BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES
Vol. 57, No. 3, 2009

Deadlock freeness supervisor for marked graph

H. SIOUD, Z. ACHOUR, A. SAVA*, and N. REZG

INRIA Nancy Grand Est & LGIPM, Ile du Saulcy, 57045 Metz Cedex, France

Abstract. This note presents a control synthesis approach for discrete event systems modeled by marked graphs with uncontrollable transitions. The forbidden behavior is specified by General Mutual Exclusion Constraints (GMEC). We prove that, even if the system to be controlled is live, the closed loop control may generate deadlock situations. Using the structural proprieties of marked graph we defined the causes of deadlock situations, and we defined a formal method to avoid them.

Key words: discrete-event system, forbidden state problem, deadlock avoidance, marked graph.

1. Introduction

The research work presented in this note deals with deadlock free control synthesis for discrete-event systems (DES). A DES is a dynamic system that evolves depending on the occurrence of events. The control synthesis consists in designing a supervisor which restricts the behavior of the system by preventing the occurrence of given events in order to guarantee the respect of specifications. Sometimes the restriction provided by the supervisor may generate deadlock situations. Obviously, this property is undesirable in practice because it is not useful to have a closed loop system which stops working as soon as it approaches a dangerous behavior.

The research work we present in this paper propose a solution to this problem for DES modeled by a particular class of Petri nets called marked graphs. First, we prove that existing control synthesis approaches for marked graphs can generate deadlock situations. Then, we analyze the cause these deadlocks and propose a method to avoid them.

In the sequel we present a brief review of papers related to our research word.

The control synthesis theory was initiated by the research work of Ramange and Wonham [1]. They proposed a formal approach based on finite state automata and formal languages. However, the luck of structure of automata models makes this approach rather difficult to use for real industrial problems. Therefore, researchers have focused their attention on Petri nets, which provides an intuitive explicit representation for behaviors like resource sharing, parallelism and synchronization.

Several control synthesis approaches use structural properties of Petri nets (PN) to build efficient supervisors. For instance, in [2, 3] the authors model the set of forbidden states by general mutual exclusion constraints (GMEC), which are linear inequalities between place markings. It proposes a formal method to design monitor places for safe and cyclic marked graphs. Furthermore, this technique has been extended in [4] by taking into account the uncontrollable nature of some transitions. The authors show that in this case, their approach provides a suboptimal solution. The control synthesis approaches proposed in [5] and [6] are based on linear algebra. This technique uses the state equation and the reachability graph of the PN model of the plant to build control places. A control synthesis approach based on the theory of regions is developed in [7].

All these approaches deal with bounded general Petri nets.

Furthermore, [8] proposes a solution to the forbidden state problem for bounded or non bounded marked graphs with controllable and uncontrollable transitions. This method uses the structural proprieties of marked graph to build a very computational efficient controller. The forbidden states are defined by GMEC and the control law is based on counting the number of firings of given controllable transitions. The drawback of the method is that the supervisor may introduce deadlocks in the closed loop system even when the initial system is live.

Deadlock avoidance problem for marked graphs has been considered in several publications. Thus, [9] extends the control synthesis approach proposed in [3] with the liveness constraint for the closed loop system. It proposes a method to efficiently solve the problem for safe marked graphs.

In this paper, we consider the control synthesis approach proposed in [8]. We analyze the deadlock occurrence and we propose an approach for deadlock free control synthesis dedicated to marked graphs not necessarily bounded and not necessarily safe.

This paper is organized as follows. Section 2 reviews important definitions related to marked graphs and presents the control synthesis method given in [8]. The deadlock avoidance approach for independent critical places is presented in Sec. 3. In Section 4 we discuss the case of dependent critical places. Concluding remarks are given in Sec. 5.

2. Marked graph and control synthesis

In this part we provide a brief presentation of the control synthesis approach proposed in [8]. First of all, we recall the definitions and the properties of marked graphs and the PN notations that will be used throughout this paper.

*e-mail: sava@enim.fr

A marked graph is an ordinary Petri net such that every place has exactly one input transition and one output transition. The main notations we use are enumerated in the sequel:

$N : (P, T, C)$	marked graph
P	set of places
T	set of transitions
C	incidence matrix
T^u	set of uncontrollable transitions
T^c	set of controllable transitions
$p^\bullet$(resp. $p^\bullet$)	output (respectively input) transition of the place p
$t^\bullet$ (resp. $t^\bullet$)	set of output (respectively input) places of the transition t
M	marking of places
M_0	initial marking of places
$\sigma[t_i]$	counts the number of times the transition t_i has been fired
$M[t > M'$	firing the transition t from marking M leads to marking M'
$R(N, M_0)$	set of reachable markings of marked graph N with initial marking M_0
$R^u(N, M)$	set of markings of reached from the marking M by firing only uncontrollable transitions.

Assumption 1 [4]. The marked graph model of the plant is structurally live.

The GMEC type constraints were introduced in [2]. The authors provide a formal definition for GMEC. They discuss the proprieties and the equivalence between GMECs.

Definition 1 [2]. Given a plant Petri net model (N, M_0), a GMEC is defined by a couple $(w,\ k)$ where w is a linear vector of positive integers and k is an integer. A marking $M \in R(N, M)$ respects a GMEC $(w,\ k)$ if and only if $wM \leq k$.

A marking is forbidden if it does not satisfy at least one GMEC. The set of forbidden markings is denoted M_f.

As some transitions may be uncontrollable, form a given marking M it is possible to reach other markings by firing only uncontrollable transitions. The set of these markings is denoted $R^u(N, M)$.

It is clear that if a marking $M' \in R^u(N, M)$ is forbidden, then the marking M must also be avoided because at this point, the system may reach uncontrollably a forbidden state. Thus, the marking M is called dangerous. The set of dangerous markings is M_d.

Hence the set of forbidden markings *MF* is the union of the set of markings which violate at least one GMEC (i.e. M_f) and the set of dangerous markings (i.e. M_d).

$$\begin{aligned} M_f &= \{M \in R(N, M_0)/\exists i \text{ s.t. } w_i M > k_i\}, \\ M_d &= \{M \in R(N, M_0)/\forall i, w_i M \leq k_i, \\ &\qquad \exists M \in R^u(N, M_0), M' \in M_f\}, \\ MF &= M_f \cup M_d. \end{aligned} \tag{1}$$

In the rest of the paper, when no confusion is possible, dangerous markings are assimilated to forbidden markings.

Definition 2. Let us consider a GMEC $(w,\ k)$. A place p is called critical if $w[p] \neq 0$. The set of critical places is $C_r(w) = \{p \in P/w[p] \neq 0\}$.

Building an optimal control law requires the worst-case analysis of each GMEC specification. Optimal control law can be defined as follows: a controllable transition t is not prevented from firing at a reachable marking M if and only if $G(w_i, M') \leq k_i$ for all GMEC specification $(w_i,\ k_i)$ where $M[t > M'$ and

$$G(w_i, M') = MAX\left\{\overrightarrow{w}_i \cdot M*,\ \forall M* \in R^u(N, M')\right\}. \tag{2}$$

The marking M^* is the worse case that can be reached by firing uncontrollable transitions.

The control synthesis technique proposed in [4] is based on computing the value of $G(w_i, M')$ using the following structural propriety of marked graphs.

Propriety 1 [8]. The marking of an oriented path $\pi = t_1 p_1 \cdots p_n t_{n+1}$ changes only by firing its extremity transitions i.e. $M(\pi) = M_0(\pi) + \overrightarrow{\sigma}[t_1] - \overrightarrow{\sigma}[t_{n+1}]$ where $M \in R(N, M_0)$ and $\sigma[t_i]$ is the number of times transition t_i has been fired.

According to the propriety 1, it is possible to estimate the marking of a critical place by analyzing its preceding subnet, i.e. influence paths.

Definition 3 [8]. A controllable transition t is called an influence transition of a place p if there is an elementary path π from t to p such t is the only controllable transition in the path. The influence path of a place p is $\pi(p)$.

The set of influence paths of a place p is $\Pi(p)$. $C(p)$ is the set of its influence transitions and $\Omega(p)$ is the set of elementary circuits containing place p.

Definition 4 [8]. The influence zone $Z(p)$ of a place p is the subnet containing all nodes s such that there exists a directed path from s to p without controllable transitions except eventually s.

The marking of any place is depending on the tokens present in its influence zone, so to estimate the marking of a place we need to estimate the marking in each path.

Definition 5 [8]. Let us consider two critical places p_1 and p_2:

- p_1 and p_2 are independent if $p_i \notin \Omega(p_j) \cup \Pi(p_j) \wedge p_j \notin \Omega(p_i) \cup \Pi(p_i)$
- p_1 and p_2 are dependent if they are not independent.

First, we discuss the particular case of a GMEC with only one critical place. Then we present the general case.

2.1. GMEC with one critical place. Let us consider a GMEC $w \cdot M \leq k$ with one critical place q. The supervisor must inhibit controllable transitions leading to forbidden markings. Thus, we must determine the worst case, i.e. the maximum value of $w \cdot M$ by firing uncontrollable transitions [4]. Consequently, the supervisor must evaluate online $Y(q, M)$, which is the maximum number of tokens that place q could get by firing only uncontrollable transitions from the marking M. The analytical expression of $Y(q, M)$ is given by theorem 1.

Theorem 1 [8]. For any critical place p and any reachable marking M,

$$Y(p, M) = \min \left\{ \min_{\pi \in \Pi(p)} M(\pi), \min_{\omega \in \Omega(p)} M(\omega) \right\}, \quad (3)$$

where $\Pi(p)$ is the set of influence paths of p and $\Omega(p)$ is the set circuits which contain p.

In other terms $Y(p, M)$ can be formulated as

$$Y(p, M) = \min \left\{ \min_{t \in C(p)} d(M, t, p\bullet), \min_{d}(M, p\bullet, \bullet p) \right\},$$

where $d(M, n_1, n_2)$ is the marking distance between the node n_1 and the node n_2, defined by the number of tokens in the places between the node n_1 and the node n_2 for the marking M.

2.2. GMEC with several critical places. If a GMEC has more than one critical place, then two cases may occur: 1) independent critical places and 2) dependent critical places.

The idea of the control synthesis technique is the same for both cases and it is given in algorithm 1. However, the maximum uncontrollably reachable marking of the critical places (i.e. the worse case) is calculated in a different way. Thus, in the sequel we focus on the case where the critical places are independent. The other case shall be discussed in Sec. 4.

Algorithm 1. Control synthesis

1. Define the set of critical places.
2. Identify the influence transitions and paths for each critical place.
3. Calculate the maximum uncontrollably reachable marking for critical places.
4. Forbid the firing of any controllable transition leading to a marking which is forbidden or dangerous.

If all the critical places are independent then each place gets to its maximum marking independently of the marking of the others critical places. Therefore, the worst-case is when each place reaches its maximum marking.

Theorem 2 [8]. Let $Cr(w) = \{p \in P / w(p) \neq 0\}$ be the set of critical places of the CGEM (w, k). If all the critical places $p_i \in Cr(w)$ are independent, then for any reachable marking M, it exists a sequence of uncontrollable transitions leading to M^*, such as

$$M^* = \sum_i Y(P_i, M).$$

Definition 6. Let $A(N, M)$ be the set of controllable transitions whose firing from the marking M is allowed by the supervisor.

The control low is given by the algorithm 2 which is an extension of the algorithm 1.

Algorithm 2. Calculate the control law

1. Initialize: $\forall t \in T^c$, $\sigma[t] = 0$, $M = M_0$, $A(N, M) = \varnothing$.
2. Define the set of critical places.
3. Calculate $G(w, M)$ for each GMEC (w, k).
   3.1 If $G(w, M) > k$, for at least one GMEC then no solution, end of the program.
   3.2 If not go to 4.
4. For each enabled controllable transition t such as $M[t > M'$, calculate $G(w, M')$:
   If for one GMEC (w, k), $G(w, M') > k$,
   Then t is prevented from firing at M,
   Else, t is allowed to fire at M, $A(N, M) = A(N, M) \cup \{t\}$.
5. Wait for a transition $t \in A(N, M)$ to fire and then update the current marking M and the counter $\sigma[t]$.
6. Go to 4.

Example 1. Let us consider the marking graph given in Fig 1. The initial marking is $M_0 = [0\ 0\ 0\ 0]^t$ and the specification is given by the following GMEC:

$$M(p_1) + M(p_2) \leq 1. \quad (4)$$

We apply algorithm 2 to compute the control law.
The set of critical places is: $C_r = \{p_1,\ p_2\}$.
Calculate $G(w, M)$:

$$Y(p_1, M) = M_0(p_1) + \sigma[t_1] - \sigma[t_3],$$
$$Y(p_2, M) = M_0(p_2) + \sigma[t_2] - \sigma[t_4],$$
$$G(w, M) = Y(p_1, M) + Y(p_2, M) =$$
$$= M_0(p_1) + M_0(p_2) + \sigma[t_1] - \sigma[t_3] + \sigma[t_2] - \sigma[t_4].$$

According to the initial marking $M_0 = [0\ 0\ 0\ 0]^t$ and to the GMEC $(M(p_1) + M(p_2) \leq 1)$, the supervisor allows firing the controllable transitions t_1 and t_2 if the following control rule is satisfied:

$$\sigma[t_1] - \sigma[t_3] + \sigma[t_2] - \sigma[t_4] \leq 1. \quad (5)$$

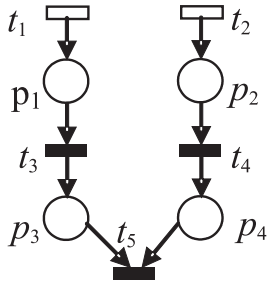

Fig. 1. Marked graph model

The control law provided by this technique is maximal permissive and very computational efficient. However, the restriction introduced by the supervisor may lead to deadlock situations as we show in the next section.

3. Deadlock freeness

Let us consider again the marked graph in Fig. 1 with a GMEC: $M(p_1) + M(p_4) \leq 1$. The process is still controllable and using the algorithm above, we obtain the following control low:

$$\sigma[t_1] - \sigma[t_3] + \sigma[t_2] - \sigma[t_5] \leq 1.$$

Firing transition t_2 from the initial marking $M_0 = [0\ 0\ 0\ 0]^t$ is allowed as it leads to a marking $M_1 = [0\ 1\ 0\ 0]^t$ which respects the GMEC. From this marking, the system can evolve uncontrollably to $M_2 = [0\ 0\ 0\ 1]^t$. Neither transitions t_1 nor t_2 can be fired without violating the GMEC. Therefore, the restriction imposed by the supervisor leads to a deadlock situation.

3.1. Deadlock analysis. The aim of the research work we present in this paper is to extend the control synthesis technique given in [8] and build a supervisor to guarantee that the closed loop system is deadlock free.

First of all we analyze the causes of deadlock. Let us consider the marked graph in Fig. 2, with the initial marking $M_0 = [0\ 0\ 0\ 0]^t$ and the following GMEC:

$$M(p_1) + M(p_3) \leq 1.$$

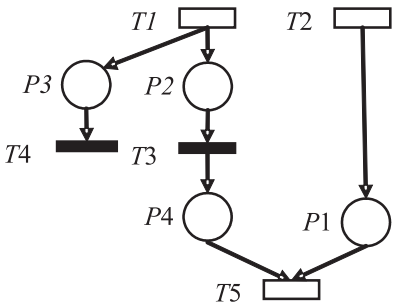

Fig. 2. Cases of deadlock

Firing transition t_2 before transition t_1 from the initial marking is allowed by the supervisor and leads to a deadlock.

The deadlock situation does not appear if transition t_1 is fired before transition t_2.

Note that the transition t_1 (respectively t_2) is an influence transition of the critical place p_3 (respectively p_1).

Moreover, firing the output transition of the critical place p_1 (i.e. t_5) depends on the influence transition t_1. Then, we can observe from the example that if the output transition of a critical place p got a common influence transition with another critical place a deadlock may occur.

Definition 7. A risky transition, denoted t_r, is the output transition of a critical place which gets more than one input place and which depends on a influence transition of another critical place.

Let B denote the set of risky transitions. Formally,

$$B = \left\{ \begin{array}{l} t_r \in T / \exists (p_i, p_j) \in C_r(w) \times C_r(w), \\ \exists t \in C(p_j) / p_i \in \bullet t_r \wedge \gamma(t, t_r) \in N \end{array} \right\} \quad (6)$$

Lemma 1. If the marked graph has at least one risky transition, then a deadlock may occur in the closed loop system.

Proof of lemma 1. Let us consider a marked graph which is structurally live (assumption 1) and a GMEC (w_i, k_i). It is obvious that, a state where $\sum_i \overrightarrow{w}_i \cdot M(p_i) = k$, can be reached by the closed loop system because it satisfies the specifications. However, the supervisor forbids the firing of the influence transitions of all the critical places until the firing of at least one output transition of a critical place.

It is clear that the marking of a critical place is increased by firing its influence transitions and decreased by firing its output transition.

Let us consider that the closed loop system is in a deadlock situation. Thus, no influence transition of critical place can be fired without violating the GMEC and the output transitions of critical places are not enabled.

If $\sum_i \overrightarrow{w}_i \cdot M(p_i) = k$ then there exists at least one marked critical place $p_i \in C_r(w_i)$. Let t_i be its output transition.

If the closed loop is in the deadlock situation that's mean t_i is not enabled hence at least one of the influence paths of t_i is not marked. Let π_i be the influence path of transition t_i which is not marked and t_{ci} be its influence transition.

The influence path π_i can not become marked if the firing of t_{ci} is forbidden by the supervisor. This situation occurs if transition t_{ci} is an influence transition of another critical place. According to definition 7, t_i is a risky transition.

Therefore, if a deadlock situation may occur, then the marked graph has necessarily at least one risky transition.

Theorem 3. Let N be a structurally live marked graph with the GMEC (w, k). The closed loop system is deadlock free if and only if N has no risky transitions regarding the given GMEC.

Proof of theorem 3. Theorem 3 is a direct consequence of lemma 1.

For each risky transition t_r, we define the following notations:

- $\pi_r(t_r)$ is the influence path of t_r,
- $\Pi_r(t_r)$ is the set of influence paths of t_r,
- $C_b(t_r)$ is the set of influence transition of t_r.

The idea of our approach consists in assuring that at least one risky transition can be enabled.

In a marked graph, a transition can be enabled, if all its influence paths are marked or if the firing of influence transitions associated to each non marked influence path is allowed by the supervisor.

Thus the control synthesis technique that we propose follows two steps. First, we determine the enabled controllable transitions whose firings do not lead uncontrollably to forbidden markings using the approach proposed in [8]. Then, we enforce the deadlock free property.

In the sequel, we present the deadlock avoidance technique, which is the main contribution of this paper.

Definition 8. Let $\tau(t_r, M)$ be the set of influence transitions of t_r who's the relative influence path is not marked: $\tau(t_r, \mathrm{M}) = \{t \in C_b(t_r)/d(M, t, t_r) = 0\}$.

In other words, $\tau(t_r, M)$ is the set of influence transitions who's firing is needed in order to enable the transition t_r.

A deadlock situation may occur in a closed loop mode, if $\forall t_r \in B$, $\tau(t_r, M) \not\subset A(N, M)$.

3.2. Deadlock avoidance technique. A controllable transition t is prevented by the supervisor if its firing violates the GMEC or if it leads to a deadlock situation. Let us consider a controllable transition $t \in T^c$. The firing of t is forbidden by the supervisor if $G(w, M') > k$ or if $\forall t_r \in B$, $\tau(t_r, M') \not\subset A(N, M)$ with $M[t > M'$.

Definition 9. Let $E(t)$ be the set of transitions that can become enabled after the firing of t and which are not synchronization transitions.

Let $t_e \in E(t)$, then $\sigma(t)$ and $\sigma(t_e)$ are dependent.

We denote $M[E(t) > M'$ the marking reached by firing all transitions $t_e \in E(t)$. For the marked graph in Fig. 2 the set of transitions that can be become enabled after firing t_1 is $E(t_1) = \{t_3, t_4\}$.

Given a controllable transition t, the condition needed to avoid deadlock is:

$$\exists t_r \in B, \text{ such that } \tau(t_r, M) \subset A(N, M') \cup \{t\}.$$

This conditions states that a deadlock can be avoided if the influence transitions of non marked influence paths of at least one risky transition t_r can be fired.

In result, the control synthesis technique with deadlock freeness of marked graph is given by the algorithm 3.

Algorithm 3. Deadlock avoidance for marked graphs:

1. Initialize $\sigma = 0$, $A(N, M) = \varnothing$, $M = M_0$.
2. Define the set of critical places C_{ri} for each GMEC$_\mathrm{i}$.
3. Define the set of risky transitions B and their influence transitions.
4. For each GMEC$_\mathrm{i}$ (w_i, k_i), calculate $G_i(w_i, M)$.
   4.1 If $\exists j$ such that $G_j(w_j, M_0) > k_j$, the problem has no solution. End program.
5. For each enabled controllable transition t calculate $G_i(w_i, M*)$ for each GMEC$_\mathrm{i}$ (w_i, k_i):
   5.1 If $\exists j / G_j(w_j, M) > k_j$ forbid the firing of t.
   Else $A(N, M) = A(N, M) \cup \{t\}$.
6. For each $t \in A(N, M)$
   If $\exists t_r \in B / \gamma(t, t_r) \in N$ then compute $A(N, M')$ and $\tau(t_r, M)$, where $M[E(t) > M'$.
   If $\tau(t_r, M) \subset A(N, M') \cup \{t\}$ then allow the firing of t.
   Else forbid the firing of t.
   Else allow firing transition t.
7. Fire a transition t and determine the new marking M.
8. Update $\sigma[t]$ and $A(N, M) = \varnothing$. Go to 5.

Example 2. We illustrate the algorithm 3 using the marked graph given in Fig. 3. We wish that the system respects the following GMEC:

GMEC$_1$: $M(p_1) + M(p_6) \leq 1$,
GMEC$_2$: $M(p_4) + M(p_7) \leq 1$.

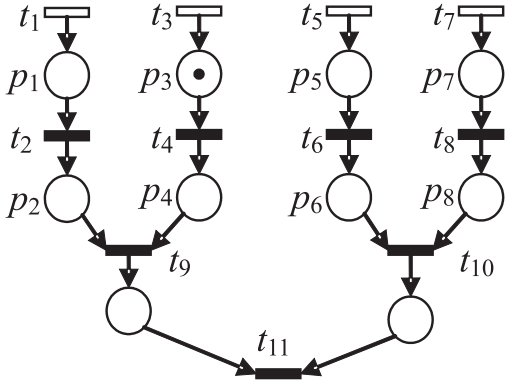

Fig. 3. Marked graph of an assembling plan

So these are the steps of resolution following the algorithm
2) $C_{r1} = \{p_1, p_6\}$; $C_{r2} = \{p_4, p_7\}$.
3) $B = \{t_9, t_{10}\}$, $C_b(t_9) = \{t_1, t_3\}$, $C_b(t_{10}) = \{t_5, t_7\}$.
4) $Y(p_1, M_0) = M_0(p_1) + \sigma(t_1) - \sigma(t_2) = 0$
$Y(p_6, M_0) = M_0(p_6) + M_0(p_5) + \sigma(t_5) - \sigma(t_{10}) = 0$
$\Rightarrow G_1(w, M_0) = Y(p_1, M_0) + Y(p_6, M_0) = 0 \leq 1$ (true)
$Y(p_4, M_0) = M_0(p_4) + M_0(p_3) + \sigma(t_2) - \sigma(t_5) = 1$
$Y(p_7, M_0) = M_0(p_7) + \sigma(t_7) - \sigma(t_8) = 0$
$\Rightarrow G_2(w, M_0) = Y(p_4, M_0) + Y(p_7, M_0) = 1 \leq 1$ (true)
4) Checking the respect of GMEC:
For $t_1 : G_1(w, M^*) = 1 \leq 1 \Rightarrow A(N, M) = \{t_1\}$
For $t_3 : G_2(w, M^*) = 2 > 1 \Rightarrow t_3 \notin A(N, M)$
For $t_5 : G_1(w, M^*) = 2 > 1 \Rightarrow A = (N, M) = \{t_1, t_5\}$
For $t_7 : G_2(w, M^*) = 1 \leq 1 \Rightarrow t_7 \notin A(N, M)$
5) Checking the deadlock avoidance:
For $t_1 : \gamma(t_1, t_9) \in N, \tau(t_5, M)$?
$d(M, t_1, t_9) = 0$ hence $t_1 \in \tau(t_9, M)$
$d(M, t_3, t_9) = 1$ hence $t_3 \notin \tau(t_9, M)$
thus $\tau(t_9, M) = \{t_1\}$
$E(t_1) = \{t_2\}$
in $M'(M[E(t_1) > M')\sigma'(t_1) = 1$, $\sigma'(t_2) = 1$
$G_1(w, M') = \sigma'(t_1) - \sigma'(t_2) + \sigma(t_5) - \sigma(t_{10}) = 0$
$G_2(w, M') = 1 + \sigma(t_3) - \sigma(t_9) + \sigma(t_7) - \sigma(t_8) = 1$
$\Rightarrow A(N, M') = \{t_1, t_5\}$,
$\tau(t_9, M) \subset A(N, M') \cup \{t_1\} \rightarrow$ So the firing of t_1 is allowed
For t_5: $\gamma(t_3, t_{10}) \in N$:
$\tau(t_{10}, M)$?
$d(M, t_5, t_{10}) = 0$ hence $t_1 \in \tau(t_{10}, M)$
$d(M, t_7, t_{10}) = 0$ hence $t_7 \in \tau(t_{10}, M)$
so $\tau(t_{10}, M) = \{t_5, t_7\}$
E$(t_5) = \{t_6\}$
in $M'(M[E(t_5) > M')\sigma'(t_5) = 1$, $\sigma'(t_6) = 1$
$G_1(w, M') = \sigma'(t_1) - \sigma'(t_2) + \sigma'(t_5) - \sigma(t_{10}) = 1$
$G_2(w, M') = 1 + \sigma'(t_3) - \sigma(t_9) + \sigma(t_7) - \sigma(t_8) = 1$
thus $A(N, M') = \varnothing$
$\tau(t_{10}, M) = \{t_5, t_7\} \not\subset A(N, M') \cup \{t_1\}$,
$\rightarrow$ the firing of t_5 is forbidden.
6) Wait for the firing of a transition.
7) Update σ, initialize $A(N, M)$, and go to step 4.

4. The case with dependent critical places

This Section deals with the deadlock avoidance technique for the case of dependent critical places. First, we recall the control synthesis approach developed in [4]. Then we propose a deadlock avoidance technique.

4.1. GMEC with two dependent critical places. Let us consider a constraint (w, k) with two dependant places q_1 and q_2 such that $w(q_1) < w(q_2)$. Considering a marking M, the worst case is the maximum uncontrollable reachable marking noted $M^* \in R^u(M, N)$, such that wM^* is the maximum possible. We admit that:

1. $\sum_p w(p)M^*(p) \leq \sum_p w(p)Y(p, M)$.
2. $M^*(q_2) = Y(q_2, M)$.

The worst case marking for the place q_2 (i.e. $M^*(q_2)$), depends on the position of q_2 and the influence zone of q_1 (i.e. $Z(q_1)$). There are 3 cases [4]:

1. $q_2 \notin Z(q_1)$.
2. $q_2 \in Z(q_1)$ and $Y(q_2, M) \geq d(M, q_1\bullet, q_2)$.
3. $q_2 \in Z(q_1)$ and $Y(q_2, M) < d(M, q_1\bullet, q_2)$.

For the first case (i.e. $q_2 \notin Z(q_1)$) there is no path of uncontrollable transitions from q_2 to q_1. The marking distance between $q_1\bullet$ and q_2 may eventually not be big enough to obtain $M^*(q_2)$. It means that tokens in q_1 are conveyed to q_2. Thus the number of tokens needed to obtain $M^*(q_2)$ is $Y(q_2, M) - d_M(q_1\bullet, q_2)$, which is equal to the number of firing $q_1\bullet$ while $q_2\bullet$ is not fired. Consequently, the number of tokens in q_1 becomes [4]:

$$M^*(q_1) = \min\Big[\min_{t\in T}^{c}[d(M, t, q_1\bullet) + d(M, q_1\bullet, q_2) - \\ -Y(q_2, M)];\ S(q_1)\Big], \tag{7}$$

where $S(q_1) = \min_{(\omega\in\Omega)} M(\omega(q_1)) = d(M, q_1\bullet, \bullet q_1)$. If there is no circuit $\omega \in \Omega$ containing q_1, then $S(q_1) = \infty$.

For the second case (i.e. $q_2 \in Z(q_1)$ and $Y(q_2, M) \geq d(M, q_1\bullet, q_2)$) there are not enough tokens in the shortest path between q_1 and q_2 to obtain $M^*(q_2) = Y(q_2, M)$. Therefore, the tokens in q_1 are convoyed to q_1. The number of token needed to get $M^*(q_2)$ is $Y(q_2, M) - d(M, q_1\bullet, q_2)$. The number of tokens in q_1 is equal to [4]:

$$M^*(q_1) = \min\Big[\min_{t\in T_{Uq2\bullet})}^{c}[d(Mt, q_1\bullet) + d(M, q_1\bullet, q_2) - \\ -Y(q_2, M)];\ (q_1)\Big]. \tag{8}$$

For de last case (i.e. $q_2 \in Z(q_1)$ and $Y(q_2, M) < d(M, q_1\bullet, q_2)$), there are enough tokens in the shortest path between q_1 and q_2 to obtain $M^*(q_2) = Y(q_2, M)$. However, if $q_2\bullet$ is fired then the marking of q_1 marking is no longer maximal, so the remainder tokens in q_1 are equal to [4]:

$$M^*(q_1) = \min\{Y(q_1, M);\ d(M, q_2\bullet, q_1) - Y(q_2, M) + \\ + \min_{t\in T}^{c}[d(M, t, q_2\bullet)]\}. \tag{9}$$

The relations (7–9) are proved in [8] and the control synthesis technique is described by algorithm 4.

Algorithm 4. Control synthesis for 2 dependent critical places

1. Initialize: $M = M_0$; $\forall t$, $\sigma(t) = 0$.
2. Identify critical places for the GMEC, their influence paths and transitions.
3. Identify the dependent critical places.
   If there are more than two dependant critical places, then end of the program.
4. Let the two dependent critical places be q_1 and q_2 such that $w(q_1) < w(q_2)$.
5. For each transition $t \in A(N, M)$, such that $M[t > M'$, calculate $Y(q_2, M')$ and
   If $q_2 \notin Z(q_1)$ then $M^*(q_1) = (7)$
   Else if $q_2 \in Z(q_1)$ and $Y(q_2, M') \geq d(M', q_1, q_2)$, then $M^*(q_1) = (8)$
   Else if $q_2 \in Z(q_1)$ and $Y(q_2, M') < d(M', q_1, q_2)$, then $M^*(q_1) = (9)$
6. For all the independent critical places p calculate $M^*(p) = Y(p, M')$;
7. Calculate $G(w, M') = wM^*$
   If $G(w, M') > k$ forbid the firing of t;
   Else allow the firing of t;
8. Wait for the firing of a transition t.
9. Update $M = M'$ and $\sigma(t) = \sigma(t) + 1$. Go to step 4.

4.2. Deadlock avoidance. Let us consider a marked graph (N, M_0) which must satisfy a GMEC (w, k) with two critical places q_1 and q_2.

The deadlock avoidance technique that we propose is close to the one developed for the case where the critical places are independent. The main idea is that, if risky transitions exist, at least one will be enabled.

However, when two critical places are dependent, a risky transition t_{r1} may belong to the influence path of another risky transition t_{r2}. Thus, $C_b(t_{r1}) \subseteq C_b(t_{r2})$. A necessary condition to enable t_{r2} is to enable t_{r1} too. Therefore, the controller starts the deadlock analyze by the risky transition with the smallest C_b.

4.3. GMEC with several dependant critical places. There is no analytical solution for the control synthesis problem for marked graphs when the GMEC has several dependent critical places [4]. To our knowledge, this problem can be solved only when all the dependant critical places are in the same path and have the same weight in the GMEC. The solution proposed in [4] for this particular case is to transform dependent critical places into an equivalent place.

Theorem 4 [8]. Let (N, M_0) be a marked graph with the GMEC (w, k) with $q_1, ..., q_n$ dependent critical places in the same path and $w(p_1) = w(p_2) = ... = w(p_n)$, the equivalent critical place denoted p_L is defined as:

$$\begin{cases} \bullet p_L = \bullet q_1 \\ p_L\bullet = q_n\bullet \\ M_0(p_L) = \sum_{i=1}^{n} M_0(q_i) \\ w(p_L) = w(q_1) = ... = w(q_n) \end{cases}. \tag{10}$$

After this transformation we get a control synthesis problem where the dependent critical places are replaced by a equivalent critical place. Therefore, we are in the case where the critical places are independent, which was treated in Sec. 3.

Example 3. We illustrate the deadlock avoidance technique for the case with dependent critical places using the marked graph given in Fig. 4. Let us consider that the behavior of this system must satisfy the following GMEC:

$$M(p_1)+M(p_2)+M(p_3)+2^*M(q_2)+M(p_6)+M(p_8) \leq 4.$$

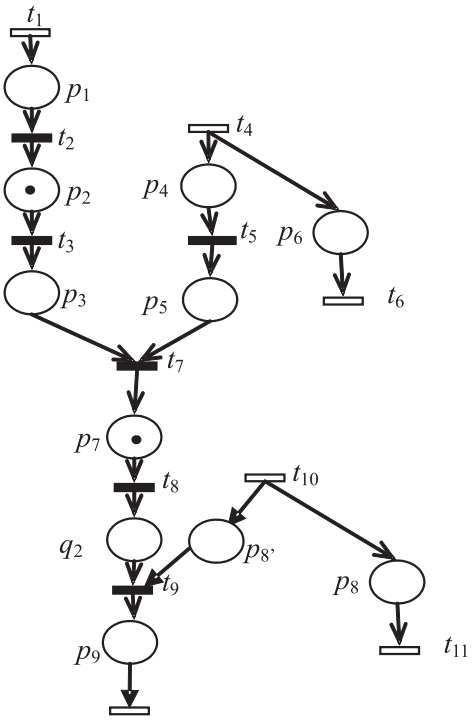

Fig. 4. Marked graph for several dependent critical places

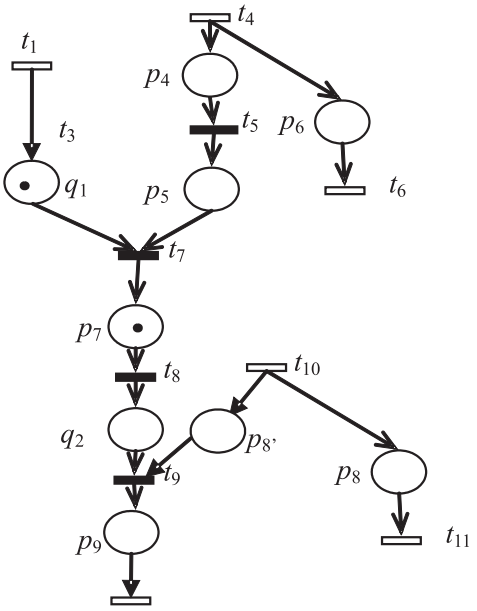

Fig. 5. Marked graph with equivalent critical place

The set of critical places is $C_r = \{p_1, p_2, p_3, \text{ and } q_2\}$. Let q_1 be the equivalent critical place to p_1, p_2, and p_3. The marked graph obtained by this transformation is given Fig. 5. The new CGEM is: $M(q_1)+2^*M(q_2)+M(p_6)+M(p_8) \leq 4$. Note than in this case q_1 and q_2 are dependent critical places. Thus we are in the case of two dependent critical places.

2) Critical places: $C_r = \{q_1, q_2, p_6, p_8\}$.
3) risky transitions: $B = \{t_7, t_9\}$, $C_b(t_7) = \{t_1, t_4\}$,
$C_b(t_9) = \{t_1, t_4, t_{10}\}$
4) the maximum uncontrollably reachable marking
$Y(p_6, M) = M_0(p_6) + \sigma(t_4) - \sigma(t_6) = 0$
$Y(p_8, M) = M_0(p_8) + \sigma(t_{10}) - \sigma(t_{11}) = 0$
q_1 and q_2 are dependent and $q_2 \notin Z(q_1)$;
$Y(q_2, M) = \min[\sigma(t_1) - \sigma(t_9) + M_0(q_2) + M_0(p_7) + M_0(q_1);$
$\sigma(t_4) - \sigma(t_9) + M_0(q_2) + M_0(p_7) + M_0(p_5) + M_0(p_4)]$
$= \min[\sigma(t_1) - \sigma(t_9) + 2;\ \sigma(t_4) - \sigma(t_9) + 1]$
$M^*(q_1) = \min[d(M, t_1, t_7) + d(M, t_7, q_2) - Y(q_2, M);\ \infty]$
$= d(M, t_1, t_7) + d(M, t_7, q_2) - Y(q_2, M)$
$= 2 + \sigma(t_1) - \sigma(t_7) + \sigma(t_7) - \sigma(t_9) - Y(q_2, M)$
$= 2 + \sigma(t_1) - \sigma(t_9) - Y(q_2, M)$
$G(w, M) = Y(p_6, M) + Y(p_8, M) + M^*(q_1) + 2^*Y(q_2, M)$
$= Y(p_6, M) + Y(p_8, M) + d(M, t_1, t_7) + d(M, t_7, q_2) +$
$+ Y(q_2, M) = 2 + \sigma(t_4) - \sigma(t_6) + \sigma(t_{10}) - \sigma(t_{11}) +$
$+ \sigma(t_1) - \sigma(t_9) + \min[\sigma(t_1) - \sigma(t_9) + 2;\ \sigma(t_4) - \sigma(t_9) + 1]$
4) Check the control policy
For $t_1 : G(w, M^*) = 4 \leq 4 \Rightarrow A(N, M) = \{t_1\}$
For $t_4 : G(w, M^*) = 4 \leq 4 \Rightarrow A(N, M) = \{t_1, t_4\}$
For $t_{10} : G(w, M^*) = 4 \leq 4 \Rightarrow A(N, M) = \{t_1, t_4, t_{10}\}$
$A(N, M) = \{t_1, t_4, t_{10}\}$
5) Check the deadlock avoidance
For t_1; $\gamma(t_1, t_7) \in N$:
$\tau(t_7, M)$?
$d(M, t_1, t_7) = 1$ hence $t_1 \notin \tau(t_7, M)$
$d(M, t_4, t_7) = 0$ hence $t_4 \in \tau(t_7, M)$
so $\tau(t_7, M) = \{t_4\}$
$\gamma(t_1, t_9) \in N$
$d(M, t_1, t_9) = 2$ hence $t_1 \notin \tau(t_9, M)$
$d(M, t_4, t_9) = 1$ hence $t_4 \notin \tau(t_9, M)$
$d(M, t_{10}, t_9) = 0$ hence $t_{10} \in \tau(t_9, M)$
so $\tau(t_9, M) = \{t_{10}\}$
$E(t_1) = \varnothing$
in $M'(M[t_1 > M')\sigma'(t_1) = 1$
$G(w, M') = 2 + \sigma(t_4) - \sigma(t_6) + \sigma(t_{10}) - \sigma(t_{11}) + \sigma'(t_1) -$
$-\sigma(t_9) + \min[3; 1] = 4$
thus $A(N, M') = \{t_1\}$
$\tau(t_7, M) \not\subset A(N, M') \cup \{t_1\}$
$\tau(t_9, M) \not\subset A(N, M') \cup \{t_1\}$
$\rightarrow$ **the firing of t_1 is forbidden**.
For t_4;
we have $\gamma(t_4, t_7) \in N$ thus we have to check if: $\tau(t_7, M) = \{t_4\} \subseteq A(N, M') \cup \{t_4\}$: it is true with out checking $A(N, M')$.
$\rightarrow$ THE FIRING OF t_4 IS ALLOWED

For t_{10};
we have $\gamma(t_{10}, t_9) \in N$ thus we have to check if: $\tau(t_9, M) = \{t_{10}\} \subseteq A(N, M') \cup \{t_{10}\}$: it is true with out checking $A(N, M')$.
$\rightarrow$ THE FIRING OF t_{10} IS ALLOWED

We can see that the controller forbids the firing of t_1 to avoid a deadlock occurrence.

5. Conclusions

In this paper we addressed deadlock avoidance for a particular class of DES control problems. More precisely, our research work deals with discrete event systems modeled by marked graphs not necessarily bounded and not necessarily safe. The uncontrollable nature of some events is taken into account. The specifications are modeled by General Mutual Exclusion Constraints (GMEC). We show that existing control synthesis approach does not consider the deadlock avoidance for closed loop system. Therefore, in this paper, we analyzed the deadlock evolutions and we proposed a simple technique to avoid them. Both cases of GMEC with independent and dependent critical places are considered.

Further research work will be done to extend this approach to marked graphs with unobservable transitions.

REFERENCES

[1] P.J.G. Ramadge and W.M. Wonham, "The control of discrete event systems", *Proc. IEEE* 77 (1), 81–98 (1989).

[2] A. Giua, F. DiCesare, and M. Silva, "Generalized mutual exclusion constraints on nets with uncontrollable transitions", *Systems, Man and Cybernetics, IEEE Int. Conf.* 2, 974–979 (1992).

[3] A. Giua, F. DiCesare, and M. Silva, "Petri net supervisor for generalized mutual exclusion constraints", 12^{th} *IFAC World Congress Sidney*, 267–270 (1993).

[4] F. Basile, P. Chiacchio, L. Recalde, and M. Silva, "Suboptimal supervisory control of Petri nets in presence of uncontrollable transitions via monitor places", *Automatica* 42, 995–1004 (2006).

[5] J. Moody and P.J. Antsaklis, "Petri net supervisors for DES with uncontrollable and unobservable transitions" , *Report* 99-004 ISIS, (1999).

[6] P. Darondeau and X.L. Xie, "Linear control of live marked graphs, *Automatica* 39 (3), 429–440 (2003).

[7] N. Rezg, X. Xie, and A. Ghaffari, "Supervisory control in discrete event systems using the theory of regions", *Discrete Event System Analysis and Control*, 391–398 (2000).

[8] A. Ghaffari, N. Rezg, and X. Xie, "Feedback control logic for forbidden state problem of marked graphs", *IEEE Trans. on Automatic Control* 48 (1), 18–29 (2003).

[9] F. Basile, P. Chiacchio, L. Recalde, and M. Silva, "Closed-loop live Petri net supervisors for GMEC", *Proc. WODES 2000*, 171–180 (2000).