006.
23. Z. Jiang, Z. Li, N. Wu and M. Zhou, A Petri net approach to fault diagnosis and restoration for power transmission systems to avoid the output interruption of substations. *IEEE Systems Journal*, vol. 12, no. 3, pp. 2566–2576, 2018.
24. C. Keroglou and C. N. Hadjicostis, Verification of AA-diagnosability in probabilistic finite automata is PSPACE-hard. Proc. IEEE Int. Conf. on Decision and Control, pp. 6712–6717, Nice, France, 2019.
25. S. Lafortune, F. Lin and C. N. Hadjicostis, On the history of diagnosability and opacity in discrete event systems. *Annual Reviews in Control*, vol. 45, pp. 257–266, 2018.
26. D. Lefebvre and C. Delherm, Diagnosis of DES with Petri net models. *IEEE Transactions on Automation Science and Engineering*, vol. 4, no. 1, pp. 114–118, 2007.
27. D. Lefebvre and C. N. Hadjicostis, Privacy and safety analysis of timed stochastic discrete event systems using Markovian trajectory-observers. *Discrete Event Systems: Theory and Applications*, vol. 30, no. 3, pp. 413–440, 2020.
28. B. Li, M. Khlif-Bouassida and A. Toguyéni, Reduction rules for diagnosability analysis of complex systems modeled by labeled Petri nets. *IEEE Transactions on Automation Science and Engineering*, vol. 17, no. 2, pp. 1061–1069, 2020.

30. G. H. Mealy, A method for synthesizing sequential circuits. *Bell System Technical Journal*, pp. 1045–1079, 1955.
31. M. Molloy, Performance analysis using stochastic Petri nets. *IEEE Transactions on Computers C*, vol. 31, pp. 913–917, 1982.
32. J. R. Norris, *Markov Chains*, Cambridge Press, pp. 60–125, 1997.
33. Y. Pencolé and A. Subias, Diagnosability of event patterns in safe labeled time Petri nets: a model-checking approach. *IEEE Transactions on Automation Science and Engineering*, doi: 10.1109/TASE.2020.3045565.
34. A. Ramirez-Trevino, E. Ruiz-Beltran, J. Aramburo-Lizarraga and E. Lopez-Mellado, Structural diagnosability of DES and design of reduced Petri net diagnosers. IEEE *Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 42, no. 2, pp. 416–429, 2012.
35. C. H. Roth, *Fundamentals of Logic Design*, Thomson-Engineering, 2004.
36. Y. Ru and C. N. Hadjicostis, Fault diagnosis in discrete event systems modeled by partially observed Petri nets. *Discrete Event Dynamic Systems: Theory and Applications*, vol. 19, pp. 551–575, 2009.
37. M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen and D. Teneketzis, Diagnosability of discrete event systems. *IEEE Transactions on Automatic Control*, vol. 40, pp. 1555–1575, 1995.
38. D. Thorsley and D. Teneketzis, Diagnosability of stochastic discrete-event systems. *IEEE Transactions on Automatic Control*, vol. 50, no. 4, pp. 476–492, 2005.
39. D. Thorsley, Diagnosability of stochastic chemical kinetic systems: A discrete event systems approach. Proc. of the American Control Conference, Baltimore, pp. 2623–2630, Maryland, USA, 2010.
40. D. Thorsley, A necessary and sufficient condition for diagnosability of stochastic discrete event systems. *Discrete Event Dynamic Systems: Theory and Applications*, vol. 27, pp. 481–500, 2017.
41. W. G. Tzeng, A polynomial time algorithm for the equivalence of probabilistic automata. *SIAM J. Comput.*, vol. 21, no.2, pp. 216–227, 1992.
42. Y. Wen, C. Li and M. Jeng, A polynomial algorithm for checking diagnosability of Petri nets. Proc. of the IEEE International Conference on Systems, Man and Cybernetics, vol. 3, pp. 2542–2547, 2005.
43. Y. Wu and C. N. Hadjicostis, Algebraic approaches for fault identification in discrete-event systems. *IEEE Transactions on Automatic Control*, vol. 50, no. 12, pp. 2048–2055, 2005.
44. Y. Yan, L. Ye and P. Dague, Diagnosability for patterns in distributed discrete event systems. Proc. of the 21st Int. Workshop on Principles of Diagnosis (DX'10), Portland, OR, United States, 2010.
45. L. Yin, Z. Li, N. Wu, S. Wang and T. Qu, Fault diagnosis in partially observed Petri nets using redundancies. *IEEE Access*, vol. 6, pp. 7541–7556, 2018.
46. X. Yin and S. Lafortune, On the decidability and complexity of diagnosability for labeled Petri nets. *IEEE Transactions on Automatic Control*, vol. 62, no. 11, pp. 5931–5938, 2017.
47. T. Yoo and S. Lafortune, Polynomial-time verification of diagnosability of partially observed discrete-event systems. *IEEE Transactions on Automatic Control*, vol. 47, no. 9, pp. 1491–1495, 2002.
48. J. Zaytoon and S. Lafortune, Overview of fault diagnosis methods for Discrete Event Systems, *Annual Reviews in Control*, vol. 37, no. 2, pp. 308–320, 2013.