Synthesis of Liveness Enforcing Supervisory Policies In Petri Nets by Stepwise Refinement

N. Somnath* and R. S. Sreenivas†
* Cooley LLP, Boston, MA 02116.
† *Senior Member, IEEE,* CSL & ISE, University of Illinois at Urbana-Champaign, Urbana, IL 61820.

***Abstract*—The refinement procedure of Suzuki and Murata [1] combines two *Petri Nets* (PNs) $N_1(\mathbf{m}_1^0)$ and $N_2(\mathbf{m}_2^0)$ in a prescribed manner to obtain a PN $N_3(\mathbf{m}_3^0)$. Under appropriate conditions, the *liveness* of the PNs $N_1(\mathbf{m}_1^0)$ and $N_2(\mathbf{m}_2^0)$ implies the *liveness* of the PN $N_3(\mathbf{m}_3^0)$.**

A PN that is not live, can be made live by a *liveness enforcing supervisory policy* (LESP). In this paper, we develop the results of Suzuki and Murata to yield a class of PNs for which an LESP for $N_3(\mathbf{m}_3^0)$ can be represented in terms of local-LESPs for $N_1(\mathbf{m}_1^0)$ and $N_2(\mathbf{m}_2^0)$.

***Index Terms*—Petri Nets, Supervisory Control, Discrete Event Systems.**

I. Introduction

Petri nets (PNs) are widely used in modeling Manufacturing- and Service-Systems, which are *Discrete-Event/Discrete-State* (DEDS) systems. The states of DEDS systems have a logical, as opposed to a numerical, interpretation. At any state, there is a set of potential (discrete-)events that can occur. The occurrence of any one would change the state of the system; this process can be repeated as often as necessary, resulting in a string of event-occurrences. Some of these event-strings could result in unfavorable outcomes, while others might result in favorable outcomes. We wish to avoid all unfavorable event-strings, while retaining as much of the favorable event-strings as possible. This is accomplished by a *supervisory policy*, which determines the set of events that are to be permitted/prevented at a given state in such a manner that unfavorable outcomes are avoided entirely. In this paper, we concern ourselves with supervisory policies that avoid *livelocks*, which is a state where some modeled-event can enter into a state of suspended animation, and never proceed to completion.

A PN is said to be *live* if it is possible to fire any transition from every reachable marking, although not necessarily immediately. The *supervisory control* of PNs supposes the existence of a set of *controllable* (*uncontrollable*) transitions that can (cannot) be prevented from firing by a *supervisory policy*. The supervisory policy decides which of the controllable transitions are permitted to fire at a marking reachable under supervision. This paper is about investigations into the existence of supervisory policies that enforce liveness in families of PNs that are not live.

The process by which a small PN is progressively transformed into a large PN, while retaining some desired property in course of this transformation, is referred to as the process of *refinement* (cf. section *V.C*, [2]). In the refinement procedure of Suzuki and Murata [1], a PN $N_1(\mathbf{m}_1^0)$ is combined in a prescribed fashion with a PN $N_2(\mathbf{m}_2^0)$ to obtain a PN $N_3(\mathbf{m}_3^0)$. In the context of supervisory control, in this paper we require a few additional conditions of the constituent PNs $N_1(\mathbf{m}_1^0)$ and $N_2(\mathbf{m}_2^0)$. Following Suzuki and Murata, we construct a PN $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$, which is essentially the PN $N_2(\mathbf{m}_2^0)$ with an extra place, and two extra arcs. We show that when our stipulated conditions are met by $N_1(\mathbf{m}_1^0)$ and $N_2(\mathbf{m}_2^0)$, there is a supervisory policy that enforces liveness in $N_3(\mathbf{m}_3^0)$ if and only if there are similar policies for the PNs $N_1(\mathbf{m}_1^0)$ and $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$. This result essentially implies that when there is a liveness enforcing supervisory policy for $N_3(\mathbf{m}_3^0)$, it can be implemented in a distributed fashion.

The rest of the paper is organized as follows. Section II introduces the relevant notations and reviews the results that are relevant to this paper. The main results are presented in section III. The conclusions are presented in section IV.

II. Notations and Definitions and Some Preliminary Observations

We use $\mathcal{N}$ ($\mathcal{N}^+$) to denote the set of non-negative (positive) integers. A *Petri net structure* $N = (\Pi, T, \Phi)$ is an ordered 3-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*, and $\Phi \subseteq (\Pi \times T) \cup (T \times \Pi)$ is a set of *arcs*. The *initial marking function* (or the *initial marking*) of a PN structure N is a function $\mathbf{m}^0 : \Pi \to \mathcal{N}$. A *Petri net* (PN) $N(\mathbf{m}^0)$ consists of a PN structure N along with its initial marking $\mathbf{m}^0$. In graphical representation of PNs places (transitions) are represented by circles (boxes), and each member of $\phi \in \Phi$ is denoted by a directed arc. If $\phi = (p, t)$ (resp. (t, p)) the arc is directed from p (resp. t) to t (resp. p). The initial marking is represented by an appropriate integer, $\mathbf{m}^0(p)$, within each place $p \in \Pi$.

The *marking* of a PN N, $\mathbf{m}^i : \Pi \to \mathcal{N}$, identifies the number of *tokens* in each place. For a given marking $\mathbf{m}^i$, a transition $t \in T$ is said to be *enabled* if $\forall p \in (^\bullet t)_N, \mathbf{m}^i(p) \geq 1$, where $(^\bullet x)_N := \{y \mid (y, x) \in \Phi, \text{where } N = (\Pi, T, \Phi)\}$. The set of enabled transitions at marking $\mathbf{m}^i$ is denoted by the symbol $T_e(N, \mathbf{m}^i)$. An enabled transition $t \in T_e(N, \mathbf{m}^i)$ can *fire*, which changes the marking $\mathbf{m}^i$ to $\mathbf{m}^{i+1}$ according to the equation $\mathbf{m}^{i+1}(p) = \mathbf{m}^i(p) - card((^\bullet t)_N \cap \{p\}) + card((t^\bullet)_N \cap \{p\})$ where $(x^\bullet)_N := \{y \mid (x, y) \in \Phi, \text{where } N = (\Pi, T, \Phi)\}$ and $card(\bullet)$ denotes the cardinality of the set argument.

A string of transitions $\sigma = t_1 t_2 \cdots t_k$, where $t_j \in T (j \in \{1, 2, \ldots, k\})$ is said to be a *valid firing string* starting from the marking $\mathbf{m}^i$, if, (1) the transition $t_1 \in T_e(N, \mathbf{m}^i)$, and (2) for $j \in \{1, 2, \ldots, k-1\}$ the firing of the transition t_j produces a marking $\mathbf{m}^{i+j}$ and $t_{j+1} \in T_e(N, \mathbf{m}^{i+j})$ is enabled. If $\mathbf{m}^{i+k}$ results from the firing of $\sigma \in T^*$ starting from the initial marking $\mathbf{m}^i$, we represent it symbolically as $\mathbf{m}^i \xrightarrow{\sigma} \mathbf{m}^{i+k}$. Given an initial marking $\mathbf{m}^0$ the set of *reachable markings* for $\mathbf{m}^0$ denoted by $\mathfrak{R}(N, \mathbf{m}^0)$, is defined as the set of markings generated by all valid firing strings starting with marking $\mathbf{m}^0$ in the PN structure N. 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 $t \in T_e(N, \mathbf{m}^j)$. A transition $t \in T$ is said to be *k-enabled* if $\exists \mathbf{m} \in \mathfrak{R}(N, \mathbf{m}^0)$, such that $\forall p \in^\bullet t, \mathbf{m}(p) \geq k$.

A PN structure $N = (\Pi, T, \Phi)$ is *Free-Choice* if $\forall p \in \Pi, (card((p^\bullet)_N) > 1 \Rightarrow (^\bullet(p^\bullet)_N)_N = \{p\})$. A PN $N(\mathbf{m}^0)$ where $N = (\Pi, T, \Phi)$ is free choice, is a *Free-Choice Petri net* (FCPN).

There are several *abstraction* procedures, where a large PN is systematically reduced to a smaller PN, while preserving some relevant property in the process. The reverse procedure, where a small PN is progressively transformed into a large PN, while retaining some property in course of this transformation, is referred to as the process of *refinement* (cf. section *V.C*, [2]). We present an overview of the abstraction/refinement results in reference [1], which is stated in the more general context of PNs with weighted-arcs.

A. Stepwise Refinement and Abstraction of Petri Nets of Suzuki and Murata [1]

Let $t_{in}, t_{out} \in T$ be two distinct transitions in a PN $N(\mathbf{m}^0)$, where $N = (\Pi, T, \Phi)$, and $k \in \mathcal{N}^+$ be a positive integer. We construct a PN structure $\widehat{N} = (\widehat{\Pi}, \widehat{T}, \widehat{\Phi})$ where $\widehat{\Pi} = \Pi \cup \{\pi_0\}$ ($\pi_0 \notin \Pi$), $\widehat{T} = T$, and $\widehat{\Phi} = \Phi \cup \{(\pi_0, t_{in}), (t_{out}, \pi_0)\}$. The PN structure $\widehat{N}$ is initialized with the marking $\widehat{\mathbf{m}}_k^0$, where

$$\widehat{\mathbf{m}}_k^0(p) = \begin{cases} \mathbf{m}^0(p) & \text{if } p \in \Pi \\ k & \text{if } p = \pi_0. \end{cases} \tag{1}$$

That is, the token load assigned to each place $p \in \Pi$ under marking $\widehat{\mathbf{m}}_k^0$ is essentially the same as that assigned by the marking $\mathbf{m}^0$. In addition, k-many tokens are assigned to the newly added place π_0 under $\widehat{\mathbf{m}}_k^0$. The PN $N(\mathbf{m}^0)$ is said to be *k-well behaved* (*k-WB*) with respect to $t_{in}, t_{out} \in T$ if and only if the following conditions hold –

1) (*WB1*) t_{in} is live in $\widehat{N}(\widehat{\mathbf{m}}_k^0)$,
2) (*WB2*) For any valid firing string σ_1 in $\widehat{N}(\widehat{\mathbf{m}}_k^0)$ such that $\#(\sigma_1, t_{in}) > \#(\sigma_1, t_{out})$, $\exists \sigma_2 \in (T - \{t_{in}\})^*$ such that $\sigma_1\sigma_2$ is a valid firing string in $\widehat{N}(\mathbf{m}_k^0)$ and $\#(\sigma_1\sigma_2, t_{in}) = \#(\sigma_1\sigma_2, t_{out})$, where $\#(\sigma, t)$ denotes the number of occurrences of transition t in string σ.
3) (*WB3*) For any valid firing string $\sigma \in T^*$ in $\widehat{N}(\widehat{\mathbf{m}}_k^0)$, $\#(\sigma, t_{in}) \geq \#(\sigma, t_{out})$.

If $N(\mathbf{m}^0)$ is *(k+1)-WB* with respect to two distinct transitions $t_{in}, t_{out} \in T$ for some $k \geq 1$, then $N(\mathbf{m}^0)$ is also *k-WB* with respect to $t_{in}, t_{out} \in T$ (cf. Property 1, [1]).

In section III this paper we restrict attention to PNs that satisfy the 1-WB property (i.e. k-WB, for $k = 1$). To simplify the notation for this special case in subsequent text we use the notation $\widetilde{\mathbf{m}}^0$ to denote the initial marking $\widehat{\mathbf{m}}_1^0$ (cf. equation 1, when $k = 1$).

We alert the reader to some notational issues involving subscripts in PN structures and initial markings found in subsequent text. Specifically, we will introduce a PN $N_2(\mathbf{m}_2^0)$, which parallels the PN $N(\mathbf{m}^0)$ introduced at the beginning of subsection II-A. In this context, the PN $\widehat{N_2}(\widehat{\mathbf{m}_2}^0)$ parallels $\widehat{N_2}(\widehat{\mathbf{m}}^0)$, for the special case when $k = 1$.

Consider two PNs $N_i(\mathbf{m}_i^0)$ $(i = 1, 2)$, where $N_i = (\Pi_i, T_i, \Phi_i)$, $(i = 1, 2)$, where $\Pi_1 \cap \Pi_2 = T_1 \cap T_2 = \emptyset$, along with a transition $t_0 \in T_1$ that is k-enabled, but not $(k+1)$-enabled. In addition, the PN $N_2(\mathbf{m}_2^0)$ is assumed to be *k-WB* with respect two distinct transitions $t_{in}, t_{out} \in T_2$ for some $k \in \mathcal{N}^+$. The transition $t_0 \in T_1$ is refined by the PN structure N_2 to yield a new structure $N_3 = (\Pi_3, T_3, \Phi_3)$ as follows (1) $\Pi_3 = \Pi_1 \cup \Pi_2$, (2) $T_3 = (T_1 \cup T_2) - \{t_0\}$, and (3) $\Phi_3 = \Phi_1 \cup \Phi_2 - (\Pi_1 \times \{t_0\}) - (\{t_0\} \times \Pi_1) \cup ((^\bullet t_0)_{N_1} \times t_{in}) \cup (t_{out} \times (t_0^\bullet)_{N_1})$. The structure N_3 is initialized with the marking $\mathbf{m}_3^0$, where

$$\mathbf{m}_3^0(p) = \begin{cases} \mathbf{m}_1^0(p) & \text{if } p \in \Pi_1 \\ \mathbf{m}_2^0(p) & \text{if } p \in \Pi_2 \end{cases}$$

Testing if $t_0 \in T_1$ is $(k+1)$-enabled in $N_1(\mathbf{m}_1^0)$ is decidable (cf. theorem 20, [1]). Additionally, testing if the PN $N_2(\mathbf{m}_2^0)$ is k-WB is also decidable (cf. theorem 21 and Corollary 22, [1]). When these preconditions on $N_1(\mathbf{m}_1^0)$ and $N_2(\mathbf{m}_2^0)$ are satisfied, it can be shown that the liveness of $N_3(\mathbf{m}_3^0)$ implies the liveness of $N_1(\mathbf{m}_1^0)$ and $\widehat{N_2}(\widehat{\mathbf{m}_{2_k}}^0)$. In addition, if $\forall \mathbf{m}_1^1 \in \mathfrak{R}(N_1, \mathbf{m}_1^0), \exists \mathbf{m}_1^2 \in \mathfrak{R}(N_1, \mathbf{m}_1^1)$, such that $\forall p \in^\bullet t_0, \mathbf{m}_1^2(p) \geq k$ (cf. *Condition A*, [1]), then the liveness of $N_1(\mathbf{m}_1^0)$ and $\widehat{N}(\widehat{\mathbf{m}}_{2_k}^0)$ implies the liveness of $N_3(\mathbf{m}_3^0)$ (cf. Theorem 11, [1]). Testing if $N_1(\mathbf{m}_1^0)$ satisfies *Condition A* is also decidable (cf. theorem 23, [1]).

The next subsection contains relevant results from the theory of supervisory control of PNs.

B. Supervisory Control of PNs

The paradigm of supervisory control of PNs assumes a subset of *controllable transitions* (*uncontrollable transitions*), denoted by $T_c \subseteq T$ $(T_u \subseteq T)$, can (cannot) be prevented from firing by an external agent called the supervisor. The controllable (uncontrollable) transitions are represented as filled (unfilled) boxes in graphical representation of PNs.

A *supervisory policy* $\mathcal{P} : \mathcal{N}^n \times T \rightarrow \{0, 1\}$, is a function that returns a 0 or 1 for each transition and each reachable marking. The supervisory policy $\mathcal{P}$ permits the firing of transition t_j at marking $\mathbf{m}^i$, only if $\mathcal{P}(\mathbf{m}^i, t_j) = 1$. If $t_j \in T_e(N, \mathbf{m}^i)$ for some marking $\mathbf{m}^i$, we say the transition t_j is *state-enabled* at $\mathbf{m}^i$. If $\mathcal{P}(\mathbf{m}^i, t_j) = 1$, we say the transition t_j is *control-enabled* at $\mathbf{m}^i$. A transition has to be state- and control-enabled before it can fire. The fact that uncontrollable transitions cannot be prevented from firing by the supervisory policy is captured by the requirement that $\forall \mathbf{m}^i \in \mathcal{N}^n, \mathcal{P}(\mathbf{m}^i, t_j) = 1$, if $t_j \in T_u$. This is implicitly assumed of any supervisory policy.

A string of transitions $\sigma = t_1 t_2 \cdots t_k$, where $t_j \in T (j \in \{1, 2, \ldots, k\})$ is said to be a *valid firing string* starting from the marking $\mathbf{m}^i$, if (1) $t_1 \in T_e(N, \mathbf{m}^i), \mathcal{P}(\mathbf{m}^i, t_1) = 1$, and (2) for $j \in \{1, 2, \ldots, k-1\}$ 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 $\mathcal{P}(\mathbf{m}^{i+j}, t_{j+1}) = 1$.

The set of reachable markings under the supervision of $\mathcal{P}$ in N from the initial marking $\mathbf{m}^0$ is denoted by $\mathfrak{R}(N, \mathbf{m}^0, \mathcal{P})$. 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 supervisory policy $\mathcal{P}$ is a *liveness enforcing supervisory policy* (LESP) if all transitions in $N(\mathbf{m}^0)$ are live under $\mathcal{P}$. The existence of an LESP for an arbitrary PN is undecidable [3], and is decidable for specific PN structures (cf. [4], [3], [5], [6], [7]).

In the next section we consider supervisory policies that enforce liveness in a family of PNs obtained by the refinement process of Suzuki and Murata defined in the previous subsection.

III. On Supervisory Policies that Enforce Liveness in a PN obtained by the Refinement Procedure of Suzuki and Murata [1]

Following the discussion in sections II-A and II-B, we impose a restriction on the PN $N_1(\mathbf{m}_1^0)$, where $N_1 = (\Pi_1, T_1, \Phi_1)$, and $T_1 = T_{1_c} \cup T_{1_u}$, where T_{1_c} (T_{1_u}) denotes the set of controllable (uncontrollable) transitions – *(P1)* the transition $t_0 \in T_{1_c}$.

For the PN $N_2(\mathbf{m}_2^0)$, $N_2 = (\Pi_2, T_2, \Phi_2)$, $\{t_{in}, t_{out}\} \subseteq T_2$, and $T_2 = T_{2_c} \cup T_{2_u}$, where T_{2_c} (T_{2_u}) denotes the set of controllable (uncontrollable) transitions, we require – *(P2)* $t_{in} \in T_{2_c}$, and *(P3)* for any valid firing string $\sigma_2 \in T_2^*$ in $\widehat{N_2}(\widehat{\mathbf{m}_2}^0), 0 \leq (\#(\sigma_2, t_{in}) - \#(\sigma_2, t_{out})) \leq 1$ (i.e. *WB3* property of section II-A holds for $k = 1$).

Requirements *P1* and *P2* are straightforward to verify, and are therefore decidable. Observation 3.1 notes that requirement *P3* is decidable too.

Observation 3.1: Testing if $N_2(\mathbf{m}_2^0)$ satisfies requirement *P3* is decidable.

Proof: Since $\widetilde{\mathbf{m}_2}^0(\pi_0) = 1, {}^\bullet\pi_0 = \{t_{out}\}$, and $\pi_0 \in^\bullet t_{in}$, $(\#(\sigma_2, t_{in}) - \#(\sigma_2, t_{out})) \leq 1$ for any valid firing string $\sigma_2 \in T_2^*$ in $\widehat{\mathbf{N_2}}(\widetilde{\mathbf{m}_2}^0)$. Therefore, requirement *P3* is not met if and only if $\exists \sigma_2 \in T_2^*$ that is valid in $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$, such that $\#(\sigma_2, t_{out}) \geq \#(\sigma_2, t_{in})$. Equivalently, requirement *P3* is not met if and only if $\exists \sigma_2 \in T_2^*$ such that $\widetilde{\mathbf{m}_2}^0 \xrightarrow{\sigma} \widetilde{\mathbf{m}_2}^1$ in $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$ such that $\widetilde{\mathbf{m}_2}^1(\pi_0) \geq 2$. The observation follows directly from the decidability of the *submarking coverability problem* (cf. theorem 3.4,[8]). ∎

The remainder of this section is about the various components of the proof of the main result of this paper, which is stated below.

Theorem 3.2: Let $N_1(\mathbf{m}_1^0)$ $(N_2(\mathbf{m}_2^0))$ be a PN, where $N_1 = (\Pi_1, T_1, \Phi_1)$ $(N_2 = (\Pi_2, T_2, \Phi_2))$ and $t_0 \in T_1$ $(\{t_{in}, t_{out}\} \subseteq T_2)$. Suppose $N_1(\mathbf{m}_1^0)$ $(N_2(\mathbf{m}_2^0))$ satisfies requirement *P1* (*P2* and *P3*), and $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$ is the PN that results when the construction of section II-A is applied to $N_2(\mathbf{m}_2^0)$ for $k = 1$. Additionally, let $N_3(\mathbf{m}_3^0)$ be the PN that is obtained by the refinement process of section II-A using these constituent PNs. There is a supervisory policy that enforces liveness in $N_3(\mathbf{m}_3^0)$ if and only if there are similar policies for the PNs $N_1(\mathbf{m}_1^0)$ and $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$.

We first show that if there is a supervisory policy $\mathcal{P}_3$ that enforces liveness in $N_3(\mathbf{m}_3^0)$, there is a supervisory policy $\mathcal{P}_1$ $(\mathcal{P}_2)$ that enforces liveness in $N_1(\mathbf{m}_1^0)$ $(\widehat{N_2}(\widetilde{\mathbf{m}_2}^0))$. Towards this end, we use the projection functions $f_1 : T_3^* \to T_1^*$ and $f_2 : T_3^* \to T_2^*$. Informally, for $\sigma_3 \in T_3^*$, returns $f_1(\sigma_3)$ is a projection of σ_3 on the set $T_1 \cup \{t_{in}\}$, followed by the replacement of each occurrence of $t_{in} \in T_2$ by $t_0 \in T_1$. Similarly, $f_2(\sigma_3)$ is a projection of σ_3 on the set T_2.

For a supervisory policy $\mathcal{P}_3 : \mathcal{N}^{card(\Pi_3)} \times T_3 \to \{0, 1\}$, the supervisory policy $\mathcal{P}_1 : \mathcal{N}^{card(\Pi_1)} \times T_1 \to \{0, 1\}$ is defined as $(\mathcal{P}_1(\mathbf{m}_1^1, t) = 1) \Leftrightarrow (t \in T_{1_u}) \vee \Big\{\exists \sigma_3 \in T_3^*,$ s.t. $\Big(\mathbf{m}_3^0 \xrightarrow{\sigma_3} \mathbf{m}_3^1$ under $\mathcal{P}_3$ in $N_3(\mathbf{m}_3^0)\Big) \wedge \Big(\mathcal{P}_3(\mathbf{m}_3^1, t) = 1\Big) \wedge \Big(\mathbf{m}_1^0 \xrightarrow{f_1(\sigma_3)} \mathbf{m}_1^1$ under $\mathcal{P}_1$ in $N_1(\mathbf{m}_1^0)\Big) \wedge \Big(\forall p \in \Pi_1, \mathbf{m}_1^1(p) = \mathbf{m}_3^1(p) + card((t_{out}^\bullet)_{N_3} \cap \{p\}) \times (\#(\sigma_3, t_{in}) - \#(\sigma_3, t_{out}))\Big)\Big\}$.

The supervisory policy $\mathcal{P}_2 : \mathcal{N}^{card(\Pi_2 \cup \{\pi_0\})} \times T_2 \to \{0, 1\}$ is defined as $(\mathcal{P}_2(\mathbf{m}_2^1, t) = 1) \Leftrightarrow (t \in T_{2_u}) \vee \Big\{\exists \sigma_3 \in T_3^*,$ s.t. $\Big(\mathbf{m}_3^0 \xrightarrow{\sigma_3} \mathbf{m}_3^1$ under $\mathcal{P}_3$ in $N_3(\mathbf{m}_3^0)\Big) \wedge \Big(\mathcal{P}_3(\mathbf{m}_3^1, t) = 1\Big) \wedge \Big(\widetilde{\mathbf{m}_2}^0 \xrightarrow{f_2(\sigma_3)} \widetilde{\mathbf{m}_2}^1$ under $\mathcal{P}_2$ in $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)\Big) \wedge \Big(\forall p \in \Pi_1, \widetilde{\mathbf{m}_2}^1(p) = \mathbf{m}_3^1(p)\Big)\Big\}$.

Observation 3.3 (3.4) notes that every string that is valid under the supervision of $\mathcal{P}_2$ (resp. $\mathcal{P}_3$) in $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$ (resp. $N_3(\mathbf{m}_3^0)$) has a corresponding string that is valid under the supervision of $\mathcal{P}_3$ (resp. $\mathcal{P}_2$) in $N_3(\mathbf{m}_3^0)$ (resp. $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$). These observations are established by an induction argument over the length of the string that is valid under the supervision of the policy in the implicant of each statement. These proofs are skipped for brevity (cf. [9] for details). Observations 3.3 and 3.4 imply observation 3.5, which notes that there is an LESP for $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$, if there is an LESP for $N_3(\mathbf{m}_3^0)$.

Observation 3.3: [9] If $\widetilde{\mathbf{m}_2}^0 \xrightarrow{\sigma_2} \widetilde{\mathbf{m}_2}^1$ under the supervision of $\mathcal{P}_2$, then $\exists \sigma_3 \in T_3^*$ such that (1) $f_2(\sigma_3) = \sigma_2$, (2) $\mathbf{m}_3^0 \xrightarrow{\sigma_3} \mathbf{m}_3^1$ under the supervision of $\mathcal{P}_3$ in $N_3(\mathbf{m}_3^0)$, and (3) $\forall p \in \Pi_2, \mathbf{m}_3^1(p) = \widetilde{\mathbf{m}_2}^1(p)$.

Observation 3.4: [9] If $\mathbf{m}_3^0 \xrightarrow{\sigma_3} \mathbf{m}_3^1$ under the supervision of $\mathcal{P}_3$ in $N_3(\mathbf{m}_3^0)$, then (1) $\widetilde{\mathbf{m}_2}^0 \xrightarrow{f_2(\sigma_3)} \widetilde{\mathbf{m}_2}^1$ under the supervision of $\mathcal{P}_2$, and (2) $\forall p \in \Pi_2, \mathbf{m}_3^1(p) = \widetilde{\mathbf{m}_2}^1(p)$.

Observation 3.5: [9] If the supervisory policy $\mathcal{P}_3$ enforces liveness in $N_3(\mathbf{m}_3^0)$, then the supervisory policy $\mathcal{P}_2$ enforces liveness in $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$.

The following observation notes that any LESP $\mathcal{P}_2$ for $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$ also enforces the *1-WB* property of section II-A in $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$.

Observation 3.6: [9] If the supervisory policy $\mathcal{P}_2$ enforces liveness in $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$, then it also enforces (*WB1*), (*WB2*) and (*WB3*) property of section II-A in $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$.

Observation 3.7 notes that if $\mathcal{P}_3$ is an LESP for $N_3(\mathbf{m}_3^0)$, then for every valid firing string under the supervision of $\mathcal{P}_1$ in $N_1(\mathbf{m}_1^0)$, there exists a corresponding firing string that is valid under the supervision of $\mathcal{P}_3$ in $N_3(\mathbf{m}_3^0)$.

Observation 3.7: [9] If$\mathcal{P}_3$ is an LESP for $N_3(\mathbf{m}_3^0)$, and $\mathbf{m}_1^0 \xrightarrow{\sigma_1} \mathbf{m}_1^1$ under the supervision of $\mathcal{P}_1$ in $N_1(\mathbf{m}_1^0)$, then $\exists \sigma_3 \in T_3^*$ such that (1) $f_1(\sigma_3) = \sigma_1$, and (2) $\mathbf{m}_3^0 \xrightarrow{\sigma_3} \mathbf{m}_3^1$ under the supervision of $\mathcal{P}_3$ in $N_3(\mathbf{m}_3^0)$.

The next observation is about the existence of a valid firing string under the supervision of $\mathcal{P}_1$ in $N_1(\mathbf{m}^0)$ for each valid string under the supervision of $\mathcal{P}_3$ in $N_3(\mathbf{m}_3^0)$.

Observation 3.8: [9] If $\mathbf{m}_3^0 \xrightarrow{\sigma_3} \mathbf{m}_3^1$ under the supervision of $\mathcal{P}_3$ in $N_3(\mathbf{m}_3^0)$, then (1) $\mathbf{m}_1^0 \xrightarrow{f_1(\sigma_3)} \mathbf{m}_1^1$ under the supervision of $\mathcal{P}_1$, and (2) $\forall p \in \Pi_1, \mathbf{m}_1^1(p) = \mathbf{m}_3^1(p) + card((t_{out}^\bullet)_{N_3} \cap \{p\}) \times (\#(\sigma_3, t_{in}) - \#(\sigma_3, t_{out}))$.

The following observation notes that $\mathcal{P}_1$ enforces liveness in $N_1(\mathbf{m}_1^0)$, if $\mathcal{P}_3$ enforces liveness in $N_3(\mathbf{m}_3^0)$.

Observation 3.9: [9] If the supervisory policy $\mathcal{P}_3$ enforces liveness in $N_3(\mathbf{m}_3^0)$, then the supervisory policy $\mathcal{P}_1$ enforces liveness in $N_1(\mathbf{m}_1^0)$.

The proof of this observation parallels that of observation 3.5 with appropriate changes, and is skipped for brevity. Observations 3.9 and 3.5 together imply the following lemma.

Lemma 3.10: [9] The existence of an LESP for the PNs $N_1(\mathbf{m}_1^0)$ and $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$ is necessary for the existence of a similar policy for the PN $N_3(\mathbf{m}_3^0)$.

To show the sufficiency of the above observation we define a policy $\widehat{\mathcal{P}}_3 : \mathcal{N}^{card(\Pi_3)} \times T_3 \rightarrow \{0,1\}$ in terms of policies $\widehat{\mathcal{P}}_1 : \mathcal{N}^{card(\Pi_1)} \times T_1 \rightarrow \{0,1\}$ and $\widehat{\mathcal{P}}_2 : \mathcal{N}^{card(\Pi_2)} \times T_3 \rightarrow \{0,1\}$ as follows $\widehat{\mathcal{P}}_3(\mathbf{m}_3^1, t) = 1 \Leftrightarrow (t \in T_{3_u}) \vee \Big\{\exists \sigma_3 \in T_3^* \text{ such that } \Big(\mathbf{m}_3^0 \xrightarrow{\sigma_3} \mathbf{m}_3^1 \text{ in } N_3\Big) \wedge \Big(\mathbf{m}_1^0 \xrightarrow{f_1(\sigma_3)} \mathbf{m}_1^1 \xrightarrow{f_1(t)} \mathbf{m}_1^2 \text{ under } \widehat{\mathcal{P}}_1 \text{ in } N_1\Big) \wedge \Big(\widetilde{\mathbf{m}_2}^0 \xrightarrow{f_2(\sigma_3)} \widetilde{\mathbf{m}_2}^1 \xrightarrow{f_2(t)} \widetilde{\mathbf{m}_2}^2 \text{ under } \widehat{\mathcal{P}}_2 \text{ in } N_2\Big)\Big\}$.

The following observation about valid firing strings under the supervision of $\widehat{\mathcal{P}}_3$ in $N_3(\mathbf{m}_3^0)$ and their corresponding strings in $N_1(\mathbf{m}_1^0)$ under the supervision of $\widehat{\mathcal{P}}_1$, and $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$ under the supervision of $\widehat{\mathcal{P}}_2$.

Observation 3.11: [9] Suppose $\mathbf{m}_3^0 \xrightarrow{\sigma_3} \mathbf{m}_3^1$ under the supervision of $\widehat{\mathcal{P}}_3$ in $N_3(\mathbf{m}_3^0)$. Then (1) $\mathbf{m}_1^0 \xrightarrow{f_1(\sigma_3)} \mathbf{m}_1^1$ under the supervision of $\widehat{\mathcal{P}}_1$ in $N_1(\mathbf{m}_1^0)$, (2) $\forall p \in \Pi_1, \mathbf{m}_1^1(p) = \mathbf{m}_3^1(p) + card((t_{out}^\bullet)_{N_3} \cap \{p\}) \times (\#(\sigma_3, t_{in}) - \#(\sigma_3, t_{out}))$, (3) $\widetilde{\mathbf{m}_2}^0 \xrightarrow{f_2(\sigma_3)} \widetilde{\mathbf{m}_2}^1$ under the supervision of $\widehat{\mathcal{P}}_2$ in $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$, and (4) $\forall p \in \Pi_2, \widetilde{\mathbf{m}_2}^1(p) = \mathbf{m}_3^1(p)$.

This result can be established by induction on the length of σ_3, and is skipped for brevity (cf. [9] for details). The following observation will find use in the proof of lemma 3.13.

Observation 3.12: [9] If the supervisory policy $\widehat{\mathcal{P}}_2$ enforces liveness in $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$, and if $\mathbf{m}_3^0 \xrightarrow{\sigma_3^1} \mathbf{m}_3^1$ under the supervision of $\widehat{\mathcal{P}}_3$ in $N_3(\mathbf{m}_3^0)$, then $\exists \sigma_3^2 \in (T_3 - \{t_{in}\})^*$ such that $\mathbf{m}_3^0 \xrightarrow{\sigma_3^1} \mathbf{m}_3^1 \xrightarrow{\sigma_3^2} \mathbf{m}_3^2$ under the supervision of $\widehat{\mathcal{P}}_3$ in $N_3(\mathbf{m}_3^0)$ such that $\#(\sigma_3^1\sigma_3^2, t_{in}) = \#(\sigma_3^1\sigma_2^3, t_{out})$

The following lemma notes that the existence of an LESP for $N_1(\mathbf{m}_1^0)$ and $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$ is sufficient for the existence of an LESP for $N_3(\mathbf{m}_3^0)$.

Lemma 3.13: [9] If $\widehat{\mathcal{P}}_1$ and $\widehat{\mathcal{P}}_2$ enforce liveness in $N_1(\mathbf{m}_1^0)$ and $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$ respectively, then $\widehat{\mathcal{P}}_3$ enforces liveness in $N_3(\mathbf{m}_3^0)$.

Lemma 3.13 and 3.10 together imply theorem 3.2 introduced at the beginning of this section. Also, if there is a supervisory policy that enforces liveness in $N_3(\mathbf{m}_3^0)$, then there is always a distributed implementation of a liveness enforcing policy.

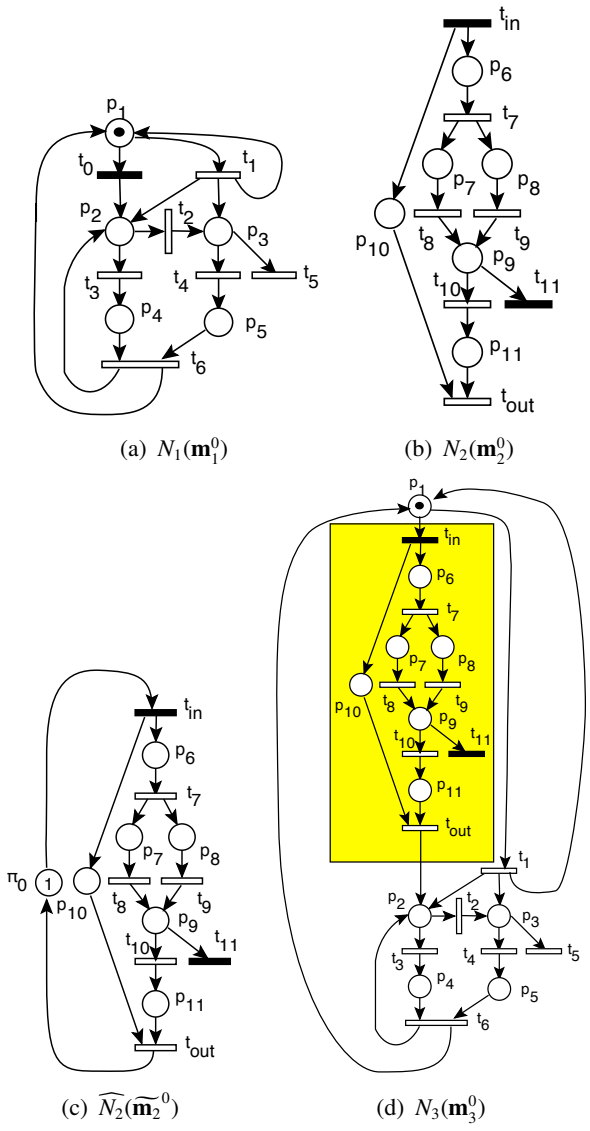
In addition to *P1*, *P2* and *P3*, suppose we required $N_1(\mathbf{m}_1^0)$ and $N_2(\mathbf{m}_2^0)$ be FCPNs. Let us also require that $t_{in} \in T_{2_c}$ be a *non-choice* transition (i.e. $({}^\bullet t_{in})_{N_2} = \emptyset$, or, $(({}^\bullet t_{in})_{N_2})^\bullet_{N_2} = \{t_{in}\}$), then $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$ is guaranteed to be an FCPN too. From theorem 3.2, we gather that there is an LESP for $N_3(\mathbf{m}_3^0)$ if and only if the FCPNs $N_1(\mathbf{m}_1^0)$ and $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$ have LESPs. If there is an LESP for an arbitrary PN, then there is a unique *minimally restrictive* LESP for the PN [3]. If the FCPNs $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$ and $N_1(\mathbf{m}_1^0)$ can be made live by supervision by $\widehat{\mathcal{P}}_2$ and $\widehat{\mathcal{P}}_1$ respectively, without loss in generality, we can assume these policies are minimally restrictive. Since minimally restrictive LESPs for FCPNs do not control-disable non-choice transitions [10], it follows that $\widehat{\mathcal{P}}_2$ will never control-disable t_{in}. Transition t_{in} is control-disabled in $N_3(\mathbf{m}_3^0)$ if and only if it is control-disabled by $\widehat{\mathcal{P}}_1$ for the equivalent marking in $N_1(\mathbf{m}_1^0)$.

Consider the FCPN $N_1(\mathbf{m}_1^0)$ shown in figure 1(a) and the FCPN $N_2(\mathbf{m}_2^0)$ shown in figure 1(b). The FCPN $N_1(\mathbf{m}_1^0)$ meets requirement *P1*, and the FCPN $N_2(\mathbf{m}_2^0)$ meets requirement *P2* and *P3*. Specifically, requirement *P3* is enforced by $p_{10} \in t_{in}^\bullet \cap {}^\bullet t_{out}$. Since $({}^\bullet t_{in})_{N_2} = \emptyset$, the PN $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$, show in figure 1(c), is also an FCPN.

The FCPN $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$ can be made live by the (minimally restrictive) supervisory policy $\widehat{\mathcal{P}}_2$ that control-disables t_{11} when p_9 has the only token in the place-set $\{\pi_0, p_6, p_7, p_8, p_9, p_{11}\}$. This supervisory policy does not control-disable the non-choice transition t_{in} for any reachable marking in $\widehat{N_2}(\widetilde{\mathbf{m}_2}^0)$ (cf. [10]).

A supervisory policy $\widehat{\mathcal{P}}_1$ that makes sure the current marking of $N_1(\mathbf{m}_1^0)$ does not leave the right-closed set of markings whose minimal elements are $\{(1\ 0\ 0\ 0\ 0)^T, (0\ 0\ 0\ 1\ 1)^T\}$ enforces liveness in $N_1(\mathbf{m}_1^0)$ (cf. [4]). From theorem 3.2 we know there

is a supervisory policy that enforces liveness in the PN $N_3(\mathbf{m}_3^0)$ shown in figure 1(d). This supervisory policy can be implemented in a distributed fashion. That is, the decision of control-disabling t_{11} can be made using just the token loads of the place-set $\{\pi_0, p_6, p_7, p_8, p_9, p_{11}\}$, where the token load of (the fictitious place) π_0 is unity only if the number of occurrences of t_{in} equals that of t_{out} in the past transition firings. The transition t_{in} is control-enabled only when there is at least one token in p_4 and p_5.



(a) $N_1(\mathbf{m}_1^0)$ (b) $N_2(\mathbf{m}_2^0)$

(c) $\widehat{N_2}(\widehat{\mathbf{m}_2}^0)$ (d) $N_3(\mathbf{m}_3^0)$

Fig. 1. (a) An FCPN $N_1(\mathbf{m}_1^0)$, that meets requirement *P1*. (b) An FCPN $N_2(\mathbf{m}_2^0)$ that meets requirements *P2* and *P3*. (c) $\widehat{N_2}(\widehat{\mathbf{m}_2}^0)$, which is also an FCPN, and (d) The FCPN $N_3(\mathbf{m}_3^0)$ obtained by the refinement process of section II-A.

IV. Conclusions

In this paper we extended the refinement procedure of Suzuki and Murata [1] to yield distributed supervisory policies that enforce liveness in a class of Petri nets.

References

[1] I. Suzuki and T. Murata, "A method for stepwise refinement and abstraction of petri nets," *Journal of Computer and System Sciences*, vol. 27, pp. 51–76, 1983.

[2] T. Murata, "Petri nets: Properties, analysis and applications," *Proceedings of the IEEE*, vol. 77, no. 4, pp. 541–580, 1989.

[3] 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, July 1997.

[4] ——, "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, February 2012.

[5] 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*, pp. 1157–1160, October 2013.

[6] 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, August 2013.

[7] E. Salimi, N. Somnath, and R. Sreenivas, "A software tool for live-lock avoidance in systems modeled using a class of petri nets," *nternational Journal of Computational Science & Applications*, vol. 5, no. 2, pp. 1–13, April 2015.

[8] M. Hack, "Decidability questions for petri nets," Ph.D. Thesis, M.I.T., Cambridge, MA, June 1976, mIT-LCS-TR-161.

[9] N. Somnath and R. Sreenivas, "On distributed supervisory policies that enforce liveness in controlled petri nets," ISE, UIUC, Urbana, IL, Tech. Report UILU-ENG-2011-2102., August 2011.

[10] R. Sreenivas, "Some observations on supervisory policies that enforce liveness in partially controlled Free Choice Petri nets," *Mathematics and Computers in Simulation*, vol. 70, pp. 266–274, 2006.