Diagnostic temporel dans les systèmes répartis à l'aide de dépliages de réseaux de Petri temporels

Claude Jard — Thomas Chatain — Pierre Bourhis

IRISA/ENS Cachan
Campus de Beaulieu
F-35042 Rennes Cedex
Claude.Jard@bretagne.ens-cachan.fr

RÉSUMÉ. *La supervision et le diagnostic dans les systèmes répartis temps-réel est une question d'une grande actualité. Dans cet article, nous présentons le problème de la supervision comme la reconstruction des histoires cachées d'un modèle temporel, à partir de l'observation répartie d'événements. Nous utilisons une approche fondée sur une sémantique d'ordre partiel des réseaux de Petri temporels.*

ABSTRACT. *Monitoring real-time concurrent systems is a challenging task. In this paper we formulate (model-based) supervision by means of hidden state history reconstruction, from event (e.g. alarm) observations. We follow a so-called true concurrency approach using time Petri nets: the model defines explicitly the causal and concurrency relations between the observable events, produced by the system under supervision on different points of observation, and constrained by time aspects.*

MOTS-CLÉS : *supervision, diagnostic, systèmes répartis, réseaux de Petri temporels.*

KEYWORDS: *supervision, diagnosis, distributed systems, time Petri nets.*

1. Introduction

Face au déploiement plus ou moins bien contrôlé des réseaux de communication à grande échelle, la question du diagnostic (par exemple repérer les causes premières d'un fourmillement d'alarmes) ou plus généralement de la supervision, est d'une grande actualité. Depuis plusieurs années notre groupe à l'Irisa développe une approche originale fondée sur l'utilisation de sémantiques d'ordre partiel de modèles comme les réseaux de Petri (Benveniste *et al.*, 2003). Le problème de la supervision peut alors être formulé comme une « inversion de modèle », où il s'agit de reconstruire les histoires possibles du modèle, compatibles avec les observations réalisées (Pradin-Chézalviel *et al.*, 1999). Les observations se présentent elles-mêmes comme un ensemble de séquences indépendantes obtenues à travers un ensemble réparti de capteurs. L'objectif de la supervision est d'utiliser le modèle pour inférer les relations de causalité et de « concurrence » (« concurrency » en anglais) entre les événements observés. Les ambiguïtés inévitables dans les observations conduisent à construire tout un ensemble d'explications possibles. Celles-ci peuvent être représentées efficacement par la notion de dépliage des réseaux de Petri.

Cet article présente l'introduction du temps dans cette problématique. L'idée est que les comportements du système observé peuvent être expliqués par un réseau de Petri contraint par le temps. L'algorithmique de diagnostic, non seulement infère les causalités, mais calcule aussi les dates possibles d'occurrence de chacun des événements observés. Techniquement, elle s'appuie sur une notion de dépliage symbolique des réseaux de Petri temporels ; notion qui n'avait pas été vraiment explorée jusqu'à présent.

L'article commence par formaliser le problème du diagnostic en présentant notamment le modèle des réseaux de Petri temporels et leur sémantique d'ordre partiel. Dans une deuxième partie est présentée l'algorithmique de diagnostic s'appuyant sur la notion de dépliage symbolique. Un petit exemple jouet sert d'illustration tout au long de l'article.

2. Le problème du diagnostic dans le cadre des modèles d'ordre partiel

2.1. *Architecture*

Considérons un système réparti formé d'un ensemble de composants en interaction. Chaque composant, par l'intermédiaire d'un capteur, est susceptible d'émettre des événements de gestion (des alarmes par exemple dans le cas du diagnostic de panne) à destination d'un site de supervision, que nous supposons ici centralisé[1]. Nous faisons l'hypothèse que chaque capteur émet en séquence ses événements, qu'ils ne sont pas perdus et que l'ordre total présenté n'est pas en contradiction avec l'ordre

1. Les méthodes et algorithmes que nous présentons dans cet article peuvent être en fait répartis sur les différents capteurs, mais ce n'est pas le sujet principal ici.

partiel défini dans le modèle (hypothèse *d'observation causale*). Ces événements remontent donc de façon indépendante vers le superviseur qui a pour tâche de retrouver leurs dépendances causales à partir du modèle proposé, sachant que les dépendances entre capteurs sont inconnues et que l'ordre sur un capteur est un entrelacement arbitraire. Cette architecture est illustrée dans la figure 1.

Dans notre exemple, nous avons considéré que le système supervisé était composé de deux machines A et B équipées chacune d'un capteur. Les capteurs font remonter indépendamment les événements de panne (α et β) et de réparation (ρ et ρ'). Imaginons par exemple la production de la séquence $\beta\rho\beta$ sur le capteur de A, et de la séquence $\alpha\rho'$ sur le capteur de B. Étant donné le modèle décrit dans le diagnostiqueur de la figure 1, celui-ci doit produire l'ensemble des explications possibles compatibles avec les observations. Précisément, les explications sont des exécutions (d'ordre partiel) possibles du modèle contenant l'ensemble des événements observés. On voit dans la figure 1 à droite que le diagnostiqueur infère les dépendances causales ainsi que les plages de retard autorisées sur chaque événement. L'existence de plusieurs explications possibles est due aux ambiguïtés (plusieurs actions du modèle correspondent au même événement observé). Les retards associés à chaque événement sont donnés par un système de contraintes représenté sous le graphe de l'ordre partiel.

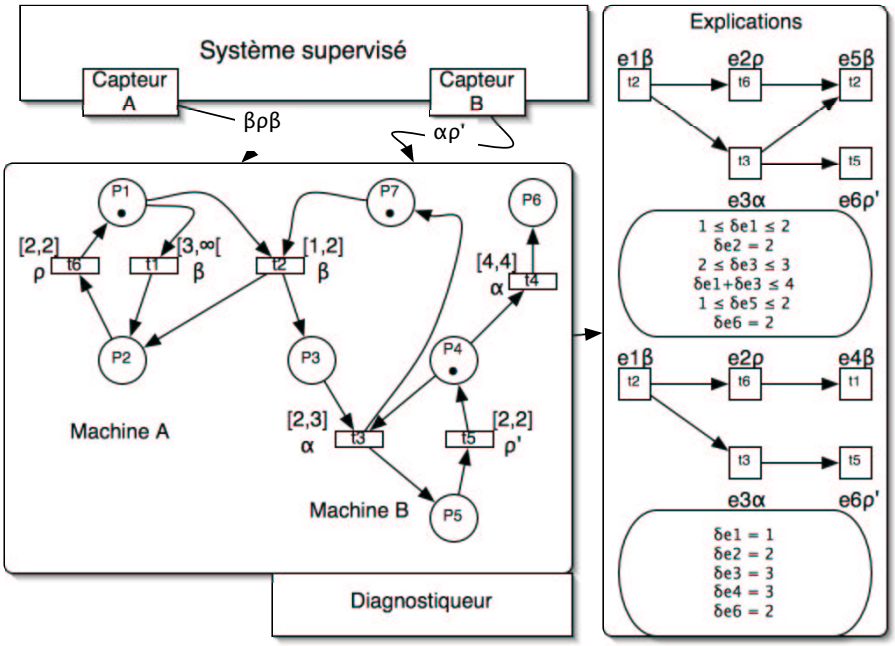

Figure 1. *Diagnostic temporel dans un système réparti à l'aide d'un modèle de réseau de Petri*

2.2. *Réseaux de Petri temporels : définition*

Nous utilisons les réseaux de Petri temporels tels qu'introduits en 1976 par P. Merlin (Merlin *et al.*, 1976). Q est l'ensemble des nombres rationnels.

Un *réseau de petri temporel* (RdPT) est un n-uplet $R \stackrel{\text{def}}{=} \langle P, T, \mathit{pre}, \mathit{post}, \mathit{dmin}, \mathit{dmax}\rangle$, dans lequel P et T sont respectivement des ensembles finis non vides de *places* et de *transitions*, *pre* et *post* associent à chaque transition $t \in T$ sa *pré-condition* notée ${}^\bullet t \stackrel{\text{def}}{=} \mathit{pre}(t) \subseteq P$ (${}^\bullet t \neq \emptyset$) et sa *post-condition* notée $t^\bullet \stackrel{\text{def}}{=} \mathit{post}(t) \subseteq P$; $\mathit{dmin} : T \longrightarrow Q$ et $\mathit{dmax} : T \longrightarrow Q \cup \{\infty\}$ donnent la *date de tir au plus tôt* $\mathit{dmin}(t)$ et la *date de tir au plus tard* $\mathit{dmax}(t)$ pour chaque transition t. Un RdPT est représenté par un graphe avec deux types de nœuds : les places (les ronds) et les transitions (les rectangles). L'intervalle fermé $[\mathit{dmin}(t), \mathit{dmax}(t)]$ est écrit à côté de chaque transition. Pour le problème de la supervision, il faut rajouter la désignation des événements observables dans les réseaux de Petri. C'est pourquoi nous considérons les *réseaux étiquetés* $\langle R, \Lambda, \lambda\rangle$ dans lesquels Λ est un ensemble de types d'événements (ou alarmes), et λ est la fonction de typage des transitions ($\alpha, \beta, \rho, \rho'$ dans la figure 1).

L'*état* (global) d'un RdPT est défini par un triplet $\langle M, \mathit{dn}, \theta\rangle$, dans lequel $M \subseteq P$ est un *marquage* défini par la présence de jetons dans les places (les points noirs), $\theta \in Q$ est sa date et $\mathit{dn} : M \longrightarrow Q$ donne la *date de naissance* $\mathit{dn}(p) \leq \theta$ de chacun des jetons du marquage $p \in M$.

Une exécution (on dira aussi processus) d'un RdPT démarre dans un *état initial* $\langle M_0, \mathit{dn}_0, \theta_0\rangle$, donné par le *marquage initial* M_0 et sa date θ_0. Initialement, tous les jetons naissent à θ_0 : $\forall p \in M_0 \quad \mathit{dn}_0(p) \stackrel{\text{def}}{=} \theta_0$.

Une transition t peut tirer à la date θ' dans l'état $\langle M, \mathit{dn}, \theta\rangle$, si :

– t est tirable : ${}^\bullet t \subseteq M$;

– le retard minimum est écoulé : $\theta' \geq \max_{p \in {}^\bullet t} + \mathit{dmin}(t)$;

– le temps global progresse : $\theta' \geq \theta$;

– toutes les transitions tirables accumulent un retard inférieur au retard maximum : $\forall t' \in T \quad {}^\bullet t' \subseteq M \implies \theta' \leq \max_{p \in {}^\bullet t'} \mathit{dn}(p) + \mathit{dmax}(t')$.

Le tir de t à la date θ' conduit à l'état $\langle (M \setminus {}^\bullet t) \cup t^\bullet, \mathit{dn}', \theta'\rangle$, dans lequel $\mathit{dn}'(p) \stackrel{\text{def}}{=} \mathit{dn}(p)$ si $p \in M \setminus {}^\bullet t$ et $\mathit{dn}'(p) \stackrel{\text{def}}{=} \theta'$ si $p \in t^\bullet$.

Tous les réseaux que nous considérons dans cet article sont *saufs*, c'est-à-dire que pour chaque état accessible $\langle M, \mathit{dn}, \theta\rangle$, si une transition t est tirable dans $\langle M, \mathit{dn}, \theta\rangle$, alors $t^\bullet \cap (M \setminus {}^\bullet t) = \emptyset$.

De plus, nous exigeons que le temps diverge : si une infinité de transitions sont tirées, le temps doit tendre vers l'infini.

Si nous regardons le modèle RdPT utilisé dans l'exemple de la figure 1, on voit que la machine A a deux modes de passage à l'état de panne temporaire. Par la transition t_1, la panne reste circonscrite à la machine, alors qu'elle se propage à la machine

B par la transition t_2. On indique que le phénomène de propagation est plus rapide que le premier type de panne (par exemple car il prend sa source dans une couche de communication plus basse dans l'architecture). La machine A peut ensuite signaler sa réparation par la transition t_6. La machine B possède aussi deux modes de pannes : le premier est simplement une panne cascadée provoquée par la propagation de la panne de la machine A (transition t_3) ; le deuxième est une panne définitive déclenchée par exemple par un temporisateur du durée 4 (transition t_4). Il est à noter que conformément à la sémantique, les comportements temporisés sont un sous-ensemble des comportements du réseau non temporisé sous-jacent. Dans notre exemple, l'explication séquentielle $t_1.t_6.t_2.t_3.t_5$, compatible avec les alarmes observées du point de vue logique est rejetée à cause des contraintes temporelles. En effet la transition t_1 ne peut pas être tirée initialement car elle perd la compétition avec la transition de propagation t_2. De façon plus subtile, on constate aussi dans l'explication du haut de la figure que la somme des retards devant les transitions t_2 et t_3 ne peut pas excéder 4, car sinon la transition t_4 aurait tiré avant, bloquant la machine B et empêchant ainsi l'explication de l'alarme ρ'.

2.3. *La sémantique d'ordre partiel de ces réseaux*

2.3.1. *Processus*

Les exécutions d'ordre partiel, ou processus, en utilisant la terminologie de la théorie des réseaux (Aura *et al.*, 1997), sont codés dans un ensemble X, défini inductivement comme dans (Engelfriet, 1991).

Chaque processus est un couple $x \stackrel{\text{def}}{=} \langle E, \Theta \rangle$, dans lequel E est un ensemble *d'événements* représentant les occurrences des transitions du réseau de Petri, et $\Theta : E \longrightarrow Q$ la fonction donnant la date de tir de chacun d'eux. Θ sera quelquefois donné par l'ensemble de ses couples $(e, \Theta(e))$.

Chaque événement est lui-même un couple $e \stackrel{\text{def}}{=} ({}^\bullet e, \tau(e))$ qui représente l'occurrence de la transition $\tau(e)$ dans le processus, associée à une condition d'activation donnée par un ensemble de places marquées du réseau. ${}^\bullet e$ est l'ensemble des *conditions* $b \stackrel{\text{def}}{=} ({}^\bullet b, \mathit{place}(b)) \in E \times P$. Un tel couple code le fait que l'événement ${}^\bullet b$ a produit un jeton dans la $\mathit{place}(b)$. On dit que l'événement e *consomme* les conditions de ${}^\bullet e$. Symétriquement, l'ensemble des conditions $\{(e, p) \mid p \in \tau(e)^\bullet\}$ *créées* par e est noté $e^\bullet$.

Soit B un ensemble de conditions, on note $\mathit{Place}(B) \stackrel{\text{def}}{=} \{\mathit{place}(b) \mid b \in B\}$, et lorsque la restriction de *place* à B est injective, son inverse est noté place_B^{-1}. Pour tout sous-ensemble $B' \subseteq B$, $\mathit{Place}_B^{-1}(B') \stackrel{\text{def}}{=} \{\mathit{place}_B^{-1}(b) \mid b \in B'\}$. Étant donné un ensemble E d'événements, on note $\mathit{cnds}(E) \stackrel{\text{def}}{=} \bigcup_{e \in E} e^\bullet$ l'ensemble des conditions créées par ces événements.

L'ensemble des conditions qui restent à la fin du processus $\langle E, \Theta \rangle$ (celles qui n'ont pas de successeurs) est $\uparrow(E) \stackrel{\text{def}}{=} \bigcup_{e \in E} e^\bullet \setminus \bigcup_{e \in E} {}^\bullet e$. Elles définissent une notion d'état

atteint par le processus par $\langle \mathit{Place}(\uparrow(E)), \mathit{dn}, \max_{e \in E} \Theta(e) \rangle$, où $\forall p \in \mathit{Place}(\uparrow(E))$, $\mathit{dn}(p) \stackrel{\text{def}}{=} \Theta({}^\bullet b)$, avec $b \stackrel{\text{def}}{=} \mathit{place}^{-1}_{\uparrow(E)}(p)$.

Nous définissons aussi la relation de dépendance $\rightarrow$ sur E comme : $e \rightarrow e'$ ssi $e^\bullet \cap {}^\bullet e' \neq \emptyset$.
Sa fermeture réflexo-transitive $\rightarrow^*$ définit la relation de *causalité* sur E. On note $\lceil e \rceil$, l'ensemble des prédécesseurs causaux de l'événement e : $\lceil e \rceil \stackrel{\text{def}}{=} \{e' \in E \mid e' \rightarrow^* e\}$. Pour tout ensemble F d'événements, on note $\lceil F \rceil \stackrel{\text{def}}{=} \bigcup_{f \in F} \lceil f \rceil$.

On peut définir maintenant l'ensemble des processus finis d'un réseau de Petri temporel démarrant à la date θ_0 dans le marquage initial M_0 inductivement comme suit :

– $\langle \{\perp\}, \{(\perp, \theta_0)\} \rangle \in X$, où $\perp \stackrel{\text{def}}{=} (\emptyset, \epsilon)$ représente l'événement initial. Noter que cet événement est initial ne code pas concrètement le tir d'une transition ; c'est pourquoi nous introduisons la transition fictive $\epsilon \notin T$. Pour la même raison, les conditions créées par $\perp$ sont spécifiques : $\perp^\bullet \stackrel{\text{def}}{=} \{(\perp, p) \mid p \in M_0\}$.

– Pour tous les processus $\langle E, \Theta \rangle \in X$ menant à l'état $\langle M, \mathit{dn}, \theta \rangle$, si une transition t peut tirer à la date θ' dans cet état, alors $\langle E \cup \{e\}, \Theta \cup \{(e, \theta')\} \rangle \in X$, où l'événement $e \stackrel{\text{def}}{=} (\mathit{Place}^{-1}_{\uparrow(E)}({}^\bullet t), t)$ représente le tir de t.

Dans les représentations des processus, en cohérence avec les notations temporelles des réseaux de Petri, nous ferons figurer le retard au tir de chaque événement $e \neq \perp$ défini par : $\delta(e) \stackrel{\text{def}}{=} \Theta(e) - \max_{b \in {}^\bullet e} \Theta({}^\bullet b)$.

2.3.2. *Processus symboliques*

En général, à cause de la nature dense du temps, il existe une infinité de processus présentant la même structure causale sur les mêmes événements et ne différant donc que par les valeurs des retards sur les événements. Nous choisissons de les grouper dans un même *processus symbolique*. L'idée de regrouper ces histoires a déjà été explorée dans le cadre de la sémantique entrelacée des réseaux de Petri temporels (Berthomieu *et al.*, 1991, Berthomieu *et al.*, 2003).

Un *processus symbolique* d'un réseau de Petri temporel est un couple $\langle E, \mathit{pred} \rangle$ avec $\mathit{pred} : (E \longrightarrow Q) \longrightarrow \textbf{bool}$, tel que pour toute application $\Theta : E \longrightarrow Q$, si $\mathit{pred}(\Theta)$, alors $\langle E, \Theta \rangle \in X$.

En pratique, *pred* est décrit par un système d'inéquations linéaires. La figure 1 montre les deux processus symboliques qui constituent en fait les explications que doit fournir le diagnostiqueur sur notre exemple. Le codage de l'explication du bas par exemple est donné par :

$$\begin{array}{ll}
e_1 = (\{(\perp, P_1), (\perp, P_7)\}, t_2) & \delta(e_1) = 1 \\
e_2 = (\{(e_1, P_2)\}, t_6) & \delta(e_2) = 2 \\
e_3 = (\{(\perp, P_4), (e_1, P_3)\}, t_3) & \delta(e_3) = 3 \\
e_4 = (\{(e_2, P_1)\}, t_1) & \delta(e_4) = 3 \\
e_5 = (\{(e_3, P_5)\}, t_5) & \delta(e_5) = 2
\end{array}$$

2.4. *Le guidage par les observations*

Considérons un réseau R modélisant un système réparti et une observation O de ce système, donnée sous la forme d'un ensemble de séquences d'alarmes observées $(\lambda_{s,1}, \ldots, \lambda_{s,n_s})$ par chaque capteur s. L'ensemble des capteurs est noté S. $\Lambda_s \subseteq \Lambda$ désigne les alarmes observées par le capteur s. Chaque alarme pouvant indiquer le capteur qui l'a produit, nous considérons que Λ est partitionné sur S.

Le calcul du diagnostic, guidée par les observations, va s'appuyer sur un dépliage du modèle du système plongé dans son architecture d'observation. Pour cela, nous allons représenter les observations par un autre réseau de Petri temporel. Le réseau à déplier, noté $\mathcal{D}(R, O)$, sera la composition des deux réseaux à travers une interface définissant formellement la façon dont les observations sont remontées au superviseur. Cette interface est matérialisée par les places s_λ et $\overline{s_\lambda}$. Les transitions $t_{s,\lambda}$ empêchent les jetons de séjourner dans les places s_λ.

Formellement, pour un réseau $R \stackrel{\text{def}}{=} \langle P, T, \mathit{pre}, \mathit{post}, \mathit{dmin}, \mathit{dmax} \rangle$ et une observation O obtenue à partir d'un ensemble S de capteurs, nous définissons un réseau $\mathcal{D}(R, O) \stackrel{\text{def}}{=} \langle P', T', \mathit{pre}', \mathit{post}', \mathit{dmin}', \mathit{dmax}' \rangle$ comme suit[2] :

– $P' \stackrel{\text{def}}{=} P \uplus \{p_{s,i} \mid s \in S,\ i = 0, \ldots, n_s\} \uplus \biguplus_{\substack{s \in S \\ \lambda \in \Lambda_s}} \{s_\lambda, \overline{s_\lambda}, \widetilde{s_\lambda}\}$;

– $T' \stackrel{\text{def}}{=} T \uplus \{t_{s,i} \mid s \in S,\ i = 1, \ldots, n_s\} \uplus \{t_{s,\lambda} \mid s \in S \ \wedge\ \lambda \in \Lambda_s\}$;

– $\forall t \in T \quad \begin{cases} \mathit{pre}'(t) \stackrel{\text{def}}{=} \mathit{pre}(t) \uplus \{\overline{s_{\lambda(t)}} \mid \lambda(t) \in \Lambda_s\} \\ \mathit{post}'(t) \stackrel{\text{def}}{=} \mathit{post}(t) \uplus \{s_{\lambda(t)} \mid \lambda(t) \in \Lambda_s\} \\ \mathit{dmin}'(t) \stackrel{\text{def}}{=} \mathit{dmin}(t) \quad \text{et} \quad \mathit{dmax}'(t) \stackrel{\text{def}}{=} \mathit{dmax}(t) \end{cases}$

– $\forall s \in S \quad \forall i \in \{1, \ldots, n_s\} \quad \begin{cases} \mathit{pre}'(t_{s,i}) \stackrel{\text{def}}{=} \{p_{s,i-1}, s_{\lambda_{s,i}}\} \\ \mathit{post}'(t_{s,i}) \stackrel{\text{def}}{=} \{p_{s,i}, \overline{s_{\lambda_{s,i}}}\} \\ \mathit{dmin}'(t_{s,i}) = \mathit{dmax}'(t_{s,i}) \stackrel{\text{def}}{=} 0 \end{cases}$

– $\forall s \in S \quad \forall \lambda \in \Lambda_s \quad \begin{cases} \mathit{pre}'(t_{s,\lambda}) \stackrel{\text{def}}{=} \{s_\lambda\} \quad \text{et} \quad \mathit{post}'(t_{s,\lambda}) \stackrel{\text{def}}{=} \{\widetilde{s_\lambda}\} \\ \mathit{dmin}'(t_{s,\lambda}) = \mathit{dmax}'(t_{s,\lambda}) \stackrel{\text{def}}{=} 0 \end{cases}$

Le marquage initial de $\mathcal{D}(R, O)$ est

$$M'_0 \stackrel{\text{def}}{=} M_0 \uplus \{p_{s,1} \mid s \in S\} \uplus \{\overline{s_\lambda} \mid s \in S \ \wedge\ \lambda \in \Lambda_s\}.$$

La figure 2 montre le réseau de la figure 1 guidée par les observations $\beta\rho\beta$ du capteur A et $\alpha\rho'$ du capteur B. Pour la lisibilité, nous n'avons pas donné le nom des places et transitions de l'environnement, ni leurs contraintes temporelles, toutes positionnées à $[0, 0]$, et nous n'avons pas représenté les places $\widetilde{s_\lambda}$.

2. Nous supposons que si deux événements d'un même processus correspondent à des transitions étiquetées par la même alarme, alors ils sont causalement liés. Si cette hypothèse n'est pas vérifiée, il existe une construction plus complexe.

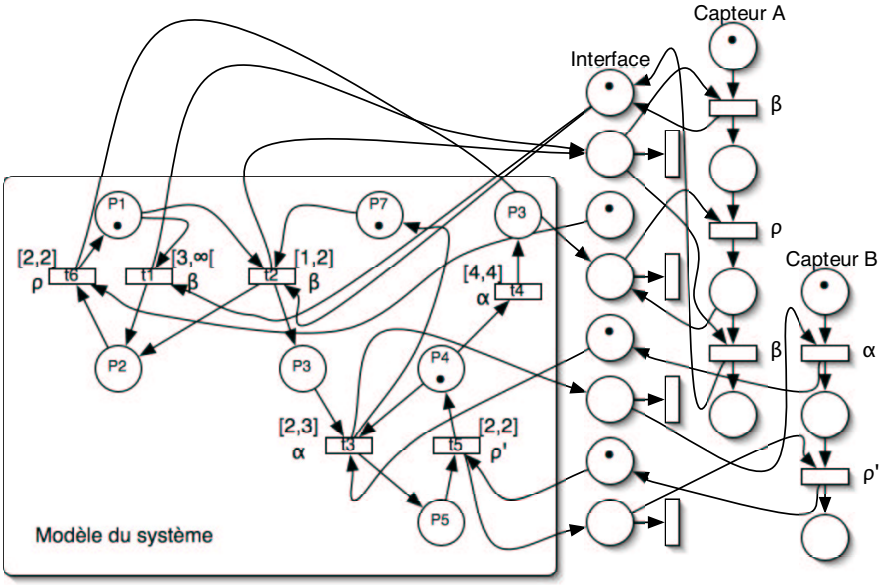

Figure 2. *Notre exemple de modèle de système guidé par les observations $\beta\rho\beta$ du capteur A et $\alpha\rho'$ du capteur B*

Nous appelons *diagnostic de l'observation O par le réseau R* tout ensemble fini de processus symboliques de $\mathcal{D}(R, O)$, qui contient tous les processus $\langle E, \Theta\rangle$ de $\mathcal{D}(R, O)$ tels que : $\{p_{s,n_s} \mid s \in S\} \uplus \{\overline{s_\lambda} \mid s \in S \ \wedge \ \lambda \in \Lambda_s\} \subseteq \mathit{Place}(\uparrow(E))$. Ces processus peuvent être projetés sur les transitions du réseau initial modélisant le système. On obtient alors tous les processus de R compatibles avec l'observation O. La figure 1 montre le diagnostic obtenu dans le cas de notre exemple.

Dans la suite, nous allons utiliser la notion de dépliage pour obtenir une représentation compacte des processus partageant des préfixes communs. Le cadre temporel dans lequel nous nous plaçons oblige à définir la notion nouvelle de dépliage symbolique des réseaux de Petri temporels, détaillée dans la partie suivante de l'article.

3. Dépliage symbolique de réseaux de Petri temporels

La notion de dépliage symbolique a déjà été introduite dans (Chatain *et al.*, 2004) pour traiter des systèmes dont la structure change dynamiquement. Nous réutilisons ici les mêmes principes pour traiter les contraintes temporelles. La situation est complexe car décider si une transition est tirable n'est pas a priori une fonction locale : elle doit rester tirable pendant un certain laps de temps défini par le retard minimum de la transition. Pendant ce temps donc, on doit

assurer que la transition reste sensibilisée, c'est-à-dire que les possibles transitions en conflit n'ont pas tiré. Mais le fait que les transitions en conflit n'ont pas tiré dépend des dates de naissance des jetons dans leurs places d'entrées, qui elles-mêmes dépendent du tir des transitions en amont, et ainsi de suite… Ce type de situation est évitée dans la sous-classe des réseaux dite à « choix libre étendu » (« extended free-choice » en anglais). Dans cette classe, que nous considérons d'abord pour faire simple, le dépliage pourra être vu comme une simple union de l'ensemble des processus. Dans le cas général, nous proposons une structure de dépliage qui, au prix de quelques duplications éventuelles de transitions, représente de façon compacte l'ensemble des processus tout en permettant leur extraction rapide. Seuls les théorèmes sont énoncés. Les preuves correspondantes peuvent être consultées dans (Chatain *et al.*, 2005).

3.1. *Pré-processus*

Pour construire le dépliage symbolique des réseaux de Petri temporels, nous avons besoin de la notion de *pré-processus*, qui étend la notion de processus : pour tous les processus $\langle E, \Theta \rangle$, et pour tous les ensembles causalement clos d'événements $E' \subseteq E$ ($\perp \in E'$ et $\lceil E' \rceil = E'$), $\langle E', \Theta' \rangle$ est appelé un *pré-processus* (où Θ' est la restriction de Θ à E'). La définition de l'état après un processus s'applique aussi aux pré-processus. Nous définissons la relation *préfixe* $\leq$ sur les pré-processus par :

$$\langle E, \Theta \rangle \leq \langle E', \Theta' \rangle \text{ ssi } \begin{cases} E \subseteq E' \\ \forall e \in E \quad \Theta'(e) = \Theta(e) \end{cases}$$

On peut décider si un pré-processus $\langle E, \Theta \rangle$ est ou non un processus : soit $\langle M, \mathit{dn}, \theta \rangle$ l'état atteint après $\langle E, \Theta \rangle$; $\langle E, \Theta \rangle$ est un processus ssi :

$$\forall t \in T \quad {}^\bullet t \subseteq M \implies \theta \leq \mathit{dmax}(t) + \max_{p \in {}^\bullet t} \mathit{dn}(p).$$

3.2. *Le cas des réseaux à choix libre (étendu)*

Un réseau de Petri temporel *à choix libre étendu* (Best, 1987) est un réseau tel que : $\forall t, t' \in T \quad {}^\bullet t \cap {}^\bullet t' \neq \emptyset \implies {}^\bullet t = {}^\bullet t'$.

On définit son *dépliage symbolique* U par l'union de tous les événements qui apparaissent dans les processus : $U \stackrel{\text{def}}{=} \bigcup_{\langle E, \Theta \rangle \in X} E$.

Théorème 1 (Extraction des pré-processus) *Soit $E \subseteq U$ un ensemble fini non vide d'événements et $\Theta : E \longrightarrow Q$ une fonction de datation. $\langle E, \Theta \rangle$ est un pré-processus ssi :*

$$\begin{cases} \lceil E \rceil = E & \textit{(E est clos par causalité)} \\ \nexists e, e' \in E \quad e \neq e' \ \wedge \ {}^\bullet e \cap {}^\bullet e' \neq \emptyset & \textit{(E est sans conflit)} \\ \forall e \in E \quad \textit{dmin}(\tau(e)) \leq \Theta(e) - \textit{da}(\tau(e)) \leq \min_{\substack{t' \in T \\ {}^\bullet t' = {}^\bullet t}} \textit{dmax}(t') & \\ & \textit{(tous les retards de tir sont respectés)} \end{cases}$$

où $\textit{da}(t) \stackrel{\text{def}}{=} \max_{b \in {}^\bullet e} \Theta({}^\bullet b)$.

Théorème 2 (Construction du dépliage) $\forall e \stackrel{\text{def}}{=} (B, t) \in \textit{cnds}(U) \times T$,

$$e \in U \textit{ ssi } \begin{cases} \textit{Place}(B) = {}^\bullet t \\ \nexists f, f' \in \lceil e \rceil \quad f \neq f' \ \wedge \ {}^\bullet f \cap {}^\bullet f' \neq \emptyset \\ \textit{dmin}(t) \leq \min_{\substack{t' \in T \\ {}^\bullet t' = {}^\bullet t}} \textit{dmax}(t') \end{cases}$$

3.3. *Le cas général*

Les théorèmes précédents deviennent peu utilisables en pratique si on lève la restriction de choix libre étendu. L'extraction des processus devient un calcul complexe comme énoncé dans (Aura *et al.*, 1997)), conformément à la non-localité de la résolution des contraintes temporelles que nous avons déjà annoncée. Pour, en quelque sorte, expliciter (et localiser) les contraintes, nous supposons connue une partition de l'ensemble P des places du réseau en ensembles $P_i \subseteq P$ de places mutuellement exclusives[3] ; plus précisément on exige que pour tout marquage atteignable M, $P_i \cap M$ soit un singleton. Pour toute place $p \in P_i$, on note $\bar{p} \stackrel{\text{def}}{=} P_i \setminus \{p\}$.

Dans l'exemple de la figure 1, nous utiliserons la partition $\{p_1, p_2\}$, $\{p_3, p_7\}$, $\{p_4, p_5, p_6\}$. Pour l'application au diagnostic présentée dans la partie 2.4, pour tout s, λ, les places s_λ, $\overline{s_\lambda}$ et $\widetilde{s_\lambda}$ sont mutuellement exclusives, ainsi que les places $p_{s,i}$, $i = 0, \ldots, n_s$ pour tout s.

3.3.1. *Sémantique de tir locale*

La notion *d'état local* d'un réseau de Petri temporel rassemble les informations nécessaires pour la décision de tir d'une transition. Elle est formellement définie par un triplet $\langle L, \textit{dn}, \theta \rangle$ avec $L \subseteq P$, $\theta \in Q$ est la date de l'état et la fonction $\textit{dn} : L \longrightarrow Q$ donne la date de naissance $\textit{dn}(p) \leq \theta$ de chaque jeton $p \in L$.

3. Si l'on ne connaît pas de telle partition, une solution consiste à étendre la structure du réseau de Petri avec une place complémentaire par place du réseau et à ajouter ces places en entrée et en sortie des transitions de telle sorte que toute place $p \in P$ du réseau soit pleine ssi sa place complémentaire est vide. Cette construction ne change pas le comportement du réseau (en faisant l'hypothèse que le réseau de Petri sans les contraintes de temps est sauf).

Reprenant la sémantique des RdPT de la section 2.2, mais en utilisant la notion d'état local plutôt que la notion de marquage global habituel, on dit qu'une transition t est *localement-tirable* à la date θ' depuis l'état local $\langle L, dn, \theta\rangle$ ssi :

$$\begin{cases} {}^\bullet t \subseteq L \\ \theta' \geq \max_{p \in {}^\bullet t} dn(p) + dmin(t) \\ \theta' \geq \theta \\ \forall t' \in T \quad {}^\bullet t' \cap L \neq \emptyset \implies \begin{cases} & \exists p \in {}^\bullet t' \quad \bar{p} \cap L \neq \emptyset \\ \vee & \theta' \leq \max_{p \in {}^\bullet t' \cap L} dn(p) + dmax(t'). \end{cases} \end{cases}$$

Cette nouvelle sémantique locale généralise la sémantique habituelle qui se trouve être un cas particulier lorsque l'on choisit les ensembles L dans les marquages du réseau.

Il arrive qu'une transition t puisse localement-tirer à la date θ' depuis un état local $\langle L, dn, \theta\rangle$ et aussi depuis un état $\langle L', dn', \theta\rangle$ tel que $L \subsetneq L'$ et dn' est la restriction de dn à L'. On choisira alors de ne considérer que les $\langle L, dn, \theta\rangle$ minimaux, car ils suffiront à exprimer tous les comportements du réseau.

3.3.2. *Processus étendus*

La notion de processus doit donc être elle-aussi généralisée. La différence réside dans le fait que les événements portent plus d'information : nous avons décidé de garder en mémoire les états locaux dans les conditions des événements (dans la sémantique ordinaire standard, seules les places vidées par la transition sont gardées).

Pour les événements étendus $\dot{e} \stackrel{\text{def}}{=} \langle B, t\rangle$, nous utilisons les mêmes notations que pour les événements simples : ${}^\bullet\dot{e} \stackrel{\text{def}}{=} B$ et $\tau(\dot{e}) \stackrel{\text{def}}{=} t$, et nous définissons $\dot{e}^\bullet \stackrel{\text{def}}{=} \{(\dot{e}, p) \mid p \in (Place(B) \setminus {}^\bullet t) \cup t^\bullet\}$. Étant donnée une place $p \in Place(\dot{e}^\bullet)$, nous notons $src(p, \dot{e})$ l'événement qui pose le jeton dans la place p[4] :

$$src(p, \dot{e}) \stackrel{\text{def}}{=} \begin{cases} \dot{e} & \text{si } p \in t^\bullet \text{ ou } \dot{e} = \perp \\ src(p, {}^\bullet b) \text{ avec } b \stackrel{\text{def}}{=} place_B^{-1}(p) & \text{sinon} \end{cases}$$

Comme pour les processus simples, l'ensemble des conditions présentes à la fin du processus étendu est $\langle \dot{E}, \Theta\rangle$ as $\uparrow(\dot{E}) \stackrel{\text{def}}{=} \bigcup_{\dot{e} \in \dot{E}} \dot{e}^\bullet \setminus \bigcup_{\dot{e} \in \dot{E}} {}^\bullet\dot{e}$. La différence est que l'on doit calculer aussi le nouvel état local associé aux ensembles de conditions $B \subseteq \uparrow(\dot{E})$. Il est défini par $\langle L, dn_L, \theta_L\rangle$, où :

– $L \stackrel{\text{def}}{=} Place(B)$,

– $dn_L(p) \stackrel{\text{def}}{=} \Theta(src(p, {}^\bullet b))$ avec $b \stackrel{\text{def}}{=} place_B^{-1}(p)$,

– $\theta_L \stackrel{\text{def}}{=} \max_{b \in B} \Theta({}^\bullet b)$.

4. Nous savons que pour les réseaux généraux, cette place peut être éloignée de la transition considérée.

L'ensemble $\dot{X}$ des *processus étendus* d'un réseau de Petri temporel démarrant à θ_0 dans le marquage initial M_0 est défini inductivement par :

– Comme pour les processus simples, $\langle\{\perp\},\{(\perp,\theta_0)\}\rangle \in \dot{X}$, où $\perp \stackrel{\text{def}}{=} (\emptyset,\epsilon)$ représente l'événement initial. L'ensemble des conditions créées par $\perp$ est : $\perp^\bullet \stackrel{\text{def}}{=} \{(\perp,p) \mid p \in M_0\}$.

– Étant donné un processus étendu $\langle\dot{E},\Theta\rangle \in \dot{X}$, pour tout $B \subseteq \uparrow(\dot{E})$ menant à un état local S, si une transition t peut localement-tirer depuis S à la date θ', alors $\langle\dot{E}\cup\{\dot{e}\},\Theta\cup\{(\dot{e},\theta')\}\rangle \in \dot{X}$.

Un événement étendu $\dot{e} \stackrel{\text{def}}{=} (B,t)$ peut être projeté sur l'événement simple correspondant $h(\dot{e}) \stackrel{\text{def}}{=} (B',t)$ avec $B' \stackrel{\text{def}}{=} \Big\{\big(h(\mathit{src}(p,\dot{f})),p\big) \mid (\dot{f},p) \in \mathit{Place}_B^{-1}({}^\bullet t)\Big\}$.

Théorème 3 (Validité des processus étendus) *Pour tout processus étendu $\langle\dot{E},\Theta\rangle \in \dot{X}$, $\langle h(\dot{E}),\Theta\circ h_{\dot{E}}^{-1}\rangle$ est un pré-processus (où $\circ$ est la composition habituelle des fonctions, et $h_{\dot{E}}^{-1}$ l'inverse de la restriction de h à $\dot{E}$, qui est bijective).*

En d'autres termes, il existe un processus $\langle E',\Theta'\rangle \in X$ tel que $\langle h(\dot{E}),\Theta\circ h_{\dot{E}}^{-1}\rangle \leq \langle E',\Theta'\rangle$. $\langle E',\Theta'\rangle$ peut être choisi tel que $\max\limits_{e'\in E'}\Theta'(e') = \max\limits_{\dot{e}\in\dot{E}}\Theta(\dot{e})$.

Théorème 4 (Complétude des processus étendus) *Pour tout processus $\langle E,\Theta\rangle \in X$, il existe un processus étendu $\langle\dot{E},\Theta'\rangle \in \dot{X}$ tel que $\langle h(\dot{E}),\Theta'\circ h_{\dot{E}}^{-1}\rangle = \langle E,\Theta\rangle$.*

À ce point, nous sommes assurés que la collection des processus étendus donne la même information que la collection des processus. L'intérêt maintenant est que le dépliage va pouvoir être défini comme étant la simple union des processus étendus, ce qui était ineffectif avec les processus dans le cas général.

D'un point de vue pratique, il est important de constater que les processus étendus sont effectivement calculables puisque les quantificateurs $\forall$ et $\exists$ sur les places et les transitions s'écrivent en un ensemble fini de disjonctions et de conjonctions. Le résultat est un système fini d'inéquations linéaires sur les $\Theta(\dot{e})$ comme on le voit sur la figure 3.

3.3.3. *Dépliage symbolique*

Comme nous l'avons fait pour les réseaux à choix libre étendu, le *dépliage symbolique* U d'un RdPT est l'union des événements étendus qui apparaissent dans les processus étendus : $U \stackrel{\text{def}}{=} \bigcup_{\langle\dot{E},\Theta\rangle\in\dot{X}} \dot{E}$.

Nous avons alors les théorèmes correspondants pour l'extraction des processus et la construction du dépliage.

Théorème 5 *Soit $\dot{E} \subseteq U$ un ensemble fini non vide d'événements étendus et $\Theta : \dot{E} \longrightarrow Q$ une fonction de datation. $\langle \dot{E}, \Theta \rangle$ est un processus étendu ssi :*

$$\begin{cases} \lceil \dot{E} \rceil = \dot{E} & \textit{(}\dot{E}\textit{ est clos par causalité)} \\ \nexists \dot{e}, \dot{e}' \in \dot{E} \quad \dot{e} \neq \dot{e}' \ \wedge \ {}^{\bullet}\dot{e} \cap {}^{\bullet}\dot{e}' \neq \emptyset & \textit{(}\dot{E}\textit{ est sans conflit)} \\ \textit{pour tout } \dot{e} \in \dot{E}, \tau(\dot{e}) \textit{ est localement-tirable à la date } \Theta(\dot{e}) \textit{ depuis l'état local } S \\ \qquad \textit{associé aux conditions } {}^{\bullet}\dot{e}. \end{cases}$$

Théorème 6 *Pour tout $\dot{e} \stackrel{\text{def}}{=} (B, t) \in cnds(U) \times T$, $\dot{e} \in U$ ssi :*

$$\begin{cases} \nexists \dot{f}, \dot{f}' \in \lceil \dot{e} \rceil \quad \dot{f} \neq \dot{f}' \ \wedge \ {}^{\bullet}\dot{f} \cap {}^{\bullet}\dot{f}' \neq \emptyset \\ \exists \Theta : \lceil \dot{e} \rceil \longrightarrow Q \quad \forall \dot{f} \in \lceil \dot{e} \rceil \quad \tau(\dot{f}) \textit{ est localement-tirable à la date } \Theta(\dot{f}) \\ \qquad \textit{depuis l'état local } S \textit{ associé aux conditions } {}^{\bullet}\dot{f}. \end{cases}$$

3.4. *Exemple de dépliage symbolique*

Nous revenons à notre exemple de la figure 1. La figure 3 montre le dépliage symbolique du réseau $\mathcal{D}(R, O)$ défini dans la sous-section 2.4. Pour garder la figure lisible, nous avons enlevé toutes les places et transitions modélisant l'environnement d'observation.

Nous voyons les deux explications de notre exemple comme des processus étendus maximaux de ce dépliage. Les contraintes linéaires apparaissant sur les événements ont été simplifiées.

4. Conclusion

Nous avons présenté une approche possible du problème de la supervision et diagnostic des systèmes temporisés, en utilisant des réseaux de Petri temporels saufs. Dans ces réseaux, les contraintes de temps sont données par des intervalles de nombres rationnels positifs indiquant les retards possibles au tir des transitions. Ces contraintes, qui doivent être résolues de manière globale, restreignent les comportements possibles du réseau. Le problème du diagnostic est de retrouver les comportements du modèle qui sont compatibles avec les observations. Nous considérons que les observations sont données par un ordre partiel issu d'un ensemble de capteurs, mais sans information de temps. Compatible avec les observations veut dire que l'ensemble des occurrences des transitions des comportements sélectionnés correspond avec l'ensemble des alarmes observées et que les dépendances causales ne sont pas en contradiction avec l'ordre local d'observation sur chacun des capteurs. Cet objectif est atteint en considérant un dépliage symbolique du réseau de Petri temporel contraint par les observations. Le résultat est un ensemble de comportements du réseau qui explicitent les causalités entre les alarmes. Notre algorithme infère aussi les retards possibles devant chaque occurrence de transition : à cause de la nature globale des contraintes

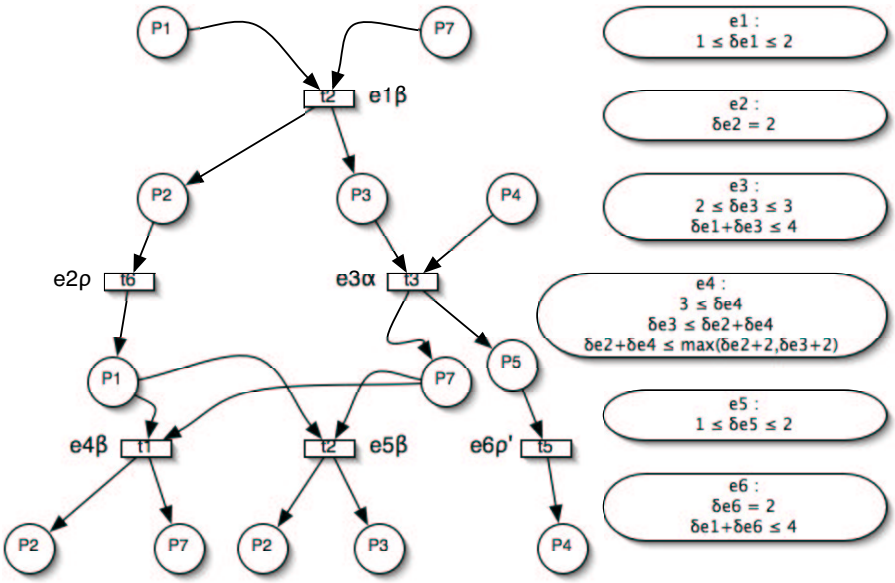

Figure 3. *Le dépliage symbolique du RdPT de la figure 1, contraint par les observations*

dans le cas général des RdPT (non à choix libre étendu), ces retards sont en général strictement inclus dans les intervalles statiques donnés dans le modèle. À notre connaissance, le dépliage symbolique utilisé est original, ainsi que son application au calcul des explications symboliques.

Une implantation prototype a été réalisée (quelques milliers de lignes de code Lisp), et nous prévoyons de l'utiliser sur de vrais exemples pour tester la complexité pratique de l'approche. Nous réfléchissons actuellement à la généralisation de la démarche à des observations portant une information temporelle, qu'il faut soigneusement élaborer dans un contexte de système réparti où plusieurs horloges physiques collaborent.

Enfin, au delà de la question du diagnostic, la définition de préfixes finis symboliques pour les réseaux de Petri temporels pourrait être utile pour les méthodes de vérification ou de synthèse de tests.

5. Bibliographie

Aura T., Lilius J., « Time Processes for Time Petri Nets », *ICATPN*, p. 136-155, 1997.

Benveniste A., Fabre E., Jard C., Haar S., « Diagnosis of asynchronous discrete event systems, a net unfolding approach », *IEEE Transactions on Automatic Control*, vol. 48, n° 5, p. 714-727, May, 2003.

Berthomieu B., Diaz M., « Modeling and Verification of Time Dependent Systems Using Time Petri Nets », *IEEE Trans. Software Eng.*, vol. 17, n° 3, p. 259-273, 1991.

Berthomieu B., Vernadat F., « State Class Constructions for Branching Analysis of Time Petri Nets », *TACAS*, p. 442-457, 2003.

Best E., « Structure Theory of Petri Nets : the Free Choice Hiatus », *Proceedings of an Advanced Course on Petri Nets : Central Models and Their Properties, Advances in Petri Nets 1986-Part I*, Springer-Verlag, London, UK, p. 168-205, 1987.

Chatain T., Jard C., « Symbolic Diagnosis of Partially Observable Concurrent Systems », *FORTE*, p. 326-342, 2004.

Chatain T., Jard C., Time Supervision of Concurrent Systems using Symbolic Unfoldings of Time Petri Nets, Technical report, INRIA/IRISA, 2005.

Engelfriet J., « Branching Processes of Petri Nets », *Acta Inf.*, vol. 28, n° 6, p. 575-591, 1991.

Merlin P., Farber D., « Recoverability of Communication Protocols – Implications of a Theoretical Study », *IEEE Transactions on Communications*, 1976.

Pradin-Chézalviel B., Valette R., Künzle L., « Scenario duration characterization of t-timed Petri nets using linear logic », *IEEE PNPM*, p. 208-217, 1999.

ANNEXE POUR LE SERVICE FABRICATION
A FOURNIR PAR LES AUTEURS AVEC UN EXEMPLAIRE PAPIER
DE LEUR ARTICLE ET LE COPYRIGHT SIGNE PAR COURRIER
LE FICHIER PDF CORRESPONDANT SERA ENVOYE PAR E-MAIL

1. ARTICLE POUR LA REVUE :
   RS - JESA – 39/2005. MSR'05

2. AUTEURS :
   Claude Jard — Thomas Chatain — Pierre Bourhis

3. TITRE DE L'ARTICLE :
   Diagnostic temporel dans les systèmes répartis à l'aide de dépliages de réseaux de Petri temporels

4. TITRE ABRÉGÉ POUR LE HAUT DE PAGE MOINS DE 40 SIGNES :
   Diagnostic temporel

5. DATE DE CETTE VERSION :
   28 juillet 2005

6. COORDONNÉES DES AUTEURS :

– adresse postale :
IRISA/ENS Cachan
Campus de Beaulieu
F-35042 Rennes Cedex
Claude.Jard@bretagne.ens-cachan.fr
– téléphone : 02 99 05 52 84
– télécopie : 02 99 84 71 71
– e-mail : Claude.Jard@bretagne.ens-cachan.fr

7. LOGICIEL UTILISÉ POUR LA PRÉPARATION DE CET ARTICLE :
   LaTeX, avec le fichier de style `article-hermes.cls`,
   version 1.2 du 03/03/2005.

8. FORMULAIRE DE COPYRIGHT :
   Retourner le formulaire de copyright signé par les auteurs, téléchargé sur :
   `http://www.revuesonline.com`

SERVICE ÉDITORIAL – HERMES-LAVOISIER
14 rue de Provigny, F-94236 Cachan cedex
Tél : 01-47-40-67-67
E-mail : revues@lavoisier.fr
Serveur web : http://www.revuesonline.com