



## SUPERVISORES DE SISTEMAS A EVENTOS DISCRETOS COM DECISÃO PARA FALHAS EM SENSORES, BASEADOS EM REDES DE PETRI SÍNCRONAS

*Gilberto Bispo da Silva Góes<sup>1</sup>*  
*Eduard Montgomery Meira Costa<sup>2</sup>*

**RESUMO** - O formalismo para sintetizar supervisores para Sistemas a Eventos Discretos que garantem a continuidade de processos é aqui introduzido. O paradigma utilizado para modelar o SED é a rede de Petri síncrona, na qual são introduzidos novos conceitos para a formalização do controle, como funções de habilitação de transições e funções de disparos forçados de transições. A definição de transições forçáveis é baseada nos trabalhos de Brandin e Wonham para SEDs temporizados. O uso da rede de Petri síncrona assegura o funcionamento do sistema através de eventos externos gerados por sensores ativos no sistema. O procedimento proposto garante a continuidade temporal do processo, mesmo havendo falha em algum sensor. Um exemplo de síntese do supervisor usando o formalismo proposto é apresentado.

**Palavras-chave:** Redes de Petri, Controle Supervisório, Sistemas a Eventos Discretos

**ABSTRACT** - The formalism to synthesize the supervisor for Discrete Event Systems that ensures the continuity of processes is introduced here. The paradigm used to model DES is the synchronous Petri net, which are introduced new concepts to formalize the control, as transitions enabling functions and transitions forced firing functions. The definition of forcible transitions is based on Brandin and Wonham for timed DES. The use of synchronous Petri net ensures the system's functionality through external events generated by active sensors in the system. The proposed procedure ensures the time continuity of the process, although occurs fault in some sensor. An example of supervisor synthesis using the proposed formalism is presented.

**Key-words:** Petri Nets, Supervisory Control, Discrete Event Systems

### 1 Introdução

Sistemas a Eventos Discretos (SEDs) (Ramadge e Wonham, 1982) são sistemas que apresentam uma evolução dinâmica descrita pela ocorrência de eventos que determinam sua interação com o ambiente e que alteram o estado do sistema. Os SEDs

---

<sup>1</sup> Mestre em Engenharia Elétrica. Professor do Departamento de Tecnologia Mecânica e Materiais do CEFET-BA. E-mail: gilbertogoes@cefetba.br

<sup>2</sup> Doutor em Engenharia Elétrica. Professor do Mestrado em Engenharia Elétrica da Universidade Federal da Bahia. Bolsista DCR/CNPq. E-mail: edmonty@ig.com.br

estão presentes em aplicações do cotidiano como redes de computadores, sistemas de manufatura e supervisão de tráfego aéreo e ferroviário. O estudo dos SEDs requer a utilização de uma representação adequada e que permita projetar um agente de controle automático, denominado supervisor. A partir de tarefas especificadas, o supervisor recebe informações da ocorrência dos eventos do SED e determina a ação de controle a ser aplicada, enviando comandos para os atuadores que inibem ou habilitam determinados eventos.

A formalização do problema de controle de SEDs utilizando autômatos e linguagens formais (Hopcroft e Ullman, 1979) é denominada de Teoria de Controle Supervisório (TCS) (Ramadge e Wonham, 1989), que é uma forma elegante de resolver o problema de controle de SEDs: a partir do modelo do SED e de uma especificação funcional, determina um supervisor. A TCS define condições para o controle considerando o comportamento lógico. Entretanto, em várias situações, há a necessidade explícita de definir instantes de tempos exatos para a aplicação de controle para inibir eventos, bem como para impor sincronismo entre as ocorrências dos eventos. Para isto, torna-se necessário a inclusão de uma representação temporal no SED.

Várias formalizações para o controle de SEDs temporizados são encontradas na literatura. Entre elas, encontra-se a abordagem da TCS para SEDs temporizados de (Brandin e Wonham, 1994), utilizando autômatos que incluem a representação do tempo definida por meio de um evento sincronizado ao relógio global, denominado evento *'tick'*. Quando se trata da necessidade de sincronização entre eventos, a álgebra de dióides (Bacelli *et al*, 1992) tem sido largamente utilizada, seja para os autômatos temporizados (Alur e Dill, 1994), como visto em (Gaubert, 1995; Costa, 2002), seja para as redes de Petri temporizadas (Chrétienne, 1983), como pode ser visto em (Libeaut, 1996). Outros formalismos para a síntese de supervisores de SEDs temporizados que não utilizam a álgebra de dióides são encontrados, como (He e Lemmon, 1998; Cofrancesco *et al*, 1991). Entretanto, é em (Silva, 1999) que é apresentado um importante formalismo para esta classe de SEDs que estende a abordagem de (Barroso, 1996) para o caso temporizado, sendo aplicado a modelos de SEDs temporizados descritos por redes *seguras*. De maneira similar a (Barroso, 1996), Silva (Silva, 1999) garante a construção de supervisores que

mantêm a mesma estrutura do modelo do SED para qualquer especificação de comportamento definida, utilizando a definição das redes de Petri Temporais Interpretadas com Função de Habilitação de Transição para estruturar o supervisor e formalizando o *Algoritmo para a Construção da Árvore de Alcançabilidade de Classes (AAAC)*, em que uma classe determina um conjunto de estados que contêm a mesma marcação com diferentes intervalos de tempo associados.

O formalismo de (Silva, 1999) se aplica a casos em que a associação dos intervalos de tempo não é tão complexa como o caso descrito pela rede de Petri com Temporização Nebulosa (Figueiredo, 1994), intervalos estes que podem ser obtidos por estimação ou por simples medição. Sua aplicação permitiu construir um algoritmo para transformação das funções da rede supervisora em linguagem de CLP (*Instruction List*).

Em outras abordagens de controle de SEDs utilizando redes de Petri, encontram-se formalismos para a transformação da estrutura da rede em programas de CLP, como nos trabalhos de (Uzam *et al*, 1996), (Frey, 2000) e (Chirn e McFarlane, 2000).

Entretanto, em nenhum destes casos, o supervisor sintetizado realiza tomadas de decisão dentro da operação do sistema. Isto é, se houver alguma falha nos sensores do sistema físico que atualizam o CLP, o sistema pode parar sua execução esperando uma resposta de algum sensor, o que não é desejado. Também, observa-se que, com a inclusão de intervalos de tempo no modelo do sistema, como é o caso de (Silva, 1999), há uma “*aparente introdução de controle*” no modelo, como é descrito em (Costa, 2001). Dessa forma, uma importante contribuição surge com a utilização das redes de Petri Síncronas (RPS) (Hilal e Ladet, 1994) associando temporizadores às transições, para a aplicação de controle a SEDs temporizados, considerando algumas características para o sistema:

1. O modelo do sistema é considerado com todos os eventos descritos como eventos *remotos* (Brandin e Wonham, 1994), isto é, têm apenas a descrição do limite inferior para que o evento se torne habilitado (o limite superior é infinito), o que descreve o sistema livre de controle;
2. Todos os tempos de vida são considerados com limite inferior de tempo igual a zero, isto é, o evento está habilitado a partir do momento que o estado é

atingido, mas que só podem disparar quando um evento externo ocorra, o que garante o uso das RPS na modelagem do SED;

3. Todos os eventos são descritos com igual prioridade de ocorrência, o que também garante que não há condições de controle prévio;

4. Alguns eventos controláveis podem ser definidos como *eventos forçáveis* (Brandin e Wonham, 1994), de forma que seja possível interferir na execução do sistema, como em (Hilal e Ladet, 1993).

Através destas considerações, pode-se utilizar o formalismo de (Barroso, 1996) para construir a rede supervisora. Neste caso, observa-se que a árvore de alcançabilidade da RPS tem uma formalização similar às redes não temporizadas, e permite incluir as funções de habilitação de transição, bem como um novo formalismo definido como temporizações que determinam limites superiores para o supervisor forçar o disparo das transições, quando necessário for. Este problema é tratado aqui.

## 2 Conceitos

Os seguintes conceitos são necessários para o entendimento deste trabalho, desde que forma a base teórica utilizada.

### ***Redes de Petri Síncronas***

Uma rede de Petri Síncrona (RPS) (Hilal e Ladet, 1994) pode ser definida como em (Silva, 1999):

**Definição 1** *Uma Rede de Petri Síncrona é uma tripla*

$$RPS = (RP, E, FE), \quad (1)$$

*em que RP é uma rede de Petri marcada; E é um conjunto de eventos externos; FE é uma função do conjunto de transições T da RP para  $E \cup \{e\}$ , com e sendo o evento que possui ocorrência permanente, isto é, ele é o elemento neutro do monóide  $(E^1 + \dots + E^p)^*$ , onde  $E = \{E^1, \dots, E^p\}$  é o conjunto de eventos externos.*

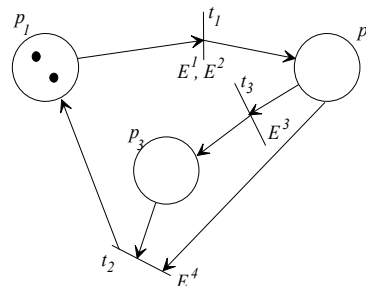
Essa definição é uma formalização mais simplificada que em (Hilal e Ladet, 1994), que se consideram todos os eventos externos com as mesmas prioridades, sendo a que será utilizada para este trabalho. Nessa definição, o evento  $e$  é um evento que

corresponde à sequência de eventos externos cujo período é zero. Uma transição sincronizada por este evento é disparada assim que ela se torna habilitada. A notação  $E_i$  refere-se ao *nome* de um evento externo e a notação  $E_j$  será utilizada para o evento associado à transição  $t_j$ .

Uma transição em uma RPS necessita que, além da habilitação formal definida para as redes de Petri, isto é, todos os lugares de entrada da transição devem ter o número de fichas que garantam seu disparo (e os lugares de saída não ultrapassem sua capacidade), é necessário que um evento externo  $E$ , que esteja associado à transição, ocorra para que ela possa disparar. Esta situação define que a transição está receptiva ao evento  $E$ , e com sua ocorrência, ela dispara, gerando uma nova marcação conforme as regras de disparo das redes de Petri clássicas.

As condições citadas sobre a receptividade de uma transição  $t$  se apresentam como uma importante formalização para a estruturação de controle de SEDs, quando é desejado avaliar a dinâmica do sistema físico sobre a visão do modelo, desde que os eventos externos são as informações vindas do sistema através dos sensores. Assim, o estado do modelo em RPS do sistema, seja este formalizado em um computador, ou em um CLP, só é atualizado quando ocorre a chegada de uma informação de um determinado sensor do sistema.

**Exemplo 1** Considere a RPS apresentada na Figura 1. Nesta rede, tem-se o conjunto de eventos externos que estão associados às transições, dado por  $E = \{E^1, E^2, E^3, E^4\}$ .



**Figura 1:** Exemplo de uma RPS.

Os eventos  $E^1$  e  $E^2$  estão associados à transição  $t_1$ , tal que quando esta transição está habilitada, ela é receptiva a estes dois eventos. Para a transição  $t_2$ , há apenas um evento associado, que é o

evento externo  $E^4$  e para a transição  $t_3$ , tem-se associado o evento  $E^3$ . Na marcação  $M_0=[2\ 0\ 0]^T$ , a única transição habilitada é a transição  $t_1$ , a qual é receptiva aos eventos externos  $E^1$  e  $E^2$ . Assim, a ocorrência de qualquer um destes eventos faz a transição  $t_1$  disparar, levando à marcação  $M_1=[1\ 1\ 0]^T$ , e uma nova ocorrência de qualquer um destes eventos leva a rede à marcação  $M_2=[0\ 2\ 0]^T$ . Da mesma forma, na marcação  $M_1$ , se ocorre o evento  $E^3$ , a transição  $t_3$  que também está receptiva, dispara levando à marcação  $M_3=[1\ 0\ 1]^T$ , e assim por diante. Entretanto, para uma marcação, como  $M_0$ , se ocorrer o evento  $E^4$ , que não está associado à transição  $t_1$ , não há mudança de marcação na rede, desde que ela é a única habilitada, porém não é receptiva a este evento.

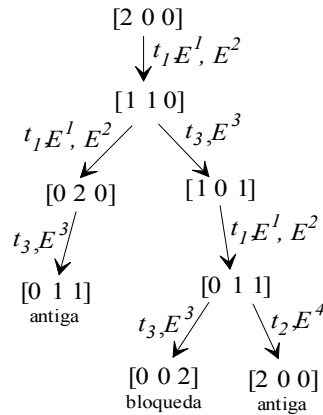
Observa-se neste exemplo que a diferença básica da regra de disparos das transições, refere-se unicamente à sua receptividade em relação a um evento externo associado a esta transição. Assim, a evolução dinâmica da RPS é similar à rede de Petri clássica.

### ***Árvore de Alcançabilidade das Redes de Petri Síncronas***

Como visto no Exemplo 1, uma transição habilitada numa marcação  $M$ , dispara se ocorrer um evento externo associado a esta transição. Uma sequência de ocorrências de eventos externos associados a transições receptivas gera uma sequência de disparos de transições, e dessa forma, a evolução dinâmica da RPS tem uma forma similar às redes de Petri clássicas, podendo ter a árvore de alcançabilidade descrita da mesma forma, apenas associando aos arcos os eventos que tornam as respectivas transições receptivas. Deve-se observar que estas condições são garantidas para o caso específico tratado aqui, que é considerando as condições citadas anteriormente, na introdução deste artigo.

De acordo com as sequências de eventos externos ocorrendo no sistema, as transições irão disparar formando sequências de marcações, como visto no Exemplo 1. Assim, pode-se construir toda a árvore de alcançabilidade da RPS, desconsiderando a ocorrência de eventos externos que não estejam associados a nenhuma transição habilitada numa determinada marcação.

**Exemplo 2** A RPS do Exemplo 1 tem sua árvore de alcançabilidade mostrada na Figura 2.



**Figura 2:** Árvore de alcançabilidade de uma RPS.

No Exemplo 2, como citado anteriormente, observa-se que apenas são consideradas as ocorrências dos eventos externos associados a transições que estejam habilitadas, tornando a árvore de alcançabilidade similar à árvore de alcançabilidade de uma rede de Petri clássica com a mesma estrutura (sem considerar a inclusão dos eventos externos). Com este formalismo, pode-se utilizar a abordagem de (Barroso, 1996) como base para construir supervisores utilizando RPS, o que é visto a seguir.

### 3 Formulação de Síntese do Supervisor

Para definir a síntese do supervisor para os SEDs nesta abordagem, é necessário incluir temporizadores para as transições das RPS. Isto é, devem ser incluídos temporizadores locais para as transições da rede, os quais são incrementados sempre que uma marcação que habilita uma transição  $t$  é alcançada. O temporizador da transição  $t$  disparada é zerado, mantendo os temporizadores das outras transições habilitadas e que não são desabilitadas com o disparo de  $t$ , na mesma marcação. Assim, tem-se:

**Definição 2** Uma Rede de Petri Síncrona com Temporizadores é uma dupla

$$RPST = (RPS, T),$$

em que RPS é uma Rede de Petri Síncrona marcada;  $T = \{\tau_1, \dots, \tau_m\}$  é um conjunto de temporizadores sincronizados a um relógio global, os quais são associados às transições, tal que  $\forall M$

$|M \in MA(RPS, M_0)$ ,  $\tau_i = 0$  se a transição  $t_i$  não está habilitada em  $M$ , e  $\tau_i = \tau_i + 1$  em sincronia com o relógio global, enquanto  $t_i$  estiver habilitada.

Com a formalização da RPST, podem-se obter os tempos exatos de ocorrência dos eventos externos associados a uma determinada transição, bem como o tempo total de execução de seqüências de disparos na evolução dinâmica da rede. Dessa forma, como os temporizadores dependem da ocorrência dos eventos externos, não faz sentido construir uma árvore de alcançabilidade para a RPST que descreva os valores desses temporizadores nos momentos de tais ocorrências. Esta inclusão é apenas um formalismo para a estrutura de controle que será apresentada adiante, e sua árvore de alcançabilidade é a mesma da RPS.

Na abordagem de (Barroso, 1996) é mostrada que a síntese do supervisor baseada em redes de Petri necessita da construção da sua árvore de alcançabilidade com um passo a mais para detecção dos estados não permitidos (com crescimento ilimitado de fichas), e esta serve como base junto à especificação de comportamento para sintetizar um supervisor formalizado sobre uma Rede de Petri com Função de Habilitação de Transição (RPFHT).

Desde que o formalismo para a construção da árvore de alcançabilidade da RPS com as condições definidas para o modelo do sistema apenas difere na inclusão dos eventos externos associados às transições e a árvore de alcançabilidade da RPST é a mesma, o Algoritmo Modificado da Árvore de Alcançabilidade (*AMArA*) de (Barroso, 1996) pode ser utilizado sem problemas para a construção da árvore de alcançabilidade modificada das RPS. De igual forma, apenas os eventos externos serão incluídos junto às transições disparáveis nos arcos da árvore, como visto no Exemplo 2.

Tendo a árvore de alcançabilidade da RPST, uma especificação de comportamento deve ser definida. Esta especificação de comportamento, ou a tarefa que o sistema deve realizar é formalizada de maneira similar a (Barroso, 1996). Esta similaridade se apresenta por ela ser definida pela evolução lógica da rede como uma linguagem ou uma marcação a ser alcançada, o que irá definir as condições de não bloqueio e funções para que a rede não alcance estados não permitidos.



Considerando que a rede evolui sincronamente com os eventos externos associados às transições, e não é interessante que a rede se mantenha parada devido a não ocorrência de algum evento externo, ou seja, se algum evento externo não ocorrer num tempo tolerado, é necessário desviar sua execução, forçando o disparo de uma transição habilitada/receptiva nesta marcação. Os tempos limites tolerados para as ocorrências dos eventos externos da rede podem ser definidos sobre os tempos obtidos nas suas respectivas ocorrências através de medições simples no sistema (resposta dos sensores somados aos tempos de recepção do sinal do sensor pelo sistema).

Como o supervisor deve ser construído utilizando uma RPST para modelar o sistema, torna-se necessário incluir na estrutura da RPST dois tipos de função associadas às transições:

1. Funções de Habilitação de Transições - responsáveis pela habilitação ou inibição da transição em determinadas marcações;
2. Funções de Disparo Forçado de Transições - responsáveis pelo disparo forçado de uma transição habilitada em uma determinada marcação.

As funções de disparo forçado são funções específicas para comparação com os temporizadores locais das transições. Estas funções disparam forçadamente transições habilitadas quando o temporizador de uma transição receptiva ultrapassa o limite máximo de tempo permitido para a ocorrência de um de seus eventos externos associados.

Com esses conceitos, define-se uma Rede de Petri Síncrona com Temporizadores e Funções de Habilitação de Transições (RPSTFHT) como a seguir:

**Definição 3** *Uma Rede de Petri Síncrona com Temporizadores e Funções de Habilitação de Transições é uma tripla*

$$RPSTFHT = (RPST, \phi, \pi),$$

*em que RPST é uma Rede de Petri Síncrona com Temporizadores marcada;  $\phi = \{\phi_1, \dots, \phi_m\} : MA(RP, M_0) \rightarrow \{0, 1\}$  é a função de habilitação das transições, que mapeia o conjunto de marcações alcançáveis em 0 ou 1;  $\Pi = \{\pi_1, \dots, \pi_m\} : \Phi \times T \times T \rightarrow \{0, 1\}$  é a função de disparos forçados das transições, tal que*

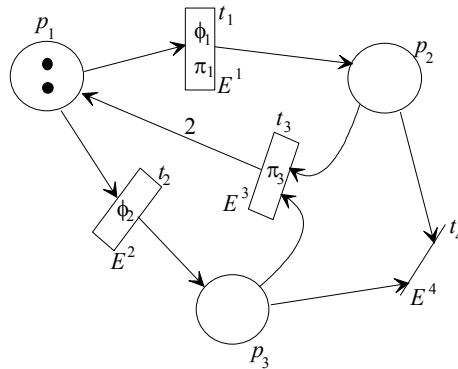
$$\pi_i = \begin{cases} 1, & \text{se } \phi_i = 1 \text{ e } \tau_i > \tau_{ref}; \\ 0, & \text{caso contrário,} \end{cases} \quad (2)$$

com  $i$  representando as transições de saída do lugar  $p_i$  receptivas a eventos externos e  $\tau_{ref}$  os valores de referência (limites máximos tolerados de tempo) para forçar a transição  $t_i$ .

Desta definição, pode-se ver que a RPSTFHT une a RPFHT com a RPS, bem como inclui um novo formalismo para forçar transições em casos de não ocorrência de determinados eventos externos associados a outras transições habilitadas/receptivas. Neste caso, para uma transição estar habilitada, ela necessita apresentar as condições da RPFHT (satisfazer as condições das redes de Petri clássicas e a função de habilitação ter valor 1). Por outro lado, se para uma dada transição habilitada/receptiva  $t_i$  uma função  $\pi_i$  for definida em relação ao limite máximo de tempo  $\tau_{ref}$  para a ocorrência de um evento externo associado a uma outra transição habilitada/receptiva  $t_j$  e seu temporizador ultrapassar este valor definido ( $\tau_i > \tau_{ref}$ ), então  $\pi_i = 1$  e ela ( $t_i$ ) é forçada a disparar. Para esta rede, o valor padrão das funções  $\phi$  é 1, quando esta função não é definida em uma transição, significando que ela sempre está habilitada. Da mesma forma, o valor padrão das funções  $\pi$  é 0, quando esta função não é definida em uma transição, significando que ela nunca é forçada a disparar, mas podendo disparar em qualquer momento de acordo com as regras de disparo das RPFHTs.

**Exemplo 3** Considere a RPSTFHT apresentada na Figura 3. Nesta rede, as funções associadas às transições são:  $t_1: \phi_1 = [\neg p_2]$ ,  $\pi_1 = [\tau_1 > 3]$ ;  $t_2: \phi_2 = [\neg p_3]$ ,  $\pi_2 = 0$  (valor padrão);  $t_3: \phi_3 = 1$  (valor padrão),  $\pi_3 = [\tau_3 > 2]$ ;  $t_4: \phi_4 = 1$  (valor padrão),  $\pi_4 = 0$  (valor padrão). No início da execução da rede, o relógio global é inicializado em conjunto com os temporizadores locais das transições  $t_1$  e  $t_2$ , que são as únicas transições habilitadas pelas funções  $\phi_1$  e  $\phi_2$ , e receptivas aos eventos externos  $E^1$  e  $E^2$ , respectivamente. A transição  $t_1$  pode disparar a qualquer instante de tempo antes de 3 unidades de tempo passados, com a ocorrência do evento externo  $E^1$  associado a ela. Entretanto, após estas 3 unidades de tempo, esta transição é forçada a disparar, levando a rede para a marcação  $M = [1 \ 1 \ 0]^T$  (caso  $E^2$  não tenha ocorrido e disparado  $t_2$ ), ou para a marcação  $M = [0 \ 1 \ 1]^T$  (caso  $E^2$  tenha ocorrido, o que levou a rede à marcação  $M = [1 \ 0 \ 1]^T$  pelo disparo de  $t_2$ ). Quando a rede alcança a marcação  $M = [0 \ 1 \ 1]^T$ , os

temporizadores das transições  $t_3$  e  $t_4$  são inicializados, desde que são as únicas transições habilitadas/receptivas aos eventos externos  $E^3$  e  $E^4$ , respectivamente. Nesta condição, a rede pára sua execução se houver a ocorrência do evento externo  $E^4$  antes do evento  $E^3$ , que a leva para a marcação  $M=[0\ 0\ 0]^T$ , ou retorna a marcação inicial  $M_0=[2\ 0\ 0]^T$ , caso ocorra o evento  $E^3$  antes do evento  $E^4$ , ou caso o temporizador da transição  $t_3$  ultrapasse o valor de 2 unidades de tempo, o que torna  $\pi_3=1$ , forçando seu disparo.



**Figura 3:** Rede de Petri Síncrona com Temporizadores e Funções de Habilitação de Transições.

Com a formalização da RPSTFHT, pode-se estruturar um supervisor para um SED modelado por uma RPST, utilizando sua árvore de alcançabilidade e uma especificação de comportamento. Para este caso, a partição do conjunto de transições é definida igualmente ao formalismo da TCS, isto é,

$$T = T_c \cup T_{uc} \quad (3)$$

(isto é, transições controláveis e transições não controláveis significando os eventos controláveis e os eventos não controláveis). Para este caso define-se o conjunto de transições forçáveis  $T_f \subseteq T_c$ , que contém as transições nas quais as funções  $\pi$  podem ser definidas diferentes do valor padrão.

Deve-se observar, que tendo definidas as condições (2) e (3), na construção do modelo do sistema em RPST devem ser consideradas as seguintes situações de necessidade:

1. Necessariamente o modelo do sistema tem de ter transições forçáveis;

2. Para cada parte do sistema, deve existir pelo menos uma transição forçável, que garanta a continuidade da evolução dinâmica em casos de falhas nos sensores ou por outro problema inerente ao sistema, que gere ociosidade;

3. Os tipos de transições que podem ser forçáveis dentro do sistema e que devem existir nas partes isoladas do sistema são:

- a. Transição de processo - ou seja, a própria transição que espera uma resposta do sensor (transição que está receptiva ao seu evento externo associado);
- b. Transição que garante que o sistema não atinge estados indesejados;
- c. Transição de reinício de processo;
- d. Transição de abandono do processo.

Partindo destas condições, o modelo terá sempre a possibilidade de descartar processos em andamento, ou reiniciá-los, ou continuá-los, ou mesmo, desviar situações indesejáveis. Essas condições são inerentes ao procedimento de modelagem de SEDs utilizando redes de Petri, como visto em (Zhou e DiCesare, 1993). Entretanto, aqui são utilizadas essas restrições específicas para a utilização das transições forçáveis, de forma a ser possível sintetizar o supervisor.

Com o modelo do sistema, a especificação de comportamento, pode ser definida por meio de uma marcação a ser atingida, ou por meio de uma linguagem formal.

Por fim, para a síntese da rede supervisora a seguinte proposição é apresentada (Góes, 2003):

**Proposição 1** *Dado um modelo de um sistema em RPST com transições forçáveis, através de sua árvore de alcançabilidade modificada, pode-se construir um supervisor não bloqueável cuja evolução é contínua mesmo havendo a não ocorrência de alguns eventos externos.*

**Demonstração:** *Pela abordagem de (Barroso, 1996), garante-se o não bloqueio através da construção das funções de habilitação de transições. Por outro lado, para uma marcação  $M$ , se duas transições  $t \in T$  e  $t' \in T_f$  estão habilitadas e,  $t$  está receptiva a um evento externo  $E$ , então  $t$  disparará com sua ocorrência (resposta do sensor que gera o evento  $E$ ). Entretanto, considerando que o sensor que gera esse evento externo tem um tempo limite máximo  $\tau_{ref}$  de sensibilidade (para dar uma resposta à transição  $t$*

da rede), a ultrapassagem deste limite ( $\tau > \tau_{ref}$ ) implica na possibilidade da ocorrência da transição  $t'$  que pode ser forçada. Caso  $t \in T_f$  e  $t'$  esteja receptiva ao evento externo  $E'$ , então tanto a transição  $t'$  pode disparar com a ocorrência do evento  $E'$  associado, como a transição  $t$  pode ser forçada a ocorrer. Para qualquer uma destas condições, sempre a condição de um evento externo não ocorrer em seu limite máximo, define uma falta no sensor e, dessa forma, o processo é continuado, impedindo o sistema de se tornar ocioso.

Tendo as condições específicas para a construção do modelo utilizando as transições forçáveis, a estruturação do supervisor é fundamentada sobre o *Algoritmo da Construção do Gerador da Suprema Sub-Linguagem Controlável (ACGS)* de (Barroso, 1996), e do *Algoritmo para Construção do Processo de Decisão do Supervisor (ACPDS)* que constrói as funções  $\pi$  das transições forçáveis do conjunto  $T_f$ . Este algoritmo é apresentado a seguir:

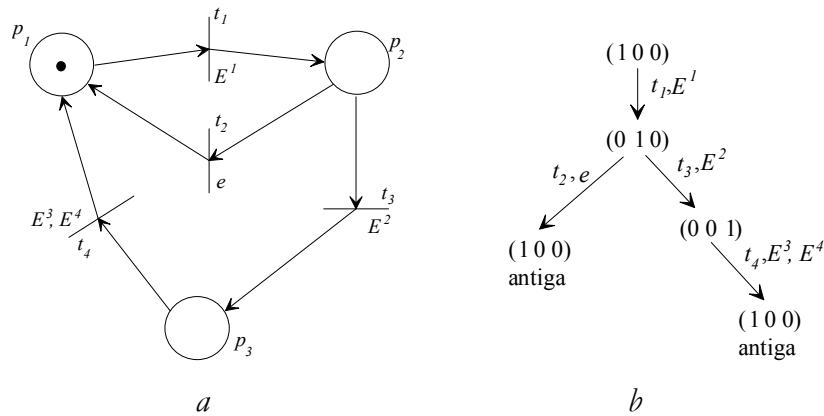
### ***Algoritmo para Construção do Processo de Decisão do Supervisor (ACPDS)***

1. Dados os valores de referência  $\tau_{ref}$  (limites máximos de resposta dos sensores), faça:
  - a. Para cada transição  $t_i$  habilitada em cada marcação  $M$ , tal que  $\phi_i = 1$ , faça:
    - i. Se  $t_i \in T_f$  e  $t_i$  é receptiva aos eventos externos  $E^{i1}, E^{i2}, \dots, E^{in}$ , faça
 
$$\pi_i = [\tau_i > \max \{ \tau_{ref,i1}, \tau_{ref,i2}, \dots, \tau_{ref,in} \}],$$
 com  $\tau_{ref,ij}$  sendo o tempo máximo para ocorrência do evento externo  $E^{ij}$ ,  $j=1,2,\dots,n$ ;
    - ii. Se  $t_i \notin T_f$  e  $\exists t_k \mid M[t_k > \wedge \phi_k = 1 \wedge t_k \in T_f]$ , faça:
      - I. Se  $t_k$  é receptiva a um evento externo  $E^k$ , então  $\pi_k = [\tau_k > \tau_{ref,k}]$ ;
      - II. Se existem  $E^{k1}, E^{k2}, \dots, E^{kn}$  associados à  $t_k$ , faça  $\pi_k = [\tau_k > \max \{ \tau_{ref,k1}, \tau_{ref,k2}, \dots, \tau_{ref,kn} \}]$ ;
      - / III. Se  $\exists E^k$  associado à  $t_k$ , faça  $\pi_k = [\tau_k > \tau_{ref,i}]$ ;
      - IV. Se existem  $t_{k1}, t_{k2}, \dots, t_{km}$  habilitadas em  $M$  e  $t_{kj} \in T_f$ ,  $j=1,2,\dots,m$ , então  $\pi_{kj}$  é definida pelas condições a.ii.I, a.ii.II. e a.ii.III.

Neste algoritmo, para cada transição habilitada em uma marcação  $M$ , a não ocorrência de um evento externo associado gera uma função de disparo forçado para a própria transição se ela é forçável, forçando a continuidade do processo, ou para uma outra transição habilitada de acordo com as regras de disparos das RPFHTs, que desvia a execução do processo para uma outra atividade.

#### 4 Exemplo Aplicativo da Abordagem Proposta

Considere a RPST da Figura 4.a, em que todas as transições são forçáveis e controláveis.



**Figura 4:** a. RPS para exemplo da utilização do ACPDS e b. árvore de alcançabilidade.

Sua árvore de alcançabilidade é apresentada na Figura 4.b. Nesta rede, deseja-se que, após a marcação  $M_1 = [0\ 1\ 0]^T$  a rede não reinicie, e que o processo de evolução seja contínuo e definido pela linguagem  $(t_1 t_3 t_4)^*$  não importando quais eventos ocorram para a habilitação de  $t_4$ .

Utilizando o ACGS de (Barroso, 1996), encontra-se que  $t_2$  nunca deve disparar. Isto é,  $\phi_2 = 0$ . Por outro lado, considerando que os eventos externos tenham seus tempos definidos por  $E^1 = 10ms$ ;  $E^2 = 50ms$ ;  $E^3 = 3ms$  e  $E^4 = 25ms$  a utilização do ACPDS define as funções de disparo forçado:  $\pi_1 = (\tau_1 > 10ms)$ ;  $\pi_3 = (\tau_3 > 50ms)$  e  $\pi_4 = (\tau_4 > \max\{3ms, 25ms\}) = (\tau_4 > 25ms)$ . Com estas funções, a rede tem uma evolução dinâmica contínua para a especificação dada, mesmo que algum destes eventos não ocorram. Por exemplo, a falha

do evento  $E^1$ , após este tempo limite ( $10ms$ ), a transição  $t_1$  é forçada. Da mesma forma, para o evento  $E^2$  (e a transição respectiva  $t_2$ ). No caso de  $t_4$ , se não ocorre o evento  $E^3$ , há a espera pela ocorrência do evento  $E^4$  que, se não ocorrer, a transição  $t_4$  é forçada a disparar. Considerando agora que a especificação definida seja que a rede tenha uma evolução contínua sem restrições, observa-se que as funções  $\pi_1$  e  $\pi_4$  são as mesmas anteriormente citadas. Entretanto, neste caso, há uma situação de conflito entre as transições  $t_2$  e  $t_3$ . De acordo com o *ACPDs*, desde que  $t_3$  é receptiva ao evento  $E^2$ , então  $\pi_3$  é a mesma função definida anteriormente. No caso de  $t_2$ , como não há evento externo associado a ela, então  $\pi_2=0$  (segue a regra comum de disparo de transição da rede de Petri).

## 5 Conclusões

Esse artigo introduz um formalismo para sintetizar supervisores para sistemas a eventos discretos com um procedimento de decisão temporal em termos de falhas em sensores no sistema. No sistema a ser definido o controle, uma rede de Petri síncrona é utilizada para modelá-lo, a qual relaciona os disparos das transições com ocorrências de eventos externos gerados pelas sensibilizações de sensores do sistema. Para a construção do supervisor são definidas as funções de habilitação das transições e as funções de disparos forçados das transições, as quais são construídas utilizando o procedimento de (Barroso, 1996) e o *Algoritmo para Construção do Processo de Decisão do Supervisor (ACPDs)*, aqui apresentado. Este último gera funções de comparação temporal para temporizadores introduzidos nas transições da rede, as quais permitem ao supervisor definir disparos forçados em determinadas transições quando os valores destes temporizadores ultrapassam os limites máximos de ocorrência dos eventos externos (respostas dos sensores ao sistema), assegurando a continuidade do processo. O procedimento apresentado garante a execução contínua do sistema sob controle, mesmo com a falha em alguns sensores.

## Referências

ALUR, R. and DILL, D. **A theory of timed automata**. Theoretical Computer Science, 1994, vol. 126. p.183–235.

BACCELLI, F., COHEN, G., OLSDER, G.J. and QUADRAT, J.P.. **Synchronisation and Linearity. An Algebra for Discrete Event Systems**. John Wiley Sons, 1992.

BARROSO, G.C. **Uma Nova Abordagem para a Síntese de Supervisores de Sistemas a Eventos Discretos**. 1996. Tese (Doutorado em Engenharia Elétrica). Universidade Federal da Paraíba, Campina Grande.

BRANDIN, B.A. and WONHAM, W.M. **Supervisory control of timed discrete-event systems**. IEEE Transactions on Automatic Control. fev.1994. vol. 39. p.329–342.

CHIRN, J-L. and McFARLANE, D.C. **Petri Nets Based Design of Ladder Logic Diagrams**. In: Control 2000, Cambridge, UK. set.2000.

CHRÉTIENNE, P. **Les Réseaux de Petri Temporisés**. Thèse d'état. Université Paris VI, Paris. 1983.

COFRANCESCO, P., CRISTOFORETTI, A. and SCATTOLINI, R. **Petri Nets Based Approach to Software Development for Real-Time Control**. IEE Proceedings-D Control Theory and Applications. maio, 1991, vol.138. p.474-478.

COSTA, E.M.M. **Síntese de Supervisores de Sistemas a Eventos Discretos Temporizados e Não Temporizados**. 2001. Tese (Doutorado em Engenharia Elétrica). Universidade Federal da Paraíba, Campina Grande.

COSTA, E.M.M. **Síntese de Supervisores de Sistemas a Eventos Discretos Temporizados Utilizando Autômatos com Temporização Variável**. In: CONGRESSO BRASILEIRO DE AUTOMÁTICA, 14. 2002, Natal. **Anais...** Natal: 2002 . p. 08.

FIGUEIREDO, J.C.A. **Redes de Petri com Temporização Nebulosa**. 1994. Tese (Doutorado em Engenharia Elétrica). Universidade Federal da Paraíba, Campina Grande.

FREY, G. **Automatic Implementation of Petri Net Based Control Algorithms on PLC**. In: Proc. of the American Control Conference. Chicago, Illinois. June, 2000. p. 2819-2823.

GAUBERT, S. **Performance evaluation of (max,+) automata**. IEEE Transactions on Automatic Control. dez.1995. vol.40. p.2014–2025.

GÓES, G.B.S. **Uma Abordagem para a Síntese de Supervisores de Sistemas a Eventos Discretos Utilizando Redes de Petri Síncronas**. 2003. Dissertação (Mestrado em Engenharia Elétrica). Universidade Federal da Bahia, Salvador.



HE, K.X. and LEMMON, M.D. **Petri Net Based Modeling and Analysis of Switched Systems**. In: Proc. of the 1998 IEEE, ISIC/CIRA/ISAS Joint Conference, Gaithersburg, MD. p.140-145.

HILAL, R. and LADET, P. **A Reactive Real-Time Systems Modeling and Programming Aid Tool Based on the Synchronous Petri Nets Formalism**. 1993. 0-8186-4250-5/93-IEEE. p.34-43.

HILAL, R. and LADET, P. **Synchronous Petri Nets: Formalization and Interpretation**. 1994. Laboratoire d'Automatique de Grenoble, ENSIEG/INPG.

HOPCROFT, J.E. and ULLMAN, J.D. **Introduction to Automata Theory, Languages and Computation**. Addison-Wesley, USA, 1979.

LIBEAUT, L. **Sur l'utilisation des Dioïdes pour la Commande des Systèmes a Événements Discrets**. 1996. Thèse de Doctorat. École Doctorale Sciences pour L'Ingenieur de Nantes.

RAMADGE, P.J.G. and WONHAM, W.M. **Supervision of discrete event processes**. In: Proceedings of 21st Conference on Decision and Control, 1982. p.1228–1229.

RAMADGE, P.J.G. and WONHAM, W.M. **The control of discrete event systems**. In: Proceedings of the IEEE, jan.1989. vol.77. p.81–98.

SILVA, V.P. **Uma Abordagem para a Síntese de Supervisores de Sistemas a Eventos Discretos a partir do Modelo Temporizado**. 1999. Dissertação (Mestrado em Engenharia Elétrica). Universidade Federal da Paraíba, Campina Grande.

UZAM, M., JONES, A.H. and AJLOUNI, N. **Conversion of Petri Nets Controllers for Manufacturing Systems Into Ladder Logic Diagrams**. 1996. Intelligent Machinery Division, Research Institute for Design, Manufacture and Marketing, University of Salford, UK.

ZHOU, M.C. and DiCESARE, F. **Petri Net Synthesis for Discrete Event Control of Manufacturing Systems**. Kluwer Academic Publishers. 1993.