NONBLOCKING CONTROL OF PETRI NETS USING UNFOLDING

Alessandro Giua * **Xiaolan Xie** **

* *Dip. Ing. Elettrica ed Elettronica, U. di Cagliari, Italy.*
Email: giua@diee.unica.it
** *INRIA/MACSI Team, ISGMP, U. de Metz, France.*
Email: xie@loria.fr

Abstract: We deal with the problem of controlling a safe place/transition nets so as to avoid a set of forbidden markings $\mathcal{F}$. If a given set of markings has property REACH, i.e., if it is closed under the reachability operator, using the technique of unfolding it is possible to efficiently design a maximally permissive supervisor to solve this control problem. We consider the additional problem of forbidding a larger set $\mathcal{F}_I$ that also contains those markings from which a marking in $\mathcal{F}$ is inevitably reached unless the controller introduces a deadlock and show how this problem can be solved still using the unfolding.

Keywords: Petri nets, discrete event systems, control, unfolding.

1. INTRODUCTION

Although *partial order* methods (Esparza *et al.*, 2002; McMillan, 1995) have proved to be a powerful instrument in the *verification* of concurrent systems, the application of these techniques to the *control* of discrete event systems has not received a lot of attention. Recently, He and Lemmon (2000; 2002) have presented an original approach based on unfolding for liveness verification and enforcing. However we have shown (Xie and Giua, 2004) that that some key results of these papers need to be refined. As a result, the applicability of unfolding for Petri net supervision is still an open issue.

In the paper we consider discrete event systems modeled by safe place/transition nets with a control specification that requires avoiding a set of forbidden marking $\mathcal{F}$. In the current state of investigation, we assume that all transitions are controllable.

In (Giua and Xie, 2004) we assumed that the set $\mathcal{F}$ has property REACH: once a forbidden marking is reached, all markings reachable from it will also be forbidden. Under this assumption the unfolding has a special property: if a configuration (i.e., a set of transition firings) is forbidden, any larger configuration should also be forbidden. We showed that in this case a simple control structure - that consists in a set of places to be added to a finite prefix of the unfolding, called order 1 unfolding - can be used to implement a maximally permissive control policy that enforces the specification.

In this paper there are three main new contributions.

Firstly, we define the notion of order 2 unfolding and show its relevance to the control of forbidden markings.

Secondly, we consider the problem of preventing the larger set $\mathcal{F}_I$ of impending forbidden marking. This is a superset of the forbidden markings that also includes all those markings from which - unless the supervisor blocks the plant - a marking in $\mathcal{F}$ is inevitably reached in a finite number of steps. In this case, we use a larger prefix of the unfolding, that we call order 2, to compute a set of control places that, added to order 1 unfolding, can be used to implement a maximally permissive control policy for this problem.

Finally, unlike (Giua and Xie, 2004) where the set of forbidden marking was given, we show that thanks to the special structure of the unfolding (it is an acyclic net) it is possible to characterize the deadlock markings of the original net by structural analysis.

The approach we present in the paper requires an exhaustive enumeration of the set of forbidden markings. It has however the advantage of allowing one to construct a maximally permissive supervisor

in the form of a "controlled" occurrence net (i.e., an occurrence net with the addition of control places) using a procedure where the set of markings of the plant needs not be exhaustively enumerated. The closed loop system in this approach can also be represented by this controlled occurrence net.

2. BACKGROUND ON PETRI NETS

The Petri net model considered in this paper is an *ordinary Place/Transition net* (P/T net) denoted $N = (P, T, F)$, where P is a set of m places; T is a set of n transitions; $F \subseteq (P \times T) \cup (T \times P)$ is the flow function. The *preset* and *postset* of a node $x \in P \cup T$ are denoted ${}^\bullet x \triangleq \{x' \,|(x', x) \in F\}$ and $x^\bullet \triangleq \{x' \,|(x, x') \in F\}$.

A *marking* is a vector $M : P \to \mathbb{N}$; we denote $M(p)$ the marking of place p. A *P/T system* or *net system* $\langle N, M_0\rangle$ is a net N with an initial marking M_0.

A transition t is *enabled* at M iff $M(p) > 0$ for all $p \in {}^\bullet t$. If t is enabled, it may *fire* yielding the marking $M' = M + C(\cdot, t)$. We write $M \ |\sigma\rangle \ M'$ to denote that the sequence of transitions $\sigma = t_{j_1} \cdots t_{j_k}$ is enabled at M and its firing yields M'.

We can associate to a sequence σ a *firing vector* $X : T \to \mathbb{N}$ such that $X(t) = k$ if the transition t is contained k times in σ.

A marking M is *reachable* in $\langle N, M_0\rangle$ iff there exists a firing sequence σ such that $M_0 \ |\sigma\rangle \ M$. The set of all markings reachable from M_0 is called *reachability set* and is denoted $R(N, M_0)$.

The *incidence matrix* of a net is an $m \times n$ matrix C where; $C(p, t) = 1$ if $(t, p) \in F$ and $(p, t) \notin F$, $C(p, t) = -1$ if $(p, t) \in F$ and $(t, p) \notin F$, else $C(p, t) = 0$.

A place p is *safe* if for all $M \in R(N, M_0)$ it holds $M(p) \leq 1$. A net system $\langle N, M_0\rangle$ is said safe if all its places are safe. A marking M of a safe net system is a binary vector and can also be seen as a set of places $M = \{p \in P \,|M(p) = 1\}$.

3. UNFOLDING

In this section we informally recall how it is possible, given a safe net system $\langle N, M_0\rangle$, to *unfold* it constructing a *labelled occurrence net* $\tilde{N}(M_0)$.

To the unfolding $\tilde{N}(M_0) = (\tilde{P}, \tilde{T}, \tilde{F})$ a *labelling function* $\ell : (\tilde{P} \to P) \cup (\tilde{T} \to T)$ is also associated: it maps each node of the unfolding into a node of the original net N. Note that usually a node p or t of N may correspond to more than one node of the unfolding, i.e., $\ell^{-1}(p) \subset \tilde{P}$ and $\ell^{-1}(t) \subset \tilde{T}$.

The labelling function can also map set of nodes into set of nodes. In particular, in the following procedure given a set of places $P' \subseteq P$ of the original net, we write $P' = \hat{\ell}(\tilde{P}')$ to denote that the set of places $\tilde{P}'$ of the unfolding has the same cardinality of P' and $P' = \left\{p \in P \,\middle|\, \tilde{p} \in \tilde{P}', p = \ell(\tilde{p})\right\}$, hence each place of $\tilde{P}'$ maps into a place of P' but no two places in $\tilde{P}'$ map into the same place of P'.

Procedure 1. (Unfolding of a safe net system $\langle N, M_0\rangle$ into an occurrence net $\tilde{N}(M_0)$)

(1) Add to the unfolding a set of source places $\tilde{P}_0$ with $\hat{\ell}(\tilde{P}_0) = \{p \in P \,|M_0(p) = 1\}$.
(2) Let $i := 0$.
(3) Let $\tilde{P}_{\exp} := \tilde{P}_i$
(4) If $\tilde{P}_i = \emptyset$ then STOP.
(5) Let $i := i + 1$.
(6) Let $\tilde{P}_i := \emptyset$.
(7) For all transitions $t \in T$
For all sets of places $\tilde{P}' \subseteq \tilde{P}_{\exp}$ such that the following three conditions are all verified:
- $\hat{\ell}(\tilde{P}') = {}^\bullet t$,
- all places in $\tilde{P}'$ are concurrent,
- $\tilde{P}' \cap \tilde{P}_{i-1} \neq \emptyset$,
(a) Add to the unfolding a new transition $\tilde{t}$ with $\hat{\ell}(\tilde{t}) = t$.
(b) Add to the unfolding a set of new places $\tilde{P}''$ with $\hat{\ell}(\tilde{P}'') = t^\bullet$.
(c) Add an arc from each place in $\tilde{P}'$ to $\tilde{t}$.
(d) Add an arc from $\tilde{t}$ to each place in $\tilde{P}''$.
(e) Let $\tilde{P}_i := \tilde{P}_i \cup \tilde{P}''$.
(f) Let $\tilde{P}_{\exp} := \tilde{P}_{\exp} \cup \tilde{P}''$.
(8) Goto 4. ■

A discussion of this procedure can be found in (Giua and Xie, 2004).

We can consider an unfolding both as a net and as a marked net where the initial marking assigns to each source place in $\tilde{P}_0$ a token, so we need not specify its initial marking and simply write $R(\tilde{N}(M_0))$ to denote its reachability set.

Note that the unfolding is a safe net so we can represent a marking with the set of non-empty place: we write $\tilde{M}_0 = \tilde{P}_0$ and in general $\tilde{M} = \left\{\tilde{p} \in \tilde{P} \,\middle|\, \tilde{M}(\tilde{p}) = 1\right\}$. It is also possible to apply the mapping $\hat{\ell}$ to markings.

Definition 2. *To each marking $\tilde{M}$ of the unfolding corresponds a marking of the original net $M = \hat{\ell}(\tilde{M}) \triangleq \left\{p \in P \,|p = \ell(\tilde{p}) \,, \tilde{p} \in \tilde{M}\right\}$. If $\hat{\ell}(\tilde{M}) = \hat{\ell}(\tilde{M}')$ we write $\tilde{M} =_P \tilde{M}'$.* ■

A firing vector $\tilde{X}$ of the unfolding is a binary vector that can also be seen as a set of transitions $\tilde{X} = \left\{\tilde{t} \in \tilde{T} \,\middle|\, \tilde{X}(\tilde{t}) = 1\right\}$.

Definition 3. *Given a transition $\tilde{t} \in \tilde{T}$, the minimal firing vector of the unfolding that contains it is called its* local configuration*; it can be show that this vector is unique and we denote it $[\tilde{t}]$. The marking reached firing configuration $\tilde{X}$ (resp., $[\tilde{t}]$) will be denoted $\tilde{M}(\tilde{X})$ (resp., $\tilde{M}([\tilde{t}])$).* ■

It is also clear that each marking $\tilde{M}$ reachable in $\tilde{N}(M_0)$ corresponds to a unique configuration in $\tilde{N}(M_0)$ (the unfolding net is acyclic) that we sometimes denote $\text{conf}(\tilde{M})$.

Given a net system $\langle N, M_0\rangle$, following He and Lemmon (2002), we consider a finite prefix of its unfolding.

Definition 4 (Order 1 unfolding). *The order 1 unfolding, denoted $\tilde{N}_1(M_0)$, is a finite prefix of*

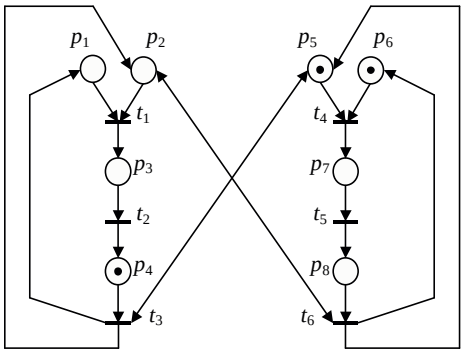

Fig. 1. A safe Petri net.

the unfolding obtained by Procedure 1 stopping the construction of the unfolding when we reach a cut-off transition $\tilde{t}$*, i.e., a transition such that:*
EITHER firing the local configuration of $\tilde{t}$ *brings back to the initial marking, i.e.,* $\tilde{M}([\tilde{t}]) =_P \tilde{M}_0$*;*
OR there exists another transition $\tilde{t}'$ *with the following properties:*
(a) $\tilde{t}'$ *has a smaller configuration than* $\tilde{t}$*:* $[\tilde{t}'] \subset [\tilde{t}]$*;*
(b) the markings reached firing the two configurations are equivalent, i.e., $\tilde{M}([\tilde{t}']) =_P \tilde{M}([\tilde{t}])$*.*
In the following we call $\tilde{t}'$ *the mirror transition of* $\tilde{t}$ *in* $\tilde{N}_1(M_0)$*.* ■

The complexity of checking if a given transition $\tilde{t}$ is a cut-off is linear in the size of $[\tilde{t}]$.

Algorithm 5. *The order 1 unfolding can be constructed using a modified version of Procedure 1 where the instruction 7.(f) is changed to*
7.(f') If t *is not a cut-off transition, then let* $\tilde{P}_{\text{exp}} := \tilde{P}_{\text{exp}} \cup \tilde{P}''$*.* ■

Example 6. Consider the net shown in Figure 1. Its order 1 unfolding is shown in Figure 2 (ignore the red subnet). Places and transitions are arranged in tiers (levels): tier 0 contains the initially marked places, tier 1 the initially enabled tansitions and their output places, etc. A place $\tilde{p}$ of the unfolding such that $\ell(\tilde{p}) = p_k$ is labelled k. A transition $\tilde{t}$ of the unfolding such that $\ell(\tilde{t}) = t_k$ is labelled k. The cut-off transitions are denoted by a thick line: they are transition 2 on tier 3 and transition 6 on tier 4. Transition 5 on tier 2 is not not a cut-off transition: after its firing the unfolding cannot proceed because a deadlock is reached. Note that we also consider as part of the order 1 unfolding the cut-off transitions and their output places. ■

The following result follows from an original result presented in (McMillan, 1995).

Proposition 7. *The labelling function maps the reachability set of the order 1 unfolding* $\tilde{N}_1(M_0)$ *into that of the original system, i.e.,* $R(N, M_0) = \left\{ M \in \mathbb{N}^m \,\middle|\, M = \ell(\tilde{M}) \,, \tilde{M} \in R(\tilde{N}_1(M_0)) \right\}$. ■

We can also define a larger finite prefix of the unfolding.

Definition 8 (Order 2 unfolding). *Once constructed* $\tilde{N}_1(M_0)$ *, assume we continue the unfolding until we reach a transition* $\tilde{t}$ *such that there exist a transition* $\tilde{t}'$ *with the following properties:*

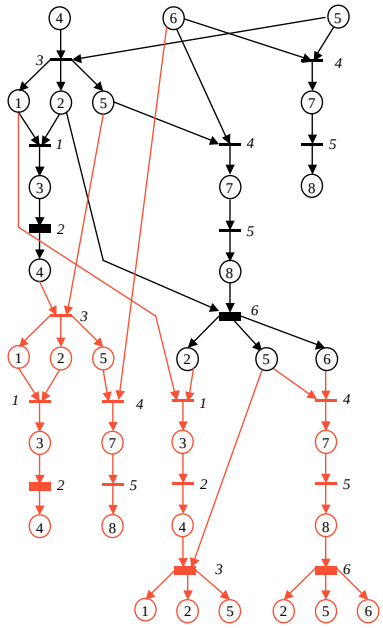

Fig. 2. The order 1 unfolding (subnet in black) and the order 2 unfolding (the complete net) of the net in Figure 1.

(a) either $\tilde{t}'$ *does not belong to* $\tilde{N}_1(M_0)$ *or it is a cut-off transition of* $\tilde{N}_1(M_0)$*;*
(b) $\tilde{t}'$ *has a smaller configuration:* $[\tilde{t}'] \subset [\tilde{t}]$*;*
(c) the two configurations reach equivalent markings: $\tilde{M}([\tilde{t}']) =_P \tilde{M}([\tilde{t}])$*.*
The resulting net, called order 2 unfolding, will be denoted $\tilde{N}_2(M_0)$*.* ■

Example 9. Consider the net shown in Figure 1. Its order 2 unfolding is shown in Figure 2. The cut-off transitions of the order 2 unfolding are the red transitions drawn with a thick line. ■

4. A CLASS OF FORBIDDEN MARKINGS

We consider a control problem where the set of forbidden marking $\mathcal{F}$ has a special structure.

Definition 10. *A set* $\mathcal{F} \subseteq R(N, M_0)$ *has property REACH wrt a net system* (N, M_0) *if* $M \in \mathcal{F}$ *and* $M' \in R(N, M) \Rightarrow M' \in \mathcal{F}$*.* ■

Thus property REACH implies that the set is closed under the reachability operator. The following result shows an important consequence of the property REACH.

Theorem 11 (Giua and Xie (2004)). *Given a set* $\mathcal{F}$ *with property REACH and a marking* $\tilde{M}$ *such that* $\hat{\ell}(\tilde{M}) \in \mathcal{F}$*, if* $\tilde{M}$ *is reachable with configuration* $\tilde{X}$*, then any larger configuration* $\tilde{X}' \geq \tilde{X}$ *leads to a marking* $\tilde{M}'$ *such that* $\hat{\ell}(\tilde{M}') \in \mathcal{F}$ *.* ■

A forbidden marking $\tilde{M}$ can be prevented controlling the transitions inputting into the places that belong to $\tilde{M}$ and that do not precede any other such transition.

Definition 12. *If* $\tilde{M}$ *is reachable with configuration* $\tilde{X}$*, the set of* control transitions *of* $\tilde{M}$ *is* $\tilde{X}_c = \left\{ \tilde{t} \in \tilde{X} \,\middle|\, (\nexists \tilde{t}' \in \tilde{X})\ \tilde{t}' \neq \tilde{t},\ \tilde{t} \in [\tilde{t}'] \right\}$. ■

We will use the following control structure to prevent reaching $\tilde{M}$.

Definition 13. *Given a marking $\tilde{M}$ with set of control transitions $\tilde{X}_c$, the control place $\tilde{p}_c$ for $\tilde{M}$ is a new place initially marked with $\left|\tilde{X}_c\right| - 1$ tokens and with an arc going to each transition in $\tilde{X}_c$. The incidence matrix of the control place is $\tilde{C}(\tilde{p}_c, \tilde{t}) = -1$ if $\tilde{t} \in \tilde{X}_c$, else $\tilde{C}(\tilde{p}_c, \tilde{t}) = 0$.* ■

The net obtained by adding these control places to the order 1 unfolding is called $\tilde{N}_{1,c}(M_0)$. This net is not necessarily an occurrence net because the control places may contain more than one token.

Example 14. Given the net in Figure 1, assume we want to forbid the set of markings $\mathcal{F} = \{(00010001)\}$. The (unique) forbidden marking is $\{p_4, p_8\}$. The two corresponding markings on the unfolding are: (a) place 4 on tier 0 and place 8 on tier 2; (b) places 4 and 8 on tier 3. The corresponding control places are, respectively, p_{c1} and p_{c2} shown in Figure 3. Control place p_{c1} is empty because its corresponding set of control transitions is a singleton: this means that transition 5 on tier 1 can never fire.

If we ignore all other control places except p_{c1} and p_{c2}, Figure 3 shows the net $\tilde{N}_{1,c}(M_0)$. ■

Definition 15. *The control policy for $\mathcal{F}$ uses the net $\tilde{N}_{1,c}(M_0)$ and can be defined as follows.*

(1) The plant and the net $\tilde{N}_{1,c}(M_0)$ are initialised with the respective initial marking.

(2) Compute a control pattern as follows: if $\tilde{T}_e$ is the set of transitions enabled in $\tilde{N}_{1,c}(M_0)$, the set of transitions that are enabled by the controller on the plant is $T_e = \ell(\tilde{T}_e)$.

(3) If a transition t fires in the plant, the unique transition $\tilde{t} \in \ell^{-1}(t)$ enabled in $\tilde{N}_{1,c}(M_0)$ is fired. If $\tilde{t}$ is a cut-off transition with mirror transition $\tilde{t}'$ and whose firing yields $\tilde{M}$, after the firing of $\tilde{t}$ the marking of the unfolding is reset to the mirror marking $\tilde{M}' = \tilde{M} - \tilde{C}\left([\tilde{t}] - [\tilde{t}']\right)$.

(4) Goto 2. ■

This control policy is maximally permissive if $\mathcal{F}$ has property REACH (Giua and Xie, 2004).

5. CONTROL POLICIES THAT DO NOT INTRODUCE BLOCKING

For some control problems it is not sufficient to prevent a net from reaching markings in a set $\mathcal{F}$ but it is also necessary to prevent the set $\mathcal{F}_I$ of markings that will inevitably lead to a marking in $\mathcal{F}$.

Definition 16. *Given a set $\mathcal{F} \subseteq R(N, M_0)$ we define its* impending set *as*

$$\mathcal{F}_I = \{M \in R(N, M_0) \mid (\exists k \in \mathbb{N}) R_{\geq k}(N, M) \subseteq \mathcal{F}, \; R_{<k}(N, M) \cap D(N, M_0) \subseteq \mathcal{F}\},$$

where $R_{\geq k}(N, M)$ (resp., $R_{<k}(N, M)$) denotes the set of markings reachable from M with a firing sequence containing at least (resp., less than) k transitions, and $D(N, M_0)$ is the set of dead markings of the net system $\langle N, M_0 \rangle$. ■

Thus, starting from a marking in $\mathcal{F}_I$ any evolution of length k or more and any evolution of length less than k that cannot be continued leads to $\mathcal{F}$. Clearly if a marking in $\mathcal{F}_I \backslash \mathcal{F}$ is reached, the only means the supervisor has to prevent the plant from reaching a marking in $\mathcal{F}$ is that of blocking it. Hence avoiding $\mathcal{F}_I$ allows the supervisor to prevent $\mathcal{F}$ without having to block the plant. Note that by definition $\mathcal{F} \subseteq \mathcal{F}_I$.

In this paper we extend the results presented in (Giua and Xie, 2004), assuming that the larger set $\mathcal{F}_I$ must be avoided. Property REACH will allow us to use unfolding to design optimal controllers.

Theorem 17. *If a set $\mathcal{F}$ has property REACH, then also the set $\mathcal{F}_I$ has property REACH.*

Proof. Consider any marking $M \in \mathcal{F}_I$. From the definition, there exists an integer k such that $R_{\geq k}(N, M) \subseteq \mathcal{F}, R_{<k}(N, M) \cap D(N, M_0) \subseteq \mathcal{F}$. Consider any marking M' reachable from M such that $M' \in R_i(N, M)$. If $i \geq k$, then $M' \in \mathcal{F}$ and hence $M' \in \mathcal{F}_I$. If $i < k$, then $M' \in \mathcal{F}_I$ since $R_{\geq k-i}(N, M') \subseteq R_{\geq k}(N, M) \subseteq \mathcal{F}$, and $R_{<k-i}(N, M') \cap D(N, M_0) \subseteq R_{<k}(N, M) \cap D(N, M_0) \subseteq \mathcal{F}$. □

Since $\mathcal{F}_I$ also has the REACH property, the control policy for $\mathcal{F}$ applies if $\mathcal{F}_I$ is known and the order 1 unfolding is enough. Unfortunately, for most control problems, $\mathcal{F}_I$ is not given. To check whether $\hat{\ell}(\tilde{M}) \in \mathcal{F}_I$, we need to check whether $\mathcal{F}$ is avoidable starting from $\tilde{M}$. Order 1 unfolding is no longer enough as it does not allow the reachability analysis for all reachable markings. Next theorem shows this is possible with order 2 unfolding.

Theorem 18. *Given a net system $\langle N, M_0 \rangle$, let $M \in R(N, M_0)$ be a reachable marking and let $\tilde{M} \in R(\tilde{N}_1(M_0))$ be a marking of the unfolding such that $\hat{\ell}(\tilde{M}) = M$. Then the order 1 unfolding $\tilde{N}_1(M)$ of net N with initial marking M is a subnet of $N_2(M_0)$ starting at $\tilde{M}$.*

Proof. Consider any configuration $\tilde{X}$ of $\tilde{N}_1(M_0)$ corresponding to marking $\tilde{M}$. Considering the order 1 unfolding $\tilde{N}_1(\tilde{M})$ starting at $\tilde{M}$. For any configuration of $\tilde{Y}$ of $\tilde{N}_1(\tilde{M})$, from the completeness of the unfolding net $\tilde{N}(M_0)$, $\tilde{X} + \tilde{Y}$ is a configuration of $\tilde{N}(M_0)$ and $\tilde{N}_1(\tilde{M})$ is a subnet of $\tilde{N}(M_0)$. The theorem is proved if any transition $\tilde{t}$ in $\tilde{Y}$ is either a cut-off transition of $\tilde{N}_2(M_0)$ or its local configuration $[\tilde{t}]$ does not contain any cut-off transition of $\tilde{N}_2(M_0)$. For this purpose assume that there exists a transition $\tilde{t}$ in $\tilde{Y}$ such that its local configuration $[\tilde{t}]$ contains a cut-off transition $\tilde{w}$ of $\tilde{N}_2(M_0)$. Of course $\tilde{w}$ belongs to $\tilde{N}_1(\tilde{M})$ as well. From the definition of $\tilde{N}_2(M_0)$, there exists another transition $\tilde{w}'$ such that (a) either $\tilde{w}'$ does not belong to $\tilde{N}_1(M_0)$ or it is a cut-off transition of $\tilde{N}_1(M_0)$; (b) $\tilde{w}'$ has a smaller configuration: $[\tilde{w}'] \subset [\tilde{w}]$; (c) the markings reached firing the two configurations are equivalent: $\tilde{M}([\tilde{w}']) =_P \tilde{M}([\tilde{w}])$. From the above definition, $\tilde{w}'$ is a transition of the

local configuration $[\tilde{t}]$. Further by construction $\tilde{t}$ is not in conflict with any transition in $\tilde{X}$ and hence $\tilde{w}'$ is not in conflict with $\tilde{X}$. As a result, $\tilde{Z} = \tilde{X} \cup [\tilde{w}']$ is configuration, $\tilde{Z} \subset \tilde{X}$ and $\tilde{w}'$ is a transition of $\tilde{N}_1(\tilde{M})$. Similarly $\tilde{w}$ is a transition of $\tilde{N}_1(\tilde{M})$ and it is a cut-off transition of $\tilde{N}_1(\tilde{M})$. Because $\tilde{t}$ follows $\tilde{w}$, it cannot be in $\tilde{N}_1(\tilde{M})$. This contradicts the fact that $\tilde{t}$ is a transition of $\tilde{N}_1(\tilde{M})$ and concludes the proof. □

Hence, if we identify in the order 2 all markings $\tilde{M}$ such that $\hat{\ell}(\tilde{M}) \in \mathcal{F}$, then we can easily identify, by reachability analysis, all markings in $\mathcal{F}_I$.
We finally show that the controlled net, when all markings in $\mathcal{F}_I$ have been forbidden, does not contain controller induced deadlocks.
Theorem 19. *Let $\tilde{N}_{1,c}(M_0)$ be the controlled unfolding net in all markings $\tilde{M}$ such that $\hat{\ell}(\tilde{M}) \in \mathcal{F}_I$ are forbidden by their related control places. Then there exist no dead marking in $\tilde{M}$ of $\tilde{N}_{1,c}(M_0)$ unless it is also a dead marking of $\tilde{N}_1(M_0)$.*

Proof. Let us assume, it is possible to reach in the controlled net a marking $\tilde{M}$ that is a control induced dead marking, i.e., a marking that is dead because of the controller but that is not dead in the order 1 unfolding. Since the control places only forbid transitions firings that lead to $\mathcal{F}_I$, then without control all transitions enabled at $\tilde{M}$ would lead to a marking in $\mathcal{F}_I$ in one step. By definition, this implies that $\hat{\ell}(\tilde{M}) \in \mathcal{F}_I$. But this is a contradiction, because we assumed no markings in $\mathcal{F}_I$ is reachable in the controlled net. □

6. DEADLOCK AVOIDANCE CONTROL

We present an approach based on linear algebra to identify markings in $\mathcal{F}_I$ and to prevent them.
We consider a particular case in which the set of forbidden marking $\mathcal{F}$ is the set of dead markings. Hence the set $\mathcal{F}_I$ is the set of the impending deadlocks and a control law that avoids this set is a maximally permissive control law that makes a blocking net nonblocking.
In this section, when we need not distinguish between order 1 and order 2 we denote an unfolding $\tilde{N}$ while its incidence matrix is the $\tilde{m} \times \tilde{n}$ matrix $\tilde{C}$. Similarly, the controlled net with the addition of $\tilde{m}_c$ control places is denoted $\tilde{N}_c$ while its incidence matrix is the $(\tilde{m} + \tilde{m}_c) \times \tilde{n}$ matrix $\tilde{C}_c$.
We first observe an important advantage of working on the unfolding.
Proposition 20. *Let us consider an unfolding net $\tilde{N}(\tilde{M}_0)$. If the vector $\tilde{X} \in \mathbb{N}^{\tilde{n}}$ satisfies $\tilde{M}_0 + \tilde{C}\tilde{X} \geq 0$, then there exists a firing sequence enabled in $\tilde{N}(\tilde{M}_0)$ whose firing count vector is $\tilde{X}$. The same result applies to the controlled net $\tilde{N}_c(\tilde{M}_{c,0})$.*

Proof. This is a classic result that holds for all acyclic nets. The unfolding is acyclic by construction, and the addition of control places (with only output arcs) does not modify this property. □

As an obvious corollary of this result, one can characterize reachability with the state equation.
Corollary 21. *The set of reachable markings of an unfolding net $\tilde{N}(\tilde{M}_0)$ is equal to the set of potentially reachable markings, i.e., $R(\tilde{N}(M_0)) = \left\{ \tilde{M} \in \mathbb{N}^{\tilde{m}} \,\middle|\, \tilde{M} = \tilde{M}_0 + \tilde{C}\tilde{X}, \tilde{X} \in \mathbb{N}^{\tilde{n}} \right\}$. The same result holds for a controlled net $\tilde{N}_c(\tilde{M}_{c,0})$.* ■
The following result gives a linear algebraic characterization of the set of deadlock markings.
Proposition 22. *Given an unfolding net $\tilde{N}(\tilde{M}_0)$, we have that a marking $\tilde{M}$ is dead if and only if for all $\tilde{t} \in \tilde{T}$ if holds*

$$\sum_{\tilde{p} \in {}^\bullet\tilde{t}} M(\tilde{p}) \leq |{}^\bullet\tilde{t}| - 1.$$

Proof. The result follows from the fact that the unfolding is a safe net, hence $\tilde{t}$ if enabled if and only if $M(\tilde{p}) = 1$ for all $\tilde{p} \in {}^\bullet\tilde{t}$. □

This result does not hold for the controlled net, because the control places are not necessarily safe. However, the following result holds.
Proposition 23. *Given a controlled net $\tilde{N}_c(\tilde{M}_{c,0})$, let $\tilde{P}$ be the set of places of the unfolding net, and $\tilde{P}_c$ the set of control places. Given any marking $\tilde{M}$, we can associate to each place $\tilde{p}_c \in \tilde{P}_c$ a binary counter $\mu(\tilde{p}_c) \in \{0, 1\}$ that satisfies the following equations:*

$$\mu(\tilde{p}_c) \leq M(\tilde{p}_c) \ \vee \ M_{c,0}(\tilde{p}_c)\mu(\tilde{p}_c) \geq M(\tilde{p}_c). \quad (1)$$

Then a marking $\tilde{M}$ is dead if and only if for all $\tilde{t} \in \tilde{T}$ if holds

$$\sum_{\tilde{p} \in \tilde{P} \cap {}^\bullet\tilde{t}} M(\tilde{p}) + \sum_{\tilde{p}_c \in \tilde{P}_c \cap {}^\bullet\tilde{t}} \mu(\tilde{p}_c) \leq |{}^\bullet\tilde{t}| - 1.$$

Proof. We first observe that the first equation (1) implies that $\mu(\tilde{p}) = 0$ if $M(\tilde{p}_c) = 0$, while the second equation (1) implies that $\mu(\tilde{p}) = 1$ if $M(\tilde{p}_c) > 0$ (note that by construction the control place is such that $M_{c,0}(\tilde{p}_c) \geq M(\tilde{p}_c)$), i.e., $\mu(\tilde{p}) = 1$ if and only if $\tilde{p}$ is marked. The results follows because $\tilde{t}$ is enabled if and only if all its input places are marked. □

Our third and final preliminary result characterizes redundant control places, i.e., places that can be removed without changing the behavior of the controlled net.
Definition 24. *Given a controlled net $\tilde{N}_c(\tilde{M}_{c,0})$, let $\tilde{N}'_c(\tilde{M}'_{c,0})$ be the net obtained from N_c removing control place $\tilde{p}'_c$. Place $\tilde{p}'_c$ is* redundant *in $\tilde{N}_c(\tilde{M}_{c,0})$ if for all reachable markings $\tilde{M} \in R(\tilde{N}_c(\tilde{M}_{c,0}))$ and for all transitions $\tilde{t} \in \tilde{p}'^\bullet$ it holds $(\forall p_c \in {}^\bullet\tilde{t} \setminus \{p'_c\})\ M(p_c) > 0 \implies M(p'_c) > 0$.* ■
Proposition 25. *With the notation of the previous definition, place $\tilde{p}'_c$ is* redundant *in $\tilde{N}_c(\tilde{M}_{c,0})$ if and only if the following integer programming problem (IPP)*

$$\begin{aligned} k = \min \ & C(\tilde{p}'_c, \cdot)\tilde{X} \\ s.t. \quad & \tilde{M}'_{c,0} + \tilde{C}'\tilde{X} \geq 0 \end{aligned}$$

— where $\tilde{C}$ and $\tilde{C}'$ are, respectively, the incidence matrices of $\tilde{N}_c$ and $\tilde{N}'_c$ — has optimal solution k^* such that $M_{c,0}(\tilde{p}') + k^* \geq 0$.

Proof. By Proposition 20, any vector $\tilde{X}$ satisfying the IPP corresponds to a firable sequence of $\tilde{N}'_c(\tilde{M}'_{c,0})$. This sequence is never disabled by place p'_c in $\tilde{N}_c(\tilde{M}_{c,0})$ if $M_{c,0}(\tilde{p}')+k^* \geq 0$. Hence $\tilde{N}'_c(\tilde{M}'_{c,0})$ and $\tilde{N}_c(\tilde{M}_{c,0})$ have the same firable sequences. □

Next algorithm shows how to design a maximally permissive deadlock avoidance controller.

Algorithm 26. Control law for $\mathcal{F}_I$

(1) Construct the order 2 unfolding $\tilde{N}_2(\tilde{M}_0)$.

(2) Determine the set of dead markings of $\tilde{N}_2(\tilde{M}_0)$, excluding the markings that include the output places $\tilde{P}_{out}$ of the cut-off transitions of the order 2 unfolding[1]*. This set corresponds to the feasible solutions $\tilde{M}$ of the following constraint set*

$$\begin{cases} \tilde{M} = \tilde{M}_0 + \tilde{C}_2\tilde{X} \\ \sum_{\tilde{p}\in{}^\bullet\tilde{t}} M(\tilde{p}) \leq |{}^\bullet\tilde{t}| - 1 \ \ (\forall \tilde{t} \in \tilde{T}) \\ \tilde{M}(\tilde{p}) = 0 \qquad\qquad (\forall \tilde{p} \in \tilde{P}_{out}) \\ \tilde{M} \in \mathbb{N}^{\tilde{m}}, \tilde{X} \in \mathbb{N}^{\tilde{n}} \end{cases}$$

and for each marking $\tilde{M}$ add to the unfolding the corresponding set of control places to obtain a net $\tilde{N}_{2,c}(\tilde{M}_{c,0})$.

(3) Determine the set of dead markings of $\tilde{N}_{2,c}(\tilde{M}_{c,0})$ as the set of feasible solutions $\tilde{M}$ of the following constraint set

$$\begin{cases} \tilde{M} = \tilde{M}_{c,0} + \tilde{C}_{2,c}\tilde{X} \\ \mu(p_c) \leq \tilde{M}(p_c) \qquad\qquad (\forall \tilde{p_c} \in \tilde{P}_c) \\ \tilde{M}_{c,0}(p_c)\mu(p_c) \geq \tilde{M}(p_c) \qquad\qquad (\forall \tilde{p_c} \in \tilde{P}_c) \\ \sum_{\tilde{p}\in\tilde{P}\cap{}^\bullet\tilde{t}} M(\tilde{p}) + \sum_{\tilde{p}_c\in\tilde{P}_c\cap{}^\bullet\tilde{t}} \mu(\tilde{p}_c) \leq |{}^\bullet\tilde{t}| - 1 \ \ (\forall \tilde{t} \in \tilde{T}) \\ \tilde{M}(\tilde{p}) = 0 \qquad\qquad (\forall \tilde{p} \in \tilde{P}_{out}) \\ \tilde{M} \in \mathbb{N}^{\tilde{m}}, \tilde{X} \in \mathbb{N}^{\tilde{n}}, \mu \in \{0,1\}^{\tilde{m}_c} \end{cases}$$

(4) If the set of dead markings determined at the previous step is not empty, add to $\tilde{N}_{2,c}$ the corresponding control places and go to 3.

(5) Let $\tilde{N}_{1,c}$ be the net obtained from $\tilde{N}_{2,c}$ removing all places and transitions that do not belong to the order 1 unfolding, and removing all control places that have arcs going to a transition that has been removed.

(6) Check all control places of $\tilde{N}_{1,c}$ for redundancy, using the IPP of Proposition 25, and remove the redundant ones. ■

The net constructed with the previous algorithm can be used to compute a maximally permissive nonblocking control policy, as in Definition 15.

[1] These markings even if they are dead in $\tilde{N}_2(\tilde{M}_0)$, do not necessarily correspond to dead markings in the original net.

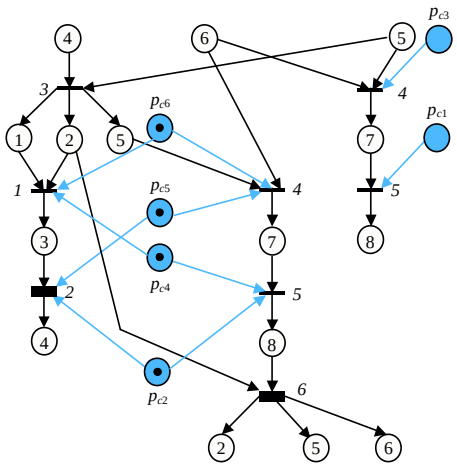

Fig. 3. The net $\tilde{N}_{1,c}$ in Example 27 before removing the redundant control places.

Example 27. The net in Figure 1 is blocking. Using the previous algorithm we first construct its order 2 unfolding (see Figure 2) and at step 2 identify three blocking markings corresponding to the unique dead marking of the original net $\{p_4, p_8\}$: (a) place 4 on tier 0 and place 8 on tier 2, (b) places 4 and 8 on tier 3, (c) places 4 and 8 on tier 6 (the rightmost places). Iterating at step 3 of the algorithm we identify new control induced markings, and add the corresponding control places to the order 2 unfolding. At step 5, removing the second order subnet, we obtain the net $\tilde{N}_{1,c}$ shown in Figure 3. Finally at step 5 we eliminate the redundant places: only places $p_{c,3}$ and $p_{c,6}$ remain at the end of the algorithm. ■

7. CONCLUSIONS

In this paper we have used the technique of unfolding to design maximally permissive nonblocking supervisors for safe Petri nets assuming that the specification is given by a set of forbidden markings with property REACH.

REFERENCES

Esparza, J., S. Römer and W. Vogler (2002). An improvement of McMillan's unfolding algorithm. *Formal Methods in System Design* **20**, 285–310.

Giua, A. and X. Xie (2004). Control of safe ordinary Petri nets with marking specifications using unfolding. In: *Proc. IFAC WODES'04: 7th Work. on Discrete Event Systems*. Reims, France. pp. 61–66.

He, K.X and M.D. Lemmon (2000). Liveness verification of discrete-event systems modeled by n-safe ordinary Petri nets. *Lecture Notes in Computer Science: Proc. 21st Int. Conf. on Application and Theory of Petri Nets (Aarhus Denmark)* **1825**, 227–243.

He, K.X. and M.D. Lemmon (2002). Liveness-enforcing supervision of bounded ordinary Petri nets using partial order methods. *IEEE Trans. Automatic Control* **47**(7), 1042–1055.

McMillan, K.L. (1995). A technique of state space search based on unfolding. *Formal Methods in System Design* **6**(1), 45–65.

Xie, X. and A. Giua (2004). Counterexamples to «Liveness-enforcing supervision of bounded ordinary Petri nets using partial order methods»,. *IEEE Trans. Automatic Control* **49**(7), 1217–1219.