# Liveness Enforcing Supervisory Policies Tolerant to Controllability Failures for Discrete-Event Systems modeled by Petri Nets

Arun Raman [a], R. S. Sreenivas [b]

[a] *Department of Computer Science and Automation, Indian Institute of Science, Bangalore, India; Formerly with Coordinated Science Laboratory, and Industrial and Enterprise Systems Engineering, University of Illinois at Urbana-Champaign*

[b] *Coordinated Science Laboratory, and Industrial and Enterprise Systems Engineering, University of Illinois at Urbana-Champaign*

**Abstract**

A *Discrete Event System* (DES) modeled by a *Petri Net* (PN) is *live* if it is possible to *fire* any transition, although not necessarily immediately, from any *marking* that is reachable from the *initial marking*. A *Liveness Enforcing Supervisory Policy* (LESP) for a PN enforces liveness by preventing the firing of a subset of *transitions* called the *controllable transitions*, which correspond to the preventable events in a DES.

In this paper, we consider the existence and synthesis of LESPs for arbitrary PNs in the presence of *faults*, where a subset of controllable transitions become temporarily uncontrollable, for a finite number of event occurrences. Following the formal specification of the fault model, we present a necessary and sufficient condition for the existence of *Fault-Tolerant LESPs* (FT-LESPs) for arbitrary PNs. We show that, even when an LESP is given, the existence of an FT-LESP for an arbitrary PN is undecidable. We then identify a class of PNs for which the existence of FT-LESPs is decidable. We conclude with some suggestions for future research.

*Key words:* Petri-Nets, Supervisory control, Deadlock, Fault-tolerant systems, Discrete-event dynamic systems, Discrete-event systems.

## 1 Introduction

A *Discrete Event System* (DES) is a discrete-state system, where the state changes at discrete-time instants due to the occurrence of events. We consider DES modeled by *Petri nets* (PNs) [1]. PNs are directed bipartite graphs in which the two sets of nodes are referred to as *places* and *transitions*. Places contain *tokens*, which can be interpreted as resources. Tokens move from one set of places to the other due to the *firing* of transitions. The firing of transitions is equivalent to the occurrence of events in the DES context. The arcs connecting a transition to its input places, along with the weights associated with them, encode the conditions that must be satisfied for that transition (event) to be *state-enabled*. Specifically, all input places of a transition must have at least the respective arc-weight-many tokens in them for the transition to be state-enabled. The weights associated with arcs connecting a transition to its output places encode consequences of the firing of the transition. Firing of a transition removes (resp. adds) the respective arc-weight-many tokens from (resp. to) its input (resp. output) places. Thus, the firing of a transition creates a new token distribution at which a different set of transitions can become state-enabled. This process continues as often as necessary. The (non-negative) integer-valued vector denoting the token distribution in the places of a PN denotes the *marking* (state) of the system. PN models are useful for modeling concurrent and asynchronous systems [1]. The execution of a PN is non-deterministic in nature. That is, if at any point more than one transition is enabled, then any of the enabled transitions can be the next to fire. These features of PNs make it useful for modeling situations where several events can occur in parallel, and the order of occurrence of events is not

⋆ This work was supported in part by the Office of Naval Research under Grant N00014-20-1-2249.

*Email addresses:* arunraman@iisc.ac.in (Arun Raman), rsree@illinois.edu (R. S. Sreenivas).

unique.

A PN is said to be live if it is possible to fire any transition, although not necessarily immediately, from any marking that is reachable from the initial marking. If a PN model of a DES is not live, it is of interest to investigate the existence of a *supervisory policy* that can make the supervised-PN live. The supervisory policy enforces liveness by preventing the firing of a subset of *controllable* transitions, which correspond to controllable activities (or events) of the DES. The set of *uncontrollable* transitions represent activities (or events) which cannot be prevented from occurring by the supervisory policy.

Liveness analysis of PN models has gained considerable attention in literature. Reference [2] introduced *monitors* to supervisory control of PNs. References [3, 4] used monitors to enforce liveness in certain classes of PNs. References [5,6] and [7] study the problem of liveness and deadlock avoidance in resource allocation systems (RASs) respectively. Reference [8] proposed a minimally restrictive control policy for flexible manufacturing systems using the vector covering approach. References [9, 10] presented a sufficient condition for liveness for a class of PNs. Reference [11] addresses the design of maximally permissive decentralized supervisors for Petri nets based on generalized mutual exclusion constraints and treats the problem of liveness with the problems of forbidden states in a very general context. Although undecidable for arbitrary PNs ( [12]), the existence of an LESP is decidable for PN structures that belong to certain classes (collectively identified as $\mathcal{H}$-class) of PNs [13–15]. Additional observations on the existence of LESPs for arbitrary PNs can be found in reference [16].

In this paper, we consider the existence and synthesis of LESPs for arbitrary PNs in the presence of *faults*, where a subset of controllable transitions become temporarily uncontrollable, at an arbitrary discrete-time instant, for a finite number of event occurrences. This could be due to a device- or line-fault, where communication between supervisor and plant is temporarily unavailable; or due to the activity of a malicious-user. We assume that the only information the supervisor has about the system is its PN model, and its current marking.

Fault-tolerance in DES modeled by PNs has largely been explored in the context of unreliable resources. Informally stated, resources are modeled as tokens and a resource (token) that was previously available can become unavailable due to faults. The unreliable availability of tokens in a PN model can take a PN from a live state to a deadlocked state. References [17–21] present Fault-tolerant deadlock avoidance algorithm with unreliable resources for assembly and several manufacturing processes respectively. Reference [22] presents a supervisory control framework for deadlock avoidance in sequential RASs with resource outages. References [23] and [24] discuss deadlock avoidance problem in Automated Manufacturing Systems modeled by PNs with unreliable resources. Reference [25] considers faults in controllers that are modeled by PNs. The concept of controllability failures was first studied in [26], where they presented a necessary and sufficient condition for the existence of a supervisor that enforced a desired language specification for a finite automaton model of the DES.

The rest of the paper is organized as follows. In Section 2, we motivate the fault semantics using an example and formally specify the fault model. We also discuss relevant notations and definitions in this section. In Section 3, we present the necessary and sufficient conditions for the existence of a fault-tolerant LESP (FT-LESP) which is essentially dependent on the membership of the initial marking to an appropriately defined set. In Section 4 we prove that the existence of FT-LESPs is undecidable for arbitrary PNs even if an LESP for that initial marking is known. This result is significant as it shows that the complexity in the synthesis of an FT-LESP is not solely inherited from the complexity in the synthesis of an LESP. In Section 5, we prove that the existence of an FT-LESP is decidable for fully controllable ordinary Free Choice PNs. The decidability comes from the fact that the set of initial markings for which an FT-LESP is right-closed for fully controllable ordinary Free Choice PNs. We conclude the paper with some directions for future work in Section 6.

## 2 Notations, Definitions, and Fault-Semantics

We use $\mathcal{N}$ ($\mathcal{N}^+$) to denote the set of non-negative (positive) integers. Given two integer-valued vectors $\mathbf{x}, \mathbf{y} \in \mathcal{N}^k$, we use the notation $\mathbf{x} \geq \mathbf{y}$ if $\mathbf{x}_i \geq \mathbf{y}_i$, and $\max\{\mathbf{x}, \mathbf{y}\}$ to denote the vector whose $i$-th entry is $\max\{\mathbf{x}_i, \mathbf{y}_i\}$, for all $i \in \{1, 2, \ldots k\}$. $T^*$ denotes the set of all possible strings that can be constructed from an alphabet $T$.

A *Petri net structure* $N = (\Pi, T, \Phi, \Gamma)$ is an ordered 4-tuple, where $\Pi = \{p_1, \ldots, p_n\}$ is a set of $n$ *places*, $T = \{t_1, \ldots, t_m\}$ is a collection of $m$ *transitions*, $\Phi \subseteq (\Pi \times T) \cup (T \times \Pi)$ is a set of *arcs*, and $\Gamma : \Phi \to \mathcal{N}^+$ is the *weight* associated with each arc. A PN is said to be *Ordinary* if the weights associated with its arcs is unitary. That is, $\forall \tau \in \Phi, \Gamma(\tau) = 1$. The *marking function* (or the *marking*) of a PN structure $N$ is a function $\mathbf{m} : \Pi \to \mathcal{N}^n$, which identifies the number of *tokens* in each place. If $\mathbf{m}$ is the marking, we use $\mathbf{m}(\pi)$ to denote the token load of a subset of places $\pi \subseteq \Pi$ of the PN. We will use the symbol $N(\mathbf{m}_0)$ to denote a PN structure $N$ along with its initial marking $\mathbf{m}_0$.

The set of transitions in the PN is partitioned into *controllable-* ($T_c \subseteq T$) and *uncontrollable-transitions* ($T_u \subseteq T$). In graphical representations of PNs, the places are represented by circles, transitions by rectangles, and arcs are represented by directed edges. If an arc has a non-unitary weight associated with it, the weight is placed

alongside the arc. For brevity, unitary weights are not explicitly represented in the graphical representation of the PN. The tokens are represented by filled-circles that reside in the circles that represent places. The controllable (uncontrollable) transitions are represented as filled (unfilled) rectangles.

We define the sets ${}^\bullet x := \{y \mid (y,x) \in \Phi\}$ and $x^\bullet := \{y \mid (x,y) \in \Phi\}$. A transition $t \in T$ is said to be *state-enabled* at a marking $\mathbf{m}_i$ if $\forall p \in {}^\bullet t, \mathbf{m}_i(p) \geq \Gamma(p,t)$. The set of state-enabled transitions at marking $\mathbf{m}_i$ is denoted by the symbol $T_e(N, \mathbf{m}_i)$. If $t_j \in T_e(N, \mathbf{m})$, then $\mathbf{m} \geq \mathbf{IN}_j$, which is the $j$-th column of the $n \times m$ *input matrix* $\mathbf{IN}$, defined as $\mathbf{IN}_{i,j} = \Gamma(p,t)$ if $p_i \in {}^\bullet t_j$ or 0 otherwise. The *output matrix* is an $n \times m$ matrix that encodes the firing of an enabled transition: $\mathbf{OUT}_{i,j} = \Gamma(t,p)$ if $p_i \in t_j^\bullet$ or 0 otherwise. The *incidence matrix* $\mathbf{C}$ of the PN $N$ is an $n \times m$ matrix, where $\mathbf{C} = \mathbf{OUT} - \mathbf{IN}$. We use $\mathbf{C}_t$ to denote the column corresponding to transition $t$ in $\mathbf{C}$.

The supervisory policy in the fault-free scenario is denoted by a function $\mathcal{P} : \mathcal{N}^n \times T \to \{0,1\}$ that returns a 0 or 1 for each marking and each transition. We say the transition $t_j$ is *control-enabled* at $\mathbf{m}_i$ if $\mathcal{P}(\mathbf{m}_i, t_j) = 1$ for some marking $\mathbf{m}_i$. A transition has to be state- and control-enabled before it can fire. The firing of a transition $t$ changes the marking $\mathbf{m}_i$ to $\mathbf{m}_{i+1}$ according to $\mathbf{m}_{i+1}(p) = \mathbf{m}_i(p) - \Gamma(p,t) + \Gamma(t,p)$. The supervisory policy does not control-disable any uncontrollable transition, that is, $\forall \mathbf{m}_i \in \mathcal{N}^n, \mathcal{P}(\mathbf{m}_i, t_j) = 1$, if $t_j \in T_u$.

A string of transitions $\sigma = t_1 \dots t_k$, where $t_j \in T$ ($j \in \{1, \dots, k\}$), is said to be a *valid firing string* starting from the marking $\mathbf{m}_i$ if 1) the transitions $t_1 \in T_e(N, \mathbf{m}_i)$, $\mathcal{P}(\mathbf{m}_i, t_1) = 1$, and 2) for $j \in \{1, 2, \dots, k-1\}$, the firing of the transition $t_j$ produces a marking $\mathbf{m}_{i+j}$ and $t_{j+1} \in T_e(N, \mathbf{m}_{i+j})$ and $\mathcal{P}(\mathbf{m}_{i+j}, t_{j+1}) = 1$. If $\mathbf{m}_{i+k}$ results from the firing of $\sigma \in T^*$ from the marking $\mathbf{m}_i$, we represent it as $\mathbf{m}_i \xrightarrow{\sigma} \mathbf{m}_{i+k}$. If $\mathbf{x}(\sigma)$ is an $m$-dimensional vector whose $i$-th component corresponds to the number of occurrences of $t_i$ in a valid string $\sigma$, and if $\mathbf{m}_i \xrightarrow{\sigma} \mathbf{m}_j$, then $\mathbf{m}_j = \mathbf{m}_i + \mathbf{C}\mathbf{x}(\sigma)$.

The set of *reachable markings* under the supervision of $\mathcal{P}$ in $N$ from the initial marking $\mathbf{m}_0$ is denoted by $\mathfrak{R}(N, \mathbf{m}_0, \mathcal{P})$ and is defined as the set of markings generated by all valid firing strings starting with marking $\mathbf{m}_0$. The set of reachable markings under the trivial supervisory policy that enables all transitions is denoted by $\mathfrak{R}(N, \mathbf{m}_0)$.

A PN $N(\mathbf{m}_0)$ is said to be *live* if $\forall t \in T, \forall \mathbf{m}_i \in \mathfrak{R}(N, \mathbf{m}_0), \exists \mathbf{m}_j \in \mathfrak{R}(N, \mathbf{m}_i)$ such that $t \in T_e(N, \mathbf{m}_j)$ (cf. *level 4 liveness*, [1]). A transition $t_k$ is *live* under the supervision of $\mathcal{P}$, if $\forall \mathbf{m}_i \in \mathfrak{R}(N, \mathbf{m}_0, \mathcal{P}), \exists \mathbf{m}_j \in \mathfrak{R}(N, \mathbf{m}_i, \mathcal{P})$ such that $t_k \in T_e(N, \mathbf{m}_j)$ and $\mathcal{P}(\mathbf{m}_j, t_k) = 1$. A policy $\mathcal{P}$ is a *liveness enforcing supervisory policy* (LESP) for $N(\mathbf{m}_0)$ if all transitions in $N(\mathbf{m}_0)$ are live under $\mathcal{P}$. The policy $\mathcal{P}$ is said to be *minimally restrictive* if for every LESP $\widehat{\mathcal{P}} : \mathcal{N}^n \times T \to \{0,1\}$ for $N(\mathbf{m}_0)$, the following condition holds: $\forall \mathbf{m}_i \in \mathcal{N}^n, \forall t \in T, \mathcal{P}(\mathbf{m}_i, t) \geq \widehat{\mathcal{P}}(\mathbf{m}_i, t)$.

The set $\Delta(N) = \{\mathbf{m}_0 : \exists \text{ an LESP for } N(\mathbf{m}_0)\}$ represents the set of initial markings for which there is an LESP for a PN structure $N$. $\Delta(N)$ is *control invariant* with respect to $N$. That is, if $\mathbf{m}_1 \in \Delta(N), t_u \in T_e(N, \mathbf{m}_1) \cap T_u$ and $\mathbf{m}_1 \xrightarrow{t_u} \mathbf{m}_2$ in $N$, then $\mathbf{m}_2 \in \Delta(N)$. There is an LESP for $N(\mathbf{m}_0)$ if and only if $\mathbf{m}_0 \in \Delta(N)$. If $\mathbf{m}_0 \in \Delta(N)$, the LESP that prevents the firing of a controllable transition at any marking when its firing would result in a new marking that is not in $\Delta(N)$, is the minimally restrictive LESP for $N(\mathbf{m}_0)$ [12].

A set of markings $\mathcal{M} \subseteq \mathcal{N}^n$ is said to be *right-closed* if $((\mathbf{m}_1 \in \mathcal{M}) \wedge (\mathbf{m}_2 \geq \mathbf{m}_1) \Rightarrow (\mathbf{m}_2 \in \mathcal{M}))$. A right-closed set, $\mathcal{M}$, is uniquely identified by its finite set of minimal elements denoted by $\min(\mathcal{M})$.

### *2.1 Motivation and Faults Semantics using an Illustrative Example*

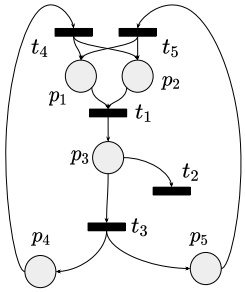


Fig. 1. Petri Net $N_i$

Consider the fully controllable PN $N_i$ shown in Figure 1. $\Delta(N_i)$ is right-closed with minimal elements $\{(1\ 1\ 0\ 0\ 0)^T, (0\ 0\ 1\ 0\ 0)^T, (0\ 0\ 0\ 1\ 0)^T, (0\ 0\ 0\ 0\ 1)^T\}$. Suppose an extraneous fault-event occurs at $(0\ 0\ 1\ 0\ 0)^T \in \Delta(N_i)$ that renders transition $t_2$ (temporarily) uncontrollable. That is, the supervisory policy cannot prevent it from firing. Then the affected transition $t_2$ can fire at $(0\ 0\ 1\ 0\ 0)^T$ and the resulting marking is not in $\Delta(N_i)$. The objective of this paper is to analyse the existence and synthesis of LESPs tolerant to such *controllability failures*.

Formally, we use the term *fault-event*, denoted by $\phi$, to refer to an extraneous discrete-event where an arbitrary subset of controllable transitions, $T_f \subseteq T_c$, becomes temporarily uncontrollable. The fault-event $\phi$ is followed (not necessarily immediately) by an extraneous *rectification-event*, denoted by $\rho$, where all transitions in $T_f \subseteq T_c$ become controllable again. That is, between the fault- and the rectification-event, the set of uncontrollable (resp. controllable) events is effectively $T_f \cup T_u$ (resp. $T_c - T_f$). Before the fault-event, and after the rectification-event, the set of uncontrollable (resp. controllable) events is $T_u$ (resp. $T_c$).

Coming back to the PN in figure 1, we observed that the firing of $t_2$ from $(0\ 0\ 1\ 0\ 0)^T$ resulted in a marking that is not in $\Delta(N_i)$. An obvious way of making the PN tolerant to fault is to constrain the marking of the PN to a subset of $\Delta(N_i)$ so that when a transition affected by fault does fire, the resulting marking is still inside $\Delta(N_i)$. In addition, that subset of $\Delta(N_i)$ should also satisfy the properties of $\Delta(N_i)$ so that the supervisory policy that constrains the marking to it enforces liveness. Consider the right-closed set $\widehat{\Delta}(N_i) \subseteq \Delta(N_i)$ with minimal elements $\{(2\ 2\ 0\ 0\ 0)^T, (0\ 0\ 2\ 0\ 0)^T, (0\ 0\ 0\ 2\ 0)^T, (0\ 0\ 0\ 0\ 2)^T, (1\ 1\ 1\ 0\ 0)^T, (1\ 1\ 0\ 1\ 0)^T, (1\ 1\ 0\ 0\ 1)^T, (0\ 0\ 1\ 1\ 0)^T, (0\ 0\ 1\ 0\ 1)^T, (0\ 0\ 0\ 1\ 1)^T\}$. Consider the policy $\widehat{\mathcal{P}}$ defined such that for any controllable transition $t_c \in T_c$ at any marking $\mathbf{m}_1 \in \widehat{\Delta}(N_i)$: $(\widehat{\mathcal{P}}(\mathbf{m}_1, t_c) = 0) \Leftrightarrow ((\mathbf{m}_1 \xrightarrow{t_c} \mathbf{m}_2) \wedge (\mathbf{m}_2 \notin \widehat{\Delta}(N_i)))$. $\widehat{\mathcal{P}}$ is an LESP for $N_i(\mathbf{m}_0)$ for any $\mathbf{m}_0 \in \widehat{\Delta}(N_i)$. It follows that, $\widehat{\mathcal{P}}(\mathbf{m}_0, t_2) = 0$ for $\mathbf{m}_0 = (0\ 0\ 2\ 0\ 0)^T$; and $\forall \mathbf{m} \in \widehat{\Delta}(N_i), \widehat{\mathcal{P}}(\mathbf{m}, t_4) = 1$ (cf. [27] for details).

We illustrate the detection semantics next. Suppose the fault-event $\phi$ occurs at $\mathbf{m}_0$, rendering the transition in the set $T_f = \{t_4\}$ to be uncontrollable. A fault-event can be detected if a controllable transition that was disabled by the LESP fired. But since the LESP $\widehat{\mathcal{P}}$ does not disable the transition $t_4$ for any marking in $\widehat{\Delta}(N_i)$, this fault will not be detected. In contrast, let $T_f = \{t_2, t_4\}$, and suppose $(0\ 0\ 2\ 0\ 0)^T \xrightarrow{\phi t_2} (0\ 0\ 1\ 0\ 0)^T$ under the supervision of $\widehat{\mathcal{P}}$. If the supervisor stores information about its past actions, then the fault can be detected by comparing the transition that fired to those that were enabled by the supervisor. However, we do not assume that the supervisor stores information about its past actions and consider a general setting in which the fault-event has to be inferred from *only* the current marking of the PN. The results in the paper are independent of how the current marking is determined. For this example, the firing of a transition affected by the fault can be detected by observing that the current marking $(0\ 0\ 1\ 0\ 0)^T$ no longer belongs to $\widehat{\Delta}(N_i)$.

Due to cost considerations, a fault may not be rectified immediately after detection. We quantify the tolerance of $N(\mathbf{m}_0)$ to a fault-event by associating a positive integer $k_r$ with it; where $k_r$ is the mandatory number of detected firings of transitions that are affected by the fault before it is rectified. Under these semantics, the fault-free scenario is represented as the case when $k_r = 0$. We can ask two kinds of questions related to $k_r$: (i) given an initial marking and a value of $k_r$, is there an LESP that is tolerant to controllability faults?, and (ii) what is the maximum value of $k_r$ for which an LESP tolerant to controllability faults can be synthesized for a given initial marking.

Continuing with the example for the case when $T_f = \{t_2, t_4\}$, if $k_r = 1$ then the fault *will* be rectified *immediately* at the marking $(0\ 0\ 1\ 0\ 0)^T$, $(0\ 0\ 2\ 0\ 0)^T \xrightarrow{\phi t_2 \rho} (0\ 0\ 1\ 0\ 0)^T$, and all transitions in $T_c$ will be controllable afterwards. No other transition in $N_i$ can fire at the marking $(0\ 0\ 1\ 0\ 0)^T$ before the occurrence of the rectification-event $\rho$. If $k_r > 1$, the rectification-event cannot occur at marking $(0\ 0\ 1\ 0\ 0)^T$, and $(0\ 0\ 2\ 0\ 0)^T \xrightarrow{\phi t_2 t_2} (0\ 0\ 0\ 0\ 0)^T$ under the supervision of $\widehat{\mathcal{P}}$. Thus, we can conclude that for $N_i(\mathbf{m}_0)$ where $\mathbf{m}_0 \in \widehat{\Delta}(N_i)$, the LESP $\widehat{\mathcal{P}}$ is tolerant to a fault-event if $k_r \leq 1$.

Consider the right-closed set $\widetilde{\Delta}(N_i) \subseteq \Delta(N_i)$ with minimal elements $\{(3\ 3\ 0\ 0\ 0)^T, (0\ 0\ 3\ 0\ 0)^T, (0\ 0\ 0\ 3\ 0)^T, (0\ 0\ 0\ 0\ 3)^T, (2\ 2\ 1\ 0\ 0)^T, (2\ 2\ 0\ 1\ 0)^T, (2\ 2\ 0\ 0\ 1)^T, (1\ 1\ 2\ 0\ 0)^T, (1\ 1\ 0\ 2\ 0)^T, (1\ 1\ 0\ 0\ 2)^T, (0\ 0\ 2\ 1\ 0)^T, (0\ 0\ 2\ 0\ 1)^T, (0\ 0\ 1\ 2\ 0)^T, (0\ 0\ 1\ 0\ 2)^T, (0\ 0\ 0\ 2\ 1)^T, (0\ 0\ 0\ 1\ 2)^T, (1\ 1\ 1\ 1\ 0)^T, (1\ 1\ 1\ 0\ 1)^T, (1\ 1\ 1\ 1\ 0)^T, (1\ 1\ 0\ 1\ 1)^T, (1\ 1\ 1\ 0\ 1)^T, (1\ 1\ 0\ 1\ 1)^T, (0\ 0\ 1\ 1\ 1)^T\}$. It follows that $\widetilde{\Delta}(N_i) \subset \widehat{\Delta}(N_i) \subset \Delta(N_i)$. The policy $\widetilde{\mathcal{P}}$ that ensures all markings, that are reachable under supervision, are within the set $\widetilde{\Delta}(N_i)$ is an LESP for $N(\mathbf{m}_0)$ for any $\mathbf{m}_0 \in \widetilde{\Delta}(N_i)$. Following previous discussion, we can claim that for $N_i(\mathbf{m}_0)$ where $\mathbf{m}_0 \in \widetilde{\Delta}(N_i)$, the LESP $\widetilde{\mathcal{P}}$ is tolerant to a single-fault-event if $k_r \leq 2$.

To summarize the detection method for the example, if the initial marking of $N_i$ is in $\widetilde{\Delta}(N_i)$, then the first firing of a transition affected by the fault will be detected when the current marking is in the set $\widehat{\Delta}(N) - \widetilde{\Delta}(N)$. The second firing of a transition affected by the fault will be detected when the current marking is in $\Delta(N_i) - \widehat{\Delta}(N_i)$. If $k_r = 2$, then the fault will be immediately rectified upon reaching $\Delta(N_i) - \widehat{\Delta}(N_i)$ and the PN can be supervised for liveness as in the fault-free case. In Section 3, we define a sequence of nested sets and use membership to them to detect firings of affected transitions by using only the current marking of the PN. Under the semantics enunciated earlier, the rectification-event $\rho$ occurs *immediately after* the $k_r$-th firing of affected transitions is detected.

### *2.2 Extension of Notations for faults scenarios*

A *supervisory policy*, in the context of faults, $\mathcal{P}_f : \mathcal{N}^n \times T \times \{0, \ldots, k_r\} \to \{0, 1\}$, returns a 0 or 1 for each marking, each transition, and the observed number of (unintended) firings of controllable transitions affected by the fault. It permits the firing of transition $t_j$ at marking $\mathbf{m}_i$ when $k_d$-many $(0 \leq k_d \leq k_r)$ unintended firings of controllable transitions have been detected, if and only if $\mathcal{P}_f(\mathbf{m}_i, t_j, k_d) = 1$. We require $\mathcal{P}_f(\mathbf{m}_i, t_u, k_d) = 1$ $\forall t_u \in T_u$, $\forall k_d$.

For a given $T_f \subseteq T_c$, a state-enabled transition $t \in T_e(N, \mathbf{m}_i)$ *can fire* under the supervision of $\mathcal{P}_f$ at marking $\mathbf{m}_i$ when $k_d$-many $(0 \leq k_d \leq k_r)$ unintended firings

of controllable transitions have been detected, if either (1) $\mathcal{P}_f(\mathbf{m}_i, t, k_d) = 1$; or (2) $0 < k_d < k_r$, and $t \in T_f$.

A string of transitions $\sigma = t_1 \dots t_k$, where $t_j \in T$ ($j \in \{1, \dots, k\}$), is said to be a *valid firing string in the presence of controllability faults*, starting from the marking $\mathbf{m}_i$, after $k_d$-many ($0 \leq k_d \leq k_r$) unintended firings of controllable transitions have been detected thus far, if (1) the transition $t_1 \in T_e(N, \mathbf{m}_i)$ can fire at the marking $\mathbf{m}_i$, and (2) for $j \in \{1, \dots, k\}$, the firing of the transition $t_j$ produces a marking $\mathbf{m}_{i+j}$, $t_{j+1} \in T_e(N, \mathbf{m}_{i+j})$ and the transition $t_{j+1}$ can fire at the marking $\mathbf{m}_{i+j}$. We denote this as $\mathbf{m}_i \xrightarrow{\sigma} \mathbf{m}_{i+k}$ under the supervision of $\mathcal{P}_f$. We say $\sigma$ is a *valid firing string of transitions under faults* from marking $\mathbf{m}_i$ under the supervision of $\mathcal{P}_f$.

The set $\mathfrak{R}_\phi(N, \mathbf{m}_0, \mathcal{P}_f, k_r, T_f)$ denotes the set of markings generated by all valid firing strings of transitions from $\mathbf{m}_0$ under the supervision of $\mathcal{P}_f$ in $N$, under the influence of a fault $\phi$ that will be rectified immediately after $k_r$-many unintended firings of controllable transitions in the set $T_f \subseteq T_c$ are detected. Consequently, $\forall k_r^2 \leq k_r^1$, $\forall T_f^2 \subseteq T_f^1 \subseteq T_c$, $\mathfrak{R}_\phi\ (N, \mathbf{m}_i, \mathcal{P}_f,\ k_r^2, T_f^2) \subseteq \mathfrak{R}_\phi(N, \mathbf{m}_i, \mathcal{P}_f, k_r^1, T_f^1) \subseteq \mathfrak{R}(N, \mathbf{m}_i)$, where we assume that $\mathcal{P}_f$ is defined for $k_r^1$.

For the example in Figure 1 with initial marking $(1\ 1\ 0\ 0\ 0)^T$ consider the supervisory policy $\mathcal{P}$ that constraints the marking to $\Delta(N_i)$ irrespective of faults. Then $\mathfrak{R}_\phi(N_i, (1\ 1\ 0\ 0\ 0)^T, \mathcal{P}, 1, \{t_2\}) = \{(0\ 0\ 0\ 0\ 0)\} \cup \mathfrak{R}(N_i, (1\ 1\ 0\ 0\ 0)^T, \mathcal{P})$. Next, consider the initial marking $(0\ 0\ 2\ 0\ 0)^T$ with $k_r = 1$ and the supervisory policy $\widehat{\mathcal{P}}$ which constrains the PN marking to $\widehat{\Delta}(N_i)$ till the first unintended firing of $t_2$ is detected, and to $\Delta(N_i)$ afterwards. For this case, $\mathfrak{R}_\phi(N_i, (0\ 0\ 2\ 0\ 0)^T, \widehat{\mathcal{P}}, 1, \{t_2\}) = \mathfrak{R}(N_i, (0\ 0\ 2\ 0\ 0)^T, \mathcal{P})$. Note that $\mathfrak{R}(N_i, (0\ 0\ 2\ 0\ 0)^T, \mathcal{P})$ is the set of reachable markings *in the absence of faults* under the supervision of $\mathcal{P}$ defined above. On the other hand, since $\widehat{\Delta}(N_i) \subset \Delta(N_i)$, we have $\mathfrak{R}(N_i, (0\ 0\ 2\ 0\ 0)^T, \widehat{\mathcal{P}}) \subset \mathfrak{R}(N_i, (0\ 0\ 2\ 0\ 0)^T, \mathcal{P})$.

**Definition 1.** *A supervisory policy $\mathcal{P}_f : \mathcal{N}^n \times T \times \{0, \dots, k_r\} \to \{0, 1\}$, is said to be a Fault Tolerant Liveness Enforcing Supervisory Policy (FT-LESP) for a PN $N(\mathbf{m}_0)$ if $\forall t \in T, \forall T_f \subseteq T_c, \forall \mathbf{m}_i \in \mathfrak{R}_\phi(N, \mathbf{m}_0, \mathcal{P}_f, k_r, T_f)$, $\exists \mathbf{m}_j \in \mathfrak{R}_\phi(N, \mathbf{m}_i, \mathcal{P}_f, k_r - k_d, T_f)$ such that $\mathcal{P}_f(\mathbf{m}_j, t, k_d) = 1$ and $t \in T_e(N, \mathbf{m}_j)$, where $k_d$ denotes the number of unintended firings of controllable transitions detected when the marking $\mathbf{m}_i$ is reached in the PN $N(\mathbf{m}_0)$ under the supervision of $\mathcal{P}_f$.*

Since a supervisory policy in the context of faults, $\mathcal{P}_f : \mathcal{N}^n \times T \times \{0, \dots, k_r\} \to \{0, 1\}$, can be effectively described by $(k_r + 1)$-many fault-free supervisory policies $\{\mathcal{P}_i : \mathcal{N}^n \times T \to \{0, 1\}\}_{i=0}^{k_r}$, where $\mathcal{P}_f(\mathbf{m}, t, i) = \mathcal{P}_i(\mathbf{m}, t)$, where $0 \leq i \leq k_r$, an FT-LESP can be represented by $(k_r + 1)$-many fault-free LESPs. Corollary 1 follows directly from this observation.

**Corollary 1.** *($\exists$ FT-LESP for $N(\mathbf{m}_0)$) $\Rightarrow$ ($\exists$ an LESP for $N(\mathbf{m}_0)$).*

An FT-LESP $\mathcal{P}_f : \mathcal{N}^n \times T \times \{0, \dots, k_r\} \to \{0, 1\}$ is said to be *minimally restrictive* for $N(\mathbf{m}_0)$ if, for $0 \leq k_d \leq k_r$, every FT-LESP $\widehat{\mathcal{P}}_f : \mathcal{N}^n \times T \times \{0, \dots, k_r\} \to \{0, 1\}$ satisfies the following condition : $\forall \mathbf{m}_i \in \mathcal{N}^n, \forall t \in T, \mathcal{P}_f(\mathbf{m}_i, t, k_d) \geq \widehat{\mathcal{P}}_f(\mathbf{m}_i, t, k_d)$. That is, if the FT-LESP $\mathcal{P}_f$ prevents the firing of a transition $t$ at a marking $\mathbf{m}_i$ after $k_d$-many fault have been detected, then *all* FT-LESPs would do the same.

### *2.3 Other Notations and Definitions*

A PN structure is *free-choice* (FC) if $\forall p \in \Pi$, $card(p^\bullet) > 1 \Rightarrow {}^\bullet(p^\bullet) = \{p\}$, where $card(\bullet)$ denotes the cardinality of the set argument. In other words, a PN structure is free-choice if and only if an arc from a place to a transition is either the unique output arc from that place, or, is the unique input arc to the transition. $\Delta(N)$ is right-closed for an FCPN and the existence of an LESP for $N(\mathbf{m}_0)$ is decidable [13].

A *decision-problem*, that is posed as a "*yes*" or "*no*" question for each input, is *decidable* (resp. *undecidable*) if there exists (resp. does not exist) a single algorithm that correctly answers "*yes*" or "*no*" to all possible inputs. It is *semi-decidable* if there exists a single algorithm that will always correctly answer "*yes*", but does not answer at all when the answer is "*no*". Every decision-problem has an associated *complementary* decision-problem. The answer to the complementary problem is "*yes*" if and only if the answer to the original decision problem is "*no*". A decision-problem is decidable if and only if the decision-problem *and* its complement, are semi-decidable (cf. section 1.2.2, [28]). "Is $\mathbf{m}_0 \in \Delta(N)$?" and "Is $\mathbf{m}_0 \notin \Delta(N)$?" are not semi-decidable [13].

## 3 Preliminary Results

Recall that $\Delta(N)$ is the set of initial markings for which a fault-free LESP exists for a PN structure $N$. In the discussion following Definition 1 we noted that an FT-LESP acts like a fault-free LESP before and after every detection of firing of transitions affected by the fault-event. Therefore, the marking before and after every detection of firing of affected transitions should belong to a set which satisfies the properties of $\Delta(N)$. Additionally, while discussing the example in Figure 1, we saw that these sets have a nested structure ($\widetilde{\Delta}(N_i) \subset \widehat{\Delta}(N_i) \subset \Delta(N_i)$ for the example). Motivated by these observations we now define, $\Delta_{k_r}(N)$, the set of initial markings for which an FT-LESP exists.

**Definition 2.** *Let $\Delta_0(N) = \Delta(N)$. Then $\Delta_k(N) \subseteq \Delta(N)$, $k \in \mathcal{N}^+$, is the set of all initial markings that satisfies the following conditions:*

*(a) It is control-invariant with respect to $N$.*
*(b) $\forall \mathbf{m}_1 \in \Delta_k(N), \exists \mathbf{m}_2, \mathbf{m}_3 \in \Delta_k(N), \exists$ a valid firing string $\sigma = \sigma_1\sigma_2$ in $N$ such that $\mathbf{m}_1 \xrightarrow{\sigma_1} \mathbf{m}_2 \xrightarrow{\sigma_2} \mathbf{m}_3, \mathbf{m}_3 \geq \mathbf{m}_2$, all transitions appear at least once in $\sigma_2$, and $\forall \sigma_3 \in pr(\sigma_1\sigma_2)$, $(\mathbf{m}_1 \xrightarrow{\sigma_3} \mathbf{m}_4) \Rightarrow (\mathbf{m}_4 \in \Delta_k(N))$. Here $pr(\bullet)$ denotes the prefix of the string argument.*
*(c) $\forall \mathbf{m}_1 \in \Delta_k(N)$, $\forall t \in T$: $(\mathbf{m}_1 \xrightarrow{t} \mathbf{m}_2) \Rightarrow (\mathbf{m}_2 \in \Delta_j(N)$, where $j \geq k-1)$.*

Properties (a) and (b) in Definition 2 are the properties of $\Delta(N)$ (Theorem 5.1 in [12]). Property (c) ensures that the marking remains in a set that satisfies the properties of $\Delta(N)$ before and after the detection of firing of transitions affected by faults. $\widehat{\Delta}(N_i)$ (respectively $\widetilde{\Delta}(N_i)$) as discussed for the example in the previous section corresponds to $\Delta_1(N_i)$ ($\Delta_2(N_i)$) in the proposed framework.

Suppose the number of firings of transitions affected by the fault detected till now is $k_d$, and the current marking $\mathbf{m} \in \Delta_{k_r-k_d}(N)$. As $\Delta_k(N)$ ($k = \{0, \ldots, k_r\}$) is control-invariant, only the firing of controllable transitions can take the marking outside $\Delta_{k_r-k_d}(N)$. Consider the supervisory policy $\mathcal{P}_f$ where $\forall \mathbf{m} \in \mathcal{N}^n$

(1) $\forall t \in T_u$: $\mathcal{P}_f(\mathbf{m}, t, k_d) = 1$.
(2) $\forall t \in T_c$: $(\mathcal{P}_f(\mathbf{m}, t, k_d) = 1) \Leftrightarrow (\mathbf{m} \xrightarrow{t} \widetilde{\mathbf{m}}$ such that $\widetilde{\mathbf{m}} \in \Delta_{k_r-k_d}(N))$.

Due to Properties (a) and (b) in Definition 2, $\mathcal{P}_f$ enforces liveness. Since $\mathcal{P}_f$ disables any controllable transition that takes the marking outside $\Delta_{k_r-k_d}(N)$, if the current marking of the supervised PN does not belong to $\Delta_{k_r-k_d}(N)$, then it must be because of the firing of a (controllable) transition affected by fault. This is the central idea for fault detection. For every marking reached under the supervision of $\mathcal{P}_f$ from $\mathbf{m} \in \Delta_{k_r-k_d}(N)$, the supervisor first tests if $\mathbf{m} \in \Delta_{k_r-k_d}(N)$. If $\mathbf{m} \notin \Delta_{k_r-k_d}(N)$, then by Property (c) of Definition 2, $\mathbf{m} \in \Delta_{k_r-k_d-1}(N)$. At this point, the supervisor detects the firing of an affected transition, updates $k_d \leftarrow k_d + 1$, and continues with the same policy as explicated above. We formalize these observations in the next theorem.

**Theorem 1.** $(\mathbf{m}_0 \in \Delta_{k_r}(N)) \Leftrightarrow (\exists$ *an FT-LESP for* $N(\mathbf{m}_0))$.

*Proof.* ($\Rightarrow$) Assume $\mathbf{m}_0 \in \Delta_{k_r}(N)$, and the fault-event $\phi$ renders $T_f \subseteq T_c$ to be temporarily uncontrollable when it occurs immediately after some marking $\mathbf{m} \in \mathfrak{R}_\phi(N, \mathbf{m}_0, \mathcal{P}_f, k_r, T_f)$ is reached. It follows that $k_d = 0$ when the the fault-event occurs. If the policy $\mathcal{P}_f$ ensures the marking of the supervised PN never leaves $\Delta_{k_r}(N)$, then $\mathbf{m} \in \Delta_{k_r}(N)$, as well. Properties (a) and (b) in Definition 2 imply that $\mathcal{P}_f$ is an LESP (by Theorem 5.1 in [12]). We use property (c) in Definition 2 to prove robustness against faults. Consider a controllable transition $t_c \in T_e(N, \mathbf{m})$, and let $\mathbf{m} \xrightarrow{\phi t_c} \overline{\mathbf{m}}$. There are three possible cases:

(1) $t_c \notin T_f$, that is $t_c$ is not affected by the fault-event. Then $t_c$ will fire if and only if $\mathcal{P}_f(\mathbf{m}, t_c, 0) = 1$, and we have $\overline{\mathbf{m}} \in \Delta_{k_r}(N)$. $k_d$ remains 0.
(2) $(t_c \in T_f) \wedge (\mathcal{P}_f(\mathbf{m}, t_c, 0) = 1)$, that is $t_c$ is affected by the fault-event but its firing is as intended by the $\mathcal{P}_f$. We have $\overline{\mathbf{m}} \in \Delta_{k_r}(N)$. $k_d$ remains 0.
(3) $(t_c \in T_f) \wedge (\mathcal{P}_f(\mathbf{m}, t_c, 0) = 0)$. Following Property (c), we have $\overline{\mathbf{m}} \in \Delta_{k_r-1}(N)$ and $k_d = 1$.

That there exists an FT-LESP for $N(\mathbf{m}_0)$ follows by replacing $\mathbf{m}$ by $\overline{\mathbf{m}}$, and repeating the above argument by induction over $k_r$-many unintended firings of $t_f \in T_f$ (that is for $k_d$ from 1 to $k_r$).

($\Leftarrow$) Assume there exists an FT-LESP $\mathcal{P}_f$ for $N(\mathbf{m}_0)$, and the fault-event $\phi$ renders $T_f \subseteq T_c$ to be temporarily uncontrollable when it occurs immediately after some marking that is reached under supervision. Then $\mathbf{m}_0 \in S_{k_r}$, where $S_{k_r} = \mathfrak{R}_\phi(N, \mathbf{m}_0, \mathcal{P}_f, k_r, T_f)$. By Corollary 1, $\exists$ an LESP for $N(\mathbf{m}_0)$. By Theorem 5.1 in [12], $S_{k_r}$ satisfies Properties (a) and (b) in Definition 2. Since there exists an FT-LESP for $N(\mathbf{m}_0)$, from all $\mathbf{m} \in \mathfrak{R}_\phi(N, \mathbf{m}_0, \mathcal{P}_f, k_r, T_f)$, the firing of every string of transitions in which unintended firings of affected transitions $t_f \in T_f$ appear less than or equal to $k_r$-many times should result in a marking that is in $\Delta(N)$. Specifically, $\forall \mathbf{m} \in S_{k_r}$, $\mathbf{m} \xrightarrow{\phi t_f} \mathbf{m}_1$. Then $\mathbf{m}_1 \in S_{k_r-1}$ for some set $S_{k_r-1}$ such that $\forall \mathbf{m}' \in S_{k_r-1}$:

(1) firing of every string of transitions in which unintended firings of affected transitions $t_f \in T_f$ appear less than or equal to $(k_r - 1)$-many times results in a marking that is in $\Delta(N)$; and
(2) $N(\mathbf{m}')$ can be made live— for the case when none of the $t_f \in T_f$ ever fire when $\mathcal{P}_f(\mathbf{m}', t_f, 1) = 0$.

Therefore, $S_{k_r-1}$ also satisfies Properties (a) and (b) in Definition 2. The rest of the proof follows by induction by replacing $k_r$ by $(k_r - 1)$ in the above argument. The induction will have $k_r$ steps with the last iteration resulting in a marking in $\Delta(N)$. Therefore, $S_{k_r} \subseteq \Delta_{k_r}(N)$ and $S_{k_r-1} \subseteq \Delta_{k_r-1}(N)$. Hence $\mathbf{m}_0 \in \Delta_{k_r}(N)$. □

We get the following result as a direct consequence of Corollary 1 and Theorem 1.

**Corollary 2.** *Given a PN $N(\mathbf{m}_0)$ for which an FT-LESP exists, $\forall k \in \mathcal{N}$, $\Delta_{k+1} \subseteq \Delta_k$.*

Another consequence of Theorem 1 is that for a given marking $\mathbf{m}$ and a value of $k_d$, there exists an FT-LESP for $N(\mathbf{m})$ if and only if $\mathbf{m} \in \Delta_{k_r-k_d}(N)$. That is, any FT-LESP must *at least* disable any controllable transition whose firing takes the PN marking outside $\Delta_{k_r-k_d}(N)$. We get the following corollary as a consequence of this observation:

**Corollary 3.** *Suppose* $\mathbf{m}_0 \in \Delta_{k_r}(N)$. *Then* $\mathcal{P}_f$ *is the minimally restrictive FT-LESP for* $N(\mathbf{m}_0)$.

## 4 FT-LESP for Arbitrary Partially Controlled PNs

Theorems 3.1 and 3.2 in [13] prove that neither the existence nor the nonexistence of an LESP for an arbitrary PN is semidecidable. In light of this theorem, we expect that the existence of an FT-LESP for an arbitrary PN is also undecidable. We prove a stronger result in this section. We work our way through a construction and some related observations to establish that despite being given an LESP for $N(\mathbf{m}_0)$, the existence of an FT-LESP for $N(\mathbf{m}_0)$ is undecidable for an arbitrary PN. That is, given $\mathbf{m}_0 \in \Delta(N)$, "Is $\mathbf{m}_0 \in \Delta_{k_r}(N)$?" is still undecidable. This result is significant because it proves that the complexity in the synthesis of an FT-LESP is not solely inherited from the complexity in the synthesis of an LESP.

We construct a PN $N$ from a PN $\widehat{N}$, and the PN $\widetilde{N}$ which was first discussed in [12]. The construction is shown in Figure 2. $\widehat{N}$ is exactly as constructed in the figure with places $\{p_i\}_{i=1}^{2}$ and transitions $\{t_j\}_{j=1}^{3}$. Its reachability graph is shown in Figure 3. $\widetilde{N}$ is constructed by connecting two arbitrary petri nets $N_l = (\Pi_l, T_l, \Phi_l, \Gamma_l)$ $(l = 1, 2)$. $\Pi_l = \{p_1^l, p_2^l, \ldots, p_n^l\}$ and $T_l = \{t_1^l, t_2^l, \ldots, t_{m_l}^l\}$ $(l = 1, 2)$ is the set of places and transitions respectively. Note that $card(\Pi_1) = card(\Pi_2) = n$. All transitions in $N_1$ ($N_2$) are uncontrollable (resp. controllable). Note that the arcs for $N_1$ and $N_2$ are not drawn in Figure 2 since we do not stipulate any particular structure. $\widetilde{N} = (\widetilde{\Pi}, \widetilde{T}, \widetilde{\Phi}, \widetilde{\Gamma})$ is constructed as follows:

- $\widetilde{\Pi} \leftarrow \Pi_1 \cup \Pi_2$, $\widetilde{T} \leftarrow T_1 \cup T_2$ and $\widetilde{\Phi} \leftarrow \Phi_1 \cup \Phi_2$.
- Create $2n + 4$ new and unused places such that $\widetilde{\Pi} \leftarrow \widetilde{\Pi} \cup \{\pi_i\}_{i=1}^{n+4} \cup \{\widetilde{\pi}_j\}_{j=3}^{n+2}$.
- Create $5n+4$ new and unused transitions: $\widetilde{T} \leftarrow \widetilde{T} \cup \{\tau_i\}_{i=1}^{n+4} \cup \{\hat{\tau}_j^i | i \in \{1,2\}, j \in \{1,2,\ldots,n\}\} \cup \{\widetilde{\tau}_j^i | i \in \{1,2\}, j \in \{1,2,\ldots,n\}\}$.
- $\forall t \in T_1$, modify $\widetilde{\Phi}$ as $\widetilde{\Phi} \leftarrow \widetilde{\Phi} \cup \{(\pi_1, t), (t, \pi_1)\}$. That is, $\pi_1$ self loops on all transitions of $\widetilde{N}$ that originally belonged to $N_1$.
- $\forall t \in T_2$, modify $\widetilde{\Phi}$ as $\widetilde{\Phi} \leftarrow \widetilde{\Phi} \cup \{(\pi_2, t), (t, \pi_2)\}$. That is, $\pi_2$ self loops on all transitions of $\widetilde{N}$ that originally belonged to $N_2$.
- Modify $\widetilde{\Phi}$ as $\widetilde{\Phi} \leftarrow \widetilde{\Phi} \cup \{(\pi_i, \tau_i), (\tau_i, \pi_{i+1})\}_{i=1}^{n+3} \cup \{(\pi_{n+4}, \tau_{n+4})\}$.
- $\forall p \in \widetilde{\Pi}$, modify $\widetilde{\Phi}$ as $\widetilde{\Phi} \leftarrow \widetilde{\Phi} \cup \{(\tau_{n+4}, p)\}$. That is every place of $\widetilde{N}$ is an output of $\tau_{n+4}$.
- $\forall i \in \{1, 2, \ldots, n\}$, modify $\widetilde{\Phi}$ as $\widetilde{\Phi} \leftarrow \widetilde{\Phi} \cup \{(\pi_{i+2}, \hat{\tau}_i^1), (p_i^1, \hat{\tau}_i^1), (\hat{\tau}_i^1, \hat{\pi}_{i+3}), (\hat{\pi}_{i+3}, \hat{\tau}_i^2), (p_i^2, \hat{\tau}_i^2), (\hat{\tau}_i^2, \pi_{i+2})\}$.
- $\forall i \in \{1, 2\}, \forall j \in \{1, 2, \ldots n\}$, modify $\widetilde{\Phi}$ as $\widetilde{\Phi} \leftarrow \widetilde{\Phi} \cup \{(\pi_{n+3}, \widetilde{\tau}_j^i), (p_j^i, \widetilde{\tau}_j^i)\}$.

Weights of all arcs in $\widetilde{\Phi} - \Phi_1 - \Phi_2$ is one. We use $\mathbf{m}_i^0 \in \mathcal{N}^n$ to represent an arbitrary pair of initial markings of $N_i$, $i = \{1, 2\}$. The initial marking of $\widetilde{N}$, $\widetilde{\mathbf{m}}_0$, is such that $\widetilde{\mathbf{m}}_0(\pi_1) = 1$, $\widetilde{\mathbf{m}}_0(\Pi_1) = \mathbf{m}_1^0$, $\widetilde{\mathbf{m}}_0(\Pi_2) = \mathbf{m}_2^0$ and all other places have zero tokens. Theorem 5.3 of [12] provides a detailed proof that $\widetilde{N}$ has an LESP if and only if $\mathfrak{R}(N_1, \mathbf{m}_1^0) \subseteq \mathfrak{R}(N_2, \mathbf{m}_2^0)$. We briefly discuss the idea of the proof for completeness. Liveness of transition $\tau_1$ can be guaranteed iff the token load of $\pi_1$ is repeatedly replenished. But since the initial marking is such that $\widetilde{\mathbf{m}}_0(\pi_1) = 1$, ${}^\bullet\pi_1 = \{\tau_{n+4}\}$ and $\widetilde{\mathbf{m}}^0(\pi_{n+4}) = 0$, the token load of $\pi_1$ can be repeatedly replenished iff the single token at $\pi_1$ at the initial marking is safely passed on to $\pi_{n+4}$. In fact, $\widetilde{N}$ is live once a token is placed in $\pi_{n+4}$ as $\tau_{n+4}^\bullet = \widetilde{\Pi}$. Therefore, the presence of a token in $\pi_{n+4}$ is a necessary and sufficient condition for liveness of $\widetilde{N}$. Now the token can reach $\pi_{n+4}$ if and only if it is not lost at $\pi_{n+3}$ by firing of the transitions $\widetilde{\tau}_j^i$, $(i = 1, 2$ and $j = 1, 2, \ldots n)$. The firing of $\widetilde{\tau}_j^i$ can be prevented iff all places in $N_1$ and $N_2$ are empty, that is, $\{p_i^j\}_{j=1}^n = 0$ for $i = 1, 2$ and $j = 1, 2, \ldots n$. Now, places $\{p_i^j\}_{j=1}^n$ can be emptied by the firing of transitions $\widehat{\tau}_j^i$ for $i = 1, 2$ and $j = 1, 2, \ldots n$. But emptying of all $\{p_i^j\}_{j=1}^n$ is possible if and only if $N_1(\mathbf{m}_1^0)$ and $N_2(\mathbf{m}_2^0)$ reach the exact same marking, which is true iff $\mathfrak{R}(N_1, \mathbf{m}_1^0) \subseteq \mathfrak{R}(N_2, \mathbf{m}_2^0)$. To see this note that the places $\pi_1$ and $\pi_2$ act as enable places for PNs $N_1$ and $N_2$ respectively. From the initial marking, $N_1$ can reach any marking in $\mathfrak{R}(N_1, \mathbf{m}_1^0)$ till the firing of uncontrollable transition $\tau_1$ which removes one token from $\pi_1$ and populates $\pi_2$. Since $\tau_2$ and all transitions in $N_2$ are controllable, $N_2$ can be steered to any marking in $\mathfrak{R}(N_2, \mathbf{m}_2^0)$. Therefore, $N_1(\mathbf{m}_1^0)$ and $N_2(\mathbf{m}_2^0)$ can reach the exact same marking iff $\mathfrak{R}(N_1, \mathbf{m}_1^0) \subseteq \mathfrak{R}(N_2, \mathbf{m}_2^0)$. The reachability inclusion problem is undecidable for arbitrary PNs [29]. Therefore, determining the existence of an LESP for $\widetilde{N}$ is undecidable.

We construct the PN $N = (\Pi, T, \Phi, \Gamma)$ with initial marking $\mathbf{m}_0$, from $\widehat{N}$ and $\widetilde{N}$ (see Figure 2) as: $\Pi \leftarrow \hat{\Pi} \cup \widetilde{\Pi}$; $T \leftarrow \hat{T} \cup \widetilde{T}$; $\Phi \leftarrow \hat{\Phi} \cup \widetilde{\Phi} \cup (t_1, \pi_1) \cup (\tau_{n+4}, p_1) \cup (\tau_{n+4}, p_2)$; and, $\mathbf{m}_0(p_1) = \mathbf{m}_0(p_2) = 2$, $\mathbf{m}_0(\widetilde{\Pi}) = \widetilde{\mathbf{m}}_0$.

**Observation 1.** *The following statements are equivalent: (a)* $N$ *is live; (b)* $\widetilde{N}$ *is live; and (c)* $\widehat{N}$ *is live.*

*Proof.* (a) $\Rightarrow$ (b) and (a) $\Rightarrow$ (c) follows from the definition of liveness.

The firing of transition $t_1$ places a token in $\pi_1$ without affecting the marking of $\widehat{N}$. If $\widehat{N}$ is live, then the token in $\pi_1$ is repeatedly replenishable. Therefore, the marking with a token in place $\pi_{n+4}$ is reachable from every marking that is reachable from the initial marking thereby guaranteeing the liveness of the subnet $\widetilde{N}$. Hence (c) $\Rightarrow$

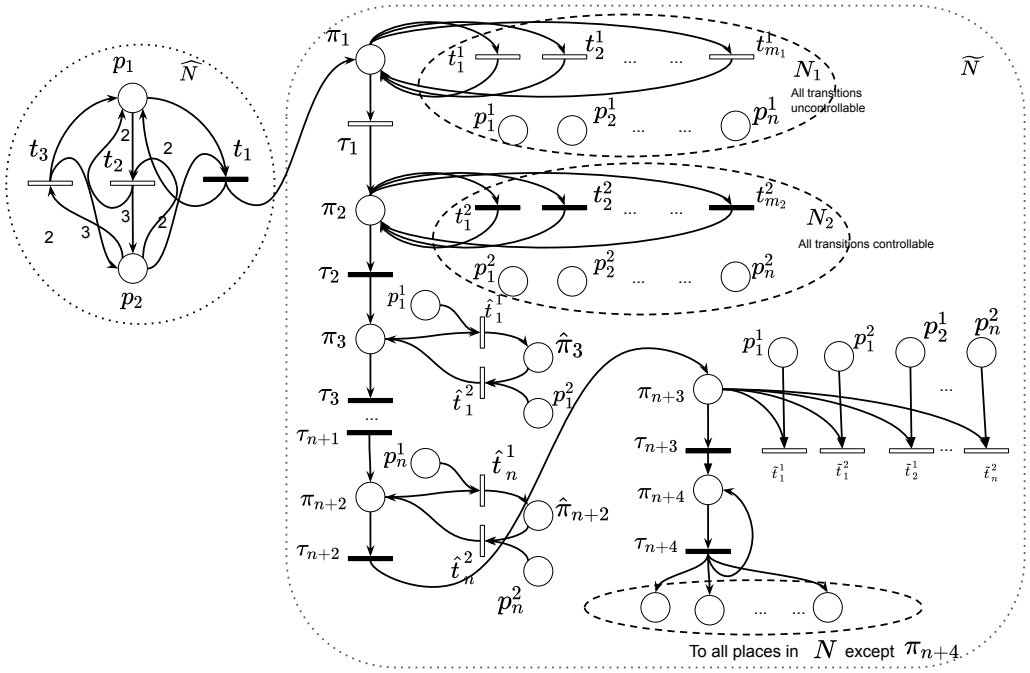


Fig. 2. A graphical illustration of the construction of the PN $N$ using the PNs $\widehat{N}$ and $\widetilde{N}$. Places $p_1^1$ to $p_n^2$ have been redrawn in the figure for ease of illustration.

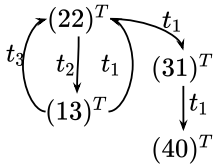


Fig. 3. Reachability graph of $\widehat{N}$ with initial marking $(2\ 2)^T$

(b). From this, it follows that $N$ is live and we have (c) $\Rightarrow$ (a)

$\widetilde{N}$ is live implies that a marking that places a token in $\pi_{n+4}$ is reachable from every marking that is reachable from the initial marking. Liveness of subnet $\widehat{N}$ follows from the observation that $\{p_1, p_2\} \in \tau_{n+4}^{\bullet}$. Therefore, (b) $\Rightarrow$ (c). □

**Observation 2.** *$\mathcal{P}'$ is an LESP for $N(\mathbf{m}_0)$, where:*

$$\mathcal{P}'(\mathbf{m}, t) = \begin{cases} 1 & \text{if } (t = t_1) \wedge (\mathbf{m}(p_1) = 1) \wedge (\mathbf{m}(p_2) = 3) \\ 0 & \text{if } (t = t_1) \wedge (\mathbf{m}(p_1) \neq 1 \vee \mathbf{m}(p_2) \neq 3) \\ 1 & \text{if } t \in T - \{t_1\} \end{cases}$$

*Proof.* That $\mathcal{P}'$ is an LESP for $\widehat{N}((2\ 2)^T)$ is clear from the reachability graph in Figure 3. From Observation 1, $\mathcal{P}'$ is an LESP for $N(\mathbf{m}_0)$. □

$\mathcal{P}'$ enforces liveness in $N$ by making the subnet $\widehat{N}$ live. Suppose $k_r = 1$ and $T_f = \{t_1\}$. If the fault-event $\phi$ occurs at a marking $\mathbf{m} \in \mathfrak{R}(N, \mathbf{m}_0, \mathcal{P}')$ when $\mathbf{m}(p_1) = 2$ and $\mathbf{m}(p_2) = 2$, then an unintended firing of the affected transition $t_1$ will take the subnet $\widehat{N}$ to the marking $(3\ 1)^T$ following which the policy $\mathcal{P}'$ does not enforce liveness in the presence of faults. In fact, it is easy to see from the reachability graph that there does not exist an FT-LESP for $\widehat{N}$ for initial marking $(2\ 2)^T$, $k_r = 1$ and $T_f = \{t_1\}$. By construction, the only way to make $N(\mathbf{m}_0)$ live in the presence of faults for $k_r = 1$ and $T_f = \{t_1\}$ is by synthesizing an LESP for $\widetilde{N}$.

**Observation 3.** *There exists an FT-LESP for $N(\mathbf{m}_0)$ for $k_r = 1$ and $T_f = \{t_1\}$ if and only if there exists an LESP for $\widetilde{N}$.*

As proved in Theorem 5.3 of [12], the existence of an LESP for $\widetilde{N}$ is undecidable due to the undecidability of the reachability inclusion problem.

**Theorem 2.** *Given an LESP for an arbitrary PN $\overline{N}(\mathbf{m}_0)$, the existence of an FT-LESP for a given set $T_f$ and a given value of $k_r$ is undecidable.*

*Proof.* Suppose for contradiction that there exists an algorithm $\mathcal{A}_f$ that takes the PN structure $\overline{N}(\mathbf{m}_0)$, the set $T_f$ and the value of $k_r$ as inputs and outputs *yes* if and only if $\mathbf{m}_0 \in \Delta_{k_r}(N)$. Then for inputs $N(\mathbf{m}_0)$ (as in the construction), $T_f = \{t_1\}$ and $k_r = 1$ the algorithm $\mathcal{A}_f$ can be used to decide if $\mathfrak{R}(N_1, \mathbf{m}_1^0) \subseteq \mathfrak{R}(N_2, \mathbf{m}_2^0)$ for arbitrary PNs $N_1$ and $N_2$, which is an undecidable problem. □

In the next section we identify a subclass of PNs for which the existence of an FT-LESP is decidable.

## 5 FT-LESP for Fully Controllable Ordinary Free Choice PNs

The main result of this section is that $\Delta_{k_r}(N)$ is right-closed for a fully controllable *Ordinary* FCPN (O-FCPNs). We first prove an intermediate result that the minimally restrictive FT-LESP for a fully controlled O-FCPN will not disable any non-choice transitions. Recall that for an FCPN $N = (\Pi, T, \Phi, \Gamma)$, a transition $t \in T$ is said to be a *non-choice* (resp. *choice*) transition if $\{t\} = ({}^\bullet t)^\bullet$ (resp. if $\{t\} \subset ({}^\bullet t)^\bullet$).

Let the initial marking $\mathbf{m}_0 \in \Delta_{k_r}(N)$ and consider a marking $\mathbf{m} \in \Delta_k(N)$ reached under the supervision of $\mathcal{P}_f$ (that is, $(k_r - k)$-many faults have been detected) such that a non-choice transition $t \in T_e(N, \mathbf{m})$. From Corollary 3, $(\mathcal{P}_f(\mathbf{m}, t, k_r - k) = 1) \Leftrightarrow ((\mathbf{m} \xrightarrow{t} \mathbf{m}_1) \wedge (\mathbf{m}_1 \in \Delta_k(N)))$. We start with the stipulation that $\mathbf{m}_1 \in \Delta_k(N)$, which allows us to specify a supervisory policy corresponding to which we can define the unintended firings, and later prove that the stipulation is indeed correct. Let $\sigma_f$ be a valid string of transitions under faults from $\mathbf{m}_1$ under the supervision of $\mathcal{P}_f$ in which the unintended occurrences of affected transitions (belonging to $T_f$) appear $k$ times and $\mathbf{m}_1 \xrightarrow{\sigma_f} \mathbf{m}_2$. In what follows, we prove that our stipulation that $\mathbf{m}_1 \in \Delta_k(N)$ is indeed correct by proving $\mathbf{m}_2 \in \Delta(N)$. Note that the rectification event occurs at $\mathbf{m}_2$ and the supervisor regains control of all transitions.

Let $\sigma_s$ denote the largest substring of $\sigma_f$ that is a valid firing string from $\mathbf{m}$, and $\mathbf{m} \xrightarrow{\sigma_s} \widehat{\mathbf{m}}_1$, under the supervision of $\mathcal{P}_f$. Also, let $\sigma_f \backslash \sigma_s$ denote the ordered string of transitions in $\sigma_f$ that did not appear in $\sigma_s$. In the first step of the proof we specify a string $(\sigma_s)(\omega_1)(t)(\sigma_f \backslash \sigma_s)$ that can be fired from $\mathbf{m}$ and observe that the resulting marking is in $\Delta(N)$.

$$\mathbf{m} \xrightarrow{t} \mathbf{m}_1 \xrightarrow{\sigma_f} \mathbf{m}_2 \xrightarrow{\omega_1} \widehat{\mathbf{m}}_4 \tag{1}$$

$$\mathbf{m} \xrightarrow{\sigma_s} \widehat{\mathbf{m}}_1 \xrightarrow{\omega_1} \widehat{\mathbf{m}}_2 \xrightarrow{t} \widehat{\mathbf{m}}_3 \xrightarrow{\sigma_f \backslash \sigma_s} \widehat{\mathbf{m}}_4 \tag{2}$$

In the second step, we prove that the string $t\sigma_f$ fired from $\mathbf{m}$ can be extended by $\omega_1$ which we then use to prove that $\mathbf{m}_2 \in \Delta(N)$. The scenario described by Equation (2) can be interpreted as a simulation of a specific path under supervision from $\mathbf{m}$ that replicates $\sigma_f$ (that is, the effect of unintended firing of transitions). $\sigma_s$ and $\sigma_f \backslash \sigma_s$ can be determined with the knowledge of $\sigma_f$. The string $\omega_1$ is determined as follows. Suppose (unintended occurrences of) controllable transitions belonging to the set $T_f$ appear $j \leq k$ times in $\sigma_s$. Since $\mathbf{m} \in \Delta_k(N)$, from Property (c) of Definition 2 and Corollary 2, we have $\widehat{\mathbf{m}}_1 \in \Delta_{k-j}(N)$. Consequently, there exists a valid firing string of transitions specified by the policy $\mathcal{P}_f$ from $\widehat{\mathbf{m}}_1$ after which $t$ will be permitted by $\mathcal{P}_f$. That is, $\exists \omega_1 \in T^*$ such that (i) $\widehat{\mathbf{m}}_1 \xrightarrow{\omega_1} \widehat{\mathbf{m}}_2$, $\mathcal{P}_f(\widehat{\mathbf{m}}_2, t, k_r - k + j) = 1$; and (ii) $\widehat{\mathbf{m}}_1 \xrightarrow{\omega_2} \overline{\mathbf{m}}_1$, $\overline{\mathbf{m}}_1 \in \Delta_{k-j}(N)$ $\forall \omega_2 \in pr(\omega_1)$. For the example PN $N_i$ in Figure 1, let $k = 1$, $\mathbf{m} = (11001)$, $t = t_1$, and $T_f = \{t_2\}$. Then from (1) and (2), we have:

$$(11001) \xrightarrow{t_1} (00101) \xrightarrow{t_2} (00001) \xrightarrow{t_5} (11000)$$

$$(11001) \xrightarrow{\epsilon} (11001) \xrightarrow{t_5} (22000) \xrightarrow{t_1} (11100) \xrightarrow{t_2} (11000)$$

**Observation 4.** *$\sigma_f \backslash \sigma_s$ is a valid firing string from $\widehat{\mathbf{m}}_3$ (in the absence of supervision).*

*Proof.* Let $t_1$ denote the first transition that appears in $\sigma_f \backslash \sigma_s$. Then $t_1$ must have an input place that is an output place of $t$. That is, $\exists p \in \{{}^\bullet t_1\} \cap \{t^\bullet\}$. If not, then $t_1$ can be fired without firing transition $t$, which is a contradiction since $t_1$ does not appear in $\sigma_s$. There are two cases: (i) $\{{}^\bullet t_j^2\}^\bullet \neq t_1$; and (ii) $\{{}^\bullet t_j^2\}^\bullet = t_1$. In the first case, $t_1$ is a choice transition. Then since $N$ is ordinary and free choice, $\{{}^\bullet t_1\} = p$ for some place $p \in \{t^\bullet\}$, and hence $t_1 \in T_e(N, \widehat{\mathbf{m}}_3)$. In the second case, $t_1$ is a non-choice transition. Then $\{{}^\bullet t_1\} \subset \{\sigma_s^\bullet\}$ and $\{{}^\bullet t_1\} \subseteq \{t^\bullet\}$. Here we use $\{\sigma_s^\bullet\}$ to denote the set of places populated by the firing of string $\sigma_s$ from $\mathbf{m}_0$. The string $\omega_1$ does not reduce the token load of the input places of the non-choice transition $t_1$ (as $\{{}^\bullet t_j^2\}^\bullet = t_1$), it follows that $t_1 \in T_e(N, \widehat{\mathbf{m}}_3)$. Continuing in the same way, if $t_k$ is the $k$-th transition in $\sigma_f \backslash \sigma_s$, then $\exists p \in \{{}^\bullet t_k\} \cap (\cup_{i=1}^{k-1} \{t_i^\bullet\})$. The rest of the proof follows by induction by using the same arguments as for $t_1$. □

**Observation 5.** *$\omega_1$ is a valid firing string from $\mathbf{m}_2$ under the supervision of $\mathcal{P}_f$.*

*Proof.* Let $t^1$ be the first transition in $\omega_1$. Since $\omega_1$ is a valid firing string from $\widehat{\mathbf{m}}_1$, it means that the firing of string $\sigma_s$ from $\widehat{\mathbf{m}}_0$ populates the input places of $t^1$ with sufficient number of tokens so as to enable the transition. Now, since $\sigma_s$ is a substring of $\sigma_f$, its firing from $\mathbf{m}_1$ also populates the input places of $t^1$ with sufficient number of tokens so as to enable transition $t^1$; and the input places of $t^1$ would not be emptied by transitions in $\sigma_f \backslash \sigma_s$. Suppose for contradiction that $t^1 \notin T_e(N, \mathbf{m}_2)$ and the firing of some transition in $\sigma_f \backslash \sigma_s$ emptied the input places of $t^1$. Then $t^1$ cannot be non-choice as $\{{}^\bullet t_j^2\}^\bullet = t^1$ and once populated $\{{}^\bullet t^1\}$ cannot be emptied without firing $t^1$. If $t^1$ is a choice transition, then it means that there exists $t' \in \{{}^\bullet t^1\}^\bullet$ that appears in $\sigma_f$. But then it appears in $\sigma_s$ also, and hence does not appear in $\sigma_f \backslash \sigma_s$ which is a contradiction. The rest of the proof follows through recursion using the same arguments by taking $\sigma_s = \sigma_s t^1$ and $\sigma_f = \sigma_f t^1$. □

**Observation 6.** $\widehat{\mathbf{m}}_4, \mathbf{m}_2 \in \Delta(N)$.

*Proof.* The string $(\sigma_s)(\omega_1)(t)(\sigma_f \backslash \sigma_s)$ is such that the unintended firing of affected transitions in $T_f$ appear $k$ times. Since $\mathbf{m} \in \Delta_k(N)$, by Property (c) of Definition

2, $\widehat{\mathbf{m}}_4 \in \Delta(N)$. Since $\widehat{\mathbf{m}}_4 \in \Delta(N)$, there exists a valid firing string $\sigma = \sigma_1\sigma_2$ in $N$ such that $\widehat{\mathbf{m}}_4 \xrightarrow{\sigma_1} \widehat{\mathbf{m}}_5 \xrightarrow{\sigma_2} \widehat{\mathbf{m}}_6, \widehat{\mathbf{m}}_6 \geq \widehat{\mathbf{m}}_5$, all transitions appear at least once in $\sigma_2$, and $\forall \sigma_3 \in pr(\sigma_1\sigma_2)$, $(\widehat{\mathbf{m}}_1 \xrightarrow{\sigma_3} \widehat{\mathbf{m}}_7) \Rightarrow (\widehat{\mathbf{m}}_7 \in \Delta(N))$. Due to the fully controllable nature of the PN, a path with such properties, $\omega_1\sigma_1\sigma_2$, also exists for $\mathbf{m}_2$. Besides, the control invariance property is trivially true. Therefore, $\mathbf{m}_2 \in \Delta(N)$. □

Since $\mathbf{m}_2 \in \Delta(N)$ is true for all values of $k$ such that $\mathbf{m} \in \Delta_k(N)$, it follows that $\mathbf{m}_1 \in \Delta_k(N)$. Therefore, the firing of a non-choice transition from $\mathbf{m} \in \Delta_k(N)$ does not take the marking outside the set. The minimally restrictive FT-LESP will not disable any non-choice transition.

**Lemma 1.** *The minimally restrictive FT-LESP for a fully controlled O-FCPN will not disable any non-choice transitions.*

**Theorem 3.** *$\Delta_{k_r}(N)$ is right-closed for a fully controlled ordinary free choice PN.*

*Proof.* If $\Delta_{k_r}(N) = \emptyset$, then it is right-closed by definition. Let $\mathbf{m}_0 \in \Delta_{k_r}(N)$. We need to prove that $\widehat{\mathbf{m}}_0 \in \Delta_{k_r}(N)$ for all $\widehat{\mathbf{m}}_0 \geq \mathbf{m}_0$. We prove this by induction. The base case is established by letting $k_r = 0$ and observing that $\Delta_0(N)(= \Delta(N))$ for an FCPN is right-closed ( [13]). The induction hypothesis is that $\Delta_i(N)$ for $i \in \{1, 2, \ldots, k_r - 1\}$ is right-closed. We know that $\mathbf{m}_0 \in \Delta_{k_r}(N)$. Since the PN is fully controlled, the path property and control invariance (Properties (a) and (b) in Definition 2) follow trivially for all $\widehat{\mathbf{m}}_0 \geq \mathbf{m}_0$. For the induction step, we need to prove that the firing of a single transition from every $\widehat{\mathbf{m}}_0 \geq \mathbf{m}_0$ results in a marking that is in $\Delta_{k_r-1}(N)$.

By Lemma 1 and the discussion preceding it, for a fully controlled O-FCPN, the firing of a non-choice transition from $\widehat{\mathbf{m}}_0$ will result in a marking in $\Delta_{k_r}(N)$. We consider the case of choice transitions and let $\widehat{\mathbf{m}}_0 = \mathbf{m}_0 + \widetilde{\mathbf{m}}$. If $T_e(N, \widehat{\mathbf{m}}_0) = T_e(N, \mathbf{m}_0)$, then $\widehat{\mathbf{m}}_0 \xrightarrow{t} \overline{\mathbf{m}}$ and $\mathbf{m}_0 \xrightarrow{t} \underline{\mathbf{m}}$, and $\overline{\mathbf{m}} = \underline{\mathbf{m}} + \widetilde{\mathbf{m}}$. We have: $(\mathbf{m}_0 \in \Delta_{k_r}(N)) \Rightarrow (\underline{\mathbf{m}} \in \Delta_{k_r-1}(N))$. By induction hypothesis, $\Delta_{k_r-1}(N)$ is right closed. Therefore, $\overline{\mathbf{m}} \in \Delta_{k_r-1}(N)$. If $T_e(N, \mathbf{m}_0) \subset T_e(N, \widehat{\mathbf{m}}_0)$, then $\widehat{\mathbf{m}}_0 \geq \mathbf{m}_0 + \sum_{t \in T_{en}} \mathbf{IN}_t$ where $T_{en} = T_e(N, \widehat{\mathbf{m}}_0) - T_e(N, \mathbf{m}_0)$. The firing of transition $t_i$ from $\widehat{\mathbf{m}}_0$ would give:

$$\widehat{\mathbf{m}}_0 + \mathbf{C}_{t_i} \geq \mathbf{m}_0 + \mathbf{OUT}_{t_i} + \sum_{t \in T_{en} - \{t_i\}} \mathbf{IN}_t$$

$(\mathbf{m}_0 \in \Delta_{k_r}(N)) \Rightarrow (\mathbf{m}_0 \in \Delta_{k_r-1}(N))$. By induction hypothesis, $\Delta_{k_r-1}(N)$ is right closed. Therefore, $\widehat{\mathbf{m}}_0 + \mathbf{C}_{t_i} \in \Delta_{k_r-1}(N)$.

□

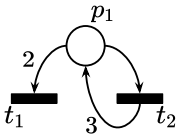


Fig. 4. PN $N_j$ for which $\Delta_1(N_j)$ is not right-closed for $k_r = 1$.

In general, $\Delta_{k_r}(N)$ is not right-closed for arbitrary PNs. Figure 4 presents an example of a PN structure that is not an O-FCPN and for which $\Delta_1(N_j)$ is not right-closed. It is clear that $\Delta_0(N_j) = \{\mathbf{m} \in \mathcal{N} : \mathbf{m} \geq 1\}$. Let $k_r = 1$ and $T_f = \{t_1\}$. Then: $1 \xrightarrow{\phi t_2 t_1 \rho} 1$ which is in $\Delta_0(N_j)$. If the initial token load is 2 then: $2 \xrightarrow{\phi t_1 \rho} 0$, which is not in $\Delta(N_j)$. We have $\Delta_1(N_j) = \Delta_0(N_j) - \{2\}$.

Algorithm 1 presents a recursive procedure for the synthesis of FT-LESP for a fully controlled O-FCPN. Letting $\Delta_0(N) = \Delta(N)$, the procedure FTLESP_FCPN($N$, min($\Delta_0$), $\mathbf{m}_0$, 0) computes a sequence of sets $\Delta_1, \ldots, \Delta_{k_r}$ each satisfying the properties in Definition 2 for a PN $N(\mathbf{m}_0)$. We use $\Delta_{k-1}(N)$ as the initial estimate of $\Delta_k(N)$ (from Corollary 2, $\Delta_k(N) \subseteq \Delta_{k-1}(N)$). The *while* condition in the algorithm tests Property (c) of Definition 2. If it is not satisfied for any of the minimal elements of $\Delta_k$ (that is, there is a transition whose firing results in a marking not in $\Delta_{k-1}$), then the minimal elements of the current estimate are raised (Step 3) by the smallest possible amount. Note that since the estimates are right-closed, raising the minimal elements actually makes the set smaller. Step 4 removes the redundant entries in the updated set by keeping only the minimal (smallest) elements. The updated estimate is then tested for Properties (a) and (b) in the (subroutine of) Step 5. We refer the reader to [13] for further details with only a note here that if any of the Properties (a) and (b) are not satisfied, then (the subroutine of) Step 5 essentially updates the estimate using a process similar to Steps 3 and 4 given here. The program exits the *while* loop either when the set $\Delta_k$ with required properties is found or if $\mathbf{m}_0$ drops out of the estimate.

We illustrate the algorithm using the PN $N_i$ in Figure 1. min($\Delta(N_i)$) = $\{(1\ 1\ 0\ 0\ 0)^T, (0\ 0\ 1\ 0\ 0)^T, (0\ 0\ 0\ 1\ 0)^T, (0\ 0\ 0\ 0\ 1)^T\}$. Firing of $t_2$ from $(0\ 0\ 1\ 0\ 0)^T$ will result in the marking $(0\ 0\ 0\ 0\ 0)^T$ which is not in $\Delta(N_i)$. The execution will go to Step 3 in the algorithm following which $(0\ 0\ 1\ 0\ 0)^T$ will be replaced by $\{(1\ 1\ 1\ 0\ 0)^T, (0\ 0\ 2\ 0\ 0)^T, (0\ 0\ 1\ 1\ 0)^T, (0\ 0\ 0\ 1\ 1)^T\}$ in $min(\Delta(N_i))$. In Step 5, we test the path property (control invariance is trivially true). While the path property for $(1\ 1\ 0\ 0\ 0)^T \xrightarrow{t_1 t_3 t_4 t_5 t_1 t_2} (1\ 1\ 0\ 0\ 0)^T$ for the original $\Delta(N_i)$ was true with the path $t_1 t_3 t_4 t_5 t_1 t_2$, it is not true for the updated version because $(1\ 1\ 0\ 0\ 0)^T \xrightarrow{t_1} (0\ 0\ 1\ 0\ 0)^T$ and $(0\ 0\ 1\ 0\ 0)^T$ is not in $\Delta(N_i)$ anymore. Therefore, the algorithm (subroutine of Step 5) will raise the minimal elements

**Algorithm 1** FTLESP_FCPN($N, \min(\Delta_{k-1}), \mathbf{m}_0, k-1$)

1: $\min(\Delta_k) = \min(\Delta_{k-1})$. Let $\min(\Delta_{k-1}) = \{\widetilde{\mathbf{m}}_j\}_{j=1}^{l}$
2: **while** $((\mathbf{m}_0 \in \Delta_k) \wedge (\exists t \in T, \exists \overline{\mathbf{m}}_i \in \min(\Delta_k)$ such that $\max\{\overline{\mathbf{m}}_i, \mathbf{IN}_t\} + \mathbf{C}_t \notin \Delta_{k-1}))$ **do**
3: Replace $\overline{\mathbf{m}}_i$ by a set of $l$ vectors $\{\widehat{\mathbf{m}}_c\}_{c=1}^{l}$ where each $\widehat{\mathbf{m}}_c$ is defined corresponding to each $j \in \{1, \ldots l\}$ as follows: $\widehat{\mathbf{m}}_c = \overline{\mathbf{m}}_i + \max\{\mathbf{0}, \widetilde{\mathbf{m}}_j - (\max\{\overline{\mathbf{m}}_i, \mathbf{IN}_t\} + \mathbf{C}_t)\}$
4: Replace the resulting set of $\{\widetilde{\mathbf{m}}_i\}_i$ by its minimal elements and modify the value of $l$ to equal the size of the minimal set of vectors. The updated $\Delta_k$ is denoted by this set of minimal elements.
5: $\min(\Delta_k) \leftarrow$ The minimal elements of the largest (right-closed) subset of $\Delta_k$ such that Properties (a) and (b) of definition 2 are satisfied for all members *AND* $\mathbf{m}_0 \in \Delta_k$. If $\mathbf{m}_0 \notin \Delta_k$, break. $\triangleright$ /* This can be obtained by using the algorithm in figure 8 of reference [13]*/
6: **if** $\mathbf{m}_0 \notin \Delta_k$ **then**
7: $\Delta_k = \emptyset$
8: **return** $\{\min(\Delta_i)\}_{i=1}^{k-1}$
9: **if** $k = k_r$ **then**
10: **return** $\{\min(\Delta_i)\}_{i=1}^{k}$
11: **else**
12: FTLESP_FCPN($N, \Delta_k, \mathbf{m}_0, k$)

and replace $(1\ 1\ 0\ 0\ 0)^T$ by $\{(2\ 2\ 0\ 0\ 0)^T, (1\ 1\ 1\ 0\ 0)^T, (1\ 1\ 0\ 1\ 0)^T, (1\ 1\ 0\ 0\ 1)^T\}$. Further steps in the iterations to obtain $\Delta_1(N_i)$ (which was denoted as $\widehat{\Delta}(N_i)$ in Section 2.1) from $\Delta(N_i)$ are shown in the Figure 5.

## 6 Conclusion

We considered the existence and synthesis of LESPs for arbitrary PNs in the presence of a single *fault* which renders a subset of controllable transitions temporarily uncontrollable for finite but possibly arbitrarily large number of transition firings. We proved necessary and sufficient conditions for the existence of a *Fault-Tolerant LESP* (FT-LESP) for an arbitrary PN. We also proved that the existence of an FT-LESP for an arbitrary PN is undecidable and that the undecidability is not inherited from the undecidability of the existence of an LESP. We then identified a class of PNs for which the existence of FT-LESPs is decidable. We did not make any assumption on the subset of transitions that are faulty. We assume that the fault- and rectification- events are extraneous and are not modeled by the DES. Modeling the supervisor and the network between the DES and the supervisor as a part of the DES and then working under the controllability-fault paradigm is one direction of future research. Approaches to policy synthesis for specific classes of PNs with assumptions on transitions affected by faults is another direction that can be looked into. Another interesting direction would be the case with multiple fault- and rectification-events.

## References


[1] J. Peterson, *Petri net theory and the modeling of systems*. Prentice Hall PTR, 1981.

[2] A. Giua, "Petri nets as discrete event models for supervisory control," *Rensselaer Polytechnic Institute, Troy, NY*, July 1992, PhD Thesis.

[3] J. Moody and P. Antsaklis, *Supervisory control of discrete event systems using Petri nets*. Springer Science & Business Media, 2012, vol. 8.

[4] M. Iordache and P. Antsaklis, *Supervisory control of concurrent systems: a Petri net structural approach*. Springer Science & Business Media, 2007.

[5] S. Reveliotis, E. Roszkowska, and J. Choi, "Generalized algebraic deadlock avoidance policies for sequential resource allocation systems," *IEEE Transactions on Automatic Control*, vol. 52, no. 12, pp. 2345–2350, 2007.

[6] A. Ghaffari, N. Rezg, and X. Xie, "Design of a live and maximally permissive petri net controller using the theory of regions," *IEEE transactions on robotics and Automation*, vol. 19, no. 1, pp. 137–141, 2003.

[7] R. Cordone, A. Nazeem, L. Piroddi, and S. Reveliotis, "Designing optimal deadlock avoidance policies for sequential resource allocation systems through classification theory: existence results and customized algorithms," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2772–2787, 2013.

[8] Y. Chen and Z. Li, "Design of a maximally permissive liveness-enforcing supervisor with a compressed supervisory structure for flexible manufacturing systems," *Automatica*, vol. 47, no. 5, pp. 1028–1034, 2011.

[9] O. Marchetti and A. Munier-Kordon, "A sufficient condition for the liveness of weighted event graphs," *European Journal of Operational Research*, vol. 197, no. 2, pp. 532–540, 2009.

[10] F. Basile, L. Recalde, P. Chiacchio, and M. Silva, "Closed-loop live marked graphs under generalized mutual exclusion constraint enforcement," *Discrete Event Dynamic Systems*, vol. 19, no. 1, pp. 1–30, 2009.

[11] F. Basile, R. Cordone, and L. Piroddi, "A branch and bound approach for the design of decentralized supervisors in petri net models," *Automatica*, vol. 52, pp. 322–333, 2015.

[12] R. Sreenivas, "On the existence of supervisory policies that enforce liveness in discrete-event dynamic systems modeled by controlled petri nets," *IEEE Transactions on Automatic Control*, vol. 42, no. 7, pp. 928–945, 1997.

[13] ——, "On the existence of supervisory policies that enforce liveness in partially controlled free-choice petri nets," *IEEE Transactions on Automatic Control*, vol. 57, no. 2, pp. 435–449, 2012.

[14] N. Somnath and R. Sreenivas, "On deciding the existence of a liveness enforcing supervisory policy in a class of partially controlled general free-choice petri nets," *IEEE Transactions on Automation Science and Engineering*, vol. 10, no. 4, pp. 1157–1160, 2013.

[15] R. Sreenivas, "On a decidable class of partially controlled petri nets with liveness enforcing supervisory policies," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 43, no. 5, pp. 1256–1261, 2013.

[16] C. Chen, A. Raman, H. Hu, and R. Sreenivas, "On liveness enforcing supervisory policies for arbitrary petri nets," *To appear, IEEE Transactions on Automatic Control*, circa 2020.

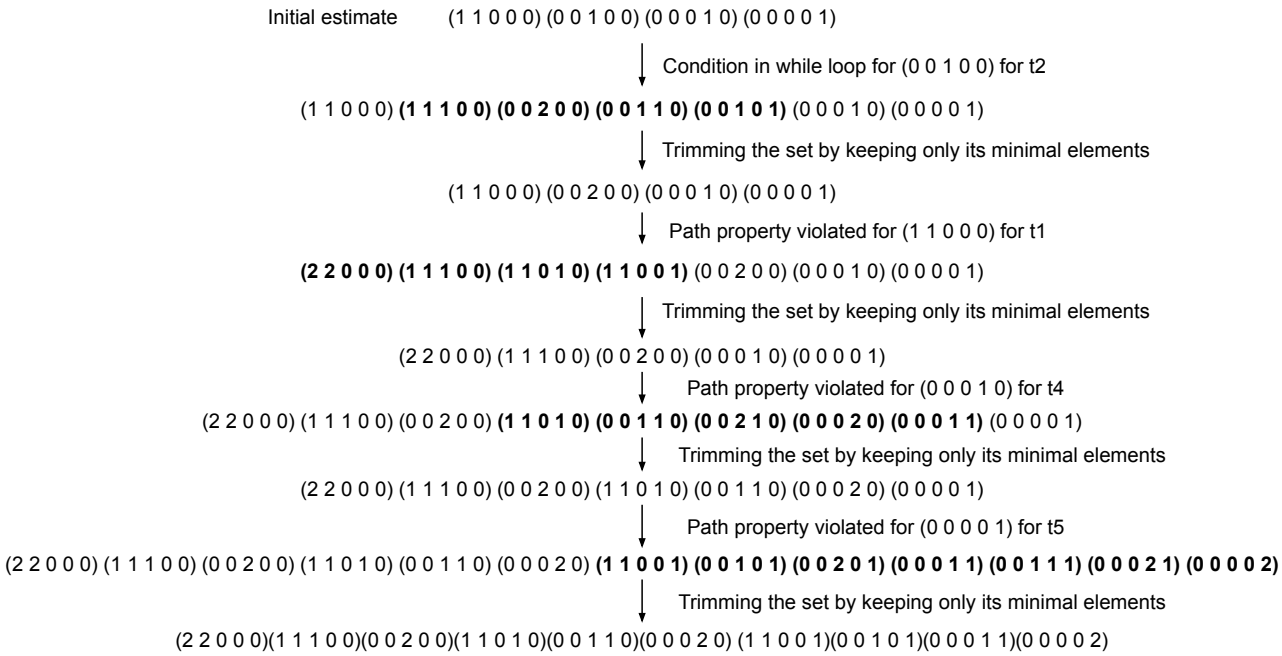


Fig. 5. Iterations to obtain $\Delta_1(N_i)$ (which was denoted as $\widehat{\Delta}(N_i)$ in Section 2.1) from $\Delta(N_i)$


[17] F.-S. Hsieh, "Fault-tolerant deadlock avoidance algorithm for assembly processes," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 34, no. 1, pp. 65–79, 2004.

[18] M. Lawley and W. Sulistyono, "Robust supervisory control policies for manufacturing systems with unreliable resources," *IEEE Transactions on Robotics and Automation*, vol. 18, no. 3, pp. 346–359, 2002.

[19] F.-S. Hsieh, "Robustness of deadlock avoidance algorithms for sequential processes," *Automatica*, vol. 39, no. 10, pp. 1695–1706, 2003.

[20] ——, "Reconfigurable fault tolerant deadlock avoidance controller synthesis for assembly production processes," in *Systems, Man, and Cybernetics, 2000 IEEE International Conference on*, vol. 4. IEEE, 2000, pp. 3045–3050.

[21] S. Wang, S. Chew, and M. Lawley, "Using shared-resource capacity for robust control of failure-prone manufacturing systems," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 38, no. 3, pp. 605–627, 2008.

[22] S. Reveliotis and Z. Fei, "Robust deadlock avoidance for sequential resource allocation systems with resource outages," *IEEE Transactions on Automation Science and Engineering*, vol. 14, no. 4, pp. 1695–1711, 2017.

[23] Y. Feng, K. Xing, Z. Gao, and Y. Wu, "Transition cover-based robust petri net controllers for automated manufacturing systems with a type of unreliable resources," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 11, pp. 3019–3029, 2017.

[24] G. Liu, P. Li, Z. Li, and N. Wu, "Robust deadlock control for automated manufacturing systems with unreliable resources based on petri net reachability graphs," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2018.

[25] L. Li, C. Hadjicostis, and R. Sreenivas, "Designs of bisimilar petri net controllers with fault tolerance capabilities," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 38, no. 1, pp. 207–217, 2008.

[26] A. Raman and R. Sreenivas, "Fault-tolerant control of discrete-event systems with controllability failures," *IEEE Control Systems Letters*, vol. 4, no. 3, pp. 674–679, 2020.

[27] V. Deverakonda and R. Sreenivas, "On a sufficient information structure for supervisory policies that enforce liveness in a class of general petri nets," *IEEE Transactions on Automatic Control*, vol. 60, no. 7, pp. 1915–1921, 2015.

[28] D. Osherson, M. Stob, and S. Weinstein, *Systems that Learn: An Introduction to Learning Theory for Cognitive and Computer Scientists*. Cambridge, MA: The MIT Press, 1986.

[29] M. H. T. Hack, "Decidability questions for petri nets." Ph.D. dissertation, Massachusetts Institute of Technology, 1976.