Repository Istituzionale dei Prodotti della Ricerca del Politecnico di Bari

Predictability Verification of Fault Patterns in Labeled Petri Nets

This is a post print of the following article

Original Citation:
Predictability Verification of Fault Patterns in Labeled Petri Nets / Cong, Xuya; Yu, Zhenhua; Fanti, Maria Pia; Mangini, Agostino Marcello; Li, Zhiwu. - In: IEEE TRANSACTIONS ON AUTOMATIC CONTROL. - ISSN 0018-9286. - STAMPA. - 70:3(2025), pp. 1973-1980. [10.1109/TAC.2024.3477959]

Availability:
This version is available at http://hdl.handle.net/11589/279367 since: 2025-01-23

Published version
DOI:10.1109/TAC.2024.3477959

Publisher:

Terms of use:

(Article begins on next page)

22 April 2026

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2024.3477959

Predictability Verification of Fault Patterns in Labeled Petri Nets

Xuya Cong, *Member, IEEE,* Zhenhua Yu, *Member, IEEE,* Maria Pia Fanti, *Fellow, IEEE,*
Agostino Marcello Mangini, *Senior Member, IEEE,* and Zhiwu Li, *Fellow, IEEE*

***Abstract*—This paper focuses on the predictability verification problem of fault patterns for both bounded and unbounded discrete event systems modeled with labeled Petri nets. A system is said to be predictable with respect to a fault pattern if any complete fault behavior in a fault pattern can be correctly predicted before its occurrence, where the fault patterns are characterized by a particular composition of a labeled Petri net with a fault pattern net. In this paper, we construct a fault pattern predictor net and a basis fault pattern predictor graph that is based on the notion of basis markings. By exploiting the fault pattern predictor net and basis fault pattern predictor graph, we derive a necessary and sufficient condition to check fault pattern predictability, which does not need the full reachability/coverability graph of a net, thus gaining practical computation benefits.**

***Index Terms*—Discrete event system, Petri net, fault pattern, predictability.**

I. INTRODUCTION

The occurrence of a fault in a system is usually hazardous and may lead to incalculable consequences. Inspired by the safety concern of a system, predictability is proposed to produce the exact fault alarms for system protection.

Discrete event systems (DESs) [1] evolve as asynchronous discrete events occur over time. The seminal work [2] initially proposes the concept of predictability (or prognosability) for DESs modeled with regular languages, where each sequence ending with a fault event should own a normal-prefix such that for all sequences with the same observation, a fault event will definitely occur after bounded steps along these normal sequences. Then, the notion of predictability has been extended to stochastic systems [3], decentralized systems [4], and systems with uncertainties [5].

All the above studies deal with the problem of predictability for bounded DESs modeled with automata. Compared with finite-state automata, Petri nets (PNs) are a more compact model that can characterize the behaviour of infinite-state systems. By utilizing the advantages of PNs, Lefebvre [6] disentangles event diagnosis and prognosis for partially observed PNs. Moreover, timed stochastic PNs are used as a modeling tool for verifying event predictability in [7].

A recent work in [8] reduces the problem of event prognosis for unbounded labeled PNs (LPNs) to a model checking problem. Motivated by the work in [8], You *et al.* [9] develop a more compact net structure, namely, a predictor net and build its predictor graph (PG) that is a variant of the reachability/coverability graph of the predictor net. Then, a necessary and sufficient condition for event predictability is provided through analyzing the structure of the PG. Focusing on bounded LPNs, the work in [10] studies the problems of event prognosability and enforcement by using a prognosability verifier, which takes the advantage of basis markings to circumvent a full state space enumeration.

Different from the above previous works [6–10], this paper addresses the problem of predictability of fault patterns instead of single fault events. Fault patterns [11–15] extend the expressiveness of fault models by introducing more complex fault behaviors [16], i.e., multiple and repeated faults, sequences of significant events, etc. Moreover, patterns are useful in generalizing the predictability definitions and separating the behaviour of the system and the prognosis tasks. Particularly, the work in [15] checks predictability of fault patterns for bounded LPNs by using a model-checking approach [17]. In this paper, a four-step approach is developed to verify fault pattern predictability of both bounded and unbounded LPNs. First, given an LPN and a fault pattern represented by a fault pattern net, we build a fault pattern labeled net (FPLN) that can characterize in an explicit way the fault pattern. Second, we build a kind of verifier called a fault pattern predictor net (FP^{2}N) by executing a particular composition of the FPLN and its nonfailure subnet. Third, to record the information about the occurrence of a future fault pattern, we construct a basis fault pattern predictor graph (BFP^{2}G) by using basis markings of subnets of the FP^{2}N, which is a variant of a basis coverability graph (BCG) [18] of the FP^{2}N. Finally, fault pattern predictability is verified by searching particular cycles in a BFP^{2}G.

The main contributions of this work are two fold. First, we study the problem of predictability of fault patterns in unbounded LPNs that has never been investigated in the literature as far as we know. Second, the notion of BFP^{2}Gs is proposed for checking predictability of fault patterns for both bounded and unbounded DESs, which can handle the problems of state space explosion and the infinite growth of state space.

The remainder of this paper is organized as follows. Section II recalls the basics of LPNs. Section III formalizes the problem of predictability of fault patterns. Section IV proposes an FP^{2}N and a BFP^{2}G for verifying predictability of fault

---

This work was partially supported by the Natural Science Foundation of China under Grant 62303375. (*Corresponding author: Zhenhua Yu.*)

X. Cong and Z. Yu are with the Institute of Systems Security and Control, College of Computer Science and Technology, Xi’an University of Science and Technology, Xi’an 710054, China (email: congxuya@xust.edu.cn; zhenhuayu@xust.edu.cn).

M. Fanti and A. Mangini are with the Department of Electrical and Information Engineering, Polytechnic of Bari, 70125 Bari, Italy (email: mariapia.fanti@poliba.it; agostinomarcello.mangini@poliba.it).

Z. Li is with the Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau (email: zwli@must.edu.mo).

Authorized licensed use limited to: Politecnico di Bari. Downloaded on January 23,2025 at 14:08:03 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2024.3477959

patterns in an LPN. Section VI concludes the paper.

II. BACKGROUND ON LPNS

Let $\mathbb{N}$ be a set of non-negative integers. A PN [19] is a four-tuple $PN = (P, T, Pre, Post)$, where P is a set of m places, T is a set of n transitions with $P \cup T \neq \emptyset$ and $P \cap T = \emptyset$, $Pre : P \times T \rightarrow \mathbb{N}$ and $Post : P \times T \rightarrow \mathbb{N}$ are the pre- and post-incidence functions that specify the arcs from places to transitions and transitions to places in the net, respectively. In general, Pre ($Post$) can be represented by an $m \times n$ matrix indexed by P and T. The incidence matrix of a PN is defined as $C = Post - Pre$. Given a place $p \in P$, its input and output sets are defined as ${}^\bullet p = \{t \in T | Post(p, t) > 0\}$ and $p^\bullet = \{t \in T | Pre(p, t) > 0\}$, respectively. The notions for ${}^\bullet t$ and $t^\bullet$ are analogously defined. For any transition $t \in T$, if ${}^\bullet t = \emptyset$, it is said to be a source transition.

A marking is a function $M : P \rightarrow \mathbb{N}$ that assigns to each place a non-negative integer number of tokens. Similarly, a marking M can be represented by an m-dimensional vector indexed by P. The marking of place p at M is denoted as $M(p)$. For the sake of brevity, a marking can be written as the sum of tokens of all places in P as $M = \sum_{p \in P} M(p)p$. A PN system $\langle PN, M_0\rangle$ is a net PN with an initial marking M_0. A transition t is enabled at M if $M \geq Pre(\cdot, t)$. The firing of a transition t at M leads to marking $M' = M + C(\cdot, t)$, which is denoted as $M[t\rangle M'$.

Marking M is said to be reachable from M_0 if there exists a transition sequence $\sigma = t_1 t_2 \dots t_k$ and markings $M_1, M_2, \dots, M_{k-1}$ such that $M_0[t_1\rangle M_1[t_2\rangle M_2 \dots M_{k-1}[t_k\rangle M$ holds, denoted as $M_0[\sigma\rangle M$. We write it as $M_0[\sigma\rangle$ if the destination marking is of no interest. Given a sequence $\sigma \in T^*$, let $\pi : T^* \rightarrow \mathbb{N}^n$ denote the function that associates to σ a vector $\pi(\sigma) = \vec{y} \in \mathbb{N}^n$, called the firing vector of σ, where T^* is the *Kleene-closure* [1] of T. The set of all reachable markings from M_0 is denoted as $R(PN, M_0)$. A net system $\langle PN, M_0\rangle$ is said to be bounded if the set $R(PN, M_0)$ is finite. Otherwise, the net is unbounded. A transition $t \in T$ is dead if for all $M \in R(PN, M_0)$, t is not enabled at M, otherwise it is quasi-live. It is live if for each reachable marking $M \in R(PN, M_0)$, t is quasi-live in $\langle PN, M\rangle$. A marking M is a deadlock marking if no transition is enabled at it. The set of all sequences that can fire in $\langle PN, M_0\rangle$ is defined as $L(PN, M_0) = \{\sigma \in T^* | M_0[\sigma\rangle\}$. A sequence $\sigma \in T^+$ ($T^+ = T^* \backslash \{\varepsilon\}$) is said to be repetitive if there exists a marking $M_1 \in R(PN, M_0)$ such that $M_1[\sigma\rangle M_2[\sigma\rangle M_3[\sigma\rangle \dots$, i.e., if it can fire infinitely often starting from M_1. An acyclic PN indicates that there are no oriented cycles. If $\langle PN, M_0\rangle$ is acyclic, then a marking M is reachable from M_0 if and only if there exists a non-negative integer vector $\vec{y}$ satisfying $M_0 + C \cdot \vec{y} = M$ [20].

Given a PN $PN = (P, T, Pre, Post)$ and a set $T' \subseteq T$ of transitions, we define the T'-induced subnet of PN as a new PN $PN' = (P, T', Pre', Post')$, where Pre' (resp., $Post'$) is the restriction of Pre (resp., $Post$) to $P \times T'$. The net PN' can be obtained from PN by removing all transitions in $T \backslash T'$.

An LPN system is a four-tuple $G = (PN, M_0, E, \lambda)$, where $\langle PN, M_0\rangle$ is a PN system, E is an alphabet (a set of labels) and $\lambda : T \rightarrow E \cup \{\varepsilon\}$ is a labeling function that assigns to a transition $t \in T$ either a symbol from E or the empty word ε. Moreover, T is partitioned into $T = T_o \cup T_u$ with $T_o \cap T_u = \emptyset$, where T_o (resp., T_u) is the set of n_o (resp., n_u) observable (resp., unobservable) transitions. For any transition $t \in T$, if $t \in T_o$ then $\lambda(t) \in E$, otherwise $\lambda(t) = \varepsilon$. A PN is said to be convergent if there exists no repetitive sequence of unobservable transitions [21]. In an LPN, the same label can be associated with more than one transition.

Let w denote the label sequence associated with a sequence $\sigma \in T^*$ such that $w = \lambda(\sigma)$ by extending the labeling function as $\lambda : T^* \rightarrow E^*$ in the usual way. Given an LPN system $G = (PN, M_0, E, \lambda)$, we define the language generated by G as $\mathcal{L}(PN, M_0) = \{w \in E^* | \exists \sigma \in L(PN, M_0) : \lambda(\sigma) = w\}$. Given a sequence $\sigma \in T^*$, let $pr(\sigma)$ denote the set of prefixes of σ, i.e., $pr(\sigma) = \{\sigma_1 \in T^* | \exists \sigma_2 \in T^* : \sigma = \sigma_1\sigma_2\}$. Finally, let $|\sigma|$ denote the length of σ.

III. FORMULATION ON PREDICTABILITY OF FAULT PATTERNS

This paper takes into account LPNs with fault patterns. First, we provide some notions about the fault patterns.

Definition 1: A fault pattern Σ_F of an LPN system $G = (PN, M_0, E, \lambda)$ is a (finite or infinite) set of firing sequences of finite length $\Sigma_F \subseteq L(PN, M_0)$.

In particular, fault patterns should be the complement of a safety property. That is to say, given an LPN $G = (PN, M_0, E, \lambda)$ and its fault pattern Σ_F, for all $\sigma \in \Sigma_F$ and $\sigma\tau \in L(PN, M_0)$, we have $\sigma\tau \in \Sigma_F$.

Definition 2: Given an LPN $G = (PN, M_0, E, \lambda)$ with $PN = (P, T, Pre, Post)$, let Σ_F be its fault pattern. A normal sequence $\sigma \in T^*$ is said to be a boundary sequence if there exists a transition $t \in T$ such that $\sigma t \in \Sigma_F$. The set of boundary sequences of G is defined as $\Psi(\Sigma_F) = \{\sigma \in L(PN, M_0) \setminus \Sigma_F | \exists t \in T : \sigma t \in \Sigma_F\}$.

In order to model fault behaviours of an LPN system, we recall the notion of a fault pattern net in [14] as follows.

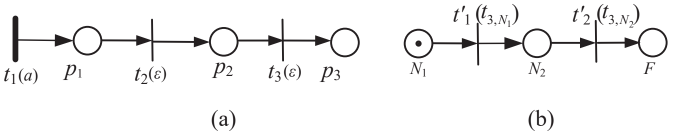
Definition 3: Given an LPN $G = (PN, M_0, E, \lambda)$ with $PN = (P, T, Pre, Post)$ and a subset $T_{sync} \subseteq T$ of r synchronization transitions, a fault pattern net is a pair (FPN, SF), where $FPN = (P^F, T^F, Pre^F, Post^F, M_0^F)$ is a PN system and SF is a synchronization function, satisfying the following statements:

- $P^F = \{N_1, \dots, N_q, F\}$ is a set of $q + 1$ places, where F is a single trapping place of the net, i.e., $F^\bullet = \emptyset$;
- T^F is a set of $q \times r$ transitions with $t_{j,p} \in T^F$ for $t_j \in T_{sync}$ and $p \in P^F \setminus \{F\}$;
- $SF : T_{sync} \times (P^F \setminus \{F\}) \rightarrow T^F$ is a bijective function associating each transition t' in T^F to a single pair $(t, p) \in T_{sync} \times (P^F \setminus \{F\})$;
- $(P^F, T^F, Pre^F, Post^F, M_0^F)$ is a state machine: each transition has one incoming arc, one outgoing arc, and any reachable marking holds 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_0^F satisfies $M_0^F(N_1) = 1$ and $M_0^F(p) = 0$ for all $p \in P^F \setminus \{N_1\}$.

Authorized licensed use limited to: Politecnico di Bari. Downloaded on January 23,2025 at 14:08:03 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2024.3477959

A fault pattern net in Definition 3 is a safe (i.e., 1-bounded) net system that generates a regular language. Note that it is convenient to extend Definition 3 to the nets that describe multiple fault patterns by introducing a set of multiple fault places. Moreover, a synchronization transition can be either observable or unobservable.



(a) (b)

Fig. 1: (a) An LPN and (b) a fault pattern net (FPN, SF).

Example 1: Given an LPN in Fig. 1(a), let us consider a fault pattern net in Fig. 1(b). For each transition $t' \in T^F$, the denomination within brackets $(t_{j,p})$ refers to the transition $t_j \in T_{sync}$ of the LPN in Fig. 1(a) and to the place $p \in P^F \setminus \{F\}$ of the fault pattern net in Fig. 1(b) such that $t' = SF(t_j, p)$.

Pair (FPN, SF) in Fig. 1(b) recognizes the firings of t_3 at least twice during the system operation no matter how it evolves between the two firings of t_3. In particular, the two transitions t'_1 and t'_2 of FPN correspond to the two successive firings of transition t_3 of the LPN in Fig. 1(a). $N = \{N_1, N_2\}$ is the set of normal places and F is the fault place. Let $T_{sync} = \{t_3\}$ and the synchronization function be specified by $SF(t_3, N_1) = t'_1$ and $SF(t_3, N_2) = t'_2$. (FPN, SF) aims to predict the set of sequences $\Sigma_F = (T \backslash \{t_3\})^* \{t_3\} (T \backslash \{t_3\})^* \{t_3\} T^*$ for the LPN in Fig. 1(a). □

Since a fault pattern may not be represented by a PN, we only consider the fault patterns that can be represented by the fault pattern nets of this research. Then, we provide the notion of a fault pattern labeled net (FPLN) that is the logic version of a fault pattern stochastic net in [14].

Definition 4: Given an LPN $G = (PN, M_0, E, \lambda)$ with $PN = (P, T, Pre, Post)$, a subset $T_{sync} \subseteq T$ with r synchronization transitions, a fault pattern Σ_F represented by (FPN, SF) with $FPN = (P^F, T^F, Pre^F, Post^F, M_0^F)$, and a synchronization function SF, an FPLN is a net defined as $\hat{G} = G \times_{SF} FPN = (\hat{PN}, \hat{M}_0, E, \hat{\lambda})$ with $\hat{PN} = (\hat{P}, \hat{T}, \hat{Pre}, \hat{Post})$ such that

- $\hat{P} = P \cup P^F$ is a set of $m + q + 1$ places;
- $\hat{T} = T \cup T^F$ is a set of $n + q \times r$ transitions;
- the matrices $\hat{Pre}$ and $\hat{Post}$ are defined as:
  - $\hat{Pre}(p, t) = Pre(p, t)$, $\hat{Post}(p, t) = Post(p, t)$ for $p \in P$ and $t \in T$,
  - $\hat{Pre}(p, t_{j,p}) = Pre^F(p, t_{j,p})$, $\hat{Post}(p, t_{j,p}) = Post^F(p, t_{j,p})$ for $p \in P^F$ and $t_{j,p} \in T^F$,
  - $\hat{Pre}(p', t_{j,p}) = Pre(p', t_j)$, $\hat{Post}(p', t_{j,p}) = Post(p', t_j)$ for $p' \in P$, $p \in P^F \setminus \{F\}$, $t_j \in T_{sync}$, and $t_{j,p} \in T^F$,
  - $\hat{Pre}(p, t) = \hat{Post}(p, t) = 0$ for $p \in P^F$ and $t \in T \setminus T_{sync}$,
  - $\hat{Pre}(F, t) = \hat{Post}(F, t) = 1$ for $t \in T_{sync}$;
- the label of a transition $t_{j,p} \in T^F$ is defined as $\hat{\lambda}(t_{j,p}) = \lambda(t_j)$, and the label of a transition $t \in T$ does not change;
- $\hat{M}_0(p) = M_0(p)$ for all $p \in P$ and $\hat{M}_0(p) = M_0^F(p)$ for all $p \in P^F$.

In plain words, an FPLN is a particular composition of an LPN with a fault pattern net based on the synchronization function SF, which can characterize in an explicit way the fault pattern. The set of transitions $\hat{T}$ in an FPLN is divided into $\hat{T} = \hat{T}_u \cup \hat{T}_o$, where $\hat{T}_u$ and $\hat{T}_o$ are the sets of unobservable and observable transitions in the FPLN, respectively. In the following, we introduce a function $\phi : \hat{T} \to T$ such that $\phi(t) = t$ for $t \in T$ and $\phi(t_{j,p}) = t_j$ for $t_{j,p} \in T^F$. Furthermore, the function ϕ can be extended to $\phi : \hat{T}^* \to T^*$ in the usual way. By using the function ϕ, $\phi(L(\hat{PN}, \hat{M}_0))$ denotes the set of transition sequences $L(\hat{PN}, \hat{M}_0)$ projected on the transition set T. According to the construction of an FPLN, we have $\mathcal{L}(\hat{PN}, \hat{M}_0) = \mathcal{L}(PN, M_0)$ and $\phi(L(\hat{PN}, \hat{M}_0)) = L(PN, M_0)$ with $\hat{M}_0(P) = M_0$.

Definition 5: Given an FPLN $\hat{G} = (\hat{PN}, \hat{M}_0, E, \hat{\lambda})$ with $\hat{PN} = (\hat{P}, \hat{T}, \hat{Pre}, \hat{Post})$, a transition $t \in T^F$ ($T^F \subsetneq \hat{T}$) is said to be a boundary transition if $F \in t^\bullet$. The set of boundary transitions of an FPLN is defined as $T_b^F = \{t \in T^F | F \in t^\bullet\}$.

Based on Definition 5, once a boundary transition t fires, a fault pattern Σ_F has occurred, i.e., we have $\phi(\sigma t) \in \Sigma_F$ with $\phi(\sigma) \notin \Sigma_F$ and $t \in T_b^F$.

Example 2: Fig. 2 shows an FPLN obtained by composing the LPN in Fig. 1(a) with the fault pattern net in Fig. 1(b), which has one boundary transition t_{3,N_2}. Once the place F has a token, it implies that a firing sequence including at least two firings of transition t_3 has occurred in the LPN starting from the initial marking M_0, i.e., the fault pattern has occurred. □

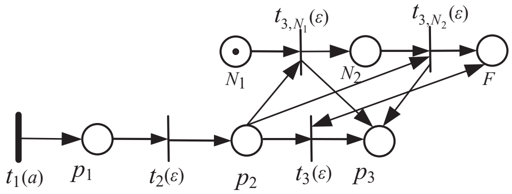


Fig. 2: An FPLN.

Definition 6: An LPN $G = (PN, M_0, E, \lambda)$ is said to be predictable with respect to (w.r.t.) a fault pattern Σ_F if

$$\begin{gathered}(\forall \sigma \in \Sigma_F)(\exists \rho \in pr(\sigma))(\forall \mu \in L(PN, M_0))\\ [M_0[\sigma\rangle \wedge \rho \notin \Sigma_F \wedge \lambda(\mu) = \lambda(\rho) \wedge \mu \notin \Sigma_F] \Rightarrow D,\end{gathered}$$

where the predictability condition D is a predicate

$$(\exists K \in \mathbb{N})(\forall \mu\mu' \in L(PN, M_0))[|\mu'| \geq K \Rightarrow \mu\mu' \in \Sigma_F].$$

By Definition 6, an LPN is predictable w.r.t. a given fault pattern if, for any sequence in the fault pattern, there exists at least one of its nonfailure prefixes such that we are certain that a fault pattern is guaranteed to occur within a finite number of steps, i.e., an alarm is set correctly. Then, we provide three necessary assumptions for the development of this research.

A1) The PN does not enter a deadlock marking before the occurrence of a fault pattern.
A2) The unobservable subnet of the PN and that of the fault pattern net are acyclic.
A3) The PN and the fault pattern net are convergent.

Assumption A1 is a counterpart of the typical assumption of diagnosability, on which the main results of this paper

Authorized licensed use limited to: Politecnico di Bari. Downloaded on January 23,2025 at 14:08:03 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2024.3477959

rely. Assumptions A2 and A3 are technical conveniences that allow us to verify the predictability of fault patterns without generating the full state space. In order to verify whether an LPN satisfies Assumption A3, we provide the following result.

Proposition 1: If the unobservable subnet of an LPN G is acyclic and there is no unobservable source transition, then the LPN is convergent.

Proof: By contradiction, suppose that the LPN is not convergent. Then, there exists a transition sequence σ that can be generated by either an unobservable transition cycle or an unobservable source transition, which contradicts the hypothesis and completes the proof. □

IV. BASIS FAULT PATTERN PREDICTOR GRAPH

This section introduces a new structure, called a basis fault pattern predictor graph (BFP^{2}G) that is used to verify predictability of fault patterns in LPNs without generating the full state space. To this end, we first construct an FP^{2}N by composing the FPLN and its nonfailure subnet, and then build a BFP^{2}G by using basis markings of subnets of the FP^{2}N.

A. Fault Pattern Predictor Net

Given an FPLN $\hat{G} = (\hat{P}N, \hat{M}_0, E, \hat{\lambda})$ with $\hat{P}N = (\hat{P}, \hat{T}, \hat{P}re, \hat{P}ost)$, its nonfailure subnet $\hat{G}^n = (\hat{P}N^n, \hat{M}_0^n, E, \hat{\lambda}^n)$ with $\hat{P}N^n = (\hat{P}^n, \hat{T}^n, \hat{P}re^n, \hat{P}ost^n)$ is derived from $\hat{G}$ by removing all transitions in $T_b^F \cup T_{sync}$ and the related arcs, and $\hat{\lambda}^n$ coincides with $\hat{\lambda}$ restricted to $\hat{T}^n$. In order to distinguish the places and transitions from $\hat{G}$ and $\hat{G}^n$, we rename each transition and each place of $\hat{G}^n$ by attaching a superscript "n".

Note that the construction of an FP^{2}N is different from the parallel composition of two LPNs in [15]. In this work, we obtain an FP^{2}N by two steps. 1) The FPLN $\hat{G}$ and its nonfailure subnet $\hat{G}^n$ are synchronized based on the same labels. Each unobservable transition, each synchronization transition, and each boundary transition is synchronized with an empty transition θ. 2) All the transitions in $\hat{G}^n$ are added to the net derived from Step 1) via the same arcs in $\hat{G}^n$.

Definition 7: Let $G = (PN, M_0, E, \lambda)$ be an LPN, $\hat{G} = (\hat{P}N, \hat{M}_0, E, \hat{\lambda})$ with $\hat{P}N = (\hat{P}, \hat{T}, \hat{P}re, \hat{P}ost)$ be its FPLN, and $\hat{G}^n = (\hat{P}N^n, \hat{M}_0^n, E, \hat{\lambda}^n)$ with $\hat{P}N^n = (\hat{P}^n, \hat{T}^n, \hat{P}re^n, \hat{P}ost^n)$ be the nonfailure subnet of $\hat{G}$. An FP^{2}N $\langle \tilde{P}N, \tilde{M}_0 \rangle$ with $\tilde{P}N = (\tilde{P}, \tilde{T}, \tilde{P}re, \tilde{P}ost)$ is defined as follows:

1) $\tilde{P} = \hat{P} \cup \hat{P}^n$;
2) $\tilde{M}_0 = [\hat{M}_0^T, (\hat{M}_0^n)^T]^T$;
3) $\tilde{T} \subsetneq \hat{T}^n \cup (T_{sync} \cup T_b^F) \times \{\theta\} \cup (\hat{T} \setminus (T_{sync} \cup T_b^F) \cup \{\theta\}) \times (\hat{T}^n \cup \{\theta\})$ where

3a) For each $t \in \hat{T} \setminus (T_{sync} \cup T_b^F)$, $t^n \in \hat{T}^n$, $p \in \hat{P}$, and $p^n \in \hat{P}^n$,

- if $\hat{\lambda}(t) = \hat{\lambda}^n(t^n) \neq \varepsilon$, let $\tilde{P}re(p, (t, t^n)) = \hat{P}re(p, t)$, $\tilde{P}ost(p, (t, t^n)) = \hat{P}ost(p, t)$, $\tilde{P}re(p^n, (t, t^n)) = \hat{P}re^n(p^n, t^n)$, and $\tilde{P}ost(p^n, (t, t^n)) = \hat{P}ost^n(p^n, t^n)$;
- if $\hat{\lambda}(t) = \hat{\lambda}^n(t^n) = \varepsilon$, let $\tilde{P}re(p, (t, \theta)) = \hat{P}re(p, t)$, $\tilde{P}ost(p, (t, \theta)) = \hat{P}ost(p, t)$, $\tilde{P}re(p^n, (\theta, t^n)) = \hat{P}re^n(p^n, t^n)$, and $\tilde{P}ost(p^n, (\theta, t^n)) = \hat{P}ost^n(p^n, t^n)$;

3b) For each $t \in T_{sync} \cup T_b^F$, $p \in \hat{P}$, let $\tilde{P}re(p, (t, \theta)) = \hat{P}re(p, t)$ and $\tilde{P}ost(p, (t, \theta)) = \hat{P}ost(p, t)$;

3c) For each $t^n \in \hat{T}^n$, $p^n \in \hat{P}^n$, let $\tilde{P}re(p^n, t^n) = \hat{P}re^n(p^n, t^n)$ and $\tilde{P}ost(p^n, t^n) = \hat{P}ost^n(p^n, t^n)$.

Given an FP^{2}N $\langle \tilde{P}N, \tilde{M}_0 \rangle$ with $\tilde{P}N = (\tilde{P}, \tilde{T}, \tilde{P}re, \tilde{P}ost)$, the set of transitions is divided into two parts $\tilde{T} = \tilde{T}^1 \cup \tilde{T}^2$, where $\tilde{T}^1$ represents the set of transitions that are exactly a single transition, and $\tilde{T}^2$ represents the set of transitions that are in the form of pairs of transitions. Specially, we use $\tilde{T}_b^F$ (resp., $\tilde{T}_{sync}$) to denote the set of pairs of transitions containing a boundary transition (resp., synchronization transition) as a component. In addition, we use $\tilde{T}_o^1$, $\tilde{T}_o^2$, $\tilde{T}_u^1$, and $\tilde{T}_u^2$ to denote the set of observable transitions in a single form, the set of pairs of observable transitions, the set of unobservable transitions in a single form, and the set of pairs of an unobservable transition and an empty transition θ, respectively. In the following, let $\tilde{T}_o = \tilde{T}_o^1 \cup \tilde{T}_o^2$, $\tilde{T}_u = \tilde{T}_u^1 \cup \tilde{T}_u^2$, and $\tilde{T}^{FP} = \tilde{T}_b^F \cup \tilde{T}_{sync}$.

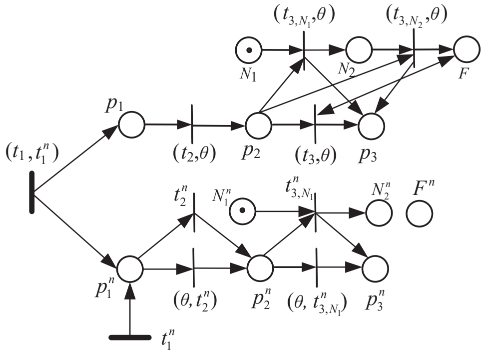


Fig. 3: An FP^{2}N.

Example 3: The PN in Fig. 3 is the FP^{2}N of the LPN in Fig. 1(a) and the fault pattern net in Fig. 1(b). As for the FP^{2}N in Fig. 3, we have $\tilde{T}^1 = \{t_1^n, t_2^n, t_{3,N_1}^n\}$, $\tilde{T}^2 = \{(t_1, t_1^n), (t_2, \theta), (\theta, t_2^n), (t_3, \theta), (t_{3,N_1}, \theta), (t_{3,N_2}, \theta), (\theta, t_{3,N_1}^n)\}$, $\tilde{T}_{sync} = \{(t_3, \theta)\}$, and $\tilde{T}_b^F = \{(t_{3,N_2}, \theta)\}$.

B. Preliminary Definitions

Similar to the BCG, for unbounded LPNs, we introduce a symbol ω to represent the tokens for unbounded places. In particular, for all $k \in \mathbb{N}$, we have $k < \omega$ and $\omega \pm k = \omega$, and we use $\mathbb{N}_\omega$ to denote the set of $\mathbb{N} \cup \{\omega\}$.

In this paper, the $\tilde{T}^1$-induced and $\tilde{T}^2$-induced subnets of $\langle \tilde{P}N, \tilde{M}_0 \rangle$ are written as $\langle \tilde{P}N^1, \tilde{M}_0 \rangle$ and $\langle \tilde{P}N^2, \tilde{M}_0 \rangle$ with $\tilde{P}N^1 = (\tilde{P}, \tilde{T}^1, \tilde{P}re^1, \tilde{P}ost^1)$ and $\tilde{P}N^2 = (\tilde{P}, \tilde{T}^2, \tilde{P}re^2, \tilde{P}ost^2)$, respectively, where $\tilde{P}re^1$ and $\tilde{P}ost^1$ (resp., $\tilde{P}re^2$ and $\tilde{P}ost^2$) are the restrictions of $\tilde{P}re$ and $\tilde{P}ost$ to $\tilde{T}^1$ (resp., $\tilde{T}^2$), respectively. The nonfailure subnet of $\langle \tilde{P}N, \tilde{M}_0 \rangle$ is denoted as $\langle \tilde{P}N^n, \tilde{M}_0 \rangle$ by removing all transitions in $\tilde{T}^{FP}$ and the related arcs. Let $\tilde{\lambda} : \tilde{T} \setminus \tilde{T}^{FP} \rightarrow E \cup (E \times E) \cup \{\varepsilon\}$ be a labeling function. In particular, if $t \in \tilde{T}_o^1$, then $\tilde{\lambda}(t) = \hat{\lambda}^n(t) \in E$; if $t = (t_o, t'_o) \in \tilde{T}_o^2$, then $\tilde{\lambda}(t) = (\hat{\lambda}(t_o), \hat{\lambda}^n(t'_o)) \in (E \times E)$; otherwise $\tilde{\lambda}(t) = \varepsilon$. Moreover, $\tilde{\lambda}$ can be extended as $\tilde{\lambda} : (\tilde{T} \setminus \tilde{T}^{FP})^* \rightarrow (E \cup (E \times E))^*$ in the usual way.

Definition 8: Given a marking $\tilde{M}$ and an observable transition $t \in \tilde{T}_o^i$ (for $i = 1, 2$), we define:

- $\Sigma^i(\tilde{M}, t) = \{\sigma \in (\tilde{T}_u^i)^* | \exists \tilde{M}' \in \mathbb{N}_\omega^{|\tilde{P}|} : \tilde{M}[\sigma\rangle \tilde{M}' \wedge \tilde{M}' \geq \tilde{P}re^i(\cdot, t)\}$ as the set of explanations of t at $\tilde{M}$ and

Authorized licensed use limited to: Politecnico di Bari. Downloaded on January 23,2025 at 14:08:03 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2024.3477959

$Y^i(\tilde{M},t) = \{\vec{y}_u \in \mathbb{N}^{|\tilde{T}_u|} | \exists \sigma \in \Sigma^i(\tilde{M},t) : \vec{y}_u = \pi(\sigma)\}$ as the set of e-vectors;

- $\Sigma^i_{min}(\tilde{M},t) = \{\sigma \in \Sigma^i(\tilde{M},t) | \nexists \sigma' \in \Sigma^i(\tilde{M},t) : \pi(\sigma') \lneqq \pi(\sigma)\}$ as the set of minimal explanations of t at $\tilde{M}$ and $Y^i_{min}(\tilde{M},t) = \{\vec{y}_u \in \mathbb{N}^{|\tilde{T}_u|} | \exists \sigma \in \Sigma^i_{min}(\tilde{M},t) : \vec{y}_u = \pi(\sigma)\}$ as the corresponding set of minimal e-vectors.

In the following, we use $Y^{2reg}_{min}(\tilde{M},t)$ to denote the set of minimal e-vectors of the nonfailure subnet of $\langle \tilde{P}N^2, \tilde{M}_0 \rangle$ (thus restricted to $\tilde{T}^2_u \setminus \tilde{T}^{FP}$), and we use $\tilde{C}_u$ to denote the incidence matrix of the $\tilde{T}_u$-induced subnet of $\langle \tilde{P}N, \tilde{M}_0 \rangle$.

Then, we define the set of basis markings for a nonfailure subnet of $\langle \tilde{P}N^2, \tilde{M}_0 \rangle$ by using the notion of a temporary set iteratively. In particular, each pair $(\tilde{M}, B)$ in a temporary set has two components, the first one $\tilde{M}$ is a current marking, and the second B is a set of pairs of the previously generated markings and the corresponding minimal e-vectors.

Definition 9: Given a nonfailure subnet of $\langle \tilde{P}N^2, \tilde{M}_0 \rangle$, a temporary set $\tilde{\mathcal{M}}^2_x$ is defined as follows:

a) $(\tilde{M}_0, \emptyset) \in \tilde{\mathcal{M}}^2_x$;

b) if $(\tilde{M}, B) \in \tilde{\mathcal{M}}^2_x$, then let $B' = B \cup \{(\tilde{M}, \pi(\sigma))\}$ and $\tilde{M}_n = \tilde{M} + \tilde{C}(\cdot, t) + \tilde{C}_u \cdot \pi(\sigma)$ for all $t \in \tilde{T}^2_o$ and $\pi(\sigma) \in Y^{2reg}_{min}(\tilde{M},t)$, and the following two statements hold:

i) if for all $(\tilde{M}'', \pi(\sigma')) \in B'$, $\sigma_1 \in (\tilde{T}^2 \setminus \tilde{T}^{FP})^*$, and $\sigma_2 \in (\tilde{T}^2_u \setminus \tilde{T}^{FP})^*$ satisfying $\tilde{M}[\sigma_1\rangle \tilde{M}_1$ and $\tilde{M}''[\sigma_2\rangle \tilde{M}_2$ with $\tilde{M}_1 \in \mathbb{N}^{|\tilde{P}|}_\omega$, $\tilde{M}_2 \in \mathbb{N}^{|\tilde{P}|}_\omega$, $\pi(\sigma_1) \leq \pi(\sigma t)$, and $\pi(\sigma_2) \leq \pi(\sigma')$ such that $\tilde{M}_1 \ngeq \tilde{M}_2$, then let $\tilde{M}' = \tilde{M}_n$ and $(\tilde{M}', B') \in \tilde{\mathcal{M}}^2_x$;

ii) if there exists $(\tilde{M}'', \pi(\sigma')) \in B'$, $\sigma_1 \in (\tilde{T}^2 \setminus \tilde{T}^{FP})^*$, and $\sigma_2 \in (\tilde{T}^2_u \setminus \tilde{T}^{FP})^*$ satisfying $\tilde{M}[\sigma_1\rangle \tilde{M}_1$ and $\tilde{M}''[\sigma_2\rangle \tilde{M}_2$ with $\tilde{M}_1 \in \mathbb{N}^{|\tilde{P}|}_\omega$, $\tilde{M}_2 \in \mathbb{N}^{|\tilde{P}|}_\omega$, $\pi(\sigma_1) \leq \pi(\sigma t)$, and $\pi(\sigma_2) \leq \pi(\sigma')$ such that $\tilde{M}_1 \gneqq \tilde{M}_2$, then for all pairs $(\tilde{M}_1, \tilde{M}_2)$ with $\tilde{M}_1 \gneqq \tilde{M}_2$, let $\tilde{M}'(p) = \omega$ and $(\tilde{M}', B') \in \tilde{\mathcal{M}}^2_x$ for all $p \in \tilde{P}$ such that $\tilde{M}_1(p) > \tilde{M}_2(p)$.

Then, we define the set of basis markings as $\tilde{\mathcal{M}}^2_B = \{\tilde{M} \in \mathbb{N}^{|\tilde{P}|}_\omega | \exists B \in 2^{\mathbb{N}^{|\tilde{P}|}_\omega \times \mathbb{N}^{|\tilde{T}_u|}} : (\tilde{M}, B) \in \tilde{\mathcal{M}}^2_x\}$.

Now, we define a dangerous pair (or basis marking) and a set of dangerous pairs (or basis markings) as follows.

Definition 10: Given a pair $(\tilde{M}, B) \in \tilde{\mathcal{M}}^2_x$ (or basis marking $\tilde{M} \in \tilde{\mathcal{M}}^2_B$), $(\tilde{M}, B)$ (or $\tilde{M}$) is said to be dangerous if there exists a transition $t \in \tilde{T}^F_b$ such that $Y^{2reg}_{min}(\tilde{M},t) \neq \emptyset$. The set of dangerous pairs (or basis markings) is denoted as $\tilde{\mathcal{M}}^2_{xd}$ (or $\tilde{\mathcal{M}}^2_{Bd}$).

A dangerous basis marking is a marking from which a fault pattern can eventually occur after firing a normal unobservable transition sequence $\sigma \in (\tilde{T}^2_u \setminus \tilde{T}^{FP})^*$, which is useful to check predictability in the next section. For a $\tilde{T}^1$-induced subnet of $\langle \tilde{P}N, \tilde{M}_0 \rangle$, the set of basis markings generated from a dangerous pair is defined iteratively in Definition 11.

Definition 11: Given a $\tilde{T}^1$-induced subnet of $\langle \tilde{P}N, \tilde{M}_0 \rangle$, let $\tilde{\mathcal{M}}^2_{xd}$ be a set of dangerous pairs and $(\tilde{M}_i, B_j)$ be a dangerous pair in $\tilde{\mathcal{M}}^2_{xd}$. A temporary set $\tilde{\mathcal{M}}^1_{x_{ij}}$ is defined as follows:

a) $(\tilde{M}_i, B_j) \in \tilde{\mathcal{M}}^1_{x_{ij}}$;

b) if $(\tilde{M}, B) \in \tilde{\mathcal{M}}^1_{x_{ij}}$, then let $B' = B \cup \{(\tilde{M}, \pi(\sigma))\}$ and $\tilde{M}_n = \tilde{M} + \tilde{C}(\cdot, t) + \tilde{C}_u \cdot \pi(\sigma)$ for all $t \in \tilde{T}^1_o$ and $\pi(\sigma) \in Y^1_{min}(\tilde{M},t)$, and the following two statements hold:

i) if for all $(\tilde{M}'', \pi(\sigma')) \in B'$, $\sigma_1 \in (\tilde{T}^1)^*$, and $\sigma_2 \in (\tilde{T}^1_u)^*$satisfying $\tilde{M}[\sigma_1\rangle \tilde{M}_1$ and $\tilde{M}''[\sigma_2\rangle \tilde{M}_2$ with $\tilde{M}_1 \in \mathbb{N}^{|\tilde{P}|}_\omega$, $\tilde{M}_2 \in \mathbb{N}^{|\tilde{P}|}_\omega$, $\pi(\sigma_1) \leq \pi(\sigma t)$, and $\pi(\sigma_2) \leq \pi(\sigma')$ such that $\tilde{M}_1 \ngeq \tilde{M}_2$, then let $\tilde{M}' = \tilde{M}_n$ and $(\tilde{M}', B') \in \tilde{\mathcal{M}}^1_{x_{ij}}$;

ii) if there exists $(\tilde{M}'', \pi(\sigma')) \in B'$, $\sigma_1 \in (\tilde{T}^1)^*$, and $\sigma_2 \in (\tilde{T}^1_u)^*$ satisfying $\tilde{M}[\sigma_1\rangle \tilde{M}_1$ and $\tilde{M}''[\sigma_2\rangle \tilde{M}_2$ with $\tilde{M}_1 \in \mathbb{N}^{|\tilde{P}|}_\omega$, $\tilde{M}_2 \in \mathbb{N}^{|\tilde{P}|}_\omega$, $\pi(\sigma_1) \leq \pi(\sigma t)$, and $\pi(\sigma_2) \leq \pi(\sigma')$ such that $\tilde{M}_1 \gneqq \tilde{M}_2$, then for all pairs $(\tilde{M}_1, \tilde{M}_2)$ with $\tilde{M}_1 \gneqq \tilde{M}_2$, let $\tilde{M}'(p) = \omega$ and $(\tilde{M}', B') \in \tilde{\mathcal{M}}^1_{x_{ij}}$ for all $p \in \tilde{P}$ such that $\tilde{M}_1(p) > \tilde{M}_2(p)$.

Then, we define the set of basis markings generated from a dangerous pair $(\tilde{M}_i, B_j) \in \tilde{\mathcal{M}}^2_{xd}$ as $\tilde{\mathcal{M}}^1_{B_{ij}} = \{\tilde{M} \in \mathbb{N}^{|\tilde{P}|}_\omega | \exists B \in 2^{\mathbb{N}^{|\tilde{P}|}_\omega \times \mathbb{N}^{|\tilde{T}_u|}} : (\tilde{M}, B) \in \tilde{\mathcal{M}}^1_{x_{ij}}\}$.

Note that the temporary sets $\tilde{\mathcal{M}}^2_x$ and $\tilde{\mathcal{M}}^1_{x_{ij}}$ are used to determine which places are labeled by the symbol ω. Particularly, in Definition 9, $\tilde{M}_n$ is derived from $\tilde{M}$ by firing transition $t \in \tilde{T}^2_o$ together with the minimal explanation restricted to $\tilde{T}^2_u \setminus \tilde{T}^{FP}$, and the pair of marking $\tilde{M}$ and the minimal e-vector $\pi(\sigma)$ is stored in B'. Then, in case b(i), each marking $\tilde{M}_1$ in a path from $\tilde{M}$ to $\tilde{M}_n$ is no greater than any marking $\tilde{M}_2$ in a path from $\tilde{M}_0$ to the predecessor of $\tilde{M}_n$, no additional symbol ω is assigned to any place of $\tilde{M}_n$, and we set $\tilde{M}' = \tilde{M}_n$. In case b(ii), for each pair of $\tilde{M}_1$ and $\tilde{M}_2$ such that $\tilde{M}_1 \gneqq \tilde{M}_2$, for all $p \in \tilde{P}$ such that $\tilde{M}_1(p) > \tilde{M}_2(p)$, we set $\tilde{M}'(p) = \omega$; and for all $p \in \tilde{P}$ such that $\tilde{M}_1(p) = \tilde{M}_2(p)$, we set $\tilde{M}'(p) = \tilde{M}_n(p)$. The meaning of Definition 11 can be explained analogously.

Example 4: Consider the FP^{2}N in Fig. 3. Based on Definitions 9 and 10, we have $\tilde{\mathcal{M}}^2_x = \{(\tilde{M}_0, \emptyset), (\tilde{M}_1, B_1)\}$ with a dangerous pair $(\tilde{M}_1, B_1)$. Moreover, by Definition 11, it gives $\tilde{\mathcal{M}}^1_{x_{11}} = \{(\tilde{M}_1, B_1), (\tilde{M}_1, B_2)\}$. Here, we have $\tilde{M}_0 = N_1 + N^n_1$, $\tilde{M}_1 = \omega p_1 + N_1 + \omega p^n_1 + N^n_1$, $B_1 = \{(\tilde{M}_0, \vec{0})\}$, and $B_2 = \{(\tilde{M}_0, \vec{0}), (\tilde{M}_1, \vec{0})\}$. ☐

C. Construction of a BFP^{2}G

Definition 12: Given an LPN $G = (PN, M_0, E, \lambda)$, let $\langle \tilde{P}N, \tilde{M}_0 \rangle$ with $\tilde{P}N = (\tilde{P}, \tilde{T}, \tilde{P}re, \tilde{P}ost)$ be its FP^{2}N. The BFP^{2}G of G is a deterministic finite-state automaton $\mathcal{B} = (\tilde{\mathcal{M}}_B, \tilde{T}_{or}, \Delta, \tilde{M}_0)$ computed by using Algorithm 1, where $\tilde{\mathcal{M}}_B \subseteq \tilde{\mathcal{M}}^2_B \cup \tilde{\mathcal{M}}^1_{B_{ij}}$ for all i and j with $(\tilde{M}_i, B_j) \in \tilde{\mathcal{M}}^2_{xd}$ is the set of states, $\tilde{T}_{or} = \tilde{T}_o \times \mathbb{N}^{|\tilde{T}_u|}$ is the set of events, $\Delta \subseteq \tilde{\mathcal{M}}_B \times \tilde{T}_{or} \times \tilde{\mathcal{M}}_B$ is the transition relation, and $\tilde{M}_0$ is the initial state.

In Algorithm 1, the set $\tilde{\mathcal{M}}_{new}$ is initialized at $\{(\tilde{M}_0, \emptyset)\}$ in Step 2. For each pair $(\tilde{M}, B) \in \tilde{\mathcal{M}}_{new}$, if it is dangerous, we call function $BasisSonNodes$ in Step 7 to compute a basis son graph for the nonfailure subnet of the FPLN, which describes the normal behaviour of the FP^{2}N from $\tilde{M}$ by firing the transitions in $\tilde{T}^1_o$ and the corresponding minimal explanations. Otherwise, Steps 11 to 20 compute each successor pair $(\tilde{M}', B')$ by firing each transition in $\tilde{T}^2_o$ and its minimal explanation restricted to $\tilde{T}^2_u \setminus \tilde{T}^{FP}$, and compute the new arc from $(\tilde{M}, B)$ to $(\tilde{M}', B')$. Then, Step 22 removes $(\tilde{M}, B)$ from $\tilde{\mathcal{M}}_{new}$ indicating that $(\tilde{M}, B)$ has been considered. The procedure from Steps 3 to 23 is executed iteratively until $\tilde{\mathcal{M}}_{new}$ is empty. Finally, by running Steps 24 to 27, the BFP^{2}G is obtained by removing the second

Authorized licensed use limited to: Politecnico di Bari. Downloaded on January 23,2025 at 14:08:03 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2024.3477959

Algorithm 1 Construction of a BFP^{2}G.

```
Input: An LPN $G = (PN, M_0, E, \lambda)$ with $PN = (P, T, Pre, Post)$ and a fault pattern $\Sigma_F$
Output: A BFP$^2$G $\mathcal{B} = (\tilde{\mathcal{M}}_B, \tilde{T}_{or}, \Delta, \tilde{M}_0)$ of $G$
1: Compute the FP$^2$N $\langle \tilde{P}N, \tilde{M}_0 \rangle$;
2: $\tilde{\mathcal{M}}_B := \emptyset$, $\Delta_x := \emptyset$, $\Delta := \emptyset$, $B := \emptyset$, $\tilde{\mathcal{M}}_x := \{(\tilde{M}_0, B)\}$, and $\tilde{\mathcal{M}}_{new} := \{(\tilde{M}_0, B)\}$;
3: while $\tilde{\mathcal{M}}_{new} \neq \emptyset$ do
4:     choose a node $(\tilde{M}, B) \in \tilde{\mathcal{M}}_{new}$;
5:     if there exists $t \in \tilde{T}_b^F$ such that $Y_{min}^{2reg}(\tilde{M}, t) \neq \emptyset$ then
6:         assign tag "dangerous" to $\tilde{M}$ and $(\tilde{M}, B)$;
7:         call BasisSonNodes$(\tilde{M}, B)$ in Algorithm 2;
8:         $\tilde{\mathcal{M}}_x := \tilde{\mathcal{M}}_x \cup \tilde{\mathcal{M}}_x^1$ and $\Delta_x := \Delta_x \cup \Delta_x^1$;
9:     end if
10:    if $(\tilde{M}, B)$ has no tag "dangerous" then
11:        for each $t \in \tilde{T}_o^2$ and $Y_{min}^{2reg}(\tilde{M}, t) \neq \emptyset$ do
12:            for each $\pi(\sigma) \in Y_{min}^{2reg}(\tilde{M}, t)$ do
13:                compute the pair $(\tilde{M}', B')$ based on Definition 9;
14:                if $(\tilde{M}', B') \notin \tilde{\mathcal{M}}_x$ then
15:                    $\tilde{\mathcal{M}}_x := \tilde{\mathcal{M}}_x \cup \{(\tilde{M}', B')\}$;
16:                    $\tilde{\mathcal{M}}_{new} := \tilde{\mathcal{M}}_{new} \cup \{(\tilde{M}', B')\}$;
17:                end if
18:                $\Delta_x := \Delta_x \cup \{((\tilde{M}, B), (t, \pi(\sigma)), (\tilde{M}', B'))\}$;
19:            end for
20:        end for
21:    end if
22:    $\tilde{\mathcal{M}}_{new} := \tilde{\mathcal{M}}_{new} \setminus \{(\tilde{M}, B)\}$;
23: end while
24: $\tilde{\mathcal{M}}_B := \{\tilde{M} \in \mathbb{N}_\omega^{|\tilde{P}|} | \exists B \in 2^{\mathbb{N}_\omega^{|\tilde{P}|} \times \mathbb{N}^{|\tilde{T}_u|}} : (\tilde{M}, B) \in \tilde{\mathcal{M}}_x\}$;
25: for each $((\tilde{M}, B), (t, \pi(\sigma)), (\tilde{M}', B')) \in \Delta_x$ do
26:     $\Delta := \Delta \cup \{(\tilde{M}, (t, \pi(\sigma)), \tilde{M}')\}$;
27: end for
```

component from each pair $(\tilde{M}, B) \in \tilde{\mathcal{M}}_x$. Note that the detailed version of Algorithms 1 and 2 is shown in [22].

Algorithm 2 *Function BasisSonNodes*$(\tilde{M}, B)$.

```
Input: A dangerous pair $(\tilde{M}, B)$ and $\tilde{P}N^1 = (\tilde{P}, \tilde{T}^1, \tilde{P}re^1, \tilde{P}ost^1)$
Output: A basis son graph $\mathcal{B}^1 = (\tilde{\mathcal{M}}_x^1, \tilde{T}_{or}^1, \Delta_x^1, (\tilde{M}, B))$
$\tilde{\mathcal{M}}_x^1 := \{(\tilde{M}, B)\}$, $\Delta_x^1 := \emptyset$, and $\tilde{\mathcal{M}}_{novel}^1 := \{(\tilde{M}, B)\}$;
while $\tilde{\mathcal{M}}_{novel}^1 \neq \emptyset$ do
    choose a node $(\tilde{M}, B) \in \tilde{\mathcal{M}}_{novel}^1$;
    for each $t \in \tilde{T}_o^1$ and $Y_{min}^1(\tilde{M}, t) \neq \emptyset$ do
        for each $\pi(\sigma) \in Y_{min}^1(\tilde{M}, t)$ do
            compute the pair $(\tilde{M}', B')$ based on Definition 11;
            if $(\tilde{M}', B') \notin \tilde{\mathcal{M}}_x^1$ then
                $\tilde{\mathcal{M}}_x^1 := \tilde{\mathcal{M}}_x^1 \cup \{(\tilde{M}', B')\}$;
                $\tilde{\mathcal{M}}_{novel}^1 := \tilde{\mathcal{M}}_{novel}^1 \cup \{(\tilde{M}', B')\}$;
            end if
            $\Delta_x^1 := \Delta_x^1 \cup \{((\tilde{M}, B), (t, \pi(\sigma)), (\tilde{M}', B'))\}$;
        end for
    end for
    $\tilde{\mathcal{M}}_{novel}^1 := \tilde{\mathcal{M}}_{novel}^1 \setminus \{(\tilde{M}, B)\}$;
end while
```

Remark 1: Based on Assumption A2, the unobservable subnet of $\langle \tilde{P}N^1, \tilde{M}_0 \rangle$ and that of the nonfailure subnet of $\langle \tilde{P}N^2, \tilde{M}_0 \rangle$ are acyclic. Thus, the minimal e-vectors can be computed by Algorithm 4.4 in [23] using matrix manipulation.

Remark 2: The BCG of an FP^{2}N contains a transition sequence that has been already in the fault pattern, which does not record the information about the occurrence of the future fault pattern. Thus, it is necessary to introduce a new structure, namely, a BFP^{2}G to check fault pattern predictability of LPNs.

Proposition 2: Given an LPN $G = (PN, M_0, E, \lambda)$ with a fault pattern Σ_F satisfying Assumption A2, let $\langle \tilde{P}N, \tilde{M}_0 \rangle$ be its FP^{2}N, $\mathcal{B}$ be the BFP^{2}G of G, and $t \in \tilde{T}_o$ be an observable transition of $\langle \tilde{P}N, \tilde{M}_0 \rangle$. If there is an arc labeled by $(t, \pi(\sigma))$ in the BFP^{2}G $\mathcal{B}$, then transition t is quasi-live.

Proof: Based on Assumption A2 and the construction of the nonfailure subnet of $\langle \tilde{P}N, \tilde{M}_0 \rangle$, the unobservable subnet of $\langle \tilde{P}N^n, \tilde{M}_0 \rangle$ is acyclic. If we ignore Steps 5 to 10 and Step 21, replace $\tilde{T}_o^2$ by $\tilde{T}_o$ in Step 11, and replace $Y_{min}^{2reg}(\tilde{M}, t)$ by $Y_{min}^{reg}(\tilde{M}, t)$ in Steps 11 and 12, then the resulting graph coincides with a BCG of the nonfailure subnet $\langle \tilde{P}N^n, \tilde{M}_0 \rangle$, where $Y_{min}^{reg}(\tilde{M}, t)$ is the set of minimal e-vectors of $t \in \tilde{T}_o$ at $\tilde{M}$ in $\langle \tilde{P}N^n, \tilde{M}_0 \rangle$. Thus, all the arcs and states in the BFP^{2}G of $\langle \tilde{P}N, \tilde{M}_0 \rangle$ are also those in the BCG of $\langle \tilde{P}N^n, \tilde{M}_0 \rangle$, but the reverse does not hold. That is to say, the result holds according to the second statement of Proposition 12 in [18]. ☐

Proposition 2 indicates that if an observable transition $t \in \tilde{T}_o$ occurs as a first component in an arc in the BFP^{2}G, then there exists a firing sequence that can enable it definitely.

V. PREDICTABILITY VERIFICATION OF FAULT PATTERNS

A. *Necessary and Sufficient Condition for Predictability*

Given a cycle c in the BFP^{2}G, we use $X(c)$ to denote the set of states in c, and $\sigma(c)$ to denote the related sequence of transition and minimal e-vector pairs. Here, a cycle is a path that starts from and ends in the same state. Moreover, we denote the projection of $\sigma(c) = (t_1, \vec{y}_1) \ldots (t_k, \vec{y}_k)$ on its first component as $P_t(\sigma(c)) = t_1 \ldots t_k$. According to the construction of the BFP^{2}G, it holds that either $P_t(\sigma(c)) \in (\tilde{T}_o^1)^*$ or $P_t(\sigma(c)) \in (\tilde{T}_o^2)^*$. In this paper, a set of basis markings $\tilde{\mathcal{M}}_B$ in the BFP^{2}G is divided into two subsets: a set of ordinary basis markings and that of ω-basis markings. A basis marking is said to be ordinary if it does not contain symbol ω; otherwise it is called an ω-basis marking. An ω-basis marking can be regarded as a basis marking set containing infinite number of ordinary basis markings. In the following, we use $D(\tilde{M})$ to represent a set of ordinary basis markings that are consistent with $\tilde{M}$. For a basis marking $\tilde{M}$, we have $D(\tilde{M}) = \{\tilde{M}_i \in \mathbb{N}^{|\tilde{P}|} | (\forall p \in \tilde{P} : \tilde{M}(p) \neq w \Rightarrow \tilde{M}_i(p) = \tilde{M}(p)) \wedge (\forall p \in \tilde{P} : \tilde{M}(p) = \omega \Rightarrow \tilde{M}_i(p) \in \mathbb{N})\}$.

Definition 13: Given an LPN $G = (PN, M_0, E, \lambda)$ and its BFP^{2}G, a sequence $\tilde{s} = (t_1, \vec{y}_1) \ldots (t_k, \vec{y}_k)$ in the BFP^{2}G is said to be repetitive if it satisfies $\tilde{C} \cdot (\pi(P_t(\tilde{s})) + \sum_{i=1}^k \vec{y}_i) \geq \vec{0}$, where $\tilde{C}$ is the incidence matrix of the FP^{2}N of G and $P_t(\tilde{s})$ is the projection of $\tilde{s}$ on its first component.

Proposition 3: Given an LPN $G = (PN, M_0, E, \lambda)$ with a fault pattern Σ_F satisfying Assumption A2, let c be a cycle in the BFP^{2}G of G. For all $\tilde{M} \in X(c)$, there exists an ordinary basis marking $\tilde{M}_1$ in $D(\tilde{M})$ such that there exists a sequence $\tilde{\sigma} \in L(\tilde{P}N^n, \tilde{M}_0)$ satisfying $\tilde{M}_1[\tilde{\sigma}\rangle \tilde{M}_2[\tilde{\sigma}\rangle \tilde{M}_3 \ldots$ if and only if c is a cycle associated with a repetitive sequence, where $\tilde{\lambda}(\tilde{\sigma}) = \tilde{\lambda}(P_t(\sigma(c)))$ and $\sigma(c) = (t_1, \vec{y}_1) \ldots (t_k, \vec{y}_k)$.

Proof: *(If)* By Definition 13, if a cycle c is associated with a repetitive sequence, then $\tilde{C} \cdot (\pi(P_t(\sigma(c))) + \sum_{i=1}^k \vec{y}_i) \geq \vec{0}$ holds. Based on Proposition 2, it implies $\tilde{M}_i \leq \tilde{M}_j$ in the case that $\tilde{M}_j$ is reachable from $\tilde{M}_i$ by firing $\tilde{\sigma}$ with

Authorized licensed use limited to: Politecnico di Bari. Downloaded on January 23,2025 at 14:08:03 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2024.3477959

$\tilde{\lambda}(\tilde{\sigma}) = \tilde{\lambda}(P_t(\sigma(c)))$ in $\langle \tilde{P}N^n, \tilde{M}_0 \rangle$. That is to say, there exists an ordinary basis marking $\tilde{M}_1$ in $D(\tilde{M})$ such that $\tilde{M}_1[\tilde{\sigma}\rangle \tilde{M}_2[\tilde{\sigma}\rangle \tilde{M}_3 \ldots$ holds.

(Only if) By Assumption A2, the unobservable subnet of $\langle \tilde{P}N^n, \tilde{M}_0 \rangle$ is acyclic. Based on the construction of the BFP^{2}G, there exists an ordinary basis marking $\tilde{M}_1$ in $D(\tilde{M})$ and a transition sequence $\tilde{\sigma} = \sigma_1 t_1 \ldots \sigma_k t_k$ with $\pi(\sigma_1) = \vec{y}_1, \ldots, \pi(\sigma_k) = \vec{y}_k$ that can fire infinitely from $\tilde{M}_1$. Then, we have $\tilde{M}_i \leq \tilde{M}_{i+1}$ for all $i \in \{1, 2, \ldots\}$ and $\tilde{C} \cdot (\pi(P_t(\sigma(c))) + \sum_{i=1}^{k} \vec{y}_i) \geq \vec{0}$ with $\tilde{\lambda}(\tilde{\sigma}) = \tilde{\lambda}(P_t(\sigma(c)))$. Hence, c is a cycle associated with a repetitive sequence. □

A cycle c is said to be reachable from a basis marking $\tilde{M}$ if there exists a basis marking $\tilde{M}' \in X(c)$ such that $\tilde{M}'$ is reachable from $\tilde{M}$. Now we are ready to provide a necessary and sufficient condition for predictability verification of fault patterns in an LPN as follows.

Theorem 1: Given an LPN $G = (PN, M_0, E, \lambda)$ with a fault pattern Σ_F satisfying Assumptions A1 to A3, G is predictable w.r.t. Σ_F if and only if there does not exist any cycle associated with a repetitive sequence that is reachable from any dangerous basis marking $\tilde{M}$ in the BFP^{2}G.

Proof: *(If)* For each dangerous basis marking in the BFP^{2}G, there exists no cycle associated with a repetitive sequence. By Algorithm 1 and Proposition 3, it hold that $(\forall \phi(\rho t) \in \Sigma_F : \phi(\rho) \notin \Sigma_F \wedge t \in T_b^F)$, $(\forall \mu \in L(\hat{P}N^n, \hat{M}_0^n) : \lambda(\phi(\rho)) = \lambda(\phi(\mu)))$, and a deadlock definitely occurs in finite steps following μ in $\langle \hat{P}N^n, \hat{M}_0^n \rangle$ due to Assumptions A2 and A3. Since $\langle \hat{P}N^n, \hat{M}_0^n \rangle$ is obtained from $\langle \hat{P}N, \hat{M}_0 \rangle$ by removing boundary transitions, synchronization transitions, and the related arcs, and $\langle \hat{P}N, \hat{M}_0 \rangle$ does not enter a deadlock before the occurrence of a fault pattern by Assumption A1, we conclude that a fault pattern definitely occurs in finite steps following μ (resp., $\phi(\mu)$) in $\langle \hat{P}N, \hat{M}_0 \rangle$ (resp., G). That is to say, the LPN G is predictable w.r.t. Σ_F based on Definition 6.

(Only if) By contrapositive, assume that there exists a cycle c associated with a repetitive sequence, which is reachable from a dangerous basis marking $\tilde{M}$ in the BFP^{2}G. By Algorithm 1, c is generated by BasisSonNodes($\tilde{M}, B$). Based on Proposition 3, there exists an ordinary basis marking $\tilde{M}_1 \in D(\tilde{M})$ such that an arbitrary long sequence can occur from $\hat{M}_1^n$ in $\langle \hat{P}N^n, \hat{M}_0^n \rangle$ with $\hat{M}_1^n = \tilde{M}_1(\hat{P}^n)$. If $\tilde{M}$ is an ordinary basis marking, then $\tilde{M}$ can enable a transition $t \in \tilde{T}_b^F$ after firing a sequence $\sigma \in (\tilde{T}_u^2 \setminus \tilde{T}^{FP})^*$ since $\tilde{M}$ is a dangerous basis marking. If $\tilde{M}$ is an ω-basis marking, then there exists an ordinary basis marking $\tilde{M}_1' \in D(\tilde{M})$ with $\tilde{M}_1' \geq \tilde{M}_1$ such that $\tilde{M}_1'$ can enable a transition $t \in \tilde{T}_b^F$ after firing a sequence $\sigma \in (\tilde{T}_u^2 \setminus \tilde{T}^{FP})^*$ since $\tilde{M}$ is a dangerous basis marking. Thus, in both two cases, by Proposition 2, there exists a sequence $\tilde{\sigma} \in L(\tilde{P}N, \tilde{M}_0) \cap (\tilde{T}^2 \setminus \tilde{T}^{FP})^*$ whose firing at $\tilde{M}_0$ leads to an ordinary basis marking $\tilde{M}' \in D(\tilde{M})$ such that $\tilde{M}'$ can enable a transition $t \in \tilde{T}_b^F$ after firing a sequence $\sigma \in (\tilde{T}_u^2 \setminus \tilde{T}^{FP})^*$ and an arbitrary long sequence can occur from $\hat{M}^{n'}$ in $\langle \hat{P}N^n, \hat{M}_0^n \rangle$ with $\hat{M}^{n'} = \tilde{M}'(\hat{P}^n)$. Here, t is a transition pair and its first component is a boundary transition that is denoted as t_f.

Let $\rho = t_{j_1} \ldots t_{j_k}$ (resp., $\mu = t_{i_1}^n \ldots t_{i_k}^n$) be a sequence related to the first (resp., second) component of $P_t(\tilde{\sigma})$, where $P_t(\tilde{\sigma})$ is the projection of $\tilde{\sigma}$ on its first component. Due to Definition 7, the FP^{2}N can generate two transition sequences that have the same observation. Then, by Definition 2, we have $\sigma = \phi(\sigma_1 t_{j_1} \ldots \sigma_k t_{j_k} \sigma_{k+1}) \in \Psi(\Sigma_F)$ and $\sigma' = \phi(\sigma_1' t_{i_1}^n \ldots \sigma_k' t_{i_k}^n \sigma_{k+1}') \in L(PN, M_0) \setminus \Sigma_F$ with $\lambda(\sigma) = \lambda(\sigma')$, where $\sigma_1, \ldots, \sigma_{k+1} \in (\hat{T}_u \setminus (T_b^F \cup T_{sync}))^*$ and $\sigma_1', \ldots, \sigma_{k+1}' \in (\hat{T}_u^n)^*$ with $\hat{T}_u^n$ being the set of unobservable transitions in $\langle \hat{P}N^n, \hat{M}_0^n \rangle$. Moreover, it holds $\sigma \phi(t_f) \in \Sigma_F$, and an arbitrary long sequence can occur following σ' without reaching Σ_F. Thus, the LPN G violates the definition of predictability, and it is not predictable w.r.t. Σ_F. □

Corollary 1: Given a bounded LPN $G = (PN, M_0, E, \lambda)$ with a fault pattern Σ_F satisfying Assumptions A1 and A2, G is predictable w.r.t. Σ_F if and only if there does not exist any cycle that is reachable from any dangerous basis marking $\tilde{M}$ in the BFP^{2}G.

Proof: For any bounded LPN, any cycle in the BFP^{2}G is associated with a repetitive sequence, and Assumption A2 implies Assumption A3. The result immediately follows from Theorem 1. □

B. Complexity Analysis and Examples

We analyze the computational complexity of the proposed approach for bounded and unbounded LPNs. In the case of bounded LPNs, the first step is to construct the BFP^{2}G of an LPN and its fault pattern, which is exponential w.r.t. the net size (especially the number of places and the initial marking). The second step is to check the existence of cycles satisfying the condition in Corollary 1, whose complexity is linear w.r.t. the number of states and arcs in the BFP^{2}G by using Tarjan's strongly connected components algorithm [24]. In the case of unbounded LPNs, the procedure is more complex. Particularly, we need to search the cycles that are associated with repetitive sequences in a BFP^{2}G by using the technique proposed in [25]. More precisely, it is necessary to solve certain linear programming problems, and verify if there exists a solution that corresponds to a cycle in the BFP^{2}G. The size of the BFP^{2}G is equal to that of the coverability graph in the worst case, which requires even more than exponential space w.r.t. the net size (especially the number of places) [26]. Actually, the complexity of constructing the BFP^{2}G is not in primitive recursive space [26]. Thus, verifying the cycles in a BFP^{2}G has an exponential-space lower bound for its complexity w.r.t. the net size (especially the number of places). In fact, if we regard the boundary transitions in an FPLN as fault transitions, then the fault pattern predictability in an LPN can be reduced to predictability of fault transitions in an FPLN. Specifically, verifying predictability of fault transitions for unbounded LPNs is shown as EXPSPACE-hard in [8], which is also for the problem studied in this paper.

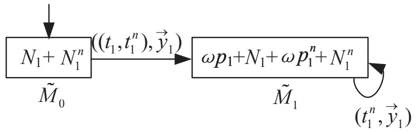


Fig. 4: The BFP^{2}G of the LPN in Fig. 1(a) with its fault pattern in Fig. 1(b).

Example 5: Consider again the LPN in Fig. 1(a) and its fault pattern Σ_F represented by (FPN, SF) in Fig. 1(b). By

Authorized licensed use limited to: Politecnico di Bari. Downloaded on January 23,2025 at 14:08:03 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2024.3477959

Algorithm 1, we construct its BFP^{2}G in Fig. 4 with two basis markings and two arcs, where the minimal e-vector on the arcs is $\vec{y}_1 = \vec{0}$. Since there exists a cycle associated with the repetitive sequence that is reachable from a dangerous basis marking $\tilde{M}_1$, the LPN is not predictable w.r.t. Σ_F based on Theorem 1. □

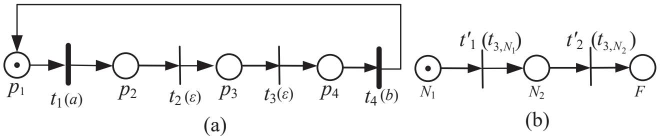


Fig. 5: (a) An LPN and (b) a fault pattern net (FPN, SF) in Example 5.

Example 6: Consider another LPN in Fig. 5(a) and its fault pattern Σ_F represented by (FPN, SF) in Fig. 5(b). By Algorithm 1, we build its BFP^{2}G in Fig. 6 with four basis markings and three arcs, where the minimal e-vectors on the arcs are $\vec{y}_1 = \vec{0}$ and $\vec{y}_2 = (t_2, \theta) + (t_{3,N_1}, \theta) + (\theta, t_2^n) + (\theta, t_{3,N_1}^n)$. The root node of the basis son graph is a dangerous pair $(\tilde{M}_3, \{(\tilde{M}_0, \vec{y}_1), (\tilde{M}_1, \vec{y}_2), (\tilde{M}_2, \vec{y}_1)\})$, i.e., $\tilde{M}_3$ is a dangerous basis marking. Since there exists no cycle that is reachable from $\tilde{M}_3$, the bounded LPN is predictable w.r.t. Σ_F according to Corollary 1. □

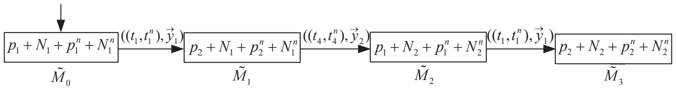


Fig. 6: The BFP^{2}G of the LPN in Fig. 5(a) with its fault pattern in Fig. 5(b).

Other examples considering more than one synchronization transition in fault patterns are illustrated in a supplementary material in [22].

VI. CONCLUSION

This paper presents a novel method to verify predictability of fault patterns for both bounded and unbounded LPNs. Particularly, by constructing and analyzing the BFP^{2}G of a given LPN, we obtain a necessary and sufficient condition for verifying predictability of fault patterns, which does not need the generation of the full reachability/coverability graph of any net. Our future work will explore the predictability enforcement of fault patterns in LPNs.

REFERENCES

[1] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*, Cham, Switzerland: Springer, 3rd, 2021.
[2] S. Genc and S. Lafortune, "Predictability of event occurrences in partially observed discrete-event systems," *Automatica*, vol. 45, no. 2, pp. 301–311, 2009.
[3] J. Chen and R. Kumar, "Stochastic failure prognosability of discrete event systems," *IEEE Trans. Autom. Control*, vol. 60, no. 6, pp. 1570–1581, Jun. 2015.
[4] X. Yin and Z. Li, "Decentralized fault prognosis of discrete-event systems using state-estimate-based protocols," *IEEE Trans. Cybern.*, vol. 49, no. 4, pp. 1302–1313, Apr. 2019.
[5] H. Liao, F. Liu, and N. Wu, "Robust predictability of stochastic discrete-event systems and a polynomial-time verification," *Automatica*, vol. 144, p. 110477, 2022.
[6] D. Lefebvre, "Fault diagnosis and prognosis with partially observed Petri nets," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 10, pp. 1413–1424, Oct. 2014.
[7] R. Ammour, E. Leclercq, E. Sanlaville, and D. Lefebvre, "Fault prognosis of timed stochastic discrete event systems with bounded estimation error," *Automatica*, vol. 82, pp. 35–41, 2017.
[8] X. Yin, "Verification of prognosability for labeled Petri nets," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1738–1744, Jun. 2018.
[9] D. You, S. Wang, and C. Seatzu, "Verification of fault-predictability in labeled Petri nets using predictor graphs," *IEEE Trans. Autom. Control*, vol. 64, no. 10, pp. 4353–4360, Oct. 2019.
[10] N. Ran, J. Hao, and C. Seatzu, "Prognosability analysis and enforcement of bounded labeled Petri nets," *IEEE Trans. Autom. Control*, vol. 67, no. 10, pp. 5541–5547, Oct. 2022.
[11] T. Jéron, H. Marchand, S. Genc, and S. Lafortune, "Predictability of sequence patterns in discrete event systems," in *Proc. 17th IFAC World Congr.*, 2008, pp. 537–543.
[12] L. Ye and P. Dague, "A general algorithm for pattern diagnosability of distributed discrete event systems," in *Proc. 24th IEEE Int. Conf. Tools with Artificial Intell.*, pp. 130–137, 2012.
[13] H. E. Gougam, Y. Pencolé, and A. Subias, "Diagnosability analysis of patterns on bounded labeled prioritized Petri nets," *Discrete Event Dynamic Syst.*, vol. 27, no. 1, 143–180, 2017.
[14] D. Lefebvre and C. N. Hadjicostis, "Diagnosability of fault patterns with labeled stochastic Petri nets," *Inform. Sci.*, vol. 593, pp. 341–363, 2022.
[15] E. Lubat, C. Coquand, Y. Pencolé, and A. Subias, "Diagnosability and predictability of pattern in labelled Petri nets," in *Proc. 33rd Int. Workshop on Principle of Diagnosis–DX*, 2022.
[16] A. Boussif, M. Ghazel, and J. C. Basilio, "Intermittent fault diagnosability of discrete event systems: an overview of automaton-based approaches," *Discrete Event Dynamic Syst.*, vol. 31, pp. 59–102, 2021.
[17] S. B. Jiang and R. Kumar, "Failure diagnosis of discrete-event systems with linear-time temporal logic specifications." *IEEE Trans. Autom. Control*, vol. 49, no. 6, pp. 934–945, Jun. 2004.
[18] E. Lefaucheux, A. Giua, and C. Seatzu, "Basis coverability graph for partially observable Petri nets with application to diagnosability analysis," in *Proc. 39th Int. Conf. Applicat. and Theory of Petri Nets and Concurrency*, 2018, pp. 164–183.
[19] T. Murata, "Petri nets: Properties, analysis and applications," *Proc. IEEE*, vol. 77, no. 4, pp. 541–580, Apr. 1989.
[20] D. Corona, A. Giua, and C. Seatzu, "Marking estimation of Petri nets with silent transitions," *IEEE Trans. Autom. Control*, vol. 52, no. 9, pp. 1695–1699, 2007.
[21] B. Bérard, S. Haar, S. Schmitz, and S. Schwoon, "The complexity of diagnosability and opacity verification for Petri nets," *Fundamenta Informaticae*, vol. 161, no. 4, pp. 317–349, 2018.
[22] [Online]. Available: https://github.com/congxuya/supplementary-material-FP
[23] M. P. Cabasino, A. Giua, M. Pocci, and C. Seatzu, "Discrete event diagnosis using labeled Petri nets. An application to manufacturing systems," *Control Eng. Practice*, vol. 19, no. 9, pp. 989–1001, 2011.
[24] R. Tarjan. "Depth-first search and linear graph algorithms," *SIAM J. Cmputing*, vol. 1, no. 2, pp. 146–160, 1972.
[25] M. P. Cabasino, A. Giua, S. Lafortune, and C. Seatzu, "A new approach for diagnosability analysis of Petri nets using verifier nets," *IEEE Trans. Autom. Control*, vol. 57, no. 12, pp. 3104–3117, Dec. 2012.
[26] C. Rackoff, "The covering and boundedness problems for vector addition systems," *Theoretical Comput. Sci.*, vol. 6, no. 2, pp. 223–231, 1978.

Authorized licensed use limited to: Politecnico di Bari. Downloaded on January 23,2025 at 14:08:03 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.