A deadlock prevention method for railway networks using monitors for colored Petri nets*

Maria Pia Fanti
Dip. di Elettrotecnica ed Elettronica
Politecnico di Bari, Italy
fanti@deemail.poliba.it

Alessandro Giua, Carla Seatzu
Dip. di Ing. Elettrica ed Elettronica
Università di Cagliari, Italy
{giua,seatzu}@diee.unica.it

Abstract – *The real-time traffic control of railway networks authorizes movements of the trains and imposes safety constraints. The paper deals with the real time traffic control focusing on deadlock prevention problem. Colored Petri nets are used to model the dynamics of the railway network system: places represent tracks and stations, tokens are trains. The prevention policy is expressed by a set of linear inequality constraints, called colored Generalized Mutual Exclusion Constraints that are enforced by adding appropriate monitor places. Using digraph tools, deadlock situations are characterized and a strategy is established to define off-line a set of Generalized Mutual Exclusion Constraints that prevent deadlock. An example shows in detail the design of the proposed control logic.*

Keywords: Railway network system control, colored Petri nets, deadlock prevention.

1 Introduction

The traffic control of *Railway Network Systems* (RNS) is a critical task in modern railway transportation. The structure of the railway traffic planning and control can be divided in two main hierarchical levels [12]. The first level is the planning level that works off-line and constructs the traffic plan and timetable. The second control level makes decisions in real-time and it has two tasks. Firstly, this level analyzes perturbed situations. In particular, the goal of the controller is to reduce delays and to make traffic return to planned paths when trains have deviations from the scheduled timetable [11]. Secondly, the real-time controller has to impose the satisfaction of safeness constraints to avoid collisions and deadlocks.

This paper focuses on the second task of the real-time controller. The RNS is modelled with *colored Petri nets* (CPNs) [2, 10] that provide a powerful framework to the analysis and the definition of safeness constraints. In the related literature, railway networks are modelled as discrete event systems [1] that define a control design problem leading to a non-convex nonlinear optimization problem. Moreover, in [8] the railway network is modelled by a Petri net and deadlock avoidance constraints are expressed as *Generalized Mutual Exclusion Constraints* (GMEC). However, the controller does not distinguish among the routes assigned to the trains, and when forks and joins are present in the network the marking does not describe completely the system state.

This paper overcomes this problem by using CPN to model the RNS structure and dynamics. More precisely, places represent tracks and stations, while transitions are the control points where the train movements are enabled or inhibited. Moreover, the trains travelling in the system are represented by colored tokens and their color is the assigned path. To characterize deadlock situations we use some results obtained in the field of Automated Manufacturing Systems where deadlock has been widely studied [3, 4, 5, 6]. We characterize deadlock states by using digraph tools that describe the interactions between trains and resources (i.e., tracks and stations). In addition, a *deadlock prevention strategy* defines off-line the rules to prevent deadlock in advance. In this framework, deadlock and collision prevention constraints are expressed by a set of linear inequality constraints, called colored GMEC. A companion paper [7] rigorously defines colored GMEC and shows how the results obtained for GMEC applied to place/transition nets can be extended to colored Petri nets. Hence, the controller takes the form of a set of colored monitor places that can be automatically computed. An example shows the design technique of the proposed control logic.

2 The railway network system

A RNS consists of three fundamental elements: railway lines, stations, vehicles (i.e., trains, single engines, etc.) travelling over these lines.

Let us consider the set $V = \{v_1, \cdots, v_{N_V}\}$ that collects all the vehicles moving over the lines and the stations. The railway lines are divided into several tracks and each track can be occupied by only one vehicle at a time. In our framework, each station is described by a resource r_i, for $i = 1, \cdots, N_S$, where N_S is the number of stations. Moreover, each track of the RNS is viewed as a resource that vehicles can acquire and it is denoted by r_i, for $i = N_S + 1, \cdots, N_S + N_T$, where N_T is the overall number of tracks. Since each station is composed of one or more tracks, and each track can accommodate only one train at a time, a finite capacity $C(r_i) \geq 1$ is assigned to each station r_i, for $i = 1, \cdots, N_S$. Moreover, each track r_i has unit capacity, i.e., $C(r_i) = 1$ for all $i = N_S + 1, \cdots, N_S + N_T$.

We also assume that the terminal stations of the train paths are connected to a "virtual" *docking station* r_0. The docking station can accommodate all the trains in

*0-7803-7952-7/03/$17.00 © 2003 IEEE.

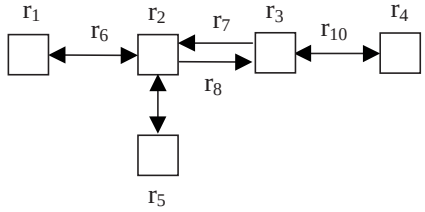

Figure 1: The railway network of Example 2.1.

the system, i.e., $C(r_0) = \infty$.

Finally, we generically call *resources* or *nodes* the stations and the tracks. Therefore, the set $R = \{r_i,\ i = 0, \cdots, N_S + N_T\}$ denotes the resource set of the system.

Other basic elements of the RNS are the control points where the trains are authorized to enter a generic node by the real-time traffic controller. In addition, a path (or route) π_k is assigned to each train $v_k \in V$ travelling in the system: each vehicle starts its travel from a station; it reaches a destination station and finally the docking station where a new path can be assigned to it. More precisely, each path is described by the following sequence of resources that ends at the docking station: $\pi_k = (r_{k_1}, \cdots, r_{k_{N_k}}, r_0)$. The set A collects all the possible paths planned in the system.

Example 2.1. Let us consider the railway composed by five stations r_i, for $i = 1, \cdots, 5$, depicted in Figure 1.

The first station is a three track station, while the remaining ones have only two tracks, i.e., $C(r_1) = 3$ and $C(r_i) = 2$ for $i = 2, 3, 4, 5$.

All intermediate tracks r_i, for $i = 6, 9, 10$, are single tracks, apart from r_7 and r_8 that represent two track segments. ■

This paper deals with the *real-time traffic control level* whose task is that of authorizing the movement of the trains and imposing safety constraints. Such a control can be applied to railway tracks and to station tracks, and its main goal is that of avoiding deadlock and collisions in all subsystems.

3 CPN and GMEC

In this section we provide some background on colored Petri nets and generalized mutual exclusion constraints. For more details we address the reader to the companion paper [7].

3.1 Overview of CPN

A *colored Petri net* (CPN) is a bipartite directed graph represented by a quintuple $N = (P, T, Co, \boldsymbol{Pre}, \boldsymbol{Post})$ where P is the set of places, T is the set of transitions, $Co : P \cup T \to \mathcal{C}l$ is a color function that associates to each element in $P \cup T$ a non empty ordered set of colors in the set of possible colors $\mathcal{C}l$.

Therefore, for all $p_i \in P$, $Co(p_i) = \{a_{i,1}, a_{i,2}, \cdots, a_{i,u_i}\} \subseteq \mathcal{C}l$ is the ordered set of possible colors of tokens in p_i, and u_i is the number of possible colors of tokens in p_i. Analogously, for all $t_j \in T$, $Co(t_j) = \{b_{j,1}, b_{j,2}, \cdots, b_{j,v_j}\} \subseteq \mathcal{C}l$ is the ordered set of possible occurrence colors of t_j, and v_j is the number of possible occurrence colors in t_j.

In the following we assume that $m = |P|$ and $n = |T|$.

Matrices $\boldsymbol{Pre}$ and $\boldsymbol{Post}$ are the pre-incidence and the post-incidence $m \times n$ dimensional matrices respectively. In particular, each element $\boldsymbol{Pre}(p_i, t_j)$ is a mapping from the set of occurrence colors of t_j to a non negative multiset[1] over the set of colors of p_i, namely, $\boldsymbol{Pre}(p_i, t_j) : Co(t_j) \to \mathcal{N}(Co(p_i))$, for $i = 1, \cdots, m$ and $j = 1, \cdots, n$. In the following we denote $\boldsymbol{Pre}(p_i, t_j)$ as a matrix of $u_i \times v_j$ non negative integers, whose generic element $Pre(p_i, t_j)(h, k)$ is equal to the weight of the arc from place p_i with respect to (wrt) color $a_{i,h}$ to transition t_j wrt color $b_{j,k}$.

Analogously, $\boldsymbol{Post}(p_i, t_j) : Co(t_j) \to \mathcal{N}(Co(p_i))$, for $i = 1, \cdots, m$ and $j = 1, \cdots, n$, and we denote $\boldsymbol{Post}(p_i, t_j)$ as a matrix of $u_i \times v_j$ non negative integers. The generic element $Post(p_i, t_j)(h, k)$ is equal to the weight of the arc from transition t_j wrt color $b_{j,k}$ to place p_i wrt color $a_{i,h}$.

The incidence matrix $\boldsymbol{C}$ is an $m \times n$ matrix, whose generic element $\boldsymbol{C}(p_i, t_j) : Co(t_j) \to \mathcal{Z}(Co(p_i))$, for $i = 1, \cdots, m$ and $j = 1, \cdots n$. In particular $\boldsymbol{C}(p_i, t_j) = \boldsymbol{Post}(p_i, t_j) - \boldsymbol{Pre}(p_i, t_j)$.

For each place $p_i \in P$, we define the *marking* $\boldsymbol{m}_i$ of p_i as a *non negative multiset* over $Co(p_i)$. The mapping $m_i : Co(p_i) \to \mathbb{N}$ associates to each possible token color in p_i a non negative integer representing the number of tokens of that color that is contained in place p_i, and $\boldsymbol{m}_i = \sum_{d \in Co(p_i)} m_i(d) \otimes d$.

In the following we denote $\boldsymbol{m}_i$ as a column vector of u_i non negative integers, whose h-th component $m_i(h)$ is equal to the number of tokens of color $a_{i,h}$ that are contained in p_i. The marking $\boldsymbol{M}$ of a CPN is an m-dimensional column vector of multisets, i.e., $\boldsymbol{M} = [\ \boldsymbol{m}_1 \ \cdots \ \boldsymbol{m}_m\ ]^T$. Finally, we denote $|\boldsymbol{M}| = \sum_{p_i \in P} |\boldsymbol{m}_i|$ the total number of tokens in the net at marking $\boldsymbol{M}$ regardless of their color.

A colored Petri net system $\langle N, \boldsymbol{M}_0 \rangle$ is a colored Petri net N with initial marking $\boldsymbol{M}_0$.

A transition $t_j \in T$ is *enabled* wrt color $b_{j,k}$ at a marking $\boldsymbol{M}$ if and only if for each place $p_i \in P$ and for all $h = 1, \cdots, u_i$, we have $m_i(h) \geq Pre(p_i, t_j)(h, k)$.

If an enabled transition t_j fires at $\boldsymbol{M}$ wrt color $b_{j,k}$, then we get a new marking $\boldsymbol{M'}$ where, for all $p_i \in P$ and for all $h = 1, \cdots, u_i$, $m'_i(h) = m_i(h) + Post(p_i, t_j)(h, k) - Pre(p_i, t_j)(h, k)$.

We will write $\boldsymbol{M}[t_j(k)\rangle \boldsymbol{M'}$ to denote that t fires at $\boldsymbol{M}$ wrt color $b_{j,k}$ yielding $\boldsymbol{M'}$.

3.2 GMEC and monitors

In the Petri nets framework a supervisory controller restricts the reachability set of the closed loop plant to a set of legal markings. In many applications, the set of legal markings is expressed by a set of linear inequality

[1] Let D be a set. A *multiset* (resp., *non negative multiset*) $\boldsymbol{\alpha}$ over D is defined by a mapping $\alpha : D \to \mathbb{Z}$ ($\alpha : D \to \mathbb{N}$) and may be represented as

$$\boldsymbol{\alpha} = \sum_{d \in D} \alpha(d) \otimes d$$

where the sum is limited to the elements such that $\alpha(d) \neq 0$.

Let $\mathcal{Z}(D)$ (resp., $\mathcal{N}(D)$) denote the set of all multisets (resp., non negative multisets) over D. The multiset $\boldsymbol{\varepsilon}$ is the empty multiset such that for all $d \in D$, $\varepsilon(d) = 0$.

constraints called *Generalized Mutual Exclusion Constraints* (GMEC). In [7] the notion of GMEC is extended to the case of colored Petri nets as follows.

Definition 3.1 ([7]). *A GMEC is a couple* $(\boldsymbol{W}, \boldsymbol{k})$ *where* $\boldsymbol{W} = [\ \boldsymbol{w}_1 \ \cdots \ \boldsymbol{w}_m\ ]$, $\boldsymbol{k} \in \mathcal{Z}(D)$, *for all* i, $\boldsymbol{w}_i : Co(p_i) \to \mathcal{Z}(D)$, *and* D *is a set of colors different from* $Co(p_i)$, $i = 1, \cdots, m$. *The set of legal markings defined by* $(\boldsymbol{W}, \boldsymbol{k})$ *can be written as*

$$\mathcal{M}(\boldsymbol{W}, \boldsymbol{k}) = \left\{ \boldsymbol{M} = \begin{bmatrix} \boldsymbol{m}_1 \\ \vdots \\ \boldsymbol{m}_m \end{bmatrix} \;\middle|\; \boldsymbol{m}_i \in \mathcal{N}(Co(p_i)), \; \boldsymbol{W} \circ \boldsymbol{M} \triangleq \sum_{i=1}^{m} \boldsymbol{w}_i \circ \boldsymbol{m}_i \leq \boldsymbol{k} \right\}. \quad (1)$$

■

Note that each term $\boldsymbol{w}_i \circ \boldsymbol{m}_i$ is a multiset that can be computed using the usual matrix algebra [7].

Moreover, as discussed in detail in [7], a GMEC can be enforced by adding a monitor place p_c and a systematic procedure can be used to compute the incidence matrix defining such a monitor place, as well as its initial marking.

Definition 3.2 ([7]). *Given a colored Petri net system* $\langle N_p, \boldsymbol{M}_{p,0} \rangle$, *with* $N_p = (P, T, Co, \boldsymbol{Pre}_p, \boldsymbol{Post}_p)$, *and a GMEC* $(\boldsymbol{W}, \boldsymbol{k})$ *with* $\boldsymbol{k} \in \mathcal{Z}(D)$, *the* monitor *that enforces this constraint is a new place* p_c *with* $Co(p_c) = D$, *to be added to* N_p. *The resulting system is denoted* $\langle N, \boldsymbol{M}_0 \rangle$, *with* $N = (P \cup \{p_c\}, T, Co, \boldsymbol{Pre}, \boldsymbol{Post})$. *Then* N *will have incidence matrix*

$$\boldsymbol{C} = \begin{bmatrix} \boldsymbol{C}_p \\ \boldsymbol{C}_c \end{bmatrix}, \quad \textit{where } \boldsymbol{C}_c = -\boldsymbol{W}^T \circ \boldsymbol{C}_p. \quad (2)$$

We are assuming that there are no selfloops containing p_c *in* N, *hence* $\boldsymbol{Pre}$ *and* $\boldsymbol{Post}$ *may be uniquely determined by* $\boldsymbol{C}$. *The initial marking of* $\langle N, \boldsymbol{M}_0 \rangle$ *is*

$$\boldsymbol{M}_0 = \begin{bmatrix} \boldsymbol{M}_{p,0} \\ \boldsymbol{m}_{c,0} \end{bmatrix}, \quad \textit{where } \boldsymbol{m}_{c,0} = \boldsymbol{k} - \boldsymbol{W}^T \circ \boldsymbol{M}_{p,0}. \quad (3)$$

We assume that the initial marking $\boldsymbol{M}_{p,0}$ *of the system satisfies the constraint* $(\boldsymbol{W}, \boldsymbol{k})$. ■

In the case of controllable and observable transitions we can prove the following result.

Theorem 3.3 ([7]). *Let* $\langle N_p, \boldsymbol{M}_{p,0} \rangle$ *be a CPN system, and* $(\boldsymbol{W}, \boldsymbol{k})$ *a colored GMEC. Let* $\langle N, \boldsymbol{M}_0 \rangle$ *be the system with the addition of the monitor place* p_c. *The monitor place* p_c *enforces the GMEC* $(\boldsymbol{W}, \boldsymbol{k})$ *when included in the closed loop system* $\langle N, \boldsymbol{M}_0 \rangle$. *The monitor place* p_c *minimally restricts the behavior of the closed loop system* $\langle N, \boldsymbol{M}_0 \rangle$, *in the sense that it prevents only transition firings that yield forbidden markings.* □

4 The CPN model of the RNS

In this paper we use colored Petri nets to model RNS. In particular, places represent resources (stations and tracks), while the firing of transitions represent the flow of vehicles into the system.

The generic place $p_i \in P$ models resource $r_i \in R$ and there is a one to one relationship between resources and places, thus in the following we always refer to P as R (and to p_i as r_i). Moreover, if there exists a link that goes from node r_h to node r_i, then in the CPN we introduce a transition t_j such that $t_j \in r_h{}^\bullet$ and $t_j \in {}^\bullet r_i$ [2]. Note that each transition represents a control point where the controller can stop the trains or can authorize a train to move on. Thus all transitions in the CPN model are assumed to be both controllable and observable.

A colored token in a place represents a vehicle in a resource. The color of each token specifies the vehicle v_k or, equivalently, the routing π_k assigned to the train. As an example, $\pi_k = (r_h, \cdots, r_q, r_0)$ can be the path (i.e. the sequence of resources) assigned to the train v_k. Hence, for each $r_i \in R$ we have $Co(r_i) = \{\pi_k \mid \pi_k \text{ contains } r_i\}$, and for each $t_j \in T$ such that $t_j \in r_h{}^\bullet$ and $t_j \in {}^\bullet r_i$, we have $Co(t_j) = \{\pi_k \mid \pi_k \text{ contains } r_h \text{ and } r_i \text{ in strict succession order}\}$.

Example 4.1. Let us consider the RNS described in Example 2.1. The corresponding CPN model is reported in Figure 2 where place r_0 represents the docking station.

Let us assume that four trains are travelling in the system, namely, v_1, v_2, v_3 and v_4. Moreover, let $\pi_1 = (r_1, r_6, r_2, r_7, r_3, r_9, r_4, r_0)$, $\pi_2 = (r_4, r_9, r_3, r_8, r_2, r_6, r_1, r_0)$, $\pi_3 = (r_1, r_6, r_2, r_{10}, r_5, r_0)$, $\pi_4 = (r_5, r_{10}, r_2, r_6, r_1, r_0)$.

Therefore, by definition $Co(r_1) = \{\pi_1, \pi_2, \pi_3, \pi_4\}$ for $i = 0, 1, 2, 6$, $Co(r_i) = \{\pi_1, \pi_2\}$ for $i = 3, 4, 9$, $Co(r_7) = \{\pi_1\}$, $Co(r_8) = \{\pi_2\}$, $Co(r_i) = \{\pi_3, \pi_4\}$ for $i = 5, 10$, and $Co(t_j) = \{\pi_1, \pi_3\}$ for $j = 1, 2, 19$, $Co(t_j) = \{\pi_2, \pi_4\}$ for $j = 13, 14, 22$, $Co(t_j) = \{\pi_3\}$ for $j = 3, 4, 17$, $Co(t_j) = \{\pi_4\}$ for $j = 15, 16, 20$, $Co(t_j) = \{\pi_1\}$ for $j = 5, 6, 7, 8, 18$, $Co(t_j) = \{\pi_2\}$ for $j = 9, 10, 11, 12, 21$.

The pre and post-incidence matrices can be easily deduced by looking at the structure of the net and at the above paths definition. As an example

$$\boldsymbol{Pre}(r_1, t_1) = \boldsymbol{Post}(r_6, t_1) = \begin{matrix} \\ \pi_1 \\ \pi_2 \\ \pi_3 \\ \pi_4 \end{matrix} \begin{matrix} \begin{matrix} \pi_1 & \pi_3 \end{matrix} \\ \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \end{matrix}$$

Now, let us assume that initially trains v_1 and v_3 are in r_1, train v_2 is in r_4 and train v_4 is in r_5. Thus the CPN system is initially at marking

$$\boldsymbol{M}_{p,0} = \begin{bmatrix} \boldsymbol{m}_{0,0} \\ \boldsymbol{m}_{1,0} \\ \boldsymbol{m}_{2,0} \\ \boldsymbol{m}_{3,0} \\ \boldsymbol{m}_{4,0} \\ \boldsymbol{m}_{5,0} \\ \boldsymbol{m}_{6,0} \\ \vdots \\ \boldsymbol{m}_{10,0} \end{bmatrix} = \begin{bmatrix} \boldsymbol{\varepsilon} \\ 1 \otimes \pi_1 + 1 \otimes \pi_3 \\ \boldsymbol{\varepsilon} \\ \boldsymbol{\varepsilon} \\ 1 \otimes \pi_2 \\ 1 \otimes \pi_4 \\ \boldsymbol{\varepsilon} \\ \vdots \\ \boldsymbol{\varepsilon} \end{bmatrix}.$$

Using the matrix notation, each term $\boldsymbol{m}_{i,0}$ may be written as a column vector of dimension $|Co(r_i)|$. As an

[2] Given a node $x \in P \cup T$ we denote as ${}^\bullet x$ and $x^\bullet$ the preset and the postset of x, respectively.

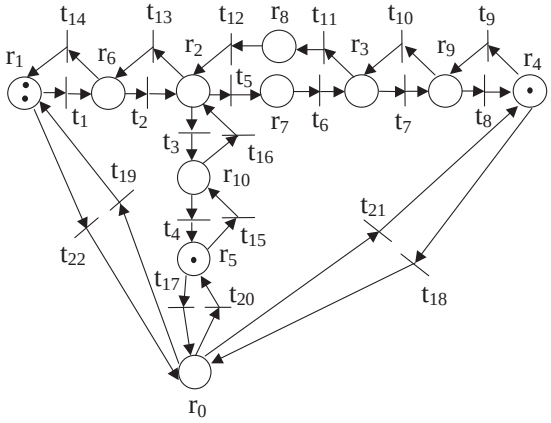

Figure 2: The CPN model of the RNS in Figure 1.

example,

$$\boldsymbol{m}_{1,0} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \begin{matrix} \pi_1 \\ \pi_2 \\ \pi_3 \\ \pi_4 \end{matrix}, \quad \boldsymbol{m}_{4,0} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{matrix} \pi_1 \\ \pi_2 \end{matrix}$$

■

4.1 Capacity constraints

As already said before, all tracks and stations have a finite capacity, apart from the docking station r_0 that is a dummy node. To ensure that each resource does not accommodate a number of trains that is greater than the corresponding capacity, we have to introduce appropriate *capacity constraints*. More precisely, for all $r_i \in R \setminus \{r_0\}$, with $i = 1, \cdots, m$, we have to impose that

$$\sum_{h=1}^{u_i} m_i(\pi_{j_h}) \leq C(r_i)$$

where $Co(r_i) = \{\pi_{j_1}, \cdots, \pi_{j_{u_i}}\}$ and $u_i = |Co(r_i)|$.

The capacity constraints may be rewritten in terms of a single GMEC $(\boldsymbol{W}, \boldsymbol{k})$, that we call *capacity GMEC*. The capacity GMEC will have as color set $D = \{z_1, \cdots, z_m\}$ because we need m capacity constraints, and is defined as follows:

$$\boldsymbol{W} = [\ \boldsymbol{w}_0 \quad \boldsymbol{w}_1 \quad \cdots \quad \boldsymbol{w}_m\ ],$$

$$\boldsymbol{w}_0 = \boldsymbol{\varepsilon}$$

$$\boldsymbol{w}_i = \begin{matrix} \pi_{j_1} & \cdots & \pi_{j_{u_i}} \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix}$$
$$\begin{bmatrix} 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \end{bmatrix} \begin{matrix} z_1 \\ \vdots \\ z_{i-1} \\ z_i \\ z_{i+1} \\ \vdots \\ z_m \end{matrix} \qquad i = 1, \cdots, m$$

$$\boldsymbol{k} = [\ C(r_1) \quad \cdots \quad C(r_m)\ ]^T \in \mathcal{Z}(D). \tag{4}$$

Using the above theory, an appropriate monitor place can be added to the open loop net so as to ensure the satisfaction of the capacity constraints.

Example 4.2. Let us consider again the CPN system in Example 4.1 associated to the RNS described in Example 2.1.

In such a case we have $m = 10$ and

$$\boldsymbol{k} = [\ 3 \quad 2 \quad 2 \quad 2 \quad 2 \quad 1 \quad 2 \quad 2 \quad 1 \quad 1\ ]^T.$$

The incidence matrix of the monitor place is equal to

$$\boldsymbol{C}_c = -\boldsymbol{W} \circ \boldsymbol{C}_p$$

where $\boldsymbol{C}_p$ is the incidence matrix of the open loop net. The incidence matrix of p_c has the following structure,

$$\boldsymbol{C}_c = [\ \boldsymbol{C}_c(p_c, t_1) \quad \cdots \quad \boldsymbol{C}_c(p_c, t_{15})\ ].$$

As an example,

$$\boldsymbol{C}_c(p_c, t_1) = \begin{matrix} \pi_1 & \pi_3 \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix}$$
$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ -1 & -1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{matrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ z_7 \\ z_8 \\ z_9 \\ z_{10} \end{matrix}$$

while all the other matrices $\boldsymbol{C}_c(p_c, t_j)$, $j = 2, \cdots, 15$, are omitted here for sake of brevity.

Finally, the monitor place p_c is initialized at marking

$$\boldsymbol{m}_{c,0} = [\ 1 \quad 2 \quad 2 \quad 1 \quad 1 \quad 1 \quad 2 \quad 2 \quad 1 \quad 1\ ]^T.$$

■

5 Deadlock prevention policy

In this section we first provide some background on digraph theory. Then we show how some theoretical results firstly obtained in the context of deadlock avoidance in Automated Manufacturing Systems [5, 6], can be used here to derive a deadlock prevention policy.

5.1 Basic definitions

A *digraph* is a couple $D = (N, E)$ where N is the set of vertices and E is the set of edges [9].

A *path* is a subdigraph of D composed by an alternating sequence of distinct vertices and arcs. If D contains a path from r_i to r_j, then r_j is said *reachable* from r_i. Moreover, if r_j (r_i) is reachable from r_i (r_j), then r_i and r_j are said *mutually reachable*. A *cycle* of D is a nontrivial path in which all vertices are distinct except the first and the last one[3].

A subdigraph $D_\mu = (N_\mu, E_\mu)$ of D is called *strong* if every two vertices of N_μ are mutually reachable. Finally, a *strong component* of D is a maximal strong subdigraph, i.e., a strong subdigraph that is not contained in any other strong subdigraph of D.

Let us finally introduce a relation that is based on the order in which the resources in a RNS are used.

[3]What we call *cycle* is sometimes called *elementary cycle*.

Definition 5.1. *A resource r_j immediately follows a resource r_i with respect to path π_k if $\pi_k = (\cdots, r_i, r_j \cdots)$. This is also denoted $r_i \rhd_k r_j$.* ■

5.2 Deadlock characterization

Given a CPN describing a RNS, a deadlock corresponds to a marking from which all transitions enabled in the plant are disabled by the capacity GMEC: such a marking is said *deadlock marking*.

In this section we establish some necessary and sufficient conditions for deadlock occurrence based on the analysis of the digraphs associated to a colored Petri net. Note that these results only apply to a CPN representing a RNS as described in Section 4. In the following however, for sake of simplicity, we will omit to precise this in the statement of all results simply referring to a CPN: we will also talk of places as resources, trains as colored tokens, etc.

We can now define two digraphs associated to a RNS represented by a CPN.

Definition 5.2. *Given a colored Petri net $N_p = (R, T, Co, \boldsymbol{Pre}, \boldsymbol{Post})$ we may associate to it two main digraphs.*

- *The* route digraph $D_R = (N_R, E_R)$ *describes the paths of all the trains travelling in the system. Each vertex in this graph represents a resource, i.e., $N_R = R$ while $E_R = \{e_{ij} \mid (\exists \pi_k \in A)\ r_i \rhd_k r_j\}$, i.e., an edge $e_{i,j}$ belongs to E_R if there exists a path where r_j follows r_i.*
- *The* transition digraph $D_T(\boldsymbol{M}_p) = (N_R, E_T(\boldsymbol{M}_p))$, *describes the interactions between trains and resources when the actual marking is $\boldsymbol{M}_p$. Each vertex in this graph still represents a resource as in the route digraph, i.e., $N_R = R$, while*

  $$E_T(\boldsymbol{M}_p) = \{e_{ij} \mid (\exists \pi_k \in A)\boldsymbol{m}_i \geq 1 \otimes \pi_k,\ r_i \rhd_k r_j\},$$

  i.e., an edge $e_{i,j}$ belongs to $E_T(\boldsymbol{M}_p)$ if there exists a train in resource r_i at marking $\boldsymbol{M}_p$ and r_j is the next resource the train has to acquire. ■

Obviously, the arc set of the transition digraph changes as the marking is updated.

Example 5.3. Figure 3 shows digraph D_R corresponding to the system and the CPN described in Examples 2.1 and 4.1. Each edge of D_R is labelled with the name of the path to which it correspond. Moreover, for sake of simplicity, the node r_0 is repeated in Figure 3.

Assume that the four trains travelling in the system are in these positions: v_1 in r_6, v_2 and v_3 in r_2, and v_4 in r_{10}. Hence, the CPN is at marking $\boldsymbol{M}_p$ equal to $\boldsymbol{m}_6 = 1 \otimes \pi_1$, $\boldsymbol{m}_2 = 1 \otimes \pi_2 + 1 \otimes \pi_3$, $\boldsymbol{m}_{10} = 1 \otimes \pi_4$, $\boldsymbol{m}_i = \boldsymbol{\varepsilon}$ elsewhere.

The corresponding transition digraph $D_T(\boldsymbol{M}_p)$ is shown in Figure 4. ■

To characterize deadlock markings we also need the following definition.

Definition 5.4. *A strong component $D_\mu = (N_\mu, E_\mu)$ of $D_T(\boldsymbol{M}_p)$is called a* Maximal-weight Zero-outdegree Strong Component *(MZSC for brevity) if the following properties hold true:*

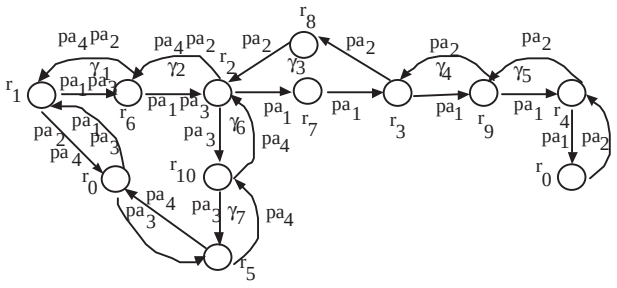

Figure 3: Digraph D_R for Example 5.3.

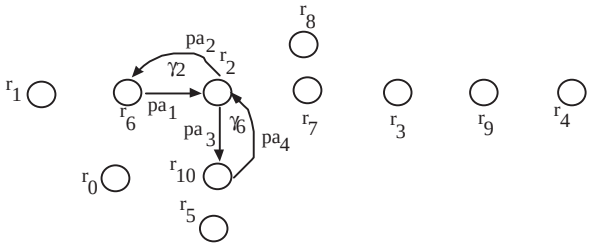

Figure 4: Digraph $D_T(\boldsymbol{M}_p)$ for Example 5.3.

(a) Maximal-weight*: all the resources from N_μ are busy, i.e., the number of tokens in each place r_i is equal to the maximal capacity of the place: $|\boldsymbol{m}_i| = C(r_i)$.*

(b) Zero-outdegree*: all the edges of $D_T(\boldsymbol{M}_p)$ outgoing from vertices of N_μ belong to E_μ.*

■

Remark 5.5. *Note that the node r_0 corresponding to the docking station can not be in a MZSC because it has an infinite capacity and all cycles containing it may be disregarded for deadlock analysis.*

It is possible to give a simple characterization of an MZSC in terms of resources allocated to the trains at a given marking.

Definition 5.6. *Given a strong subdigraph $D_\mu = (N_\mu, E_\mu)$ of D_R and a marking $\boldsymbol{M}_p$, we denote the set of trains that occupy a resource of N_μ and require a resource of N_μ at next step as*

$$V(\boldsymbol{M}_p)_\mu = \{v_k \in V \mid (\exists r_i, r_j \in N_\mu)\ \boldsymbol{m}_i \geq 1 \otimes \pi_k, \quad r_i \rhd_k r_j,\ e_{i,j} \in E_\mu\}.$$

■

The following result holds.

Proposition 5.7. *A necessary condition for a strong subdigraph $D_\mu = (N_\mu, E_\mu)$ of D_R to be an MZSC in $D_T(\boldsymbol{M}_p)$ is that $|V(\boldsymbol{M}_p)_\mu| = C(N_\mu)$ where $C(N_\mu) = \sum_{r_i \in N_\mu} C(r_i)$ is the sum of the capacities of the resources in N_μ.*

Proof. First we observe that if D_μ is a MZSC then (by the maximal-weight condition) the number of tokens in

N_μ at $\boldsymbol{M}_p$ is equal to $\sum_{r_i \in N_\mu} |\boldsymbol{m}_i| = \sum_{r_i \in N_\mu} C(r_i) = C(N_\mu)$. Furthermore, each of these tokens corresponds to a train in the set of resources N_μ that (by the zero-outdegree condition) requires at the next step a resource in N_μ, i.e., $C(N_\mu) = |V(\boldsymbol{M}_p)_\mu|$. □

In [5] and [6] necessary and sufficient conditions for deadlock occurrence have been characterized in terms of digraph analysis.

Proposition 5.8. *A marking $\boldsymbol{M} = [\boldsymbol{M}_p^T \ \boldsymbol{m}_c]^T$ is a deadlock marking for a CPN with capacity constraint iff there exists at least one MZSC in $D_T(\boldsymbol{M}_p)$.*

Proof. The statement is a slightly different formulation of Theorem 1 from [5] in terms of net marking rather that system state. As such, it applies to CPN modelling RNS. □

From proposition 5.7 and Proposition 5.8, the following Corollary is derived.

Corollary 5.9. *If $\boldsymbol{M} = [\boldsymbol{M}_p^T \ \boldsymbol{m}_c]^T$ is a deadlock marking for a CPN with capacity constraint, then there exists a strong component $D_\mu = (N_\mu, E_\mu)$ of D_R such that $|V(\boldsymbol{M}_p)_\mu| = C(N_\mu)$.* □

Example 5.10. Let us consider again Example 5.3 and the transition digraph $D_T(\boldsymbol{M}_p)$ in Figure 4 corresponding to the defined marking $\boldsymbol{M}_p$. It is easy to verify that the strong component $D_\mu = \gamma_2 \cup \gamma_6 = (\{r_6, r_2, r_{10}\}, \{e_{6,2}, e_{2,10}, e_{10,2}, e_{2,6}\})$ of D_R is an MZSC in $D_T(\boldsymbol{M}_p)$. Moreover, we obtain: $V(\boldsymbol{M}_p)_\mu = \{v_1, v_2, v_3, v_4\}$, and $|V(\boldsymbol{M}_p)_\mu| = C(N_\mu) = 4$. ■

5.3 Second level deadlocks

By imposing constraints of the form $|V(\boldsymbol{M}_p)_\mu| \leq C(N_\mu) - 1$ we can prevent any strong component of D_R from becoming an MZSC in the transition digraph.

However, avoiding a deadlock marking is not sufficient to guarantee the liveness of the CPN. Indeed, it is possible that some critical states are reached that are not deadlocks, but they necessary evolve to a deadlock marking in the next step: these states are called *Second Level Deadlocks* (SLD) [5]. Clearly, if a SLD marking is reached, then a controller that has been designed to prevent reaching a deadlock marking for the original net will create a new deadlock marking.

We discuss in this subsection how it may be possible to also prevent a SLD.

A SLD can be characterized in terms of a particular interaction among the cycles of D_R that can be represented by a new digraph.

Definition 5.11. *Given a colored Petri net with route digraph $D_R = (N_R, E_R)$ we define the* second level digraph *$D_R^2 = (N^2, E_R^2)$ such that:*

- *the set of vertices $N^2 = \{\gamma_1, \gamma_2, \cdots, \gamma_N\}$ is equal to the set of cycles of D_R that do not contain the dummy node[4] r_0;*
- *an edge $e_{u,s}$ belongs to E_R^2 if:*

[4]The dummy node r_0 has infinity capacity and all cycles containing it may be disregarded for deadlock analysis as mentioned in remark 5.5.

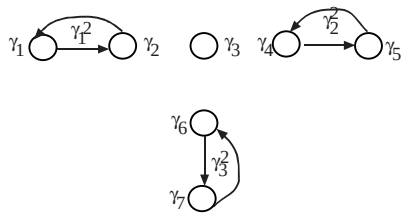

Figure 5: Digraph D_R^2 obtained from digraph D_R in Figure 3.

  i) γ_u and γ_s have only one vertex in common (say r_j) with capacity $C(r_j) = 1$;
  ii) there exists a path $\pi_k \in A$ such that $r_i \rhd_k r_j \rhd_k r_h$ requiring resources r_i, r_j, r_h in strict order of succession, with $e_{i,j} \in \gamma_u$ and $e_{j,h} \in \gamma_s$. ■

Now let γ_u^2 be a cycle in D_R^2 (second level cycle). From the previous definitions it follows that a subset of cycles of D_R (say Γ_u) is associated with vertices of γ_u^2. So, the capacity of γ_u^2 can be defined as

$$C(\gamma_u^2) = \sum_{r \in \{\gamma \ | \ \gamma \in \Gamma_u\}} C(r)$$

i.e., as the sum of the capacities of all the resources in Γ_u.

Finally, let Γ^2 indicate the subset of cycles of D_R^2, enjoying the following property: $\gamma_u^2 \in \Gamma^2$ iff the corresponding set Γ_u collects cycles that are all disjoint except for one vertex of unit capacity, common to all of them.

For each $\gamma_u^2 \in \Gamma^2$ and for each marking $\boldsymbol{M}_p$ we introduce the following set: $V(\boldsymbol{M}_p)_{\gamma_u^2} = \{v_k \in V \ | \$ at marking $\boldsymbol{M}_p$ the token representing v_k is in $r \in \Gamma_u\}$.

As shown by the following proposition easily derived from the results proved in [5], the set Γ^2 plays an important role in defining SLD conditions.

Proposition 5.12. *If $\boldsymbol{M} = [\boldsymbol{M}_p^T \ \boldsymbol{m}_c]^T$ is a SLD marking for a CPN with capacity constraint, then there exists in D_R^2 a* second level cycle *$\gamma_u^2 \in \Gamma^2$ such that: $|V(\boldsymbol{M}_p)_{\gamma_u^2}| = C(\gamma_u^2) - 1$.* □

Example 5.13. Considering the cycles of D_R depicted in Figure 3, the second level cycles of D_R^2 are derived and shown in Figure 5.

We suppose that the four trains in the system are in the following state: v_1 and v_2 are in r_5 with $\pi_1 = \pi_2 = (r_5, r_{10}, r_2, r_6, r_1, r_0)$, v_3 and v_4 are in r_2 with $\pi_3 = \pi_4 = (r_1, r_6, r_2, r_{10}, r_5, r_0)$. Hence, the CPN is at marking $\boldsymbol{M}_p$ where $\boldsymbol{m}_2 = 2 \otimes \pi_3$, $\boldsymbol{m}_5 = 2 \otimes \pi_4$, and $\boldsymbol{m}_i = \boldsymbol{\varepsilon}$ elsewhere. The solid lines in Figure 6 depicts the transition digraph $D_T(\boldsymbol{M}_p)$. For convenience, Figure 7 also depicts the second transitions (dashed lines) in the residual paths of the trains.

The described marking exhibits a SLD for the CPN. Indeed, the second level cycle $\gamma_3^2 \in \Gamma^2$ is in second level deadlock condition, were γ_3^2 corresponds to the cycle set $\Gamma_u = \gamma_6 \cup \gamma_7 = (\{r_2, r_{10}, r_5\}, \{e_{2,10}, e_{10,5}, e_{5,10}, e_{10,2}\})$.

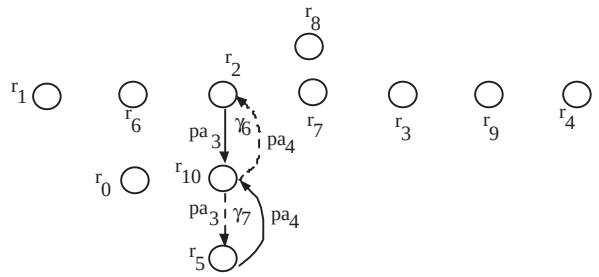

Figure 6: Digraph $D_T(\boldsymbol{M}_p)$ for Example 5.13.

Hence, the necessary condition of Proposition 5.12 is verified, i.e., $|V(\boldsymbol{M}_p)_{\gamma_3^2}| = |\{v_1, v_2, v_3, v_4\}| = C(\gamma_3^2) - 1 = 4$. ■

5.4 Deadlock prevention

Corollary 5.9 and Proposition 5.12 establish the deadlock and SLD prevention conditions on the marking of the CPN. To establish a direct relation among $|V(\boldsymbol{M}_p)_\mu|$, where $D_\mu = (N_\mu, E_\mu)$ is a strong subdigraph of D_R, and the marking of the CPN, the following index set is defined:

$$H_\mu(r_i) = \{h \mid \quad a_{i,h} \in Co(r_i) \cap Co(r_k) \text{ with } e_{i,k} \in E_\mu \text{ and } r_k \in N_\mu \text{ for each } r_i \in N_\mu\}.$$

A controller will prevent reaching a deadlock or a SLD marking if it can enforce the following *deadlock prevention GMEC*:

- for each strong subdigraph D_μ of D_R

$$|V(\boldsymbol{M}_p)_\mu| = \sum_{r_i \in N_\mu} \sum_{h \in H_\mu(r_i)} \boldsymbol{m}_i(h) \leq C(N_\mu) - 1 \tag{5}$$

- for each $\gamma_u^2 \in \Gamma^2$ of D_R^2

$$|V(\boldsymbol{M}_p)_{\gamma_u^2}| = \sum_{r_i \in N_{\Gamma_u}} |\boldsymbol{m}_i| \leq C(\gamma_u^2) - 2. \tag{6}$$

Note that being the number of trains in the system always limited (say $N_{\max}$) it may happen that some of the constraints (5) and (6) are trivially verified because $N_{\max} \leq C(N_\mu) - 1$ or $N_{\max} \leq C(\gamma_u^2) - 2$. Obviously, the deadlock prevention strategy can be simplified by neglecting such constraints.

The GMEC given by Equations (5) and (6) restrict the reachability set of the closed loop plant, to avoid deadlock and SLD. However, the imposed GMEC can eventually lead to a situation similar to a deadlock, which is known as *restricted deadlock* (RD) because the constraint for SLD may create in turn higher level deadlocks. The following proposition establishes the conditions that must be verified to obtain a RD free closed loop system.

Proposition 5.14. *If $\boldsymbol{M} = [\boldsymbol{M}_p^T \ \boldsymbol{m}_c]^T$ is a RD marking for a CPN with capacity constraint, then one of the following two conditions are verified: a) there exist at least two cycle sets Γ_1 and Γ_2 of D_R corresponding to the cycles $\gamma_1^2, \gamma_2^2 \in \Gamma^2$ such that $|V(\boldsymbol{M}_p)_{\gamma_1^2}| = C(\gamma_1^2) - 2$ and $|V(\boldsymbol{M}_p)_{\gamma_2^2}| = C(\gamma_2^2) - 2$; b) there exists at least a cycle set Γ_1 of D_R corresponding to $\gamma_1^2 \in \Gamma^2$ and a cycle γ_1 of D_R such $|V(\boldsymbol{M}_p)_{\gamma_1^2}| = C(\gamma_1^2) - 2$ and $|V(\boldsymbol{M}_p)_{\gamma_1}| = C(\gamma_1) - 1$.*

Proof. If $\boldsymbol{M}_p$ is a RD marking of the closed loop system, the restricted deadlock is not determined by the GMEC in Equation (5) because $\boldsymbol{M}_p$ is not a SLD marking. Hence, one of the following conditions is verified.

a) There exist at least two constraints defined by Equation (6) that determine the RD marking, say $|V(\boldsymbol{M}_p)_{\gamma_1^2}| < C(\gamma_1^2) - 2$ and $|V(\boldsymbol{M}_p)_{\gamma_2^2}| < C(\gamma_2^2) - 2$. More precisely there is a transition t_j that is disabled by the constraint $|V(\boldsymbol{M}_p)_{\gamma_1^2|}| < C(\gamma_1^2) - 2$ and a transition $t_{j'}$ that is disabled by the constraint $|V(\boldsymbol{M}_p)_{\gamma_2^2}| < C(\gamma_2^2) - 2$. Hence, there exists an edge $e_{v,q} \in E_R$, corresponding to transition t_j, such that $r_v \notin \Gamma_1$ and $r_q \in \Gamma_1$, and $|V(\boldsymbol{M}_p)_{\gamma_1^2}| = C(\gamma_1^2) - 2$. Analogously, there exists an edge $e_{i,m} \in E_R$, corresponding to transition $t_{j'}$, such that $r_i \notin \Gamma_2$ and $r_m \in \Gamma_2$, and $|V(\boldsymbol{M}_p)_{\gamma_2^2}| = C(\gamma_2^2) - 2$. This proves the first condition.

b) There exists at least one constraint defined by Equation (6) (say $|V(\boldsymbol{M}_p)_{\gamma_1^2}| < C(\gamma_1^2) - 2$) and one constraint defined by Equation (5) (say $|V(\boldsymbol{M}_p)_{\gamma_1}| < C(\gamma_1) - 1$) that cause the RD marking. More precisely there is a transition t_j that is disabled by the constraint $|V(\boldsymbol{M}_p)_{\gamma_1^2}| < C(\gamma_1^2) - 2$ and a transition $t_{j'}$ that is disabled by the constraint $|V(\boldsymbol{M}_p)_{\gamma_1}| < C(\gamma_1) - 1$. Hence, there exists an edge $e_{v,q} \in E_R$, corresponding to transition t_j, such that $r_v \notin \Gamma_1$ and $r_q \in \Gamma_1$, and $|V(\boldsymbol{M}_p)_{\gamma_1^2}| = C(\gamma_1^2) - 2$. Analogously, there exists an edge $e_{i,m} \in E_R$, corresponding to transition $t_{j'}$, such that $r_i \notin \gamma_1$ and $r_m \in \gamma_1$, and $|V(\boldsymbol{M}_p)_{\gamma_1}| = C(\gamma_1) - 1$. This proves the second condition. □

We define the following parameters:

$$C_1 = \min_{\gamma_i^2, \gamma_j^2 \in \Gamma^2, i \neq j} \left\{C(\gamma_i^2) - 2 + C(\gamma_j^2) - 2\right\},$$

$$C_2 = \min_{\gamma_i^2 \in \Gamma^2, \gamma_j \in D_R} \left\{C(\gamma_i^2) - 2 + C(\gamma_j) - 1\right\},$$

while $C_0 = \min\{C_1, C_2\}$.

Corollary 5.15. *If $|\boldsymbol{M}_{p,0}| < C_0$, the closed loop system with the monitors that enforce the deadlock prevention GMEC in Equations (5) and (6) is deadlock free.*

Proof. Follows from Proposition 5.14, because $\boldsymbol{M}_{p,0}$ is not a RD marking.

The following example enlightens the proposed prevention strategy.

Example 5.16. Let us consider again the CPN in Figure 2.

To obtain the deadlock prevention GMEC, we have to determine the sets $V(\boldsymbol{M}_p)_{\gamma_v}$ associated with cycle γ_v with $v = 1, \cdots, 7$, the set $V(\boldsymbol{M}_p)_\mu$ associated with the strong component $D_\mu = \gamma_2 \cup \gamma_6 =$

$(\{r_6, r_2, r_{10}\}, \{e_{6,2}, e_{2,10}, e_{10,2}, e_{2,6}\})$ of D_R (see Figure 3) and the sets $V(\boldsymbol{M}_p)_{\gamma_u^2}$ with $u = 1, \cdots, 3$ associated with the second level cycles $\gamma_u^2 \in \Gamma^2$ of D_R^2 with $u = 2, 3$. Considering the previously defined sets, the following conditions are imposed by the prevention policy. Note that we suppose four trains in the system, and we do not consider the always-verified constraints (for example the constraint $|V(\boldsymbol{M}_p)_{\gamma_1^2}| \leq 4$).

$$\begin{cases} |V(\boldsymbol{M}_p)_{\gamma_1}| \leq 3 & m_1(\pi_1) + m_1(\pi_3) + \\ & m_6(\pi_2) + m_6(\pi_4) \leq 3 \quad (1) \\ |V(\boldsymbol{M}_p)_{\gamma_2}| \leq 2 & m_2(\pi_2) + m_2(\pi_4) + \\ & m_6(\pi_1) + m_6(\pi_3) \leq 2 \quad (2) \\ |V(\boldsymbol{M}_p)_{\gamma_4}| \leq 2 & m_3(\pi_1) + m_9(\pi_2) \leq 2 \quad (3) \\ |V(\boldsymbol{M}_p)_{\gamma_5}| \leq 2 & m_4(\pi_2) + m_9(\pi_1) \leq 2 \quad (4) \\ |V(\boldsymbol{M}_p)_{\gamma_6}| \leq 2 & m_2(\pi_3) + m_{10}(\pi_2) \leq 2 \quad (5) \\ |V(\boldsymbol{M}_p)_{\gamma_7}| \leq 2 & m_5(\pi_2) + m_{10}(\pi_1) \leq 2 \quad (6) \\ |V(\boldsymbol{M}_p)_{\gamma_2 \cup \gamma_6}| \leq 3 & m_2(\pi_2) + +m_2(\pi_3) + \\ & m_2(\pi_4) + m_6(\pi_1) + \\ & m_6(\pi_3) + m_{10}(\pi_2) \leq 3 \quad (7) \\ |V(\boldsymbol{M}_p)_{\gamma_2^2}| \leq 3 & m_3(\pi_1) + m_3(\pi_2) + \\ & m_4(\pi_1) + m_4(\pi_2) \\ & + m_9(\pi_1) + m_9(\pi_2) \leq 3 \quad (8) \\ |V(\boldsymbol{M}_p)_{\gamma_3^2}| \leq 3 & m_2(\pi_1) + m_2(\pi_2) + \\ & m_2(\pi_3) + m_2(\pi_4) + \\ & m_5(\pi_1) + m_5(\pi_2) + \\ & m_{10}(\pi_1) + m_{10}(\pi_2) \leq 3 \quad (9) \end{cases}$$

Moreover, we obtain $C_0 = \min\{6, 5\} = 5$. Since the initial marking is such that $|\boldsymbol{M}_{p,0}| < C_0$, the resulting closed loop system is deadlock and RD free.

The above 9 constraints can be rewritten in terms of a single GMEC $(\boldsymbol{W}', \boldsymbol{k}')$, that we call *deadlock prevention GMEC*. The deadlock prevention GMEC will have as color set $D' = \{z_1', \cdots, z_9'\}$ because we have to impose 9 constraints, and is defined as follows:

$$\boldsymbol{W}' = [\ \boldsymbol{w}_0' \quad \boldsymbol{w}_1' \quad \cdots \quad \boldsymbol{w}_{10}'\ ]$$

$$\boldsymbol{w}_0' = \boldsymbol{\varepsilon}$$

$$\boldsymbol{k}' = [\ 3 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 3 \quad 3 \quad 3\ ]^T \in \mathcal{Z}(D').$$

As an example, we report here the numerical values of $\boldsymbol{w}_2'$ and $\boldsymbol{w}_3'$, while the other $\boldsymbol{w}_i'$'s are omitted for sake of brevity:

$$\boldsymbol{w}_2' = \begin{array}{c} \begin{matrix} \pi_1 & \pi_2 & \pi_3 & \pi_4 \end{matrix} \\ \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \end{array} \begin{matrix} z_1' \\ z_2' \\ z_3' \\ z_4' \\ z_5' \\ z_6' \\ z_7' \\ z_8' \\ z_9' \end{matrix} \qquad \boldsymbol{w}_3' = \begin{array}{c} \begin{matrix} \pi_1 & \pi_2 \end{matrix} \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 1 \\ 0 & 0 \end{bmatrix} \end{array} \begin{matrix} z_1' \\ z_2' \\ z_3' \\ z_4' \\ z_5' \\ z_6' \\ z_7' \\ z_8' \\ z_9' \end{matrix}$$

Note that each matrix $\boldsymbol{w}_i'$ has as many rows as the number of constraints (i.e., 9 rows) and as many columns as the number of colors that may be contained in place r_i.

Moreover, by looking at matrix $\boldsymbol{w}_2'$ we may observe that its first row is null because the marking $\boldsymbol{m}_2$ is not involved in the first constraint. On the contrary, the non null elements in its second row, relative to π_2 and π_4 are due to the fact that $m_2(\pi_2)$ and $m_2(\pi_4)$ are involved in the second constraint. The value 1 is due to the fact that 1 is the associated coefficient in the corresponding linear constraint. ■

6 Conclusions

In this paper, we provide a Colored Petri Net model to describe a Railway Network System and to derive the traffic controller. The introduced framework allows us to define a supervisor controller guaranteeing safeness and deadlock freeness in the railway traffic control system. Starting from the analysis of deadlock on the basis of digraph tools, a deadlock prevention strategy is defined and expressed by a set of linear inequality constraints. Moreover, we have shown how collision and deadlock prevention constraints can be expressed as colored GMEC and the controller can be realized by a set of monitor places.

References

[1] B. De Schutter, T. van den Boom, "Model predictive control for railway networks," *2001 IEEE/ASME Int. Conf. on Advanced Intelligent Mechatronics*, Como, Italy, July 2001.

[2] A.A. Desrochers, R.Y. Al-Jaar, *Applications of Petri nets in manufacturing systems*, New York, IEEE Press, 1995.

[3] 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.

[4] M.P. Fanti, B. Maione, S. Mascolo, B. Turchiano, "Control policies conciliating deadlock avoidance and flexibility in FMS resource allocation," *ETFA95, INRIA/IEEE Symp. on Emerging Technologies and Factory Automation*, Paris, France, October 1995.

[5] M.P. Fanti, B. Maione, S. Mascolo, B. Turchiano, "Event based feedback control for deadlock avoidance in flexible production systems", *IEEE Trans. on Robotics and Automation*, Vol. 13, No. 3, pp. 347-363, 1997.

[6] M.P. Fanti, B. Maione, B. Turchiano, "Deadlock avoidance in flexible production systems with multiple capacity resources", *Studies in Informatics and Control*, Vol. 7, No. 4, pp. 343-364, 1998.

[7] M.P. Fanti, A. Giua, C. Seatzu, "A deadlock prevention method for railway networks using monitors for colored Petri nets," *2003 IEEE Int. Conf. on Systems, Man and Cybernetics*, Washington, USA, October 2003.

[8] A. Giua, C. Seatzu, "Liveness enforcing supervisors for railway networks using ES^{2}PR Petri nets," *Int. Workshop on Discrete Event Systems*, WODES02, Zaragoza, Spain, October 2002.

[9] F. Harary, R.Z. Norman, D. Cartwright, *Structural models: an introduction to the theory of directed graphs*, John Wiley & Sons, Inc. New York, 1965.

[10] K. Jensen, *Colored Petri nets: basic concepts, analysis methods and practical use*, Vol. 1, New York Springer, 1992.

[11] M. Missikoff, "An object-oriented approach to an information and decision support systems for railway traffic control," *Emerging Application of Artificial Intelligence*, Vol. 11, pp. 25-40, 1998.

[12] E.A.G. Weits, "Simulation of railway traffic control," *Int. Trans. Operational Research*, Vol. 5, No. 6, pp. 461-469, 1998.