Design of $\mathcal{T}$-Liveness Enforcing Supervisors in Petri Nets

Marian V. Iordache, *Student Member, IEEE*, and Panos J. Antsaklis, *Fellow, IEEE*

***Abstract*—This paper presents a procedure for the design of supervisors that enforce the transitions in a given set $\mathcal{T}$ to be live. $\mathcal{T}$-liveness enforcement corresponds to full liveness enforcement when $\mathcal{T}$ equals the total set of transitions. Rather than assuming a given initial marking, this procedure generates at every iteration a convex set of admissible initial markings. In the case of full liveness enforcement and under certain conditions also in the case of $\mathcal{T}$-liveness enforcement, the convex set of each iteration includes the set of markings for which liveness/$\mathcal{T}$-liveness can be enforced. When the procedure terminates, and if it terminates, the final convex set contains only markings for which $\mathcal{T}$-liveness can be enforced. Then, the supervisor keeping the Petri net (PN) marking in this convex set can be easily designed using the place invariant based approach. This paper focuses on the fully controllable and observable PNs. Several extensions of the procedure, including to partially controllable and observable PNs, are outlined.**

***Index Terms*—Deadlock prevention, liveness, Petri nets (PNs).**

I. Introduction

This paper presents a procedure for the design of supervisors that enforce the transitions in a set $\mathcal{T}$ to be live. We call this property $\mathcal{T}$-liveness. Liveness (or full liveness) is a special case of $\mathcal{T}$-liveness, as it means that all transitions in a Petri net (PN) are live. $\mathcal{T}$-liveness enforcement arises naturally when not all transitions need to be live, such as when certain transitions model failures or initialization processes.

The procedure presented in this paper makes no assumptions on the PN structure; the PNs are allowed to be unbounded and generalized (i.e., with integer arc weights). The supervisors generated are least restrictive for a large class of PNs. In particular, the supervisors are always least restrictive when the procedure is used to enforce full liveness. Note also that the procedure is not dependent on the initial marking. Instead, the set of initial markings for which a supervisor enforces $\mathcal{T}$-liveness is characterized as the feasible set of a system of linear marking inequalities. Thus, a $\mathcal{T}$-liveness supervisor produced by our approach is defined for a set of initial markings, rather than for a single initial marking. Moreover, when the supervisor is least restrictive, enforcing $\mathcal{T}$-liveness by any method is possible only for the initial markings for which the supervisor is defined. This procedure can also be extended to handle PNs that have uncontrollable and/or unobservable transitions. However, the supervisors designed under this circumstance are usually not least restrictive. On the negative side, the procedure does not have guaranteed termination, and divergence may arise frequently in practice. Further, even when the procedure terminates, the computations may be complex. However, these computations are performed offline. Once a supervisor has been designed, running it in real-time involves only trivial computations.

In the literature, there is little work on $\mathcal{T}$-liveness. However, there is a number of papers on full liveness enforcement. Typically, liveness enforcement has been studied for a fixed initial marking and with various assumptions on the structure of the PN. This differentiates the prior work from the method presented in this paper. Note that the problem of characterizing the set of markings for which a PN can be made $\mathcal{T}$-live is decidable in the case of PNs with controllable and observable transitions [1]. The algorithm proposed in [1] searches the marking space to find a set of minimal markings; based on this set the least restrictive $\mathcal{T}$-liveness enforcing supervisor can be immediately derived. However, the approach of [1] is not very practical for two reasons: 1) the coverability graph is to be evaluated for every marking considered during the search and 2) the number of minimal markings may be large (e.g., exponential in the size of the net). Other constructive results on liveness enforcement are restricted to particular classes of PNs. Among them we mention the following. Liveness enforcing supervisors have been obtained for classes of conservative PNs [2]–[4]. Other classes of PNs for which liveness supervisors have been constructed are in [5] and [6]. Unfolding, which in essence generates a reduction of the reachability graph, has been used in [7] to construct liveness supervisors for n-safe PNs. Only a few papers have considered liveness enforcement under partial controllability [7], [8]. To our knowledge, to date there are no liveness enforcement methods dealing with partial observability. However, note that in practice the full observability assumption can be unrealistic.

Our approach is most related to the deadlock prevention procedure we presented in [9], and its improvement in [10]. With regard to the methodology we use, we note the following. The $\mathcal{T}$-liveness procedure does not use reachability analysis of PNs. The procedure is iterative, at every iteration correcting new deadlock situations. Using iterations to correct deadlock situations appears also in [11] and [4]. The supervision technique that we use is supervision based on place invariants [12]–[14]. Further, the procedure uses two PN transformations: one to almost ordinary PNs and another one to asymmetric-choice nets. The first transformation was inspired by a similar transformation in [11]. With regard to the second transformation, note that a transformation to free-choice nets, a particular class of asymmetric-choice nets, has also been used in [15].

Manuscript received January 18, 2002; revised March 19, 2003 and April 23, 2003. Recommended by Associate Editor R. S. Sreenivas. This work was supported by the Lockheed Martin Corporation, by the National Science Foundation under Grant NSF ECS99-12458, and by the DARPA/IXO-NEST Program under Grant AF-F30602-01-2-0526.

The authors are with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN 46556 USA (e-mail: iordache.1@nd.edu; antsaklis.1@nd.edu).

Digital Object Identifier 10.1109/TAC.2003.819078

0018-9286/03$17.00 © 2003 IEEE

Authorized licensed use limited to: UNIVERSITY NOTRE DAME. Downloaded on October 6, 2009 at 17:25 from IEEE Xplore. Restrictions apply.

The notation, the definitions, and the prior results used in this paper are given in Section II. Section III presents motivating examples. The $\mathcal{T}$-liveness procedure is defined in Section IV. Section V includes illustrative examples. The procedure is analytically proved in Section VI. Specifically, Theorem 3 proves that the supervisors constructed by the $\mathcal{T}$-liveness procedure enforce $\mathcal{T}$-liveness, and Theorem 4 gives a sufficient condition for the supervisors to be least restrictive. Finally, three extensions of the procedure are presented in Section VII. First, Section VII-A shows how to obtain the least restrictive supervisor when the designed supervisor is not least restrictive. Then, Section VII-B shows how to incorporate additional constraints on the marking. Finally, Section VII-C presents the extension of the procedure to PNs with uncontrollable and unobservable transitions.

II. Preliminaries

We denote a PN by $\mathcal{N} = (P, T, F, W)$, where P is the set of places, T the set of transitions, F the set of transition arcs, and W the transition arc weight function. We use the symbol μ to denote a marking and we write $(\mathcal{N}, \mu_0)$ when we consider the PN $\mathcal{N}$ with the initial marking μ_0. The incidence matrix of a PN is denoted by D, where the rows correspond to places and the columns to transitions. Also, by denoting a place by p_i or a transition by t_j, we usually mean that p_i corresponds to the i'th row of D and t_j to the j'th column of D. We write $\mu \xrightarrow{\sigma} \mu'$ to express that the marking μ enables the firing sequence σ, and μ' is reached by firing σ.

A PN $\mathcal{N} = (P, T, F, W)$ is **ordinary** if $\forall f \in F : W(f) = 1$. We call $\mathcal{N}$ PT-ordinary[1] if $\forall p \in P \, \forall t \in T$, if $(p, t) \in F$ then $W(p, t) = 1$. A PN $\mathcal{N}$ is said to be with **asymmetric choice** if for all places p_i and p_j such that $p_i \bullet \cap p_j \bullet \neq \emptyset$ we have that either $p_i \bullet \subseteq p_j \bullet$ or $p_j \bullet \subseteq p_i \bullet$.

Given a PN $(\mathcal{N}, \mu_0)$, a transition t is **live** if any reachable marking enables some firing sequence which includes t. Given $\mathcal{T} \subseteq T$, the PN is $\mathcal{T}$-live if all transitions $t \in \mathcal{T}$ are live; for $\mathcal{T} = T$, $\mathcal{T}$-liveness corresponds to the usual definition of liveness.

A **supervisor Ξ** is a function $\Xi : \mathbb{N}^{|P|} \to 2^T$ that[2] maps to every marking a set of transitions that the PN is allowed to fire. We denote by $\mathcal{R}(\mathcal{N}, \mu_0, \Xi)$ the set of reachable markings when $(\mathcal{N}, \mu_0)$ is supervised with Ξ. We say that **$\mathcal{T}$-liveness can be enforced** in $\mathcal{N}$ if an initial marking μ_0 and a supervisor Ξ exist such that $(\mathcal{N}, \mu_0)$ supervised by Ξ is $\mathcal{T}$-live.

We use supervision based on place invariants [16], [14] to construct a PN representation of a supervised PN. In supervision based on place invariants the supervisor enforces a set of linear marking inequalities $L\mu \geq b$ on a PN $\mathcal{N}$. The supervisor is a PN with the same set of transitions as $\mathcal{N}$. The places of the supervisor are called **control places**. The supervised net, also called **closed-loop PN**, is the PN obtained by putting together $\mathcal{N}$ and the supervisor PN. This construction is summarized in the following theorem.

Theorem 1: [14], [13] Consider a PN with incidence matrix D_p and initial marking μ_{p0}, and a set of n_c linear constraints $L\mu_p \geq b$ to be imposed on it. If $L\mu_{p0} - b \geq 0$, then a PN supervisor with incidence matrix $D_c = LD_p$ and initial marking $\mu_{c0} = L\mu_{p0} - b$ enforces the constraint $L\mu_p \geq b$ when included in the closed-loop system $D_S = [D_p^T, \, D_c^T]^T$. Furthermore, the supervision is least restrictive.

It can be seen that in Theorem 1, the control places satisfy the invariant equation

$$L\mu_p - \mu_c = b. \tag{1}$$

A **siphon** is a set of places $S \subseteq P$, $S \neq \emptyset$, such that $\bullet S \subseteq S \bullet$. A siphon S is **minimal** if there is no siphon $S' \subset S$. A siphon S is **controlled** with respect to a initial marking or a set of initial markings if for all reachable markings it contains at least one token. Also, given a marking μ, S is **empty** if the total marking of S is zero. The requirement that a siphon S is controlled can be written as

$$\sum_{p \in S} \mu(p) \geq 1 \tag{2}$$

where μ is the marking. The siphon S can be invariant controlled in order to always satisfy (2). The invariant is created by adding an additional place, called *control place*, which we denote by C. See Theorem 1 or [11], [17], [18], and [2]. Thus, the equation of the marking of C is

$$\mu(C) = \sum_{p \in S} \mu(p) - 1. \tag{3}$$

The following lemma is proven in [19]. The lemma will be later used in the proof of one of the main results.

Lemma 1: Let $\mathcal{N} = (P, T, F, W)$ be a PN of incidence matrix D. Assume that there is an initial marking μ_I which enables an infinite firing sequence σ. Let $U \subseteq T$ be the set of transitions which appear infinitely often in σ. Then, there is a nonnegative integer vector x such that $Dx \geq 0$, $\forall t_i \in U$: $x(i) \neq 0$ and $\forall t_i \in T \setminus U$: $x(i) = 0$.

In what follows, we introduce a special type of subnets, which we call *active subnets*. An active subnet is a part of a PN which can be made live by supervision for appropriate initial markings.

Definition 1: Let $\mathcal{N} = (P, T, F, W)$ be a PN of incidence matrix D, $T^A \subseteq T$, $P^A = T^A \bullet$, $F^A = F \cap \{(T^A \times P^A) \cup (P^A \times T^A)\}$, and W^A the restriction of W to F^A. We say that $\mathcal{N}^A = (P^A, T^A, F^A, W^A)$ is an **active subnet** of $\mathcal{N}$ if there is a nonnegative vector $x \neq 0$ such that $Dx \geq 0$ and $T^A = \{t_i \in T : x_i \neq 0\}$ (where t_i is the transition corresponding to the i'th column of D and x_i the i'th entry of x). We say that $\mathcal{N}^A$ is **$\mathcal{T}$-minimal** if $\mathcal{T} \subseteq T^A$ and $T_x^A \not\subseteq T^A$ for any other active subnet $\mathcal{N}_x^A = (P_x^A, T_x^A, F_x^A, W_x^A)$ such that $\mathcal{T} \subseteq T_x^A$.

Note that in view of Lemma 1, $\mathcal{T}$-liveness can be enforced for some initial marking iff a $\mathcal{T}$-minimal active subnet exists. Next we define a subclass of siphons, which we call *active siphons*.

Definition 2: Given an active subnet $\mathcal{N}^A$ of a PN $\mathcal{N}$, a siphon of $\mathcal{N}$ is said to be an **active siphon** (with respect to $\mathcal{N}^A$) if it is or includes a siphon of $\mathcal{N}^A$. An active siphon is **minimal** if it does not include another active siphon (with respect to the same active subnet).

Even though we consider $\mathcal{T}$-liveness enforcement in arbitrary PNs, the following theorem is fundamental to our approach, in

[1] The name reflects the fact that all arcs (p, t) from a place p to a transition t satisfy the requirement of an ordinary PN that $W(p, t) = 1$.

[2] $|P|$ denotes the number of elements of P.

Authorized licensed use limited to: UNIVERSITY NOTRE DAME. Downloaded on October 6, 2009 at 17:25 from IEEE Xplore. Restrictions apply.

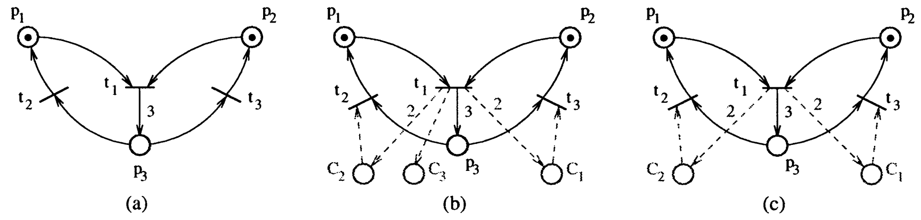


Fig. 1. Motivating examples.

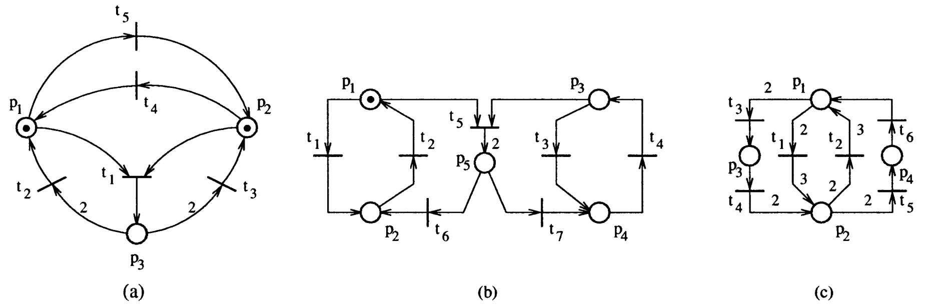


Fig. 2. Motivating examples.

which we iteratively generate intermediary PNs that are PT-ordinary and with asymmetric choice.

Theorem 2: [19] Given a PT-ordinary asymmetric-choice PN $\mathcal{N}$, let $\mathcal{T}$ be a set of transitions and $\mathcal{N}^A$ a $\mathcal{T}$-minimal active subnet. If all minimal active siphons with respect to $\mathcal{N}^A$ are controlled, the PN is $\mathcal{T}$-live (and T^A-live).

The previous theorem indicates that for the purpose of enforcing $\mathcal{T}$-liveness, we can restrict our attention to the control of the siphons which are minimal and active.

III. Motivation

Consider the PN of Fig. 1(a). It is of interest to determine all initial markings for which a liveness enforcing supervisor exists. It can be noticed that the following set of marking inequalities characterizes all initial markings for which liveness can be enforced:

$$\mu_1 + \mu_3 \geq 1 \tag{4}$$

$$\mu_2 + \mu_3 \geq 1 \tag{5}$$

$$\mu_1 + \mu_2 + \mu_3 \geq 2. \tag{6}$$

Furthermore, each inequality is necessary; by removing any of the inequalities we can find an initial marking satisfying the remaining inequalities for which liveness cannot be enforced. Once we have come up with the set of initial markings for which liveness can be enforced, we can create a supervisor enforcing liveness as in Theorem 1. The supervised PN is shown in Fig. 1(b), where the control places C_1, C_2 and C_3 correspond to (4)–(6). As specified in Theorem 1, the initial marking of the control places depends on the initial marking μ_0 of the PN as follows:

$$\mu_{0,C_1} = \mu_{0,1} + \mu_{0,3} - 1 \tag{7}$$

$$\mu_{0,C_2} = \mu_{0,2} + \mu_{0,3} - 1 \tag{8}$$

$$\mu_{0,C_3} = \mu_{0,1} + \mu_{0,2} + \mu_{0,3} - 2. \tag{9}$$

However, it can be noticed that by removing the control place C_3 liveness is still enforced [Fig. 1(c)] for all initial markings satisfying (4)–(6). Then, to follow the notation we use in the rest of this paper, we can write (4) and (5) as matrix inequality $L\mu \geq b$, and (6) as matrix inequality $L_0\mu \geq b_0$; then we can say that liveness is enforced for all initial markings μ_0 satisfying $L\mu_0 \geq b$ and $L_0\mu_0 \geq b_0$ by the supervisor enforcing $L\mu \geq b$ (as in Theorem 1). Given a PN $\mathcal{N}$ and a set of transitions $\mathcal{T}$, the purpose of the $\mathcal{T}$-liveness procedure of this paper is to generate constraints $L\mu \geq b$ and $L_0\mu \geq b_0$ such that the supervisor enforcing $L\mu \geq b$ on $\mathcal{N}$ enforces $\mathcal{T}$-liveness for all initial markings μ_0 satisfying $L\mu_0 \geq b$ and $L_0\mu_0 \geq b_0$.

Next, consider the PN of Fig. 2(a). It can be seen that only the transitions t_4 and t_5 can be made live. So, there are no initial markings for which liveness is enforcible. However, there are initial markings for which $\{t_4, t_5\}$-liveness is enforcible. These initial markings can be described by the inequality

$$2\mu_1 + 2\mu_2 + \mu_3 \geq 2. \tag{10}$$

The only active subnet is defined by the set of transitions $T^A = \{t_4, t_5\}$, and the only siphon equals the total set of places of the PN. For all nonzero initial markings this siphon is controlled. However, a nonzero initial marking does not imply that (10) is always satisfied. This suggests that the empty siphon criterion for deadlock is not very useful for $\mathcal{T}$-liveness enforcement in PNs which are not PT-ordinary and with asymmetric choice, as is the case for this PN. Furthermore, this would also suggest the use of transformations to asymmetric-choice and PT-ordinary nets, in order to take advantage of Theorem 2.

In the PN of Fig. 2(b), there are initial markings for which liveness can be enforced. However assume that we are only interested in enforcing $\{t_1, t_2\}$-liveness. Then, the markings for which $\{t_1, t_2\}$-liveness can be enforced are described by

$$\mu_1 + \mu_2 + \mu_5 \geq 1. \tag{11}$$

The only $\{t_1, t_2\}$-minimal active subnet is $\mathcal{N}_1^A$ with $P_1^A = \{p_1, p_2\}$ and $T_1^A = \{t_1, t_2\}$. Then, $\{p_1, p_2, p_5\}$ is

Authorized licensed use limited to: UNIVERSITY NOTRE DAME. Downloaded on October 6, 2009 at 17:25 from IEEE Xplore. Restrictions apply.

the only minimal active siphon with respect to $\mathcal{N}_1^A$. Two other active subnets are $\mathcal{N}_2^A$ and $\mathcal{N}_3^A$ defined by $T_2^A = \{t_3, t_4\}$ and $T_3^A = \{t_2, t_4, t_5, t_6, t_7\}$, respectively. This example shows that a $\mathcal{T}$-minimal active subnet may not be unique: both $\mathcal{N}_1^A$ and $\mathcal{N}_3^A$ are $\{t_2\}$-minimal active subnets.

Finally, note that in some problems the set of markings for which $\mathcal{T}$-liveness can be enforced cannot be represented as a conjunction of linear marking inequalities. For such problems the $\mathcal{T}$-liveness procedure of this paper can behave in two ways: 1) it does not converge and 2) it does not generate the least restrictive $\mathcal{T}$-liveness enforcing supervisor. Note that we prove in Theorem 4 that behavior 2) may happen only if the PN has more than one $\mathcal{T}$-minimal active subnets. As an example, consider the PN of Fig. 2(c). For both markings $\mu_0 = [2, 0, 0, 0]$ and $\mu_1 = [0, 2, 0, 0]$ liveness can be enforced. However, $\mu_2 = 0.5\mu_0 + 0.5\mu_1$ is a deadlock marking. Therefore, no conjunction of linear marking inequalities can describe the set of initial markings for which liveness can be enforced.

IV. $\mathcal{T}$-Liveness Enforcing Procedure

A. Procedure

Given a target PN $\mathcal{N}_0$, the liveness enforcing procedure generates a sequence of asymmetric-choice PT-ordinary PNs, $\mathcal{N}_1$, $\mathcal{N}_2, \ldots \mathcal{N}_k$, increasingly enhanced for liveness. $\mathcal{N}_1$ is $\mathcal{N}_0$ transformed to be PT-ordinary and with asymmetric choice. The other PNs are obtained as follows: in each iteration i the new minimal active siphons of $\mathcal{N}_i$ are controlled, and then, if needed, the PN is transformed to be with asymmetric choice and PT-ordinary. Thus, the iteration i produces the asymmetric-choice PT-ordinary net $\mathcal{N}_{i+1}$. The active siphons of each $\mathcal{N}_i$ are taken with respect to an active subnet $\mathcal{N}_i^A$ computed for every iteration i; if $\mathcal{T}$ is the set of transitions of $\mathcal{N}_0$ to be enforced to be live, $\mathcal{N}_i^A$ is a $\mathcal{T}$-minimal active subnet of $\mathcal{N}_i$. Controlling a siphon involves enforcing a linear marking inequality. Let $L_i\mu \geq b_i$ be the total set of inequalities enforced in $\mathcal{N}_i$. Because $\mathcal{N}_k$ is the last PN in the sequence, it has no uncontrolled active siphons. Therefore, in view of Theorem 2, $\mathcal{N}_k$ is $\mathcal{T}$-live for all initial markings which satisfy $L_k\mu \geq b_k$. Finally, the constraints defined by (L_k, b_k) can be easily translated in constraints in terms of the markings of $\mathcal{N}_0$, which define the supervisor for liveness enforcement in $\mathcal{N}_0$.

In the procedure

- μ_p is the marking of the places which are not control places;
- μ_c is the marking of the control places;
- the PN of iteration i is $\mathcal{N}_i = (P_i, T_i, F_i, W_i)$;
- the active subnet of $\mathcal{N}_i$ is $\mathcal{N}_i^A = (P_i^A, T_i^A, F_i^A, W_i^A)$.

The procedure notation is such that (1) describes the invariants enforced by the control places at any iteration. We denote a set of constraints $X\mu \geq x$ as (X, x). We give the detailed description of the specific steps of the procedure in the following subsections. Thus, we annotate the procedure steps with the number of the subsection in which we describe in detail the specific operation.

```
Input: The target PN $\mathcal{N}_0$ and $\mathcal{T} \neq \emptyset$.
Output: Two sets of constraints $(L, b)$ and $(L_0, b_0)$.
A. $\mathcal{N}_0$ is transformed to be PT-ordinary and with asymmetric choice (Section IV-C).[3] The transformed net is $\mathcal{N}_1$. Let $i = 1$, $P = P_1$, and $\mathcal{C} = \emptyset$.
B. A $\mathcal{T}$-minimal active subnet $\mathcal{N}_1^A$ is computed for $\mathcal{N}_1$ (Section IV-D).[4] If none exists, the procedure terminates and declares that $\mathcal{T}$-liveness cannot be enforced for any initial marking.
C. While true do
 1) Let $(A, d)$ and $(A_0, d_0)$ be empty sets of marking constraints.
 2) If no uncontrolled minimal active siphon is found (Section IV-B.2), the next step is D.[5]
 3) For every uncontrolled minimal active siphon $S$:
  Test whether (2) needs control place enforcement (Section IV-B.2). If it does, include (2) in $(A, d)$.
  Else include (2) in $(A_0, d_0)$.
 4) Let $\mathcal{N}_i' = (P_i', T_i', F_i', W_i')$ be the PN structure obtained by enforcing $A\mu \geq d$ in $\mathcal{N}_i$ as in Theorem 1, and let $A^I\mu' = d$ be the corresponding place invariant equations (see (1)).
 5) If $\mathcal{N}_i'$ is not PT-ordinary and with asymmetric choice, the PN is transformed to be so (Section IV-C); let $\mathcal{N}_{i+1}$ be the transformed net. Update $A^I$ according to the net transformations (Section IV-C.III). Let $A^u$ be the updated $A^I$ (this means that $A^I\mu' = d$ in $\mathcal{N}_i'$ corresponds to $A^u\mu = d$ in $\mathcal{N}_{i+1}$, where $\mu'$ and $\mu$ are markings of $\mathcal{N}_i'$ and $\mathcal{N}_{i+1}$).
 6) Let $P = P \cup (P_{i+1} \setminus P_i')$, $\mathcal{C}^o = \mathcal{C}$, and $\mathcal{C} = \mathcal{C} \cup (P_i' \setminus P_i)$. Let [6]$\mu_p = \mu|_P$ and $\mu_c = \mu|_\mathcal{C}$, for any marking $\mu$ of $\mathcal{N}_{i+1}$. For each place in $P_{i+1} \setminus P_i'$ add a null column to each of $L$ and $L_0$, to match the size of $\mu$. Similarly, add null columns to $A_0$ to match the size of $\mu$. Let [7]$A_p = A^u|_P$, $A_{p0} = A_0|_P$, $A_c = A^u|_{\mathcal{C}^o}$, and $A_{c0} = A_0|_{\mathcal{C}^o}$.
 7) If $(L, b)$ is empty, include $A_p\mu_p \geq d$ in $(L, b)$ and $A_{p0}\mu_p \geq d_0$ in $(L_0, b_0)$.
 Else, do the following
 (a) If $(A_0, d_0)$ is not empty, include $(A_{p0} + A_{c0}L)\mu_{p0} \geq d_0 + A_{c0}b$ in $(L_0, b_0)$.
```

[3] Transforming PNs to PT-ordinary and asymmetric-choice PNs has polynomial complexity.

[4] The computation of the active subnets has polynomial complexity.

[5] In the worst case, the number of uncontrolled minimal siphons depends exponentially of the size of the net.

[6] Given a set of places X, $\mu|_X$ is the restriction of μ to the places of X.

[7] $A^u|_P$ is the restriction of A^u to the columns corresponding to places in P; $A_0|_P$, $A^u|_{\mathcal{C}^o}$, \ldots, have a similar meaning.

Authorized licensed use limited to: UNIVERSITY NOTRE DAME. Downloaded on October 6, 2009 at 17:25 from IEEE Xplore. Restrictions apply.

```
    (b) If $(A, d)$ is not empty, include $(A_p + A_c L)\mu_p \geq d + A_c b$ in $(L, b)$.
  8) Compute the new active subnet $\mathcal{N}^A_{i+1}$ (Section IV-D). Let $i = i + 1$. The next step is C.1.
D. Restrict $L$ and $L_0$ to $\mathcal{N}_0$: $L = L|_{P_0}$ and $L_0 = L_0|_{P_0}$.
E. Optionally, the redundant constraints of $(L, b)$ and $(L_0, b_0)$ are removed.[8]
```

The final constraints (L, b) and (L_0, b_0) are such that $\mathcal{T}$-liveness is enforced for all initial markings μ_0 such that $L\mu_0 \geq b$ and $L_0\mu_0 \geq b_0$ when $(\mathcal{N}_0, \mu_0)$ is supervised according to $L\mu \geq b$. We proceed by describing specific operations involved by the procedure.

B. Generating Marking Constraints

The marking constraints generated by the procedure correspond to the constraints (2) on the uncontrolled minimal active siphons of each iteration. The constraints (2) are included in the sets of constraints (L, b) and (L_0, b_0) after being written in terms of the places of the net which are not control places; we discuss this in Section IV-B.1. Then, in Section IV-B.2, we discuss the detection of uncontrolled siphons and the detection of uncontrolled siphons which do not need a control place in order to be controlled.

1) Sets of Inequalities (L, b) and (L_0, b_0): The procedure is set up so that the PN of each iteration satisfies $\mu_c = L\mu_p - b$ (and so $L\mu_p \geq b$) for all reachable markings if $\mu_c = L\mu_p - b$ is satisfied at the initial marking. The constraints $L\mu_p \geq b$ are recursively obtained as follows. The siphons in a iteration i may contain control places added in previous iterations. So, (2) may involve not only places of the target net $\mathcal{N}_0$, but also control places. However, the marking of the control places appearing in (2) can be eliminated by using $\mu_c = L\mu_p - b$. Thus, the operations in the step C.7 correspond to adding new constraints to (L, b) and (L_0, b_0), after substituting the control place markings by $\mu_c = L\mu_p - b$.

2) Siphons Not Needing Control: Here, we discuss the step C.3 of the procedure. A siphon S is **uncontrolled** if (2) is not implied by $\mu_c = L\mu_p - b$, $L_0\mu_p \geq b_0$, $A\mu \geq d$, and $A_0\mu \geq d_0$. In other words, S is uncontrolled iff the system of $\mu|_S = 0$, $\mu_c = L\mu_p - b$, $L_0\mu_p \geq b_0$, $A\mu \geq d$, and $A_0\mu \geq d_0$ has an integer solution $\mu \geq 0$. We design the procedure, in particular the transformation to PT-ordinary asymmetric-choice PNs, in such a way that an uncontrolled siphon is always a siphon which did not exist at a previous iteration. Thus, at step C.3, it is enough to check only the new siphons which appeared due to the steps C.4 and C.5 of the previous iteration. It can be seen that checking whether a siphon is uncontrolled may involve solving an integer program.

There are siphons which satisfy (2) at all reachable markings if (2) is satisfied at the initial marking. Such siphons do not need a control place to ensure that (2) is satisfied. We identify that an uncontrolled siphon S does not need a control place C by checking whether C would satisfy $C\bullet \subseteq \bullet S$. When this is the case, (2) is included in (A_0, d_0), which contains constraints on the initial marking.

C. Transforming PNs to PT-Ordinary Asymmetric-Choice PNs

The transformation of PNs to PT-ordinary asymmetric-choice PNs consists of applying first a transformation to PT-ordinary PNs, which we call *PT-transformation*, and then of a transformation to asymmetric-choice PNs, which we call *AC-transformation*. There are many ways in which these transformations could be done. Our concern has been to design the transformations so that we can prove the procedure generates $\mathcal{T}$-liveness supervisors, and the supervisors are permissive. To this end we impose three requirements **R1)**, **R2)**, and **R3)**, which we state later. Before stating the requirements, we have to mention that the transformations we use employ *transition splits*; a transition is split when decomposed into a sequence of places and transitions. The requirements we impose are written in terms of the notation of the $\mathcal{T}$-liveness procedure. The requirements are as follows.

R1) No control place in $\mathcal{C}$ is in the postset of a transition created by a transition split.

R2) Any set of inequalities $X\mu \geq x$ which hold true in $\mathcal{N}_i$, hold true also in $\mathcal{N}_{i+1}$, for $i \geq 1$.[9]

R3) The constraints $A\mu \geq d$ enforced on $\mathcal{N}_i$ in step C.4 are satisfied in $\mathcal{N}_{i+1}$.[10]

1) Transformation of PNs to PT-Ordinary PNs: We use a modified form of the similar transformation from [11], and we call it the **PT-transformation**. Let $\mathcal{N} = (P, T, F, W)$ be a PN. In this transformation, each transition $t_j \in T$ such that $W(p, t_j) > 1$ for some $p \in \bullet t_j$, is **split** (decomposed) in a sequence of new places $p_{j,1}, p_{j,2}, \ldots p_{j,m-1}$ and new transitions $t_{j,0}, t_{j,1}, t_{j,2}, \ldots t_{j,m-1}$, where m is a parameter depending on t_j: $m = \max_{(p,t_j)\in F} W(p, t_j)$. The new places and transitions are connected as follows:

i) $\bullet p_{j,i} = t_{j,i}$, $t_{j,i}\bullet = p_{j,i}$ and $p_{j,i}\bullet = t_{j,i-1}$, for $i = 1 \ldots m - 1$;

ii) $\bullet t_{j,i} = \{p \in \bullet t_j : W(p, t_j) > i\}$, for $i = 0 \ldots m - 1$;

iii) $t_{j,0}\bullet = t_j\bullet$.

Note that t_j resembles very much $t_{j,0}$: $t_{j,0}$ has all the connections of t_j plus one additional transition arc. *After the transition split is performed, we denote $t_{j,0}$ by t_j.*

The **PT-transformation** consists in splitting all transitions t such that $W(p, t) > 1$ for some $p \in \bullet t$. In this way, the transformed PN is PT-ordinary. Note that

$$|p_{j,i} \bullet| = |\bullet p_{j,i}| = 1, \qquad i = 1, \ldots, m - 1 \qquad (12)$$

$$|t_{j,i} \bullet| = 1, \qquad , i = 1 \ldots m - 1. \qquad (13)$$

We use the convention that a split transition t_j is also a transition of the PT-transformed net, as we denote $t_{j,0}$ by t_j.

2) Transformation of PNs to Asymmetric-Choice PNs: Let $\mathcal{N} = (P, T, F, W)$ be a PN and $\mathcal{N}' = (P', T', F', W')$ be the transformed PN, where $P \subseteq P'$, $T \subseteq T'$. The idea of the

[8] This operation may involve integer programming.

[9] That is, for all markings μ_0 of $\mathcal{N}_i$ satisfying $(\forall \mu \in \mathcal{R}(\mathcal{N}_i, \mu_0): X\mu \geq x)$, we have that for all markings $\mu_{0,i+1}$ of $\mathcal{N}_{i+1}$ such that $\mu_{0,i+1}|_{\mathcal{N}_i} = \mu_0$, $(\forall \mu_{i+1} \in \mathcal{R}(\mathcal{N}_{i+1}, \mu_{0,i+1}): X\mu_{i+1}|_{\mathcal{N}_i} \geq x)$ holds true.

[10] If μ_{i+1} denotes a marking of $\mathcal{N}_{i+1}$, this corresponds to $\forall \mu_{i+1}: A^u \mu_{i+1} = d \Rightarrow A\mu_{i+1}|_{\mathcal{N}_i} \geq d$.

Authorized licensed use limited to: UNIVERSITY NOTRE DAME. Downloaded on October 6, 2009 at 17:25 from IEEE Xplore. Restrictions apply.

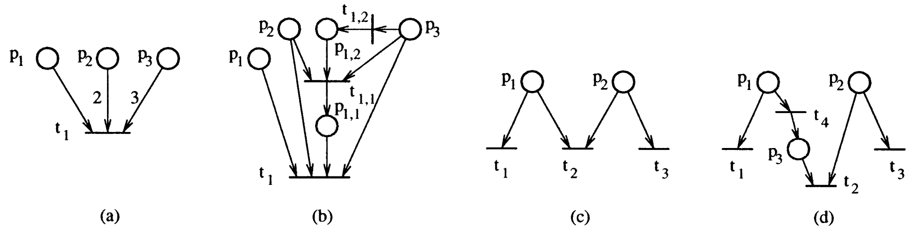


Fig. 3. Illustration of the transition split. (a) Initial configuration and (b) PT-transformation. (c) Initial configuration and (d) AC-transformation.

transformation is as follows. Given the transition t, $p_i \in \bullet t$ and $p_j \in \bullet t$ such that $p_i\bullet \not\subseteq p_j\bullet$ and $p_j\bullet \not\subseteq p_i\bullet$, remove t from either the postset of p_i or that of p_j by adding an additional place and transition, as illustrated in Fig. 3(c)–(d). Note that this operation corresponds to a modified form of the transition split of the PT-transformation. We call the transformation to asymmetric-choice PNs **AC-transformation**. The algorithm of the AC-transformation is given here.

```
Input: $\mathcal{N}$ and optionally $M \subseteq P$; the default is $M = P$.
Output: $\mathcal{N}'$
Initialize $\mathcal{N}'$ to be identical with $\mathcal{N}$.
Let $x$ be a vector indexed by the transitions of $T$. For all $t \in T$ set $x(t) = 1$ if $|\bullet t| > 1$ and $x(t) = 0$ otherwise.
While $\|x\| \neq \emptyset$ do[11]
 1) Select a transition $t \in \|x\|$ and set $x(t) = 0$.
 2) Construct $U = \{(p_i, p_j) \in P \times P : p_i \in \bullet t, p_j \in \bullet t, p_i\bullet \not\subseteq p_j\bullet \text{ and } p_j\bullet \not\subseteq p_i\bullet\}$.
 3) if $U$ is empty, then continue with the next iteration.
 4) Let $Q := \emptyset$.
 5) For every $(p_i, p_j) \in U$
  a) A place $p \in \{p_i, p_j\} \cap M$ is selected. If possible, $p$ is selected such that (i) below holds true. Else, if possible, $p$ is selected such that (ii) holds true:
    i) $p = p_i$ (or $p = p_j$) if $p_i$ (or $p_j$) has been previously selected for another element of $U$.
    ii) $p$ appears in another element of $U$.
  b) If a place $p$ could be selected (i.e., if $\{p_i, p_j\} \cap M \neq \emptyset$) then $Q := Q \cup \{p\}$.
  c) For all $t' \in p\bullet \setminus \{t\}$ set $x(t') = 1$ if $|\bullet t'| > 1$.
 6) For all $p \in Q$, delete from $\mathcal{N}'$ the transition arc $(p, t)$ and add a new place $p'$ and a new transition $t'$ such that $\bullet t' = \{p\}$, $t'\bullet = \{p'\}$, $p'\bullet = \{t\}$, $W'(p, t') = W'(t', p') = 1$, $W'(p', t) = W(p, t)$, and $x(t') = 0$.
```

Note that the operation in the step 6 of the algorithm is a **transition split**. Further, the second argument of the transformation, M, is used to select the transitions to be split. Indeed, in general there are many ways in which to choose transitions to split such that the transformed net is with asymmetric choice. The $\mathcal{T}$-liveness procedure selects M such that the requirement R2 is satisfied, thus ensuring that the constraints added in the previous iterations remain enforced. Therefore the choice of M at the AC-transformation of the step C.5 is $M = P_i' \setminus P_i$, that is, the set of control places resulted by enforcing $A\mu \geq d$ at step C.4. For the AC-transformation at the step A of the procedure, the default value of M in the AC-transformation is used.

3) Transformation Effect on Marking Constraints: Note that the way we implement the PT- and AC-transformations ensures that for all $i \geq 1, \mathcal{N}_{i+1}$ can be seen as $\mathcal{N}_i$ connected to another PN via additional arcs to the transitions of $\mathcal{N}_i$ (not unlike the connection between a plant PN and a supervisor PN). Thus, the marking constraints already enforced in $\mathcal{N}_i$ are not disturbed, and so requirement R2 is satisfied.

Let $\mathcal{N}$ be a PN and assume that $\mathcal{N}$ is PT-transformed and then AC-transformed; let $\mathcal{N}_t$ be the resulting PN. Let $l^T\mu \geq b$ be a marking constraint enforced in $\mathcal{N}$ for initial markings in some set $\mathcal{M}_I$. It can be checked that the form of $l^T\mu \geq b$ in $\mathcal{N}_t$ is $l_t^T\mu_t \geq b_t$, obtained from $l^T\mu \geq b$ with the substitution

$$\mu(p) \longrightarrow \mu_t(p) + \sum_{z=1}^{r} \mu_t(p_z) + \sum_{i=1}^{k} \sum_{j=1}^{m_i - 1} j\mu_t(p_{i,m_i-j}) \quad (14)$$

for each place p of $\mathcal{N}$, where k and m_i are determined in $\mathcal{N}$: $k = |p\bullet|$, $m_i = W(p, t_i)$ $\forall t_i \in p\bullet$. The places $p_{i,j}$ are the places resulted by splitting the transitions $t_i \in p\bullet$, where the notation of Section IV-C.1 is used. The places p_z are the places resulting from the AC-transformation which satisfy $\bullet\bullet p_z = p$. Consider an inequality (3) at step C.3 of iteration i which is enforced in step C.4. We use (14) in order to derive the form of (3) in $\mathcal{N}_{i+1}$. Let C be the control place enforcing (3) in $\mathcal{N}_i'$. Then (3) is transformed to

$$\mu(C) + \sum_{z=1}^{r} \mu(p_z) + \sum_{i=1}^{k} \sum_{j=1}^{m_i - 1} j\mu(p_{i,m_i-j}) = \sum_{p \in S} \mu(p) - 1 \quad (15)$$

where the notation is similar to (14): $k = |C\bullet|$, $m_i = W(C, t_i)$ $\forall t_i \in C\bullet$, $p_{i,j}$ are the places resulted by splitting the transitions $t_i \in C\bullet$, and p_z are the places resulting from the AC-transformation such that $\bullet\bullet p_z = C$. Note that the siphon S remains controlled, that is (2) is still true. Therefore requirement R3) is satisfied.

The considerations above showed that the transformations of this section satisfy the requirements R2) and R3). The next result states that R1) is also satisfied.

Proposition 1: At every iteration i, the requirement R1) is satisfied.

[11] $\|x\|$ denotes $\{t \in T : x(t) \neq 0\}$

Authorized licensed use limited to: UNIVERSITY NOTRE DAME. Downloaded on October 6, 2009 at 17:25 from IEEE Xplore. Restrictions apply.

Proof: Let $\bullet_i$ and $\bullet'_i$ denote the preset/postset operators in $\mathcal{N}_i$ and $\mathcal{N}'_i$, respectively. First, note that the transitions of $\mathcal{N}_i$ obtained through transitions splits form the set $T_i \setminus T_0$. Note also that if R1 is not satisfied, there is a control place C and a transition $t \in T_i \setminus T_0$ such that $C \in t\bullet_i$. However, $C \in t\bullet_i$ implies $|t \bullet_i| \geq 2$. So, we prove by induction that for all i and $\forall t \in T_i \setminus T_0$: $|t \bullet_i| = 1$. At $i = 1$ we have $\forall t \in T_1 \setminus T_0$: $|t\bullet_1| = 1$, by construction. Given an iteration number i, assume $\forall t \in T_i \setminus T_0$: $|t\bullet_i| = 1$. We prove $\forall t \in T_{i+1} \setminus T_0$: $|t\bullet_{i+1}| = 1$. Assume the contrary, that $\exists t \in T_{i+1} \setminus T_0$: $|t \bullet_{i+1}| > 1$. Then $t \in T_i \setminus T_0$ and there is a control place C added in step C.4 of iteration i such that $C \in t\bullet'_i$. Let S be the siphon controlled by C. Note that in view of the transition split operation, $|t \bullet_i| = 1$ implies $W_i(t, t\bullet_i) = 1$; also, since $\mathcal{N}_i$ is PT-ordinary, $W_i(p,t) = 1\ \forall p \in \bullet_i t$. Further, $C \in t\bullet'_i$ implies that $t \in \bullet_i S$ and firing t in $\mathcal{N}_i$ from some enabling marking increases the total marking of S. However, this contradicts $t \in S\bullet_i$ (since S is a siphon) and $|t \bullet_i| = 1$ in $\mathcal{N}_i$. The conclusion follows. ■

D. Computation of a $\mathcal{T}$-Minimal Active Subnet

The following algorithm computes a $\mathcal{T}$-minimal active subnet if one exists, or declares failure otherwise. A $\mathcal{T}$-minimal active subnet does not exist iff at no initial marking can all transitions of $\mathcal{T}$ be made live (see Definition 1 and Lemma 1).

```
Input: $\mathcal{N} = (P,T,F,W)$ and $\mathcal{T} \subseteq T$, $\mathcal{T} \neq \emptyset$.
Output: The $\mathcal{T}$-minimal active subnet $\mathcal{N}^A = (P^A, T^A, F^A, W^A)$.
 1) Check the feasibility of $Dx \geq 0$ subject to $x \geq 0$ and $x(t) \geq 1\ \forall t \in \mathcal{T}$, where $D$ is the incidence matrix of $\mathcal{N}$.
  If infeasible then exit and declare failure.
  else let $x_0$ be a solution,[12] $M = \|x_0\|$, and $x_s = x_0$.
 2) For $i = 1 \ldots |T|$, if $t_i \in M \setminus \mathcal{T}$ do
  a) Check the feasibility of $Dx \geq 0$ subject to $x \geq 0$, $x(t_i) = 0$, $x(t) = 0\ \forall t \in T \setminus M$ and $x(t) \geq 1\ \forall t \in \mathcal{T}$.
  b) If feasible then let $x^*$ be a solution; $M = \|x^*\|$ and $x_s = x^*$.
 3) The active subnet is $\mathcal{N}^A = (P^A, T^A, F^A, W^A)$, $T^A = \|x_s\|$, $P^A = T^A\bullet$, $F^A = F \cap \{(T^A \times P^A) \cup (P^A \times T^A)\}$ and $W^A$ is the restriction of $W$ to $F^A$.
```

This algorithm needs to be used only once, to compute $\mathcal{N}_1^A$. For $i > 1$, $\mathcal{N}_i^A$ can be obtained by repeating the changes done to $\mathcal{N}_{i-1}$ in $\mathcal{N}_{i-1}^A$, as in the following *update algorithm*.

```
Input: $\mathcal{N}_{i-1}^A = (P_{i-1}^A, T_{i-1}^A, F_{i-1}^A, W_{i-1}^A)$, $\mathcal{N}_i = (P_i, T_i, F_i, W_i)$ and the sets $\Sigma(t)$, denoting for each $t \in T_{i-1}$ which has been split the set of the new transitions in $T_i \setminus T_{i-1}$ which appeared by splitting $t$.
Output: $\mathcal{N}_i^A = (P_i^A, T_i^A, F_i^A, W_i^A)$.
 1)$T_i^A = T_{i-1}^A \cup \{t \in T_i : \exists t_u \in T_{i-1}^A \text{ and } t \in \Sigma(t_u)\}$
 2) The active subnet is $\mathcal{N}_i^A = (P_i^A, T_i^A, F_i^A, W_i^A)$, $P_i^A = T_i^A\bullet$, $F_i^A = F_i \cap \{(T_i^A \times P_i^A) \cup (P_i^A \times T_i^A)\}$ and $W_i^A$ is the restriction of $W_i$ to $F_i^A$.
```

V. Examples

This section illustrates the $\mathcal{T}$-liveness procedure on two examples.

A. Example 1 ($\mathcal{T}$-Liveness Enforcement)

Consider the PN of Fig. 4(a), which is not PT-ordinary and not with asymmetric choice. Three transitions cannot be made live, for any marking: t_1, t_2, t_3. We want to enforce $\mathcal{T}$-liveness for $\mathcal{T} = \{t_4, t_5\}$.

The first iteration begins with the PT- and AC-transformed net $\mathcal{N}_1$, in Fig. 4(b). The $\mathcal{T}$-minimal active subnet $\mathcal{N}_1^A$ is shown in Fig. 4(c). At the step C.3 there is a single minimal active siphon, $\{p_1, p_2, p_3\}$. Then, the constraint $\mu_1 + \mu_2 + \mu_3 \geq 1$ is added to (A, d). At step C.4, the control place C_1 is added [Fig. 4(d)]; the invariant $A^I \mu' = d$ is $\mu'_1 + \mu'_2 + \mu'_3 - \mu'_{C_1} = 1$. The PN $\mathcal{N}'_1$ is $\mathcal{N}_1$ plus the control place C_1, in Fig. 4(d). At step C. 5 $\mathcal{N}'_1$ is transformed to be with asymmetric-choice. The transformed net $\mathcal{N}_2$ is shown in Fig. 4(e). By (15), the updated invariant $A^u \mu = d$ is

$$\mu_1 + \mu_2 + \mu_3 - \mu_{C_1} - \mu_{p_{1,2}} - \mu_{p_{2,2}} - \mu_{p_{3,2}} = 1. \qquad (16)$$

At step C.7, since (A_0, d_0) and (L, b) are empty, only $A_p \mu_p \geq d$ is added to (L, b), where $A_p \mu_p \geq d$ is $\mu_1 + \mu_2 + \mu_3 - \mu_{p_{1,2}} - \mu_{p_{2,2}} - \mu_{p_{3,2}} \geq 1$.

At the second iteration, the only new minimal active siphon is $S = \{p_1, p_2, p_{2,1}, p_{3,1}, p_{2,2}, p_{3,2}, C_1\}$. The check whether S is uncontrolled is as follows. The siphon is uncontrolled if

$$\mu_1 + \mu_2 + \mu_{p_{2,1}} + \mu_{p_{3,1}} + \mu_{p_{2,2}} + \mu_{p_{3,2}} + \mu_{C_1} \geq 1 \qquad (17)$$

is not implied by the current constraints; in our case there is only one constraint: (16). In other words, S is uncontrolled iff the system of $\mu_1 + \mu_2 + \mu_{p_{2,1}} + \mu_{p_{3,1}} + \mu_{p_{2,2}} + \mu_{p_{3,2}} + \mu_{C_1} \leq 0$ and (16) has a nonnegative integer solution. Thus the procedure detects that S is uncontrolled, and sets (A, d) to (17). Then the control place C_2 is added in step C.4 [Fig. 4(e)]. At step C.5 we obtain the PT-transformed net $\mathcal{N}_3$, represented in Fig. 4(f). The invariant $A^u \mu = d$ is $\mu_1 + \mu_2 + \mu_{p_{2,1}} + \mu_{p_{3,1}} + \mu_{p_{2,2}} + \mu_{p_{3,2}} + \mu_{C_1} - \mu_{C_2} - \mu_{p_{c,1}} - \mu_{p_{c,2}} - \mu_{p_{c,3}} = 1$. Then, at step C.7, (L, b) is not empty; $\mu_{C_1} = L\mu_p - b$ is replaced in $A_p \mu_p \geq d$; the inequality $2\mu_1 + 2\mu_2 + \mu_3 + \mu_{p_{2,1}} + \mu_{p_{3,1}} - \mu_{p_{c,1}} - \mu_{p_{c,2}} - \mu_{p_{c,3}} - \mu_{p_{1,2}} \geq 2$ is obtained and added to (L, b).

At the third iteration, although there are new active siphons, there is no new minimal active siphon. Therefore the procedure exits the loop C at step C.2. After step D, we have

$$L = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 1 \end{bmatrix} \quad \text{and} \quad b = \begin{bmatrix} 1 \\ 2 \end{bmatrix}.$$

At step E a redundant constraint is removed. The procedure terminates with $L = [2, 2, 1]$, $b = 2$, and empty constraints (L_0, b_0). The supervised net is shown in Fig. 4(g). For all initial

[12] $L_k|_{\mathcal{N}_0}$ is L_k restricted to the columns corresponding to the places of $\mathcal{N}_0$.

Authorized licensed use limited to: UNIVERSITY NOTRE DAME. Downloaded on October 6, 2009 at 17:25 from IEEE Xplore. Restrictions apply.

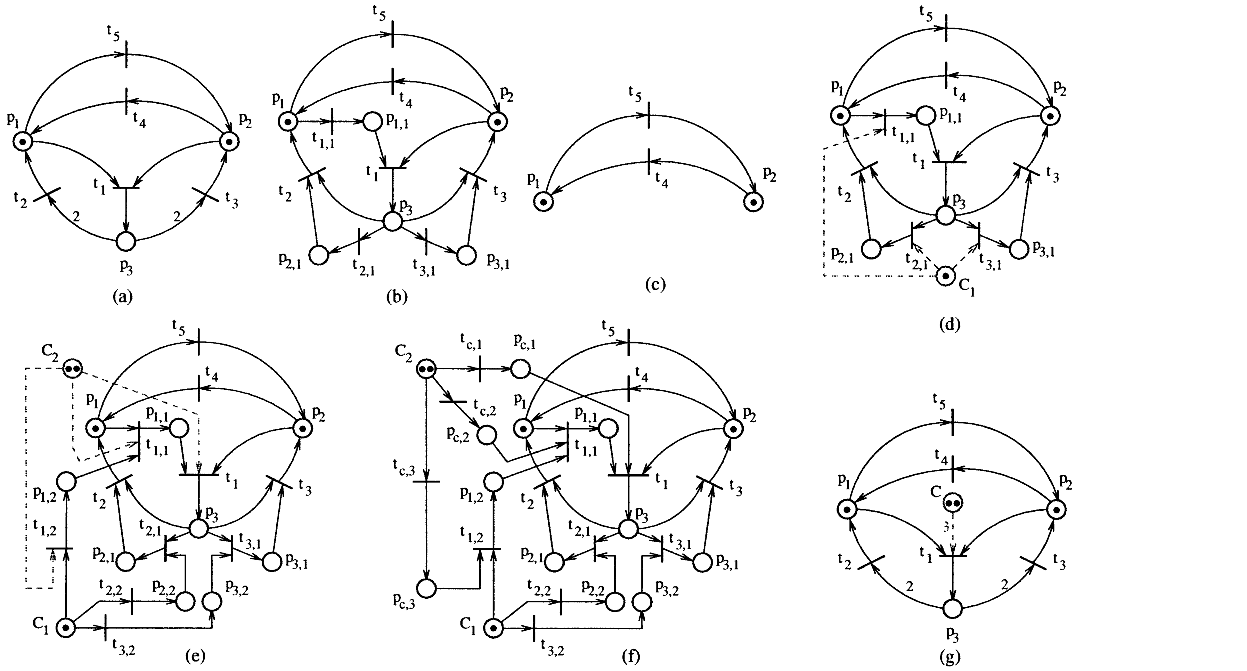


Fig. 4. Example 1. (a) $\mathcal{N}_0$. (b) $\mathcal{N}_1$. (c) $\mathcal{N}_1^A$, the same as $\mathcal{N}_2^A$ and $\mathcal{N}_3^A$. (d) $\mathcal{N}_1$ and the added control place. (e) $\mathcal{N}_2$ and added control place. (f) $\mathcal{N}_3$. (g) $\mathcal{N}_0$ supervised for $\mathcal{T}$-liveness.

markings μ_0 satisfying $L\mu_0 \geq b$, $\mathcal{T}$-liveness is enforced in a least restrictive manner (Theorems 3 and 4).

B. Example 2 (Liveness Enforcement)

Consider the PN of Fig. 5(a) for liveness enforcement. The intermediary PNs $\mathcal{N}_1$, $\mathcal{N}_2$ and $\mathcal{N}_3$ are represented in Fig. 5(b)–(d), where the control places added to $\mathcal{N}_1$, $\mathcal{N}_2$ and $\mathcal{N}_3$ are connected with dashed lines. In the first iteration, there is a single minimal siphon, $\{p_1, p_2, p_3, p_4\}$, and the control place p_7 is added. In the second iteration there are two new minimal siphons: $\{p_4, p_5, p_7, p_8\}$ and $\{p_4, p_6, p_7, p_9\}$ and two control places p_{10} and p_{11}, respectively, are thus added. In the third iteration there are two new minimal siphons: $\{p_4, p_6, p_9, p_{10}, p_{15}\}$ and $\{p_4, p_5, p_8, p_{11}, p_{14}\}$, and so the control places p_{16} and p_{17}, respectively, are added. At the fourth iteration no new minimal siphons are found, and so the procedure terminates. The constraints enforced by p_7, p_{10}, p_{11}, p_{16} and p_{17} are, respectively

$$\begin{aligned} \mu_1 + \mu_2 + \mu_3 + \mu_4 &\geq 1 \\ \mu_1 + \mu_2 + \mu_3 + 2\mu_4 + \mu_5 - \mu_9 &\geq 2 \\ \mu_1 + \mu_2 + \mu_3 + 2\mu_4 + \mu_6 - \mu_8 &\geq 2 \\ \mu_1 + \mu_2 + \mu_3 + 3\mu_4 + \mu_5 + \mu_6 - \mu_{12} &\geq 3 \\ \mu_1 + \mu_2 + \mu_3 + 3\mu_4 + \mu_5 + \mu_6 - \mu_{13} &\geq 3. \end{aligned}$$

After removing the redundant constraints, the supervisor of $\mathcal{N}_0$ is defined by $L = [1, 1, 1, 3]$ and $b = 3$, and is the least restrictive liveness enforcing supervisor (Theorems 3 and 4). There are no constraints (L_0, b_0).

VI. Theoretical Results

The proofs of the following results use the notation of the $\mathcal{T}$-liveness procedure (Section IV-A), and so the PN at the beginning of iteration i is $\mathcal{N}_i = (P_i, T_i, F_i, W_i)$, and the active subnet $\mathcal{N}_i^A = (P_i^A, T_i^A, F_i^A, W_i^A)$. Additionally we introduce the following definitions. A marking μ of $\mathcal{N}_i$ is **valid** if a) for all control places added in the iterations $1, \ldots, i-1$ the invariant equations of the form (15) hold true, and b) $\mu(p) = 0$ for all places p other than control places and places of $\mathcal{N}_0$. Note that all markings of $\mathcal{N}_0$ are valid. Two *valid* markings μ_i and μ_j of $\mathcal{N}_i$ and $\mathcal{N}_j$ are **equivalent** if $\mu_i(p) = \mu_j(p)$ for all places p of $\mathcal{N}_0$. Next we introduce a firing sequence notation. Both the PT- and AC-transformations (Section IV-C) perform transition splits. A transition t_i may be split in more than just one iteration, and the transitions $t_{i,k}$ resulted by splitting t_i may also be split in subsequent iterations. Given a transition t of $\mathcal{N}_0$ and an iteration number j, we denote by $\sigma_{0,j}(t)$ an arbitrary transition sequence of $\mathcal{N}_j$ such that a) $\sigma_{0,j}(t)$ enumerates the transitions (including t itself) in which t of $\mathcal{N}_0$ is successively split until (and including) the iteration $j-1$, and b) valid markings μ of $\mathcal{N}_j$ exist such that μ enables $\sigma_{0,j}(t)$. In this way firing the sequence $\sigma_{0,j}(t)$ in $\mathcal{N}_j$ corresponds to firing t in $\mathcal{N}_0$. If t is not split, we let $\sigma_{0,j}(t) = t$. The notation $\sigma_{i,j}(t)$ for $i < j$ and t in $\mathcal{N}_i$, is similarly defined by taking $\mathcal{N}_i$ instead of $\mathcal{N}_0$. If $\sigma = t_1t_2t_3, \ldots$, we let $\sigma_{i,j}(\sigma) = \sigma_{i,j}(t_1)\sigma_{i,j}(t_2)\sigma_{i,j}(t_3)\ldots$. For instance, in Example 1 $\sigma_{0,2}(t_2) = t_{2,1}t_2$, in Example 2 $\sigma_{0,1}(t_4)$ is any of $t_8t_9t_4$ and $t_9t_8t_4$ and $\sigma_{2,3}(t_{10}) = t_{14}t_{10}$.

A. Proof of the $\mathcal{T}$-Liveness Procedure

The next result proves that the supervisors generated by the procedure enforce $\mathcal{T}$-liveness. The assumptions are that $\mathcal{T}$-liveness enforcement is possible for some initial marking, and that the procedure terminates. In view of Definition 1 and Lemma 1, the first assumption ensures that a $\mathcal{T}$-minimal active subnet exists. When no $\mathcal{T}$-minimal active subnet exists, the

Authorized licensed use limited to: UNIVERSITY NOTRE DAME. Downloaded on October 6, 2009 at 17:25 from IEEE Xplore. Restrictions apply.

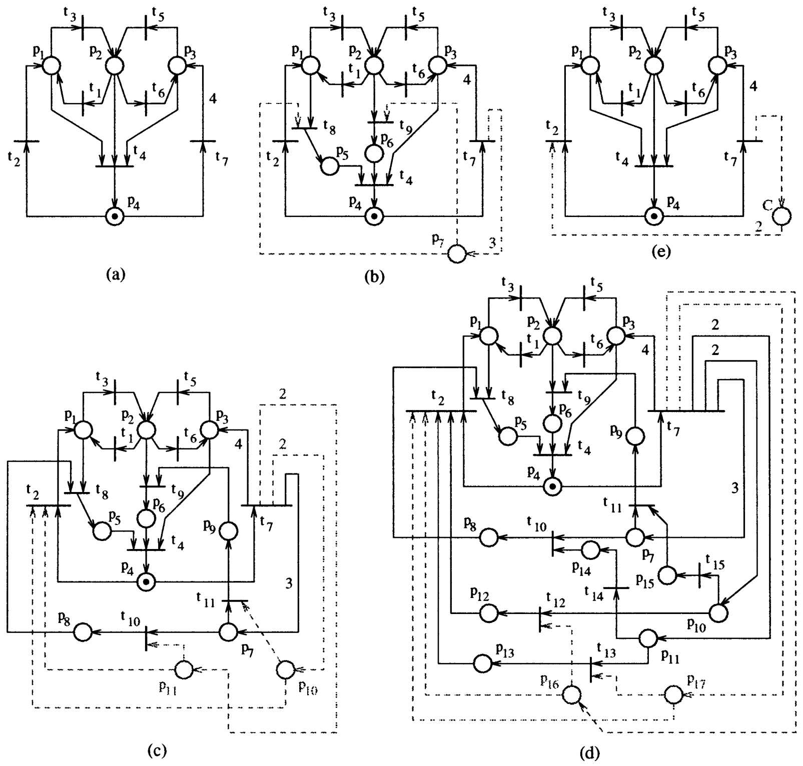


Fig. 5. Example 2. (a) $\mathcal{N}_0$. (b) $\mathcal{N}_1$. (c) $\mathcal{N}_2$. (d) $\mathcal{N}_3$. (e) the supervised PN.

procedure terminates at step B and declares that $\mathcal{T}$-liveness cannot be enforced.

Theorem 3: Assume that a $\mathcal{T}$-liveness enforcing supervisor exists for some initial marking of $\mathcal{N}_0$. If the procedure terminates, $(\mathcal{N}_0, \mu_0)$ supervised according to $L\mu \geq b$ is $\mathcal{T}$-live for all initial markings μ_0 satisfying $L\mu_0 \geq b$ and $L_0\mu_0 \geq b_0$.

Proof: The proof is by contradiction. Let k be the number of the last iteration. First, we prove that for any marking μ of $\mathcal{N}_0$ satisfying $L\mu \geq b$ and $L_0\mu \geq b_0$, the equivalent marking μ_k of $\mathcal{N}_k$ exists, and $(\mathcal{N}_k, \mu_k)$ is $\mathcal{T}$-live. Then, we show that assuming the supervised $(\mathcal{N}_0, \mu)$ not $\mathcal{T}$-live contradicts that $(\mathcal{N}_k, \mu_k)$ is $\mathcal{T}$-live. Let (L_k, b_k) and $(L_{0,k}, b_{0,k})$ be the sets of constraints (L, b) and (L_0, b_0) at the end of iteration $k-1$. The final sets of constraints (L, b) and (L_0, b_0) are obtained from $(L_k|_{\mathcal{N}_0}, b_k)$[13] and $(L_{0,k}|_{\mathcal{N}_0}, b_{0,k})$, after removing redundant constraints at step E. Let μ be a marking of $\mathcal{N}_0$, μ_k a marking of $\mathcal{N}_k$, $\mu_{k,p} = \mu_k|_{P_k \setminus \mathcal{C}}$ and $\mu_{k,c} = \mu_k|_{\mathcal{C}}$. Assume that $\mu_k|_{P_0} = \mu$ and $\mu_k(p) = 0\ \forall p \in P_k \setminus (P_0 \cup \mathcal{C})$. Then $L\mu \geq b$ and $L_0\mu \geq b_0$ imply $L_k\mu_{p,k} \geq b_k$ and $L_{0,k}\mu_{p,k} \geq b_{0,k}$. Furthermore, $L_k\mu_{p,k} \geq b_k$ implies that we can define $\mu_{k,c} = L_k\mu_{p,k} - b_k$. Thus μ_k is by construction valid and equivalent to μ. Since the procedure terminates at iteration k, $\mathcal{N}_k$ contains no uncontrolled active siphons, and so $(\mathcal{N}_k, \mu_k)$ is $\mathcal{T}$-live by Theorem 2.

Let $\mathcal{N}_S$ be the closed loop of $\mathcal{N}_0$ and the supervisor enforcing $L\mu \geq b$ (Theorem 1). Assume that from an initial marking μ_0 of $\mathcal{N}_0$ satisfying $L\mu_0 \geq b$ and $L_0\mu_0 \geq b_0$, the supervised net can reach a marking μ_S for which a transition $t \in \mathcal{T}$ is dead. We show that this leads to contradiction. Let $\mu = \mu_S|_{\mathcal{N}_0}$, and let $\mu_{0,k}$ and μ_k be the equivalent markings of μ_0 and μ in $\mathcal{N}_k$. Since $(\mathcal{N}_k, \mu_k)$ is $\mathcal{T}$-live, μ_k enables a transition sequence σ in $\mathcal{N}_k$ which includes t. Let $T_R = T_k \setminus T_0$, i.e., T_R is the set of transitions that appeared by transition split operations in all iterations. Firing any transition $t_x \in T_R$ always reduces the marking of some places in $P_0 \cup \mathcal{C}$ (Proposition 1), while firing $t_x \in T_0$ may increase the marking of some places in $P_0 \cup \mathcal{C}$. Note also that since t appears in σ, $t \in \mathcal{T}$ and $\mathcal{T} \subseteq T_0$, σ must include transitions $t_x \in T_0$. Let t_1 be the first transition in T_0 that appears in σ. Then we can write σ as $\sigma = \sigma_1\sigma_1'$, where t_1 appears only once in σ_1. It can be proved that σ_1 contains a subsequence $\sigma_{0,k}(t_1)$ (we prove this as Proposition 2 in the Appendix). Since all transitions of σ before t_1 are in T_R, and firing them only decrease markings of $P_0 \cup \mathcal{C}$, $\sigma_{0,k}(t_1)$ is enabled by μ_k. Let t_2 be the next transition of σ in T_0. Similarly, $\sigma_{0,k}(t_1)\sigma_{0,k}(t_2)$ is enabled by μ_k. We continue this way and eventually find t_j in σ and in T_0 such that $t_j = t$. We have that μ_k enables $\sigma_{0,k}(t_1)\sigma_{0,k}(t_2)\ldots\sigma_{0,k}(t_j)$. However, this implies that μ enables $t_1t_2\ldots t_j$ in $\mathcal{N}_S$, and since $t_j = t$, t is not dead in $(\mathcal{N}_S, \mu_S)$, which is a contradiction. ■

B. Permissivity

The supervisors generated by the procedure, when it terminates, are least restrictive for a large class of PNs. Our next theorem gives a sufficient condition for the supervisors to be least restrictive. Since the supervisors generated by our procedure are defined on a set of initial markings rather than on a single initial marking, we say they are least restrictive when for all initial markings μ_0 of $\mathcal{N}_0$ the following are satisfied:

- if $L\mu_0 \not\geq b$ or $L_0\mu_0 \not\geq b_0$, no $\mathcal{T}$-liveness enforcing supervisor of $(\mathcal{N}_0, \mu_0)$ exists.

[13] $L_k|_{\mathcal{N}_0}$ is L_k restricted to the columns corresponding to the places of $\mathcal{N}_0$.

Authorized licensed use limited to: UNIVERSITY NOTRE DAME. Downloaded on October 6, 2009 at 17:25 from IEEE Xplore. Restrictions apply.

– if $L\mu_0 \geq b$ and $L_0\mu_0 \geq b_0$, the supervisor enforcing $L\mu \geq b$ is the least restrictive $\mathcal{T}$-liveness enforcing supervisor of $(\mathcal{N}_0, \mu_0)$.

Theorem 4: Assume that the procedure terminates and $\mathcal{N}_1$ has a single $\mathcal{T}$-minimal active subnet. Then the $\mathcal{T}$-liveness enforcement procedure provides the least restrictive $\mathcal{T}$-liveness enforcing supervisor.

Proof: The proof is organized as follows. Let μ_0 be a marking of $\mathcal{N}_0$ and $\mu_{0,i}$ an equivalent marking of $\mathcal{N}_i$. We prove that $(\mathcal{N}_0, \mu_0)$ cannot be made $\mathcal{T}$-live if $(\mathcal{N}_i, \mu_{0,i})$ cannot be made $\mathcal{T}$-live. Then we use this fact to prove that no $\mathcal{T}$-liveness supervisors exist for the initial markings μ_0 which do not satisfy $L\mu_0 \geq b$ and $L_0\mu_0 \geq b_0$. Finally, given μ_0 satisfying $L\mu_0 \geq b$ and $L_0\mu_0 \geq b_0$, we prove that the supervisor enforcing $L\mu \geq b$ is the least restrictive $\mathcal{T}$-liveness enforcing supervisor of $\mathcal{N}_0$.

To prove our first claim, we prove by contradiction that $(\mathcal{N}_i, \mu_{0,i})$ cannot be made $\mathcal{T}$-live if $(\mathcal{N}_{i+1}, \mu_{0,i+1})$ cannot be made $\mathcal{T}$-live, where $i \geq 0$ and $\mu_{0,i+1}$ is the equivalent marking of $\mu_{0,i}$. For $i = 0$, assume that $(\mathcal{N}_0, \mu_0)$ can be made $\mathcal{T}$-live when $(\mathcal{N}_1, \mu_{0,1})$ cannot be made $\mathcal{T}$-live. Then, μ_0 enables an infinite transition sequence σ in which all transitions of $\mathcal{T}$ appear infinitely often. However, this implies that $\sigma_{0,1}(\sigma)$ is also enabled by $\mu_{0,1}$, contradicting the assumption that $(\mathcal{N}_1, \mu_{0,1})$ cannot be made $\mathcal{T}$-live. For $i \geq 1$, assume that $(\mathcal{N}_i, \mu_{0,i})$ can be made $\mathcal{T}$-live when $(\mathcal{N}_{i+1}, \mu_{0,i+1})$ cannot be made $\mathcal{T}$-live. Let σ be an infinite firing sequence enabled by $\mu_{0,i}$ such that all transitions of $\mathcal{T}$ occur infinitely often in σ. Since $(\mathcal{N}_{i+1}, \mu_{0,i+1})$ cannot be made $\mathcal{T}$-live, $\sigma' = \sigma_{i,i+1}(\sigma)$ is not enabled in $\mathcal{N}_{i+1}$. Then $\sigma = \sigma_1 t_1 \sigma_2$, $\mu_{0,i} \xrightarrow{\sigma_1} \mu_1$, $\mu_{0,i+1} \xrightarrow{\sigma_{i,i+1}(\sigma_1)} \mu_1'$, μ_1 enables t_1, but μ_1' does not enable $\sigma_{i,i+1}(t_1)$. This corresponds to the following: $\mathcal{N}_i$ has an active siphon S_1 which is controlled in $\mathcal{N}_{i+1}$ with C_1 and $\mu_1'(C_1)$ does not allow $\sigma_{i,i+1}(t_1)$ to fire. Hence, $t_1 \in C_1\bullet$ was satisfied when C_1 was added to $\mathcal{N}_i$. This implies $t_1 \in S_1\bullet$. Firing $\sigma_{i,i+1}(t_1)$ in $\mathcal{N}_{i+1}$ produces the same marking change for the places in P_i as firing t_1 in $\mathcal{N}_i$. Since $\sigma_{i,i+1}(t_1)$ is not allowed by $\mu_1'(C_1)$ to fire, firing t_1 from μ_1 empties S_1. Since t_1 is fired in the sequence $\sigma = \sigma_1 t_1 \sigma_2$, S_1 is an empty active siphon of $(\mathcal{N}_i, \mu_1)$. An empty active siphon implies a nonempty set T_x of dead transitions from the active subnet. Therefore, the transitions in T_x do not appear infinitely often in σ. Let $T_{x1} = \{t \in T_1^A : \exists t_u \in \sigma_{1,i}(t) \text{ and } t_u \in T_x\}$. The active subnets $\mathcal{N}_i^A$ for $i > 1$ are computed using the update algorithm of Section IV-D, therefore, $T_{x1} \neq \emptyset$. Using the same construction as in the proof of Theorem 3, the projection of σ on T_1 (let it be σ^1) is enabled by $\mu_{1,0}$, where $\mu_{1,0}$ is the restriction of $\mu_{i,0}$ to the places of P_1. Note that the transitions of T_{x1} do not appear infinitely often in σ^1. We apply Lemma 1 for $\mathcal{N}_1$ and σ^1, and using the notation of Lemma 1, we let $T_x^A = \|x\|$; T_x^A defines an active subnet and $\mathcal{T} \subseteq T_x^A$, as all transitions of $\mathcal{T}$ appear infinitely often in σ^1. However T_1^A is not a subset of T_x^A, for $T_1^A \setminus T_x^A \supseteq T_{x1} \neq 0$. Therefore, $\mathcal{N}_1^A$ is not the single $\mathcal{T}$-minimal subnet. This contradicts the theorem assumptions.

The second part of the proof, showing that all $\mathcal{T}$-liveness enforcing supervisors forbid the markings such that $L\mu \not\geq b$ or $L_0\mu \not\geq b_0$, is also by contradiction. Assume that $\mathcal{N}_0$ can be made $\mathcal{T}$-live for a marking μ_0 which does not satisfy all constraints $L\mu \geq b$ and $L_0\mu \geq b_0$. Let (L_d, b_d) and $(L_{0,d}, b_{0,d})$ be the constraints (L, b) and (L_0, b_0) before step D. Since step D only removes redundant constraints, μ_0 does not satisfy all constraints of $L_d\mu \geq b_d$ and $L_{0,d}\mu \geq b_{0,d}$. Let i be the first iteration in which an inequality $l_1'\mu \geq b_1$ is added such that its restriction $l_1\mu \geq b_1$ to P_0 is one of the inequalities of $L_d\mu \geq b_d$ and $L_{0,d}\mu \geq b_{0,d}$ not satisfied by μ_0. The markings forbidden at every iteration i are those for which there are empty active siphons. Therefore, $\mathcal{N}_i$ has an empty active siphon for $\mu_{0,i}$, where $\mu_{0,i}$ is the equivalent marking of μ_0 in $\mathcal{N}_i$. As shown in the previous paragraph, this implies that $(\mathcal{N}_i, \mu_{0,i})$ cannot be made $\mathcal{T}$-live. Then $(\mathcal{N}_0, \mu_0)$ cannot be made $\mathcal{T}$-live, which is a contradiction.

Finally, let μ_0 be a marking satisfying $L\mu_0 \geq b$ and $L_0\mu_0 \geq b_0$. Let Ξ_0 be the supervisor enforcing $L\mu \geq b$ on $(\mathcal{N}_0, \mu_0)$. Assume there is a $\mathcal{T}$-liveness enforcing supervisor Ξ less restrictive than Ξ_0. We show that this leads to contradiction. Let $(\mathcal{N}_0, \mu_0, \Xi_0)$ and $(\mathcal{N}_0, \mu_0, \Xi)$ be the closed loops of $(\mathcal{N}_0, \mu_0)$ with Ξ_0 and Ξ, respectively. Then there is a (possibly empty) firing sequence σ enabled from μ_0 in both $(\mathcal{N}_0, \mu_0, \Xi_0)$ and $(\mathcal{N}_0, \mu_0, \Xi)$, such that $\mu_0 \xrightarrow{\sigma} \mu$ and $\exists t \in T_0$, t is enabled by μ, t is allowed to fire at μ by Ξ, and t is not allowed to fire at μ by Ξ_0. Then, the marking μ' such that $\mu \xrightarrow{t} \mu'$ satisfies $L\mu' \not\geq b$. Therefore, by the previous part of the proof, $\mathcal{T}$-liveness cannot be enforced in $(\mathcal{N}_0, \mu')$. Then Ξ is not a $\mathcal{T}$-liveness enforcing supervisor of $(\mathcal{N}_0, \mu_0)$, which is a contradiction. ■

Note that in case of liveness enforcement $\mathcal{T}$ equals the whole set of transitions. Then the only possible $\mathcal{T}$-minimal active subnet is the whole net. Consequently, Theorem 3 has the following corollary.

Corollary 1: Assume that liveness is enforcible in $\mathcal{N}_0$ for some initial marking and the procedure terminates. If $\mathcal{T} = T_0$, the procedure provides the least restrictive liveness enforcing supervisor.

Another consequence of Theorem 4 is that the procedure will not terminate for a PN $\mathcal{N}_0$ with a single $\mathcal{T}$-minimal subnet when the set of markings for which $\mathcal{T}$-liveness can be enforced cannot be represented as a conjunction of linear marking inequalities. Finally, note that the proof of Theorem 4 ensures also that at all iterations i, the markings for which $\mathcal{T}$-liveness can be enforced in $\mathcal{N}_0$ is a subset of the set of markings satisfying (L, b) and (L_0, b_0). Formally, let L_i, b_i, $L_{0,i}$ and $b_{0,i}$ denote L, b, L_0 and b_0 after the step 7 of the iteration i. Denoting by $L_i|_{\mathcal{N}_0}$ and $L_{0,i}|_{\mathcal{N}_0}$ the restrictions of L_i and $L_{0,i}$ to the places of $\mathcal{N}_0$, we have the following result:

Corollary 2: Assume that $\mathcal{N}_1$ has a single $\mathcal{T}$-minimal active subnet. Let μ be a marking of $\mathcal{N}_0$ for which $\mathcal{T}$-liveness can be enforced. Then, for all iterations i, $L_i|_{\mathcal{N}_0}\mu \geq b_i$ and $L_{0,i}|_{\mathcal{N}_0}\mu \geq b_{0,i}$.

VII. Extensions

The procedure can be extended in several directions. First, the procedure can be extended to find the least restrictive $\mathcal{T}$-liveness enforcing supervisor even when $\mathcal{N}_1$ has several $\mathcal{T}$-minimal active subnets. Second, an additional input can be provided to the procedure, containing constraints that specify knowledge on the

Authorized licensed use limited to: UNIVERSITY NOTRE DAME. Downloaded on October 6, 2009 at 17:25 from IEEE Xplore. Restrictions apply.

initial markings for which the PN $\mathcal{N}_0$ will be used, and knowledge on the reachable space for such initial markings. Third, the procedure can be extended to handle PNs with uncontrollable and/or unobservable transitions. These three extensions are discussed next.

A. General Least Restrictive Design

Let $\mathcal{N}_1^{A,1}, \mathcal{N}_1^{A,2}, \ldots \mathcal{N}_1^{A,p}$ be the $\mathcal{T}$-minimal active subnets of $\mathcal{N}_1$. Let $\mathcal{N}_0^{A,1}, \mathcal{N}_0^{A,2}, \ldots \mathcal{N}_0^{A,p}$ be the corresponding $\mathcal{T}$-minimal active subnets in $\mathcal{N}_0$. Theorem 4 does not apply, as we have $p\,(p > 1)$ $\mathcal{T}$-minimal subnets. However, it applies for $T_0^{A,i}$-liveness, as there is a single $T_0^{A,i}$-minimal active subnet: $\mathcal{N}_1^{A,i}$ (we denote by $T_0^{A,i}$ the set of transitions of $\mathcal{N}_0^{A,i}$ and $i = 1 \ldots p$). Then the procedure can be applied for $T_0^{A,i}$-liveness enforcement for $i = 1 \ldots p$. Assuming the procedure terminates, let $L^{(i)}\mu \geq b^{(i)}$ and $L_0^{(i)}\mu \geq b_0^{(i)}$ be the generated constraints for each $i = 1 \ldots p$. Then, it can be proved [20] that the supervisor that enforces the disjunction $L^{(1)}\mu \geq b^{(1)} \vee L^{(2)}\mu \geq b^{(2)} \vee \cdots \vee L^{(p)}\mu \geq b^{(p)}$ and requires the initial marking μ_0 to satisfy also $L_0^{(1)}\mu \geq b_0^{(1)} \vee L_0^{(2)}\mu \geq b_0^{(2)} \vee \cdots \vee L_0^{(p)}\mu \geq b_0^{(p)}$, is the least restrictive $\mathcal{T}$-liveness enforcing supervisor of $\mathcal{N}_0$. This solution is also possible when the other two extensions that follow are applied. However, in the case of uncontrollable and unobservable transitions, least restrictive design is no longer guaranteed [20].

B. Additional Constraints

The $\mathcal{T}$-liveness enforcement procedure can be enhanced with two additional inputs: *initial-marking constraints* (IMCs) and *reachable-marking constraints* (RMCs). The IMCs specify initial markings of interest. The RMCs specify constraints satisfied by all markings reachable from the initial markings of interest. The IMCs and RMCs are useful as they can help the procedure converge. Assuming a set RMC of the form $L_R\mu \leq b_R$ and a set $\mathcal{M}_0$ of initial markings of interest, the following are the main changes in the $\mathcal{T}$-liveness procedure.

1) At step A: (L_0, b_0) is initialized to (L_R, b_R).
2) At step C.3: check whether (2) is consistent with $\mathcal{M}_0$. That is, after including (2) in (A, d) or (A_0, d_0), it is checked whether there are any solutions to $\mu_c = L\mu_p - b$, $L_0\mu_p \geq b_0$, $A\mu \geq d$, $A_0\mu \geq d_0$, $\mu|_{P_0} \in \mathcal{M}_0$, and $\mu_p|_{P_i \setminus P_0} = 0$, where $\mu_p = \mu|_P$ and $\mu_c = \mu|_{\mathcal{C}}$. If no solutions exist, it can be shown that no $\mathcal{T}$-liveness enforcing supervisors exist for initial markings in $\mathcal{M}_0$.

A detailed treatment of this topic can be found in [20].

C. Uncontrollable and Unobservable Transitions

In the presence of uncontrollable and/or unobservable transitions, the goal of the procedure is to ensure that the final constraints $L\mu \geq b$ obtained after the step E are *admissible*. Admissibility is the quality of a set of constraints $L\mu \geq b$ ensuring that the construction of Theorem 1 creates a supervisor that does not attempt to "control" uncontrollable transitions or "detect" firings of unobservable transitions. Methods for the transformation of inadmissible constraints to admissible constraints appear in [13] and [16]. Unfortunately, if the $\mathcal{T}$-liveness procedure generates inadmissible constraints, transforming them to admissible constraints $L_a\mu \geq b_a$ does not guarantee that enforcing $L_a\mu \geq b_a$ ensures $\mathcal{T}$-liveness [20]. Therefore, the procedure attempts to obtain constraints $L\mu \geq b$ that are admissible by construction. In fact, the procedure ensures that

$$LD_{uc} \geq 0 \quad LD_{uo} = 0 \tag{18}$$

where D_{uc} and D_{uo} are the restrictions of the incidence matrix D of $\mathcal{N}_0$ to the sets of uncontrollable and unobservable transitions, respectively. Ensuring (18) is sufficient for admissibility [13], [16]. The procedure achieves (18) by means of the following change of the step C.3.

If (2) needs control place enforcement, transform (2) to an inequality $l\mu \geq c$ that is *admissible with respect to* $\mathcal{N}_0$ and add (l, c) to (A, d). Note that if the procedure could not transform (2) to an admissible constraint (l, c), it cannot produce a $\mathcal{T}$-liveness enforcing supervisor.

Next, we describe the algorithm used to transform (2) to an inequality $l\mu \geq c$ that is admissible with respect to $\mathcal{N}_0$.

The admissibility requirement is that the constraint $l\mu \geq c$ is admissible in $\mathcal{N}_0$ when written in terms of the places of $\mathcal{N}_0$. That is, $((l_p + l_cL)\mu_p)|_{\mathcal{N}_0} \geq c + l_cb$ is to be admissible in $\mathcal{N}_0$, for $l_c = l|_{\mathcal{C}}$ and $l_p = l|_P$. Let i denote the iteration number of the algorithm. The admissibility requirement can be written as follows. Let D_{uc} and D_{uo} be the restrictions of the incidence matrix of $\mathcal{N}_0$ to the uncontrollable transitions and unobservable transitions, respectively. Let N be the matrix such that $lN = (l_p + l_cL)|_{\mathcal{N}_0}$. Then, in view of (18), we require

$$lND_{uc} \geq 0 \tag{19}$$

$$lND_{uo} = 0. \tag{20}$$

The constraint $l\mu \geq c$ should be such that the requirement R1 of Section IV-C is satisfied. Let C be the control place enforcing $l\mu \geq c$ in $\mathcal{N}_i'$. Requirement R1) for C can be written as $C \notin (T_i \setminus T_0)\bullet$, which corresponds to

$$lD_s \leq 0 \tag{21}$$

where D_s is the restriction of the incidence matrix D_i of $\mathcal{N}_i$ to the columns corresponding to the transitions of $T_i \setminus T_0$. To ensure that (2) is satisfied when $l\mu \geq c$ is satisfied, we impose

$$l(p) \geq 0 \qquad \forall p \in S \tag{22}$$

$$l(p) \leq 0 \qquad \forall p \in P_i \setminus S \tag{23}$$

$$\sum_{p \in S} l(p) \geq 1 \tag{24}$$

$$c = 1. \tag{25}$$

One situation which may cause the $\mathcal{T}$-liveness procedure to diverge is when l has a single nonzero entry; that entry is positive, in view of (24). To avoid this, failure is declared if l contains a single nonzero entry. The algorithm is as follows.

Input: $\mathcal{N}_0 = (P_0, T_0, F_0, W_0)$, T_{uc} – the set of uncontrollable transitions of $\mathcal{N}_0$, T_{uo} – the set of unobservable transitions of $\mathcal{N}_0$, P_i – the set of places at the current iteration i, the current constraints $L\mu \geq b$ and $L_0\mu \geq b_0$, and the siphon S.

Output: A constraint $l\mu \geq c$ admissible with respect to $\mathcal{N}_0$.

Authorized licensed use limited to: UNIVERSITY NOTRE DAME. Downloaded on October 6, 2009 at 17:25 from IEEE Xplore. Restrictions apply.

```
 1) Let $c=1$, $l(p)=1\ \forall p\in S$, and $l(p)=0\ \forall p\notin S$.
 2)If (19) and (20) are satisfied then exit and return $l$ and $c$.
 3) Let $f=TRUE$ and $A=S$.
 4) While $f$ is $TRUE$
  a) Check[14] the feasibility of $\sum_{p\in A} l(p)\geq 1$ with the additional constraints (19)-(24).
  b) If infeasible, set $f=FALSE$.
  c) Else let $A=A\setminus\{p\in S: l(p)\neq 0\}$; if $A=\emptyset$, set $f=FALSE$.
 5)If $|S\setminus A|<2$ then declare siphon control failure and exit.[15]
 6) Solve the linear integer program $\min_{l}(\sum_{p\in S} l(p) - \sum_{p\notin S} l(p))$ subject to $l(p) \geq 1\ \forall p\in S\setminus A$ and (19)-(24).
```

This algorithm can be illustrated on the PN of Fig. 6(a). All transitions are controllable and observable except for t_2, which is unobservable. When the procedure is applied for $\{t_1\}$-liveness, the control place p_5 is added at the first iteration, to enforce the admissible constraint $2\mu_1+\mu_3\geq 1$ (Fig. 6(b)). Then, as $W(p_5,t_3)=2$, t_3 is split, and so the place p_6 is generated [Fig. 6(c)]. We illustrate the transformation to admissible constraints on the constraint (2) for the active siphon $S=\{p_2,p_3,p_4,p_5\}$ obtained at the second iteration. At the second iteration, the matrices L_0 and b_0 are empty, while

$$L=[2\quad 0\quad 1\quad 0\quad -1] \quad \text{and} \quad b=[1].$$

At step 1 of the transformation, $l=[0,1,1,1,1,0]$ and $c=1$. At step 2, $l_p=[l_1,l_2,l_3,l_4,l_6]$ (i.e., $l_p=[0,1,1,1,0]$), $l_c=l_5$ (i.e., $l_c=1$). Let L_x be L restricted to the first four columns. Then, $N=[I_4,L_x^T,0_{4\times 1}]^T$ and $lN=[2,1,2,1]$. There are no inequalities (19) to check, as there are no uncontrollable transitions. Further, (20) is not satisfied, as $D_{uo}=[-1,-1,2,0]^T$. Therefore, (2) is not admissible with respect to $\mathcal{N}_0$. At step 4, the constraints (19)–(24) are: $-l_1-l_2+2l_3=0$ as (20), $-l_5+l_6\leq 0$ as (21), $l_i\geq 0$ for $i=2\ldots 5$ as (22), $l_i\leq 0$ for $i=1,6$ as (23), and $l_2+l_3+l_4+l_5\geq 1$ as (24). In constraint (21)$D_s=[0,0,0,0,-1,1]^T$ is the restriction of the incidence matrix to the transition t_5 – the only transition of the net generated by transition splits. Thus step 4 generates $A=\emptyset$. So, at step 6: $l=[0,2,1,1,1,0]$ and $c=1$. The constraint $l\mu\geq c$ in $\mathcal{N}_2$ corresponds to $((l_p+l_cL)\mu_p)|_{\mathcal{N}_0}\geq c+l_cb$ in $\mathcal{N}_0$, that is $2\mu_1+2\mu_2+2\mu_3+\mu_4\geq 2$, which is indeed admissible, as (18) is satisfied. Enforcing $l\mu\geq c$ generates the control place p_7 of Fig. 6(c).

Finally, note that this extension of the procedure to partial controllability and observability is in general suboptimal, in the sense that the supervisors are typically not least restrictive. A sufficient condition for optimality is given in [20].

VIII. Concluding Remarks

In this paper we have introduced a procedure which, given a Petri net and a set of transitions $\mathcal{T}$, synthesizes a supervisor enforcing all transitions in $\mathcal{T}$ to be live. The procedure relies on structural properties of Petri nets, and can be applied to arbitrary Petri nets. The procedure is optimal for a large class of Petri nets, in the sense that if it terminates, the designed supervisors are least restrictive. In particular, this optimality applies to the case of full liveness enforcement (i.e., when $\mathcal{T}$ equals the total set of transitions). A situation in which the procedure will not terminate is when our sufficient condition for optimality applies and the target Petri net has the property that the set of markings for which $\mathcal{T}$-liveness can be enforced is not the set of integer points of a convex polyhedron. However, it is possible to help the procedure terminate by using additional constraints restricting the set of initial markings of interest. The operations performed in an iteration of the procedure may be computationally complex, however all computations are performed offline; trivial computations are required to run a supervisor online. The procedure is fully automated and has been software implemented.

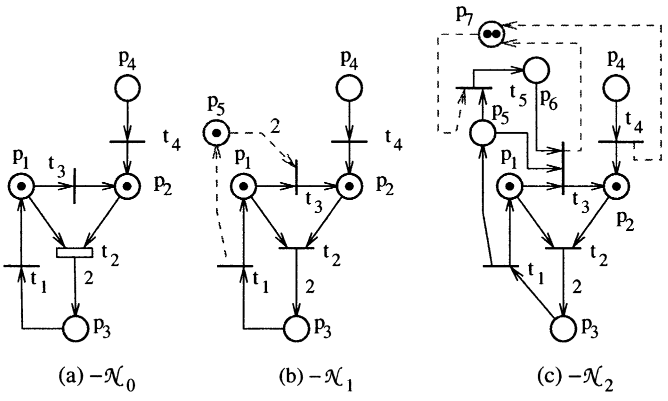


Fig. 6. Example of Section VII-C.

Appendix

Proposition 2: Let μ be a valid marking of $\mathcal{N}_k$, σ an enabled firing sequence and $t\in T_0$. Assume that t appears in σ. Then each transition $t_i\neq t$ of $\sigma_{0,k}(t)$ appears in σ before the first occurrence of t in σ; let s be the sequence in which these transitions appear in σ before the first occurrence of t in σ. There is a subsequence s_0 of s such that the sequence s_0t equals a $\sigma_{0,k}(t)$.

Proof: Let P_R be the set of places resulted through split operations in the iterations $1\ldots k-1$. The marking μ is valid, so t cannot be fired unless the places $\bullet t\cap P_R$ are marked, which cannot become marked unless the transitions in $\bullet(\bullet t\cap P_R)$ are fired. Next, let $T_{x1}=\bullet(\bullet t\cap P_R)$. The transitions of T_{x1} cannot fire unless the places $\bullet T_{x1}\cap P_R$ are marked, which cannot happen unless the transitions in $\bullet(\bullet T_{x1}\cap P_R)$ fire before. Let $T_{x2}=\bullet(\bullet T_{x1}\cap P_R)$. We continue in the same way until we get $T_{xk}=\emptyset$. This proves the first part of the proposition, as the transitions of $\sigma_{0,k}(t)$ are $\{t\}\cup T_{x1}\cup\ldots\cup T_{xk-1}$.

Given a transition t_i, let $T_x(t_i)=\bullet(\bullet t_i\cap P_R)$. Let t_1 be the last transition from $T_x(t)$ appearing in s before t. Let t_2 be the last transition from $(T_x(t)\cup T_x(t_1))\setminus\{t_1\}$ appearing in s before t_1. Let t_3 be the last transition from $(T_x(t)\cup T_x(t_1)\cup T_x(t_2))\setminus\{t_1,t_2\}$ appearing in s before t_2. We continue this way until t_m such that $(T_x(t)\cup\bigcup_{i=1}^{m} T_x(t_i))\setminus\{t_1,t_2,\ldots t_m\}=\emptyset$. Let s_0 be the sequence $t_m,t_{m-1},\ldots t_1,t$. By construction, s_0 is a sequence $\sigma_{0,k}(t)$. ■

[14] The feasibility check involves solving a linear program.

[15] $|S\setminus A|$ denotes the number of elements of $S\setminus A$.

Authorized licensed use limited to: UNIVERSITY NOTRE DAME. Downloaded on October 6, 2009 at 17:25 from IEEE Xplore. Restrictions apply.

REFERENCES

[1] R. Valk and M. Jantzen, "The residue of vector sets with applications to decidability problems in Petri nets," *Acta Inform.*, vol. 21, pp. 643–674, 1985.

[2] J. Ezpeleta, J. M. Colom, and J. Martínez, "A Petri net based deadlock prevention policy for flexible manufacturing systems," *IEEE Trans. Robot. Automat.*, vol. 11, pp. 173–184, Apr. 1995.

[3] J. Park and S. Reveliotis, "Deadlock avoidance in sequential resource allocation systems with multiple resource acquisitions and flexible routings," *IEEE Trans. Automat. Contr.*, vol. 46, pp. 1572–1583, Oct. 2001.

[4] F. Tricas, F. Garcia-Valles, J. M. Colom, and J. Ezpeleta, "New methods for deadlock prevention and avoidance in concurrent systems," *Actas de las Jornadas de Concurrencia 2000*, pp. 97–110, June 2000.

[5] R. S. Sreenivas, "An application of independent, increasing, free-choice Petri nets to the synthesis of policies that enforce liveness in arbitrary Petri nets," *Automatica*, vol. 44, no. 12, pp. 1613–1615, Dec 1998.

[6] ——, "On supervisory policies that enforce liveness in a class of completely controlled Petri nets obtained via refinement," *IEEE Trans. Automat. Contr.*, vol. 44, pp. 173–177, Jan. 1999.

[7] K. He and M. Lemmon, "Liveness-enforcing supervision of bounded ordinary Petri nets using partial order methods," *IEEE Trans. Automat. Contr.*, vol. 47, pp. 1042–1055, July 2002.

[8] J. Park and S. Reveliotis, "Liveness-enforcing supervision for resource allocation systems with uncontrollable behavior and forbidden states," *IEEE Trans. Robot. Automat.*, vol. 18, pp. 234–240, Apr. 2002.

[9] M. V. Iordache, J. O. Moody, and P. J. Antsaklis, "A method for the synthesis of deadlock prevention controllers in systems modeled by Petri nets," in *Proc. 2000 Amer. Control Conf.*, 2000, pp. 3167–3171.

[10] M. V. Iordache, "Synthesis of deadlock prevention supervisors using Petri nets," *IEEE Trans. Robot. Automat.*, vol. 18, pp. 59–68, Feb. 2002.

[11] K. Lautenbach and H. Ridder, "The linear algebra of deadlock avoidance—A Petri net approach," Univ. Koblenz, Inst. Comput. Sci., Germany, Tech. Rep., 1996.

[12] A. Giua, F. DiCesare, and M. Silva, "Generalized mutual exclusion constraints on nets with uncontrollable transitions," in *Proc. IEEE Int. Conf. Systems, Man, Cybernetics*, 1992, pp. 974–979.

[13] J. O. Moody and P. J. Antsaklis, *Supervisory Control of Discrete Event Systems Using Petri Nets*. Norwell, MA: Kluwer, 1998.

[14] E. Yamalidou, J. O. Moody, P. J. Antsaklis, and M. D. Lemmon, "Feedback control of Petri nets based on place invariants," *Automatica*, vol. 32, no. 1, pp. 15–28, 1996.

[15] R. S. Sreenivas, "On a free-choice equivalent of a Petri net," in *Proc. 36th IEEE Int. Conf. Decision Control*, 1997, pp. 4092–4097.

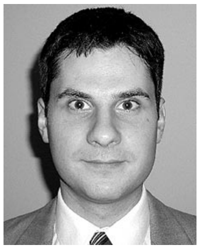
[16] J. O. Moody and P. J. Antsaklis, "Petri net supervisors for DES with uncontrollable and unobservable transitions," *IEEE Trans. Automat. Contr.*, vol. 45, pp. 462–476, Mar. 2000.

[17] K. Barkaoui and I. Abdallah, "Deadlock avoidance in fmss based on structural theory of petri nets," in *Proc. IEEE Symp. Emerging Technologies Factory Automation*, 1995.

[18] K. Barkaoui and J. F. Pradat-Peyre, "On liveness and controlled siphons in petri nets," in *Application and Theory of Petri Nets*. New York: Springer-Verlag, 1996, vol. 1091, LNCS, pp. 57–72.

[19] M. V. Iordache and P. J. Antsaklis, "Generalized conditions for liveness enforcement and deadlock prevention in Petri nets," in *Application and Theory of Petri Nets*. New York: Springer-Verlag, 2001, vol. 2075, LNCS, pp. 184–203.

[20] M. V. Iordache, "Methods for the supervisory control of concurrent systems based on Petri net abstractions," Ph.D. dissertation, Univ. Notre Dame, Notre Dame, IN, 2003.



Marian V. Iordache (S'02) received the undergraduate degree from the Politehnica University of Bucharest, Bucharest, Romania, in 1996 and the M.S. degree in electrical engineering from the University of Notre Dame, Notre Dame, IN, in 1999. He expects to receive the Ph.D. degree from the University of Notre Dame in January 2004.

His technical research interests include Petri nets, discrete-event systems, supervisory control, and hybrid systems.

Mr. Iordache was a recipient of the Center for Applied Mathematics Fellowship from the University of Notre Dame.

Panos J. Antsaklis (S'74–M'76–SM'86–F'91) received the M.S. and Ph.D. degrees from Brown University, Providence, RI, and the Undergraduate degree from the National Technical University of Athens (NTUA), Greece.

He is the H. C. and E. A. Brosey Professor of Electrical Engineering and Director of the Center for Applied Mathematics at the University of Notre Dame, Notre Dame, IN. His work includes analysis of behavior and design of control strategies for complex autonomous intelligent systems. His recent research focuses on networked embedded systems and addresses problems in the interdisciplinary research area of control, computing, and communication networks, and on hybrid and discrete-event dynamical systems. He has authored a number of publications in journals, conference proceedings and books, and he has edited four books on intelligent autonomous control and on hybrid systems. In addition, he has coauthored (with J. Moody) the research monograph *Supervisory Control of Discrete Event Systems Using Petri Nets* (Norwell, MA: Kluwer, 1998) and (with A. N. Michel) the graduate textbook *Linear Systems* (New York: McGraw-Hill, 1997).

He serves on the Editorial Boards of several journals, and he currently serves as Associate Editor at Large of the IEEE TRANSACTIONS ON AUTOMATIC CONTROL. He has been Guest Editor of Special Issues on Hybrid Systems in the IEEE TRANSACTIONS ON AUTOMATIC CONTROL and the PROCEEDINGS OF THE IEEE. He has served as Program Chair and General Chair of major systems and control conferences, and he was the 1997 President of the IEEE Control Systems Society (CSS). He is a Distinguished Lecturer of the IEEE Control Systems Society, a recipient of the IEEE Distinguished Member Award of the CSS, and an IEEE Third Millennium Medal recipient.

Authorized licensed use limited to: UNIVERSITY NOTRE DAME. Downloaded on October 6, 2009 at 17:25 from IEEE Xplore. Restrictions apply.