Techniques de recouvrement des défaillances des systèmes de production

A. Khatab, L. Piétrac et E. Niel

Laboratoire d'Automatique industrielle de l'INSA de Lyon.

Bat. Antoine de Saint Exupery

27, Av. Jean Capelle 69621 Villeurbanne Cedex

Tel : (33) 4 72 43 81 98, Fax : (33) 4 72 43 85 35

nomauteur@lai.insa-lyon.fr

Résumé :

Les résultats présentés dans cet article sont issus des travaux de thèse de A. Khatab soutenus au LAI en Décembre 2000. Ces travaux sont une extension de la théorie de contrôle par supervision des Systèmes à Evénements Discrets (SED) de Ramadage et Wonham aux Systèmes à Evénements Discrets Temporels (SEDT). Dans cet article sera présentée une architecture de supervision/surveillance développée au sein du groupe Systèmes de Production Sûrs de Fonctionnement (SPSF) du Groupement de Recherche en Productique (GRP). Les concepts de contrôlabilité, stabilité et stabilisabilité des SEDT seront ensuite définis. Enfin, deux techniques de recouvrement permettant au système d'assurer la continuité de service, seront proposées et nous montrerons qu'elles relèvent des concepts de stabilité et de stabilisabilité.

Mots clés : contrôle, supervision, stabilisation, recouvrement, systèmes à événements discrets

1 Introduction

En se plaçant résolument dans le cadre des systèmes réactifs - réactivité induite par la faculté de la commande de certains systèmes à réagir en réponse à des événements non désirés, cet article aborde deux techniques de recouvrement permettant de caractériser les propriétés essentielles d'une commande sûre mais également de pouvoir en engendrer formellement l'expression. Dans cet esprit qui relève plus particulièrement de l'Automatique, nous évoquerons les concepts de commandabilité (contrôlabilité) et de stabilité, concepts indispensables à l'expression des trajectoires de commande voire de la gestion des modes de fonctionnement.

Les résultats présentés sont issus des travaux de thèse [Kha00] effectués au sein de l'équipe Sûreté et Supervision de Systèmes de Production (3SP) du Laboratoire d'Automatique Industrielle (LAI) de l'INSA de Lyon. Dans ces travaux, nous considérons la réactivité comme relevant du domaine des systèmes à événements discrets temporel (SEDT), étant donné qu'elle ne s'exerce que par rapport à l'occurrence d'une faute, d'une défaillance, de l'absence ou de la disparition d'une information etc.

Dans un premier temps (section 1), le modèle SEDT sera brièvement présenté. Dans un second temps (section 3) sera proposée une architecture de Supervision/Surveillance [Com00] dévelopée au sein du groupe de travail SPSF (Systèmes de Production Sûrs de Fonctionnement) du GRP (Groupement de Recherche en Productique). La section 4 introduit la définition des concepts de stabilité et de stabilisabilité. Ensuite, les propriétés afférentes à la commande sûre seront explicitées (section 5). Le problème de recouvrement sera abordé dans une approche hors ligne (le système de commande sera alors caractérisé par sa robustesse vis à vis du degré de perturbation admissible). Il en découlera la gestion des modes de fonctionnement où seront distingués le nominal (fonctionnement attendu et naturel) et l'exception (fonctionnement non attendu mais pouvant être prévisible). L'alternance possible entre modes de fonctionnement sera exposée, elle introduira alors deux techniques de recouvrement et nous montrerons qu'elles relèvent des concepts de stabilité et de stabilisabilité [Kha00].

2 Modèle SEDT et synthèse de contrôleur

Un Système à Evénements Discrets (SED) est un système dynamique qui évolue en fonction de l'occurrence instantanée d'événements. C'est un système défini par une fonction de transition sur un espace d'états discret.

Pour la modélisation, l'analyse et le contrôle de cette classe de système, la considération de la dimension temporelle est primordiale. Les travaux de recherche menés dans cet esprit ont permis le développement de plusieurs modèles temporels, dits Systèmes à Evénements Discrets Temporels (SEDT).

Dans le cadre de ce travail, nous exploitons un modèle SEDT basé sur la théorie des automates. Ainsi, Un SEDT est représenté par deux automates temporels dépendants : un automate temporel statique et l'autre dynamique [Kha00]. La dimension temporelle (discrète) est représentée par une horloge externe génératrice de *top* d'horloge. A chaque

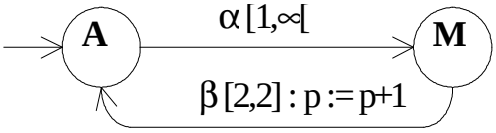

FIG. 1: *Automate temporel statique*

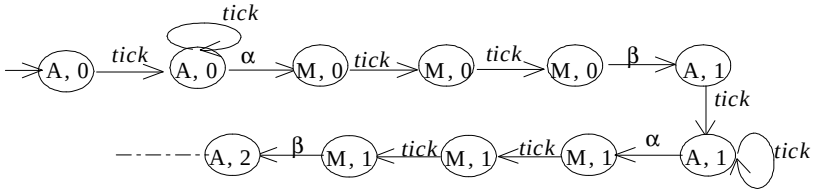

FIG. 2: *Extrait de l'automate temporel dynamique*

événement est associé un intervalle temporel caractérisant ses différents instants possibles d'occurrence ; les bornes inférieure et supérieure de cet intervalle représentent respectivement le *retard* et le *deadline* d'occurrence de l'événement.

Afin d'illustrer cela, considérons l'exemple suivant :

Exemple 1 *considérons une machine d'usinage de pièces. Elle admet deux états : Marche (M) et Arrêt (A). L'automate temporel statique correspondant peut être représenté par l'automate de la figure 1. Le démarrage de la machine (événement α) peut s'effectuer au plus tôt 1 unité de temps (d'où l'intervalle temporel [1,∞[) à partir de l'état où il est validé. En outre, l'usinage d'une pièce est réalisé en exactement 2 unités de temps (l'intervalle temporel de β est donc [2,2]). Initialement supposée nulle, la variable p permet de relever le nombre de pièces usinées.*

L'automate temporel dynamique correspondant est donné par la figure 2 où l'événement tick represente l'ecoulement du temps[1]*. L'occurrence de l'événement α n'est possible qu'après une unité de temps, alors que l'événement β ne peut se produire qu'après exactement deux unités de temps.*

S'agissant du contrôle de cette classe de systèmes, plusieurs approches ont été développées. Pour toutes ces approches, l'objectif du contrôle est de restreindre le fonctionnement du système afin de répondre à un ensemble de contraintes de fonctionnement. Ces contraintes peuvent être de sécurité (évitement de situations catastrophiques) où encore de vivacité (permettre une évolution non-bloquante). Globalement, ces différentes approches

[1] Ce modèle SEDT est un modèle à temps discret. Il existe d'autres modèles, dits à temps dense (*dense real time*), tels que le modèle automate d'Allur et Dill [All94].

se distinguent selon que le contrôle est effectué sur l'état (appelé contrôle statique par retour d'état) ou sur les trajectoires d'événements (appelé aussi contrôle dynamique).

Dans [Kha00] une contrainte (ou prédicat) est caractérisée par un sous-ensemble d'états de l'espace d'états de l'automate temporel dynamique d'un SEDT. L'objectif du contrôle est d'assurer l'ordonnancement correct des événements de manière à ce que l'évolution du système soit maintenue *invariante* dans l'ensemble des états de la contrainte à respecter. Dans cette approche, le concept de base est le concept de *contrôlabilité* (par analogie à la commandabilité en automatique continue). Un prédicat de contraintes est alors dit *contrôlable* si le système y évolue et y reste confiné indéfiniment. Pour plus de détails, le lecteur intéressé peut se référer aux travaux de thèse [Kha00].

3 Architecture de Supervision Surveillance

La synthèse de lois de commande sûres pour des systèmes de production sujets aux perturbations relève du domaine de la sûreté et de la supervision. Elle s'inscrit plus particulièrement dans la phase de conception de la commande *hors-ligne* et les lois résultantes sont ensuite implantées pour une phase d'exploitation *en-ligne*. Selon la démarche de synthèse qui caractérise avant tout la validation formelle des trajectoires de commande engendrées, il s'agit de définir les différents modules et relations soutenant les actions dites de surveillance et de supervision qui s'intègrent naturellement dans les deux boucles de commande classiques. La première boucle de commande, relative au fonctionnement nominal, repose sur l'utilisation de modèles SEDT (spécifications nominales et processus physique à commander) à partir desquels la synthèse s'opère de manière classique en faisant abstraction des défaillances envisageables. Elle conduit à la structure de commande en boucle fermée dite de bas niveau. La seconde boucle fait référence au fonctionnement sous faute lorsqu'il est admis. La commande est alors élaborée à partir d'états ayant été diagnostiqués comme fautifs ou de pannes et récupérables selon des stratégies relevant de la décision : dans ce contexte la démarche de récupération évoque la synthèse de lois de commande stabilisante.

En se basant sur l'architecture (fig. 3) développée au sein de la communauté SPSF du GRP, nous présenterons d'une manière succinte les fonctions concernées par le maintien d'un fonctionnement sous défaillance. Ce type de réactivité reste particulièrement bien adapté à l'enclenchement du fonctionnement dégradé dès la détection d'une déviation de

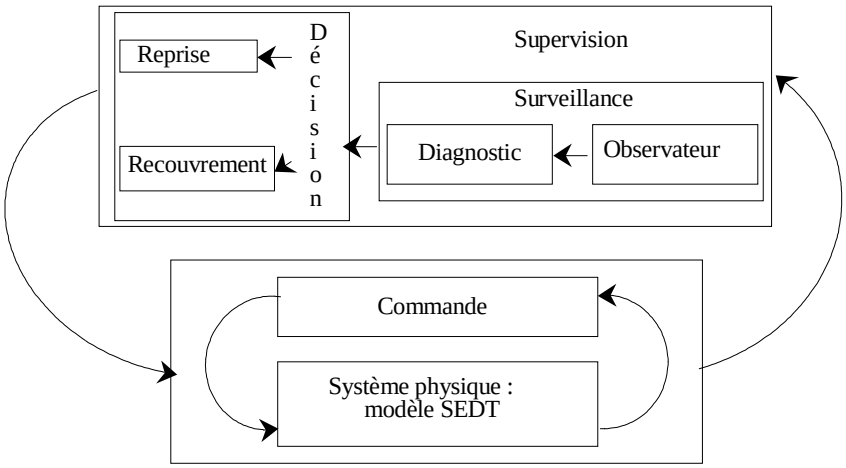

FIG. 3: *Architecture de contrôle et supervision des SEDT*

comportement due à une défaillance.

1. **Système commandé** : il s'agit d'un modèle du système physique (dans notre cas c'est un modèle automate temporel intégrant les défaillances) dont la dynamique se plie à des contraintes dites nominales. Le(s) contrôleur(s) synthétisé(s) fait abstraction des événements de défaillance et confère au système son mode de fonctionnement nominal. Les contraintes nominales peuvent être aussi bien qualitatives que quantitatives.
2. **Surveillance** : ce module a pour premier rôle de recueillir (observation) en permanence toutes les informations en provenance du processus commandé en vue d'une reconstitution de l'état réel et de relever tout indicateur de défaillance (détection). En général les fonctions de reprise et de recouvrement dépendent de la trace du processus commandé et du type de défaillance apparue, à cette fin le module de surveillance proposé comporte un système de diagnostic qui est chargé d'identifier la défaillance détectée. La fonction de la surveillance est ainsi dotée d'un caractère plutôt passif vis-à-vis du processus commandé. Son rôle se limite à la collecte et au traitement des informations en provenance du processus commandé sans réellement agir sur ce dernier.
3. **Supervision** : Celle-ci, incluant la surveillance, possède un rôle actif et est supportée, selon la nature de la défaillance, par plusieurs fonctions : décision, reprise et recouvrement. Les fonctions de recouvrement et de reprise sont définies relativement aux notions de la stabilité et de la stabilisabilité des SEDT. Dans ce contexte, la

stabilisabilité concerne la possibilité (existence d'une loi de commande stabilisante) de conduire un système depuis un état de panne vers un des fonctionnements permis (nominal ou dégradé) et à faire en sorte qu'il y reste confiné indéfiniment.

Dans cet article, nous nous limitons au problème de recouvrement.

Avant d'aborder les deux techniques de recouvrement, attardons nous sur la definition des concepts de stabilité et de stabilisabilité.

4 Stabilité et stabilisabilité des SEDT

Les concepts de stabilité et de stabilisabilité font référence aux propriétés intrinsèques des systèmes tolérants aux fautes. La stabilité est définie comme l'aptitude d'un système à pouvoir atteindre, à partir de tout état, un sous-ensemble d'états et de le visiter régulièrement. La stabilisabilité concerne la possibilité de contrôler un système dans l'objectif de le rendre stable.

Dans le cadre de la sûreté de fonctionnement, de tels concepts ont pour objectif majeur de conférer à la commande la possibilité de récupérer un fonctionnement suite à la manifestation d'une défaillance. Les exigences de performances prescrites n'étant pas toujours respectées, il est nécessaire d'admettre pour certaines classes de systèmes des fonctionnements dits d'exception ou encore dégradés. Dans cet esprit, l'objectif est de proposer un cadre formel d'étude et de développer des techniques associées pour la maîtrise des systèmes à fonctionnement non nominal (voire sous risques).

Plus explicitement, supposons que le fonctionnement nominal du système soit caractérisé par un ensemble d'états D construit sur l'espace d'états de l'automate temporel dynamique G d'un SEDT. Le concept de base consiste à synthétiser un contrôleur qui assure le retour, en un nombre fini d'étapes (ou d'événements), vers cet ensemble D après une quelconque sortie de D. Intuitivement, un système sera dit stable par rapport à son fonctionnement nominal s'il est apte à y converger naturellement après occurrence d'une défaillance.

5 Techniques de recouvrement des défaillances

L'approche proposée, tout comme [Nou97][Sar99][Rez95] dans un cadre de modélisation logique de base, intègre les défaillances dans le processus physique (modèle où les

défaillances sont explicitement pris en compte). La coexistence des deux boucles de commande conduit à distinguer deux modes de fonctionnement : un mode de fonctionnement nominal (NFM) caractérisant un fonctionnement en l'absence de défaillances et un mode dégradé ou d'*exception* (DFM) permettant d'assurer la continuité de service après l'occurrence d'une défaillance. Celle-ci est perçue comme étant un événement incontrôlable dont l'occurrence déstabilise le système. Le fonctionnement ainsi récupéré peut ne plus respecter les critères de performances établis dans le fonctionnement nominal (fig. 4).

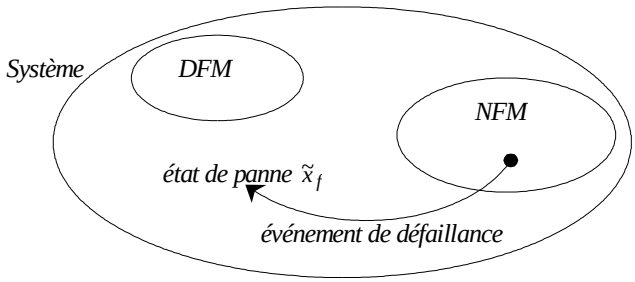

FIG. 4: *Modes de fonctionnement sous défaillances d'un système*

Deux techniques de recouvrement sont proposées selon le type de défaillance survenue [Nou97][Sar99] [Rez95] [Kha98], ce choix résulte d'une fonction de décision. La première technique (fig. 5) consiste à ramener le système depuis son état de panne vers le fonctionnement nominal (Reprise). La deuxième solution (fig. 6) peut être vue comme une fonction de compensation suivie d'une fonction de reprise. Elle consiste à imposer un fonctionnement dégradé approprié à la défaillance et ce jusqu'à la disparition de celle-ci, après quoi le système est reconduit vers son mode de fonctionnement nominal. Les deux solutions proposées par le recouvrement consistent en la synthèse d'une loi de commande permettant de stabiliser le système depuis un état de panne. Cependant, la deuxième solution conduisant le système vers un fonctionnement dégradé peut être vue comme une reconfiguration matérielle (changement ou remplacement d'équipement défaillant) ou un reparamétrage de la commande nominale par relaxation des contraintes nominales imposées au départ [Com00].

Précisons que les deux techniques de recouvrement préconisées sont définies lorsqu'il existe une action corrective permettant au système de continuer son fonctionnement en présence des défaillances. De telles actions dites aussi de compensation sont entreprises selon le type et la nature de la flexibilité du système et caractérisent le degré de réactivité

des systèmes vis-à-vis des défaillances.

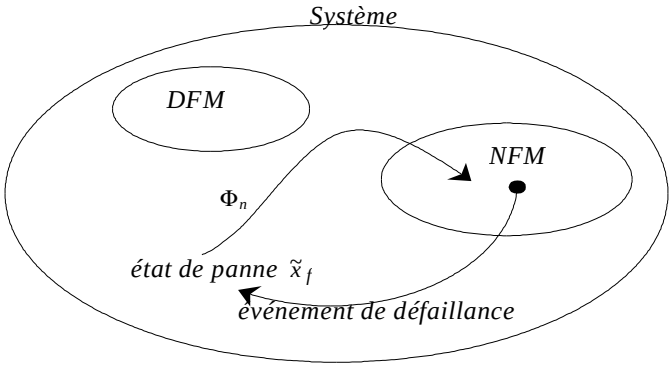

FIG. 5: *Première technique de recouvrement : retour au NFM.*

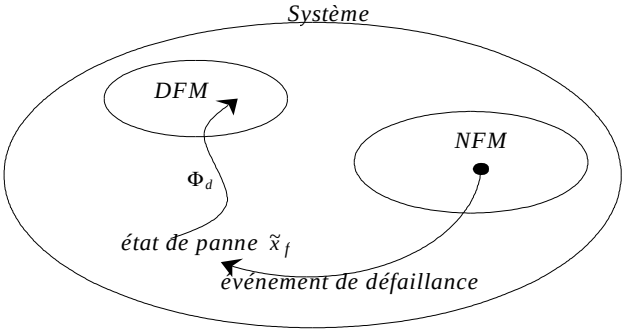

FIG. 6: *Deuxième technique de recouvrement : contrôleur par retour d'états* Φ_d

6 Conclusion

Nous avons proposé deux techniques formelles de recouvrement aux défaillances pour les SEDT. Celles-ci constituent une extension des travaux entrepris dans le même contexte pour les SED et les VDES (SED à structure vectorielle) [Nou97] [Sar99][Rez95].

Il est également montré que ces techniques de recouvrement relèvent des concepts de stabilité et de stabilisation.

Par la définition des deux modes de fonctionnement (nominal et dégradé) d'un système, nous avons adopté une approche modulaire pour la synthèse de contrôleur. Il s'agit de synthétiser, d'une part, un contrôleur guarantissant un fonctionnement nominal et, d'autre part, un deuxième contrôleur conduisant le système, après occurrence d'une défaillance, soit vers son mode nominal (première technique de recouvrement) soit vers son mode dégradé (deuxième technique de recouvrement).

Références

[All94] **Allur R., Dill D. L.** A theory of timed automata. *Theoritical Computer Sciences*, 1994. Vol. 126, no. 2, p. 183–235.

[Com00] **Combacau M., Berruet P., Charbonaud P., Khatab A.** Supervision and monitoring of production systems. *2nd conf. on Managment and Control of Production and Logistics (MCPL), Grenoble, France.*, Jul. 2000. CDROM, 6 p.

[Kha98] **Khatab A., Niel E.** Supervisory Control of Timed Discrete Event Systems in the Operationnal Safety context. *International Workshop on Discrete Event Systems WoDES, Cagliari, Sardinia*, Aug. 1998. p. 334–339.

[Kha00] **Khatab A.** *contrôle et contrôle stabilisant des Systèmes à Evénements Discrets Temporels : Application au recouvrement des défaillances des systèmes de production*. Thèse de Doctorat : Institut National des Sciences Appliquées de Lyon, France, 200, 196 p.

[Nou97] **Nourelfath M.** *Extension de la théorie de la supervision à la surveillance et à la commande des Systèmes à Evénements Discrets*. Thèse de Doctorat : Institut National des Sciences Appliquées de Lyon, France, 1997, 145 p.

[Rez95] **Rezg N., Niel E.** Monitoring system for discrete event system using failure-tolerance techniques. *Conférence INRIA/IEEE sur les technologies émergentes et l'automatisation des systèmes de fabrications ETFA'95, Paris*, Oct 1995. p. 383–391.

[Sar99] **Sarri P.** *Stabilisation et contrôle optimale des Systèmes à Evénements Discrets à Structure Vectorielle* . Thèse de Doctorat : Institut National des Sciences Appliquées de Lyon, France, 1999, 165 p.