FEEDBACK CONTROL LOGIC FOR
BACKWARD CONFLICT FREE CHOICE NETS

Francesco Basile* Ciro Carbone*
Pasquale Chiacchio*

*Dip. di Ingegneria dell'Informazione ed Ing. Elettrica,
Università di Salerno, Via Ponte Don Melillo, 84084 -
Fisciano (SA), ITALY, e-mail: {fbasile, ccarbone}@unisa.it*

Abstract: In this paper, the forbidden state problem, in the context of supervisory control of discrete event systems modelled by Petri nets, is discussed. The forbidden state problem is specified by generalized mutual exclusion constraints (GMECs). The case of backward conflict free and free choice uncontrollable subnet is considered. The uncontrollable subnet is first extended to a number of well formed free choice nets and then decomposed in marked graph components, which can be obtained from minimal T-invariants of the extended net. The forbidden state problem is so re-formulated into an equivalent one, based on the decomposed net, such that it can be solved by a linear programming problem. Thus, a polynomial complexity solution, suitable for on-line control, is achieved, improving the existing results in literature for this net subclass. *Copyright© 2005 IFAC.*

Keywords: Supervisory control, Petri nets, Discrete Event Systems.

1. INTRODUCTION

Petri nets have been successfully proposed as modelling formalism for DES control (Giua *et al.*, 1992; Bruce H. Krogh and Lawrence E. Holloway, 1991; Moody and Antsaklis, 1998) alternative to controlled automata (P.J.Ramadge and W.M. Wonham, 1989). In Petri Net control area a transition may be controllable or uncontrollable. A controllable transition may be disabled by the supervisor — a controlling agent which ensures that the behavior of the system is within a legal one. The presence of uncontrollable transitions makes not legal any marking from which it is possible to reach by firing only uncontrollable transitions a no-legal marking. Enforcing Generalized Mutual Exclusion Constraints (GMECs) on a Petri Net (PN) model is a very interesting research topic in supervisory control of Discrete Event Systems (DESs) area. A lot of DES control problems (boundness, mutual exclusion in resources sharing, deadlock avoidance, etc.) can be formulated in terms of GMECs (Moody and Antsaklis, 1998). Three kinds of solutions to this problem can be found in the literature: analytical solutions (Bruce H. Krogh and Lawrence E. Holloway, 1991), PN based controllers (Giua *et al.*, 1992; Moody and Antsaklis, 2000), integer linear programming problem solution based controllers (Li and Wonham, 1994). The first one is very efficient for on-line control but it can be applied only to cyclic, safe and live marked graphs; recently, analytical solutions have been extended to general marked graphs (Ghaffari *et al.*, 2003). The second one gives, in general, a non maximally permissive solution. The last one can be applied to any acyclic uncontrollable subnet but it is not efficient from a computational point of view.

In this paper we restrict the uncontrollable plant net subclass to make easier the control problem. This approach was very successful since the graphical nature of PN makes easy to recognize if a PN model belongs to a certain net subclass.

Here we consider the problem of enforcing GMECs on PNs whose uncontrollable subnet is a Backward Conflict Free Choice Net (BCFCN). The main feature of this subclass is that every arc

from a place is either a unique outgoing arc to or a unique incoming arc from a transition and each place has only one incoming arc. BCFCNs model not only concurrency and synchronization of activities as the Marked Graph (MG) subclass but also decisions (Murata, 1989). The proposed control syntheses consists of

Off-line computation: The BCFCN uncontrollable plant model is extended to a number of well formed free choice nets and then decomposed in marked graph components. Such components can be obtained from minimal T-invariants of the extended net.

On-line computation: The forbidden state problem is re-formulated into an equivalent one, based on the decomposed net and it can be solved by a linear programming problem, having a polynomial complexity. An important consequence of the Rank theorem is that we can decide in polynomial time if a FCN is well-formed.
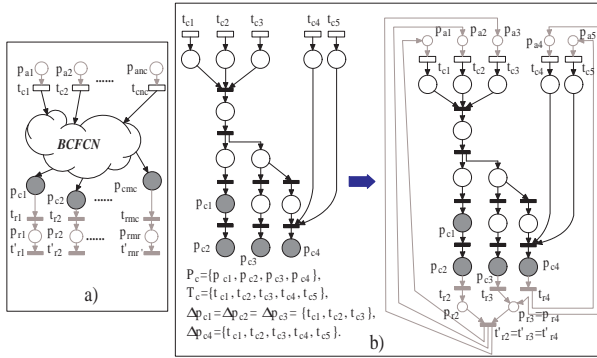

Fig. 1. a) Subnets $\{\mathcal{N}_{r_i}\}_{i=1..m_c}$ and places $\{p_{a_j}\}_{j=1..n_c}$ are added to the BCFCN uncontrollable subnet to get well-formedness. b) Application of the algorithm 1 to a simple BCFCN.

2. BACKGROUND

In this section PN notations and theory are briefly recalled. Please, refer to (Murata, 1989) for further details. An ordinary net is a structure $\mathcal{N} = \langle P, T, \mathbf{Pre}, \mathbf{Post} \rangle$ where: P is a set of m *places* represented by circles; T is a set of n *transitions* represented by bars; **Pre** (**Post**) is the $| P | \times | T |$ sized, binary valued, pre-(post-)incidence matrix. The *preset* and *postset* of a node $X \in P \cup T$ are denoted $^\bullet X$ and $X^\bullet$. The incidence matrix $\mathbf{C}$ of the net is denoted as $\mathbf{C}$. An ordinary net $\mathcal{N}$ is a Marked Graph (MG) if $^\bullet p = p^\bullet = 1, \forall p \in P$. An ordinary net $\mathcal{N}$ is a Free Choice Net (FCN) if $\forall p \in P, |p^\bullet| \leq 1$ or $^\bullet\{p^\bullet\} = \{p\}$. A net $\mathcal{N}$ is Backward Conflict Free (BCF) iff $|^\bullet p| = 1$. We denote by BCFCN a BCF free choice net. The net *marking* is denoted as $\mathbf{m}$. A P/T system or net system $\langle \mathcal{N}, \mathbf{m}_0 \rangle$ is a P/T net $\mathcal{N}$ with an initial marking $\mathbf{m}_0$. The notation $\mathbf{m}[t > \mathbf{m}'$ means that an enabled transition t may fire at $\mathbf{m}$ yielding $\mathbf{m}'$. A *firing sequence* from $\mathbf{m}_0$ is a (possibly empty) sequence of transitions $\sigma = t_1...t_k$ such that $\mathbf{m}_0[t_1 > \mathbf{m}_1[t_2 > \mathbf{m}_2...[t_k > \mathbf{m}_k$. A marking $\mathbf{m}$ is reachable in $\langle \mathcal{N}, \mathbf{m}_0 \rangle$ iff there exists a firing sequence σ such that $\mathbf{m}_0[\sigma > \mathbf{m}$. Given a net system $\langle \mathcal{N}, \mathbf{m}_0 \rangle$ the set of reachable markings is denoted $R(\mathcal{N}, \mathbf{m}_0)$. The function $\boldsymbol{\sigma} : T \to \mathbb{N}$, where $\boldsymbol{\sigma}(t)$ represents the number of occurrences of t in σ, is called firing count vector of the

fireable sequence σ. If $\mathbf{m}_0[\sigma > \mathbf{m}$, we can write $\mathbf{m} = \mathbf{m}_0 + \mathbf{C}(\cdot, t) \cdot \boldsymbol{\sigma}$, known as the *state equation* of the system.

Right (Left) annuller vectors of $\mathbf{C}$ are called *T-flows* (*P-flows*), i.e. $\mathbf{x} : T \to \mathbb{Q}, \ \mathbf{x} \neq \mathbf{0} \mid \mathbf{Cx} = 0 \ (\mathbf{x} : P \to \mathbb{Q}, \ \mathbf{x} \neq \mathbf{0} \mid \mathbf{x}^T \mathbf{C} = 0)$. P-flows (T-flows) form a linear space (it is also possible to consider real-valued solutions; however since incidence matrices only have integer entries, every real-valued solution is the product of a real scalar and a rational-valued solution). When positive integer solutions are considered, right (left) annuller vectors of $\mathbf{C}$ are called *T-invariants* (*P-invariants*), i.e. $\mathbf{x} : T \to \mathbb{N}, \ \mathbf{x} \neq \mathbf{0} \mid \mathbf{Cx} = 0 \ (\mathbf{x} : P \to \mathbb{N}, \ \mathbf{x} \neq \mathbf{0} \mid \mathbf{x}^T \mathbf{C} = 0)$; P-invariants (T-invariants) do not form a linear space. The *support* of a T-invariant (P-invariant) $\mathbf{x}$ is defined as $\| \mathbf{x} \| = \{t \in T \mid \mathbf{x}(t) > 0\} \ (\| \mathbf{x} \| = \{p \in P \mid \mathbf{x}(p) > 0\})$. A T-invariant (P-invariant) $\mathbf{x}$ has a *minimal support* iff there exists no other invariant $\mathbf{x}'$ such that $\| \mathbf{x}' \| \subset \| \mathbf{x} \|$. A T-invariant (P-invariant) is *canonical* iff the greatest common divisor of its components is 1. A T-invariant (P-invariant) is said to be *minimal* iff it is canonical and has a minimal support. A T-invariant (P-invariant) $\mathbf{x}$ is said to be positive iff $\mathbf{x} > \mathbf{0}$. $\mathcal{N}$ is *consistent* iff $\exists \mathbf{y} \in (\mathbb{N}^+)^n$ such that $\mathbf{Cy} = \mathbf{0}$.

A P/T system is *live* when, from every reachable marking, every transition can ultimately occur. $\mathcal{N}$ is *structurally live* iff $\exists \mathbf{m}_0$ such that $\langle \mathcal{N}, \mathbf{m}_0 \rangle$ is live. A place $p \in P$ is said to be *k-bounded* iff $\forall \mathbf{m} \in R(\mathcal{N}, \mathbf{m}_0), \ \mathbf{m}(p) \leq k$. A net system $\langle \mathcal{N}, \mathbf{m}_0 \rangle$ is said to be k-bounded iff each of its places is k-bounded, and it is bounded iff it is bounded for some $k \in \mathbb{N}$. A net $\mathcal{N}$ is *structurally bounded* iff $\forall \mathbf{m}_0$ the net system $\langle \mathcal{N}, \mathbf{m}_0 \rangle$ is bounded. $\mathcal{N}$ is structurally bounded iff $\exists \mathbf{x} \in (\mathbb{N}^+)^m$ such that $\mathbf{x}^T \mathbf{C} \leq \mathbf{0}$. $\mathcal{N}$ is *conservative* iff $\exists \mathbf{x} \in (\mathbb{N}^+)^m$ such that $\mathbf{x}^T \mathbf{C} = \mathbf{0}$.

A *path* is an alternative sequence of places and transitions that joins two distinct nodes, places and transitions, with an arc (if the arc is directed, the path is called directed). A net is (*strongly*) *connected* if there exists a (directed) path from any node, place or transition, to any other node.

From now on we assume that, given a net system $\langle \mathcal{N}_i, \mathbf{m}_{0i} \rangle$, the set of places, the set of transitions and the incidence matrix are denoted respectively as $P_i, T_i, \mathbf{C}_i$.

3. PROBLEM STATEMENT

Let consider a set of legal markings expressed by a set of n_c linear inequality constraints, called Generalized Mutual Exclusion Constraint (GMEC). A single GMEC is a couple $(\mathbf{l}, k)$ where $\mathbf{l} : P \to \mathbb{Z}$ is a $m \times 1$ weight vector and $k \in \mathbb{Z}$. Given the net system $\langle \mathcal{N}, \mathbf{m}_0 \rangle$, a GMEC defines a set of markings that will be called *legal markings*: $\mathcal{M}(\mathbf{l}, \mathbf{k}) = \{\mathbf{m} \in \mathbb{N}^m \mid \mathbf{l}^T \mathbf{m} \leq k\}$. If $\mathbf{l}(p) \neq 0$, the place p is called *critical place* and it is drawn as a shaded circle. The set of critical places of a GMEC $(\mathbf{l}, k)$ is denoted by $P_c(\mathbf{l}, k)$. The markings that are not legal are called *forbidden markings*.

It is assumed that the set of transitions T of a net is partitioned into two disjoint subsets: T_{uc}, the set of uncontrollable transitions (drawn as filled boxes), and T_c, the set of controllable transitions (drawn as empty boxes). A controllable transition may be disabled by the supervisor — a controlling agent which ensures that the behavior of the system is within a legal one. By T_{uc}^* we denote the set of all possible sequences of uncontrollable transitions. A controlling agent, called *supervisor*, must ensure that the forbidden markings are not

be reached. Since uncontrollable transitions cannot be disabled, in addition to the markings that do not satisfy the GMEC also the set of markings

$$\mathcal{M}_{fu}(\boldsymbol{l},k) = \{\boldsymbol{m} \mid \boldsymbol{m}[\sigma > \boldsymbol{m}', \ \boldsymbol{m}' \notin \mathcal{M}(\boldsymbol{l},k), \sigma \in T_u^*\}$$

with $\boldsymbol{m} \in \mathbb{N}^m$, has to be forbidden. The set of legal markings under control is
$$\mathcal{M}_c(\boldsymbol{l},k) = (\mathcal{M}(\boldsymbol{l},k) \cap R(\mathcal{N},\boldsymbol{m}_0)) \setminus \mathcal{M}_{fu}(\boldsymbol{l},k),$$
and obviously $\mid \mathcal{M}_c(\boldsymbol{l},k) \mid \leq \mid \mathcal{M}(\boldsymbol{l},k) \mid$.

A supervisor is *maximally permissive* if it forces the set of constraints to be obeyed, while allowing any action that is not forbidden by the constraints. The computation of the set $\mathcal{M}_c(\boldsymbol{l},k)$ is the key issue of the supervisor synthesis.

In (Li and Wonham, 1994) it has been shown that, if the uncontrollable plant subnet is acyclic, $\mathcal{M}_c(\boldsymbol{l},k)$ can be computed as solution of an Integer Linear Programming (ILP) problem having NP-hard complexity. The derived supervisor, that is maximally permissive, enables a transition $t \in T_c$ under the net marking $\hat{\boldsymbol{m}}$ if $\hat{\boldsymbol{m}}[t > \boldsymbol{m}$ and

$$\boldsymbol{l}^T \boldsymbol{m} + \boldsymbol{l}^T \boldsymbol{C}_{uc} \boldsymbol{\sigma}_{uc}^* \leq k \qquad (1)$$

where $\boldsymbol{\sigma}_{uc}^*$ is the solution of the following ILP

$$max_{\boldsymbol{\sigma}_{uc}} \boldsymbol{l}^T \boldsymbol{C}_{uc} \boldsymbol{\sigma}_{uc}$$
$$s.t. \begin{cases} \boldsymbol{\sigma}_{uc} \geq \boldsymbol{0} \\ \boldsymbol{C}_{uc} \boldsymbol{\sigma}_{uc} \geq -\boldsymbol{m} \end{cases} \qquad (2)$$

The contribution of this paper is twofold:
1) it will be shown that the ILP problem (2), when applied to a BCFCN system under some hypotheses, can be computed by solving a Linear Programming (LP) problem (so having polynomial complexity) without loss of permissiveness;
2) also BCFCN systems having cyclic uncontrollable subnets can be considered.

4. WELL-FORMED FREE CHOICE NETS

In this section some results, well known in FCN theory (Desel and Esparza, 1995), are recalled. These results are largely used in the paper since BCFCNs are extended into FCNs.

(Well-formed nets) A connected net $\mathcal{N}$ is *well-formed* if there exists a marking $\boldsymbol{m}_0$ of $\mathcal{N}$ such that $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ is a live and bounded system.

(MG-component) Let $\mathcal{N}'$ be the subnet of a net $\mathcal{N}$ generated by a non-empty set Σ of nodes. $\mathcal{N}'$ is a *MG-component* of $\mathcal{N}$ if:
- $\forall t \in \Sigma, \ \ ^{\bullet}t \cup t^{\bullet} \subseteq \Sigma$, and
- $\mathcal{N}'$ is a strongly connected MG.

Let us consider a minimal T-invariant $\boldsymbol{x}$, the subnet generated by $^{\bullet} \parallel \boldsymbol{x} \parallel \cup \parallel \boldsymbol{x} \parallel \cup \parallel \boldsymbol{x} \parallel^{\bullet}$ is said to be *induced* by minimal T-invariant $\boldsymbol{x}$.

Theorem 1. Let $\mathcal{N}$ be a well-formed free choice net. Minimal T-invariants induce MG-components.

Theorem 2. Well-formed free choice nets are covered by MG-components, i.e. each transition belongs to a MG-component. ∎

Given a vector $\boldsymbol{x}: P \to \mathbb{N}$ ($\boldsymbol{y}: T \to \mathbb{N}$) and a set $P' \subseteq P$ ($T' \subseteq T$), the vector $\boldsymbol{x}' = \boldsymbol{x}|P'$ ($\boldsymbol{y}' = \boldsymbol{y}|T'$) is defined as follows: $\boldsymbol{x}'(p) = \boldsymbol{x}(p)$ ($\boldsymbol{y}'(t) = \boldsymbol{y}(t)$) if $p \in P'$ ($t \in T'$) and $\boldsymbol{x}'(p) = 0$ ($\boldsymbol{y}'(t) = 0$) otherwise.

The following proposition states that the behavior of a MG-component is not restricted by the rest of the system.

Proposition 3. Let $\mathcal{N}'$ be a MG-component of a net $\mathcal{N}$. Let $\boldsymbol{m}_0$ be a marking of $\mathcal{N}$, and let σ be a sequence of transitions of T' in $\mathcal{N}'$. $\boldsymbol{m}_0[\sigma > \boldsymbol{m} \Longleftrightarrow \boldsymbol{m}_{0|P'}[\sigma > \boldsymbol{m}_{|P'}$.

(Clusters) Let x be a node of a net. The *cluster* of x, denoted by $[x]$, is the minimal set of nodes such that
- $x \in [x]$,
- if a place p belongs to x then $p^{\bullet}$ is included in $[x]$, and
- if a transition t belongs to $[x]$ then $^{\bullet}t$ is included in $[x]$.

The following theorem provides operative conditions to test if a free choice net is well-formed.

Theorem 4. **(The Rank Theorem)** Let $\mathcal{N}$ be a FCN. Let $\boldsymbol{C}$ be the incidence matrix of $\mathcal{N}$ and C_N the set of clusters of $\mathcal{N}$.

The net $\mathcal{N}$ is well-formed iff
(a) it is connected, and has at least one place and one transition,
(b) it has a positive P-invariant,
(c) it has a positive T-invariant, and
(d) $Rank(\boldsymbol{C}) = |C_N| - 1$. ∎

5. AN ALGORITHM TO EXTEND A BCFCN INTO STRONGLY CONNECTED FCNS

In this section the concept of GMEC critical subnet is introduced. By working on this subnet it is possible to re-formulate the ILP problem (2) as a LP one. At this aim a BCFCN extension into strongly connected FCNs is proposed.

(Influence Path) An *influence path* $\pi_t(p) = tp_1t_1p_2t_2...p_kt_kp$ of a critical place p is a directed path joining t to p such that t is a controllable transition and all other transitions in the path are uncontrollable. Influence paths are essential to identify the set of transitions whose firing can change the marking of a critical place. Let $\Pi(p)$ be the set of all the influence paths of p. Let define the set $\Delta_p \subseteq T_c$ as follows: $\Delta_p = \{t_c \in T_c | \exists \ \pi_{t_c}(p) \in \Pi(p)\}$.

(Influence Zone) The influence zone of a critical place p_c is the subnet with all nodes s for which there exists a directed path from s to p_c without controllable transitions except eventually s.

(GMEC Critical Subnet) The *GMEC Critical subnet*, denoted as $\mathcal{N}_{cs}(\boldsymbol{l},k)$, is the subnet containing any place or transition that belongs to the influence zone of each critical place of $(\boldsymbol{l},k)$.

Without loss of generality the case of a unique GMEC is considered. All the results presented

can be immediately extended to the general case. Therefore, afterwards, for the sake of brevity we use P_c instead of $P_c(\boldsymbol{l}, k)$ and $\mathcal{N}_{cs}$ instead of $\mathcal{N}_{cs}(\boldsymbol{l}, k)$.

(Assumption) We assume that the net $\mathcal{N}_{cs}$ is BCFCN. ∎

If the critical subnet (assumed to be a BCFCN) is not connected, the algorithm has to be applied to each connected component. The aim of the algorithm is to extend the critical subnet into a strongly connected FCN conservative and consistent. Loosely speaking, such extension is made a) without introducing any incoming or outgoing arc to places or transitions of the critical subnet except incoming arcs to controllable transitions or outcoming arcs from critical places as shown in fig. 1b; b) by synchronizing concurrent influence paths and by joining influence paths coming from choices in order to obtain a conservative and consistent net. Let us define $\mathcal{N}_{r_i}$ the subnet formed by t_{r_i}, p_{r_i}, t'_{r_i} connected as in fig. 1a.

Algorithm 1. Extension of critical subnet into a strongly connected FCN
Input: $\mathcal{N}_{cs}$ – Connected BCFCN.
Output: $\mathcal{N}_w$ – Strongly connected FCN.
```
begin
    (* Add the sub-net to make closures (cfr. Fig. 1a)*)
    P_c* := ∅;
    for p_c_i ∈ P_c do
    begin
        Δ_p_c_i := {t_c ∈ T_c|∃ π_t_c(p_c_i) ∈ Π(p_c_i)};
        if [∀t_c ∈ Δ_p_c_i, ∄π_t_c(p_c_j), p_c_j ∈ P_c − {p_c_i}
            and p_c_i ∈ π_t_c(p_c_j)]
        then
        begin
            ⟨Connect place p_c_i to the sub-net N_ri
                with an arc from p_c_i to t_ri⟩;
            P_c* := P_c* ∪ {p_c_i};
        end
    end
    for t_c_i ∈ T_c do
    begin
        ⟨Add a place p_a_i and connect it to the transition t_c_i⟩;
    end
    (* Search concurrencies and choices *)
    while [P_c* ≠ ∅] do
    begin
        p_c_i ∈ P_c*;
        P_c* := P_c* − {p_c_i};
        if [∃p_c_j ∈ P_c*|Δ_p_c_i ∩ Δ_p_c_j ≠ ∅] then
        (* There is a concurrency or choice *)
        begin
            ⟨ Merge transitions t'_r_i, t'_r_j ⟩;
            if [∃t_i ∈ π_t_c(p_c_i), ∃t_j ∈ π_t_c(p_c_j)
                and ∃p ∈ π_t_c(p_c_i) ∩ π_t_c(p_c_j)|p• ⊇ {t_i, t_j}] then
            begin (* There is choice *)
                ⟨ Merge places p_r_i, p_r_j ⟩;
                if [∃t̂_c ∈ T_c|t̂_c ∈ (Δ_p_c_i ∪ Δ_p_c_j)\Δ_p] then
                begin (* Synchronization after a choice *)
                    if [t̂_c ∈ Δ_p_c_i] then
                        ⟨∀t_k ∈ Δ_p_c_i \Δ_p, connect t_r_i to p_a_k⟩;
                    else
                        ⟨∀t_k ∈ Δ_p_c_j \Δ_p, connect t_r_j to p_a_k⟩;
                end
            end
        end
    end
```

```
    if [|t•_r_i| = 1] then
        ⟨∀t_k ∈ Δ_p_c_i, connect t'_r_i to p_a_k⟩;
    end
end.
```

Fig. 1b shows an example in which the algorithm is applied to a simple BCFCN. In order to apply our approach it is required that $\mathcal{N}_w$ is well-formed and thus Rank theorem can be used after $\mathcal{N}_w$ has been built by the algorithm 1.

6. MAIN RESULT

In this section it is shown that the ILP problem (2) formulated on the uncontrollable plant subnet can be transformed into an equivalent LP problem. This LP problem represents the unique on line computation required by our approach. To write the LP problem a number of off-line steps has to be performed as it is detailed in the following.

Let define the net system $\langle \mathcal{N}_w, \boldsymbol{m}_{w0} \rangle$ where $\mathcal{N}_w$ is the well-formed FCN net obtained from algorithm 1 and $\boldsymbol{m}_{w0}(p) = \boldsymbol{m}_0(p)$ if $p \in P_{cs}$ and $\boldsymbol{m}_{w0}(p) = 0$ if $p \notin P_{cs}$.

Let $\langle \mathcal{N}_w, \boldsymbol{m}_{w0} \rangle$ be the well-formed FCN system defined above, $\langle \tilde{\mathcal{N}}_{wd}, \tilde{\boldsymbol{m}}_{wd0} \rangle$ is the net system given by all MG-components of $\langle \mathcal{N}_w, \boldsymbol{m}_{w0} \rangle$ with $\sum_{q \in \mathcal{P}_r(p)} \tilde{\boldsymbol{m}}_{wd0}(q) = \boldsymbol{m}_{w0}(p)$ where $\mathcal{P}_r(p) \subseteq \tilde{P}_{wd}$ is the set of places associated to a $p \in P_w$ in the net $\tilde{\mathcal{N}}_{wd}$ (since p may belong to more than one MG-component).

Similarly, if a transition t belongs to more than one MG-component we denote by $\mathcal{T}_r(t) \subseteq \tilde{T}_{wd}$ the set of transitions in the net $\tilde{\mathcal{N}}_{wd}$ associated to $t \in T_w$ after the MG decomposition.

Finally, let define $T_{cwd} = \bigcup_{t_c \in T_c} \mathcal{T}_r(t_c)$. For example, if we consider the MG decomposition shown in Fig. 3c, $\mathcal{P}_r(p_{15}) = \{p_{15}^1, p_{15}^2\}$ and $\mathcal{T}_r(t_5) = \{t_5^1, t_5^2\}$.

Lemma 5. Let $\langle \mathcal{N}_{cs}, \boldsymbol{m}_{cs0} \rangle$ be a critical BCFCN net system and let $\langle \mathcal{N}_w, \boldsymbol{m}_{w0} \rangle$ be the well formed FCN system defined above,
$$\boldsymbol{m}_{w0|P_{cs}}[\sigma_{uc} > \boldsymbol{m}_{w|P_{cs}} \iff \boldsymbol{m}_{cs_0}[\sigma_{uc} > \boldsymbol{m}_{cs}.$$
Proof: The proof is immediate since the enabling of uncontrollable transitions does not depend on places and transitions outside critical subnet when controllable transition are disabled. ∎

Let denote $\hat{P} = \{p_{r_1}, ..., p_{r_{m_r}}\} \cup \{p_{a_1}, ..., p_{a_{n_c}}\}$ and $\hat{T} = \{t_{r_1}, ..., t_{r_{m_c}}\} \cup \{t'_{r_1}, ..., t'_{r_{n'_r}}\}$.

Lemma 6. Let $\langle \mathcal{N}_{wd}, \boldsymbol{m}_{wd0} \rangle$ be the net generated by removing from $\langle \tilde{\mathcal{N}}_{wd}, \tilde{\boldsymbol{m}}_{wd0} \rangle$ the places that belong to the set $\hat{P}$ and transitions that belong to the set $\hat{T} \cup T_{cwd}$. Let σ_u be a sequence of uncontrollable transitions in N_{wd},

$$\boldsymbol{m}_{wd0}[\sigma_{uc} > \boldsymbol{m}_{wd} \iff \tilde{\boldsymbol{m}}_{wd0|P_{wd}}[\sigma_{uc} > \tilde{\boldsymbol{m}}_{wd|P_{wd}}.$$

Proof: Places and transitions removed from $\langle \tilde{\mathcal{N}}_w, \tilde{\boldsymbol{m}}_w \rangle$ are both controllable transitions and places and transitions added by the algorithm 1 to the critical subnet. Thus, the marking of a place in the set P_{wd} cannot be influenced by places and transitions added by the algorithm 1 without a

firing of a controllable transition. In addition, all the sequence of uncontrollable transitions enabled in the net system $\langle \tilde{\mathcal{N}}_w, \tilde{\boldsymbol{m}}_w \rangle$ are still enabled in the net system $\langle \mathcal{N}_{wd}, \boldsymbol{m}_{wd} \rangle$. ∎

Let $(\boldsymbol{l}^T, k)$ be a GMEC on the plant net $\mathcal{N}$. The equivalent GMEC $(\boldsymbol{l}_{wd}^T, k)$ on the net $\mathcal{N}_{wd}$ can be obtained as follows:

$$\boldsymbol{l}^T \cdot \boldsymbol{m} \leq k \iff \sum_{p \in P_{cs}} \boldsymbol{l}^T(p)\boldsymbol{m}_{cs}(p) \leq k \iff$$

$$\sum_{p \in P_{cs}} \boldsymbol{l}^T(p) \sum_{q \in \mathcal{P}_r(p)} \boldsymbol{m}_{wd}(q) \leq k \iff$$

$$\sum_{p \in P_{cs}} \sum_{q \in \mathcal{P}_r(p)} \boldsymbol{l}^T(p)\boldsymbol{m}_{wd}(q) \leq k \iff \boldsymbol{l}_{wd}^T \cdot \boldsymbol{m}_{wd} \leq k.$$

Given a GMEC the off-line supervisor synthesis steps can be resumed as follows: 1) build the critical subnet $\mathcal{N}_{cs}$; 2) build $\mathcal{N}_w$ by the algorithm 1 and verify that it is a well formed net; 3) build $\tilde{\mathcal{N}}_{wd}$; 4) build $\mathcal{N}_{wd}$; 5) transform the GMEC into an equivalent one on the $\mathcal{N}_{wd}$ net.

The following proposition proves that the ILP problem (2) formulated on the uncontrollable plant subnet can be transformed into an equivalent LP problem re-formulated on the net $\mathcal{N}_{wd}$, that represents the only on-line computation.

Proposition 7. Let $\langle \mathcal{N}, \boldsymbol{m} \rangle$, $(\boldsymbol{l}, k)$, $\langle \mathcal{N}_{wd}, \boldsymbol{m}_{wd0} \rangle$, $(\boldsymbol{l}_{wd}, k)$ be, respectively, a plant net system, a GMEC to be enforced on the plant net system, the decomposition of the plant and the equivalent GMEC to be enforced on the decomposed net system. A controllable transition $t \in T_c$ has to be enabled under the net marking $\hat{\boldsymbol{m}} \in R(\mathcal{N}, \boldsymbol{m}_0)$ iff $\hat{\boldsymbol{m}}[t > \boldsymbol{m}$ and

$$\boldsymbol{l}_{wd}^T \boldsymbol{m}_{wd} + \boldsymbol{l}_{wd}^T \boldsymbol{C}_{wd} \boldsymbol{\sigma}_{wd}^* \leq k \qquad (3)$$

where $\boldsymbol{\sigma}_{wd}^*$ is the solution of the following LP

$$
\begin{aligned}
max \quad & \boldsymbol{l}_{wd}^T \boldsymbol{C}_{wd} \boldsymbol{\sigma}_{wd} \\
s.t. \quad (a) \quad & \boldsymbol{\sigma}_{wd} \geq \boldsymbol{0} \\
(b) \quad & \boldsymbol{C}_{wd} \boldsymbol{\sigma}_{wd} \geq -\boldsymbol{m}_{wd} \qquad (4) \\
(c) \quad & \sigma_{wd_i} \leq \boldsymbol{x}_{wd_j}^T \boldsymbol{m}_{wd}, \\
& \forall j = 1..N_p : \boldsymbol{x}_{wd_j}^T \mathbf{Pre}_{wd}(., i) > 0 \\
(d) \quad & \sum_{q \in \mathcal{P}_r(p)} \boldsymbol{m}_{wd}(q) = \boldsymbol{m}(p) \quad \forall p \in P_{cs}
\end{aligned}
$$

with variables $\boldsymbol{\sigma}_{wd}$ and $\boldsymbol{m}_{wd}$ and where P_{cs} is the set of places of the GMEC critical subnet $\mathcal{N}_{cs}$, N_p is the number of minimal P-invariants (the vectors $\boldsymbol{x}_{wd_j}^T$) of the net $\mathcal{N}_{wd}$.

Proof: Equations (4-a,b) come from the ILP (2). Equation (4-c) ensures that in presence of a token-free circuit the state equation of each MG component represented by (4-b) gives no spurious solutions (Murata, 1989).

The programming problem (4) is LP since it can be verified that the constraint matrix is totally unimodular. For the sake of brevity we omit the proof but we underline that the matrix $\boldsymbol{C}_{wd}$ is
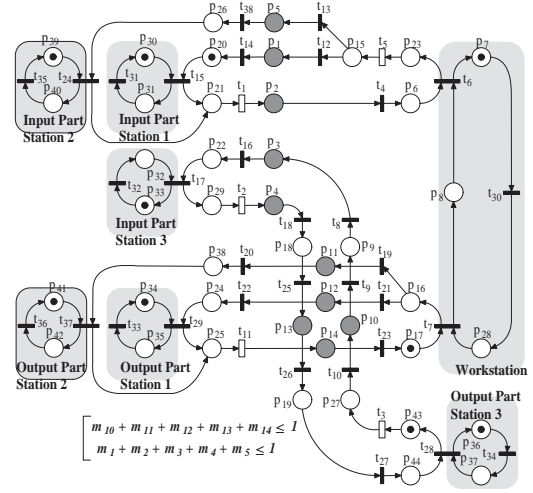

Fig. 2. PN model of a manufacturing system.

totally unimodular since it is a MG incidence matrix. From lemma 5 we know that the reachability problem of the critical subnet under uncontrollable transition firings can be solved on the $\langle \mathcal{N}_w, \boldsymbol{m}_w \rangle$ system (assumed to be a well formed free choice net and thus covered by MG components). From proposition 3 we know that a MG component is not influenced by the rest of the system. Since no join place (i.e. a place p with $|{}^\bullet p| > 1$) is present in the net $\mathcal{N}_{cs}$, in a MG component there is no uncontrollable transition which can be enabled by the firing of a transition that does not belong to this MG component (only in the subnet added by the algorithm join places may be found). Thus, the reachability problem of the critical subnet under uncontrollable transition firings can be solved on the $\langle \tilde{\mathcal{N}}_{wd}, \tilde{\boldsymbol{m}}_{wd} \rangle$ by consider any possible token allocation in each MG component according to initial marking. From lemma 6 we know that the reachability problem of the $\langle \tilde{\mathcal{N}}_{wd}, \tilde{\boldsymbol{m}}_{wd} \rangle$ net system under uncontrollable transition firings can be solved on the $\langle \mathcal{N}_{wd}, \boldsymbol{m}_{wd} \rangle$ net system. Equation (4-c) ensures that tokens are allocated in each MG-component according to $\boldsymbol{m}_{wd}$ since any choice in the net $\mathcal{N}_{cs}$ is free. Since only fireable sequences of uncontrollable transitions verify (4-a,b,c,d), we have the proof. ∎

7. CASE STUDY

In order to illustrate an application of our method we consider an example of coordinating multiple automated guided vehicles (AGVs) inspired to that one proposed in (Bruce H. Krogh and Lawrence E. Holloway, 1991). The PN in fig. 2 models an automated material handling system consisting of three AGVs which transport material between pairs of stations. The system has three lines: line 1 - connecting Workstation to Input Part Stations 1 and 2; line 2 - connecting Input Part Station 3 to Output Part Station 3; line 3 - connecting Workstation to Output Part Station 1
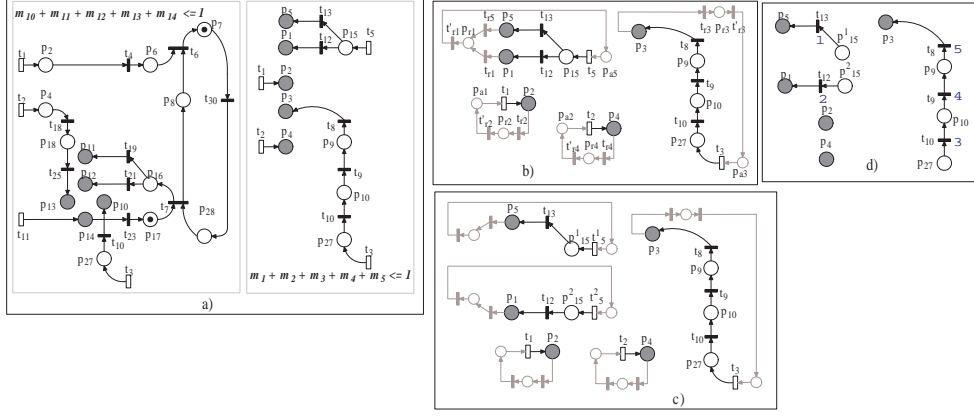
Fig. 3. a) Step 1: critical subnets $\mathcal{N}_{cs_1}$ and $\mathcal{N}_{cs_2}$. b) Step 2: apply algorithm 1 to each connected component of $\mathcal{N}_{cs_2}$. Let $\mathcal{N}_{w_2}$ be the obtained net. c) Step 3: MG-decomposition of $\mathcal{N}_{w_2}$: $\widetilde{\mathcal{N}}_{wd_2}$. d) Step 4: build $\mathcal{N}_{wd_2}$.

and 2. Respect to the example proposed in (Bruce H. Krogh and Lawrence E. Holloway, 1991) we introduce choices between uncontrollable transitions which model the AGV capability to decide to load from (unload onto) Input (Output) Part Station 1 or 2. The GMECs to be imposed are:

$$\begin{cases} (1) & m_{10} + m_{11} + m_{12} + m_{13} + m_{14} \leq 1 \\ (2) & m_1 + m_2 + m_3 + m_4 + m_5 \leq 1 \end{cases} \quad (5)$$

This means that, in order to avoid collisions between AGVs on the lines 1 and 2, only one token has to be present in critical places p_1, p_2, p_3, p_4, p_5 at any time. Equally, in order to avoid collisions between AGVs on the lines 2 and 3, only one token has to be present in critical places $p_{10}, p_{11}, p_{12}, p_{13}, p_{14}$ at any time. The first step in our method is to find the two critical subnets $\mathcal{N}_{cs_1}$ and $\mathcal{N}_{cs_2}$ associated to GMECs (5.1) and (5.2) (see fig. 3a). For the sake of brevity, let us to consider only the subnet $\mathcal{N}_{cs_2}$ associated to the GMEC (5.2) (see fig. 3d). As step 2, the algorithm 1 is applied to each connected component of the BCFCN in fig. 3a, in order to get the associated strongly connected FCNs. $\mathcal{N}_{cs_1}$ is transformed in $\mathcal{N}_{w_1}$ and $\mathcal{N}_{cs_2}$ is transformed in $\mathcal{N}_{w_2}$ (see fig. 3b). By applying the Rank theorem it is verified that $\mathcal{N}_{w_1}$ and $\mathcal{N}_{w_2}$ are well formed nets. The third step in our net decomposition is to calculate all the minimal T-invariants of the well-formed FCNs in fig. 3b, thus obtaining the MG-component decomposition, as shown in fig. 3c. The last step consists of building the nets $\mathcal{N}_{wd_1}$ and $\mathcal{N}_{wd_2}$ starting from the nets $\widetilde{\mathcal{N}}_{wd_1}$ and $\widetilde{\mathcal{N}}_{wd_2}$ (see fig. 3d). Related to this GMEC, in order to complete the off-line computation, the linear programming problem (4), to be executed on-line, is devised as follows

$$max \quad \sigma_{wd_1} + \sigma_{wd_2} + \sigma_{wd_5}$$
$$s.t. \quad \sigma_{wd_1}, \sigma_{wd_2}, \sigma_{wd_3}, \sigma_{wd_4}, \sigma_{wd_5}, \boldsymbol{m}_{wd}(p_{15}^1), \boldsymbol{m}_{wd}(p_{15}^2) \geq 0$$
$$-\sigma_{wd_1} + \boldsymbol{m}_{wd}(p_{15}^1) \geq 0 \quad (6)$$
$$-\sigma_{wd_2} + \boldsymbol{m}_{wd}(p_{15}^2) \geq 0$$
$$-\sigma_{wd_3} \geq -\boldsymbol{m}(p_{27})$$
$$\sigma_{wd_3} - \sigma_{wd_4} \geq -\boldsymbol{m}(p_{10})$$

$$\sigma_{wd_4} - \sigma_{wd_5} \geq -\boldsymbol{m}(p_9)$$
$$\boldsymbol{m}_{wd}(p_{15}^1) + \boldsymbol{m}_{wd}(p_{15}^2) = \boldsymbol{m}(p_{15})$$
$$\sigma_{wd_1} - \boldsymbol{m}_{wd}(p_{15}^1) \leq \boldsymbol{m}(p_5)$$
$$\sigma_{wd_2} - \boldsymbol{m}_{wd}(p_{15}^2) \leq \boldsymbol{m}(p_1)$$
$$\sigma_{wd_3}, \sigma_{wd_4}, \sigma_{wd_5} \leq \boldsymbol{m}(p_9) + \boldsymbol{m}(p_{10}) + \boldsymbol{m}(p_{27})$$

with variables $\sigma_{wd_1}, \sigma_{wd_2}, \sigma_{wd_3}, \sigma_{wd_4}, \sigma_{wd_5}, \boldsymbol{m}_{wd}(p_{15}^1),$ $\boldsymbol{m}_{wd}(p_{15}^2)$. Notice that the indexes i of the σ_{wd_i}'s refer to the numbers associated to the transitions in fig. 3d.

Equally, another LP problem has to be written in order to impose the constraint 5.1. Notice that $\mathcal{N}_{cs_1}$ and $\mathcal{N}_{cs_2}$ are BCFCNs, whereas the PN of fig. 2 is not backward conflict free.

REFERENCES

Bruce H. Krogh and Lawrence E. Holloway (1991). Synthesis of feedback control logic for discrete maufacturing systems. *Automatica* **27**(4), 641–651.

Desel, Jörg and Javier Esparza (1995). *Free Choice Petri nets*. number 40. Cambridge University Press Cambridge Tracts in Theoretical Computer Science.

Ghaffari, A., N. Rezg and X. Xie (2003). Feedback control logic for forbidden-state problems of marked graphs: Application to a real manufacturing system. *IEEE Trans. on Automatic Control* **48**(1), 18–29.

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

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

Moody, J.O. and P.J. Antsaklis (2000). Petri net supervisors for DES with uncontrollable and unobservable transitions. *IEEE Trans. on Automatic Control* **45**(3), 462–476.

Moody, John and Panos Antsaklis (1998). *Supervisory Control of Discrete Event System Using Petri Nets*. Kluwer Ac.

Murata, Tadao (1989). Petri nets: Properties, analysis and applications. *Proceedings of IEEE* **77**(4), 541–580.

P.J.Ramadge and W.M. Wonham (1989). The control of discrete event systems. *Proceedings of IEEE* **77**(1), 637–659.