CLOSED-LOOP LIVE PETRI NET SUPERVISORS FOR GMEC

F. Basile*, P. Chiacchio
Dip. di Informatica e Sistemistica,
Via Claudio 21, 80125 Napoli, Italy
fbasile@unina.it, pasquale.chiacchio@unina.it

L. Recalde, M.Silva
Dep. de Informática e Ingegnería de Sistemas,
Maria de Luna 3, E-50015 Zaragoza, Spain
lrecalde@posta.unizar.es, silva@posta.unizar.es

Keywords: supervisory control, closed-loop liveness, generalized mutual exclusion constraint, monitor places, control safe marked graphs.

Abstract Avoiding forbidden states by a supervisory control policy may lead to a non live system, even in the case of generalized mutual exclusion constraints (GMECs) enforced by monitor places. This leads to a problem which is very interesting in practice, but difficult even for the restricted class of marked graphs (MGs). We obtain two sufficient conditions that guarantee liveness of a MG plant with uncontrollable transitions, controlled by a monitor. A set of predicates are derived that enforce, in a maximally permissive way, a mutual exclusion constraint and closed-loop liveness for live control safe MG under some restrictions. These predicates can be implemented by a Petri Net.

Introduction

A control theory for discrete event systems (DES) modeled by Petri Net (PN) has been developed, extending general PN models with the concept of *controllable* transitions. Two possibilities can be explored. In the first one, controllable transitions may be *disabled* by an external control input represented by the value of a logical predicate; in this case we speak of controlled PNs (CtlPNs) (L.E. Holloway et al., 1997). In the second one, that we adopt here, the *feedback control policy* is implemented by a PN whose marking enables or disables, according to the logical specifications, the controllable transitions to which are connected by arcs in the closed-loop net; controller's input arcs to *uncontrollable* transitions are not allowed. In this case we have a *compiled* supervisor

*This work has been carried on when Francesco Basile was visiting the University of Zaragoza from January to June 1999.

and the closed-loop system properties can be analyzed in a single framework, because the plant and the controller are represented by PNs. What we lose is the expressive power of the control law, that cannot always be implemented by a Petri Net, in a maximally permissive form (L.E. Holloway et al., 1997).

Here we consider the problem of forbidden state specification in conjunction with liveness specification under control. Avoiding forbidden states is a very common specification for a DES and a lot of work has been done on the subject (L.E. Holloway et al., 1997), but unfortunately, it may lead the system to deadlocks. This is due to the fact that a way to avoid forbidden states is not to allow the system to operate at all (Holloway and Krogh, 1992). In this paper we consider, as forbidden state specification, the generalized mutual exclusion constraints (GMECs) that limit a weighted sum of tokens in a subset of places. For some net subclasses it was shown that it is possible to impose a GMEC by a *monitor* (Giua et al., 1992; Yalimalidou et al., 1996): a place is added for each MEC, whose initial marking represents available units of resources and whose outgoing (only to controllable transitions) and incoming transitions represent the acquisition and release of units of resources. The monitor synthesis is very efficient from the computational point of view and it represents a compiled supervisor. It may so be possible to verify if the net controlled by a monitor is closed-loop live: some results are presented here. If this is not the case, we show that liveness may be enforced in some cases.

Because of the difficulty of the addressed problem, the relevance of MGs in automated manufacturing systems modelling, and the fact that they are a well studied net subclass, in the paper we suppose that the plant net belongs to a subclass of live MGs: MGs with control safe places (for this particular MG subclass a GMEC can be enforced by a set of monitors – Giua et al., 1993). For this MG subclass, a control synthesis method is presented here to enforce a mutual exclusion constraint in conjunction with liveness, under some restrictions.

1. BACKGROUND

A place/transition (P/T) net is a structure $N = (P, T, Pre, Post)$ where: P is a set of m *places* represented by circles; T is a set of n *transitions* represented by bars; $P \cap T = \emptyset$, $P \cup T \neq \emptyset$; $Pre : P \times T \to \mathbb{N}$ ($Post : P \times T \to \mathbb{N}$) is the pre- (post-) incidence function that specifies the input (output) arcs directed from places to transitions (from transitions to places), with $\mathbb{N}$ set of non-negative integers. The pre- and post-incidence functions can be represented as $m \times n$ matrices $\mathbf{Pre}$ and $\mathbf{Post}$ with elements $Pre(p_i, t_i)$ and $Post(p_i, t_i)$, respectively. The incidence matrix $\boldsymbol{C}$ of the net is defined as $\boldsymbol{C} = \mathbf{Post} - \mathbf{Pre}$. For pre- and post-sets we use the conventional dot notation, e.g. ${}^{\bullet}t = \{p \in P \mid \mathbf{Pre}(p, t) \neq 0\}$, which can be naturally extended to set of nodes. A *marking* is a $m \times 1$ vector $\boldsymbol{m} : P \rightarrow \mathbb{N}$ that assigns to each place of a P/T net a non-negative integer number of tokens. A P/T system or net system $< N, \boldsymbol{m}_0 >$ is a P/T net N with an initial marking $\boldsymbol{m}_0$. A transition $t \in T$ is enabled at a marking $\boldsymbol{m}$ iff $\boldsymbol{m} \geq \mathbf{Pre}(\cdot, t)$. If t is enabled, then it may fire yielding a new marking $\boldsymbol{m}' = \boldsymbol{m} + \mathbf{Post}(\cdot, t) - \mathbf{Pre}(\cdot, t) = \boldsymbol{m} + \mathbf{C}(\cdot, t)$. The notation $\boldsymbol{m}[t > \boldsymbol{m}'$ will mean that an enabled transition t may fire at $\boldsymbol{m}$ yielding $\boldsymbol{m}'$. A *firing sequence* from $\boldsymbol{m}_0$ is a (possibly empty) sequence of transitions $\sigma = t_1...t_k$ such that $\boldsymbol{m}_0[t_1 > \boldsymbol{m}_1[t_2 > \boldsymbol{m}_2..[t_k > \boldsymbol{m}_k$. A marking $\boldsymbol{m}$ is reachable in $< N, \boldsymbol{m}_0 >$ iff there exists a firing sequence σ such that $\boldsymbol{m}_0[\sigma > \boldsymbol{m}$. Given a net system $< N, \boldsymbol{m}_0 >$ the set of reachable markings is denoted $R(N, \boldsymbol{m}_0)$. The function $\boldsymbol{\sigma} : T \rightarrow \mathbb{N}$, where $\boldsymbol{\sigma}(t)$ represents the number of occurrences of t in σ, is called firing count vector of the fireable sequence σ. If $\boldsymbol{m}_0[\sigma > \boldsymbol{m}$, then we can write in vector form $\boldsymbol{m} = \boldsymbol{m}_0 + \boldsymbol{C}(\cdot, t) \cdot \boldsymbol{\sigma}$. This is known as the *state equation* of the system. The solutions of the state equation that do not correspond to reachable markings will be called *spurious*. Right annuler vectors of $\boldsymbol{C}$ are called T semiflows, i.e. $\boldsymbol{x} : T \rightarrow \mathbb{N}, \boldsymbol{x} \neq \mathbf{0} \mid \boldsymbol{C}\boldsymbol{x} = 0$. A Marked graph (MG) is an ordinary P/T net such that $\forall p \in P, \mid {}^\bullet p \mid = \mid p^\bullet \mid = 1$. A P/T system is *live* when, from every reachable marking, every transition can ultimately occur; and it is *deadlock-free* when every reachable marking enables some transition.

A *mutual exclusion constraint* (MEC) $(\boldsymbol{w}, k)$, that is expressed by a linear inequality, defines the following set of *legal markings*: $\mathcal{L} = \mathcal{M}(\boldsymbol{w}, k) \equiv \{\boldsymbol{m} \in \mathbb{N}^m \mid \boldsymbol{w} \cdot \boldsymbol{m} \leq k\}$ with $\boldsymbol{w} \in \mathbb{Z}^m, k \in \mathbb{Z}$. The support of $\boldsymbol{w}$ is the set $Q_w = \{p \in P \mid \boldsymbol{w}(p) \neq 0\}$. It was shown (Giua et al., 1992) how a general $(\boldsymbol{w}, k)$ can be reduced to the case $\boldsymbol{w} \leq \mathbf{1}$ and so it will be assumed here without loss of generality.

We assume that the set of transitions T of a net is partitioned into two disjoint subset: T_u, the set of uncontrollable transitions, and T_c, the set of controllable transitions. A controllable transitions may be disabled by the supervisor, a controlling agent which ensures that the behaviour of the system be within a legal behaviour. An uncontrollable transition represents an event which may not be prevented from occurring by a supervisor. Controllable transitions will be drawn as empty boxes, and uncontrollable ones as black bars.

Given a system $< N, \boldsymbol{m}_0 >$ and a MEC $(\boldsymbol{w}, k)$, because of the occurrence of an uncontrollable transition t_u enabled at a certain legal marking $\boldsymbol{m}$, a forbidden marking $\boldsymbol{m}'$ may be reached, so it is necessary avoid also the set of markings $\mathcal{M}_{fu}(\boldsymbol{w}, k) = \{\boldsymbol{m} \in \mathbb{N}^m \mid \boldsymbol{m}[\boldsymbol{\sigma} > \boldsymbol{m}',\ \boldsymbol{m}' \notin \mathcal{M}(\boldsymbol{w}, k), \boldsymbol{\sigma} \in T_u^*\}$. So in presence of uncontrollable transition the set of legal markings under control will be $\mathcal{M}_c(\boldsymbol{w}, k) = (\mathcal{M}(\boldsymbol{w}, k) \cap R(N, \boldsymbol{m}_0)) \setminus \mathcal{M}_{fu}(\boldsymbol{w}, k)$. As a result of the presence of uncontrollable transition it is $\mathcal{M}_c(\boldsymbol{w}, k) \subseteq \mathcal{M}(\boldsymbol{w}, k)$, i.e. the cardinality of the set of legal markings is decreased. A supervisory control policy is said to be *maximally permissive* if it prevents only transitions firings that yield forbidden markings.

2. ENFORCING MEC AND LIVENESS ON CONTROL SAFE MARKED GRAPHS

Let N be a net structure, and t_i an uncontrollable transition. The control subnet for t_i is $N_i = (P_i, T_i, Pre_i, Post_i)$ where $P_i \subseteq P$ is the set of places connected to t_i by a direct path containing only uncontrollable transitions (direct circuits containing only uncontrollable transitions are not allowed); $T_i = {}^\bullet P_i \cap P_i{}^\bullet$; $Pre_i = Pre \cap (P_i \times T_i)$, and $Post_i = Post \cap (P_i \times T_i)$. The set of control transitions for t_i is $A_i = \{t \in T \mid (\exists p \notin P_i) p \in {}^\bullet t \wedge (\exists p' \in P_i) p' \in t^\bullet\}$.

In the case of MGs, given a constraint $(\boldsymbol{w}, k)$ the problem is to control the firing of the single input transition of a place in Q_w in order to meet the constraint. Let $p_i \in Q_w$ and t_i be its input transition; $N_{A_i} = (P_{A_i}, T_{A_i}, Pre_{A_i}, Post_{A_i})$ the control subnet associated to t_i; $A_i = \{t^1_{A_i}, ..., t^{m_i}_{A_i}\}$ the set of control transitions for t_i (that we assume is not empty), with $\mid A_i \mid = m_i$. Thus, we may speak of control subnets and control transitions associated to a place $p_i \in Q_w$. In fig. 1 (b) is shown the control net N_{A_1} associated to the place p_1 of the net system in fig. 1 (a); in fig. 1 (c) is shown the control subnet N_{A_1} associated to the place p_2 of the same net system.

If we force a MEC on a live MG a *deadlock* may occur. It is so important to be sure that the single output transition of a place in Q_w may be always fired under a reachable marking. Let $p_i \in Q_w$ and t_{oi} be its output transition; $N_{B_i} = (P_{B_i}, T_{B_i}, Pre_{B_i}, Post_{B_i})$ the control subnet associated to t_{oi}, where $P_{B_i} \subseteq P$ is the set of places connected to t_{oi} by a direct path containing only uncontrollable transitions and a constrained place p, i.e. $p \in Q_w$; $B_i = \{t^1_{B_i}, ..., t^{n_i}_{B_i}\}$ the set of control transitions for t_{oi} (that we assume is not empty), with $\mid B_i \mid = n_i$. Let k_i be the number of constrained places in the net N_{Bi}. Note that if $p_i{}^\bullet = p_j{}^\bullet$ then $N_{Bi} = N_{Bj}$. Thus, we may speak of control subnets and control transitions associated to an output transition of a place $p_i \in Q_w$. In fig. 1 (d) is shown the control subnet N_{B_1} associated to the transition t_{o1} of the net system in fig. 1 (a), while the control subnet N_{B_2} is shown in fig. 1 (e).

In the following we consider a special class of MG systems, called *control safe* MG, that is so defined:

Definition 1 *A place p_i of a MG system is said to be control safe iff for all $t \in A_i$ there exists a direct circuit containing a single token passing through t and p_i. In a control safe MG all places are control safe.*

We assume that for a given $(\boldsymbol{w}, k)$ each place $p \in Q_w$ is control safe.

This assumption reduces the complexity of the problem of checking if a place $p \in Q_w$ may be marked firing only uncontrollable transitions, as it was shown in (Giua et al., 1993). This is due to the fact that it is not necessary to record which transition fires, but just to check the number of firings of transitions $t \in A_i$. Along this line here we use this assumption also to reduce the complexity of the problem of checking the liveness of a transition t_{oi}. The idea is to check under a given net marking $\boldsymbol{m}$ only if it is possible that the number of firings of transitions $t \in B_i$ that may be control enabled without violating the constraint is bigger than or equal to the number of firings of transitions $t \in B_i$ that have not yet occurred.

Note 1 *We make two assumptions:*
- *no place $p \in Q_w$ belongs to the control subnet of any place $p' \in Q_w$, i.e. $Q_w \cap (\cup_{p_i \in Q_w} P_i) = \emptyset$;*
- *the output transition of a place $p_i \in Q_w$ is not a control transition for a place $p_j \in Q_w$, i.e. if $p_i, p_j \in Q_w$ then $t_{oi} \notin A_j$.*

These two assumptions are purely technical (it is always possible (Giua et al., 1992) to transform the constraint $(\boldsymbol{w}, k)$ into an equivalent one such that they are satisfied) and are very similar to the notion of *independent events* (Li and Wonham, 1994) and to the *precedence path input condition (PPIC)* (Holloway and Krogh, 1992).

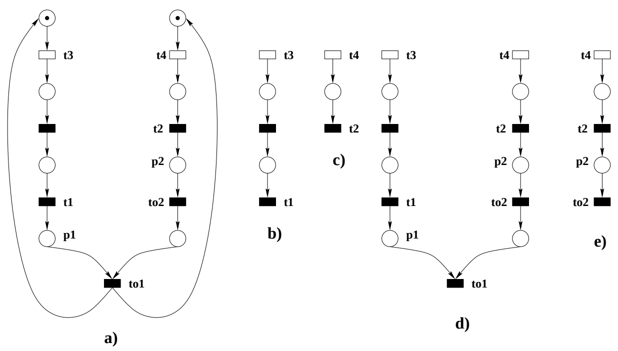

Figure 1 a) a net system; b) control subnet associated to p_1; c) control subnet associated to p_2; d) control subnet associated to t_{o1}; e) control subnet associated to t_{o2}.

2.1. ON THE LIVENESS OF MONITOR CONTROLLED MG SYSTEMS

The simplest way to force a MEC on a net system is by a monitor place. It has been shown (Giua et al., 1992) how it is possible to compute in presence of uncontrollable transitions, the *monitor* based-solution that enforces a given $(\boldsymbol{w}, k)$: a control place is added for each MEC, whose output arcs are connected only to controllable transitions. The first step of our controller design methodology consists in the liveness checking of the closed loop net controlled by a monitor. The following theorems show that if the MG with the monitor is live and a restriction on the control subnets is verified, then the state equation of the system has no spurious deadlocks. This means that given a closed-loop system that verifies the restrictions, if its state equation has a solution which is a deadlock, then the system cannot be live. Checking the absence of these solutions can be reduced to solving a ILP (Recalde et al., 1998). So, it is possible to check the liveness of the considered net system solving a ILP.

Theorem 1 *Let $(N, \boldsymbol{m}_0)$ be a MG with a monitor p associated to a MEC, and such that for every $t \in p^\bullet$, $\mathbf{Pre}(p,t) = 1$. If $(N, \boldsymbol{m}_0)$ is live, there are no spurious solutions of the state equation.*

Proof : Assume a spurious deadlock $\boldsymbol{m}_d = \boldsymbol{m}_0 + \boldsymbol{C} \cdot \boldsymbol{\sigma}_d$ exists. Let σ_0 be the largest sequence such that $\boldsymbol{m}_0[\sigma_0 >$ and $\boldsymbol{\sigma}_0 \leq \boldsymbol{\sigma}_d$, and let $\boldsymbol{m}_1 = \boldsymbol{m}_0 + \boldsymbol{C} \cdot \boldsymbol{\sigma}_0$. The system is live, hence there is at least one transition t enabled in $\boldsymbol{m}_1$. Since this transition is not enabled in $\boldsymbol{m}_d$, and MG are persistent, $\mathbf{Pre}(p,t) > 0$ and $\boldsymbol{m}_1(p) > 0$. MG do not have spurious solutions, hence from the MG point of view, there is a fireable sequence that corresponds to $\boldsymbol{\sigma}_d - \boldsymbol{\sigma}_0$. Let t' be the first transition of this sequence. Since $\boldsymbol{m}_1(p) > 0$, this transition cannot violate the precondition associated to the monitor, i.e., t' is fireable. Contradiction. ■

Theorem 2 *Let $(N, \boldsymbol{m}_0)$ be a MG with a monitor associated to a MEC and such that for every t_{oi} the control subnet N_{B_i} does not have any other output transition, i.e. $(T_{B_i} \setminus t_{oi})^\bullet \subset P_{B_i}$. If $(N, \boldsymbol{m}_0)$ is live, there are no spurious solutions of the state equation.*

Proof: Let p be the monitor of the system and $\boldsymbol{w} \cdot \boldsymbol{m} \leq k$ the MEC. Assume a spurious deadlock $\boldsymbol{m}_d = \boldsymbol{m}_0 + \boldsymbol{C} \cdot \boldsymbol{\sigma}_d$ exists. We will see that this marking can be effectively reached from $\boldsymbol{m}_0$, which contradicts liveness of system. This will be done in three steps:

1. Reach a marking in which all the k tokens are in the monitor place, p. For each control subnet N_{Bi} that is not "empty of tokens", take its output transition, t_{oi}. Fire the shortest sequence that contains all these output transitions, σ_0 (it exists since the system is live). Let $\boldsymbol{m}_1 = \boldsymbol{m}_0 + \boldsymbol{C} \cdot \boldsymbol{\sigma}_0$. From the note 1, an output transition cannot belong to any A_i, hence this sequence does not mark any other control subnet, i.e., $\boldsymbol{m}_1(p) = k$.

Observe that this firing vector can be decomposed in two parts: the transitions in $\boldsymbol{\sigma}_d$ and the rest. That is, $\boldsymbol{\sigma}_0 = \boldsymbol{\sigma}_{d0} + \boldsymbol{\sigma}_{x0}$, with $\boldsymbol{\sigma}_{d0}$ the largest vector verifying $\boldsymbol{\sigma}_{d0} \leq \boldsymbol{\sigma}_d$.

2. Let $\boldsymbol{x} \geq \boldsymbol{\sigma}_{x0}$, be a T-semiflow. It is clear that $\boldsymbol{m}_d = \boldsymbol{m}_0 + \boldsymbol{C} \cdot (\boldsymbol{\sigma}_d + \boldsymbol{x}) = \boldsymbol{m}_1 + \boldsymbol{C} \cdot (\boldsymbol{\sigma}_d + \boldsymbol{x} - \boldsymbol{\sigma}_0)$.

Divide $\boldsymbol{\sigma}_d + \boldsymbol{x} - \boldsymbol{\sigma}_0$ in two parts: (1) a group $\boldsymbol{\sigma}_1$ composed of transitions not belonging to any control subnet and subsets containing all the transitions of control subnets N_{Bi}, and (2) other group $\boldsymbol{\sigma}_2$ with "incomplete" control subnets.

We will see that $\boldsymbol{\sigma}_1$ corresponds to a fireable sequence. Let $\boldsymbol{m}_2 = \boldsymbol{m}_1 + \boldsymbol{C} \cdot \boldsymbol{\sigma}_1$. First, we will see that $\boldsymbol{m}_2 \geq \mathbf{0}$. For the monitor p and the places in control subnets, p', $\boldsymbol{\sigma}_1$ corresponds to a T-semiflow, hence, $\boldsymbol{m}_2(p) = \boldsymbol{m}_1(p) \geq 0$ and $\boldsymbol{m}_2(p') = \boldsymbol{m}_1(p') \geq 0$. For the places not belonging to any control subnet, p'', $\boldsymbol{m}_2(p'') = \boldsymbol{m}_d(p'') - \boldsymbol{C}(p'', T) \cdot \boldsymbol{\sigma}_2$, and since $\boldsymbol{\sigma}_2$ does not contain any output transition t_{oi}, $\boldsymbol{m}_2(p'') = \boldsymbol{m}_d(p'') + \mathbf{Pre}(p'', T) \cdot \boldsymbol{\sigma}_2 \geq 0$. Therefore, since MG do not have spurious solutions of the state equation, $\boldsymbol{\sigma}_1$ corresponds to a fireable sequence in the MG.

Order the transitions of $\boldsymbol{\sigma}_1$ in such a way that: (1) the sequence is fireable in the MG and (2) all the transitions in a certain N_{Bi} are put together, i.e., no input transition of other subnet N_{Bj} is fired till the output transition t_{oi} has been fired. It is clear that this corresponds to a fireable sequence.

3. Finally, we must prove that $\boldsymbol{\sigma}_2$ is fireable. Since $\boldsymbol{m}_d = \boldsymbol{m}_2 + \boldsymbol{C} \cdot \boldsymbol{\sigma}_2 \geq \mathbf{0}$, the only problem may be due to the monitor. In $\boldsymbol{\sigma}_2$ there is no output transition of the control subnets, therefore $\boldsymbol{m}_2(p) = \boldsymbol{m}_d(p) - \boldsymbol{C}(p, T) \cdot \boldsymbol{\sigma}_2 = \boldsymbol{m}_d(p) + \mathbf{Pre}(p, T) \cdot \boldsymbol{\sigma}_2 \geq \mathbf{Pre}(p, T) \cdot \boldsymbol{\sigma}_2$. ■

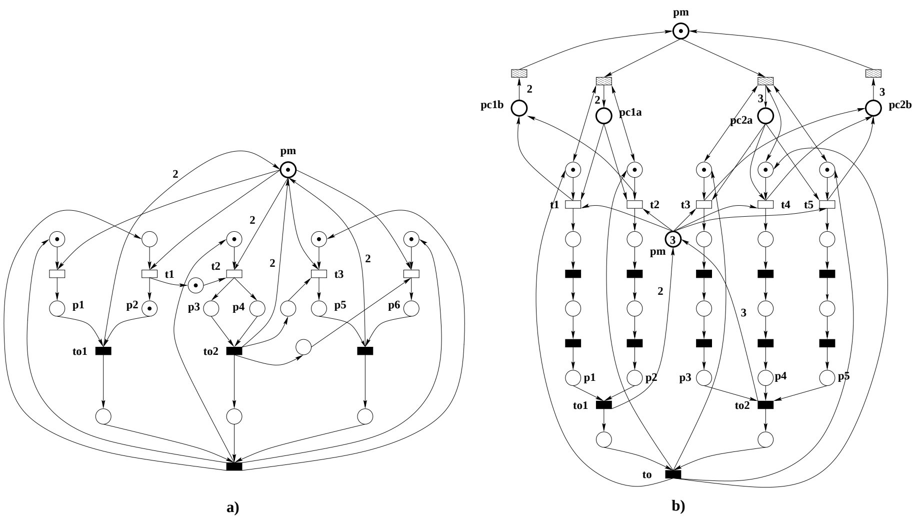

Figure 2 (a) For this live net system the state equation gives a spurious deadlock solution: monitor place p_m has output arcs with weight greater than 1 and N_{B_1} has more than one output transitions (t_1, t_{o1}). (b) A suboptimal controller to force a MEC and closed-loop liveness on the net system in fig. 3 (a).

In fig. 2 (a) an example of a net controlled by a monitor and not meeting the hypothesis of theorems above is presented. Although the closed-loop system is live, its state equation gives a spurious deadlock solution. The monitor place p_m enforces the MEC $\boldsymbol{m}(p_1) + \boldsymbol{m}(p_2) + \boldsymbol{m}(p_3) + \boldsymbol{m}(p_4) + \boldsymbol{m}(p_5) + \boldsymbol{m}(p_6) \leq 2$; a spurious solution is obtained firing $t_2\, t_{o2}\, t_3$. It can be seen that spurious solutions may also be found if more than one monitor is added.

2.2. THE CONTROLLER SYNTHESIS

For sake of simplicity in the following we assume that $\mid A_i \mid = 1$, i.e. for each place $p \in Q_w$ there is only one controllable transition that has to be control enabled to mark p. This assumption is not essential to the technique that we are going to introduce to force liveness in presence of a constraint $(\boldsymbol{w}, k)$.

In the following, we restrict to the case in which the control subnets of different output transitions, $t_{oj} \neq t_{oj}$, do not have a common part, that is, $B_i \cap B_j = \emptyset$. This restriction simplifies the problem: the places of the GMEC support that belong to the same control subnet, can be studied on an equal footing without problem of priorities among them. In other words, we are addressing the case of systems *MGs with separate control subnets*.

Let us assume that the indexes of the sets B_i are ordered according to the number of controllable transitions, i.e. if $i < j$ then $n_i \leq n_j$. We denote as *constrained* a transition $t \in B_j$ under a given marking $\boldsymbol{m}$, if the path from t to t_{oj} along the single token circuit is not marked, otherwise we denote it as *unconstrained*. We introduce a set of *counters* variables denoted as $C_i(\boldsymbol{m})$ whose value is equal to k minus the number of unconstrained transitions under the marking $\boldsymbol{m}$ belonging to B_j, with $j \neq i$. So we have that: a) the firing of a transition $t \in B_j, j \neq i$ will decrement the value of C_i in one unit; b) the firing of the output transitions $t_{oj}, j \neq i$ will increment the value of C_i in n_j units; c) the firing of a transition $t \in B_i$ does not change the value of C_i; d) the initial value of C_i is equal to k decremented by the summation of unconstrained transitions in the sets $B_j, j \neq i$ under the initial marking.

Note that every time a tradition t_{oi} fires, n_i unconstrained transitions of the set B_i become constrained, and a number of n_i transitions can be control enabled in the sets $B_j, j \neq i$, without violating the constraint. Also, note that every time a transition t_{ol} fires, it is always possible to fire a transition t_{ok}, with $k < l$, without violating the constraint. At a given marking $\boldsymbol{m}$ a transition $t \in B_i$ such that $\boldsymbol{m}[t > \boldsymbol{m}'$ may be left free to fire iff a sequence can be fired afterwards that enables t_{oi}, or equivalently, iff one of the following conditions is true.

- $C_i \geq n_i$, *i.e. every constrained transition* $t \in B_i$ *may left free to fire and then it is possible to enable* t_{oi}.
- $C_l \geq n_l + 1$, *with* $l > i$, *i.e. it is possible to fire* t_{ol} *and so* t_{oi} *because* $n_l \geq n_i$.

• $\left[\bigwedge_{l=1}^{|s|}[C_{s_l} + \sum_{j=1}^{s_{l-1}} \sharp B_{s_j} \geq n_l + 1] \wedge \right.$
$\left.\left[[C_i + \sum_{j=1}^{s_l} \sharp B_{s_j} \geq n_i] \vee_{q>i} [C_q + \sum_{j=1}^{s_l} \sharp B_{s_j} \geq n_q + 1]\right]\right]$, *for a* $s \in S_i$, *where* S_i *is the set of all the subsequences of the sequence* $1...i$ *and* s_l *is the* l*-th element of the subsequence* s *and* s_0 *is the empty subsequence;* $\sharp B_{s_j}$ *denote the number of transition that have been fired in the set* B_{s_j}*. This condition checks if firing a sequence* $t_{or}..t_{os}$ *with* $r \leq s < i$ *it is possible to fire* t_{oq}*, with* $q \geq i$*.*

A possible supervisor to force a $(\boldsymbol{w}, k)$ and liveness on a MG, is so given by a set logical predicates, each of them associated to the control input of a controllable transition, in CtlPN framework. In addition to this, here we show that it is possible to implement the three conditions above by means of control places and replicating controllable transitions. It is so possible for a given transition to translate the enabling condition of the control input into an equivalent one given in terms of the net structure. Note that an uncontrollable transition cannot have an input arc from any added control place, while we suppose that all uncontrollable transitions are observable and so an output arc to a control place can be added. In the following we will show how to implement the firing condition $C_i \geq n_i$, other cases may be derived similarly:

• *add a place, named* p_{c_i}*, with initial marking equal to* $k - \sum_{p \in N_{B_j}, j \neq i} \boldsymbol{m}_0(p)$*, where* N_{B_j} *is the control subnet of* t_{oj}*, and let* $Pre_c(p_{c_i}, t) = 1$ *if* $t \in B_j$ *with* $j \neq i$*,* $Post_c(p_{c_i}, t_{oj}) = n_j$ *with* $j \neq i$*,* $Pre_c(p_{c_i}, t) = Post_c(p_{c_i}, t) = n_i$ *if* $t \in B_i$*;*

• *let consider the net structure* $N_c = (P_c, T, Pre_c, Post_c)$ *with* $P_c = P \cup p_{ci}$ *and initial marking* m_{c0}*; it is immediate to see that the enabling condition of a transition* $t \in B_i$ *with respect to* p_{ci}*, i.e.* $\boldsymbol{m}_c(p_{ci}) \geq Pre_c(p_{ci}, t)$ *in the net system* $(N_c, \boldsymbol{m}_{c0})$ *is equivalent to check if* $C_i \geq n_i$ *in the original net system.*

Observe that expressing the second condition shown above requires a replication of the transition $t \in C_i$, and as for third condition, a number of replications equal to the $\vee$ operator occurrences are needed. Consider the net in fig. 3 (a), where the monitor place p_m enforcing the MEC $\boldsymbol{m}(p_1) + \boldsymbol{m}(p_2) + \boldsymbol{m}(p_3) + \boldsymbol{m}(p_4) + \boldsymbol{m}(p_5) \leq 3$ is shown. The net system is not live. As for the control subnets of place $p \in Q_w$ we have that $A_1 = \{t_1\}$, $A_2 = \{t_2\}$, $A_3 = \{t_3\}$, $A_4 = \{t_4\}$, $A_5 = \{t_5\}$ while as for the control subnets of their output transitions we obtain $B_a = B_1 = B_2 = \{t_1, t_2\}$, $B_b = B_3 = B_4 = B_5 = \{t_3, t_4, t_5\}$. As said above, in order to enforce MEC and closed loop liveness two control places p_{ca}, and p_{cb} are introduced. Note that the weights of self-loop arcs outgoing from p_{ca} and p_{cb} depend on the cardinality of the set B_a and B_b respectively. Here we point out the firing conditions of a transition $t \in B_b$: $C_2 \geq 3$, i.e. every constrained transition $t \in B_b$ may left free to fire and then it is possible to enable t_{o2}; $[C_1 \geq n_1+1] \wedge [C_1 + \sharp B_b \geq n_2]$, i.e. it is possible to fire t_{o1} and then t_{o2}, and noticing that it is always true that $[C_1 + \sharp B_b \geq 3]$, we have that the condition is reduced to $[C_1 \geq 3]$. Since we have to check two conditions, a replication is needed for each transition $t \in B_b$. The resulting controller is shown in fig. 3 (b), while in fig. 3 (c) only the controller structure is shown, where B_b' denotes a replication of the set B_b.

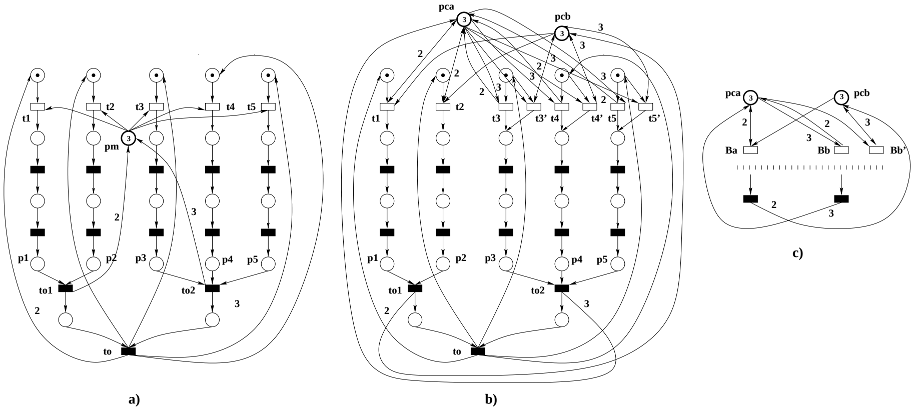

Figure 3 Replications of transitions are necessary to force a MEC and closed-loop liveness on the net system in a).

Obtaining a maximally permissive controller is not a simple task, and in general the controller may be very complex, so suboptimal approach may be acceptable in some cases. In fig. 2 (b) for the same problem presented in fig. 3 (a), a simpler controller structure is shown. Here the idea is to leave free to fire all the transitions that belong to a set of controllable transitions B_i, and a number of transitions belonging only to one other set B_j until the transition t_{oi} fires.

3. CONCLUDING REMARKS

Several results on the liveness of plant MG, where a MEC has been forced via a monitor place, have been presented in this paper. First, two sufficient conditions have been obtained which guarantee that no solution of the state equation is a spurious deadlock. As a consequence, checking liveness in these cases can be reduced to solving a ILP (Recalde et al., 1998). Also, a PN controller to make live a controlled control safe MG meeting the MEC specification has been proposed under certain restrictions (MGs with separate control subnets).

Two main directions can be considered for future research.

1. *Generalization of the controller* to larger net subclasses. Removing the constraint that systems have separate control subnets is being addressed at the moment, and seems promising. The following example illustrates which kind of problems appear, and how they can in this case

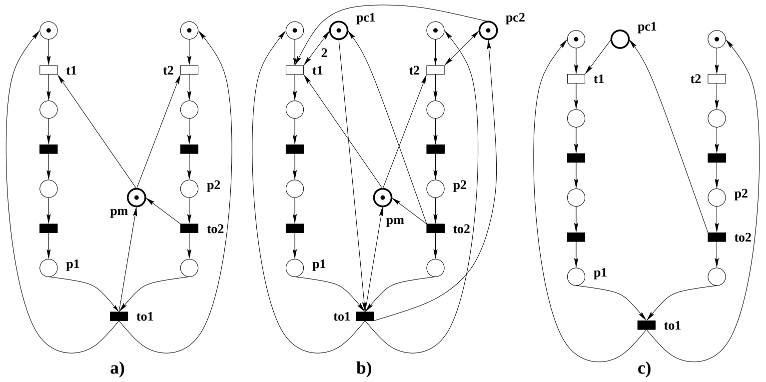

Figure 4 a) the MEC $\boldsymbol{m}(p_1) + \boldsymbol{m}(p_2) \leq 1$ is forced on the net system; b) a MEC and closed-loop liveness is forced on the net system; c) a simplification of controller shown in b).

be solved. It may occur that $B_i \cap B_j \neq \emptyset$, as in fig. 4, where the MEC $\boldsymbol{m}(p_1) + \boldsymbol{m}(p_2) \leq 1$ is the control specification and $B_2 \subset B_1$. Enforcing the MEC on this net system by a monitor as in in fig. 4 (a), a deadlock may occur if t_1 fires before t_2. In order to extend the method presented above, we can note that nothing has to be changed as for the firing conditions of t_2. On the other hand, to control the firing of t_1 an output arc from t_{o2} to p_{c1}, and another from p_{c1} to t_{o1} must be added, as shown in fig. 4 (b). The added arc from t_{o2} to p_{c1} is needed to increment after the firing of t_{o2} the number of unconstrained controllable transitions represented by the marking of the place p_{c1}, because the direct circuit from p_2 to t_{o1} does not contain any place $p \in Q_w$. The controller can be simplified as in fig. 4 (c). More ambitious generalizations, like removing the control safe restriction, or even allowing more general plants than MG, look difficult since some the basic ideas used to obtain the controllers are no longer applicable.

2. *Modularity of the controller.* Given two MECs $(\boldsymbol{w}_1, k_1)$, $(\boldsymbol{w}_2, k_2)$ and their respective supervisory control policies, the maximally permissive control policy to enforce the two MECs on the plant is to prevent transition firings that yield markings not belonging to the set $\mathcal{M}_c(\boldsymbol{w}_1, k_1) \cup \mathcal{M}_c(\boldsymbol{w}_2, k_2)$. But, even if each one of the two control policies ensures separately closed-loop liveness, this is not the case when they are both forced on the plant. Consider the net in fig. 5 (a), where the monitor place p_{m1} enforcing the MEC $\boldsymbol{m}(p_1) + \boldsymbol{m}(p_4) \leq 1$ and the monitor place p_{m2} enforcing the MEC $\boldsymbol{m}(p_2) + \boldsymbol{m}(p_3) \leq 1$ are shown. The net system is not live, but if we consider a single monitor in isolation we obtain a live net system. This is due to the fact that the non-conflicting condition between two marked languages forced by each monitor on the plant is not fulfilled (Wonham, 1989). The same occurs if the controllers are derived according to the synthesis method exposed

in the previous subsection. In fig. 5 (b) the places (p_{c1a},p_{c1b}) enforce $\boldsymbol{m}(p_1) + \boldsymbol{m}(p_4) \leq 1$ and (p_{c2a},p_{c2b}) enforce $\boldsymbol{m}(p_2) + \boldsymbol{m}(p_3) \leq 1$ on the net in fig. 5 (a) and if they are considered separately, they ensure liveness. But the resulting net system if both are put at the same time is not live. In this particular case a way to make live the net system is to add additional self-loops, represented by dotted lines in the figure, from the control places p_{c1i} to the set B_1 and vice versa. Further work should be done to improve the controllers from the modularity point of view.

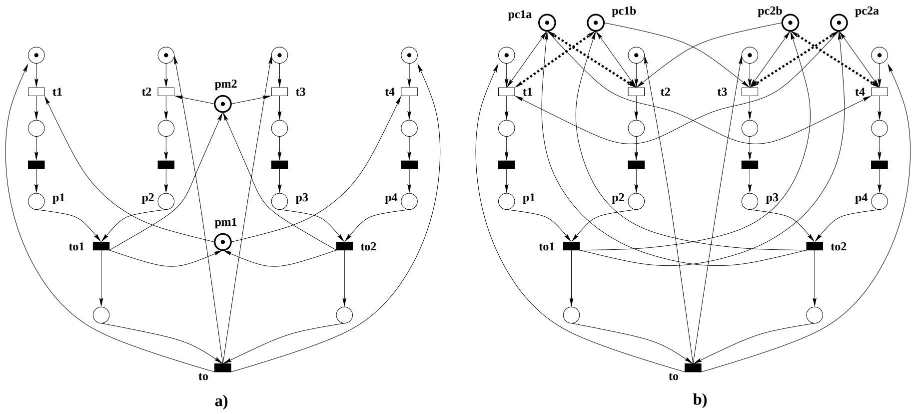

Figure 5 a) the controller synthesis is not modular; b) additional self-loops, represented by dotted lines in the figure, has to be added to meet the specifications.

References

Giua, A., Cesare, F. D., and Silva, M. (1993). Petri net supervisors for generalized mutual exclusion constraints. *Proc. 1993 IFAC World Congress (Sydney, Australia)*, pages 267–270.

Giua, A., DiCesare, F., and Silva, M. (1992). Generalized mutual exclusion constraints on nets with uncontrollable transitions. *1992 IEEE Int. Conf. on Systems, Man, and Cybernetics (Chigago, Illinois)*, pages 974–979.

Holloway, L. and Krogh, B. (1992). On closed-loop liveness of discrete-event systems under maximally permissive control. *IEEE Trans. on Automatic Control*, 37(5):622–697.

L.E. Holloway, B.H. Krogh, and Giua, A. (1997). A survey of petri nets methods for controlled discrete event systems. *Discrete Event Dynamic Systems: Theory and Applications*, 7(7):151–190.

Li, Y. and Wonham, W. (1994). Control of vector discrete-event systems II - controller synthesis. *IEEE Trans. on Automatic Control*, 39(3):512–531.

Recalde, L., Teruel, E., and Silva, M. (1998). On linear algebraic tecniques for liveness analysis of p/t systems. *J. of Circuits, Systems, and Computers*, 1(8):223–265.

Wonham, W. (1989). The control of vector discrete-event systems. *Proc. of IEEE*, 77(1):81–98.

Yalimalidou, K., Moody, J., Lemmon, M., and Antsaklis, P. (1996). Feedback control of petri nets based on place invariants. *Automatica*, 32(1):15–28.