IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 25, 2017, accepted January 17, 2018, date of publication January 30, 2018, date of current version March 12, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2796640

Fault Diagnosis in Partially Observed Petri Nets Using Redundancies

LI YIN[1], ZHIWU LI[1,2], (Fellow, IEEE), NAIQI WU[1,3], (Senior Member, IEEE), SHOUGUANG WANG[4], (Senior Member, IEEE), AND TING QU[5]

[1]Institute of Systems Engineering, Macau University of Science and Technology, Taipa 999078, Macau
[2]School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China
[3]School of Electro-Mechanical Engineering, Guangdong University of Technology, Guangzhou 510006, China
[4]School of Information and Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310000, China
[5]School of Electrical and Information Engineering, Jinan University (Zhuhai Campus), Zhuhai 519070, China

Corresponding authors: Zhiwu Li (zwli@must.edu.mo) and Naiqi Wu (nqwu@must.edu.mo)

This work was supported in part by the Science and Technology Development Fund (FDCT), MSAR, under Grants 078/2015/A3 and 106/2016/A3, and in part by the National Natural Science Foundation of China under Grants U1401240 and 51475095.

ABSTRACT This paper is devoted to the development of an approach to the diagnosability of a system described in the framework of partially observed Petri nets (POPNs) such that the developed fault diagnosis technique can be widely applicable to systems with mutable initial states and partial observations. Existing studies show that the diagnosability of a discrete event system (DES) can be improved by suitable sensor selections or redundancies. This paper proposes a redundancy-building method for a POPN with a certain sensor selection such that no matter how the POPN is initially marked, it achieves maximally structural diagnosability, i.e., the diagnosability of a system cannot be further improved based on the given sensor selection and knowledge of the plant model, which is critical and fundamental in fault recovery capabilities for operating large and complex DESs. To make the proposed method practically applicable, we do not require prior knowledge of faults or special structure of a system, instead we model faults as abnormal events occurring on transitions or places in the plant but not special transitions. Necessary and sufficient conditions for maximally structural diagnosability of a system are established. Redundancies (externally observable places) that guarantee behavior permissiveness and maximally structural diagnosability are built by solving integer linear programming problems.

INDEX TERMS Discrete event system, Petri net, fault diagnosis, diagnosability.

I. INTRODUCTION

Discrete event systems (DESs) are a class of man-made systems whose evolution is driven by the occurrences of events and described by discrete state spaces [1]. Much attention has been paid to the study on discrete event systems from researchers and practitioners using Petri nets and finite state machines, including system modeling [3] and identification [19], scheduling [6], [9], [10], [13], [14], [17], deadlock analysis [11], recovery [12] and control [2], [4], [5], [18], opacity [8], and general supervisory control problems [7], [15], [16], [20], [21]. Fault diagnosis has become an important issue since DESs are inevitably fault-prone as their complexity increases. The notion of diagnosability of DESs is first introduced by Sampath *et al.* in [22], [23], where a well-designed finite state machine (FSM) is used as a tool to detect and identify faults occurring in a DES modeled by an automaton. Petri nets, one of several mathematical modeling languages of DESs, become increasingly popular in modeling and control of DESs due to their graphical representation and advantages in designing plant controllers or supervisors [24], [25].

Generally, the methods on fault diagnosis in the framework of Petri nets usually fall into three categories based on state space analysis, structural information, and algebraic techniques [37], respectively. The methods by state space analysis follow the idea of using automata to describe the behavior of a plant [22] and [23]. The work in [26] implements fault diagnosers by linear approximations of the coverability trees that consist of marking variations obtained from the observable places only. In [27], Cabasino *et al.* study fault detection through the basis reachability graph of a system modeled by a Petri net with unobservable transitions. Faults can also be diagnosed based on both marking variations and the observations of transition firings [28]. The investigation in [31] and [32] reports the necessary and sufficient conditions for diagnosability and k-diagnosability in a labeled

bounded Petri net via integer linear programming. In [33], necessary and sufficient conditions for diagnosability and k-diagnosability for both bounded and unbounded Petri nets are established. The approaches utilizing structural information are developed by event detectability. Their basic idea is to distinguish the firing of any pair of transitions by a suitable sensor selection and infer the firing of some particular failure transitions. The concept of minimum observable places needed for a given Petri net is introduced in [34], aiming to build a minimal diagnoser to identify the firing of fault transitions on-line. Ru *et al.* [38] conduct a similar study and show that the problem of an optimal sensor selection is NP-complete in DESs modeled by partially observable Petri nets. The third line of fault diagnosis is based on coding theory [39]–[42], where faults are modeled as abnormal events occurring on the original transitions or places in a plant model. By this type of methods, no assumption is made on how faults influence the states and no priori knowledge of faults is needed when a DES model is built. Prock [43] uses place invariants to detect faults based on the fact that some parameters or invariant laws of a DES are maintained if no fault occurs. By employing algebraic decoding techniques, the work in [39] shows that faults can be detected and identified by an incorporating redundancy.

Up to now, although many methods for different fault diagnosis problems have been developed, there are still some issues to be addressed in this field. Among them, the following two are the main concerns. First, the existing methods involve a repeated computation process if the initial state changes, which usually leads to prohibitive costs. For instance, the methods involving reachability graph analysis suffer from extraordinary complexity and are not reusable for different initial states, which impedes their applications in many practical cases such as flexible manufacturing systems. Second, the diagnosability of faults greatly relies on sensor selections. Existing studies usually assume that every node (a place or a transition) of a system is ideally observable by employing a sensor. However, some places or transitions are not able to be measured or monitored by sensors. This implies that, in many cases, the fault diagnosis problem needs to be considered under a given sensor selection. For example, the assumption in [39] that markings are completely observable may not hold. There is the same problem for the state-space-based and structural-information-based methods, where every node of a system is supposed to be observable if a sensor is deployed for it.

This paper proposes a method to diagnose faults for a system whose places and transitions are partially measured or monitored by sensors with mutable initial states. That is to say, the method should be applicable to a partially observed Petri net system under a given sensor selection and be reusable for different initial markings. This is done by building a redundancy for a system to diagnose fault occurrences similar to [39], while the necessary requirement that all places are observable is relaxed. Although Hamming distance and Nearest Neighbor Decoding are used to decide the fired transitions in this paper, different from the work in [35], we focus on building a redundancy to ensure correct identification of the transition firing sequences based on the obtained observations under a given sensor selection, while the work in [35] studies the necessary and sufficient conditions for identifying transition firing sequences and solve the problem by selecting suitable sensors. Given the notion of diagnosability in [22], some faults are not diagnosable by building redundancies under particular sensor selections and initial markings. However, the occurrences of those faults can be determined in particular situations. For that reason, the diagnosability concept is extended to different levels to describe the highest level of diagnosability of the faults that can be achieved. We demonstrate that the redundancy by the proposed approach is minimal (in the sense of the number of added places) and the system achieves maximally structural diagnosability. The main contributions of this work can be summarized as follows:

1) We define simultaneous diagnosability, structural diagnosability, obstinate diagnosability and casual diagnosability. The maximally structural diagnosability that a system can achieve by employing a redundancy is characterized.
2) Necessary and sufficient conditions are provided for diagnosability of a system whose places and transitions are partially measured or monitored with mutable initial states.
3) An approach is developed to build redundancies (added observable places) for a system under a certain sensor selection in the case that an alternative is necessary when some key sensors are absent.
4) An approach is proposed to diagnose faults in a DES without assumptions of acyclicity [29], [30], deadlock-freedom [32] and complete marking observations [40] of a plant. This developed formalism can be widely applied to systems with high robustness requirement such as autopilot, where the initial states are mutable and some faults are unforeseen.

This paper is structured as follows. Section 2 reviews the basics of POPNs. Section 3 formulates the considered problem. The necessary and sufficient conditions for a POPN system that is of maximally structural diagnosability are reported in Section 4. An approach to construct redundancies is elaborated upon in Section 5. Section 6 concludes this paper.

II. PRELIMINARIES

In this section, we outline the basic definitions of partially observable Petri nets (POPNs) [36], fault models [39] and observations.

A. PARTIALLY OBSERVED PETRI NETS

Petri nets are one of the mathematical modeling languages, providing elegant formalism for describing a DES and its behavior. Partially observed Petri nets are a special type of Petri nets whose places and transitions are partially observable only.

A net structure N of a POPN is a four-tuple $N = (P, T, F, W)$, where $P = \{p_1, p_2, \ldots, p_n\}$ is a finite and non-empty set of places graphically represented by circles; $T = \{t_1, t_2, \ldots, t_m\}$ is a finite and non-empty set of transitions visualized by rectangles with $P \cap T = \emptyset$; $F \subseteq (P \times T) \cup (T \times P)$ is called a flow relation of the net, represented by directed arcs from places to transitions or from transitions to places; $W : (P \times T) \cup (T \times P) \to \mathbb{N} = \{0, 1, 2, \ldots\}$ is a mapping that assigns a weight to an arc: $W(x, y) > 0$ if $(x, y) \in F$, and $W(x, y) = 0$, otherwise. Let $x \in P \cup T$ be a transition or place in $N = (P, T, F, W)$. The preset of x, denoted by ${}^\bullet x$, is defined as ${}^\bullet x = \{y \in P \cup T \mid (y, x) \in F\}$. The postset of x, denoted by $x^\bullet$, is defined as $x^\bullet = \{y \in P \cup T \mid (x, y) \in F\}$. A POPN is pure if $\forall p \in P$, ${}^\bullet p \cap p^\bullet = \emptyset$. This paper considers pure POPNs only and we assume $\forall t \in T$, ${}^\bullet t \neq \emptyset$.

A marking of a Petri net is a function $M : P \to \mathbb{N}^n$. $M(p)$ denotes the number of tokens in place p. In this paper, n and m represent the number of places and transitions in a net structure, respectively. Tokens in a place p are represented by black dots pictorially or by $M(p)$ numerically. (N, M_0) is called a Petri net system or a Petri net for the sake of simplicity in the case of no confusion. Since a marking of a Petri net can be thought of as an element of the free vector space over the whole finite place set P with respect to $\mathbb{N}^n$, it is usually described as a (column) vector for algebraic manipulation. At marking M, a transition t is enabled if $\forall p \in {}^\bullet t$, $M(p) \geqslant W(p, t)$ or t is disabled otherwise. We use $En(N, M)$ to denote the set of transitions that are enabled at M. If a transition t is enabled at marking M, t can fire. A new marking M' is reached after t fires at M with $M'(p) = M(p) - W(p, t) + W(t, p)$, $\forall p \in P$, which is denoted by $M[t\rangle M'$.

Marking M'' is said to be reachable from M if there exist a transition sequence $\sigma = t_0 t_1 \ldots t_k \in T^*$ and markings M_1, M_2, …, M_k such that $M[t_0\rangle M_1[t_1\rangle M_2 \ldots M_k[t_k\rangle M''$ holds. In this case, σ is said to be a feasible transition sequence at M, which is denoted by $M[\sigma\rangle M''$ or simply by $M[\sigma\rangle$ if the reachable marking M'' after firing σ is of no interest. An m-dimensional vector $\vec{\sigma}$ is called the Parikh vector of the transition sequence σ if its i-th entry is the number of occurrences of t_i in σ. We use languages to describe the behavior of a POPN.

Definition 1: The language generated by a net system (N, M_0) with $N = (P, T, F, W)$, denoted by $\mathcal{L}(N, M_0)$, is a set of feasible transition sequences at M_0, i.e., $\mathcal{L}(N, M_0) = \{\sigma \mid \sigma \in T^*, M_0[\sigma\rangle\}$.

A net structure $N = (P, T, F, W)$ can be sufficiently represented by two $n \times m$ nonnegative integer matrices B^- and B^+ that are called the input and output matrices of N, respectively. The output matrix $B^+ = [b_{ij}^+]$ is used to describe the flow relation $T \times P$, where $b_{ij}^+ = W(t_j, p_i)$ denotes the weight of the arc from t_j to p_i. The input matrix $B^- = [b_{ij}^-]$ describes the flow relation $P \times T$, where $b_{ij}^- = W(p_i, t_j)$ denotes the weight of the arc from p_i to t_j. If N is pure, N can be completely represented by an incidence matrix $B = B^+ - B^-$. Then, the state evolution of a Petri net can be represented as

$$M_{k+1} = M_k + (B^+ - B^-)\vec{\sigma}_k = M_k + B\vec{\sigma}_k \tag{1}$$

where $\vec{\sigma}_k$ is restricted to have exactly one non-zero entry with value 1. If the j-th entry of $\vec{\sigma}_k$ is 1, then t_j fires. Accordingly, we use vector $\vec{t}_j = [0 \ldots 1 \ldots 0]^\tau$ with its j-th entry being 1 to denote the firing of t_j. Thus, for each k, σ_k represents the firing of a transition.

Remark 1: This restriction ensures that labels of transitions in a POPN (to be defined) can be observed sequentially by restricting the maximal number of transition firings at each time epoch. As done in the literature, this requirement is common for the practical cases such that the fault-diagnosis scheme developed underlying this restriction can be applied.

The places in a POPN can be categorized into two classes: observable and unobservable ones, whose sets are denoted by P_o and P_u, respectively. Let $r = |P_o|$. A place configuration $V \in \{0, 1\}^{r \times n}$ is used to describe the projection of a marking M over the set of observable places P_o, where $p \in P_o$ if there is a place sensor (e.g., a counter) associated with p and the sensor can indicate the number of tokens in p, otherwise $p \in P_u$, i.e., p is unobservable. Due to unobservable places, only partial entries of a marking are measured or observed. For any marking M, the observable entries (observed marking) can be defined as $M_o = VM$.

Analogously, the transitions in a POPN can be categorized into two classes: observable and unobservable ones, whose sets are denoted by T_o and T_u, respectively. Let Σ be a finite set of labels. A transition t is said to be observable if there is a sensor associated with t and a label $\omega \in \Sigma$ can be observed if t fires. A transition labeling configuration $L : T \to \Sigma \cup \{\varepsilon\}$ is a function that assigns a label $\omega \in \Sigma$ to an observable transition or ε to unobservable transitions, where ε indicates that no information can be observed, i.e., $L(t) = \omega \in \Sigma$ if $t \in T_o$, otherwise $L(t) = \varepsilon$. Thus, POPNs are a special type of Petri nets and can be defined as follows.

Definition 2: A partially observed Petri net (POPN) is a four-tuple $Q = (N, M_0, V, L)$, where

- (N, M_0) is a Petri net system, where $N = (P, T, F, W)$ is a Petri net structure with n places and m transitions and M_0 is the initial marking,
- $V \in \{0, 1\}^{r \times n}$ is a place sensor configuration, and
- $L : T \to \Sigma \cup \{\varepsilon\}$ is a transition labeling configuration.

When building a POPN for a system, the place sensor configuration V and transition labeling configuration L are determined by the physical characteristics of the system.

Example 1: For the POPN Q_1 shown in Fig. 1, there are four places and five transitions. Its incidence matrix B and place sensor configuration V are

$$B = \begin{pmatrix} -1 & 1 & -1 & 0 & 0 \\ 0 & -2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & -1 & -2 \end{pmatrix}; \quad V = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

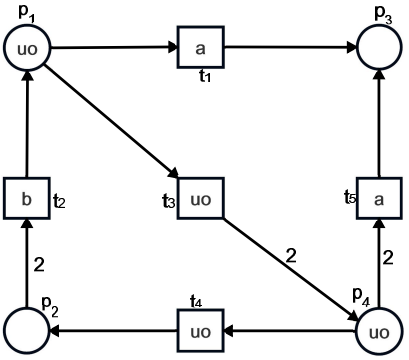

FIGURE 1. Partially observed Petri net Q_1.

A label a can be observed when t_1 or t_5 fires, b can be observed when t_2 fires, and no label can be observed when t_3 or t_4 fires, i.e., $P_o = \{p_2, p_3\}$, $P_u = \{p_1, p_4\}$, $L(t_1) = L(t_5) = a$, $L(t_2) = b$ and $L(t_3) = L(t_4) = \varepsilon$. Suppose that Q_1 is initially marked with $[4, 1, 0, 2]^\tau$. The observed marking of Q_1 at the initial state is $[1, 0]^\tau$. After t_1 fires, it is $[1, 1]^\tau$.

B. FAULT MODELS

The POPN in Definition 2 can model a DES for the ideal case, but cannot describe some unexpected events that may occur in practice. Faults are such unexpected events that cause abnormal state evolutions in a system. In this paper, two kinds of atomic faults are considered by following the development in [39] such that a fault in real world can be abstracted into an atomic fault or the combination of them.

1) A *transition fault* models a fault that an event occurs without consuming (depositing) expected tokens from (to) places associated with the transition. Precondition and postcondition faults are used to represent different cases. In a Petri net system, a precondition fault is an unexpected event that a transition t fires without consuming any token from the places in ${}^\bullet t$ and a postcondition fault is the one that a transition t fires without depositing any token to the places in $t^\bullet$. Postcondition and precondition faults associated with t are denoted by f_t^- and f_t^+, respectively. If a precondition fault and a postcondition fault associated with the same transition occur at the same time, their effects would offset each other and the system would run as if there is no fault. Thus, this paper does not consider such a case.
2) A *place fault* is an unexpected change of the tokens in a single place only. By Eq. (1), a place fault at time epoch k results in M_{k+1} incorrectly, which models sensor errors and memory failures. We use $f(p_i)$ to denote a place fault associated with p_i, whose occurrence is accompanied by the firing of a transition. A place fault affects the place itself only and is independent of other place faults. Note that, by the above fault models, no assumption is made on how faults influence system states. Thus, a fault diagnosis method based on such models requires no priori knowledge of faults such that it is possible to identify unforeseen faults.

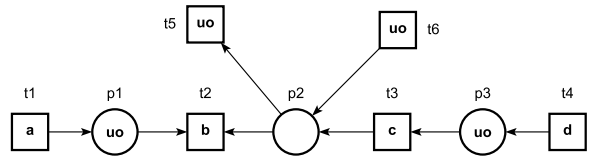

FIGURE 2. A simplified parking assist system.

The above defined transition and place faults are thought of as atomic faults whose occurrences are assumed to be independent, i.e., the occurrence of a fault is not affected by others. A system can be subject to an atomic fault or a combination of atomic faults. The POPN shown in Fig. 2 is a simplified parking assist system. Transitions t_1 and t_4 denote the order "go backward" and "go forward", t_2 (t_3) indicates that the engine executes the order "go backward" ("go forward"), and t_5 (t_6) represents that the obstacles behind the car go forward (backward). The marked place p_1 means that a "go back" order is received by the processor, and p_3 implies that a "go forward" order is received. The tokens in p_2 show the distance between the car and the obstacles. The faults of the system can be modeled by atomic faults. For example, the engine obtains an order of "go back" and acts accordingly, but the car does not move due to slip. This failure can be represented by $f_{t_1}^-$. If the distance sensor returns wrong distance data, it can be denoted by a place fault associated with p_2. The aim of this work is to identify the occurrences of atomic faults. At each time epoch, a transition can fire normally, and faults (precondition, postcondition, and place faults) can also occur. Then, an event-set Ω that can concurrently occur at a time epoch is a proper subset of $\{t, f_t^+, f_t^- | t \in T\} \cup \{f(p) | p \in P\}$. Specifically, $t \in \Omega$ means that t fires at a time epoch, $f_t^+ \in \Omega$ ($f_t^- \in \Omega$) indicates that a postcondition (precondition) fault associated with t occurs, and $f(p) \in \Omega$ if the number of tokens in p increases or decreases unexpectedly when t fires. According to the fault model, an event-set Ω can be characterized by its characteristic vector, denoted by $\vec{\Omega} = (\vec{\sigma}, \vec{\upsilon^+}, \vec{\upsilon^-}, \vec{e}^n)$, satisfying

1) $\vec{\sigma} = \vec{t}$ if $t \in \Omega$;
2) $\vec{\upsilon^+} = \vec{t}$ if $f_t^+ \in \Omega$, otherwise $\vec{\upsilon^+} = \mathbf{0}^\tau$;
3) $\vec{\upsilon^-} = \vec{t}$ if $f_t^- \in \Omega$, otherwise $\vec{\upsilon^-} = \mathbf{0}^\tau$;
4) $\vec{e}^n \in \mathbb{Z}^n$, where $\mathbb{Z}$ is the set of integers. $\vec{e}^n(i)$ represents the number of tokens increased (positive) or decreased (negative) by a place fault associated with p_i.
5) $\vec{\upsilon^+}^\tau \times \vec{\upsilon^-} = 0$ implies that a transition is not subject to both postcondition and precondition faults at the same time.

An event-set Ω with $\vec{\Omega} = (\sigma, \vec{\upsilon^+}, \vec{\upsilon^-}, \vec{e}^n)$ is feasible at marking M if $M' = M + B\vec{\sigma} + B^-\vec{\upsilon^+} - B^+\vec{\upsilon^-} + \vec{e}^n \geqslant \mathbf{0}^\tau$.[1] Similarly, $M[\Omega\rangle M'$ denotes that Ω is feasible at M and M' is reached after its occurrence. Suppose that $(\vec{\sigma_k}, \vec{\upsilon_{k^+}}, \vec{\upsilon_{k^-}}, \vec{e_k^n})$

[1] In this paper, a disabled transition may become enabled due to some place faults. That is to say, event-set Ω being feasible at a marking M does not require that transition $t \in \Omega$ should be enabled at M.

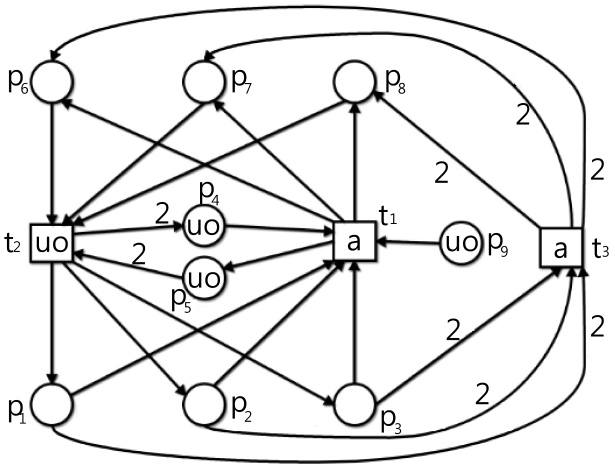

FIGURE 3. Partially observed Petri net Q_2.

is the characteristic vector of an event-set occurring at time epoch k in a system Q. It evolves as follows:

$$M_{k+1} = M_k + B\vec{\sigma}_k + B^-\vec{\upsilon}_{k^+} - B^+\vec{\upsilon}_{k^-} + \vec{e}^n_k. \tag{2}$$

Example 2: In POPN Q_2 shown in Fig. 3, $P_o = \{p_1, p_2, p_3, p_6, p_7, p_8\}$, $L(t_1) = L(t_3) = a$ and $L(t_2) = \varepsilon$. The transposed matrix B of the incidence matrix of Q_2 is

$$B^\tau = \begin{pmatrix} -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 2 & -2 & -1 & -1 & -1 & 0 \\ -2 & -2 & -2 & 0 & 0 & 2 & 2 & 2 & 0 \end{pmatrix}$$

Suppose that t_1 fires with a precondition fault and a place fault increases the number of tokens in p_1 by one at time epoch k, i.e., the event-set Ω_k can be denoted by $(\vec{\sigma}_k, \vec{\upsilon}_{k^+}, \vec{\upsilon}_{k^-}, \vec{e}^n_k)$ where $\vec{\upsilon}_{k^+} = [1,0,0]^\tau$, $\vec{\upsilon}_{k^-} = [0,0,0]^\tau$, $\vec{e}^n_k = [1,0,0,0,0,0,0,0,0]^\tau$ and $\vec{\sigma}_k = [1,0,0]^\tau$. If the current marking of Q_2 is $M_k = [2,2,2,1,1,0,0,0,1]^\tau$ and Ω_k occurs, then Q_2 evolves to $M_{k+1} = [3,2,2,1,2,1,1,1,1]^\tau$.

Given a POPN system $Q = (N, M_0, V, L)$, if an event-set sequence $\alpha = \Omega_0\Omega_1 \ldots \Omega_k$ occurs from marking M_0 such that $M_0[\Omega_0\rangle M_1 \ldots [\Omega_k\rangle M_{k+1}$ holds, α is said to be feasible from M_0. For an event-set sequence $\alpha = \Omega_1\Omega_2 \ldots \Omega_k$ with $\vec{\Omega}_i = (\vec{\sigma}_i, \vec{\upsilon}_{i^+}, \vec{\upsilon}_{i^-}, \vec{e}^n_i)$ $(i \in \{1, 2, \ldots, k\})$, $\mathcal{L}(\alpha)$ is used to denote the corresponding transition sequence $\sigma_1\sigma_2 \ldots \sigma_k$.

Suppose that a transition t fires twice sequentially in a system and a transition fault associated with t occurs. No matter the fault occurs when t fires for the first or second time, the state of the system is the same after the normal firing of t and the occurrence of its fault. However, faults occur in different time epochs may have different physical meanings. Hence, faults associated with a same transition or place but occurring at different time epochs are considered to be different. To specify what we focus on in this paper, the following assumptions are made.

Assumption 1: For each time epoch, at most η place faults can occur. Suppose that $(\vec{\sigma}_k, \vec{\upsilon}_{k^+}, \vec{\upsilon}_{k^-}, \vec{e}^n_k)$ is the characterisitic vector of an event-set that occurs at time epoch k. For any $k \in \mathbb{N}$, $\vec{e}^n_k$ is restricted to have at most η non-zero entries.

This assumption, as also made in [40], guarantees that the redundancy proposed in the following section can be constructed efficiently. Since each fault occurs with small probability, this assumption does not weaken the application of the method developed in this paper. Note that the assumption does not present a restriction on how many tokens can be changed by a place fault except that the number of tokens in a place should be nonnegative. Thus, the unexpected change of tokens in a single place at a time epoch is regarded as the consequence of one place fault. That is to say, for a place, at most one place fault associated with it occurs per time epoch.

Assumption 2: Deadlocks in a system (no transition is enabled) are assumed to occur if the system output does not change for a time that is long enough.

Any enabled transition will eventually fire unless it is disabled. It is reasonable to conclude that a system is deadlocked if there is no output for a time long enough in practice. In [23], a system is supposed to be live after the occurrence of faults and there is no arbitrarily long sequence of unobservable transitions, which is difficult to verify.

C. OBSERVATIONS IN PARTIALLY OBSERVED PETRI NETS

In a partially observed Petri net, one can observe transition labels from transition sensors and token change in observable places.

Definition 3: Let $Q = (N, M_0, V, L)$ be a POPN and Ω be a feasible event-set at a reachable marking M such that $M[\Omega\rangle M'$. 1) The observed marking variation from M to M' is expressed as $\Delta M_o = M'_o - M_o = VM' - VM$, where M_o (M'_o) is the observed marking of M (M'); 2) The observed label is $l \in \Sigma \cup \{\varepsilon\}$ with $l = L(t)$; 3) The observation function is a mapping $\Psi : \mathbb{E} \to \mathbb{N}^r \times (\Sigma \cup \{\varepsilon\})$ with $\Psi(\Omega) = (\Delta M_o, l)$, where $\mathbb{E}$ is the set of event-sets and r is the number of observable places.

Example 3: Take POPN Q_2 shown in Fig. 3 as an instance. Suppose that there is an event-set Ω_k with $\vec{\Omega}_k = (\vec{\sigma}_k, \vec{\upsilon}_{k^+}, \vec{\upsilon}_{k^-}, \vec{e}^n_k)$, where $\vec{\upsilon}_{k^+} = [1,0,0]^\tau$, $\vec{\upsilon}_{k^-} = [0,0,0]^\tau$, $\vec{e}^n_k = [1,0,0,0,0,0,0,0,0]^\tau$ and $\vec{\sigma}_k = [1,0,0]^\tau$. If Ω_k occurs at $M_k = [2,2,2,1,1,0,0,0,1]^\tau$ such that $M_{k+1} = [3,2,2,1,2,1,1,1,1]^\tau$ is reached, we have $\Delta M_o = VM_{k+1} - VM_k = [1,0,0,1,1,1]^\tau$ and the observed label is a. Thus, the observation $\Psi(\Omega_k) = ([1,0,0,1,1,1]^\tau, a)$.

Suppose that a feasible event-set Ω with $t \in \Omega$ occurs. By Eq. (2), the variation on the observed marking of Q is computed by

$$\begin{aligned} \Delta M_o &= \begin{cases} V(B^+\vec{t} + \vec{e}^n) \\ V(-B^-\vec{t} + \vec{e}^n) \\ V(B\vec{t} + \vec{e}^n) \end{cases} \\ &= \begin{cases} \theta_t^+ + \vec{e}^r, & f_t^+ \in \Omega \\ -\theta_t^- + \vec{e}^r, & f_t^- \in \Omega \\ \theta_t + \vec{e}^r, & \{f_t^+, f_t^-\} \cap \Omega = \emptyset \end{cases} \end{aligned} \tag{3}$$

where $\vec{t}$ is the Parikh vector of t, $\vec{e}^n$ represents the place faults associated with all the n places, $\vec{e}^r = V\vec{e}^n$ indicates the place

faults associated with observable places only, r is the number of observable places and vectors θ_t, θ_t^+, and θ_t^- denote $VB\vec{t}$, $VB^+\vec{t}$, and $VB^-\vec{t}$, respectively. For instance, in POPN Q_2 shown in Fig. 3, $r = 6$, $\theta_{t_1} = [-1, -1, -1, 1, 1, 1]^\tau$, $\theta_{t_1^-} = [1, 1, 1, 0, 0, 0]^\tau$ and $\theta_{t_1^+} = [0, 0, 0, 1, 1, 1]^\tau$.

Assumption 3: The observations are obtained from transition and place sensors without delay.

This assumption is justified due to the fact that the known regular delays can be omitted. Under Assumption 3, the observation function can be extended to event-set sequences. An observation sequence is generated by sequentially concatenating the observations at time epochs.

Definition 4: Given a POPN system $Q = (N, M_0, V, L)$, suppose that a sequence of event-sets $\alpha = \Omega_0\Omega_1 \dots \Omega_k$ occurs from marking M_0 and the system reaches marking M_{k+1}, i.e., $M_0[\Omega_0\rangle M_1 \dots [\Omega_k\rangle M_{k+1}$. The observation sequence ψ due to α is expressed as

$$\begin{aligned}\psi &= \Psi(\alpha) = \Psi(\Omega_0)\Psi(\Omega_1)\dots\Psi(\Omega_k)\\ &= (\Delta M_o^0, l_0)(\Delta M_o^1, l_1)\dots(\Delta M_o^k, l_k). \end{aligned} \tag{4}$$

If there is no output after time epoch k, by Assumption 2, it can be inferred that M_{k+1} is a deadlock state. The observation sequence is denoted as

$$\begin{aligned}\psi &= \Psi(\Omega_0)\Psi(\Omega_1)\dots\Psi(\Omega_k)\\ &= (\Delta M_o^0, l_0)(\Delta M_o^1, l_1)\dots(\Delta M_o^k, l_k)\perp. \end{aligned} \tag{5}$$

where $\perp$ is the symbol denoting a deadlock.

If an event-set Ω occurs, there are three possible cases for $\Psi(\Omega) = (\Delta M_o, l)$. Case 1: an observable transition fires and the observed marking evolves. In this case, we are informed that a transition has fired. Case 2: an unobservable transition fires and the observed marking evolves. By Assumption 3, the firing of an unobservable transition can be inferred by $\Psi(\Omega)$, i.e., if the state of observable places evolves without observing a label, an unobservable transition fires necessarily. Case 3: an unobservable transition fires without any observed marking evolution, i.e., $\Delta M_o = \mathbf{0}^\tau$ and $L(t) = \varepsilon$, no information is observed, or an empty observation $(\mathbf{0}^\tau, \varepsilon)$ is obtained. Notice that, in this case, the occurrence of event-set Ω does not influence the sequential observations. That is to say, the observation obtained at one time epoch is concerned with a single event-set only.

III. PROBLEM FORMULATION

To formulate the considered problem, we extend the concept of diagnosability in [22] in the context of automata to the following four categories: simultaneous diagnosability, structural diagnosability, obstinate diagnosability and casual diagnosability.

Definition 5: Given a POPN $Q = (N, M_0, V, L)$, let $x \in P \cup T$ be a node of Q, f_x denote a fault associated with x and Ω be an event-set containing f_x. Node x is said to be *simultaneously diagnosable* if $\Psi(\Omega) \neq (\mathbf{0}^\tau, \varepsilon)$ and for any event-set Ω' satisfying $\Psi(\Omega) = \Psi(\Omega'), f_x \in \Omega'$.

Simultaneous diagnosability requires that the fault occurrences should be diagnosed without delay, while the diagnosability presented in [22] and [23] allows a finite delay, which implies that the condition for simultaneous diagnosability is much more strict. Although the notion of simultaneous diagnosability is not explicitly and formally formulated in [39] and [40], it can be realized by the coding approaches under the assumption that all places are observable in the framework of label-free Petri nets. Note that, in a POPN model used in this paper, only a part of places is observable. Next, we show that structural diagnosability of a fault with a finite delay in the framework of POPNs is equivalent to the simultaneous diagnosability, which is independent of initial markings.

Definition 6: Let $x \in P \cup T$ be a node of $Q = (N, M_0, V, L)$ and f_x a fault associated with x. Node x is said to be *structurally diagnosable* if there exists a finite nonnegative integer k such that for arbitrary two event-set sequences $\alpha = \Omega_0\Omega_1 \dots \Omega_i \dots \Omega_{i+k}$ and $\alpha' = \Omega'_0\Omega'_1 \dots \Omega'_i \dots \Omega'_{i+k}$ and any initial marking M_0 from which α and α' are feasible, $f_x \in \Omega_i$ and $\Psi(\alpha) = \Psi(\alpha')$ imply $f_x \in \Omega'_i$.

Proposition 1: Let $x \in P \cup T$ be a node of a POPN $Q = (N, M_0, V, L)$. Then, x is structurally diagnosable if and only if it is simultaneously diagnosable.

Proof: ($\Rightarrow$) It is done by contradiction. Suppose that x is structurally diagnosable but not simultaneously diagnosable. Let $\alpha = \Omega_0\Omega_1 \dots \Omega_i \dots \Omega_{i+k}$ be an event-set sequence that is feasible from M_0 and $f_x \in \Omega_i$, where f_x is a fault associated with x. The structural diagnosability of x implies that there exists a finite nonnegative integer k such that for any event-set sequence $\alpha' = \Omega'_0\Omega'_1 \dots \Omega'_i \dots \Omega'_{i+k}$ satisfying $M_0[\alpha'\rangle$, $f_x \in \Omega'_i$ is true if $\Psi(\alpha) = \Psi(\alpha')$. There are two cases: $k > 0$ and $k = 0$.

If $k > 0$, we split α into α_1 and α_2 with $\alpha_1 = \Omega_0\Omega_1 \dots \Omega_i$ and $\alpha_2 = \Omega_{i+1} \dots \Omega_{i+k}$. Let $\alpha'_1 = \Omega'_0\Omega'_1 \dots \Omega'_i$ be an event-set sequence satisfying $f_x \notin \Omega'_i$ and $\Psi(\alpha'_1) = \Psi(\alpha_1)$. Since x is structurally diagnosable and $k > 0$, event-set sequence α'_1 exists such that $M_0[\alpha'_1\rangle M'$, while no event-set sequence $\alpha'_2 = \Omega'_{i+1} \dots \Omega'_{i+k}$ satisfies $M'[\alpha'_2\rangle$ and $\Psi(\alpha'_2) = \Psi(\alpha_2)$. That is to say, no event-set sequence α'_2 with $\Psi(\alpha_2) = \Psi(\alpha'_2)$ is feasible from M' due to the absence of tokens in certain places. Assume that α'_2 is infeasible from marking M' owing to the fact that β_1 tokens in a place p are consumed if α'_2 occurs while there are only β_2 tokens in p with $\beta_2 < \beta_1$. However, by the definition of structural diagnosability, x is also structurally diagnosable if the POPN is initially marked with M'_0 such that $M'_0(p') = M_0(p')$, $p' \in P$, $p' \neq p$ and $M'_0(p) = M_0(p) + \beta_1$. With initial marking M'_0, there exists α'_2 satisfying $\Psi(\alpha'_2) = \Psi(\alpha_2)$ such that $M''[\alpha'_2\rangle$, where $M'' = M' - M_0 + M'_0$. This implies that there exists an event-set sequence α' such that $M_0[\alpha'\rangle, f_x \notin \Omega'_i$ and $\Psi(\alpha) = \Psi(\alpha')$, which contradicts that x is structurally diagnosable.

If $k = 0$, let $\alpha' = \Omega_0\Omega_1 \dots \Omega_{i-1}\Omega'_i$, where Ω'_i is an event-set satisfying $f_x \notin \Omega'_i$. Since x is structurally diagnosable, we have $\Psi(\alpha) \neq \Psi(\alpha')$ if $f_x \in \Omega_i$. Consider that, from the initial time epoch to $k-1$, α and α' are the same. We have $\Psi(\Omega_i) \neq \Psi(\Omega'_i)$ and $\Psi(\Omega_i) \neq (\mathbf{0}^\tau, \varepsilon)$, which implies simultaneous diagnosability and contradicts the assumption that x

is not simultaneously diagnosable. Then, it can be concluded that x is structurally diagnosable only if it is simultaneously diagnosable.

($\Leftarrow$) It is obvious by their definitions. ■

Structural diagnosability implies that the occurrence of a fault can be determined necessarily and immediately based on observations. However, under a certain sensor selection, the occurrences of some faults are not able to be decided immediately and necessarily. They are determined if they change the behavior of a system. In this case, they are said to be obstinately diagnosable. In order to formally describe obstinate diagnosability, we present the behavior-disturbed faults first.

Given a POPN $Q = (N, M_0, V, L)$, suppose that $\alpha = \Omega_0\Omega_1 \ldots \Omega_{k-1}$ is an event-set sequence that occurs from the initial time epoch to k, i.e., $\mathcal{L}(\alpha) \in \mathcal{L}(N, M_0)$. The behavior of Q is said to be disturbed at time epoch k if any of following two cases holds: 1) Event-set Ω_k is such an event-set that occurs at time epoch k and event-set sequence $\alpha' = \Omega_0\Omega_1 \ldots \Omega_{k-1}\Omega_k$ satisfies $\mathcal{L}(\alpha') \notin \mathcal{L}(N, M_0)$, and 2) the system is deadlocked at time epoch k, while $\exists s' \neq \varepsilon$ such that $ss' \in \mathcal{L}(N, M_0)$, where $\mathcal{L}(\alpha) = s$. With the above discussion, we can describe behavior-disturbed faults associated with a certain node of a system.

Definition 7: Given a POPN $Q = (N, M_0, V, L)$, $\alpha = \Omega_0\Omega_1 \ldots \Omega_{k-1}$ is an event-set sequence that occurs from M_0, i.e., $M_0[\alpha\rangle M_k$. Let $x \in P \cup T$ be a node of Q and F_x the set of faults associated with x. Suppose that event-set sequence $\alpha' = \Omega'_0\Omega'_1 \ldots \Omega'_{k-1}$ satisfies $M_0[\alpha'\rangle M'_k$ and $\Omega'_i = \{y | y \in \Omega_i, y \notin F_x\}$, $i \in \mathbb{N}_{k-1}$. The faults associated with x in Q with respect to α are said to be behavior-disturbed with respect to event-set sequence α, denoted by $Bd(Q, x, \alpha) = 1$, if 1) the system is deadlocked at M_k while $En(N, M'_k) \neq \emptyset$, or 2) $M_k[\Omega_k\rangle$, $t \in \Omega_k$ and $t \notin En(N, M'_k)$. Otherwise, the faults associated with x are not behavior-disturbed, i.e., $Bd(Q, x, \alpha) = 0$.

There are two cases for faults associated with a node being behavior-disturbed. In Case 1, an enabled transition is disabled by faults and, in Case 2, a disabled transition fires due to the occurrences of faults. The obstinate diagnosability can be defined as follows:

Definition 8: Given a POPN $Q = (N, M_0, V, L)$, let $x \in P \cup T$ be a node of Q. Suppose that α is a feasible event-set sequence from M_0 with $Bd(Q, x, \alpha) = 1$. Node x is *obstinately diagnosable* if for any event-set sequence α' satisfying $M_0[\alpha'\rangle$ and $\Psi(\alpha) = \Psi(\alpha')$, $Bd(Q, x, \alpha') = 1$.

Similarly, we define casual diagnosability.

Definition 9: Given a POPN $Q = (N, M_0, V, L)$, let $x \in P \cup T$ be a node of Q and $Fa \subsetneqq P \cup T$ be a set of nodes of Q. Suppose that α is a feasible event-set sequence from M_0 with $Bd(Q, x, \alpha) = 1$. Node x is *casually diagnosable* if for any event-set sequence α' satisfying $M_0[\alpha'\rangle$ and $\Psi(\alpha) = \Psi(\alpha')$, there exists $y \in Fa$ such that $Bd(Q, y, \alpha') = 1$.

According to the definitions of structural, obstinate and casual diagnosability, we have Property 1 given below immediately.

Property 1: Given a POPN $Q = (N, M_0, V, L)$, let $x \in P \cup T$ be a node of Q.

1) x is obstinately diagnosable if it is structurally diagnosable.
2) x is casually diagnosable if it is obstinately diagnosable.

Given a POPN, the occurrences of faults associated with some nodes cannot be determined due to limited observations. However, a redundancy can make them diagnosable.

Definition 10: A redundant embedding of a POPN $Q = (N, M_0, V, L)$ (with n places and m transitions) is a POPN $Q_r = (N', M'_0, V', L)$ ($n + z$ ($z > 0$) places and m transitions) whose states evolve as

$$M_{k+1} = M_k + \begin{pmatrix} B \\ B_r \end{pmatrix} \vec{\sigma}.$$

and for an arbitrary initial marking M_0 with which Q is initialized, there exists $M_r \in \mathbb{N}^z$ such that $\mathcal{L}(N', M'_0) = \mathcal{L}(N, M_0)$, where

$$M'_0 = \begin{pmatrix} M_0 \\ M_r \end{pmatrix}.$$

The z places, added in Q_r whose incidence matrix is $[B^\tau, B_r^\tau]^\tau$, are called a redundancy. Obviously, the added places are observable.

By Property 1, a transition or a place of a POPN is obstinately diagnosable if it is structurally diagnosable, while the converse is not always true. Thus, the diagnosability of a transition or a place is said to be *improved* if it becomes structurally diagnosable from being obstinately diagnosable by employing a redundancy. For example, if a place p becomes structurally diagnosable by employing redundancy B_1 while it is only obstinately diagnosable by employing redundancy B_2 or without redundancy, we can say that the diagnosability of p is improved by employing B_1. Also, there is a similar relationship between obstinate and casual diagnosability. Later, we prove that all nodes of a POPN defined in this paper can achieve at least casual diagnosability.

Definition 11: Given a POPN $Q = (N, M_0, V, L)$, a node $x \in P \cup T$ is said to be *maximally-structurally diagnosable* if one of the following statements is true:

1) x is structurally diagnosable,
2) x is obstinately diagnosable and structural diagnosability cannot be achieved by employing a redundancy, and
3) x is casually diagnosable and obstinate diagnosability cannot be achieved by employing a redundancy.

Q is said to be *maximally-structurally diagnosable* if each node of Q is maximally-structurally diagnosable.

Based on the above discussion, the fault diagnosis problem addressed in this paper can be stated as follows.

Problem 1: Given a POPN $Q = (N, M_0, V, L)$, find a redundant embedding $Q_r = (N', M'_0, V', L)$ with z observable places being added such that

1) Q_r is maximally-structurally diagnosable;

2) Let Q'_r be another redundant embedding of Q with z' places being added. If Q'_r is also maximally-structurally diagnosable, then $z' \geq z$ holds.

IV. CONDITIONS FOR DIAGNOSABILITY

In this section, we establish the diagnosability conditions of different nodes in a POPN.

A. TRANSITION FAULTS

We start with faults associated with transitions. We employ Hamming distance and Nearest Neighbor Decoding (NND) [47] to derive the necessary and sufficient conditions for diagnosability of different nodes in a POPN. The Hamming distance $d_H(x, y)$ betweens two vectors $x, y \in F^n$ (F is a finite field) is defined as the number of coefficients in which they differ. For example, $a = [1, 2, 3, 4, 5]^\tau$ and $b = [1, 3, 2, 4, 5]^\tau$ are two 5-dimensional vectors. We have $d_H(a, b) = 2$. A subset of F^n is called a code. Let $C \subseteq F^n$ be a set of n-dimensional vectors which are called words. The minimum Hamming distance of code C, denoted by $d_H(C)$, is $d_H(C) = min(\{d_H(x, y)|x, y \in C, x \neq y\})$. If there is only one word x in C, we define $d_H(C) = d_H(x, \mathbf{0}^\tau)$. For example, let $a_1 = [1, 2, 3, 4, 5]^\tau$, $a_2 = [1, 3, 2, 4, 5]^\tau$ and $a_3 = [2, 5, 6, 7, 8]^\tau$ be the three elements of a code C. We have $d_H(a_1, a_2) = 2$, $d_H(a_1, a_3) = 5$, $d_H(a_2, a_3) = 5$ and $d_H(C) = 2$.

Lemma 1: ([47]) If $x, y, z \in F^n$,

1) $d_H(x, y) \geqslant d_H(z, y) - d_H(z, x)$,
2) $d_H(x, y) \leqslant d_H(z, y) + d_H(z, x)$, and
3) $d_H(x, y) = d_H(x + z, y + z)$.

Given a code $C \subseteq F^n$ and a vector $y \in F^n$, $x \in C$ is the nearest neighbour to y if $d_H(x, y) = min(d_H(z, y)|z \in C)$. Nearest Neighbor Decoding (NND) employs the following decoding strategy. Let y be an n-dimensional vector and $C \subseteq F^n$ be a code. Function $NND : F^n \to C$ maps an n-dimensional vector to a word in C. We have $NND(y) = x$, $x \in C$, if x is the nearest neighbour to y. For example, if $a_1 = [1, 2, 3, 4, 5]^\tau$, $a_2 = [1, 3, 2, 4, 5]^\tau$, $a_3 = [2, 5, 6, 7, 8]^\tau$, $C = \{a_1, a_2, a_3\}$ and $y = [1, 2, 3, 4, 6]^\tau$, we have $NND(y) = a_1$ since $d_H(a_1, y) = 1$, $d_H(a_2, y) = 3$ and $d_H(a_3, y) = 5$.

In a POPN $Q = (N, M_0, V, L)$, transitions can be classified according to the labels to which they map. For instance, suppose $L(t) = \omega$, transition t can be classified by $|T_\omega| = 1$ or $|T_\omega| > 1$, where $T_\omega = \{t|l(t) = \omega\}$. First, let us consider the case $|T_\omega| = 1$.

Proposition 2: Given a POPN $Q = (N, M_0, V, L)$, suppose that transition t is the only transition labelled by $\omega \in \Sigma \cup \{\varepsilon\}$ (i.e., $L(t) = \omega$), $|T_\omega| = 1$, and Ω is an event-set containing f_t^- (i.e., $f_t^- \in \Omega$). Then, under Assumption 1, for any $\Omega' \in \{\Omega^*|\Psi(\Omega) = \Psi(\Omega^*)\}$, $f_t^- \in \Omega'$ and $\Psi(\Omega') \neq (\mathbf{0}^\tau, \varepsilon)$ if and only if

1) $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$, and
2) $d_H(\theta_t^-, \mathbf{0}^\tau) \geqslant \eta + 1$ if $\omega = \varepsilon$, where $\theta_t^+ = VB^+\vec{t}$ and $\theta_t^- = VB^-\vec{t}$.

Proof: ($\Rightarrow$) Suppose that $\Psi(\Omega) = (\Delta M_o, \omega)$. By $|T_{L(t)}| = 1$, $t \in \Omega'$ definitely holds if $f_t^- \in \Omega$ and $\Psi(\Omega) = \Psi(\Omega')$. According to Eq. (3), $\Delta M_o = -\theta_t^- + \vec{e}^r$, where $\vec{e}^r \in \mathbb{Z}^r$ with $d_H(\vec{e}^r, \mathbf{0}^\tau) \leqslant \eta$ is the vector representing faults associated with observable places. If $d_H(\theta_t^-, \mathbf{0}^\tau) \geqslant \eta + 1$ is true under $\omega = \varepsilon$, then, based on Lemma 1, $d_H(\Delta M_o, \mathbf{0}^\tau) = d_H(-\theta_{t'}^- + \vec{e}^r, \mathbf{0}^\tau) = d_H(\theta_{t'}^-, \vec{e}^r) \geqslant d_H(\theta_{t'}^-, \mathbf{0}^\tau) - d_H(\vec{e}^r, \mathbf{0}^\tau) = \eta + 1 - \eta > 0$, which implies $\Psi(\Omega) \neq (\mathbf{0}^\tau, \varepsilon)$. Let $\vec{e}_i^r \in \mathbb{Z}^r$, $d_H(\vec{e}_i^r, \mathbf{0}^\tau) \leqslant \eta$, $i \in \{1, 2, 3\}$. By $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$, we can easily show that $d_H(-\theta_t^- + \vec{e}_1^r, \theta_t + \vec{e}_2^r) \geqslant d_H(-\theta_t^-, \theta_t) - d_H(\vec{e}_1^r, \mathbf{0}^\tau) - d_H(\vec{e}_2^r, \mathbf{0}^\tau) \geqslant 2\eta + 1 - \eta - \eta = 1$ and $d_H(-\theta_t^- + \vec{e}_1^r, \theta_t^+ + \vec{e}_3^r) \geqslant d_H(-\theta_t^-, \theta_t^+) - d_H(\vec{e}_1^r, \mathbf{0}^\tau) - d_H(\vec{e}_3^r, \mathbf{0}^\tau) \geqslant 2\eta + 1 - \eta - \eta = 1$, which indicates $f_t^- \in \Omega'$ if $f_t^- \in \Omega$, $\Psi(\Omega) = \Psi(\Omega')$ and $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$. Thus, for any $\Omega' \in \{\Omega^*|\Psi(\Omega) = \Psi(\Omega^*)\}$, we have $f_t^- \in \Omega'$ and $\Psi(\Omega') \neq (\mathbf{0}^\tau, \varepsilon)$ if the conditions hold.

($\Leftarrow$) If $\omega = \varepsilon$ and $d_H(\theta_t^-, \mathbf{0}^\tau) < \eta + 1$, there exists $\vec{e}^r = \theta_t^-$ such that $\Psi(\Omega) = \Psi(\Omega') = (\mathbf{0}^\tau, \varepsilon)$, which means that no information is obtained when t fires with a precondition fault. Suppose that $d_H(\theta_t^+, \mathbf{0}^\tau) < 2\eta + 1$. Obviously, there exist $\vec{e}_1^r$ and $\vec{e}_2^r$ such that $d_H(-\theta_t^- + \vec{e}_1^r, \theta_t + \vec{e}_2^r) = d_H(\theta_t^+ + \vec{e}_1^r, \mathbf{0}^\tau + \vec{e}_2^r) = 0$ holds, implying that the same observation is obtained no matter a postcondition fault associated with t occurs or not. Thus, for any event-set $\Omega' \in \{\Omega^*|\Psi(\Omega) = \Psi(\Omega^*)\}$, we have $f_t^- \in \Omega'$ and $\Psi(\Omega') \neq (\mathbf{0}^\tau, \varepsilon)$ only if the conditions hold. ■

Corollary 1: Given a POPN $Q = (N, M_0, V, L)$, suppose that transition t is the only transition labelled by $\omega \in \Sigma \cup \{\varepsilon\}$, i.e., $L(t) = \omega$, $|T_\omega| = 1$ and Ω is an event-set containing f_t^+, i.e., $f_t^+ \in \Omega$. Then, under Assumption 1, for any $\Omega' \in \{\Omega^*|\Psi(\Omega) = \Psi(\Omega^*)\}$, $f_t^+ \in \Omega'$ and $\Psi(\Omega') \neq (\mathbf{0}^\tau, \varepsilon)$ if and only if

1) $d_H(\theta_t^-, \mathbf{0}^\tau) \geqslant 2\eta + 1$, and
2) $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant \eta + 1$ if $\omega = \varepsilon$.

Proof: It can be proved similarly as Proposition 2. ■

For the case $|T_\omega| > 1$, the firing of a transition cannot be determined by the obtained label only since multiple transition maps to the same label. Thus, to identify the firing of a transition, more information is necessary and we have the following results.

Proposition 3: Given a POPN $Q = (N, M_0, V, L)$, suppose that transition $t \in T$ satisfies $L(t) = \omega, \omega \in \Sigma \cup \{\varepsilon\}$ and $|T_\omega| > 1$ and Ω is an event-set containing f_t^-, i.e., $f_t^- \in \Omega$. Then, under Assumption 1, for any $\Omega' \in \{\Omega^*|\Psi(\Omega) = \Psi(\Omega^*)\}, f_t^- \in \Omega'$ and $\Psi(\Omega') \neq (\mathbf{0}^\tau, \varepsilon)$ if and only if

1) $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$,
2) $\forall t' \in T_\omega \backslash \{t\}$, $d_H(\theta_t^-, \theta_{t'}^-) \geqslant 2\eta + 1$, and
3) $d_H(\theta_t^-, \mathbf{0}^\tau) \geqslant \eta + 1$ if $\omega = \varepsilon$.

Proof: ($\Rightarrow$) Let $\vec{e}^r \in \mathbb{Z}^r$ with $d_H(\vec{e}^r, \mathbf{0}^\tau) \leqslant \eta$ be a vector representing faults associated with observable places. According to Eq. (3), $\Delta M_o = -\theta_t^- + \vec{e}^r$. By Lemma 1, $d_H(\Delta M_o, \mathbf{0}^\tau) = d_H(-\theta_t^- + \vec{e}^r, \mathbf{0}^\tau) = d_H(\theta_t^-, \vec{e}^r) \geqslant d_H(\theta_t^-, \mathbf{0}^\tau) - d_H(\vec{e}^r, \mathbf{0}^\tau) = \eta + 1 - \eta > 0$ if $d_H(\theta_t^-, \mathbf{0}^\tau) \geqslant \eta + 1$, which implies $\Psi(\Omega) \neq (\mathbf{0}^\tau, \varepsilon)$. We use $\vec{e}_i^r \in \mathbb{Z}^r$ to denote a vector satisfying $d_H(\vec{e}_i^r, \mathbf{0}^\tau) \leqslant \eta$, $i \in$

$\{1, 2, 3, 4\}$. Then, by Lemma 1, we have $d_H(a_1 + b_1, a_2 + b_2) \geqslant d_H(a_1, a_2) - d_H(b_1, \mathbf{0}^\tau) - d_H(b_2, \mathbf{0}^\tau)$, which indicates that for any $t' \in T_\omega \backslash \{t\}$, $d_H(-\theta_t^- + \vec{e}_1^r, \theta_{t'}^+ + \vec{e}_2^r) \geqslant 1$, $d_H(-\theta_t^- + \vec{e}_1^r, -\theta_{t'}^- + \vec{e}_3^r) \geqslant 1$ and $d_H(-\theta_t^- + \vec{e}_1^r, \theta_{t'} + \vec{e}_4^r) \geqslant 1$ if $\forall t' \in T_\omega \backslash \{t\}$, $d_H(\theta_t^-, \theta_{t'}^-) \geqslant 2\eta + 1$ holds. Thus, $t \in \Omega'$ is trivial if $\forall t' \in T_\omega \backslash \{t\}$, $d_H(\theta_t^-, \theta_{t'}^-) \geqslant 2\eta + 1$, and $\Psi(\Omega) = \Psi(\Omega')$. Since $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$, we have $d_H(-\theta_t^- + \vec{e}_1^r, \theta_t + \vec{e}_2^r) \geqslant 1$ and $d_H(-\theta_t^- + \vec{e}_1^r, \theta_t^+ + \vec{e}_3^r) \geqslant 1$ due to $d_H(a_1 + b_1, a_2 + b_2) \geqslant d_H(a_1, a_2) - d_H(b_1, \mathbf{0}^\tau) - d_H(b_2, \mathbf{0}^\tau)$, which implies $f_t^- \in \Omega'$ if $f_t^- \in \Omega$, $\Psi(\Omega) = \Psi(\Omega')$, $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$ and $\forall t' \in T_\omega \backslash \{t\}$, $d_H(\theta_t^-, \theta_{t'}^-) \geqslant 2\eta + 1$. Thus, the given conditions are sufficient.

($\Leftarrow$) Suppose $\omega = \varepsilon$, $\Psi(\Omega) = (\mathbf{0}^\tau, \varepsilon)$ is true if $d_H(\theta_t^-, \mathbf{0}^\tau) < \eta + 1$ and $\vec{e}^r = \theta_t^-$, which implies $d_H(\theta_t^-, \mathbf{0}^\tau) \geqslant \eta + 1$ if $\omega = \varepsilon$ and $\Psi(\Omega') \neq (\mathbf{0}^\tau, \varepsilon)$. If $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$ is not true, there exist $\vec{e}_1^r$ and $\vec{e}_2^r$ such that $d_H(-\theta_t^+ - \vec{e}_1^r, \theta_t + \vec{e}_2^r) = 0$, which means that the same observation may be obtained no matter f_t^- occurs or not. Thus, we show the necessity of $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$. Suppose that $\exists t' \in T_\omega \backslash \{t\}$ such that $d_H(\theta_t^-, \theta_{t'}^-) < 2\eta + 1$. There exist $\vec{e}_1^r$ and $\vec{e}_2^r$ such that $d_H(-\theta_t^- + \vec{e}_1^r, -\theta_{t'}^- + \vec{e}_2^r) = 0$. This means that the same observation is obtained no matter t fires with a postcondition fault or t' fires with a postcondition fault. Thus, the given conditions are necessary. ∎

Corollary 2: Given a POPN $Q = (N, M_0, V, L)$, suppose that transition $t \in T$ satisfies $L(t) = \omega$, $\omega \in \Sigma \cup \{\varepsilon\}$ and $|T_\omega| > 1$, and Ω is any event-set containing f_t^+, i.e., $f_t^+ \in \Omega$. Then, under Assumption 1, for any $\Omega' \in \{\Omega^* | \Psi(\Omega) = \Psi(\Omega^*)\}$, $f_t^+ \in \Omega'$ and $\Psi(\Omega') \neq (\mathbf{0}^\tau, \varepsilon)$ if and only if

1) $d_H(\theta_t^-, \mathbf{0}^\tau) \geqslant 2\eta + 1$,
2) $\forall t' \in T_\omega \backslash \{t\}$, $d_H(\theta_t^+, \theta_{t'}^+) \geqslant 2\eta + 1$, and
3) $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant \eta + 1$ if $\omega = \varepsilon$.

Proof: It is easy to be proved as Proposition 3. ∎

Now we present the necessary and sufficient conditions under which all transitions in POPN $Q = (N, M_0, V, L)$ are structurally diagnosable. Let $T_{L(t)}$ denote T_ω if $L(t) = \omega$.

Theorem 1: Given a POPN $Q = (N, M_0, V, L)$, all transitions in Q are structurally diagnosable under Assumption 1 if and only if $\forall t \in T$,

1) $d_H(\theta_t^-, \mathbf{0}^\tau) \geqslant 2\eta + 1$, $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$; and
2) $d_H(\{\theta_{t'}^+ | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$, $d_H(\{\theta_{t'}^- | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$.

Proof: ($\Rightarrow$) For any transition t, we have $|T_{L(t)}| = 1$ or $|T_{L(t)}| > 1$. For the case $|T_{L(t)}| = 1$, obviously if $d_H(\theta_t^-, \mathbf{0}^\tau) \geqslant 2\eta + 1$ and $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$, then the conditions given in Proposition 2 and Corollary 1 must hold.

For the case $|T_{L(t)}| > 1$, $d_H(\{\theta_{t'}^- | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$ guarantees that $\forall t' \in T_\omega \backslash \{t\}$, $d_H(\theta_t^-, \theta_{t'}^-) \geqslant 2\eta + 1$ holds such that the conditions given in Proposition 3 are met. Similarly, the conditions in Corollary 2 are guaranteed by $d_H(\{\theta_{t'}^- | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$. Thus, $\forall t \in T$, t is structurally diagnosable.

($\Leftarrow$) If t is structurally diagnosable and $|T_{L(t)}| = 1$, the conditions given in Proposition 2 and Corollary 1 should be true. Thus, $d_H(\theta_t^-, \mathbf{0}^\tau) \geqslant 2\eta + 1$ and $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$ hold obviously. Since $d_H(\{\theta_{t'}^+ | t' \in T_{L(t)}\}) = d_H(\theta_t^+, \mathbf{0}^\tau)$ if $|T_{L(t)}| = 1$, we have $d_H(\{\theta_{t'}^+ | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$. Similarly, we can show $d_H(\{\theta_{t'}^- | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$. If $|T_{L(t)}| > 1$ and $\forall t' \in T_{L(t)}$, t' is structurally diagnosable, by Proposition 3, $d_H(\{\theta_{t'}^- | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$ and $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$ hold necessarily. Similarly, by Corollary 2, we have $d_H(\{\theta_{t'}^+ | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$ and $d_H(\theta_t^-, \mathbf{0}^\tau) \geqslant 2\eta + 1$. ∎

For a POPN $Q = (N, M_0, V, L)$, the following property holds if all transitions in Q are structurally diagnosable.

Property 2: Suppose that all transitions in POPN $Q = (N, M_0, V, L)$ are structurally diagnosable under Assumption 1. Let $\Psi(\Omega) = (\Delta M_o, \omega)$ be an observation and $C = \{\theta_t, \theta_t^+, -\theta_t^- | t \in T_\omega\}$ be a code. The following results hold.

1) $NND(\Delta M_o) = -\theta_t^-$, if $f_t^- \in \Omega$;
2) $NND(\Delta M_o) = \theta_t^+$, if $f_t^+ \in \Omega$;
3) $NND(\Delta M_o) = \theta_t$, if $t \in \Omega$ and $\{f_t^+, f_t^-\} \cap \Omega = \emptyset$.

Proof: We use $\vec{e}_i^r \in \mathbb{Z}^r$, $i \in \mathbb{N}$, to denote a combination of faults associated with observable places.

1) In the case $f_t^- \in \Omega$, $\Delta M_o = -\theta_t^- + \vec{e}_1^r$ holds according to Eq. (3). Under Assumption 1, we have $d_H(\Delta M_o, -\theta_t^-) = d_H(\vec{e}_1^r, \mathbf{0}^\tau) \leqslant \eta$. For any $a \in C$, $a \neq -\theta_t^-$, by Proposition 2, in no case $-\theta_t^- + \vec{e}_1^r = a + \vec{e}_2^r$ holds, which implies $d_H(a, \Delta M_o) > \eta$. Thus, $NND(\Delta M_o) = -\theta_t^-$ if $f_t^- \in \Omega$.
2) Similarly, we can prove that $NND(\Delta M_o) = \theta_t^+$ if $f_t^+ \in \Omega$.
3) In the case that t fires without any transition fault ($t \in \Omega$, $\{f_t^+, f_t^-\} \cap \Omega = \emptyset$), we have $\Delta M_o = \theta_t + \vec{e}_1^r$. Then, $d_H(\Delta M_o, \theta_t) = d_H(\vec{e}_1^r, \mathbf{0}^\tau) \leqslant \eta$ holds according to Assumption 1. Suppose that $a \in C$ and $a \neq \theta_t$. Similarly, if $a = \theta_{t'}^+$ or $a = \theta_{t'}^-$ where $t' \in T_\omega$, we have $d_H(a, \Delta M_o) > \eta$. If $a = \theta_{t'}$, $t' \in T_\omega \backslash \{t\}$, then, as the net is pure, we have $\theta_t = \theta_t^+ - \theta_t^-$ and $\theta_t^+(i) \cdot \theta_t^-(i) = 0, \forall i \in \{1, 2, \ldots, r\}$. Thus, $d_H(\theta_{t'}, \theta_t) \geqslant d_H(\theta_{t'}^+, \theta_t^+) \geqslant 2\eta + 1$ and $d_H(\theta_{t'}, \theta_t) \geqslant d_H(\theta_{t'}^-, \theta_t^-) \geqslant 2\eta + 1$, leading to $d_H(a, \Delta M_o) = d_H(\theta_{t'}, \theta_t + \vec{e}_1^r) \geqslant 2\eta + 1 - \eta > \eta$. That is to say, $NND(\Delta M_o) = \theta_t$, if $t \in \Omega$ and $\{f_t^+, f_t^-\} \cap \Omega = \emptyset$.

Thus, we have these conclusions. ∎

B. PLACE FAULTS

In what follows, we proceed our discussion to place faults associated with both observable and unobservable places. By Property 2, the transition firings and the occurrences of the pertinent faults can be determined based on observations if all transitions of a POPN are structurally diagnosable. Then, the following theorem holds.

Theorem 2: Given a POPN $Q = (N, M_0, V, L)$, any observable place $p \in P_o$ is structurally diagnosable under Assumption 1 if all transitions in Q are structurally diagnosable.

Proof: Suppose that $\Psi(\Omega) = (\Delta M_o, \omega)$ is the observation and t is the transition that fires. Vector $\vec{e}^r \in \mathbb{Z}^r$ is used to denote the place faults associated with observable places.

As t is structurally diagnosable, by $\Psi(\Omega)$, one can decide if there is a fault when t fires. Then, $\vec{e}^r$ is calculated according to the result of transition fault diagnosis by utilizing Eq. (3). If $\vec{e}^r(p) \neq 0$, a place fault associated with p occurs, otherwise no fault associated with p occurs. Thus, any observable $p \in P_o$ is structurally diagnosable if all transitions in Q are structurally diagnosable. ■

Note that, for a POPN $Q = (N, M_0, V, L)$, the condition given in Theorem 2 is only sufficient but not necessary. We do not pursue a necessary and sufficient condition since the goal of this paper is to achieve maximally structural diagnosability for a POPN. For an unobservable place, it cannot achieve structural diagnosability as given by the following proposition.

Proposition 4: Given a POPN $Q = (N, M_0, V, L)$, any unobservable place $p \in P_u$ is not structurally diagnosable.

Proof: Suppose that Ω is the event-set that occurs and $\Psi(\Omega) = (\Delta M_o, \omega)$ is the observation. For an unobservable place p, no matter if there is a fault associated with p, one obtains the same observation $\Psi(\Omega)$. Thus, an unobservable place is not structurally diagnosable. ■

Proposition 4 indicates that faults associated with an unobservable place p cannot achieve structural diagnosability by employing a redundancy. As a result, a place should be monitored by a sensor if faults associated with it need to be structurally diagnosable.

Proposition 5: Given a POPN $Q = (N, M_0, V, L)$, an unobservable place p is casually diagnosable under Assumption 1 if all transitions in Q are structurally diagnosable.

Proof: Suppose that, for an unobservable place p, its initial marking is $M_0(p)$. Let α be a feasible event-set sequence from M_0 with $Bd(Q, p, \alpha) = 1$. If all transitions in Q are structurally diagnosable, the firing times of a transition in ${}^\bullet p \cup p^\bullet$, and the occurrences of faults associated with it can be determined based on $\Psi(\alpha)$ when $M_0[\alpha\rangle M$. By assumption that no fault associated with p occurs, the number of tokens in $p' \in P_u$ at each time epoch k can be calculated according to Eq. (2), which is denoted by $M_k^e(p')$.

There are two cases if $Bd(Q, p, \alpha) = 1$: an enabled transition is disabled and a disabled transition is enabled. In the first case, suppose that transition t is disabled by faults associated with p at time epoch k. We observe $\perp$ (no output for a time long enough) while $\forall p' \in {}^\bullet t \cap P_o$, the number of tokens in p' is greater than $W(p', t)$ and $\forall p' \in {}^\bullet t \cap P_u$, $M_k^e(p') \geqslant W(p', t)$. This observation indicates that $\exists p' \in {}^\bullet t \cap P_u$ such that the faults associated with p' disable t. Thus, we can conclude that for any event-set sequence α' satisfying $M_0[\alpha'\rangle$ and $\Psi(\alpha) = \Psi(\alpha')$, there is at least one element $y \in Fa = {}^\bullet t \cap P_u$ such that $Bd(Q, y, \alpha') = 1$. In the other case, the firing of t with $M_k^e(p) < W(p, t)$ is observed. Since firing t with $M_k^e(p) < W(p, t)$ implies that t is enabled by faults associated with p at time epoch k, for any event-set sequence $\alpha' \in \{\alpha^* | M_0[\alpha^*\rangle, \Psi(\alpha) = \Psi(\alpha^*)\}$, we have $Bd(Q, p, \alpha') = 1$ accordingly. Thus, p is casually diagnosable if all transitions in Q are structurally diagnosable. ■

Proposition 6: Given a POPN $Q = (N, M_0, V, L)$, a casually diagnosable place p is obstinately diagnosable under Assumption 1 if for any $t \in p^\bullet$ satisfying $|{}^\bullet t \cap P_u| > 1$, there exists $t' \in p^\bullet$ such that $\theta_t^- \geqslant \theta_{t'}^-$ and ${}^\bullet t' \cap P_u = \{p\}$.

Proof: Suppose that for any $t \in p^\bullet$ satisfying $|{}^\bullet t \cap P_u| > 1$, there exists $t' \in p^\bullet$ such that $\theta_t^- \geqslant \theta_{t'}^-$ and ${}^\bullet t' \cap P_u = \{p\}$. When t is disabled by faults associated with p, t' must be also disabled by faults associated with p. Then, one can decide if the faults associated with p are behavior-disturbed. If any $t \in p^\bullet$ is enabled by faults associated with p, the faults must be behavior-disturbed. Thus, we come to this conclusion. ■

According to the discussion above, we have the following conclusion.

Theorem 3: Given a POPN $Q = (N, M_0, V, L)$, Q is maximally-structurally diagnosable if and only if $\forall t \in T$,

1) $d_H(\theta_t^-, \mathbf{0}^\tau) \geqslant 2\eta + 1$, $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$, and
2) $d_H(\{\theta_{t'}^+ | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$, $d_H(\{\theta_{t'}^- | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$.

Proof: ($\Rightarrow$) By Theorem 1, all transitions in Q are structurally diagnosable if $\forall t \in T$, $d_H(\theta_t^-, \mathbf{0}^\tau) \geqslant 2\eta + 1$, $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$, $d_H(\{\theta_{t'}^+ | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$ and $d_H(\{\theta_{t'}^- | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$ are true. Then, it is easy to conclude that all observable places in Q are structurally diagnosable according to Theorem 2. By Proposition 4, an unobservable place cannot be structurally diagnosable. However, it can be obstinately or casually diagnosable since all transitions are structurally diagnosable. Let p be an unobservable place that is casually diagnosable but not obstinately diagnosable. Since the transitions and observable places are structurally diagnosable, there exists an unobservable place $p' \neq p$ such that the faults associated with p or p' can disable a transition t with the same firing sequence from the initial marking. Thus, no matter what redundancy is employed, the observations for the faults associated with p and p' are the same. Place p cannot be obstinately diagnosable by employing a redundancy. Then, Q is maximally-structurally diagnosable if the conditions given in the theorem are true.

($\Leftarrow$) Q's maximally structural diagnosability implies that $\forall t \in T$ is structurally diagnosable, which holds only if $\forall t \in T$, $d_H(\theta_t^-, \mathbf{0}^\tau) \geqslant 2\eta + 1$, $d_H(\theta_t^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$, $d_H(\{\theta_{t'}^+ | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$ and $d_H(\{\theta_{t'}^- | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$ are satisfied by Theorem 1. Thus, the given conditions are necessary. ■

C. FAULT DIAGNOSIS ALGORITHM

In what follows, we introduce the procedures to diagnose faults that occur in a POPN $Q = (N, M_0\ V, L)$ with maximally structural diagnosability. Suppose that, at time epoch k, the observation is $\Psi(\Omega_k) = (\Delta M_o^k, l_k)$. Based on $\Psi(\Omega_k)$, both the following events can be decided by using NND: 1) the transition that fires, and 2) whether a transition fault occurs or not. A place fault associated with observable places can be diagnosed according to the differences between ΔM_o^k and $NND(\Delta M_o^k)$, i.e., $\vec{e}_k^r = \Delta M_o^k - NND(\Delta M_o^k)$. Then, by assumption that no fault associated with an unobservable

place occurs, the expected marking M_k^e can be calculated according to

$$M_k^e = M_{k-1}^e + B\vec{\sigma_k} + B^-\vec{\upsilon_{k+}} - B^+\vec{\upsilon_{k-}} + \vec{e_k^n}$$

where $\forall p \in P_o$, $\vec{e_k^n}(p) = \vec{e_k^r}(p)$ and $\forall p \in P_u$, $\vec{e_k^n}(p) = 0$. Note that $\vec{e_k^r} \in \mathbb{Z}^r$ is the vector indicating the place faults associated with observable places while $\vec{e_k^n} \in \mathbb{Z}^n$ is the vector denoting the place faults associated with all places. The expected marking at the initial time epoch is equal to the initial marking. If a transition enabled by faults associated with an unobservable place p fires, $M_k^e(p) < 0$, otherwise, no fault associated with p occurs or the faults associated with p are not behavior-disturbed.

In the case that deadlock information is obtained at time epoch k, the expected marking of Q at time epoch k is equal to the expected marking at time epoch $k-1$, since no event occurs at time epoch k, i.e.,

$$M_k^e = M_{k-1}^e$$

If the faults associated with an unobservable place p are behavior-disturbed, there exists at least one transition t such that $\forall p' \in {}^\bullet t$, $M_k^e(p') \geqslant W(p', t)$ holds. If p is the only unobservable place in ${}^\bullet t$, the occurrences of faults associated with p are unambiguous, otherwise, we can conclude that only the faults associated with at least one unobservable place in ${}^\bullet t$ are behavior-disturbed. The procedure to diagnose faults is given in Algorithm 1.

Note that, we do not identify the exact number of tokens changed by the place faults associated with unobservable places. For an unobservable place p, $\vec{e_k^n}(p)$ is not the actual number of tokens changed by the faults associated with p: $\vec{e_k^n}(p) = 0$ indicates that no place fault associated with p occurs or the faults are not behavior-disturbed; $\vec{e_k^n}(p) = 1$ means that the faults associated with p increase the number of tokens in p; $\vec{e_k^n}(p) = -1$ denotes that the faults associated with p decrease the number of tokens in p; $\vec{e_k^n}(p) = -2$ represents the case that the place faults associated with at least one unobservable place in P_f are behavior-disturbed, where $P_f = \{p' | \vec{e_k^n}(p') = -2\}$.

Algorithm 1 Fault Diagnosis for a POPN at Time Epoch k

Input: POPN $Q = (N, M_0, V, L)$, expected marking M_{k-1}^e and observation $\Psi(\Omega_k)$ or $\perp$;
Output: fault vectors: $\vec{\upsilon_{k+}}$, $\vec{\upsilon_{k-}}$ and $\vec{e_k^n}$;
Initialize: set all entries of $\vec{\upsilon_{k+}}$, $\vec{\upsilon_{k-}}$ and $\vec{e_k^n}$ to $\mathbf{0}^\tau$;
if $\Psi(\Omega_k) = (\Delta M_o^k, l_k)$ is observed **then do**

1) Let $C = \{\theta_t, \theta_t^+, -\theta_t^- | t \in T_{l_k}\}$;
2) Use NND to determine the transition t that fires;
3) Set $\vec{\upsilon_{k+}} = \vec{t}$ if $NND(\Delta M_o^k) = \theta_t^+$ or $\vec{\upsilon_{k-}} = \vec{t}$ if $NND(\Delta M_o^k) = -\theta_t^-$;
4) Diagnose place faults associated with an observable place p: set $\vec{e_k^n}(p) = \vec{e_k^r}(p)$ where $\vec{e_k^r} = \Delta M_o^k - NND(\Delta M_o^k)$;
5) Calculate the expected marking M_k^e;
6) Diagnose the place fault associated with an unobservable place p: set $\vec{e_k^n}(p) = 1$ if $M_k'(p) < 0$;
7) Return $\vec{\upsilon_{k+}}$, $\vec{\upsilon_{k-}}$ and $\vec{e_k^n}$.

else $\perp$ is observed **then do**

1) Set $M_k^e = M_{k-1}^e$;
2) Search the transition set $Ts = \{t | \forall p \in {}^\bullet t, M_k^e(p) \geqslant W(p, t)\}$;
3) Calculate $\vec{e_k^n}$
   for any $p \in P_u$
   for any $t \in p^\bullet \cap Ts$
   if $|{}^\bullet t \cap P_u| > 1$ and $\vec{e_k^n}(p) = 0$ **then do**
   Set $\vec{e_k^n}(p) = -2$;
   else Set $\vec{e_k^n}(p) = -1$;
   end if;
4) Return $\vec{\upsilon_{k+}}$, $\vec{\upsilon_{k-}}$ and $\vec{e_k^n}$.

end if

V. REDUNDANT EMBEDDINGS

Given a POPN $Q = (N, M_0, V, L)$, this section discusses how to build a redundancy for achieving maximally structural diagnosability. The net structure of such a redundancy and its initial marking are obtained by solving an integer linear programming problem. In what follows, we discuss how the integer linear programming is formulated and solved.

A. CONSTRAINTS FOR BEHAVIOR PERMISSION

A redundancy is formed by adding places into the original POPN. The added places should not disturb the behavior of a POPN as a controller, otherwise they cannot be called a redundancy. To do so, constraints should be imposed on the weights of arcs between the added places and transitions in the original POPN. Suppose that POPN $Q_r = (N', M_0', V', L)$ is a redundant embedding of POPN $Q = (N, M_0, V, L)$ with z places being added. We need to ensure that the language generated by Q_r is equal to that generated by Q. This can be done by properly determining the weights of the arcs between the added places and transitions and the initial marking of those places.

Definition 12: Let $Q = (N, M_0, V, L)$ be a POPN and its extended POPN by adding a place p be $Q_r = (N', M_0', V', L)$. Place p is said to be no-behavior-effect on Q if for any M_0, there exists a marking M_0' such that $\forall q \in P, M_0'(q) = M_0(q)$, and $\mathcal{L}(N, M_0) = \mathcal{L}(N', M_0')$.

In order to analyze the effect of an added place on the behavior of POPN $Q = (N, M_0, V, L)$, a kind of special transition vectors is introduced.

Definition 13: A transition sequence σ_T of $Q = (N, M_0, V, L)$ is said to be a T-increase if $B\vec{\sigma_T} \geqslant \mathbf{0}^\tau$.

For example, transition sequences σ_1 and σ_2 with $\vec{\sigma_1} = [0, 1, 1, 2, 0]^\tau$ and $\vec{\sigma_2} = [0, 2, 2, 4, 0]^\tau$ are two T-increases of Q_1 shown in Fig. 1. A transition t is said to be contained in a T-increase σ_T if $\vec{\sigma_T}(t) > 0$.

Property 3: In a POPN, transition t cannot fire infinitely if it is not contained in any T-increase.

Proof: If no T-increase contains t, any transition firing sequence that includes t necessarily decreases the number of tokens in at least one place. Let p denote such a place. No matter how many tokens are in p at the initial state, the tokens can be exhausted by firing t, which leads to t being disabled finally. Thus, t cannot fire infinitely if t is not contained by any T-increase. ■

Proposition 7: Let $Q_r = (N', M_0', V', L)$ be a redundant embedding of POPN $Q = (N, M_0, V, L)$ and $[B^\tau, B_r^\tau]^\tau$ be the incidence matrix of Q_r. Then, a T-increase σ_T of Q is a T-increase of Q_r if $B_r\vec{\sigma_T} \geqslant \mathbf{0}^\tau$.

Proof: By $B\vec{\sigma_T} \geqslant \mathbf{0}^\tau$ and $B_r\vec{\sigma_T} \geqslant \mathbf{0}^\tau$, we have $[B^\tau, B_r^\tau]^\tau\vec{\sigma_T} = B\vec{\sigma_T} + B_r\vec{\sigma_T} \geqslant \mathbf{0}^\tau$. Thus, σ_T is also a T-increase of Q_r. ■

Proposition 8: Let $Q_r = (N', M_0', V', L)$ be a redundant embedding of POPN $Q = (N, M_0, V, L)$. $B_r(p) \in \mathbb{N}^m$ is a vector whose j-th entry denotes the arc weight between the added place p and transition $t_j, j \in \mathbb{N}_m$. Then, p has no effect on the behavior of Q_r if and only if $B_r(p)\vec{\sigma_T} \geqslant 0$ holds for all T-increase σ_T of Q.

Proof: ($\Rightarrow$) For any transition sequence $\sigma \in \mathcal{L}(N, M_0)$, σ can be expressed as a linear combination of several T-increases and a non-T-increase sequence σ_e. Since σ_e is not a T-increase, the number of transitions in it is finite according to Property 3. Therefore, there exists a constant β that is greater than the number of tokens consumed by firing σ_e. The number of tokens consumed by firing σ is less than β if $B_r(p)\vec{\sigma_T} \geqslant 0$ holds for any T-increase σ_T. As above discussed, any feasible transition sequence in Q is also feasible in Q_r. Obviously, if a transition sequence is not feasible in Q, it is also prohibited in Q_r. Thus, if $B_r(p)\vec{\sigma_T} \geqslant 0$ holds for all T-increases σ_T of Q, for any M_0, there is a marking M_0' such that $\forall q \in P, M_0'(q) = M_0(q)$, and $\mathcal{L}(N, M_0) = \mathcal{L}(N', M_0')$, which means that place p has no effect on the behavior of the Q.

($\Leftarrow$) Suppose that σ_1 is a T-increase satisfying $B_r(p)\vec{\sigma_1} = -\nu < 0, \nu \in \mathbb{N}$. If σ is a transition sequence constructed by repeating σ_1 κ times, $\kappa \in \mathbb{N}$, we have $\sigma \in \mathcal{L}(N, M_0)$. Obviously, there exists an integer $\kappa \in \mathbb{N}$ such that $\beta - \nu\kappa < 0$, which implies that there is no marking M_0' satisfying: $\forall q \in P$, $M_0'(q) = M_0(q)$, and $\mathcal{L}(N, M_0) = \mathcal{L}(N', M_0')$. Thus, place p has effect on the behavior of Q if there exists a T-increase σ_1 such that $B_r(p)\vec{\sigma_1} < 0$. ■

Theorem 4: Let $Q_r = (N', M_0', V', L)$ be a redundant embedding of $Q = (N, M_0, V, L)$. Then, an added place p has no effect on the behavior of Q_r if and only if there exists a nonnegative vector y^τ such that $B_r(p) \geqslant y^\tau B$, where $B_r(p)$ is the vector denoting the arc weights between the added place p and transitions in Q.

Proof: ($\Rightarrow$) Let σ_T be a T-increase of Q. $y^\tau B\vec{\sigma_T} \geqslant 0$ holds for any nonnegative vector y^τ. Then, $B_r(p)\vec{\sigma_T} \geqslant 0$ is true for any T-increase σ_T if there exists a nonnegative vector y^τ such that $B_r(p) \geqslant y^\tau B$. Thus, by Proposition 8, p has no effect on the behavior of Q.

($\Leftarrow$) If there is no nonnegative vector y^τ satisfying $B_r(p) \geqslant y^\tau B$, by setting $y^\tau = \mathbf{0}^\tau$, there is at least one negative entry of $B_r(p)$ and its corresponding column of B is nonnegative. Let $B_r(p, i)$ be the negative entry and $B(:, i) \geqslant 0$. There necessarily exists a vector $\vec{\sigma}$ such that $B\vec{\sigma} \geqslant \mathbf{0}^\tau$ and $B_r(p)\vec{\sigma} < 0$, where all entries of $\vec{\sigma}$ are zero except that the i-th entry is one. Thus, place p has effect on the behavior of Q due to Proposition 8. ■

Let $W(p_{ai}, t_j)$, $j \in \mathbb{N}_m$, denote the weight of the arc between an added place p_{ai} and transition t_j. We use $B_r(p_{ai})$ to denote vector $[W(p_{ai}, t_1), W(p_{ai}, t_2), \ldots, W(p_{ai}, t_m)]$. Based on Theorem 4, if the z added places are a redundancy, the weights of arcs between the z added places and the transitions should satisfy the following constraints:

$$\begin{aligned} y_i^\tau B &\leqslant B_r(p_{ai}), \quad \forall i \in \mathbb{N}_z = \{1, 2, \ldots, z\} \\ y_i^\tau &\geqslant 0, \quad \forall i \in \mathbb{N}_z \end{aligned} \tag{6}$$

The problem for setting the initial marking for the added places can be formulated as an integer linear programming problem. Since an added place p_{ai} should have no effect on the behavior of the POPN, the initial number of tokens in p_{ai} should be greater than the sum of tokens that can be consumed. The maximum number of tokens can be obtained by the following integer linear programming problem:

$$\begin{aligned} &maximize \ -B_r(p_{ai}) \times \vec{\sigma} \\ &subject\ to\ M_0 + B\vec{\sigma} \geqslant 0 \\ &\vec{\sigma} \geqslant 0 \end{aligned} \tag{7}$$

where M_0 is the initial marking of Q, B is the incidence matrix of Q and $\vec{\sigma}$ is a vector with integer variables as entries.

B. CONSTRAINTS FOR DIAGNOSABILITY

An effective redundancy embedding ensures maximally structural diagnosability. In order to simplify the description of the problem, we define a nonzero counter function.

Definition 14: A nonzero counter function is defined as $Z_n : H \to \mathbb{N}$, where H is a set of vectors and $Z_n(\vec{a}) = k$, $\vec{a} \in H$, denotes that k entries of $\vec{a}$ are nonzero.

For example, $\vec{a} = [-1, 0, 3, -2, 0, 1]$ is a vector. We have $Z_n(\vec{a}) = 4$, since there are four nonzero entries. Let $Q_r = (N', M_0', V', L)$ be a redundant embedding of $Q = (N, M_0, V, L)$. Then, for maximally structural diagnosability, we present constraints on the arc weights between the added places and transitions as follows. To ensure that $\forall t_j \in T$, $d_H(\theta_{t_j}^-, \mathbf{0}^\tau) \geqslant 2\eta + 1$ and $d_H(\theta_{t_j}^+, \mathbf{0}^\tau) \geqslant 2\eta + 1$, the arc weights between the added place $p_{ai}, i \in \mathbb{N}_z$, and transitions should satisfy

$$\begin{aligned} &Z_n(\theta_{t_j}^+) + \sum_{i=1}^{z} g_{i,j}^+ \geqslant 2\eta + 1 \\ &Z_n(\theta_{t_j}^-) + \sum_{i=1}^{z} g_{i,j}^- \geqslant 2\eta + 1 \\ &W(p_{ai}, t_j) \leqslant \mathbb{M} g_{i,j}^+, \quad \forall i \in \mathbb{N}_z \\ &W(p_{ai}, t_j) \geqslant -\mathbb{M}(1 - g_{i,j}^+) + 1, \quad \forall i \in \mathbb{N}_z \\ &W(p_{ai}, t_j) \geqslant -\mathbb{M} g_{i,j}^-, \quad \forall i \in \mathbb{N}_z \\ &W(p_{ai}, t_j) \leqslant \mathbb{M}(1 - g_{i,j}^-) - 1, \quad \forall i \in \mathbb{N}_z \end{aligned} \tag{8}$$

where $W(p_{ai}, t_j)$ denotes the arc weight between p_{ai} and t_j, $\mathbb{M}$ is a positive integer constant that is big enough, and $g^+_{i,j} \in \{0, 1\}$ ($g^-_{i,j} \in \{0, 1\}$) is a binary variable corresponding to p_{ai} and t_j. Let $g_{i,j} = g^-_{i,j} + g^+_{i,j}$. Then, since there is only one arc between a transition and a place, we have

$$g^-_{i,j} + g^+_{i,j} \leqslant 1 \tag{9}$$

Thus, $g_{i,j} \in \{0, 1\}$ is a binary variable. If there exist two transitions t_1 and t_2 such that $L(t_1) = L(t_2)$, to guarantee that $\forall t \in T$, $d_H(\{\theta^+_{t'} | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$ and $d_H(\{\theta^-_{t'} | t' \in T_{L(t)}\}) \geqslant 2\eta + 1$ hold, the following constraints should be imposed

$$\begin{aligned}
&Z_n(\theta^-_{t_1} - \theta^-_{t_2}) + \sum_{i=1}^{z} r^-_{i,1} \geqslant 2\eta + 1\\
&Z_n(\theta^+_{t_1} - \theta^+_{t_2}) + \sum_{i=1}^{z} r^+_{i,1} \geqslant 2\eta + 1\\
&W(p_{ai}, t_1) - W(p_{ai}, t_2) \geqslant r^-_{i,1} - \mathbb{M}(1 - h^{i-}_{1,2}), \quad \forall i \in \mathbb{N}_z\\
&W(p_{ai}, t_1) - W(p_{ai}, t_2) \leqslant r^-_{i,1} + \mathbb{M}h^{i-}_{1,2}, \quad \forall i \in \mathbb{N}_z\\
&W(p_{ai}, t_1) - W(p_{ai}, t_2) \geqslant r^+_{i,1} - \mathbb{M}(1 - h^{i+}_{1,2}), \quad \forall i \in \mathbb{N}_z\\
&W(p_{ai}, t_1) - W(p_{ai}, t_2) \leqslant r^+_{i,1} + \mathbb{M}h^{i+}_{1,2}, \quad \forall i \in \mathbb{N}_z;\\
&r^-_{i,1} \leqslant g^-_{i,1}, \quad \forall i \in \mathbb{N}_z\\
&r^+_{i,1} \leqslant g^+_{i,1}, \quad \forall i \in \mathbb{N}_z
\end{aligned} \tag{10}$$

where $h^{i+}_{1,2} \in \{0, 1\}$, $h^{i-}_{1,2} \in \{0, 1\}$, $r^+_{i,1} \in \{0, 1\}$ and $r^-_{i,1} \in \{0, 1\}$ are binary variables. These constraints on the arc weights between added places and transitions should be satisfied to ensure maximally structural diagnosability.

C. ALGORITHM FOR REDUNDANCY CONSTRUCTION

Based on the above discussion, we present an algorithm for building a redundancy to diagnose faults with minimum added places and arcs, as given in Algorithm 2.

If Q_r with incidence matrix $[B^\tau, B^\tau_r]^\tau$ is a redundant embedding of Q, B_r is necessarily a solution of the integer linear programming problem given in Algorithm 2. Since the resulting redundancy is obtained by adding the minimal number of places, Problem 1 can be solved to do so. Note that, the information of initial marking M_0 is not used to obtain the matrix B_r, i.e., B_r is independent of M_0. If the initial marking of a POPN changes, the redundancy remains valid by re-marking it as M_r, which can be easily obtained by solving (7). Thus, Algorithm 2 is reusable for different initial markings.

D. EXAMPLE: REDUNDANCY DESIGN

We take the POPN Q_1 in Fig. 1 as an example to illustrate the proposed method. Suppose that Q_1 is initially marked with $M_0 = [4, 1, 0, 2]^\tau$. We design a redundancy for Q_1 to diagnose faults with the assumption that at most one place fault occurs per time epoch. Since all the places in ${}^\bullet t_3 \cup t_3^\bullet$ are unobservable, at least three observable places should be added to ${}^\bullet t_3$ and another three to $t_3^\bullet$. Thus, the minimum number of added places is six, i.e., $z = 6$. Every added place can at most connect a transition once and there are at most 30 arcs between the added places and the transitions. To make Q_1 maximally-structurally diagnosable, all arc weights should satisfy (6), (8) and (9). For instance, since $Z_n(\theta^+_{t_1}) = 1$ and $Z_n(\theta^-_{t_1}) = 0$, the arc weights between the added places and t_1 should satisfy

$$\begin{aligned}
&1 + \sum_{i=1}^{6} g^+_{i,1} \geqslant 3\\
&\sum_{i=1}^{6} g^-_{i,1} \geqslant 3\\
&W(p_{ai}, t_1) \leqslant \mathbb{M}g^+_{i,1}, \quad \forall i \in \{1, 2, \ldots, 6\}\\
&W(p_{ai}, t_1) \geqslant -\mathbb{M}(1 - g^+_{i,1}) + 1, \quad \forall i \in \{1, 2, \ldots, 6\}\\
&W(p_{ai}, t_1) \geqslant -\mathbb{M}g^-_{i,1}, \quad \forall i \in \{1, 2, \ldots, 6\}\\
&W(p_{ai}, t_1) \leqslant \mathbb{M}(1 - g^-_{i,1}) - 1, \quad \forall i \in \{1, 2, \ldots, 6\}\\
&g^-_{i,1} + g^+_{i,1} = g_{i,1}, \quad \forall i \in \{1, 2, \ldots, 6\}
\end{aligned}$$

where $\mathbb{M}$, a positive integer constant that is big enough, is set to be 100. By $L(t_1) = L(t_5) = a$, $Z_n(\theta^+_{t_1} - \theta^+_{t_5}) = 0$ and $Z_n(\theta^-_{t_1} - \theta^-_{t_5}) = 0$, the arc weights between the added places

Algorithm 2 Redundancy Construction

Input: a POPN $Q = (N, M_0, V, L)$
Output: matrix B_r and marking M_r
Initialize: $z = 1$, $ans = 0$
while $\{ans = 0\}$ **do**

1) Set constraints *cons* for the linear programming problem:
   $\forall i \in \mathbb{N}_z$: set the arc weights between the added places and transitions according to (6), (8) and (9);
   if {there exist two transitions t_1 and t_2 such that $L(t_1) = L(t_2)$} **then do**
   set the arc weights between t_1, t_2 and the added places according to (10);
   end if
2) Solve the integer linear programming problem:

$$\begin{cases} min \sum_{i=1}^{z} \sum_{j=1}^{m} (g_{i,j}) \\ \text{subject to: } cons \end{cases}$$

3) **if** {there is a solution} **then do**
   (a) $B_r(p_{ai}, t) = W(p_{ai}, t)$;
   (b) Obtain M_r by solving (7);
   (c) Set $ans = 1$.
   else
   (a) $z = z + 1$.
   end if

end While

(4) Return B_r and M_r.

TABLE 1. The weights of arcs between the added places and the transitions.

	p_{a1}	p_{a2}	p_{a3}	p_{a4}	p_{a5}	p_{a6}
t_1	-1	-1	1	2	-1	5
t_2	1	1	0	-1	1	-1
t_3	1	1	2	-1	-1	-1
t_4	-1	-1	-1	1	0	1
t_5	-2	-2	-2	1	1	1

and t_1 should also satisfy

$$\sum_{i=1}^{6} r_{i,1}^{+} \geqslant 3$$
$$\sum_{i=1}^{6} r_{i,1}^{-} \geqslant 3$$
$$W(p_{ai}, t_1) - W(p_{ai}, t_5) \geqslant r_{i,1}^{+} - \mathbb{M}(1 - h_{1,5}^{i+}), \quad \forall i \in \{1, 2, \ldots, 6\}$$
$$W(p_{ai}, t_1) - W(p_{ai}, t_5) \leqslant r_{i,1}^{+} + \mathbb{M}h_{1,5}^{i+}, \quad \forall i \in \{1, 2, \ldots, 6\}$$
$$W(p_{ai}, t_1) - W(p_{ai}, t_5) \geqslant r_{i,1}^{-} - \mathbb{M}(1 - h_{1,5}^{i-}), \quad \forall i \in \{1, 2, \ldots, 6\}$$
$$W(p_{ai}, t_1) - W(p_{ai}, t_5) \leqslant r_{i,1}^{-} + \mathbb{M}h_{1,5}^{i-}, \quad \forall i \in \{1, 2, \ldots, 6\}$$
$$r_{i,1}^{+} \leqslant g_{i,1}^{+}, \quad \forall i \in \{1, 2, \ldots, 6\}$$
$$r_{i,1}^{-} \leqslant g_{i,1}^{-}, \quad \forall i \in \{1, 2, \ldots, 6\}$$

Then, we should build the constraints to ensure that the added places form a redundancy of Q_1. Take place p_{a1} as an example. The constraints on the weights of arcs between p_{a1} and transitions are

$$-1 \times y_1 + 0 \times y_2 + 1 \times y_3 + 0 \times y_4 - W(p_{a1}, t_1) \leqslant 0$$
$$1 \times y_1 + -2 \times y_2 + 0 \times y_3 + 0 \times y_4 - W(p_{a1}, t_2) \leqslant 0$$
$$-1 \times y_1 + 0 \times y_2 + 0 \times y_3 + 2 \times y_4 - W(p_{a1}, t_3) \leqslant 0$$
$$0 \times y_1 + 1 \times y_2 + 0 \times y_3 + -1 \times y_4 - W(p_{a1}, t_4) \leqslant 0$$
$$0 \times y_1 + 0 \times y_2 + 1 \times y_3 + -2 \times y_4 - W(p_{a1}, t_5) \leqslant 0$$
$$-y_i \leqslant 0, \quad \forall i \in \{1, 2, 3, 4\}$$

For this example, there are 210 variables and 312 constraints with the following linear objective function

$$min \sum_{i=1}^{6} \sum_{j=1}^{5} g_{i,j}$$

The solution for this integer linear programming problem is shown in Table 1. After the structure of the redundancy is determined, we should initialize the added places with enough tokens. As discussed previously, the minimum number of initial tokens for each added place can be obtained by solving an integer linear programming problem. Take the initial marking setting for p_{a6} as an example. The integer linear programming problem can be expressed as

$$\begin{aligned} &maximize \ -[5, -1, -1, 1, 1] \times \sigma \\ &subject\ to\ [4, 1, 0, 2]^{\tau} + B\sigma \geqslant 0 \\ &\sigma \geqslant 0 \end{aligned}$$

The solution for this integer linear programming problem is five. Thus, p_{a6} should be initially marked with at least five tokens. The minimum number of tokens for the six added places are six, six, two, five, four and five, respectively.

In summary, to make Q_1 maximally-structurally diagnosable, six observable places need to be added. The structure of the redundancy can be described by incidence matrix B_r, where

$$B_r = \begin{pmatrix} -1 & 1 & 1 & -1 & -2 \\ -1 & 1 & 1 & -1 & -2 \\ 1 & 0 & 2 & -1 & -1 \\ 2 & -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 0 & 1 \\ 5 & -1 & -1 & 1 & 1 \end{pmatrix}$$

and the initial marking of the added places is $[6, 6, 2, 5, 4, 5]^{\tau}$.

VI. CONCLUSION

We study the problem of fault diagnosis in a discrete event system modeled by a partially observed Petri net with a certain sensor selection. The necessary and sufficient conditions for maximally structural diagnosability of a system are developed and, accordingly, a redundancy is built to ensure that the POPN reaches maximally structural diagnosability without changing the sensor selection for the original system. In the existing work, it requires prior knowledge of faults or a special structure, which may not be realistic in practice. To solve this problem, in this work, faults are modeled as abnormal events that can occur on any transition or place but not special transitions. Also, the proposed method takes the advantage of the structural properties of a POPN and can be easily adapted to systems with different initial markings. It is demonstrated that the proposed method can achieve fault tolerance and provide analytical characterizations of the redundant systems. To reduce the structure of redundancies or the cost for sensors, we will consider fault diagnosis problem with optimal sensor selection by considering the fault diagnosis techniques proposed in [48] in the future work.

REFERENCES

[1] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*. New York, NY, USA: Springer, 2009.
[2] Z. Li, G. Liu, M. Hanisch, and M. Zhou, "Deadlock prevention based on structure reuse of Petri net supervisors for flexible manufacturing systems," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 42, no. 1, pp. 178–191, Jan. 2012.
[3] J. Zhang, M. Khalgui, Z. Li, G. Frey, O. Mosbahi, and H. Ben Salah, "Reconfigurable coordination of distributed discrete event control systems," *IEEE Trans. Control Syst. Technol.*, vol. 23, no. 1, pp. 323–330, Jan. 2015.
[4] Y. Chen, Z. Li, K. Barkaoui, and M. Uzam, "New Petri net structure and its application to optimal supervisory control: Interval inhibitor arcs," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 10, pp. 1384–1400, Oct. 2014.

[5] J. Ye, Z. Li, and A. Giua, "Decentralized supervision of Petri nets with a coordinator," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 6, pp. 955–966, Jun. 2015.

[6] X. Wang, I. Khemaissia, M. Khalgui, Z. Li, O. Mosbahi, and M. Zhou, "Dynamic low-power reconfiguration of real-time systems with periodic and probabilistic tasks," *IEEE Trans. Autom. Sci. Eng.*, vol. 12, no. 1, pp. 258–271, Jan. 2015.

[7] Y. Chen, Z. Li, K. Barkaoui, and A. Giua, "On the enforcement of a class of nonlinear constraints on Petri nets," *Automatica*, vol. 55, pp. 116–124, May 2015.

[8] Y. Tong, Z. Li, C. Seatzu, and A. Giua, "Verification of state-based opacity using Petri nets," *IEEE Trans. Autom. Control*, vol. 62, no. 6, pp. 2823–2837, Jun. 2017.

[9] X. Wang, Z. Li, and W. Wonham, "Dynamic multiple-period reconfiguration of real-time scheduling based on timed DES supervisory control," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 101–111, Feb. 2016.

[10] N. Wu, M. Zhou, L. Bai, and Z. Li, "Short-term scheduling of crude oil operations in refinery with high-fusion-point oil and two transportation pipelines," *Enterprise Inf. Syst.*, vol. 10, no. 6, pp. 581–610, 2016.

[11] M. Uzam, Z. Li, G. Gelen, and R. S. Zakariyya, "A divide-and-conquer-method for the synthesis of liveness enforcing supervisors for flexible manufacturing systems," *J. Intell. Manuf.*, vol. 27, no. 5, pp. 1111–1129, Oct. 2016.

[12] Y. Chen, Z. Li, A. Al-Ahmari, N. Wu, and T. Qu, "Deadlock recovery for flexible manufacturing systems modeled with Petri nets," *Inf. Sci.*, vol. 381, pp. 290–303, Mar. 2017.

[13] F. Yang, N. Wu, Y. Qiao, M. Zhou, and Z. Li, "Scheduling of single-arm cluster tools for an atomic layer deposition process with residency time constraints," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 3, pp. 502–516, Mar. 2017.

[14] Y. Hou, N. Wu, M. Zhou, and Z. Li, "Pareto-optimization for scheduling of crude oil operations in refinery via genetic algorithm," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 3, pp. 517–530, Mar. 2017.

[15] Z. Ma, Z. Li, and A. Giua, "Characterization of admissible marking sets in Petri nets with conflicts and synchronizations," *IEEE Trans. Autom. Control*, vol. 62, no. 3, pp. 1329–1341, Mar. 2017.

[16] Z. Ma, Y. Tong, Z. Li, and A. Giua, "Basis marking representation of Petri net reachability spaces and its application to the reachability problem," *IEEE Trans. Autom. Control*, vol. 62, no. 3, pp. 1078–1093, Mar. 2017.

[17] S. Zhang, N. Wu, Z. Li, T. Qu, and C. Li, "Petri net-based approach to short-term scheduling of crude oil operations with less tank requirement," *Inf. Sci.*, vol. 417, pp. 247–261, Nov. 2017.

[18] X. Cong, M. P. Fanti, A. M. Mangini, and Z. Li, "Decentralized diagnosis by Petri nets and integer linear programming," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published, doi: 10.1109/TSMC.2017.2726108.

[19] H. Zhang, L. Feng, N. Wu, and Z. Li, "Integration of learning-based testing and supervisory control for requirements conformance of black-box reactive systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 15, no. 1, pp. 2–15, Jan. 2018, doi: 10.1109/TASE.2017.2693995.

[20] S. Wang, D. You, and M. Zhou, "A necessary and sufficient condition for a resource subset to generate a strict minimal siphon in S^4PR," *IEEE Trans. Autom. Control*, vol. 62, no. 8, pp. 4173–4179, Aug. 2017.

[21] S. Wang, D. You, M. Zhou, and C. Seatzu, "Characterization of admissible marking sets in Petri nets with uncontrollable transitions," *IEEE Trans. Autom. Control*, vol. 61, no. 7, pp. 1953–1958, Jul. 2016.

[22] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Diagnosability of discrete-event systems," *IEEE Trans. Autom. Control*, vol. 40, no. 9, pp. 1555–1575, Sep. 1995.

[23] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. C. Teneketzis, "Failure diagnosis using discrete-event models," *IEEE Trans. Control Syst. Technol.*, vol. 4, no. 2, pp. 105–124, Mar. 1996.

[24] Z. Ma, Z. Li, and A. Giua, "Design of optimal Petri net controllers for disjunctive generalized mutual exclusion constraints," *IEEE Trans. Autom. Control*, vol. 60, no. 7, pp. 1774–1785, Jul. 2015.

[25] Y. Tong, Z. Li, and A. Giua, "On the equivalence of observation structures for Petri net generators," *IEEE Trans. Autom. Control*, vol. 61, no. 9, pp. 2448–2462, Sep. 2016.

[26] T. Ushio, I. Onishi, and K. Okuda, "Fault detection based on Petri net models with faulty behaviors," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, vol. 1. San Diego, CA, USA, Oct. 1998, pp. 113–118.

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

[28] S.-L. Chung, "Diagnosing PN-based models with partial observable transitions," *Int. J. Comput. Integr. Manuf.*, vol. 18, nos. 2–3, pp. 158–169, 2005.

[29] M. P. Cabasino, A. Giua, S. Lafortune, and C. Seatzu, "Diagnosability analysis of unbounded Petri nets," in *Proc. 48th IEEE Conf. Decision Control, 28th Chin. Control Conf.*, Shanghai, China, Dec. 2009, pp. 1267–1272.

[30] M. P. Cabasino, A. Giua, and C. Seatzu, "Diagnosability of bounded Petri nets," in *Proc. 48th IEEE Conf. Decision Control 28th Chin. Control Conf.*, Shanghai, China, Dec. 2009, pp. 1254–1260.

[31] F. Basile, P. Chiacchiot, and G. De Tommasi, "Sufficient conditions for diagnosability of Petri nets," in *Proc. Int. Workshop Discrete Event Syst.*, Gothenburg, Sweden, May 2008, pp. 370–375.

[32] F. Basile, P. Chiacchio, and G. De Tommasi, "On K-diagnosability of Petri nets via integer linear programming," *Automatica*, vol. 48, no. 9, pp. 2047–2058, Sep. 2012.

[33] 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.

[34] D. Lefebvre and C. Delherm, "Diagnosis of DES with Petri net models," *IEEE Trans. Autom. Sci. Eng.*, vol. 4, no. 1, pp. 114–118, Jan. 2007.

[35] D. Lefebvre, "Firing sequences estimation in vector space over Z_3 for ordinary petri nets," *IEEE Trans. Syst., Man, Cybern. A, Syst. Human*, vol. 38, no. 6, pp. 1325–1336, Nov. 2008.

[36] D. Lefebvre, "Fault diagnosis and prognosis with partially observed Petri nets," *IEEE Trans. Syst., Man, Cybern. A, Syst. Human*, vol. 44, no. 10, pp. 1413–1424, Oct. 2014.

[37] D. Lefebvre, *Diagnosis of Discrete Event Systems With Petri Nets*. Rijeka, Croatia: InTech, 2008.

[38] Y. Ru and C. N. Hadjicostis, "Sensor selection for structural observability in discrete event systems modeled by Petri nets," *IEEE Trans. Autom. Control*, vol. 55, no. 8, pp. 1751–1764, Aug. 2010.

[39] C. N. Hadjicostis and G. C. Verghese, "Monitoring discrete event systems using Petri net embeddings," in *Proc. Int. Conf. Appl. Theory Petri Nets*, Williamsburg, VA, USA, Jun. 1999, pp. 188–207.

[40] Y. Wu and C. N. Hadjicostis, "Non-concurrent fault identification in discrete event systems using encoded Petri net states," in *Proc. 41st IEEE Conf. Decision Control*, vol. 4. Las Vegas, NV, USA, Dec. 2002, pp. 4018–4023.

[41] Y. Wu and C. N. Hadjicostis, "Distributed non-concurrent fault identification in discrete event systems," in *Proc. Conf. Comput. Eng. Syst. Appl.*, Lille, France, Jul. 2003.

[42] L. Li, C. N. Hadjicostis, and R. S. Sreenivas, "Designs of bisimilar Petri net controllers with fault tolerance capabilities," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 38, no. 1, pp. 207–217, Jan. 2008.

[43] J. Prock, "A new technique for fault detection using Petri nets," *Automatica*, vol. 27, no. 2, pp. 239–245, Mar. 1991.

[44] Y. Ru and C. N. Hadjicostis, "Fault diagnosis in discrete event systems modeled by partially observed Petri nets," *Discrete Event Dyn. Syst.*, vol. 19, no. 4, pp. 551–575, 2009.

[45] T. Murata, "Petri nets: Properties, analysis and applications," *Proc. IEEE*, vol. 77, no. 4, pp. 541–580, Apr. 1989.

[46] Z. Li, N. Wu, and M. Zhou, "Deadlock control of automated manufacturing systems based on Petri nets—A literature review," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 42, no. 4, pp. 437–462, Jul. 2012.

[47] L. S. Chen and S. Y. Shen, *Basic Theory of Coding*. Beijing, China: Higher Education Press, 2005.

[48] G. H. Zhu, Z. W. Li, N. Q. Wu, and A. M. Al-Ahmari, "Fault identification of discrete event systems modeled by Petri nets with unobservable transitions," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published, doi: 10.1109/TSMC.2017.2762823.

LI YIN received the B.E. degree in remote sensing from Wuhan University, Wuhan, China, in 2007, and the M.S. degree in GIS from the Institute of Remote Sensing Technology Application, CNNC Beijing Research Institute of Uranium Geology, Beijing, in 2014.

He is currently pursuing the Ph.D. degree in system control with the Macau University of Science and Technology, Macau, China. His research interests include discrete-event systems and fault-tolerant dynamic systems with applications to manufacturing.

ZHIWU LI (M'06–SM'07–F'16) received the B.S. degree in mechanical engineering, the M.S. degree in automatic control, and the Ph.D. degree in manufacturing engineering from Xidian University, Xi'an, China, in 1989, 1992, and 1995, respectively.

He joined Xidian University in 1992. Over the past decade, he was a Visiting Professor with the University of Toronto, Technion–Israel Institute of Technology, Martin Luther University of Halle-Wittenberg, Conservatoire National des Arts et Métiers, Meliksah Universitesi, King Saud University, and the University of Cagliari. He is currently with the Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau. His current research interests include Petri net theory and application, the supervisory control of discrete event systems, workflow modeling and analysis, system reconfiguration, game theory, and data and process mining.

Dr. Li is a member of the Discrete Event Systems Technical Committee of the IEEE Systems, Man, and Cybernetics Society, and the IFAC Technical Committee on Discrete Event and Hybrid Systems from 2011 to 2014. He was a recipient of an Alexander von Humboldt Research Grant from the Alexander von Humboldt Foundation, Germany, and Research in Paris, France. He serves as a frequent Reviewer for 60 international journals, including *Automatica* and a number of the IEEE TRANSACTIONS, as well as many international conferences. He is the Founding Chair of the Xi'an Chapter of the IEEE Systems, Man, and Cybernetics Society. He is listed in Marquis Who's Who in the world, 27th Edition, in 2010.

NAIQI WU (M'04–SM'05) received the B.S. degree in electrical engineering from the Huainan Institute of Technology, Huainan, China, in 1982, and the M.S. and Ph.D. degrees in systems engineering from Xi'an Jiaotong University, Xi'an, China, in 1985 and 1988, respectively.

From 1988 to 1995, he was with the Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China, and with Shantou University, Shantou, China, from 1995 to 1998. He moved to the Guangdong University of Technology, Guangzhou, China, in 1998. He joined the Macau University of Science and Technology, Taipa, Macau, in 2013, where he is currently a Professor with the Institute of Systems Engineering. He is the author or co-author of one book, five book chapters, and 130 peer-reviewed journal papers. His research interests include production planning and scheduling, manufacturing system modeling and control, discrete event systems, Petri net theory and applications, intelligent transportation systems, and energy systems. Dr. Wu was an Associate Editor of the IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS, PART C, the IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING, and the IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, and the Editor-in-Chief of *Industrial Engineering Journal*.

SHOUGUANG WANG (M'10–SM'12) received the B.S. degree in computer science from the Changsha University of Science and Technology, Changsha, China, in 2000, and the Ph.D. degree in electrical engineering from Zhejiang University, Hangzhou, China, in 2005.

He joined Zhejiang Gongshang University in 2005, where he is currently a Professor with the School of Information and Electronic Engineering. He was a Visiting Professor with the Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ, USA, from 2011 to 2012. He was the Dean of the Department of Measuring and Control Technology and Instrument from 2011 to 2014. He was a Visiting Professor with the Electrical and Electronic Engineering Department, University of Cagliari, Cagliari, Italy, from 2014 to 2015.

He is the author or co-author of over 50 papers. His main research interests include Petri net theory and application, and the supervisory control of discrete event systems.

TING QU received the B.S. and M.S. degrees in mechanical engineering from Xi'an Jiaotong University, Xi'an, China, in 2001 and 2004, respectively, and the Ph.D. degree in industrial and manufacturing systems engineering from The University of Hong Kong, Hong Kong, in 2008. From 2008 to 2010, he was a Post-Doctoral Research Fellow and then a Research Assistant Professor with the Department of Industrial and Manufacturing Systems Engineering with The University of Hong Kong. He joined the Guangdong University of Technology, Guangzhou, China, in 2010, and he moved to Jinan University (Zhuhai Campus), Zhuhai, China, in 2016, where he is currently a Professor with the School of Electrical and Information Engineering. He has published over 100 technical papers with over half of them in reputable journals. His research interests include IoT-based smart manufacturing systems, logistics and supply chain management, and industrial product/production service systems. He serves as an Associate Editor (Asia) of the *International Journal of Computer Integrated Manufacturing* and an Editorial Board Member of *Industrial Engineering* (Chinese).