# Deadlock Characterization for Petri Nets Controlled Using GMEC's and Observers

Alessandro Giua, Carla Seatzu
Dip. di Ing. Elettrica ed Elettronica, Università di Cagliari, Italy
Phone: +39-070-675-5751 – Fax: +39-070-675-5782 – Email: {giua,seatzu}@diee.unica.it

**Abstract**

In this paper we deal with the problem of controlling a Petri net whose marking cannot be measured but is estimated using an observer. The control objective is that of enforcing a set of generalized mutual exclusion constraints (GMEC) and all transitions are assumed to be controllable. Clearly, the use of marking estimates may significantly reduce the performance of the closed-loop system and may lead to a deadlock. If the net times out, i.e., if no transition firing occurs within a reasonable amount of time in the controlled system, an efficient procedure may be invoked to recover the net from a controller induced deadlock. The novel contribution of this paper is that of exploring in detail the characterization of those cases in which the proposed recovery procedure works.

## 1 Introduction

In this paper we deal with the problem of controlling a Petri net whose marking cannot be measured. The state-feedback control of discrete event systems with incomplete information has already been discussed in the literature [7, 8, 13, 15]. In particular, we assume that the net structure is completely known while the initial marking is only known to belong to a "macromarking", i.e., we know the token contents of subsets of places but not the exact token distribution.

In previous works [7, 8] we have shown how it is possible to estimate the actual marking of the net based on the observation of a word of events (i.e., transition firings) and an algorithm was given for computing the marking estimate and error bound. The estimate is always a lower bound of the actual marking. The system that computes the estimate is called an observer. The special structure of Petri nets allows us to use a simple linear algebraic formalism for estimate and error computation. In particular, the set $\mathcal{C}$ of *markings consistent with an observed word*, i.e., the set of markings in which the system may actually be given the observed word, can easily be described in terms of the observer estimate and can be characterized as the integer solutions of a linear constraint set. Other approaches to the design of Petri net observers can also be found in [12].

In [7, 8] we have also shown how the estimate generated by the observer may be used to design a state feedback controller, that ensures that the controlled system never enters a set of forbidden states. We considered a special class of safeness specifications that limit the weighted sum of markings in subsets of places called generalized mutual exclusion constraints (GMEC).

Clearly, the use of marking estimates, as opposed to the exact knowledge of the actual marking of the plant, leads to a worse performance of the closed-loop system. In fact, in a safeness problem the aim of the controller is that of preventing all those transition firings that lead to a forbidden marking. If the actual marking is not known, but is known to belong to a given set $\mathcal{C}$, the controller must forbid all transitions firing that from "any" marking in $\mathcal{C}$ may lead to a forbidden marking, i.e., the controller may disable transitions whose firing is perfectly legal. Because of this it may be the case that the controlled system is blocking.

In [2] we have shown that using siphon analysis, the set of deadlock markings $\mathcal{M}_b$ of a structurally bounded net can be characterized as the integer solutions of a linear constraint set.

The characterization based on siphon analysis has been used in [2] to derive an efficient deadlock recovery procedure that is proposed here in a slightly different form. More precisely, we assume that if no transition firing occurs within a reasonable amount of time in a controlled system — we say that the *net has timed out* — one can conclude that a deadlock has occurred and a recovery procedure should be invoked. We have also shown how the linear algebraic characterization of deadlock markings may be used to improve the marking estimate, thus providing a better characterization of the set of consistent markings.

In this paper we explore in detail the characterization of those cases in which the proposed procedure works. More precisely, these are the novel contributions.

— The algorithm used to compute the maximally permissible control pattern — given a set of consistent states produced by the observer — is formally presented in section 4 where we also show that it enjoys an important monotonicity property.

— The properties of the deadlock recovery algorithm are studied in subsection 5.3.

— In section 6 sufficient conditions are given to ensure that the controlled net will never time out or to ensure that, in the case that a time-out occurs, the proposed procedure will always recover the net from deadlock.

Finally, the presented results are applied to a manufacturing example.

## 2 Background on Petri nets

In this section we recall the formalism used in the paper. For more details on Petri nets we address to [10].

A *Place/Transition net* (P/T net) is a structure $N = (P, T, Pre, Post)$, where $P$ is a set of $m$ places; $T$ is a set of $n$ transitions; $Pre : P \times T \to \mathbb{N}$ and $Post : P \times T \to \mathbb{N}$ are the *pre*– and *post*– incidence functions that specify the arcs; $C = Post - Pre$ is the incidence matrix.

A *marking* is a vector $M : P \to \mathbb{N}$ that assigns to each place of a $P/T$ net a non–negative integer number of tokens, represented by black dots. In the following we denote $M(p)$ the marking of place $p$.

A transition $t$ is enabled at $M$ if $M \geq Pre(\cdot, t)$ and may fire yielding the marking $M' = M + C(\cdot, t)$. We write $M\ [w\rangle\ M'$ to denote that the enabled sequence of transitions $w$ may fire at $M$ yielding $M'$. Finally, we denote $w_0$ the sequence of null length.

A marking $M$ is *reachable* in $N$ from $M_0$ iff there exists a firing sequence $w$ such that $M_0\ [w\rangle\ M$. The set of all

markings reachable from $M_0$ defines the *reachability set* of $\langle N, M_0\rangle$ and is denoted $R(N, M_0)$.

A nonnegative integer vector $\vec{x} \neq \vec{0}_m$ such that $\vec{x}^{\,T} \cdot C = \vec{0}_n{}^T$ is called a *P–invariant* (here $\vec{0}_k$ denotes a $k \times 1$ vector of zeros).

A transition $t$ is said to be *live* if for any $M \in R(N, M_0)$, there exists a sequence of transitions firable from $M$ which contains $t$. A Petri net is said to be live if all transitions are *live*. A Petri net is said to be *deadlock–free* if at least one transition is enabled at every reachable marking.

A place $p$ is said to be *bounded* if there exists a constant $k$ such that $M(p) \leq k$ for all $M \in R(N, M_0)$. A net system is bounded if all places are bounded. A net is *structurally bounded* if it is bounded for all initial markings.

**Definition 1.** Given a net $N = (P, T, Pre, Post)$, and a subset $T' \subseteq T$ of its transitions, we define the $T'-$*induced subnet of* $N$ as the new net $N' = (P, T', Pre', Post')$ where $Pre', Post'$ are the restriction of $Pre, Post$ to $T'$. The net $N'$ can be thought as obtained from $N$ removing all transitions in $T \setminus T'$. We also write $N' \prec_{T'} N$. ■

Now, let us recall a linear algebraic characterization of deadlock markings [2] that is valid for ordinary and structurally bounded Petri nets. Note that similar linear characterizations have been independently proposed in [1, 3, 5, 11].

**Theorem 2 ([2]).** Given a structurally bounded net $N$ with $m$ places, a marking $M \in \mathbb{N}^m$ is a deadlock marking if and only if there exists a vector $\vec{s} \in \{0,1\}^m$ such that the following set of linear equations is satisfied:

$$\mathcal{D}(N) := \begin{cases} K_1 \cdot Pre^T \cdot \vec{s} \geq Post^T \cdot \vec{s} & (a) \\ K_2 \cdot \vec{s} + M \leq K_2 \cdot \vec{1}_m & (b) \\ \vec{s} + M \geq \vec{1}_m & (c) \\ Pre^T \cdot \vec{s} \geq \vec{1} & (d) \\ M \in \mathbb{N}^m & (e) \\ \vec{s} \in \{0,1\}^m & (f) \end{cases} \quad (1)$$

where $K_1 = \max_{t \in T} Post^T(\cdot, t) \cdot \vec{1}$ and $K_2$ is any positive integer greater or equal to the maximum structural bound of $p$, for any $p \in P$. ■

By virtue of the linear characterization above, we define the set of blocking markings of a net $N$ as:

$$\mathcal{M}_b(N) = \{M \mid \exists \vec{s} \in \{0,1\}^m : (M, \vec{s}) \in \mathcal{D}(N)\}. \quad (2)$$

Finally, we present a useful technical result.

**Proposition 3.** Given a net $N = (P, T, Pre, Post)$, and a subset of transitions $T' \subseteq T$, let $N' \prec_{T'} N$ be the $T'-$induced subnet of $N$. Then $\mathcal{D}(N) \subseteq \mathcal{D}(N')$, or equivalently $\mathcal{M}_b(N) \subseteq \mathcal{M}_b(N')$.

**Proof:** Let us define $n' = |T'|$ and $n = |T| > n'$. Then it is easy to see that constraints 1.a and 1.d in $\mathcal{D}(N)$ are each composed by $n$ inequalities, i.e., the corresponding $n'$ inequalities in $\mathcal{D}(N')$ plus additional ones. This proves the statement. □

## 3 Marking estimation with macromarkings

In this paper we assume that the initial marking is available in the form of a *macromarking*.

**Definition 4 ([8]).** The *macromarking defined by* $V \in \mathbb{N}^{m \times r}$ *and* $\vec{b} \in \mathbb{N}^r$ is the set of markings $\mathcal{V}(V, \vec{b}) = \{M \in \mathbb{N}^m \mid V^T M = \vec{b}\}$. ■

We make the following assumptions. A1) The structure of the net $N = (P, T, Pre, Post)$ is known, while the initial marking $M_0$ is not. A2) The event occurrences (i.e., the transition firings) can be observed. A3) The initial marking $M_0$ belongs to the macromarking $\mathcal{V}(V, \vec{b})$, i.e., it satisfies the equation $V^T M_0 = \vec{b}$.

We also introduce the following notation.

**Definition 5 ([7]).** After the word $w$ has been observed we define the set of $w-$consistent markings as $\mathcal{C}(w) = \{M \in \mathbb{N}^m \mid \exists M_0 \in \mathcal{V}(V, \vec{b}),\ M_0[w\rangle M\}$, i.e., as the set of all markings in which the system may be given the observed behavior and the initial marking. ■

Given an evolution of the net $M_0[t_{\alpha_1}\rangle M_1[t_{\alpha_2}\rangle \cdots$, we use the following algorithm to compute estimate $\mu_w$ and bound $B_w$ of each actual marking $M_w$ based on the observation of the word of events $w = t_{\alpha_1} t_{\alpha_2} \cdots t_{\alpha_k}$, and of the knowledge of the initial macromarking $\mathcal{V}(V, \vec{b})$.

**Algorithm 6. ( Marking Estimation with Event Observation and Initial Macromarking [7])**

Assume that the initial macromarking is $\mathcal{V}(V, \vec{b})$.

1. Let the initial estimate be $\mu_{w_0} = \vec{0}_m$.
2. Let the initial bound be $B_{w_0} = \vec{b}$.
3. Let the current observed word be $w = w_0$.
4. Wait until $t$ fires.
5. Update the estimate $\mu_w$ to $\mu'_{wt}$ with $\mu'_{wt}(p) = \max\{\mu_w(p), Pre(p, t)\}$.
6. Let $\mu_{wt} = \mu'_{wt} + C(\cdot, t)$.
7. Let $B_{wt} = B_w - V^T \cdot (\mu'_{wt} - \mu_w)$.
8. Goto 4. ■

The set of consistent markings can be characterized in terms of the estimate and bound as follows.

**Theorem 7 ([7]).** Given a net with initial macromarking $\mathcal{V}(V, \vec{b})$, an observed word $w \in L(N, M_0)$, and the corresponding estimated marking $\mu_w$ and bound $B_w$ computed by Algorithm 6, the set of $w-$*consistent markings* coincides with the set of $(\mu_w, B_w)-$*consistent markings*, i.e., $\mathcal{C}(w) = \mathcal{M}(\mu_w, B_w) \stackrel{\text{def}}{=} \{M \in \mathbb{N}^n \mid M \geq \mu_w,\ V^T \cdot M = V^T \cdot \mu_w + B_w\}$. ■

## 4 Control using observers

In this section we show how the marking estimate can be used by a control agent to enforce a given specification on the plant behavior [8]. We make several assumptions that are briefly discussed here.

— We assume that the specification on the desired behavior is given as a set of legal markings $\mathcal{L}$.

— We consider a special type of state specifications called *generalized mutual exclusion constraints* (GMEC) that have been considered by various authors [6, 9, 14]. Given an integer matrix $L = [\vec{l}_1 \cdots \vec{l}_q]$ with $\vec{l}_j \in \mathbb{Z}^m$ and a vector $\vec{k} = [k_1, \cdots, k_q]$ with $k_j \in \mathbb{Z}$, a GMEC $(L, \vec{k})$ defines the set of legal states $\mathcal{L} = \{M \in \mathbb{N}^m \mid L^T \cdot M \leq \vec{k}\}$.

— The controller may disable transitions to prevent the plant from entering a forbidden marking, computing a control pattern $f(t, M) : T \times \mathbb{N}^m \to \{0, 1\}$. If $f(t, M) = 0$ then $t$ is disabled by the controller at $M$.

— All transitions are controllable, i.e., can be disabled by the controller.

When an observer is used in the control loop the actual marking $M$ is not known and only the set of consistent

markings $\mathcal{C} \subseteq \mathbb{N}^m$ is available to the controller. The control law thus becomes a function $f(t, \mathcal{C}) : T \times 2^{\mathbb{N}^m} \rightarrow \{0, 1\}$ and can be given as follows.

**Definition 8. (State feedback for GMEC with observer)**

Given a GMEC $(L, \vec{k})$ and a set of consistent markings $\mathcal{C} \subseteq \mathbb{N}^m$, the firing of transition $t$ should be prevented if and only if there exists a legal consistent marking $M$ such that the firing of $t$ from $M$ leads to a forbidden marking, i.e.,

$$f(t, \mathcal{C}) = \begin{cases} 0 & \text{if } (\exists M)\ M \in \mathcal{C},\ L^T \cdot M \leq \vec{k}, \\ & \quad M[t\rangle M',\ (\exists j)\ \vec{l}_j \cdot M' > k_j \\ 1 & \text{otherwise.} \end{cases}$$

■

The computation of the control pattern may be carried out solving a number of linear integer programming problems (IPP) as given in the following algorithm.

**Algorithm 9. (Computation of the optimal state feedback with observer)**

The control law in definition 8 can be computed as follows.

1. For all transitions $t$, let $J_t = \{j \mid \vec{l}_j^T \cdot C(\cdot, t) > 0\}$ be the set of indices of those constraints that may potentially be violated by the firing of $t$.
2. Solve for each $j \in J_t$ the IPP

$$\begin{cases} \max\ \vec{l}_j^T \cdot M' \\ \text{s.t.} \\ M \in \mathcal{C} & (a) \\ L^T \cdot M \leq \vec{k} & (b) \\ M \geq Pre(\cdot, t) & (c) \\ M' = M + C(\cdot, t) & (d) \end{cases} \tag{3}$$

   and let $h_j(t)$ be its optimal solution.
3. Define

$$f(t, \mathcal{C}) = \begin{cases} 0 & \text{if } (\exists j \in J_t) h_j(t) > k_j \\ 1 & \text{otherwise.} \end{cases} \tag{4}$$

   the desired control pattern. ■

Thus a transition $t$ is disabled only if it may fire (constraint (c)) and there exists a consistent marking $M$ (constraint(a)) that is legal (constraint (b)) and from which the firing of $t$ leads to a marking $M'$ (constraint (d)) that is not legal because for at least one $j$ it holds $h_j(t) = \vec{l}_j^T \cdot M' > k_j$. Note that under the assumption that the actual marking is legal, we need not solve IPP (3) for all those constraints such $\vec{l}_j^T \cdot C(\cdot, t) \leq 0$, because they may never be violated by the firing of $t$.

**Remark 10.** If $\mathcal{C} = \mathcal{M}(\mu, B)$, i.e., the set of consistent markings can be described using the marking estimate $\mu$ and bound $B$ as suggested by theorem 7, we simply substitute constraint $(a)$ in (3) with

$$\begin{cases} V^T \cdot M = V^T \cdot \mu + B \\ M \geq \mu \\ M \in \mathbb{N}^m \end{cases}$$

■

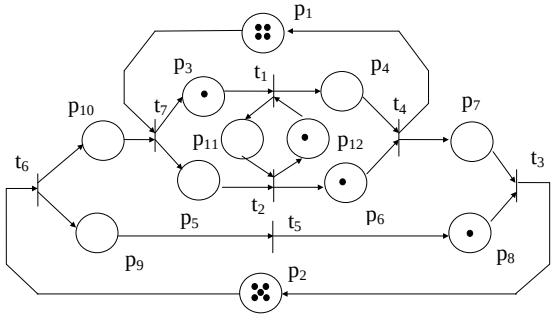


**Figure 1:** Event graph model of the assembly system.

Finally, we state a useful elementary proposition.

**Proposition 11.** Let $\mathcal{C}'$ and $\mathcal{C}''$ be two sets of consistent markings, with $\mathcal{C}' \subseteq \mathcal{C}''$. Then $f' = f(\cdot, \mathcal{C}')$ *is at least as permissive as* $f'' = f(\cdot, \mathcal{C}'')$ i.e., for all $t$ it holds $f(t, \mathcal{C}') \geq f(t, \mathcal{C}'')$. We denote this writing $f' \geq f''$.

**Proof:** For all $t$ and for all $j$, $\mathcal{C}' \subseteq \mathcal{C}''$ implies $h'_j(t) \leq h''_j(t)$, where $h'_j(t)$ and $h''_j(t)$ denote the solutions of (3) with, resp., $\mathcal{C} = \mathcal{C}'$ and $\mathcal{C} = \mathcal{C}''$. Thus the result follows from the definition of $f$ given in (4). □

A trivial consequence of this proposition is the following. When the actual marking $M$ is perfectly known the set of consistent markings is $\mathcal{C}' = \{M\}$. On the contrary, if the actual marking can only be estimated by an observer, then the set of consistent markings is $\mathcal{C}'' \supseteq \mathcal{C}'$. This means that the control pattern computed using an observer may be more restrictive than the optimal state feedback computed when the actual marking is known. As shown in the following example this may often lead to a block.

### 4.1 A manufacturing example

We apply the above methodology to a manufacturing system whose Petri net model is shown in fig. 1.

This assembly system, that is similar to the one described in [4], consists of five machines, $\mathcal{M}_1$, $\mathcal{M}_2$, $\mathcal{M}_3$, $\mathcal{M}_4$ and $\mathcal{M}_5$ whose operational process is modeled by the firing of transitions $t_1$, $t_2$, $t_3$, $t_4$ and $t_5$, respectively. The markings of places $p_1$ and $p_2$ represent the number of assembly servers for $t_4$ and $t_3$ respectively. The marking of places $p_3$, $p_5$, and $p_9$ represent the availability of parts to be processed (raw materials), while the marking of places $p_4$, $p_6$, $p_7$ and $p_8$ represent the availability of semi–finished products. Places $p_{11}$ and $p_{12}$ ensure that machines $t_1$ and $t_2$ work alternatively.

The Petri net model in fig. 1 is a strongly connected event graph with $m = |P| = 12$ and $n = |T| = 7$. There exist eleven elementary circuits, that correspond to an equal number of P-invariants. If we assume that the initial marking of the net is that in fig. 1, we have (here to avoid a heavy notation we denote as $M_i$ the marking of place $p_i$): $M_{11}+M_{12} = 1$, $M_1+M_3+M_4 = 5$, $M_1+M_5+M_6 = 5$, $M_1+M_3+M_6+M_{11} = 6$, $M_1+M_4+M_5+M_{12} = 5$, $M_2 + M_8 + M_9 = 6$, $M_2 + M_3 + M_4 + M_7 + M_{10} = 6$, $M_2 + M_5 + M_6 + M_7 + M_{10} = 6$, $M_2 + M_3 + M_6 + M_7 + M_{10} + M_{11} = 7$, $M_2 + M_4 + M_5 + M_7 + M_{10} + M_{12} = 6$. We assume that the above set of P-invariants coincides with the macromarking, thus $B_{w_0} = \vec{b} = [1\ 5\ 5\ 6\ 5\ 6\ 6\ 6\ 7\ 6]^T$.

Moreover, we assume that the controller must enforce two specifications: (a) $M_3 + M_5 \leq 3$ and (b) $M_9 \leq 3$.

If the marking of the net is measurable, then the controlled net is live, as can be verified by reachability analysis.

If the marking of the plant is not measurable, an observer

must be used in the control loop. The resulting closed loop behavior is represented in the reachability graph within the dashed rectangle in fig. 2. Here each node is labeled as: $(M\,/\,\mu\,/B)$.
We can immediately observe that the error estimate $M-\mu$ decreases as the length of the observed word increases. Nevertheless, after the firing of $t_3$ we reach a blocking condition. In fact, the controller prevents the firing of both transitions $t_6$ and $t_7$ even if their firing is perfectly legal. This is due to the fact that there exists at least one marking in $\mathcal{C}(t_1t_4t_3)$ that would produce the violation of one of the controller specifications if either transition $t_6$ or $t_7$ fires. In particular, the firing of $t_6$ may potentially violate specification (b), while the firing of $t_7$ may potentially violate specification (a).

## 5 A procedure for deadlock recovery and estimate updating

Let us suppose that we can be sure that the net is blocked if a sufficiently long time has elapsed without observing any event occurrence. We say, in this case, that *the net has timed out.*

**Proposition 12 ([2]).** Assume that the net $N=(P,T,Pre,Post)$ controlled with the control pattern $f(\cdot,\mathcal{C})$ has timed out. Let us define $T'=\{t\in T\mid f(t,\mathcal{C})=1\}$ as the subset of $T$ containing the transitions enabled by the controller, and let $N'\prec_{T'}N$ be the $T'-$induced subnet of $N$. Then the actual (unknown) marking $M$ of the controlled net $N$ is a deadlock marking for the uncontrolled net $N'$, i.e., it belongs to $\mathcal{C}'=\mathcal{C}\cap\mathcal{M}_b(N')$. ■

We now present an automatic procedure that tries to exploit the information that the net has timed out to recover from this blocking condition and improve the estimate.

### 5.1 Deadlock recovery

The deadlock recovery procedure we firstly present in [2] in a slightly different form consists in recomputing the control pattern using a new IPP that adds to the constraints in (3) some additional constraint to capture the fact that the actual (unknown) marking $M$ belongs to $\mathcal{M}_b(N')$ for the net $N'$ defined in proposition 12.

**Algorithm 13. (Control Pattern Updating After Net Time-Out)**
Given a net $N=(P,\,T,Pre,Post)$ controlled using an observer, let $\mu$ and $B$ be the current value of estimate and bound, and define $\mathcal{C}=\mathcal{M}(\mu,B)$. Assume that the computed control pattern $f(\cdot,\mathcal{C})$ has led the net to a time-out. We can update the control pattern using the following procedure.

1. Let $i=0$ and define $f_0(\cdot)\stackrel{\text{def}}{=}f(\cdot,\mathcal{C})$ as the initial control pattern.
2. Let $T_i=\{t\in T\mid f_i(t)=1\}$ be the set of transitions enabled by the current control pattern, and let $N_i\prec_{T_i}N$ be the net obtained by $N$ removing all transitions not in $T_i$.
3. Update the control pattern to $f_{i+1}=g(f_i)$, where
$$g(f_i)\stackrel{\text{def}}{=}f(\cdot,\mathcal{C}\cap\mathcal{M}_b(N_i)). \tag{5}$$
4. If $f_{i+1}=f_i$ THEN exit: the deadlock recovery procedure has failed.
5. Wait until
   (a) EITHER a transition fires and THEN exit: the net has recovered from the deadlock
   (b) OR a new net time-out occurs and THEN let $i=i+1$ and go to 2. ■

Note that the operator $g:\{0,1\}^n\to\{0,1\}^n$ defined by (5) is a function of $f_i$ because $N_i$ is defined using $f_i$.
In this algorithm the knowledge that a time-out has occurred is used to restrict the set of consistent markings and construct a new control pattern (step 3) that, as the next proposition shows, is at least as permissive as the previous one. If the new control pattern is still blocking and a new time-out occurs the procedure is repeated until either the net recovers from deadlock, or until we cannot update the control pattern any more and the procedure fails.
We now present some elementary results concerning this algorithm.

**Proposition 14.** Algorithm 13 has the following properties:
— for all $i$, the updated control pattern computed at step 3 *is at least as permissive as* the previous one, i.e., $f_{i+1}\geq f_i$;
— the algorithm terminates in a finite number of steps;
— if the algorithm terminates at step 4 with $i=\bar{\imath}$, the final control pattern $f_{\bar{\imath}}$ is a fix point of the operator $g$.

**Proof:** The first statement can be proved by induction. In fact we observe (base step) that, by proposition 11, $\mathcal{C}\cap\mathcal{M}_b(N_0)\subseteq\mathcal{C}$ implies $f_1=f(\cdot,\mathcal{C}\cap\mathcal{M}_b(N_0))\geq f(\cdot,\mathcal{C})=f_0$. Assume now that $f_i\geq f_{i-1}$ for a given $i$: we prove (induction step) that the same inequality also holds for $i+1$. In fact, $f_i\geq f_{i-1}$ implies $N_{i-1}\prec_{T_{i-1}}N_i$. Thus $\mathcal{C}\cap\mathcal{M}_b(N_i)\subseteq\mathcal{C}\cap\mathcal{M}_b(N_{i-1})$ by proposition 3 and this implies, by proposition 11, that $f_{i+1}=f(\cdot,\mathcal{C}\cap\mathcal{M}_b(N_i))\geq f(\cdot,\mathcal{C}\cap\mathcal{M}_b(N_{i-1}))=f_i$.
The second statement follows from the fact that each time the loop in the algorithm is repeated, either $f_{i+1}=f_i$ (and in this case the algorithm terminates), or, by the previous statement, $f_{i+1}\gneq f_i$ and eventually the maximally permissive control that enables all transitions is reached in a number of steps less or equal to $|T|$.
The third statement follows trivially from the fact that if the algorithm terminates at step 4, then $f_{\bar{\imath}}=f_{\bar{\imath}+1}=g(f_{\bar{\imath}})$. □

### 5.2 Improving the marking estimate

Assume that given an observed word $w$, a current estimate $\mu_w$ and bound $B_w$, a blocking condition occurs, and that after $\bar{\imath}$ iterations of algorithm 13 a newly enabled transition $t$ fires. At this point, before the firing of $t$, the set of consistent markings is $\mathcal{M}(\mu_w,B_w)\cap\mathcal{M}_b(N_{\bar{\imath}})$, using the notation defined in the previous subsection. This set corresponds to the dark area in fig. 3.
We should keep this information when computing the new set of consistent markings $\mathcal{C}(wt)$ after the firing of $t$. Nevertheless, this would destroy the framework that inspired the estimate algorithm 6, in the sense that the set of consistent markings would loose the structure given by theorem (7).
Thus, we propose the following alternative solution. For each place $p_i\in P$ we solve an IPP of the form:

$$\begin{cases}\min M(p_i)\\ s.t.\\ M\in\mathcal{M}(\mu_w,B_w)\\ M\in\mathcal{M}_b(N_{\bar{\imath}})\end{cases} \tag{6}$$

Now, we define $\mu^*=[\mu_1^*\ \cdots\ \mu_m^*]^T$ where $\mu_i^*$ is the solution of the $i$–th IPP and let $B^*=B_w-V^T(\mu^*-\mu_w)$ be the corresponding bound. We use $\mu^*$ and $B^*$ as new

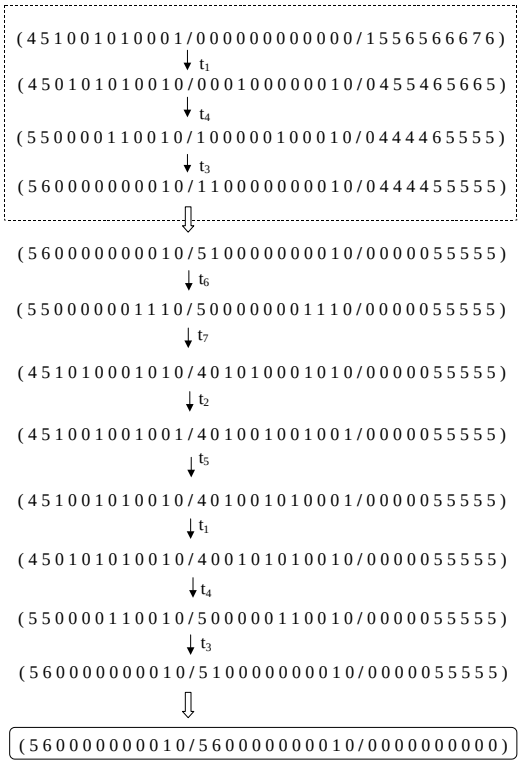


**Figure 2:** One possible evolution of the net in figure 1.

current values of the estimate $\mu_w$ and bound $B_w$ and continue from step 5 of algorithm 6, computing the updated estimate $\mu'_{wt}$.
This is equivalent to approximate the set of $w-$consistent markings after recovery, with the set $\mathcal{M}(\mu^*, B^*) = \{M \in \mathbb{N}^m \mid M \geq \mu^*, V^T \cdot M = V^T \cdot \mu^* + B^*\}$.
This set is also shown in fig. 3: being $\mathcal{M}(\mu_w, B_w) \cap \mathcal{M}_b(N_{\bar{i}}) \subseteq \mathcal{M}(\mu^*, B^*) \subseteq \mathcal{M}(\mu_w, B_w)$ we may be losing information, but nevertheless we can keep on with a linear algebraic characterization of the set of consistent markings in the simple form given by theorem (7).

### 5.3 Numerical example

In this section we show how the deadlock recovery procedure may be efficiently applied to the net in fig. 1. If we assume that the initial marking is that in fig. 1, then the first blocking condition occurs after the firing of the sequence $w = t_1 t_4 t_3$, as already discussed in subsection 4.1.
At this point, when a sufficiently long time has elapsed we apply algorithm 13 to update the control pattern. In particular, we have that the set of transitions enabled by the actual control pattern is $T_0 = T \setminus \{t_6, t_7\}$, while after only one iteration, we find out that $f = f_1 = \vec{1}$, i.e., all transitions become control enabled and the net has recovered from the observer induced deadlock. Finally, by solving $m = 12$ IPP, we may also improve the marking estimate.
To completely demonstrate the effectiveness of the proposed approach, in fig. 2 we have reported one possible evolution of the closed loop system with observer, assuming that also the deadlock recovery procedure is applied. We used larger arrows to denote that no transition has fired, but only the marking estimation has been updated. As it can be seen, at the end of this evolution path, the marking is completely reconstructed and no further deadlock may occur.
The same can be repeated for any other evolution starting from the initial marking in fig. 1, as it can be easily seen by looking at the whole reachability graph, that has not been reported here for brevity's requirements.

## 6 A sufficient condition for deadlock freeness

It is important to determine necessary and sufficient conditions to characterize those cases in which the deadlock recovery procedure works.
Here we consider a particular class of macromarkings, such that the vectors $\vec{v}_j$ are $P-$invariants. In this case, it is possible to show that the set of consistent markings at each step is a subset of the initial macromarking.

**Proposition 15.** Let the initial macromarking $\mathcal{V}(V, \vec{b})$ be such that $V^T C = \vec{0}$, i.e., each column $\vec{v}_j$ of $V$ is a P-invariant. Then, for all observed words $w$, $\mathcal{C}(w) \subseteq \mathcal{C}(w_0) \equiv \mathcal{V}(V, \vec{b})$.
**Proof:** First note that for all observed words $w$, $V^T \mu_w + B_w = \vec{b}$, whenever $V$ is a matrix of P-invariants. In fact, by algorithm 6, each time a new transition fires we have $V^T \mu_{wt} + B_{wt} = V^T [\mu'_{wt} + C(\cdot, t)] + \left[B_w - V^T(\mu'_{wt} - \mu_w)\right] = V^T \mu_w + B_w + V^T C(\cdot, t) = V^T \mu_w + B_w$, while initially, $V^T \mu_{w_0} + B_{w_0} = \vec{b}$.
Furthermore, $\mu_w \geq \vec{0} = \mu_{w_0}$, thus for all observed word $w$, the set of $w-$consistent markings is $\mathcal{C}(w) = \{M \in \mathbb{N}^n \mid M \geq \mu_w, V^T M = \vec{b}\} \subseteq \{M \in \mathbb{N}^n \mid V^T M = \vec{b}\} = \mathcal{C}(w_0)$. □
We use the previous result to give a sufficient condition to ensure that the controlled net will never time out.

**Theorem 16.** Consider a net $N$ with initial macromarking $\mathcal{V}(V, \vec{b})$ such that $V^T C = 0$, and controlled with algorithm 9. Let $T_0 = \{t \in T \mid f(t, \mathcal{C}(w_0)) = 1\}$ be the set of transitions enabled by the initial control pattern and let $N_0 \prec_{T_0} N$ be the $T_0-$induced subnet of $N$.
Then the closed loop system will never reach a blocking state, i.e., the net will never time out, if the following constraint set

$$\begin{cases} V^T M = \vec{b} \\ M \in \mathcal{M}_b(N_0) \end{cases} \tag{7}$$

does not admit any admissible solution for $M \in \mathbb{N}^m$.
**Proof:** First note that when the net is initialized, the set of consistent markings coincides with the initial macromarking, i.e., $\mathcal{C}(w_0) = \mathcal{V}(V, \vec{b}) = \{M \in \mathbb{N}^m \mid V^T M = \vec{b}\}$. If the constraint set (7) does not admit a feasible solution, the net is never blocked when the control pattern $f(\cdot, \mathcal{C}(w_0))$ is applied, regardless of the initial marking $M \in \mathcal{V}(V, \vec{b})$.
After a word $w$ has been observed, the set of consistent marking is $\mathcal{C}(w) \subseteq \mathcal{C}(w_0)$ (by proposition 15) while the actual marking still belongs to $\mathcal{V}(V, \vec{b})$, being $V$ a matrix of P-invariants. Thus by proposition 11 it holds that $f(\cdot, \mathcal{C}(w)) \geq f(\cdot, \mathcal{C}(w_0))$, and regardless of the current marking the controlled net is not blocked. □

We finally extend the previous result, giving a sufficient condition to ensure that, even if a time-out may occur, algorithm 13 will always successfully recover the net from a deadlock.
Consider a net $N$ with set of consistent markings $\mathcal{C}$. Assume that algorithm 13 is invoked but at step 5 we always execute step 5.b, until the algorithm stops at step 4 with $f_{i+1} = f_i$: this is the maximally permissive control pattern that could be applied if the net always times

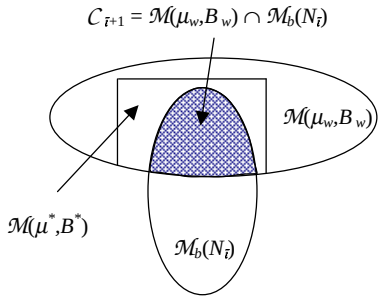


**Figure 3:** Generic inclusion relationship among sets $\mathcal{M}(\mu_w, B_w)$, $\mathcal{M}(\mu^*, B^*)$ and $\mathcal{M}_b(N_{\bar{i}})$.

out when the set of consistent markings is $\mathcal{C}$. A formal definition is the following.

**Definition 17.** Given a net $N$ controlled with an observer, and a set of consistent states $\mathcal{C}$, let us define $f_0 \stackrel{\text{def}}{=} f(\cdot, \mathcal{C})$ the initial control vector and let $f_{i+1} = g(f_i)$ for $i \geq 0$.
The *maximal control pattern* associated to $\mathcal{C}$ is $f_{\max}(\cdot, \mathcal{C}) \stackrel{\text{def}}{=} \lim_{i \to \infty} f_i$, i.e., it is the fixed point of $g$ reached iterating from $f_0$. Note that by proposition 14 part 2, this fixed point is reached in a finite number of steps (less or equal to the cardinality of the set of transitions $T$). ■

**Theorem 18.** Consider a net $N$ with initial macromarking $\mathcal{V}(V, \vec{b})$ such that $V^T C = 0$, and controlled with algorithm 9. Let $T_{\max} = \{t \in T \mid f_{\max}(t, \mathcal{V}(V, \vec{b})) = 1\}$ be the set of transitions enabled by the maximal control pattern associated to the initial consistent set $\mathcal{C}(w_0) = \mathcal{V}(V, \vec{b})$, as defined in the previous proposition. Let $N_{\max} \prec_{T_{\max}} N$ be the $T_{\max}-$induced subnet of $N$.
If a net time-out occurs and the procedure given in algorithm 13 is applied, the net will always recover from a deadlock if the following constraint set

$$\begin{cases} V^T M = \vec{b} \\ M \in \mathcal{M}_b(N_{\max}) \end{cases} \tag{8}$$

does not admit any admissible solution for $M \in \mathbb{N}^m$.

**Proof:** Firstly, observe that if the constraint set (8) does not admit a feasible solution, the time-out procedure is always capable of recovering from an initial deadlock, because eventually the control pattern $f_{\max}(t, \mathcal{V}(V, \vec{b}))$ will be reached and there exists at least an enabled transition regardless of the initial unknown marking $M \in \mathcal{V}(V, \vec{b})$.
Secondly, observe that by induction on the iteration step in algorithm 13, it is immediate to show that $\mathcal{C}' \subseteq \mathcal{C}''$ implies $f_{\max}(t, \mathcal{C}') \geq f_{\max}(t, \mathcal{C}'')$.
Finally, as in the proof of theorem 16, the result follows from the fact that after a word $w$ has been observed, the set of consistent markings is $\mathcal{C}(w) \subseteq \mathcal{C}(w_0)$ (by proposition 15) while the actual marking still belongs to $\mathcal{V}(V, \vec{b})$, being $V$ a matrix of P-invariants. □

**Example 19.** Let us consider again the manufacturing system in subsection 4.1. The initial macromarking considered is such that $V^T C = 0$, thus the assumption of theorem 18 are fulfilled. If we compute the maximal control pattern as defined in definition 17, we find out that $f_{\max}(\cdot, \mathcal{V}(V, \vec{b})) = \vec{1}$, that implies $N_{\max} = N$ according to the notation of theorem 18. Now, if we consider the set $\{M \in \mathbb{N}^m \mid V^T \cdot M = \vec{b},\ M \in \mathcal{M}_b(N)\}$, we find out that it does not admit any admissible solution for $M \in \mathbb{N}^m$. By theorem 18 this implies that if a net time-out occurs and we apply the procedure given in algorithm 13, then the net will always recover from deadlock. ■

## 7 Conclusions

In this paper we have dealt with the problem of enforcing a set of GMEC on a timed Petri net by a state feedback control under the assumption that the system state is not measurable but can only be estimated. We show that the use of an estimate instead of the actual marking, may lead to a deadlock even if the controlled system is live. In the case that the net system is structurally bounded, we propose an algorithm that accelerates the state estimation and helps us to detect the observer induced deadlock. A characterization of those cases in which the proposed procedure works is finally provided.

## References

[1] K. Barkaoui, A. Chaoui, B. Zouari, "Supervisory control of discrete event systems using structure theory of Petri nets ," *1997 IEEE Int. Conf. on Systems, Man and Cybernetics*, pp. 3750-3755, (Orlando, USA) 1997.

[2] F. Basile, P. Chiacchio, A. Giua, C. Seatzu, "Deadlock recovery of controlled Petri net models using observers," *8th IEEE International Conference on Emerging Technologies and Factory Automation*, (Antibes, France), pp. 441–449, October 2001.

[3] F. Chu, X. Xie, "Deadlock analysis of Petri nets using siphons and mathematical programming," *IEEE Trans. on Robotics and Automation*, Vol. 13, No. 6, pp. 793–804, 1997.

[4] Di Cesare, F., G. Harhalakis, J.M. Proth, M. Silva and F.B. Vernadat, *Practice of Petri nets in manufacturing*, Chapman and Hall, 1993.

[5] J. Ezpeleta, J.M. Colom, J. Martinez, "A Petri net based deadlock prevention policy for flexible manufacturing systems", *IEEE Trans. On Robotics and Automation*, Vol. 11, No. 2, pp. 173–184, 1995.

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

[7] A. Giua, "Petri net state estimators based on event observation," *Proc. 36th Int. Conf. on Decision and Control*, San Diego, California, pp. 4086–4091, December 1997.

[8] A. Giua, C. Seatzu, "Observability of place/transition nets," *IEEE Trans. on Automatic Control*, Vol. 47, No. 9, pp. 1424 - 1437, 2002.

[9] Y. Li, W.M. Wonham, "Control of vector discrete-event systems — part II: controller synthesis," *IEEE Trans. on Automatic Control*, Vol. 39, No. 3, pp. 512–531, 1994.

[10] T. Murata, "Petri nets: properties, analysis and applications," *Proc. IEEE*, Proc. 77, N. 4, pp. 541–580, 1989.

[11] J. Park, S.A. Reveliotis, "Deadlock avoidance in sequential resource allocation systems with multiple resource acquisitions and flexible routings," *IEEE Trans. on Automatic Control*, Vol. 46, No. 10, pp. 1572–1583, 2001.

[12] A. Ramírez–Treviño, I. Rivera–Rangel, E. López–Mellado, "Observer design for discrete event systems modeled by intrerpreted Petri nets," *2000 IEEE Int. Conf. on Robotics and Automation*, pp. 2871–2876, April 2000.

[13] S. Takai, T. Ushio, S. Kodama, "Static-state feedback control of discrete-event systems under partial observation," *IEEE Trans. on Automatic Control*, Vol. 40, No. 11, pp. 1950–1955, 1995.

[14] K. Yamalidou, J.O. Moody, M.D. Lemmon, P.J. Antsaklis, "Feedback control of Petri nets based on place invariants," *Automatica*, Vol. 32, No. 1, 1996.

[15] L. Zhang, L.E. Holloway, "Forbidden state avoidance in controlled Petri nets under partial observation," *Proc. 33rd Allerton Conf.* (Monticello, Illinois), pp. 146–155, October 1995.