Synthèse de lois de surveillance pour les procédés industriels complexes

Hector Mendez Azua

Institut National Polytechnique de Grenoble

THESE

pour obtenir le grade de

DOCTEUR DE L'INPG

Spécialité : **≪AUTOMATIQUE-PRODUCTIQUE≫**

préparée au Laboratoire d'Automatique de Grenoble

dans le cadre de l'École Doctorale **≪Électronique, Électrotechnique, Automatique, Télécommunication et Signal≫**

présentée et soutenue publiquement

par

Héctor MENDEZ AZUA

le 23 septembre 2002

Titre :

SYNTHÈSE DE LOIS DE SURVEILLANCE POUR LES PROCÉDÉS INDUSTRIELS COMPLEXES

Directeur de thèse :

M. Bernard DESCOTES-GENON

JURY :

M. Pierre LADET	Président
M. Michel COMBACAU	Rapporteur
M. Eric NIEL	Rapporteur
M. Jean-Marc FAURE	Examinateur
M. Claude SOURISSE	Examinateur
M. Bernard DESCOTES-GENON	Directeur de thèse
M. Eric ZAMAI	Co-encadrant

À mes parents

Remerciements

Le travail présenté dans ce mémoire a été préparé successivement au sein des équipes Conduite des Systèmes de Production (CSP) puis Conduite Robuste, Surveillance et Supervision (CROSS) du Laboratoire d'Automatique de Grenoble (LAG). Je voudrais utiliser quelques lignes de ce manuscrit pour remercier toutes les personnes qui ont participé, de façon directe ou indirecte, à mon parcours tout au long de ces trois années de travail.

Tout d'abord je voudrais remercier Monsieur Luc DUGARD, directeur du Laboratoire d'Automatique de Grenoble, pour m'avoir accueilli dans son laboratoire. Je tiens aussi à remercier Monsieur Bernard DESCOTES-GENON, Professeur à l'Université Joseph Fourier à Grenoble, pour m'avoir accueilli dans l'équipe CSP, pour avoir accepté de diriger ce travail, pour tous ses conseils et pour toute la confiance qu'il a eu envers mon travail. Également je remercie Madame Mireille Jacomino pour son accueil au sein de l'équipe CROSS, pour sa sympathie, ses conseils et ses remarques qui m'ont beaucoup aidé.

J'exprime toute ma gratitude à Monsieur Pierre LADET, Professeur à l'Institut National Polytechnique de Grenoble, pour avoir accepté de présider mon jury.

Je remercie très particulièrement Monsieur Eric ZAMAI, Maître de Conférences à l'Institut National Polytechnique de Grenoble pour son encadrement, pour tous ses conseils, sa disponibilité, son soutien inestimable et pour son immense patience. Il n'est pas toujours facile de travailler avec quelqu'un si "facilement irritable" que moi. Il a su le faire et pour cela je lui exprime ma gratitude et toute ma reconnaissance.

Je suis très reconnaissant envers Messieurs Michel COMBACAU, Professeur à l'Université Paul Sabatier de Toulouse et Eric NIEL, Professeur à l'Institut National des Sciences Appliquées de Lyon, pour l'intérêt qu'ils ont porté à mon travail en acceptant d'en être les rapporteurs, et pour tous les conseils et remarques qu'ils m'ont fait. Celles-ci m'ont permis d'améliorer significativement le travail réalisé.

Je tiens également à exprimer ma gratitude à Messieurs Jean-Marc FAURE, Professeur à l'Ecole Nationale Supérieure de Cachan et Claude SOURISSE, Président du Club Automatique à Paris pour l'honneur qu'ils m'ont fait en acceptant d'être examinateurs de ce travail.

Je remercie également toutes les personnes que j'ai rencontré depuis mon arrivée au LAG pour leur soutien et pour leur amitié. A André, Philippe, Dominique, Erwan et Yves pour leurs remarques et pour leur amitié, pour eux un grand merci. Ma gratitude aussi pour l'ensemble du personnel administratif et technique qui m'a permis d'accomplir mon travail dans un environnement très agréable.

Ce travail a bénéficié de l'appui financier du Consejo Nacional de Ciencia y Tecnología (CONACYT) du Mexique. Je tiens à remercier cet organisme pour m'avoir donné l'op-

portunité de vivre cette expérience. Je remercie aussi le personnel de la Société Française d'Exportation des Ressources Éducatives (SFERE) par son suivi pédagogique et par son aide dans les démarches administratives quelquefois un peu dures pour nous, les étrangers en France.

Je voudrais adresser une pensée pour ma famille qui m'a toujours soutenu et pour mes amis au Mexique, merci pour leurs encouragements à distance. Finalement un grand merci à tous mes amis mexicains (de naissance et d'adoption) à Grenoble qui m'ont aidé à faire de mon séjour à Grenoble une aventure inoubliable. Je ne cite pas leurs noms car ils sont si nombreux que je risque d'en oublier quelques-uns. Si ce document arrive à leurs mains, ils sauront se reconnaître.

Table des matières

Introduction Générale

Introduction Générale

Dans l'industrie manufacturière d'aujourd'hui, les marchés mondialisés sont en perpétuelle évolution. Le contexte de développement des produits, souvent perturbé par des variations internes ou externes, a un caractère particulièrement fluctuant. Pour survivre et évoluer dans ce contexte fortement instable, les maîtres mots des industriels sont devenus plus que jamais : réduction des coûts et des délais de production, amélioration de la qualité de fabrication pour accroître encore la productivité de l'entreprise. Pour atteindre ces objectifs, des améliorations doivent être apportées pour faire face aux situations et problèmes inconnus qui peuvent se produire au cours d'un cycle de production. Lorsque nous nous focalisons sur les aléas issus du procédé lui-même, nous abordons alors la problématique de la supervision et de la surveillance temps réel des procédés industriels.

L'étude d'un telle problématique vise à spécifier et concevoir des Systèmes Automatisés de Production Sûrs de Fonctionnement en vue d'une meilleure exploitation en présence de dysfonctionnements et ainsi aider les industriels à mieux maîtriser leur production. Dans ce cadre, de nombreuses approches et solutions différentes ont été proposées, accompagnées du développement de procédures fines de supervision, de surveillance, de diagnostic, d'aide à la décision, de recouvrement, etc.

Cependant, disposer de toutes les "compétences" requises pour superviser, surveiller, diagnostiquer, décider, etc., ne rime pas forcément avec la performance du système global. En effet, à l'image de la gestion du personnel dans une entreprise, une gestion adaptée de ces compétences doit être proposée en fonction du contexte de production, des niveaux de qualité affichés, des normes écologiques et/ou lois en termes de sécurité en vigueur et bien entendu de la gravité du dysfonctionnement détecté.

La proposition d'un tel concept de gestion existe. Cependant, l'approche concernée n'offre aucun moyen pour développer efficacement des lois de gestion adaptées de ces compétences.

Le travail que nous présentons dans ce document propose d'apporter sa contribution à cette problématique. Il prend donc naturellement place au sein du domaine de la surveillance, de la commande et de la supervision des procédés industriels complexes. Son originalité réside dans la proposition d'une technique de synthèse de lois de surveillance adaptées aux différents besoins du milieu industriel, proche de la synthèse de correcteurs dans le domaine de l'automatique continue.

Partant du constat qu'une des limitations du domaine est le manque de propriétés qu'il faut savoir rechercher lorsqu'on souhaite spécifier une loi de surveillance, nous proposons un contexte de rédaction de cahier des charges à ce jour fermé par un ensemble de sept propriétés (modes de marches, sécurité, écologie, productivité, qualité, priorités, récursivité).

Fort de ces propriétés, et compte tenu de la nécessité de prendre en compte les différents

modes de marches et d'arrêts d'une installation pour être en mesure de la commander, de la surveiller et de la superviser convenablement, nous avons proposé une identification d'un modèle de référence pour la surveillance, la commande et la supervision. Cette identification a été réalisée sur la base de celle déjà effectuée dans des travaux antérieurs (LAAS). Le modèle a ensuite été étendu pour prendre en compte les modes des marches et d'arrêts. Le modèle obtenu est générique et représente l'ensemble des possibilités que doit offrir un système de surveillance, commande et supervision. Cet aspect générique est garanti par le simple constat que les compétences qui doivent être mises au service de la réactivité aux défaillances du procédé sont identiques quelle que soit la nature du procédé considéré. En revanche, la façon de les organiser autour de la défaillance dépend forcément du procédé considéré, ainsi que de nombreux autres facteurs.

Afin d'adapter les traitements de défaillances à ces nombreux facteurs déclinés sous la forme de propriétés (modes, normes législatives, productivité, qualité, etc.), une technique générale de synthèse de lois de surveillance a été proposée. Elle se base sur l'intégration progressive des propriétés au sein du modèle de référence en s'appuyant sur les caractéristiques structurelles du modèle.

Ce mémoire est organisé en quatre parties dont les thèmes sont donnés ci-après.

La première partie présente de manière générale la problématique de la commande, de la surveillance et de la supervision dans les systèmes automatisés de production. Dans cet objectif, ces systèmes sont présentés au travers des architectures de commande qui les caractérisent. Fort de ces caractéristiques et des besoins exprimés en terme de réactivité aux aléas de fonctionnement de la partie opérative, la terminologie du domaine est présentée. Elle s'appuie sur celle développée dans le cadre du groupe de travail "Automatisation des Systèmes Sûrs de Fonctionnement" du Groupement pour la Recherche en Productique. Ensuite, une étude de la commande, de la surveillance et de la supervision est réalisée en s'appuyant sur les travaux réalisés dans différentes équipes de recherche appartenant à des laboratoires comme le LURPA (Cachan), le LAI (Lyon), le LAIL (Lille), le LAAS (Toulouse), et à des organismes industriels tels que l'ADEPA. Toutes ces approches intègrent toute ou partie des différents éléments requis pour la surveillance, la commande et/ou la supervision. De surcroît, elles s'accordent sur un point essentiel : quelle que soit la problématique considérée (commande, surveillance et/ou supervision), il est nécessaire de développer des lois respectant le cahier des charges fixé. Cette partie s'achève alors sur la présentation de notre contribution et de la démarche que nous avons retenue. Notre contribution porte sur la spécification d'une technique de synthèse de lois de surveillance. Notre démarche consiste à identifier un modèle générique de surveillance, commande et supervision, à spécifier les propriétés qu'il faut rechercher pour enfin en synthétiser une loi de surveillance les respectant.

La partie II est ainsi entièrement consacrée à l'identification du modèle de référence pour la surveillance, la commande et la supervision des procédés industriels complexes. Cette identification s'appuie sur celle proposée dans le cadre des travaux développés au LAAS. Une extension du modèle de référence est proposée. Cette extension s'appuie essentiellement sur l'intégration des modes de marches et d'arrêts spécifiés dans le cadre du GEMMA. En effet, le traitement d'une défaillance doit dépendre du mode dans lequel elle a été détectée. Ceci a eu pour résultat direct d'accroître considérablement la taille du modèle, puisqu'il passe désormais de 31 à 98 activités de référence et de 171 à plus de 1200 processus élémentaires liant ces activités. Les possibilités qui doivent être offertes par un système de surveillance, commande et

supervision en termes de traitements de défaillances sont donc désormais plus fines et plus proches des besoins industriels. Cette partie se termine par une proposition d'une formalisation du modèle de référence sur la base de la théorie des automates.

La partie III est quant à elle entièrement dédiée à la proposition d'une technique de synthèse de lois de surveillance. Dans ce but, la problématique de la synthèse est tout d'abord étudiée au travers de plusieurs approches, notamment celles issues de l'automatique continue. Fort de cette analyse, les propriétés qui doivent être recherchées pour synthétiser une loi de surveillance sont présentées. Elles se déclinent en termes de modes de marches et d'arrêts, de normes législatives comme la sécurité ou l'écologie, de besoins internes à l'entreprise tels que productivité et assurance qualité, de priorités entre ces normes et besoins internes, et enfin en terme de réglage d'un niveau de tolérance à la prise en compte de défaillances répétitives. Compte tenu de la nature très hétérogène des propriétés qui doivent être recherchées (critères versus contraintes), et de la structure même du modèle de référence que nous avons établi, nous avons proposé une technique générale de synthèse basée sur le raffinement successif du modèle de référence par intégration progressive des propriétés.

Dans la partie IV, nous développons un exemple d'application sur un atelier réel. Le procédé pilote considéré (SAPHIR) est celui du Laboratoire d'Automatique de Grenoble. Les avantages de notre approche tels que l'assistance à la rédaction du cahier des charges dans un contexte fermé par les propriétés qui doivent être recherchées, la prise en compte permanente du niveau d'expertise de l'opérateur humain tout au long de la phase de synthèse, l'aspect générique de la démarche de synthèse proposée, et les possibilités offertes quant à la validation voire la vérification de la loi de surveillance obtenue y sont exposés.

Première partie

Cadre de l'étude

Chapitre 1

Cadre de l'étude

1.1 Introduction

Ce chapitre est consacré à la présentation du contexte de notre travail et à la définition des concepts de base de notre étude. Nous commencerons tout d'abord par présenter les caractéristiques des Systèmes Automatisés de Production (SAP). Cette présentation servira à mettre en évidence la complexité à laquelle les SAP doivent faire face. Dans ce contexte, nous procéderons à la description générale d'une structure hiérarchique et modulaire pour leur commande. Une analyse des structures hiérarchiques servira à introduire l'aspect organisationnel de la commande des systèmes de production et les mécanismes décisionnels utilisés dans ces structures. Ensuite nous introduirons la problématique de la prise en compte des défaillances de la partie opérative, à savoir la surveillance et la supervision. Finalement, nous présenterons une étude critique d'une sélection de travaux qui sont en relation directe avec la problématique que nous traitons.

1.2 Les Systèmes Automatisés de Production

Dans ce paragraphe, nous nous intéressons à la présentation des concepts liés à l'automatisation des systèmes automatisés de production. Notre objectif est de présenter brièvement ce qu'est un système automatisé de production, quels sont ses objectifs, de quelle façon les systèmes de production automatisés sont organisés et finalement nous nous proposons de situer notre travail dans cette organisation. Commençons par définir les Systèmes Automatisés de Production (SAP).

"Tout système de production a pour objectif de transformer, sous certaines conditions, un élément initial en un élément final, afin que sa valeur, par rapport à certains critères, soit augmentée" (de Bonneval [1993]).

1.2.1 Objectifs

La réalisation d'une telle mission dépend de la satisfaction d'un ensemble d'objectifs. Ces objectifs sont classés selon quatre classes différentes (Pourcel [1986]) :

objectifs techniques : cette classe propose des objectifs liés aux techniques de conception et de transformation employées dans les processus de production. Nous pou-

vons distinguer les objectifs techniques suivants :

- *diminuer la durée du cycle de production.* La durée du cycle de production est définie par la somme des durées de chacune des étapes nécessaires à l'élaboration des produits. Ces durées comprennent les traitements administratifs, les durées d'approvisionnement, de transfert, etc. La réduction de ces durées se traduit par une amélioration des volumes de production par unité de temps, donc par des gains économiques ;

- *améliorer la qualité des produits.* Un des objectifs des systèmes automatisés de production est d'assurer des niveaux de qualité conformes aux attentes des clients afin de maintenir une position sur le marché face à la concurrence. Mais la quête des améliorations de qualité a aussi des raisons internes. Une amélioration de la qualité des produits conduit à une diminution des rebuts, ce qui se traduit par un accroissement du volume de production et une diminution des coûts ;

- *améliorer la disponibilité du système de production.* L'objectif d'amélioration de la disponibilité des systèmes automatisés de production vise à augmenter le taux de service du système et l'engagement des machines à travers l'amélioration de certains indicateurs. Parmi ces indicateurs nous trouvons : la fiabilité des équipements (l'objectif est de minimiser l'occurrence et la durée des pannes des machines), la politique de maintenance (intégration de maintenance préventive pour augmenter la fiabilité et la disponibilité, en plus de l'intégration d'une maintenance corrective qui, suite à un dysfonctionnement de la machine, permet sa réutilisation dans les plus brefs délais), la politique de pilotage (coordination entre les ressources), etc. ;

- *augmenter la flexibilité du système de production.* Il existe plusieurs définitions de la flexibilité suivant que l'on s'intéresse, par exemple, à la capacité du système de fabrication à s'adapter à des variations de la demande (flexibilité décisionnelle du système de gestion (Briand [1999])) ou à des aléas de fonctionnement des ressources (flexibilité physique de l'atelier (Erschler [1993])). La flexibilité physique correspond à la possibilité de modifier ses caractéristiques fonctionnelles afin d'accepter la fabrication de nouvelles variantes de produits anciens ou de nouveaux produits. L'objectif de ce type de flexibilité est d'offrir aux clients une grande variété de produits en utilisant les mêmes ressources matérielles. Pour ce qui concerne la flexibilité décisionnelle, l'équipe Organisation et Conduite de Systèmes Discrets (OCSD) du Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS) a proposé une structure comportant cinq niveaux décisionnels (Figure 1.1). Ces niveaux ont été établis pour mieux exploiter la flexibilité physique du système de production et pour intégrer les consignes du client dans le système de production. Les niveaux intégrant cette structure sont : Planification, Ordonnancement Prévisionnel, Ordonnancement Temps Réel, Coordination et Commande Locale (Ahmed et al. [1996], Esquirol et P.Lopez [1999]). Les deux premiers niveaux concernent les décisions prises hors-ligne. **La planification** (Hetreux [1996]) est utilisée dans la définition des plans de fabrication. **L'ordonnancement prévisionnel** (Lopez [1991]) sert à définir le routage des produits dans l'atelier. Les trois derniers niveaux s'intègrent dans l'exploitation temps-réel du système de production. Le niveau **ordonnancement temps réel** (Billaut [1993]) souvent appelé *pilotage* assure la cohérence entre les décisions prévisionnelles et les contraintes temps-réel issues du comportement réel du système de production. **La coordination** (Bako [1990]) permet de gérer de manière cohérente les interactions entre les différentes ressources de l'atelier en fonction des contraintes telles que les ressources partagées, les séquencements obligatoires, les synchronisations diverses ou les parallélismes, etc. Finalement, **la commande locale** est l'interface entre les capteurs/actionneurs du procédé et le système de

commande chargé de mettre en œuvre les décisions prises au niveau coordination. La flexibilité décisionnelle naît en fait de cette structuration qui donne au système de production un pouvoir d'adaptation important dans ses prises de décisions.

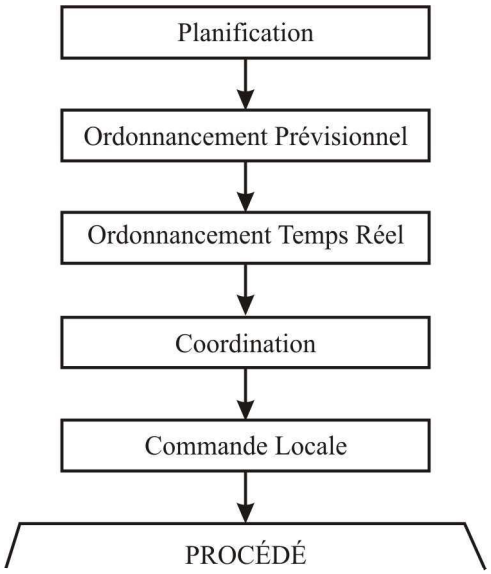

FIG. 1.1: *Structure décisionnelle à cinq niveaux pour un SAP*

objectifs économiques : les objectifs économiques concernent les bénéfices financiers de l'entreprise. Parmi ces objectifs, nous pouvons citer la *diminution des coûts de production*, la diminution de la valeur des stocks et l'optimisation de la capacité de production du système. La diminution des coûts de production s'intègre à tous les niveaux de la structure décisionnelle, dès les niveaux décisionnels hors-ligne (par exemple la prévention des approvisionnements), jusqu'au plus bas niveaux (diminution des rebuts, des gaspillages etc.). La *diminution de la valeur des stocks* est aussi une nécessité pour l'entreprise afin d'employer l'argent immobilisé à des investissements productifs. La réduction des stocks est une opération difficile et délicate. Il faut mettre en relation les fonctions "approvisionnement" avec le fonctionnement des magasins, analyser les demandes des clients, établir des négociations avec les fournisseurs, etc. Un autre objectif que nous pouvons citer dans cet aspect est *la recherche de la production optimale*. Cet objectif est en relation étroite avec les objectifs que nous venons de citer (diminution des coûts de production et de stockage). Une production optimale ne consiste pas à produire le maximum possible, mais "le nécessaire". Un volume de production supérieur à la demande induit des coûts de stockage plus importants. Un volume inférieur conduit à des pénalités économiques résultant du non respect des engagements de délais de livraison.

objectifs humains : *l'amélioration des conditions de travail* constitue un des objectifs majeurs de la production. Les systèmes de production comportent souvent des tâches dangereuses, difficiles d'accès ou très pénibles pour les opérateurs humains (i.e. manipulations de produits chimiques, conditions de températures difficiles, etc). L'automatisation des systèmes de production tend à réduire l'intervention humaine dans ces tâches – dans la métallurgie, la mécanique de précision, l'industrie automobile, etc. – pour lui confier plutôt des fonctions de supervision et de prise de décisions.

objectifs de pilotage : ils visent à accroître la maîtrise *des coûts de production et de stockage*, et de *l'amélioration des temps de réaction en cas de perturbation*. Pour les deux premiers objectifs, une amélioration des procédures de fonctionnement ainsi qu'une meilleure fiabilité des informations communiquées contribuent largement à l'optimisation des coûts de production et de stockage. En ce qui concerne l'amélioration des temps de

réaction en présence de perturbations, deux solutions doivent être envisagées : prévoir hors ligne des mesures correctives de planification et d'ordonnancement pour résoudre les problèmes engendrés par les évolutions du marché (indisponibilité temporaire d'une matière première, modification du cahier des charges par le client, etc.), adjoindre aux couches des niveaux temps réel toutes les compétences requises afin de résoudre au mieux les problèmes qui peuvent se présenter pendant la phase de transformation des produits (dysfonctionnements des machines, modification des commandes, etc.). Ce dernier point fera l'objet d'une étude plus approfondie dans la suite de ce mémoire.

Dans le cadre de notre travail, nous allons plus particulièrement nous intéresser aux deux derniers niveaux de la structure décisionnelle présentée dans la Figure 1.1 : niveau de coordination et niveau de commande locale.

1.2.2 Schématisation d'un SAP

D'une manière générale, les systèmes automatisés de production que nous venons de présenter sont schématisés selon trois types d'entités (Figure 1.2) :

- une partie opérative (ou procédé) qui regroupe l'ensemble des organes physiques (machines) qui interagissent sur le produit pour lui conférer sa valeur ajoutée,
- une partie commande qui comprend l'ensemble des moyens logiciels et matériels ainsi que les informations permettant la gestion du procédé,
- une interface qui permet la communication entre la partie opérative et la partie commande.

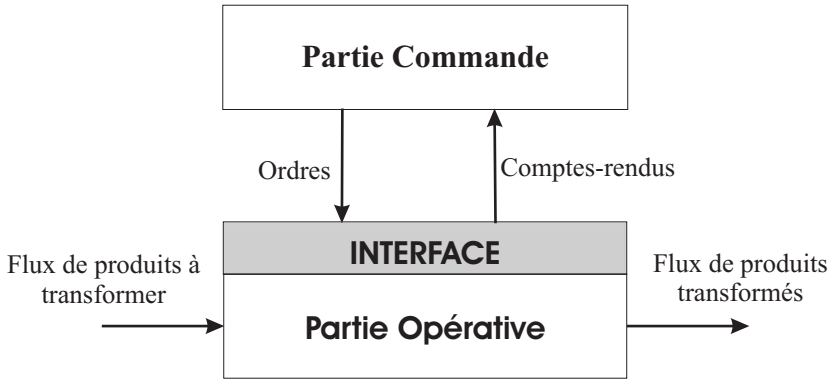

FIG. 1.2: *Schéma d'un Système Automatisé de Production*

Dans cette schématisation, le **bloc de commande** est chargé des décisions concernant les actions qui doivent être exécutées par le procédé afin de transformer le produit selon les consignes imposées par l'utilisateur. Ces ordres sont envoyés sous la forme de requêtes de commande, par exemple, *percer un trou d'un diamètre de 10mm*. Ces ordres sont reçus par le **procédé** qui agit en conséquence sur le produit et atteste des actions effectuées par l'envoi d'informations vers l'entité qui a envoyé l'ordre (le bloc commande). Dans notre exemple, il s'agit de lui notifier que le trou a été percé. Ceci se fait via le bloc **interface**. L'interface adapte l'information qui transite de la partie commande vers le procédé (requêtes) ou vice versa (informations) en utilisant deux types de composants :

- *actionneurs :* chargés de traduire les requêtes de commande en actions effectives dans le procédé,

– *capteurs :* considérés comme des systèmes de mesure pour la commande. Leur type est très différent selon les grandeurs qu'ils mesurent (capteurs de proximité, capteurs analogiques de mesure de courant électrique, capteurs d'effort, etc.).

Dans les systèmes de production réels actuels, la quantité de capteurs/actionneurs à interfacer est tellement importante que cela conduit à un degré de complexité souvent difficile à maîtriser. Une démarche classique pour faire face à cette complexité consiste à organiser le système de commande en plusieurs niveaux de complexité moindre. De cette façon, les objectifs de commande son réorganisés en sous-objectifs plus faciles à manipuler. Par exemple, pour un robot chargé de transporter des pièces d'un endroit à un autre, la requête "transporter de A vers B" pourra être décomposée en "mouvement en X", "mouvement en Y" et "mouvement en Z". Les principes de cette structuration sont présentés dans le paragraphe suivant.

1.3 Structure hiérarchique et modulaire de la commande temps réel

Les structures hiérarchiques et modulaires ont été proposées afin de faire face à la complexité des systèmes automatisés de production. Le principe de ces structures est de décomposer le système de commande selon plusieurs autres niveaux de complexité moindre (Jones [1989]; O'Grady et al. [1994]). Ensuite, chaque niveau est décomposé horizontalement en plusieurs modules indépendants afin d'améliorer l'organisation de l'architecture (Verlinde [1989]). Cette structure est qualifiée de *"structure hiérarchique et modulaire de la commande temps réel"* (Figure 1.3). Plusieurs études ont été développées en utilisant ces structures (Sahraoui [1987]; Combacau [1991]; Parayre [1992]; Berruet [1998]; Dangoumau [2000]).

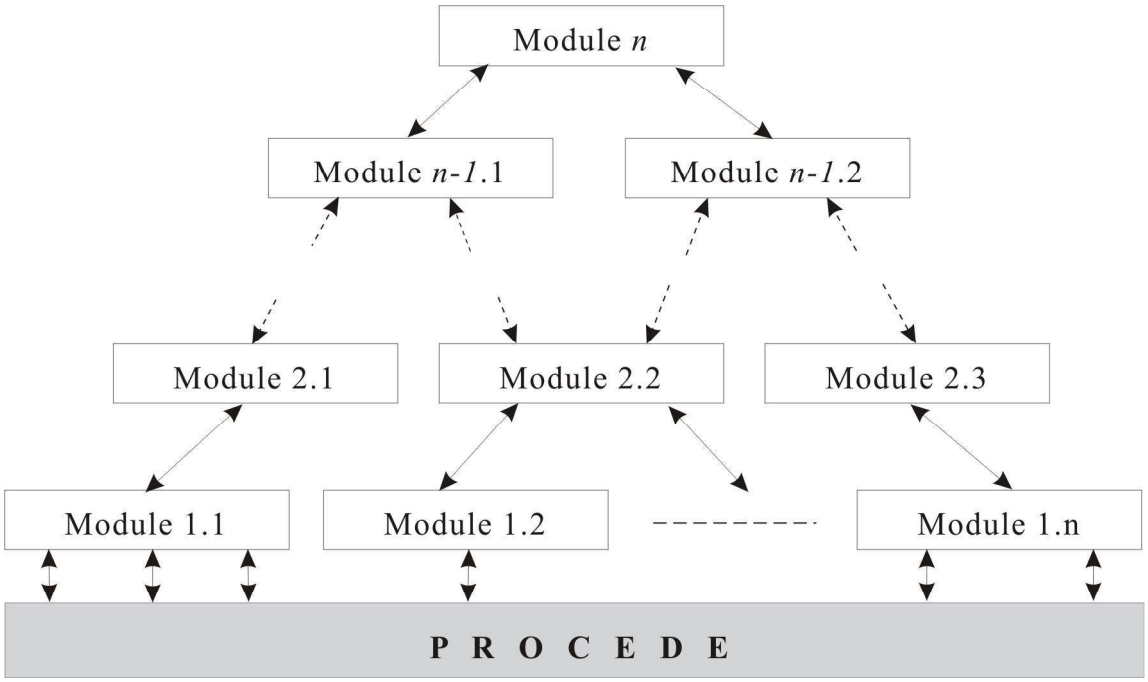

FIG. 1.3: *Structure hiérarchique et modulaire de la commande temps réel*

La structuration du système de commande implique une grande quantité d'informations circulant à travers les composants de la structure hiérarchique (modules). Nous

avons donc besoin d'un mécanisme de communication permettant d'exploiter l'information qu'elle véhicule. Le mécanisme que nous présentons illustre les règles qui doivent être suivies pour permettre un bon fonctionnement de la structure hiérarchique.

Dans une structure hiérarchique, chaque module d'un niveau *i* est lié à un niveau *i+1*. Chaque module est rattaché à un ou plusieurs modules du niveau immédiatement inférieur (*i-1*) ; le niveau 1 correspondant au niveau de commande locale (Sahraoui [1987]).

Chaque module (Figure 1.4) envoie des ordres aux modules qui se trouvent dans le niveau immédiatement inférieur (*requêtes de commande*). C'est le cas de l'envoi d'une requête "transférer came du poste de positionnement vers l'axe d'assemblage 3". Ces requêtes sont affinées et envoyées successivement aux niveaux inférieurs. Les ordres sont envoyés selon un niveau d'abstraction établi en fonction des capacités de service offerts par le niveau *i-1*. Chaque ordre est ainsi envoyé en fonction de la requête reçue du niveau *i+1* avec une prise en compte des contraintes locales du niveau d'abstraction considéré (prise en compte des contraintes de synchronisation, de partage, état courant du sous-système commandé, etc.). Ainsi, dans l'exemple, pour la requête reçue dans le niveau *i*, ce niveau doit décomposer cette requête en trois opérations pour accomplir le service demandé : "mouvement en X=0", "mouvement en Y=10" et "mouvement en Z=0". Ces opérations sont transmises à son niveau inférieur (*i-1*) sous la forme de nouvelles requêtes, accompagnées des données nécessaires pour accomplir l'objectif (dans notre exemple, les coordonnées correspondant à chaque mouvement).

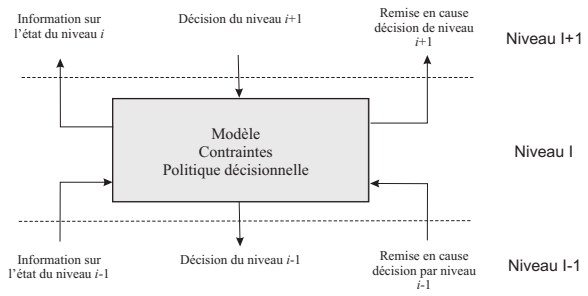

FIG. 1.4: *La décision dans une structure hiérarchique*

Généralement, lorsqu'un module *i* envoie une requête de commande, il attend un compte-rendu attestant que la requête a bien été effectuée par le module du niveau i-1. Néanmoins, en présence de dysfonctionnements, un module peut remettre en cause les ordres reçus de son niveau supérieur. Dans ce cas, le principe de fonctionnement de la hiérarchie doit imposer que seul le module qui a émis la requête est en mesure de pouvoir la modifier. Si cela n'est pas le cas, le niveau *i-1* risque de violer des contraintes inconnues pour lui (Combacau [1991]).

Parmi les avantages qu'offrent les structures hiérarchiques et modulaires, nous pouvons citer :

Facilité organisationnelle : cet avantage permet d'approcher des solutions performantes en termes de conception et de mise en œuvre. Par rapport à la conception, la décomposition des objectifs de commande en sous-objectifs les rend plus maîtrisables et plus faciles à aborder. Cette décomposition aide à la mise en œuvre.

Suppression de conflits décisionnels : chaque module de la structure ne peut être en relation qu'avec un seul module de niveau supérieur (à l'exception du module du niveau *n*, qui n'a pas de niveau supérieur). Dans chaque niveau, tous les modules sont coordonnés par leur module du niveau supérieur. Cela inhibe les décisions contradictoires lancées par d'autres modules.

En revanche, nous nous devons de préciser que de telles architectures ne répondent pas forcément à toutes les exigences du terrain. Par exemple, il est clair qu'un tour à commande numérique et un système de chargement de pièces doivent se synchroniser directement au niveau local sans passer forcément par un module de coordination (Zamaï [1997]). Cependant, nous noterons dès à présent que nous retenons l'hypothèse de travail sur les structures hiérarchiques et modulaires comme étant une des bases de notre approche. Ceci sera repris et précisé dans la partie II.

Revenons-en plutôt maintenant au problème évoqué plus haut, à savoir la présence inéluctable d'informations issues du niveau inférieur remettant en cause les décisions prises au niveau I. Dans ce cas, comme est stipulé dans Combacau [1991], il est nécessaire d'adjoindre au système de commande un système de **surveillance** et de **supervision** (Zamaï et al. [1998b]). Afin d'assurer une bonne compréhension de toute la suite du mémoire, nous nous proposons dans le paragraphe suivant de clarifier la terminologie employée dans le domaine de la surveillance, de la commande et de la supervision. Dans ce but, nous nous sommes appuyés sur le travail développé depuis près de cinq ans au sein du Groupement pour la Recherche en Productique (GRP), et plus particulièrement dans son groupe de travail "Automatisation des Systèmes Sûrs de Fonctionnement" (ASSF).

1.4 Terminologie du GT ASSF du GRP

Une précision doit tout d'abord être apportée ici avant de dévoiler la terminologie utilisée. Comme nous l'avons déjà précisé, il est illusoire de considérer qu'un procédé réel exécute toujours correctement le service qui lui est demandé. Dans ce cas, il s'agit de traiter l'occurrence de défaillances de la partie opérative. Cependant, cette classe de problèmes issue du procédé n'est pas la seule à devoir être prise en compte. En effet, si nous prenons l'exemple d'un système complexe constitué de plusieurs centres de commande interconnectés via un réseau local industriel, lorsque ce dernier est victime d'une rupture le rendant incapable de remplir son rôle, le système de commande est alors en panne. Traiter ce type de défaillances relève entièrement de la sûreté de fonctionnement. La mise en œuvre du principe de redondance matérielle (doublage du réseau, des calculateurs, etc.) est souvent préconisée. Cependant, retenons dès à présent que nous ne nous intéresserons pas dans la suite de notre mémoire à cette dernière classe de défaillances. Seules les défaillances de la partie opérative retiendront toute notre attention. Cette précision étant faite, nous nous proposons maintenant de clarifier la terminologie du domaine. L'ensemble des définitions reportées dans cette section sont extraites de l'article de synthèse *"Supervision and monitoring of production systems"* (Combacau et al. [2000]).

1.4.1 Termes généraux

Avant d'aller plus avant dans la terminologie, il est nécessaire de bien s'accorder sur les concepts liés à la remise en cause d'une décision.

- Faute : action, volontaire ou non, dont le résultat est la non prise en compte correcte d'une directive, d'une contrainte exprimée par le cahier des charges.
- Défaut : écart existant entre la valeur réelle d'une caractéristique du système et sa valeur nominale.
- Erreur : partie du système ne correspondant pas (ou ne correspondant pas complètement) au cahier des charges. En toute logique, une erreur est la conséquence d'une

faute.

- Erreur latente : l'erreur est latente tant que la partie erronée du système n'est pas sollicitée. Elle devient effective au moment de la sollicitation de la partie erronée.
- Dysfonctionnement : exécution d'une fonction du système au cours de laquelle le service rendu n'est pas délivré ou est délivré de manière incomplète.
- Panne : état d'un système incapable (à la suite d'une défaillance) d'assurer le service spécifié.
- Symptôme : événement ou ensemble de données au travers desquels le système de détection identifie le passage du procédé dans un fonctionnement anormal. C'est le seul élément dont a connaissance le système de surveillance au moment de la détection d'une anomalie.
- Défaillance : événement caractéristique d'une situation pour laquelle une opération n'est pas exécutée par une machine parce que son état ne correspond pas aux spécifications nominales.

1.4.2 La supervision

La supervision recouvre les aspects *fonctionnement normal* et *fonctionnement anormal* d'un système automatisé de production :

- en fonctionnement normal, son rôle est surtout de prendre en temps réel les décisions correspondant aux degrés de liberté exigés par la flexibilité décisionnelle. Pour cela elle est amenée à faire de l'ordonnancement temps réel, de l'optimisation, à modifier en ligne la commande et à gérer le passage d'un algorithme de surveillance à un autre.
- en présence de défaillances, la supervision doit prendre toutes les décisions nécessaires pour assurer le retour vers un fonctionnement normal ; il peut s'agir de choisir par exemple une solution curative, d'effectuer des ré-ordonnancements "locaux", de prendre en compte la stratégie de surveillance de l'entreprise, de déclencher des procédures d'urgence, etc.

Le concept de supervision s'applique dans un cadre hiérarchisé à deux niveaux au moins. A un niveau local, la supervision peut disparaître complètement (tout est prévu et figé à l'avance : la surveillance est intégrée à la commande). En revanche, à des niveaux plus abstraits, la supervision doit devenir prépondérante par rapport à la commande et à la surveillance.

1.4.3 La surveillance

La surveillance est chargée de recueillir en permanence tous les signaux en provenance du procédé et de la commande, de suivre en temps réel les évolutions du système commandé, de faire toutes les inférences nécessaires pour dresser des historiques de fonctionnement, et, le cas échéant, pour mettre en œuvre un processus de traitement de défaillance.

Dans cette définition, la surveillance est limitée aux fonctions qui collectent des informations, les archivent, font des inférences, etc., sans agir réellement, ni sur le procédé,

ni sur le système de commande. La surveillance a donc un rôle passif vis-à-vis du système de commande et du procédé. Étudions désormais les fonctions de base sur lesquelles s'appuient la supervision, la surveillance et la commande.

1.4.4 Les fonctions de supervision, de surveillance et de commande

Les fonctions présentées dans ce paragraphe sont utilisées pour concrétiser les opérations de surveillance et de commande des systèmes de production. Chacune de ces fonctions a un rôle particulier. Nous procédons à leur présentation en les regroupant par rapport à leur appartenance : supervision, commande et surveillance.

- **Fonctions de supervision :**
  - La décision (Combacau [1991]) : détermine un état accessible pour le retour au nouveau fonctionnement normal et les différentes actions correctives à suivre pour atteindre cet état.
- **Fonctions de commande :**
  - La commande (Belkadi [1989]; Huvenoit [1994]; Charbonnier et al. [octobre, 1994]) : son rôle est de faire exécuter un ensemble d'opérations par le procédé en fixant des consignes de fonctionnement en réponse à des ordres d'exécution. Elle pourra également être amenée à exécuter des opérations de test, de réglage, de nettoyage permettant de garantir que le système de production pourra assurer sa mission.
  - La reprise (de Bonneval et al. [1992]; Mabrouk et al. [1996]) : assure l'exécution d'une séquence d'actions correctives destinées à rendre au système de production tout ou partie des fonctionnalités requises pour assurer sa mission, la perte d'une partie des fonctionnalités initialement disponibles faisant suite à l'occurrence d'une défaillance,
  - L'urgence (Combacau [1991]; de Bonneval [1993]) : cette fonction est chargée d'appliquer des actions prioritaires et prédéfinies sur le système commandé afin d'assurer la sécurité de l'installation et du personnel.
- **Fonctions de surveillance :**
  - La détection (Holoway et Krogh [1990]; Combacau [1991]; Cruette [1991]; Toguyeni [1992]) : vérifie les services demandés en vue de repérer le fonctionnement normal ou anormal du système. Nous pouvons distinguer deux classes d'opérations anormales :
    - la première classe regroupe les situations correspondant au viol des contraintes du procédé (une collision par exemple),
    - la deuxième inclut les situations comprenant les lois de commande non respectées (par exemple les délais de fabrication).
  - Le diagnostic (Combacau [1991]; Chaillet [1995]; Hammami et al. [1995]) : établit un lien de cause à effet entre un symptôme observé et la défaillance qui est survenue, ses causes et ses conséquences. Cette fonction est généralement déclinée en trois sous-fonctions : la localisation détermine quel est le sous-système responsable de la défaillance, l'identification caractérise la cause de la défaillance et l'explication élabore les conclusions.

– Le suivi (Tawegoum [1995]; Zamaï [1997]) : cette fonction est chargée de maintenir en permanence un historique des traitements effectués pendant le processus de production et de conserver une trace des événements que perçoit le système.

Les fonctions que nous venons de présenter satisfont en partie les besoins de la commande, de la surveillance et de la supervision. D'autres sont requises comme par exemple le pronostic, la classification, etc., mais nous ne les considérerons pas dans notre approche. En revanche leur prise en compte sera bien entendu nécessaire dans le futur.

Partant de cet ensemble de fonctionnalités réparties en trois grandes catégories, nous nous proposons maintenant d'étudier leurs interactions. Cette étude s'appuie sur les travaux développés dans (Combacau [1991]).

1.4.5 Les niveaux d'intégration de la surveillance, de la commande et de la supervision

Jusqu'à présent, nous nous sommes attachés à décrire, d'un point de vue fonctionnel, les systèmes de commande, de surveillance et de supervision. En revanche, nous ne nous sommes pas préoccupés de l'interaction de ces systèmes. Faut-il en effet considérer les systèmes de surveillance-supervision comme intégrés au système de commande? séparés? ou encore mixtes?

La première approche consiste à intégrer la surveillance-supervision au système de commande. On parlera alors de *"surveillance-supervision intégrée"*. Ici, toutes les évolutions possibles du système commandé doivent être prévues hors ligne, que ce soit en fonctionnement normal ou anormal, afin de leur affecter un traitement spécifique. De cette façon, et en particulier sur l'occurrence d'une défaillance de la partie opérative, le système de commande-surveillance-supervision peut appliquer le "bon" traitement correctif. Cependant, ce concept d'intégration pose un problème majeur. Est-il toujours envisageable de modéliser exhaustivement le comportement du système commandé à la fois en fonctionnement normal et anormal? Ceci peut se concevoir aisément pour une machine simple dont l'interface est constituée de peu de capteurs/actionneurs. Mais qu'en est-il pour des niveaux de commande plus agrégés comme la coordination? Dans ce cas, la couverture totale des situations de défaillance est parfaitement illusoire. En conclusion, nous pouvons dire que ce type d'approche se prête bien à la commande de procédés non complexes et qui nécessitent de surcroît une forte réactivité. Dans un contexte de structure hiérarchique et modulaire, il est évident que l'intégration de la surveillance-supervision à la commande est à préconiser dans tous les modules du niveau local.

La deuxième approche revient à séparer le système de surveillance-supervision de la commande. On parlera alors de *"surveillance-supervision séparée"*. Ici, la commande a la charge du fonctionnement normal alors que la surveillance-supervision gère le fonctionnement anormal. Le principal avantage de cette approche réside dans le choix adapté des outils attribués à chacun des systèmes. Cependant, une telle séparation entraîne forcément un risque de conflits décisionnels. En effet, en présence de défaillances, la supervision peut être amenée à lancer des ordres (de reprise par exemple) vers le système commandé tout à fait contradictoires avec ceux de la fonction commande.

Une solution à ces problèmes consiste à jouer sur les avantages des deux approches précédentes. On parlera alors de *surveillance-supervision mixte*. Ici, la commande intègre un sous-ensemble de fonctions comme la détection et la reprise alors que les autres fonctions de surveillance-supervision sont séparées de la commande (Combacau [1991]). Dans

ce cas, le besoin de recenser toutes les situations de défaillance observables disparaît. En effet, seules les évolutions normales doivent être prises en compte ; toute évolution qui diffère de celle prévue par la commande est immédiatement considérée comme anormale. Dans ce cas, la détection (intégrée dans le système de commande) caractérise cette situation sous la forme d'un symptôme de défaillance afin que le reste des fonctions de surveillance-supervision (diagnostic, décision, etc.) prenne le relais.

Enfin, d'un point de vue mise en œuvre et en facteur à l'ensemble de ces approches, nous tenons à souligner l'attention qui doit être portée à l'attribution du canal de communication inter-modules de la structure décisionnelle. En effet, selon l'attribution de ce canal à tout ou partie des fonctions de surveillance-commande-supervision, le système peut, en présence de défaillances, se retrouver bloqué (par exemple, en attente d'un compte rendu qui n'arrivera pas, car la connectique du capteur est défectueuse). C'est le cas notamment lorsque que le canal de communication est la propriété exclusive de la fonction commande. Dans ce cas, le système de surveillance-supervision adjoint (comme une verrue!) au système de commande se retrouvera forcément séparé du système qu'il est sensé superviser!

1.5 Conclusion

Dans ce paragraphe nous avons présenté les concepts liés aux systèmes de production automatisés, leurs objectifs et les concepts liés aux éléments qui permettent d'atteindre ces objectifs. Nous avons montré les problèmes liés à la complexité des systèmes de production et la façon de faire face à ces problèmes grâce aux structures hiérarchiques et décisionnelles. Ensuite, nous avons présenté les concepts liés à la commande, chargés de tout ce qui correspond au fonctionnement normal des systèmes automatisés de production et les concepts correspondants à la surveillance, qui traite les problèmes de dysfonctionnement dans ces mêmes systèmes. Nous avons aussi présenté la supervision, chargée de la coordination entre la commande et la surveillance et les techniques utilisées pour faire cette coordination (surveillance intégrée, surveillance séparée et surveillance mixte). Cette partie a été consacrée à la présentation des concepts de base de notre travail. Maintenant nous présentons comment tous ces concepts ont été traités par différents laboratoires et organismes industriels français. Cette présentation a pour objectif de montrer les différents traitements des problématiques que nous avons mentionnés. L'étude critique des avantages et des inconvénients des approches présentées nous servira à identifier et à clarifier les besoins dans notre domaine de travail : *la surveillance-commande-supervision des systèmes automatisés de production.*

Chapitre 2

État de l'art

2.1 Introduction

Dans le chapitre précédent, nous avons été amenés à camper les bases de la commande, de la surveillance et de la supervision. Fort des concepts exprimés, nous nous proposons maintenant de dresser un état de l'art du domaine. Tout d'abord, nous commencerons par la présentation de travaux développées par des organismes industriels tels que l'ADEPA et l'EXERA. Ces approches traitent de la conception et de la conduite des systèmes de production. Nous poursuivrons avec la présentation de travaux effectués au sein de laboratoires universitaires. La première des approches présentées est développée au LURPA[1] de Cachan. Ces travaux concernent la sûreté de fonctionnement des systèmes réactifs. Ils proposent une méthode de spécification avec une couverture allant de la vérification du cahier des charges des systèmes à événements discrets jusqu'à la validation des spécifications décrites en Grafcet. Nous continuerons avec l'analyse d'une approche qui montre les principes de l'élaboration des lois de commande en utilisant une technique de synthèse basée sur les concepts de la théorie de la commande. Cette approche a été développée au LAI[2] de Lyon. Après l'examen d'un ensemble de travaux développées au LAIL[3] de Lille concernant la commande des systèmes de production et la gestion des modes, nous présenterons pour finir ceux développés au LAAS[4] de Toulouse orientés vers la surveillance, la commande et la supervision des systèmes de production. Chacune des approches présentées sera étudiée à l'aide de critères tels que le type de défaillances pris en compte, le niveau d'intégration des fonctions de surveillance-supervision, etc.

2.2 Guide des modes de marches et d'arrêts GEMMA et Guide pratique de spécification de la conduite des systèmes de production

Ce paragraphe présente deux approches développées par des organismes qui travaillent dans le cadre de la conception et du développement de la commande des systèmes automatisés de production.

1. Laboratoire Universitaire de Recherche en Production Automatisée
2. Laboratoire d'Automatique Industrielle
3. Laboratoire d'Automatique et d'Informatique de Lille
4. Laboratoire d'Analyse et d'Architecture des Systèmes

La première approche, le GEMMA, est définie comme un "outil-méthode" qui présente l'ensemble des modes opératoires qui peuvent être pris en compte au cours d'un cycle de production. Elle est constituée d'un guide graphique qui doit être complété progressivement lors de la conception du système (Figure 2.1). Le GEMMA répertorie ainsi 16 modes différents observables au cours d'un cycle de production. Un mode supplémentaire a été prévu afin d'identifier le système de production dans un état "hors-énergie". Ces modes sont regroupés en trois grandes familles : les procédures de fonctionnement, les procédures d'arrêt et de remise en route et enfin, les procédures en défaillance de la partie opérative. Chaque mode est représenté par un "rectangle-état" identifié par un code et par le nom du mode. Les relations entre les modes proposés sont matérialisées sous la forme de flèches.

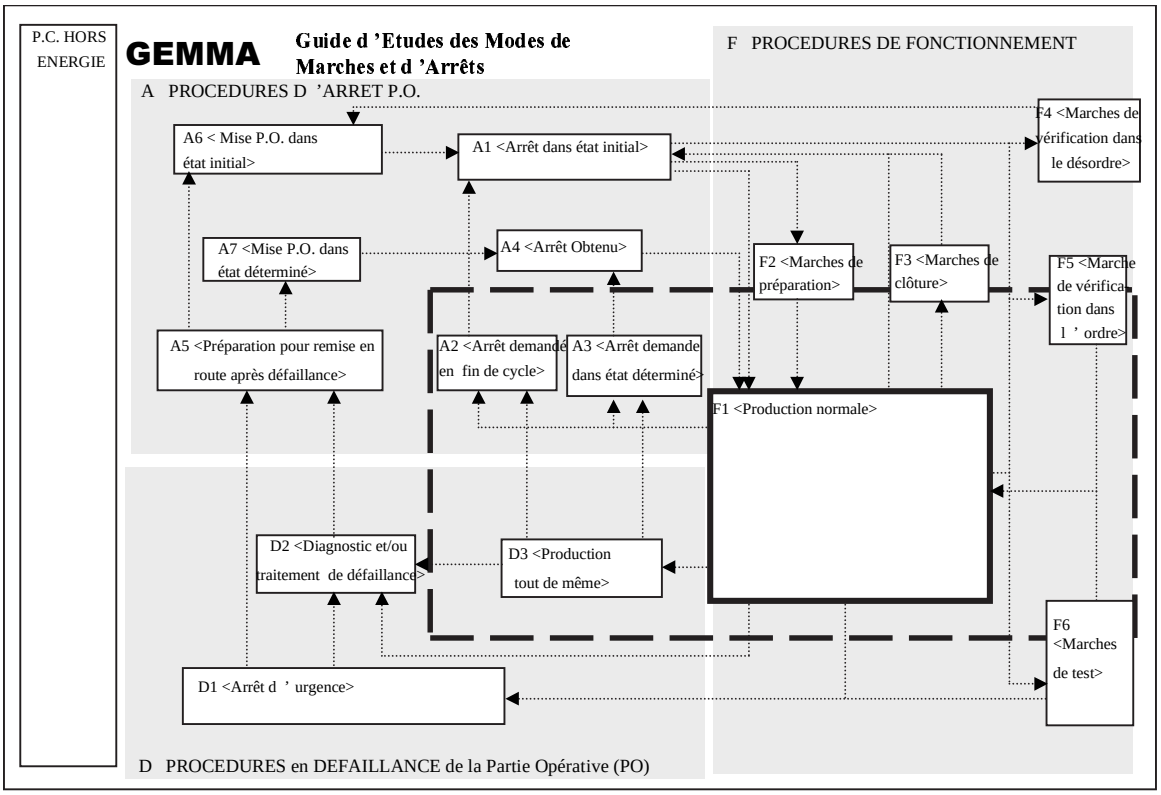

FIG. 2.1: *Le GEMMA: Guide d'Études de Modes de Marches et d'Arrêts*

La procédure utilisée dans cette approche est, en premier lieu, une sélection des modes qui correspondent aux phases de production autorisées par le concepteur de la commande. Une fois cette sélection effectuée, il lui revient la charge de spécifier les liaisons entre les modes choisis et les conditions d'évolution entre modes. La conception des Grafcets de commande (Blanchard [1979]; GREPA [1985]) correspondant à chaque mode est la dernière étape proposée par l'approche. Pour davantage d'informations, le lecteur pourra se reporter à (ADEPA [1981]) et (Moreno et Peulot [1997]).

Bien que novatrice et capitale dans la structure de la conception de la commande d'automatisme, cette approche présente néanmoins deux inconvénients majeurs. Premièrement, elle offre à l'utilisateur un cadre assez restreint et intuitif à la conception des grafcets de commande. Deuxièmement, elle ne fournit aucun outil formel pour la validation et la vérification des lois de commande obtenues.

Afin d'apporter un premier élément de réponse au premier problème, l'association

EXERA[5] en coordination avec Gimélec[6] a proposé la méthode DEMIOPS[7]. Cette méthode est basée sur une analyse fonctionnelle du système de production. Cette analyse conduit à décrire complètement les fonctions du système de production et leurs relations, qui sont systématiquement caractérisées, classées et évaluées. La taille et la complexité du système sont traitées par une application structurée de l'analyse fonctionnelle. La méthode consiste à décomposer le système de production en plusieurs entités fonctionnelles organisées dans une hiérarchie. Cette organisation rend possible la division du problème en plusieurs sous-problèmes, séparables et plus faciles à décrire. De cette façon, la description des installations est abordée progressivement au cours du développement du projet. Examinons maintenant plus en détail cette méthode.

Tout d'abord, le système de production est décrit systématiquement selon des points de vue différents. Ainsi, les objectifs du projet sont exprimés selon les points de vue "installation", "système", "sous-système" et finalement "machine". Dans chaque cas, il est nécessaire d'établir un niveau d'étude pour chaque phase du processus de production. Ce niveau correspond à la conception des étapes nécessaires pour accomplir les objectifs dans chaque phase de production. Une décomposition plus détaillée est ensuite proposée afin de définir les entités matérielles nécessaires pour assurer la fonction principale. Chacune de ces entités est appelée *bloc fonction*. Le bloc fonction permet de nommer l'objet à étudier en précisant son périmètre. Il représente et délimite les matériels permettant d'assurer une fonction principale sur un flux de produit(s) ou un lien physique. Un bloc fonction est défini à un niveau de description donné, il peut se décomposer en un ensemble de blocs fonctions qui seront donc situés à un niveau de description inférieur. Par exemple, le bloc fonction correspondant à un plus haut niveau correspond à l'usine alors que celui correspondant au plus bas niveau est une machine du système de production (Figure 2.2). Un bloc fonction a un fonctionnement qui lui confère le maximum d'autonomie par rapport à la fonction principale. Il est caractérisé par des états du procédé (marche normale, arrêt, en sécurité, etc.).

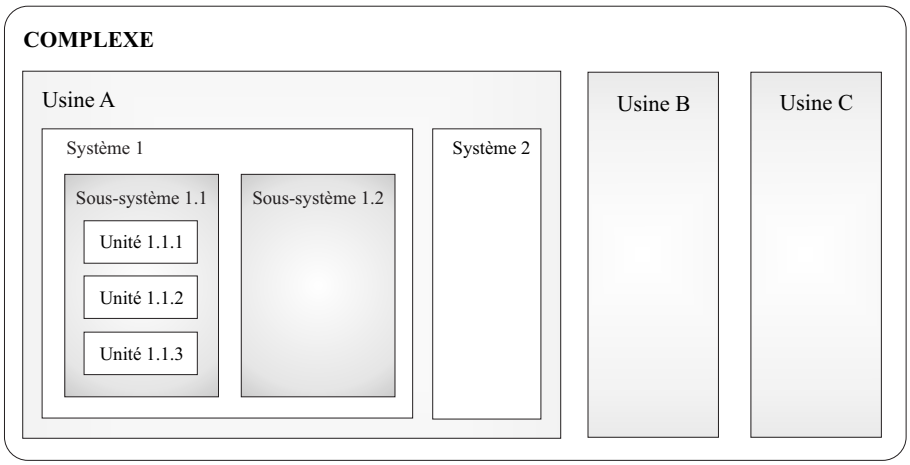

FIG. 2.2: *Décomposition d'une installation en blocs fonctions*

Une fois que les blocs fonctions ont été définis, il est nécessaire d'établir leurs relations ou *configurations*. Une configuration peut correspondre à une ou plusieurs phases de production permettant d'assurer des missions différentes ou de traiter un nouveau type de produit. Finalement, pour chaque bloc fonction, un graphe d'état (basé sur la norme IEC 1512 : *Model and terminology for batch control* ou sur le GEMMA) est élaboré. Il

5. Association des Exploitants d'Équipements de mesure, de Régulation et d'Automatisme
6. Groupement des Industries de l'Équipement Électronique, du Contrôle-Commande et des Services Associés
7. DEsign Method for Integrated Operation of Production System

permet de représenter tous les états nécessaires (recenser sans risque d'oublis les états importants), ainsi que les conditions de transition d'un état à l'autre. Cette procédure est présentée dans la Figure 2.3.

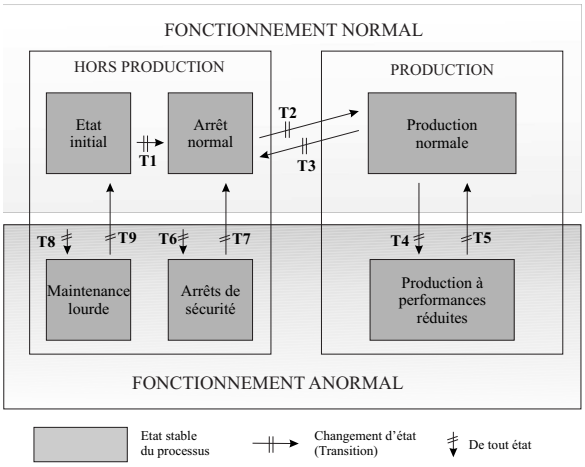

FIG. 2.3: *Exemple d'un graphe d'état défini pour un bloc fonction*

Cette approche offre une méthodologie pour la spécification de la commande sûre de fonctionnement d'un système de production. Elle propose ainsi une structuration pour la conception de la commande-surveillance-supervision. En ce sens, elle peut être caractérisée d'**approche intégrée**. Elle offre ainsi des avantages certains en terme de réactivité aux défaillances de la partie opérative puisque toutes les situations, normales ou anormales, auront été prévues à l'avance. Cependant, comme nous avons pu le signaler plus haut, elle n'est pas adaptée à la surveillance-supervision des procédés dits complexes bien que proposant une méthode de décomposition du problème. Enfin, nous pouvons regretter le manque de flexibilité lié au traitement de défaillances ; seules deux issues ont été prévues : états d'arrêt de sécurité ou production forcée dans le cas d'une défaillance prévue.

Afin d'apporter une solution à la carence d'outils formels pour la validation et la vérification du GEMMA, l'équipe ISA (Ingénierie des Systèmes Automatisés) du Laboratoire Universitaire de Recherche en Production Automatisée (LURPA) a proposé des travaux que nous exposons dans le paragraphe suivant.

2.3 Spécification et validation de cahier des charges de systèmes à événements discrets (LURPA-Cachan)

Les travaux de l'équipe ISA visent à assister et à optimiser les activités de conception de la commande et de la conduite des systèmes de production. Dans ce paragraphe, nous présentons brièvement une approche développée au sein de cette équipe.

En 1998, dans le cadre de la thèse (Lampérière-Couffin [1998]), une méthode permettant de couvrir les phases allant de la vérification du cahier des charges des systèmes à événements discrets à la validation des spécifications décrites en Grafcet est développée (Figure 2.4). L'objectif principal est de proposer des techniques de vérification et de validation formelles concernant à la fois des propriétés de sûreté et de vivacité.

La méthode utilisée pour la vérification et la validation de la spécification est basée sur une formalisation algébrique du cahier des charges (exprimé initialement en langage naturel) et du grafcet de spécification. Cette formalisation rend plus facile la vérification

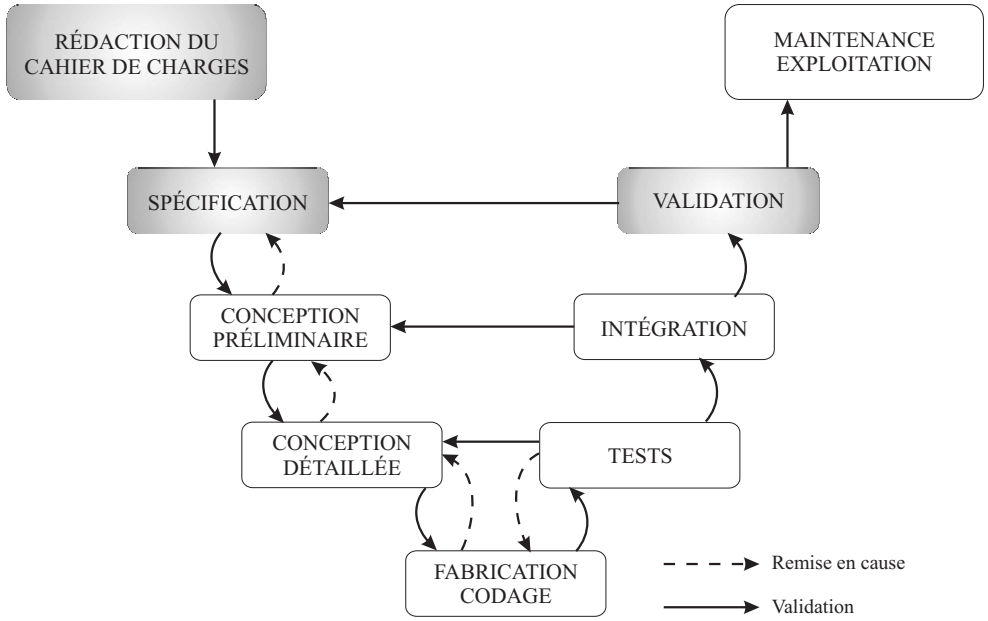

FIG. 2.4: *Cycle de vie des systèmes réactifs (Delfieu [1995])*

de ces éléments car ils sont décrits avec le même formalisme. La méthode adoptée est représentée dans la figure 2.5.

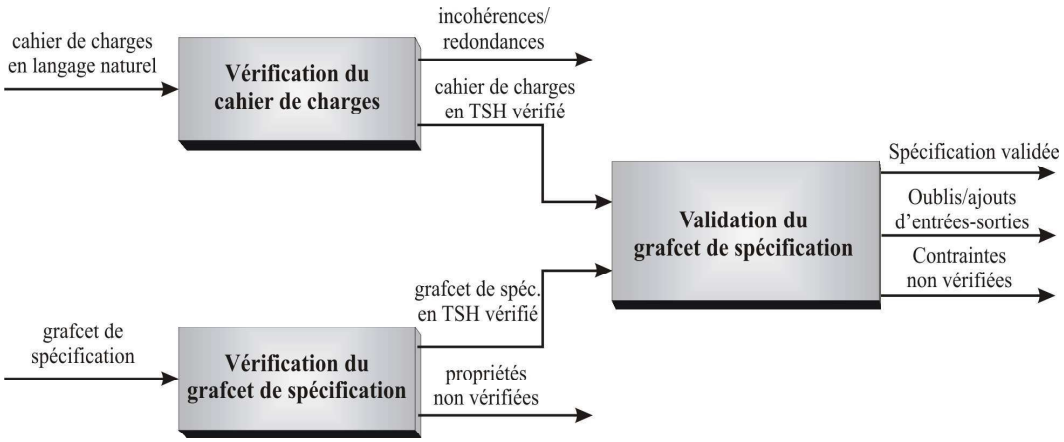

FIG. 2.5: *Méthode pour la validation d'un grafcet de spécification*

L'outil de modélisation Grafcet décrit un ensemble de règles qui doivent être vérifiées dans les grafcets de commande. La vérification du grafcet correspond à la vérification de ces règles. Elle comporte deux aspects : une vérification syntaxique et une vérification dynamique. La première vérification concerne les propriétés structurelles du grafcet (respect de l'alternance étape-transition, respect de la hiérarchie de forçage, etc.). Quant à la vérification dynamique, elle concerne les propriétés comportementales telles que réinitiabilité, stabilité, blocage, etc. (Delfieu [1995]).

La méthode de vérification de grafcet comprend 5 étapes (Figure 2.6).

1. vérification syntaxique du grafcet,

2. écriture du grafcet de spécification en TSH[8],

8. Théorie du Signal Hyperfini

3. déduction de propriétés dynamiques de la structure grafcet,

4. simplification des équations d'évolution du grafcet de spécification,

5. vérification des équations représentant le grafcet de spécification.

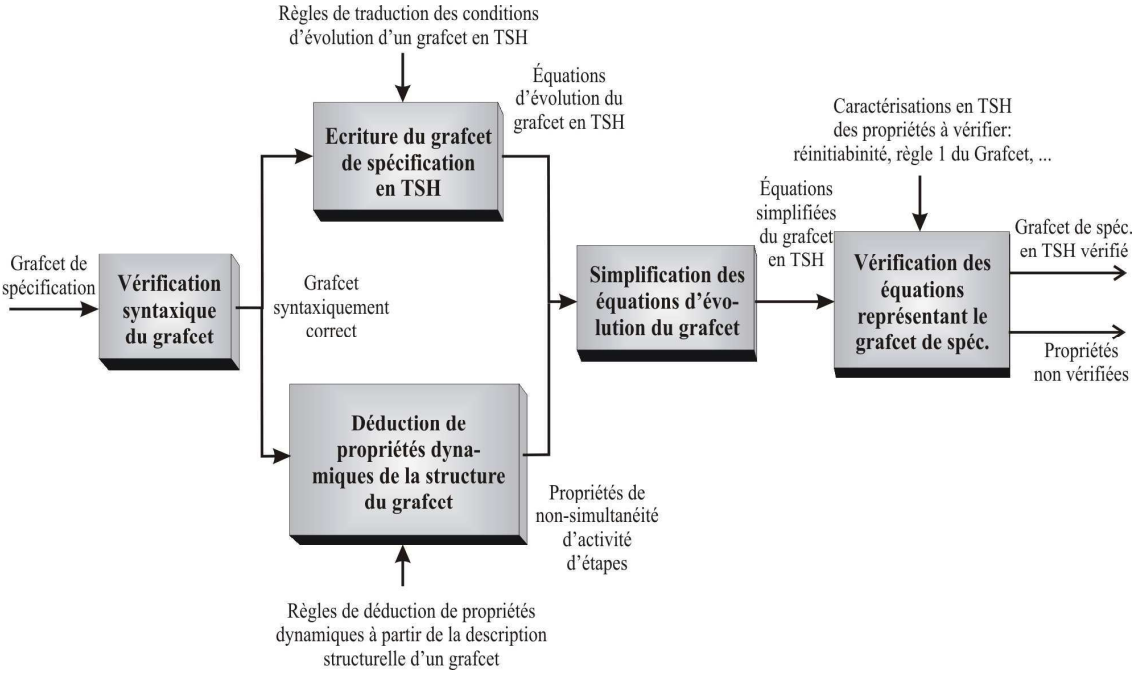

FIG. 2.6: *Méthode pour la vérification d'un grafcet de spécification*

Par ailleurs, la vérification des cahiers des charges représente la preuve de la cohérence des contraintes exprimées dans ce cahier, c'est-à-dire, l'élimination d'incohérences ou de redondances. Les incohérences correspondent aux contraintes impossibles à réaliser simultanément. Les redondances décrivent les contraintes exprimées plusieurs fois ou les contraintes induites par d'autres contraintes.

La modélisation du cahier des charges sous une forme algébrique a besoin d'une étape intermédiaire, l'expression du cahier des charges en logique temporelle. La logique temporelle a l'avantage de disposer des opérateurs proches du langage naturel (Figure 2.7). La logique utilisée pour la spécification des systèmes réactifs est la logique temporelle arborescente PCTL (Laroussinie [1994] . Ensuite, le cahier des charges est traduit en TSH (Frachet et al. [1996b,a]) afin qu'il puisse être vérifié à partir des expressions algébriques résultantes.

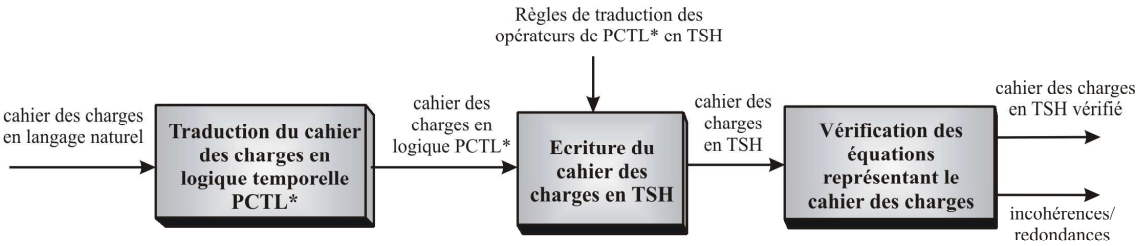

FIG. 2.7: *Méthode pour la vérification d'un cahier de charges*

Finalement, la validation du grafcet consiste à prouver que les évolutions possibles du grafcet satisfont bien aux propriétés extraites du cahier des charges. Elle est donc relative à l'existence ou à l'enchaînement des situations possibles du grafcet.

La validation du grafcet est effectuée en utilisant les représentations du cahier des charges et des évolutions du grafcet sous forme d'équations différentielles développées en TSH (Figure 2.8). En effet, puisque les spécifications du cahier des charges et le grafcet de spécifications sont représentées sous la forme d'équations, la démonstration des propriétés se ramène alors à la manipulation de ces équations en utilisant des techniques de calcul algébrique.

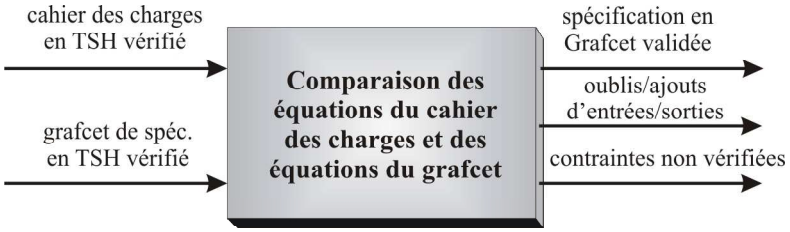

FIG. 2.8: *Méthode pour la validation de spécifications décrites en Grafcet*

Cette approche offre une méthode formelle pour vérifier la cohérence entre ce qui a été défini par l'utilisateur (cahier des charges) et les résultats obtenus en termes de commande (grafcet de commande). De plus, la technique proposée permet de valider ce grafcet afin de s'assurer qu'il vérifie les propriétés de sûreté et d'absence de blocages, propriétés primordiales dans la sûreté des systèmes (Zaytoon et al. [1997]). Du point de vue de la surveillance et de la supervision, cette approche prévoit des actions correctrices associées aux défaillances prévues dans le cahier des charges. En ce sens, cette approche peut être qualifiée d'approche intégrée. A ce titre, elle présente les avantages et les inconvénients inhérents à ce type d'approches. Enfin, nous remarquerons que la méthode proposée par cette approche pour prendre en compte les défaillances de la partie opérative s'appuie exclusivement sur l'analyse des risques selon un point de vue unique : la sécurité des hommes et des machines. Comme nous le verrons par la suite dans la partie III de ce mémoire, la sécurité n'est pas le seul critère qui doit être pris en compte lors de la spécification des traitements de défaillances, que ce soit pour une approche intégrée, séparée ou mixte. D'autres, comme par exemple des critères écologiques ou économiques, doivent être considérés.

2.4 Synthèse de commande des systèmes à événements discrets (LAI-Lyon)

Les travaux développés par l'équipe Sûreté et Supervision des Systèmes de Production (3SP) du Laboratoire d'Automatique Industrielle (LAI) de Lyon portent essentiellement sur la mise au point de techniques formelles pour la génération de lois de Commande sûres de fonctionnement. Leurs travaux sont basés sur la théorie de la commande proposée par Ramadge et Wonham [1987]. L'objectif est de définir l'ensemble des trajectoires qui correspondent aux spécifications souhaitées pour la commande d'un Système à Événements Discrets (SED) et ce en tenant compte de l'occurrence de défaillances de la partie opérative.

Le point de départ de cette approche consiste à spécifier l'ensemble des évolutions normales offertes par le procédé. Ces évolutions, encore appelées trajectoires, sont représentées ici par des automates. La deuxième étape consiste à demander à l'utilisateur de spécifier le cahier des charges : il s'agit de décrire l'ensemble des trajectoires souhaitées (type de programme, type d'outil à utiliser pour l'usinage, etc.). Lors de la dernière étape, l'ensemble des séquences qui vérifient les propriétés établies dans le cahier des charges sont

"extraites" du modèle du fonctionnement normal du procédé et des spécifications de commande.

A un niveau de détail accru, le procédé est vu comme un SED qui évolue spontanément suite à l'occurrence d'événements : les requêtes de commandes envoyées vers le procédé, sont les **événements contrôlables**, les comptes rendus émis par le procédé, sont les **événements incontrôlables**. Ainsi, le fonctionnement général peut être décrit comme un ensemble de séquences d'événements qui constituent le langage formel dans l'alphabet d'événements (Ramadge et Wohanm [1989]). Par exemple, considérons le comportement d'un robot d'assemblage. Ce dernier, à un niveau de modélisation agrégé, peut être observé via deux états : robot libre ou occupé. L'alphabet d'événements du système correspond aux situations qui provoquent le passage d'un état à un autre, c'est-à-dire, la mise en marche du robot (passage de l'état *robot libre* à l'état *robot occupé*) et la fin du travail du robot (retour vers l'état *robot libre*). Les événements contrôlables doivent donc être interdits ou autorisés selon l'état courant du procédé, ce qui n'est pas le cas pour les événements incontrôlables. Par exemple, dans le cas du robot, l'événement de mise en route est un événement contrôlé ; l'utilisateur peut décider de l'instant de démarrage du cycle d'assemblage. L'événement de fin d'assemblage est quant à lui complètement incontrôlable ; il peut se produire trop tôt, à temps ou encore pas du tout. Afin de contrôler les événements contrôlables, cette approche préconise l'usage d'un superviseur couplé au procédé (Figure 2.9). Ce superviseur est également un SED qui évolue selon les événements incontrôlables engendrés par le procédé. Le rôle de ce superviseur est bien entendu d'autoriser ou d'interdire l'occurrence d'événements dirigés vers le procédé. Par exemple, pour prendre une pièce, le robot doit au moins avoir sa pince ouverte. Si tel n'est pas le cas, l'événement "saisir pièce" doit être interdit.

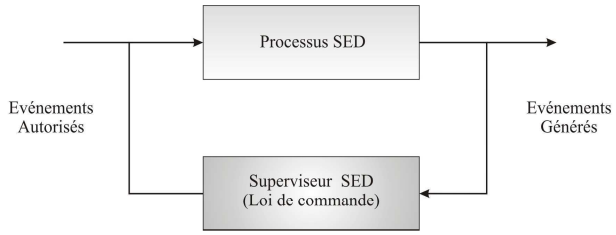

FIG. 2.9: *Schéma d'un processus supervisé : système en boucle fermée*

Si le procédé et le superviseur sont modélisés par des *acceptateurs* G et C (les acceptateurs sont des modèles qui acceptent un langage régulier), alors le langage de l'acceptateur global est obtenu en faisant le produit synchrone de $L(G)$ et de $L(C)$. De cette façon $L(C/G)$ représente le fonctionnement en boucle fermée. Cela revient ainsi à synthétiser un superviseur C où le comportement en boucle fermée C/G respecte la spécification. Ceci est réalisé via un *sous-langage suprême contrôlable*. Ce langage est obtenu par une composition du comportement du procédé et des contraintes de comportement qui conduisent à l'obtention des trajectoires de contrôle acceptées.

Les travaux récents de l'équipe 3SP du LAI portent sur des extensions de la théorie de la supervision ou théorie de Ramadge et Wonham. Le principe de base est la séparation entre le modèle des possibilités physiques du procédé commandé et le modèle des contraintes que le cahier des charges impose à ce même procédé commandé. Les modèles sont construits à partir d'automates à états, ce qui permet de construire facilement le composé de plusieurs modèles de procédé ainsi que le composé d'un modèle de procédé et d'un modèle de contraintes.

Les travaux menés ont porté sur des extensions de cette théorie : stabilisation de Systèmes à Événements Discrets (SED) à structures vectorielles (Sarri [1999]), supervision par structure hiérarchique distribuée (Chafik et Niel [2000]; Chafik [2000]) et recouvrement

de défaillances de SED temporels (Khatab [2000]). L'objectif suivi était, entre autres, de proposer des solutions au problème de l'explosion combinatoire en réduisant la taille des modèles (Niel et al. [2001]).

Des travaux menés actuellement (Kamach et al. [2002]) portent sur l'étude multi-modèles du procédé. Cette démarche consiste à construire des modèles différents d'un même procédé lorsque celui-ci se trouve dans des configurations répondant à des objectifs différents. Pour un système de production, ces différents objectifs correspondent par exemple à des modes de marches différents. En ne décrivant que des comportements pertinents du point de vue de l'objectif visé, chaque modèle est de taille plus réduite qu'un modèle devant permettre l'étude de tous les objectifs. Cependant l'utilisation de plusieurs modèles nécessite la mise en place d'un mécanisme de sélection du modèle utilisé ainsi que d'un mécanisme de suivi de l'état du procédé afin de permettre un changement cohérent de modèle.

De la même manière, les contraintes ne sont plus regroupées sous forme d'un superviseur centralisé, mais scindées en superviseurs propres à chaque modèle du procédé. Des mécanismes sont là aussi nécessaires pour sélectionner le superviseur actif et le changement cohérent de superviseur. De plus, les propriétés de blocage et de contrôlabilité nécessitent d'être redéfinies pour ces nouvelles structures.

Les travaux développés visent donc à spécifier hors ligne toutes les lois de commande-surveillance-supervision permettant de piloter un procédé de manière sûre (Nourelfath et Niel [2000]). Cette approche peut donc être classée dans la catégorie "approche intégrée" de commande-surveillance-supervision. Elle est donc soumise aux avantages et aux inconvénients classiques : forte réactivité mais inadéquation à la surveillance-supervision des procédés dits complexes même si, d'un point de vue commande, une technique de hiérarchisation des superviseurs est proposée ; il n'en demeure pas moins que toutes les défaillances ne pourront jamais être prévues à l'avance. En dehors de ces critiques classiques portant sur les niveaux d'intégration de la surveillance-supervision, nous devons retenir ici un avantage capital apporté par le LAI : une approche **formelle** de synthèse des lois de commande réactives. Cette synthèse s'appuie sur des règles permettant la validation et la vérification des lois de commande générées.

2.5 Reconfiguration et gestion des modes des systèmes automatisés de production (LAIL-Lille)

Les travaux de l'équipe Production Flexible Manufacturière du Laboratoire d'Automatique et d'Informatique industrielle de Lille concernent la sûreté et l'exploitation des systèmes de production. Nous commencerons par la présentation d'une approche développée en 1991 pour la vérification des ordres émanant du système de commande vers le procédé (Cruette [1991]). Dans cette approche, le modèle du procédé est utilisé en filtre de commande, positionné entre la partie commande et la partie opérative (procédé) au sein d'un module de surveillance (Figure 2.10).

Le rôle du filtre de commande est de s'assurer de la validité des consignes à envoyer vers le procédé selon son état courant. Ceci est rendu possible grâce à une remise à jour permanente du modèle. Le bloc de contrôle commande a un rôle coordonné à celui du filtre de commande. Il agit sur les comptes rendus émanant du procédé et non sur les consignes. Un contrôle de ces informations (filtres de valeurs de capteurs) permet alors de vérifier la réalisation des services demandés au procédé.

Lorsqu'une erreur de capteur est décelée (par le bloc contrôle de commandes), le bloc

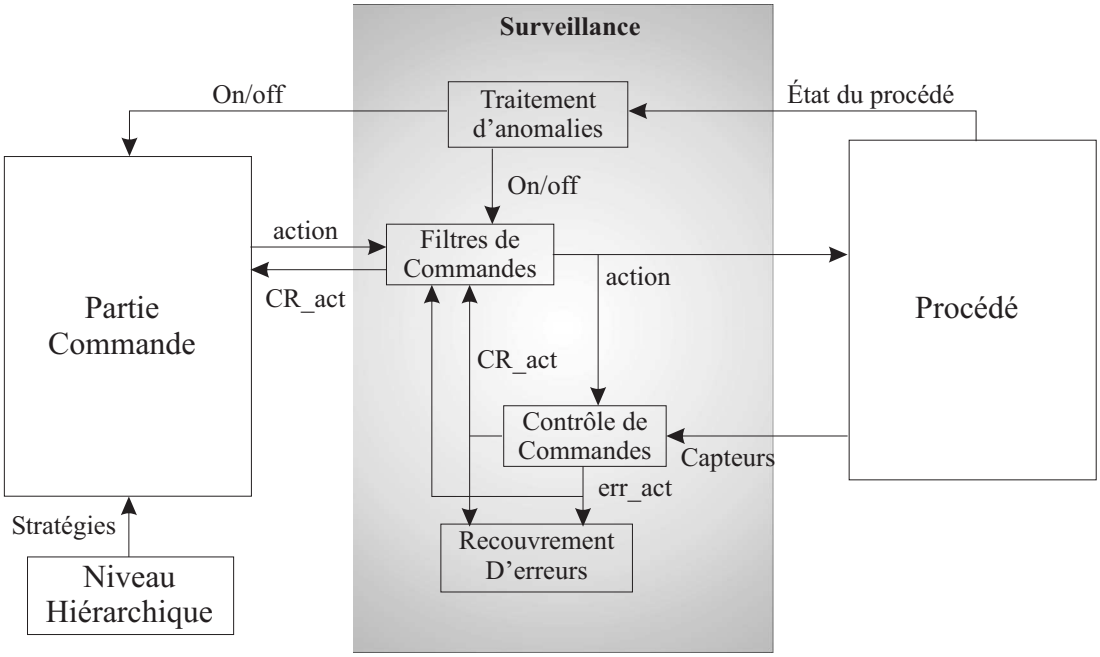

FIG. 2.10: *Représentation du modèle en filtre de commande*

de recouvrement des erreurs est activé afin de replacer la partie opérative dans un "état initialement souhaité par le système de commande" (Khattabi [1993]). Enfin, un bloc de traitement d'anomalies est chargé des défaillances matérielles inattendues. Son rôle est double : détecter ce type d'anomalies, puis gérer la mise hors service du composant à l'origine de la défaillance.

Cette approche a été étendue (Toguyeni et al. [1996]), par l'adjonction d'un système de supervision de la surveillance, du pilotage et de la gestion des modes de marches (Figure 2.11). La surveillance est toujours basée sur le principe du filtre pour détecter d'éventuelles évolutions anormales du procédé (détection). Ensuite, selon la gravité de la défaillance (étape de classification (Toguyeni [1992])), un recouvrement d'erreur est envisagé (conséquences graves de la défaillance) ou un diagnostic est lancé. Le pilotage est dédié quant à lui à la résolution des indéterminismes de la partie commande.

Une classification des ressources de production a conduit à considérer trois types de décisions de reconfiguration effective (Berruet et al. [1999]) :

- reconfiguration mineure : elle concerne uniquement les ressources engagées en production (ressources qui au début de l'horizon de production ont été mises en marche automatique),
- reconfiguration significative : elle concerne les ressources engagées et les ressources en attente (les ressources en attente sont des ressources initialisées qui peuvent être mises rapidement en marche automatique en cas de besoin),
- reconfiguration majeure : elle considère toutes les ressources du système de production.

La reconfiguration est mise en œuvre via la gestion des modes (Dangoumau et al. [2000]) et une phase de recouvrement (Figure 2.12). Ainsi, lors de l'occurrence d'une défaillance, la fonction de recouvrement a en charge de déterminer un état à partir duquel il est possible d'assurer la poursuite de la production. Lorsqu'une reconfiguration effective

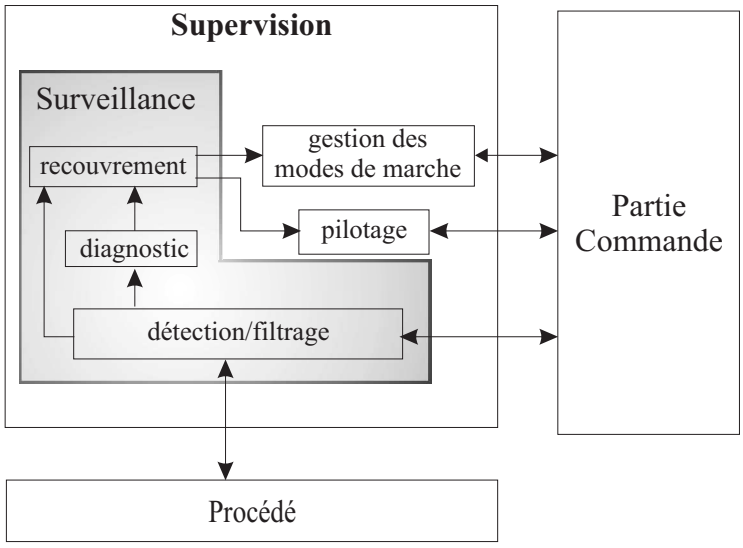

FIG. 2.11: *Représentation du modèle fonctionnel de la supervision*

du système est nécessaire, les décisions à prendre concernent les pièces en cours de production et les pièces brutes en entrée du système. Les décisions à prendre consistent alors à déterminer les ressources de production et les paramètres nécessaires pour réaliser une nouvelle gamme opératoire (partielle ou complète).

Comme nous avons pu le constater, l'approche développée au LAIL a fait l'objet de nombreux travaux de recherche couvrant tous les aspects de la commande, de la surveillance et de la supervision en mettant toujours l'accent sur la réactivité aux défaillances de la partie opérative et sur celles de la commande. D'un point de vue très général, l'approche globale peut être qualifiée de séparée. Elle bénéficie donc d'un avantage certain en terme de choix d'outils dédiés aux fonctions de commande, de surveillance et de supervision. Du point de vue des conflits décisionnels occasionnés par ce type d'approche en présence de défaillances, une solution semble avoir été apportée via l'outil de supervision basé sur le mécanisme de gestion des modes. Cependant, nous émettons quelques réserves quant à la position du bloc de détection/filtrage (filtre de valeurs de capteurs/filtre de commande). En effet, bien que l'approche propose tout un système de reconfiguration du procédé suite à l'occurrence de défaillances, il n'en demeure pas moins que le filtre de commande s'opposera à l'émission de requêtes de reconfiguration vers le procédé. En effet, celui-ci recevra des ordres incohérents par rapport à ceux attendus. Une démarche simple permettrait de résoudre ces problèmes en s'appuyant à la fois sur le mécanisme de commutation de modes et sur la spécification de plusieurs filtres (un par mode) autorisant ainsi des ordres compatibles avec le mode en cours. Cependant, si une telle démarche était mise en œuvre, le classique problème de couverture de toutes les situations possibles serait alors mis en exergue.

En sus de ces observations, nous pouvons également noter que cette approche n'exploite pas assez le concept des modes de marche. En effet, l'application d'une marche forcée (consistant à continuer à utiliser une machine/outil même en présence de défaillances) n'est pas prévue. Pourtant, en situation réelle, de nombreuses machines peuvent continuer à produire en marche dégradée. C'est le cas des tours à commande numérique qui, lorsqu'une qualité de fabrication stricte n'est pas requise, peuvent ignorer l'usure de l'outil de coupe (détection de vibrations anormales).

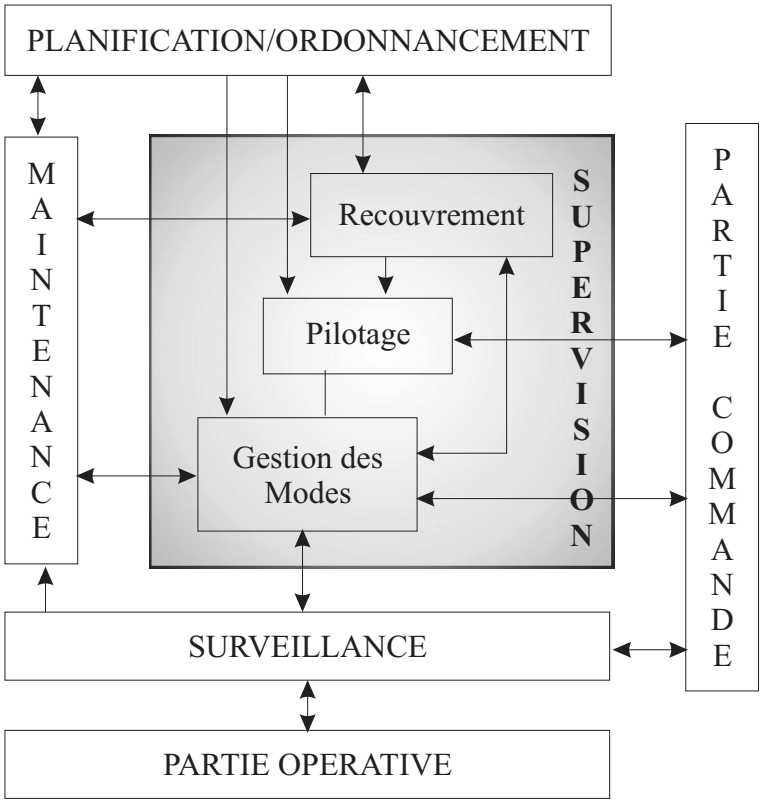

FIG. 2.12: *Structure de contrôle-commande intégrant la gestion de modes*

2.6 Commande et surveillance pour les systèmes à événements discrets (LAAS-Toulouse)

Ce paragraphe est dédié à la présentation des travaux développés au sein de l'équipe Supervision et Surveillance du groupe Organisation et Conduite des Systèmes Discrets (OCSD) du Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS) de Toulouse.

L'environnement général de l'approche est basé sur une structure hiérarchique et modulaire de commande, surveillance et supervision (Jones [1989], M.Combacau et al. [1998]). Tous les nœuds de la structure intègrent l'ensemble des fonctions de commande, surveillance et supervision décrites dans le chapitre précédent (cf. 1.4.4).

"Dans cette approche, la surveillance-supervision n'est plus vue seulement comme un palliatif à la commande" (Zamaï [1997]). Dans ce but, des propositions ont tout d'abord été apportées quant à la définition du rôle de la fonction décision. Une distinction a en effet été faite entre la phase d'élaboration des séquences de reprise (décision) et de sa mise en œuvre effective (reprise). Une fonction suivi a été ensuite définie pour satisfaire aux besoins de la surveillance en terme de mise à jour des modèles du procédé. Le rôle essentiel de cette fonction est d'absorber toutes les informations reçues par le module. Cela permet non seulement de recaler les modèles au plus prés de l'état réel du procédé, mais également d'assurer une grande précision dans l'historique des traitements associés aux produits considérés.

En sus de ces fonctions, l'auteur s'appuie sur d'autres fonctions (commande, détection et diagnostic) déjà proposées au sein de l'équipe OCSD dans des travaux antérieurs (Combacau [1991], Chaillet-Subias et Courvoisier [1996]). Ici, la détection est intégrée à la commande (Combacau [1991]). Le principe de fonctionnement est basé sur une coopé-

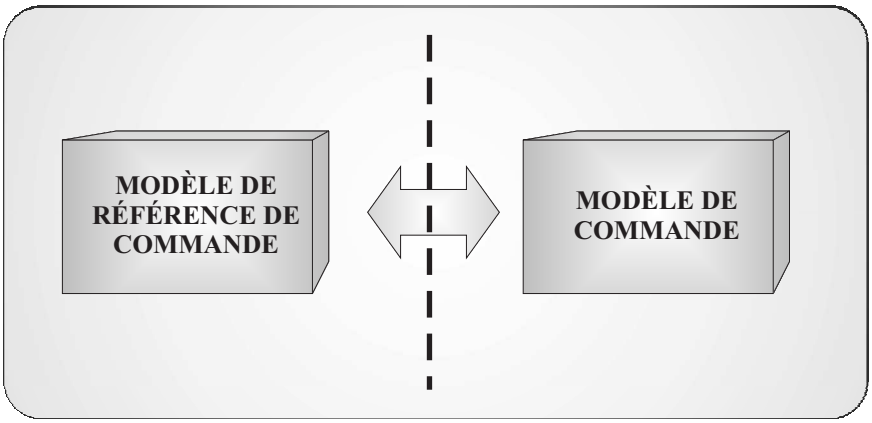

FIG. 2.13: *Représentation d'un module de contrôle-commande basé sur un modèle de référence*

ration dynamique entre un modèle de commande et un modèle de référence du procédé (cf. Figure 2.13). Le modèle du procédé modélise l'ensemble des états utilisables du procédé en y intégrant l'ensemble des contraintes physiques comme les ressources partagées, séquencements obligatoires, etc. Le bloc de commande contient quant à lui un modèle de la séquence opératoire devant être exécutée ; il s'agit là de l'ensemble des états autorisés dépouillés dans cette approche de toute contrainte physique. En effet, elles sont déjà représentées dans le modèle de référence. Lorsqu'une commande est émise vers le procédé, le modèle de référence est consulté pour vérifier si les ressources physiques nécessaires à cette opération sont disponibles. Si tel est le cas, l'ordre de commande est transmis au procédé sinon une erreur de commande est détectée. En retour, un compte rendu de commande est attendu par le bloc de commande. Si ce compte rendu ne traduit pas une évolution possible (analyse comportementale) de la séquence de commande, ou bien si ce dernier n'arrive pas dans les temps voulus (analyse temporelle), les fonctions de surveillance et de supervision doivent prendre le relais pour traiter la défaillance. A noter dans cette approche de la commande/détection que lorsque le compte rendu attendu est bloquant pour la commande (aucun état accessible), la détection consulte le modèle de référence (ensemble des états utilisables) pour vérifier si le compte rendu n'y traduit pas une évolution possible. Si tel est le cas, l'état réel du procédé peut alors être représenté. Une séquence de reprise pourra alors être envisagée.

Nous noterons dés à présent une caractéristique essentielle de cette approche : son aptitude à détecter toutes les défaillances de la partie opérative sans être condamnée à en dresser une liste exhaustive. Quelle que soit la nature du procédé, l'exploitation du modèle de référence et du modèle de commande permettent de caractériser quatre symptômes génériques de défaillances. Cet aspect sera repris de manière plus détaillée dans la partie III.

Les travaux de A. Chaillet (Chaillet [1995]) ont quant à eux porté sur la spécification d'un système d'information contenant toutes les informations relatives à la structure du procédé (entités physiques, liens entre ces entités, etc...) et requises par des fonctions telles que le diagnostic ou encore la décision. Ce système d'information a été mis en place en parallèle à la structure hiérarchique de commande surveillance (Figure 2.14). Un centre de gestion assure les différentes communications entre la structure hiérarchique et le système d'information en proposant divers services comme la "Recherche", la "Vérification", la "Mise à jour" ou la "Récupération". Une utilisation contrôlée de ces services permet de déclencher des diagnostics détaillés dans les modules concernés.

Dès lors, doté de ce pool de fonctions (détection, commande, suivi, diagnostic, décision,

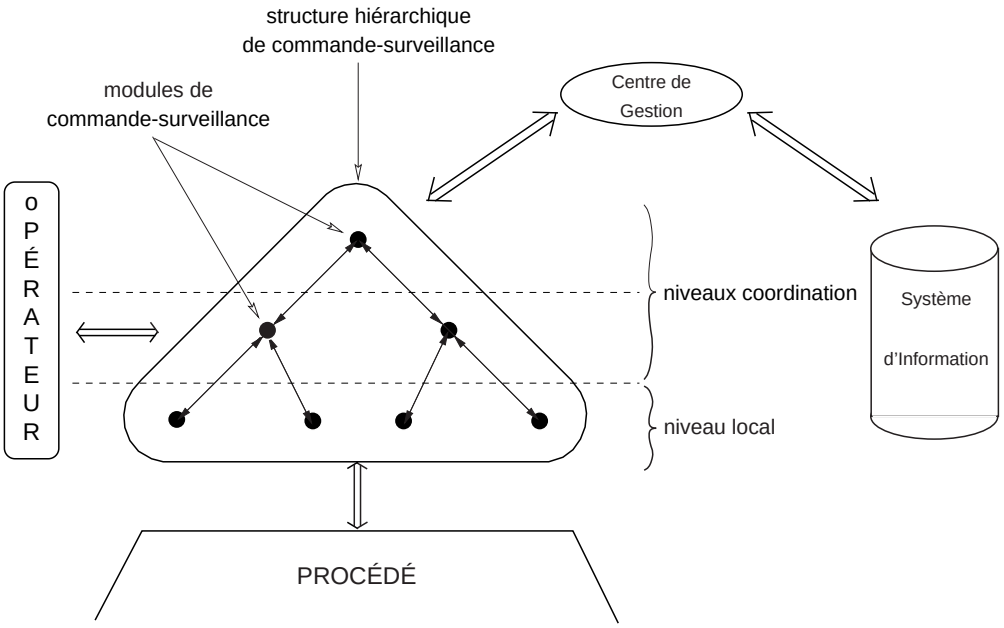

FIG. 2.14: *Architecture globale de l'approche LAAS*

reprise et urgence), E. Zamaï (Zamaï [1997]) a proposé une nouvelle structuration des modules de commande-surveillance-supervision de manière à accroître les performances de la surveillance : augmenter la réceptivité du module aux événements externes, étendre les traitements de surveillance applicables à ces perturbations et enfin laisser le choix à l'utilisateur des traitements qu'il souhaite réellement appliquer en présence de défaillances (Figure 2.15).

Pour accroître les performances du module en terme de réceptivité, une étude basée sur le formalisme SA-DT a été réalisée sur les flots d'informations qui sont susceptibles de transiter par le module. Elle a mis en évidence quatre catégories de données (Zamaï et al. [1998a]). A chaque instant, chacune de ces quatre catégories d'information est significative pour l'une ou plusieurs des fonctions de commande et/ou de surveillance. Un moteur d'exploitation a alors été élaboré pour prendre en compte ces informations et les aiguiller convenablement vers les fonctions adéquates. Dans le but de fournir à l'utilisateur l'ensemble des traitements de surveillance-commande qu'il est possible d'appliquer en présence d'une défaillance, un modèle (Zamaï et al. [1998b]) exhaustif de ces traitements a été proposé. Ce modèle est constitué des ressources physiques gérées par le module, des fonctions de surveillance, de commande et de supervision et des produits qui sont transformés par les ressources physiques. Ce modèle est basé sur le concept d'activités et sa structure de contrôle est générique. Chacune des activités le constituant est représentée par un n-uplet des différents éléments préalablement énumérés (M.Combacau et al. [1998]) (par exemple, le n-uplet <commande, détection, suivi, ressource, produit>caractérise une activité de commande en fonctionnement optimal). Une liste exhaustive des différents n-uplet (activités de surveillance-commande) participant à ces traitements (enchaînements d'activités) a été élaborée. L'existence d'un tel modèle de référence des traitements de surveillance-commande donne alors la possibilité à l'utilisateur de sélectionner les traitements qui satisfont les contraintes de production. Ces contraintes de production dépendent de celles imposées par la politique de production de l'entreprise (produire tout de même, tolérer quelques défaillances, bloquer la production quelle que soit la défaillance détectée, etc..) ainsi que celles imposées par la fabrication du produit. Les premiers pas vers le développement d'un outil de conception de ces stratégies ont été faits en proposant un guide méthodologique très intuitif visant à aider l'utilisateur dans cette tâche.

La solution globale proposée consiste donc à intégrer un superviseur (Zamaï et al.

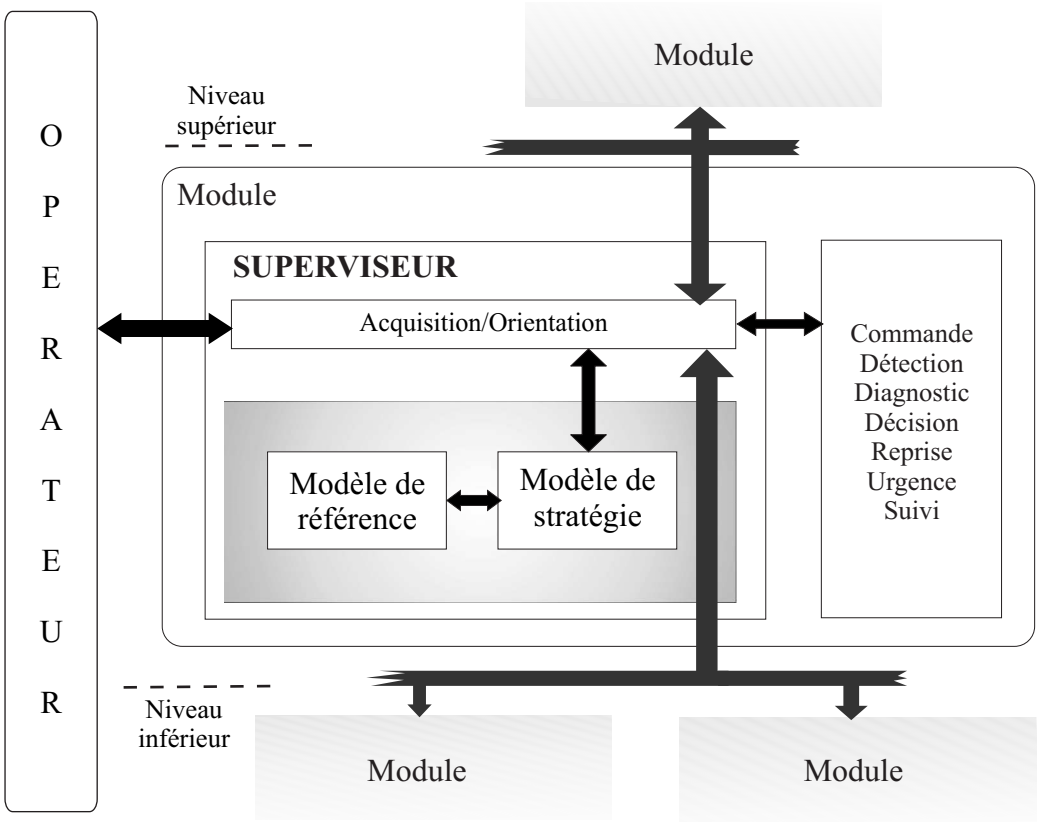

FIG. 2.15: *Représentation d'un module de surveillance-commande*

[1998b], Chaillet-Subias et al. [1997]) dans chacun des modules de la structure hiérarchique considérée. Ce superviseur est constitué des trois éléments décrits précédemment, à savoir les modèles de référence et de stratégie de surveillance-commande et le moteur d'exploitation. Ce dernier est chargé de la sélection de la ou des fonctions de surveillance, de commande ou de supervision vers lesquelles l'information doit être dirigée et du respect de la stratégie de surveillance imposée par l'utilisateur (organisation judicieuse des fonctions de surveillance, de commande et de supervision). D'un point de vue fonctionnel, lorsqu'une requête est reçue par le module, elle est orientée par le superviseur vers la ou les fonctions adéquates. Le superviseur crée alors le n-uplet correspondant pour prendre cette nouvelle activité de surveillance-commande-supervision en considération. Au contraire, dans le cas d'un événement issu du niveau inférieur, le superviseur l'orientera d'abord vers la ou les fonctions de surveillance-commande proposées par l'activité (n-uplet) en cours. Ensuite, selon le résultat de la prise en compte de l'événement, une nouvelle activité sera créée par le superviseur pour représenter l'évolution du traitement de l'événement imposé par la stratégie de surveillance (Alligier [2001]).

Les travaux plus récents de l'équipe Supervision Surveillance de du groupe OCSD s'orientent désormais d'une part vers la spécification et la mise en œuvre d'une fonction de pronostic (M.Combacau et al. [2001]) et d'autre part vers une réflexion de fond portant sur l'extension de l'approche globale dans le cadre d'une structure distribuée.

Les travaux proposés par le LAAS traitent donc de la surveillance temps réel des défaillances du procédé. L'approche globale se prête aussi bien à une approche séparée que mixte. En revanche, étant donné sa complexité, elle sera davantage préconisée pour les niveaux hauts de la commande hiérarchisée plutôt qu'au niveau local.

L'avantage essentiel de cette approche concerne la proposition du modèle de référence

pour la surveillance-commande-supervision qui représente toutes les façons de surveiller, superviser et commander un procédé industriel, que ce soit en situations normales ou anormales. Ainsi, connaître hors ligne ces différents traitements ouvre des perspectives très intéressantes pour concevoir des stratégies de surveillance-supervision. Il est important de noter de surcroît que cette approche propose également un guide méthodologique d'élaboration des stratégies de surveillance-supervision en tenant compte de certains besoins industriels. Nous noterons enfin, que cette approche se prête bien à une automatisation partielle des fonctions de surveillance, à la demande des utilisateurs. L'opérateur humain peut en effet se substituer à tout ou partie du système sans que cela ne nuise à son fonctionnement.

Néanmoins, nous pouvons énumérer quelques limitations de cette approche. En premier lieu, parmi les 31 activités de surveillance-commande-supervision que l'auteur propose, certaines sont ambiguës. C'est le cas de l'activité 45 (R, Dt, Sv, Dg) qui est définie de trois façons différentes :

1. un diagnostic est demandé par le niveau supérieur alors que le système se trouvait dans un état de repos (activité minimale de surveillance, (R, Dt, Sv)),

2. un diagnostic est en cours d'élaboration,

3. suite à une situation d'urgence, le diagnostic qui avait été lancé n'est pas encore achevé. Le fait de ne pas connaître exactement dans quelle situation le système se trouve peut nous conduire à une mauvaise prise de décision. En effet, les actions à suivre après un diagnostic ne seront pas les mêmes selon que le système se trouve dans une situation d'urgence ou non.

En second lieu, l'utilisation d'un critère réducteur pour l'obtention des activités de surveillance-commande est assez problématique. Dire que l'urgence et la détection (contrainte 3) ne doivent pas être activées en même temps est aberrant. Une détection est nécessaire même en situation d'urgence. Par exemple, dans le cadre du pilotage d'un robot industriel, si, suite à la détection d'une collision, une procédure d'urgence est lancée, il n'en demeure pas moins qu'il est nécessaire de surveiller tous les capteurs de sur-course. Ici, la désactivation de la fonction détection entraînera des dommages rédhibitoires pour le robot. La fonction détection est donc indispensable.

Enfin, cette approche propose d'intégrer les besoins des industriels (qualité de fabrication et productivité) afin de surveiller-superviser au mieux leurs installations via une stratégie de surveillance. Cependant, comment surveiller au mieux une installation sans prendre en compte ses propres modes de marches et d'arrêts?

2.7 Conclusion

Au travers de ce chapitre, nous avons défini le contexte de notre étude au travers d'un ensemble d'approches de surveillance, de commande et de supervision proposées à la fois par des organismes industriels et des laboratoires de recherche universitaires. Pour chacune de ces approches, nous avons montré leurs caractéristiques principales, leurs avantages et leurs inconvénients. Ces approches ont été analysées selon plusieurs critères comme le type de défaillances prise en compte, le niveau d'intégration des fonctions de la surveillance-supervision, la technique de détection préconisée ou encore le degré de réactivité aux défaillances de la partie opérative.

Dans le cadre des approches dites intégrées, nous avons pu également mettre en exergue qu'un effort incontestable a été fait en faveur de méthodes de synthèse de lois de commandes sous des formes certes différentes (GEMMA/EXERA ou encore théorie de la commande LAI) mais qui concourent cependant au même but. Cet effort doit être maintenu ne serait-ce que pour des raisons évidentes d'intégration dans le milieu industriel (Regimbal [2002]), de vérification de l'adéquation des lois de commande générées et enfin de validation. Quelles que soient les propositions faites dans ce sens, nous avons pu noter qu'un modèle du fonctionnement normal de la partie opérative était requis afin d'en extraire la loi de commande répondant au cahier des charges.

En revanche, dans le cadre des approches dites mixtes voire même séparées, cet effort reste sans aucun doute insuffisant. Seule l'approche proposée par le LAAS dans Zamaï [1997] ouvre des perspectives intéressantes dans ce sens via les concepts de modèles de référence pour la surveillance-commande, et le modèle de stratégies de surveillance. Cependant, comme nous avons pu le noter, la méthode de génération des lois de surveillance proposée s'apparente plus à une démarche "intuitive" qu'une démarche formelle telle que proposée dans (Ramadge et Wonham [1987]).

Compte tenu de ces conclusions, nous nous proposons maintenant de dresser l'ensemble des hypothèses de travail de l'approche de surveillance, commande et supervision que nous proposerons dans les parties II et III de ce mémoire.

Chapitre 3

Cahier des charges de notre approche

3.1 Introduction

Dans le chapitre précédent, nous avons présenté un ensemble de travaux qui s'attachent aux problèmes de commande, de surveillance et de supervision pour les systèmes automatisés de production. Une étude critique présentant les avantages et les inconvénients de chacune de ces approches a été faite.

Dans ce chapitre, nous nous proposons d'exposer les besoins de la surveillance et de la supervision afin d'une part de sélectionner la ou les approches les plus appropriées, d'autre part de mettre en exergue nos hypothèses de travail et enfin de présenter au lecteur le positionnement de notre contribution.

3.2 Spécification des besoins

Notre approche de la surveillance et de la supervision des procédés industriels se caractérise essentiellement par une volonté forte en terme de flexibilité. En ce sens, nous souhaitons proposer une démarche la plus complète possible permettant à un industriel de spécifier, concevoir et mettre en œuvre sa propre stratégie de surveillance répondant au mieux à ses besoins.

Cependant, avant de présenter plus en détails notre cahier des charges, nous nous proposons de récapituler l'analyse faite au chapitre 2 sous la forme d'un tableau comparatif.

3.2.1 Synthèse des travaux

Le tableau 3.1 présente un comparatif entre les approches présentées dans le chapitre 2 de ce document.

Cette comparaison nous permet d'identifier un ensemble de besoins qui doivent être pris en compte dans le domaine de la surveillance, de la commande et de la supervision. Ils sont détaillés dans le paragraphe suivant.

	Démarche de synthèse	Type d'approche	Lois de surveillance adaptées
(ADEPA, 1981)	Intuitive	Intégrée	Non
(Exera, 1998)	Intuitive	Intégrée	Non
(Lampérière, 1998)	Formelle	Intégrée	Non
(Niel, 1996)	Formelle	Intégrée	Non
(Cruette, 1991)	Intuitive	Intégrée	Non
(Toguyeni, 1996)	Intuitive	Intégrée	Non
(Dangoumau,2000)	Intuitive	Intégrée	Non
(Combacau, 1991)	Intuitive	Mixte	Non
(Zamaï, 1997)	Intuitive	Mixte/Séparée	Oui

TAB. 3.1: *Tableau comparatif entre les approches de commande, de surveillance et de supervision présentées*

3.2.2 Besoins de la surveillance et de la supervision

L'étude bibliographique menée nous a permis d'identifier les besoins réels de la surveillance et de la supervision. Nous nous proposons maintenant d'exposer ces besoins, repris de chacune des approches étudiées, sous la forme d'une liste.

Précisons cependant que nous nous plaçons désormais volontairement dans le cadre de la surveillance et de la supervision de procédés dits complexes et que notre approche trouvera sa place à des niveaux de commande supérieurs à celui de la commande locale. De ce fait, notre approche ne peut être classée en tant qu'approche intégrée de surveillance-supervision. Elle se qualifie donc tout naturellement en tant qu'approche séparée et pourra être facilement étendue à une approche mixte ; ceci dépendra de la mise en œuvre des fonctions de surveillance, de commande et de supervision.

1. *Nécessité de disposer de toutes les fonctions de surveillance et de supervision.* Il va de soi que dans le cadre d'une approche séparée ou mixte, le système réactif doit s'appuyer sur des fonctions telles que la détection, la commande, le suivi, le diagnostic, la décision, la reprise ou encore l'urgence. Seules les approches développées au LAIL et au LAAS proposent actuellement un tel niveau d'intégration.

2. *Nécessité de garantir l'acheminement de l'information même si la commande se trouve bloquée.* Tel que nous l'avons vu précédemment, le fait de baser le fonctionnement du système de surveillance sur le fonctionnement du système de commande provoque des blocages qui empêchent la surveillance et/ou la supervision de réaliser correctement leur travail. L'approche développée au LAAS répond parfaitement à cet objectif. Elle propose en effet un "superviseur" basé sur un moteur d'exploitation capable de prendre en compte toutes les informations issues à la fois des niveaux supérieurs (requêtes), des niveaux inférieurs (informations, comptes rendus, remises en cause, etc.), des informations reçues et données par un opérateur humain et enfin des informations provenant d'un système d'information.

3. *Nécessité de proposer plusieurs traitements de défaillances (flexibilité des traitements).* Hormis les approches dites intégrées, seule l'approche proposée par le LAAS offre des traitements de surveillances adaptables en fonction des besoins des industriels. Ceci permet de changer radicalement la vision classique de la surveillance qui

consistait, et ce quelle que soit la défaillance, à lancer toujours le même traitement, à savoir : détection, diagnostic, décision puis reprise. D'autres sont désormais proposés comme par exemple diagnostiquer tout en continuant à commander le procédé.

4. *Nécessité de disposer d'une bibliothèque de l'ensemble des traitements de surveillance.* Bien entendu, ce point du cahier des charges découle directement du point précédent. Pour qu'un médecin puisse proposer des traitements adaptés à son patient, le dictionnaire VIDAL (VIDAL [2002]) lui propose non seulement toute une "batterie" de médicaments, mais également toutes les façons de les combiner entre eux afin de guérir au mieux le patient. C'est ce que propose Eric Zamaï dans sa thèse via le modèle de référence pour la surveillance.

5. *Nécessité de s'appuyer sur une technique de synthèse des stratégies de surveillance-supervision.* Si nous reprenons l'exemple du médecin, nous pouvons affirmer que sans les études qu'il a suivi, il serait incapable de traiter correctement un patient, même s'il dispose du VIDAL. Nous pouvons donc retenir de cet exemple que sans la technique d'exploitation, ce dernier n'est d'aucune utilité. Il en va de même pour l'exploitation du modèle de référence proposé dans (Zamaï [1997]). Le guide proposé est malheureusement trop intuitif pour aborder efficacement la génération des stratégies de surveillance. En revanche, bien que dédiée à la spécification hors ligne des traitements de défaillances, l'approche développée au LAI est du plus grand intérêt pour ce qui est de la synthèse des lois de commande sûres. Une projection évidente doit être envisagée pour la surveillance et la supervision temps réel. Le même constat sera fait pour les travaux développés dans le cadre de l'EXERA.

6. *Nécessité de disposer d'une technique de détection de défaillances qui ne soit pas basée sur le recensement exhaustif des défaillances de la partie opérative.* L'identification de toutes les situations de défaillance qui peuvent se présenter au niveau d'un procédé complexe peut devenir très difficile, voire impossible. Une technique générique de caractérisation des symptômes de défaillances est donc requise. Ceci est proposé au LAAS dans (Combacau [1991]).

7. *Nécessité d'intégrer dès la phase de conception les modes de marches et d'arrêts.* Il va de soi qu'une défaillance sera certainement traitée différemment selon que le procédé se trouve en fonctionnement normal ou dégradé. Par ce simple constat, nous pouvons déjà imaginer que plusieurs stratégies de surveillance-supervision peuvent être établies pour chaque mode proposés dans le GEMMA. Ceci n'est pas intégré dans l'approche LAAS. Une extension de cette approche par le GEMMA nous semble donc incontournable.

3.3 Proposition de notre contribution

Compte tenu du cahier des charges de la surveillance et de la supervision spécifié dans le paragraphe précédent, nous nous proposons tout d'abord de dresser une liste exhaustive des hypothèses de travail sur lesquelles notre approche s'appuie, puis de proposer la démarche que nous avons retenue pour notre contribution.

3.3.1 Hypothèses de travail

Au regard de l'analyse des besoins que nous avons précédemment menée, nous avons pu dégager l'adéquation de certaines approches à nos besoins. En premier lieu, nous

pouvons dire que l'approche développée au LAAS couvre une grande partie de ces besoins : elle est dédiée à la commande, à la surveillance et à la supervision des procédés industriels complexes, elle garantit la prise en compte permanente des informations transitant à travers la structure décisionnelle, elle propose toutes les fonctions de surveillance et de supervision requises, elle met à disposition un modèle de référence des activités de surveillance et de supervision ainsi que la façon de les utiliser et enfin elle propose un guide intuitif d'élaboration des stratégies de commande, surveillance et supervision. En revanche, elle n'intègre pas les modes de marches et d'arrêts proposés dans le GEMMA par l'ADEPA et ne propose pas de technique de synthèse formelle des stratégies de surveillance telles que peuvent le proposer les équipes 3SP du LAI, ISA du LURPA ou encore l'EXERA.

En conséquence, nous proposons dans le cadre de nos travaux d'étendre l'approche développée au LAAS en intégrant les avantages des approches proposées par le LAI, le LURPA, l'EXERA et l'ADEPA. Notre approche adopte donc au final les hypothèses générales de travail suivantes :

1. adoption de la terminologie proposée par le groupe de travail ASSF du GRP,
2. surveillance, commande et supervision des procédés complexes industriels,
3. structure hiérarchique et modulaire de surveillance, de commande et de supervision,
4. disponibilité des fonctions de détection, diagnostic, commande, décision, reprise, suivi et urgence,
5. approche séparée ou mixte (Combacau [1991]),
6. intégration du superviseur proposé par E.Zamaï (Zamaï [1997]) au sein de tous les modules de la structure décisionnelle ; le superviseur conservera, sur le principe, son modèle de référence et son modèle de stratégie de surveillance,
7. utilisation du mécanisme de détection proposé dans (Combacau [1991]),
8. prise en compte des modes de marches proposés dans le GEMMA par l'ADEPA,
9. prise en compte des travaux portant sur la synthèse des lois de commande proposés par le LAI, le LURPA et l'EXERA.

3.3.2 Contribution : démarche retenue

Notre contribution portera donc sur l'extension de l'approche proposée par E.Zamaï dans sa thèse. Cette extension concernera exclusivement le modèle de référence pour la surveillance, la commande et la supervision ainsi que la technique de génération des lois de surveillance et de supervision.

Dans ce but, nous proposerons en premier lieu une révision importante du modèle de référence. Comme nous le verrons dans la partie II, cette révision portera non seulement sur la modification de certaines contraintes telles que l'exclusion mutuelle entre la détection et l'urgence, mais également sur l'intégration des modes de marches et d'arrêts du GEMMA.

En second lieu, nous proposerons une amélioration significative du guide intuitif de génération des lois de surveillance-supervision à partir du modèle de référence. L'objectif

majeur visé consiste à mettre à disposition de tout exploitant, une démarche de conception simple et rigoureuse, s'appuyant sur des outils connues du mode industriel, comme le GEMMA par exemple. Cette technique s'appuiera non seulement sur un changement d'outil de modélisation du modèle de référence, sur la spécification des critères qui doivent être pris en compte pour synthétiser une loi de surveillance-supervision, et enfin sur la proposition d'une technique d'intégration de ces critères au sein du modèle de référence afin d'en déduire la loi de surveillance-supervision correspondante.

3.4 Conclusion

Dans le cadre de ce chapitre, nous avons présenté les besoins liés à l'intégration d'un système de surveillance et de supervision au sein d'une architecture décisionnelle hiérarchique et modulaire. Ces besoins se sont exprimés selon sept points. Premièrement, une approche de surveillance, commande et supervision doit au moins s'appuyer sur des fonctionnalités telles que la détection, la reprise, la décision, la commande, le suivi, le diagnostic et encore l'urgence. Deuxièmement, ces fonctions doivent être "alimentées" par des informations pertinentes ("au bon moment, au bon endroit, à la bonne personne") en fonction du contexte de production. Troisièmement, il a été démontré de l'utilité de pouvoir développer des traitements de défaillances flexibles (organisation du travail des fonctions de surveillance, commande et supervision), et donc adaptés aux besoins des industriels. Quatrièmement, la nécessité de se doter d'une "bibliothèque" des traitements de défaillances utilisables a été mise en évidence (modèle de référence). Cinquièmement, nous avons proposé d'intégrer à ce modèle de référence les modes de marches et d'arrêts issus du GEMMA. Sixièmement, sur la base des besoins exprimés par un industriel, et avec le support du modèle de référence, une technique de synthèse de lois de surveillance doit être proposée afin de systématiser la phase de conception et d'intégration de ces lois en entreprise. Enfin, nous avons mis en exergue l'utilité d'appuyer notre approche sur une fonction de détection générique et donc indépendante de la complexité du procédé considéré.

Au terme de ce chapitre, nous avons délimité le contexte de notre contribution et proposé la démarche retenue que nous allons détailler dans la suite de ce mémoire.

Deuxième partie

Extension du modèle de référence

Chapitre 1

Analyse du Modèle de Référence

1.1 Introduction

Parmi les apports de l'approche proposée par le LAAS dans Zamaï [1997], le modèle de référence pour la surveillance, la commande et la supervision est sans aucun doute le plus important. Il représente en effet une "cartographie" de tous les traitements de défaillances de la partie opérative applicables en entreprise. Ce modèle de référence, élaboré hors ligne, bénéficie d'une structure de contrôle parfaitement générique et donc adaptée à tous les procédés industriels quelles que soient leur nature ou leur taille.

Afin de mieux appréhender les modifications importantes que nous apporterons au sein des chapitres 2 et 3 de cette partie, nous nous proposons ici d'exposer plus en détails ce modèle de référence. A cette fin, nous commencerons tout d'abord par présenter ses caractéristiques essentielles (fiche technique). Après quoi, nous exposerons la technique de conception du modèle développée par l'auteur. Nous terminerons alors ce chapitre par une analyse fine des points faibles du modèle.

1.2 Caractéristiques du modèle de référence

Le modèle de référence définit l'ensemble des états utilisables que doit proposer un système de surveillance, commande et supervision efficace. Il propose actuellement 31 activités de référence, 165 façons de les enchaîner et plus de 336 arcs. Un extrait du modèle est donné dans la figure 1.1.

Les caractéristiques essentielles de ce modèle peuvent être énumérées comme suit :

1. il est modélisé sur la base des "réseaux de Petri à objets" (Valette [1995], David et Halla [1992]) ;
2. la structure de contrôle du réseau est générique ;
3. le marquage initial du réseau comporte deux volets :
   - les fonctions de surveillance-commande-supervision (comme la détection, la commande, etc),
   - les ressources qui dépendent de l'atelier ;

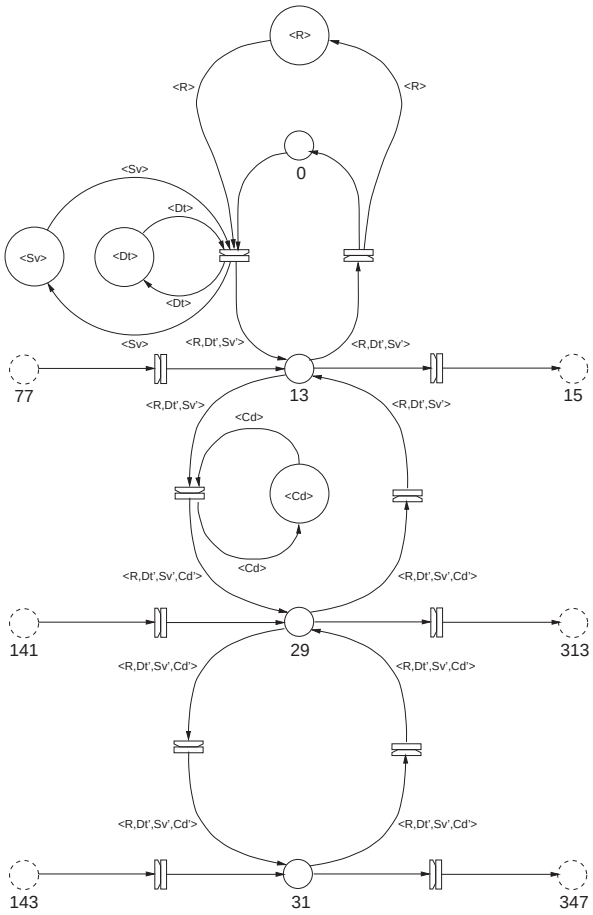

FIG. 1.1: *Extrait du modèle de référence pour la surveillance-commande*

4. les activités de référence sont modélisées par des jetons. Ces jetons sont des n-uplets d'instances d'objets qui caractérisent dynamiquement l'activité en cours d'exécution ;

5. toutes les places du réseau (0, 13, 29, etc.) sont des places indiquant la classe d'activité de référence en cours d'exécution ;

6. les transitions de ce réseau de référence représentent les événements de début et de fin d'activité : toute transition "début d'activité" ou "fin d'activité" est encadrée en amont et en aval par des places d'activités.

Ce réseau de référence a été prévu pour fonctionner en relation exclusive avec le modèle de la loi de surveillance-commande-supervision. Il évolue sur demande de cette stratégie selon les informations reçues par le superviseur ("données traitées", "comptes rendus", "requêtes diverses", etc.), puis traitées par les fonctions de surveillance, commande et supervision. Comme nous le verrons plus loin, l'utilité du modèle de référence en ligne peut être remise en cause.

Ce modèle est un modèle générique. Seuls les jetons modélisant les ressources physiques et les produits dépendent de l'atelier considéré. Ainsi, quelle que soit l'entreprise considérée, le modèle de référence peut être intégré à chacun des nœuds de la structure décisionnelle retenue. En revanche, le nombre de ces nœuds dépend bien entendu de la complexité de l'atelier considéré.

1.3 Technique de conception du modèle

La technique générale proposée dans (Zamaï [1997]) s'apparente assez à celle de la synthèse de lois de commande au sens exprimé dans (Ramadge et Wonham [1987]). Cette synthèse peut s'illustrer sur la base de la figure 1.2 proposée initialement dans les travaux présentés dans (Combacau [1991]).

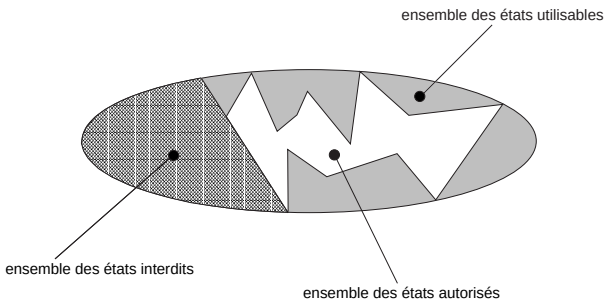

FIG. 1.2: *Les trois classes d'états d'un système*

Cette figure illustre le concept d'états d'un système. Un système peut être représenté au travers de ses états observables. Parmi ces états, certains peuvent être considérés comme interdits (par exemple, la coexistence de la fonction diagnostic et la fonction décision ; le diagnostic doit être achevé pour qu'une décision puisse être prise). D'autres sont considérés comme utilisables (par exemple, diagnostiquer en même temps que la commande, ce qui caractérise une marche forcée). Enfin les états dits autorisés satisfont pleinement au cahier des charges donné par l'industriel (dans un contexte de manipulation de produits explosifs, seuls les états de commande et d'urgence devront être conservés).

Pour obtenir l'ensemble des états observables, l'auteur propose d'utiliser une table de vérité à 9 entrées, chacune de ces entrées étant une des fonctions de surveillance, de commande et de supervision associées à une ressource et éventuellement à un produit. La table complète est constituée de 512 lignes (2^9 états). Les 0 et les 1 contenus dans les cases de cette table déterminent si l'élément correspondant appartient (1) ou n'appartient pas (0) à l'état. Au final, l'auteur propose 512 activités observables.

Dans le cadre de l'obtention du modèle de référence pour une ressource physique quelconque, l'auteur définit un processus de raffinement basé sur 5 contraintes. Ces contraintes expriment les associations qui doivent être interdites et les associations obligatoires entre les fonctions de surveillance, de commande et de supervision. Pour des raisons de concision, nous ne justifierons aucune de ces contraintes. Pour plus de détails, le lecteur pourra se reporter à (Zamaï [1997]).

- Le suivi doit être toujours associé à chacune des activités.
- La détection et l'urgence ne peuvent pas être associées en même temps.
- Le diagnostic et la décision ne peuvent cohabiter.
- La reprise et la commande s'excluent mutuellement.
- L'urgence doit s'accompagner de l'association du diagnostic ou de la décision.

L'intégration de ces contraintes au modèle complet (512 états) revient à rejeter 481 activités, ce qui réduit le modèle de référence à 31 activités. Elles sont représentées par des 9-uplets du type :

$< R, P, Dt, Sv, Cd, Dg, Dc, Rp, Ug >$

$R, P, Dt, Sv, Cd, Dg, Dc, Rp, Ug \in \{0, 1\}$

Où:

R=Ressource, P=Produit, Dt=Détection, Sv=Suivi, Cd=Commande,
Dg =Diagnostic, Dc =Décision, Rp =Reprise, Ug =Urgence

Par exemple, l'activité de référence **<1,0,1,1,1,0,1,0,0>** représente un état où seuls les éléments *détection, suivi, commande* et *décision* sont associés à la *ressource*.

Afin de rendre plus accessible la lecture du document, nous avons volontairement simplifié l'écriture du 9-uplet, en le réduisant au n-uplet des éléments associés à un instant t. Ainsi, la représentation de l'activité prise comme exemple devient désormais $< R, Dt, Sv, Cd, Dc >$. Cette activité de référence représente une prise de décision dans un contexte de phase de préparation ou de maintenance qui n'a pas été interrompue malgré l'occurrence d'une défaillance. La décision devra concerner la commande en cours toujours active et une éventuelle reprise (continuer à produire, arrêter puis reprendre, etc.). La fonction détection est toujours active. En effet, au cours de cette activité, la détection est faite par rapport aux consignes de commande envoyées vers le procédé.

Afin d'obtenir les transitions utilisables entre les 31 activités de référence, l'auteur propose une base de 18 autres contraintes permettant par exemple de rejeter l'enchaînement aberrant suivant : $< R, Dt, Sv > \mapsto < R, Dt, Sv, Dc >$. Ce passage traduit une prise de décision sans qu'un diagnostic n'ait été fait!.

Ainsi, même si dans l'absolu 930 enchaînements élémentaires (nombre d'arrangements de 2 activités parmi 31: $A_2^{31} = 31 \times 30$) sont observables, l'intégration de ces contraintes réduit l'espace des transitions à 165. Pour les mêmes raisons évoquées précédemment, nous ne listerons pas ici l'ensemble de ces 18 contraintes.

Le modèle de référence ayant désormais été présenté en détails, nous nous proposons maintenant de mettre en exergue un certain nombre de faiblesses pour lesquelles des solutions doivent être envisagées.

1.4 Les points faibles du modèle de référence

A ce jour, trois points faibles ont pu être mis en évidence au sein du modèle de référence. Ces faiblesses se répartissent autour de trois piliers du modèle, à savoir : les contraintes portant sur les activités, la liste des éléments pris en compte dans les n-uplets pour construire les activités observables, et enfin la technique de conception du modèle.

Parmi les cinq contraintes proposées par l'auteur, une en particulier doit être remise en cause. Elle interdit en effet la cohabitation simultanée des fonctions détection et urgence. A première vue, cette dernière semble justifiée ne serait-ce que pour éviter le déclenchement d'alarmes en cascade. En effet, lorsqu'une procédure d'urgence est lancée, le procédé est piloté d'une manière généralement brutale souvent incompatible avec les règles et principes du fonctionnement normal. Aussi est-il normal que les informations issues des capteurs soient interprétées comme anormales par la fonction détection. Afin d'éviter de détecter ces dysfonctionnements pourtant normaux dans une telle situation, l'auteur propose tout simplement d'inhiber la fonction détection durant un traitement d'urgence. Cependant, nous pouvons montrer aisément que même pendant l'exécution d'une procédure d'urgence, la fonction détection doit être toujours active, ne serait-ce que pour détecter des situations encore plus catastrophiques. Prenons l'exemple d'un robot de type SCARA. En présence

de défaillances lors d'un déplacement indiquant une collision d'un des bras du robot, une procédure d'arrêt d'urgence doit être lancée afin d'une part de stopper les mouvements et d'autre part de mettre à zéro le point de consigne du contrôleur local de l'axe Z (remontée en $Z = 0,0$). En admettant que le codeur absolu associé à la position de l'axe Z renvoie des mesures erronées, une remontée trop importante de l'axe n'est pas exclue. Aussi, la prise en compte du capteur de sur-course affecté à l'axe Z doit être assurée dans ce cas. Inhiber la fonction détection n'est donc pas la solution. Afin de faire face à la fois au problème de déclenchement d'alarmes en cascade mais également d'assurer la surveillance des capteurs de sur-course par exemple, nous proposons que la fonction détection reste active quelle que soit l'activité et que les modèles sur lesquels elle travaille soient différents selon l'activité de référence en cours. Il s'agit alors d'un changement de référenciel pour les mécanismes utilisés par la fonction détection. Ceci sortant largement de notre cadre de travail, nous ne détaillerons pas davantage la détection.

Le deuxième point de faiblesse que nous avons pu mettre en évidence concerne l'indéterminisme des définitions données aux activités de référence. Par exemple, l'activité $< R, Dt, Sv, Cd >$ représente la commande d'une ressource physique sans qu'un produit ne soit transformé. Cela peut donc caractériser au moins deux situations différentes :

1. soit la commande d'une ressource nécessitant une préparation préalable à la production : mise en position d'un robot, ouverture d'un étau, mise en rotation d'un mandrin, etc.

2. soit à une activité de maintenance (test, vérification, etc.) hors production (produit=0) de la ressource concernée.

Cet indéterminisme peut donc rapidement devenir rédhibitoire en phase d'exploitation, ne serait-ce que pour envisager de prendre une décision. Si une telle ambiguïté existe, c'est que le problème est certainement sous-dimensionné. L'ajout d'un élément supplémentaire au sein des n-uplets qui caractérisent une activité devrait résoudre le problème. Dans le cadre de nos travaux, nous avons proposé de prendre en compte les modes de marches et d'arrêts proposés dans le GEMMA. Comme nous le verrons dans le chapitre suivant, l'intégration de ce nouvel élément résout non seulement le problème d'indéterminisme, mais apporte également des perspectives fort intéressantes pour l'élaboration des lois de surveillance-commande-supervision. En effet, si le modèle a pour vocation de proposer tous les traitements de défaillances qu'il est possible d'appliquer en entreprise, il va de soi que nous devrions y retrouver les modes de marches, points de départ de nombreux traitements de défaillances : une défaillance peut se produire dans chacun des modes de marches (production normale, dégradée, urgence, etc.). Selon le mode dans lequel la défaillance a été détectée, un traitement de défaillance devrait lui être associé (Méndez et al. [2002b]).

Le dernier point sur lequel nous souhaitons intervenir est la technique d'élaboration du modèle de référence. Même si la proposition conjointe d'une table de vérité contrainte permettant d'obtenir l'ensemble des activités de référence utilisables et d'un programme d'élimination des arcs interdits a montré son efficacité, il n'en demeure pas moins que nous pourrions être tentés de remplacer cette technique par celle proposée par Ramadge et Wonham dans le cadre de la synthèse de lois de commande (Ramadge et Wohanm [1989]). Le problème est en fait exactement le même : d'une part, nous disposons d'un modèle complet des états et transitions observables, d'autre part nous disposons d'une liste de spécifications (exclusions mutuelles, séquencements obligatoires, etc.) facilement modélisables par des automates. Le recours à une telle technique nous permettrait de valider et vérifier automatiquement le modèle obtenu. Bien que cette proposition présente un aspect tout à fait intéressant et innovant, nous ne l'avons pas mise en œuvre dans le cadre de cette thèse afin de concentrer notre recherche sur la synthèse de lois de surveillance.

1.5 Conclusion

Dans ce chapitre, nous avons présenté plus en détails le modèle de référence pour la surveillance, la commande et la supervision proposé dans (Zamaï [1997]). Ce modèle représente l'ensemble des traitements de défaillances qui peuvent être utilisés dans le cadre de la conduite réactive de procédés industriels complexes. Après un bref résumé de la technique employée par l'auteur pour construire ce modèle, nous avons mené une analyse critique qui nous a conduit à mettre en exergue trois limitations majeures. En premier lieu, nous avons montré que le modèle présente des activités indéterministes du point de vue des définitions, en deuxième lieu, nous avons démontré que les n-uplets modélisant les activités de référence étaient sous-dimensionnées, et enfin nous avons montré que la technique employée pour construire le modèle pouvait être remplacée par une autre, "plus formelle". Ce dernier point ne sera pas développé dans le cadre de ces travaux, mais devra certainement faire l'objet d'un travail futur. Pour chacun de ces points, nous avons proposé des solutions dont les deux premières sont mises en œuvre dans le chapitre suivant.

Chapitre 2

Extension du modèle de référence

2.1 Introduction

Ce chapitre est entièrement dédié à l'extension du modèle de référence proposé par le LAAS. Ainsi, comme nous avons pu le voir dans le chapitre précédent, nous allons nous attacher ici à revisiter les contraintes de réduction du modèle des états observables et à intégrer dans les n-uplets modélisant les activités de référence, les modes de marches et d'arrêts du GEMMA. Tout naturellement, ce chapitre a été structuré autour de deux paragraphes. Le premier s'attachera à déterminer le nouvel espace d'activités de références (utilisables). Pour cela, nous serons amenés à modifier l'une des cinq contraintes proposées, puis nous étudierons la répartition des activités de référence au sein des différents modes de marches et d'arrêts proposés dans le GEMMA. Le second paragraphe sera quant à lui dédié à la spécification des nouvelles transitions de référence qui doivent être proposées pour lier convenablement les nouvelles activités de référence obtenues.

2.2 Spécification des nouvelles activités de référence

2.2.1 Modification des contraintes

Comme nous avons pu le prouver dans le chapitre 1 de cette partie, parmi les cinq contraintes portant sur la viabilité des activités de référence, il en existe une qui est trop restrictive. Il s'agit de l'exclusion mutuelle entre les fonctions urgence et détection. Nous proposons donc ici de relâcher cette contrainte :

"La fonction détection doit toujours être associée à une activité de référence".

Après avoir repris la table de vérité proposée dans la thèse (Zamaï [1997]) et suite à l'application de cette contrainte, nous avons rejeté et ajouté au modèle original douze activités. La taille du modèle reste donc constante. La liste réactualisée des 31 activités utilisables est donnée dans le tableau suivant (Figure 2.1) :

Au travers de tous ces états, nous pouvons désormais constater que la détection est toujours associée, même en présence de la fonction urgence. **En conséquence, nous nous devons maintenant d'insister sur le fait que toute fonction de détection amenée à être utilisée dans cette approche devra nécessairement s'appuyer sur des modèles de détection en adéquation avec l'activité de référence en**

ACT	R	P	Dt	Sv	Cd	Dg	Dc	Rp	Ug	Uplet
0	0	0	0	0	0	0	0	0	0	<>
13	1	0	1	1	0	0	0	0	0	<R, Dt, Sv>
15	1	1	1	1	0	0	0	0	0	<R, P, Dt, Sv>
29	1	0	1	1	1	0	0	0	0	<R, Dt, Sv, Cd>
31	1	1	1	1	1	0	0	0	0	<R, P, Dt, Sv, Cd>
45	1	0	1	1	0	1	0	0	0	<R, Dt, Sv, Dg>
47	1	1	1	1	0	1	0	0	0	<R, P, Dt, Sv, Dg>
61	1	0	1	1	1	1	0	0	0	<R, Dt, Sv, Cd, Dg>
63	1	1	1	1	1	1	0	0	0	<R, P, Dt, Sv, Cd, Dg>
77	1	0	1	1	0	0	1	0	0	<R, Dt, Sv, Dc>
79	1	1	1	1	0	0	1	0	0	<R, P, Dt, Sv, Dc>
93	1	0	1	1	1	0	1	0	0	<R, Dt, Sv, Cd, Dc>
95	1	1	1	1	1	0	1	0	0	<R, P, Dt, Sv, Cd, Dc>
141	1	0	1	1	0	0	0	1	0	<R, Dt, Sv, Rp>
143	1	1	1	1	0	0	0	1	0	<R, P, Dt, Sv, Rp>
173	1	0	1	1	0	1	0	1	0	<R, Dt, Sv, Dg, Rp>
175	1	1	1	1	0	1	0	1	0	<R, P, Dt, Sv, Dg, Rp>
205	1	0	1	1	0	0	1	1	0	<R, Dt, Sv, Dc, Rp>
207	1	1	1	1	0	0	1	1	0	<R, P, Dt, Sv, Dc, Rp>
301	1	0	1	1	0	1	0	0	1	<R, Dt, Sv, Dg, Ug>
303	1	1	1	1	0	1	0	0	1	<R, P, Dt, Sv, Dg, Ug>
317	1	0	1	1	1	1	0	0	1	<R, Dt, Sv, Cd, Dg, Ug>
319	1	1	1	1	1	1	0	0	1	<R, P, Dt, Sv, Cd, Dg, Ug>
333	1	0	1	1	0	0	1	0	1	<R, Dt, Sv, Dc, Ug>
335	1	1	1	1	0	0	1	0	1	<R, P, Dt, Sv, Dc, Ug>
349	1	0	1	1	1	0	1	0	1	<R, Dt, Sv, Cd, Dc, Ug>
351	1	1	1	1	1	0	1	0	1	<R, P, Dt, Sv, Cd, Dc, Ug>
429	1	0	1	1	0	1	0	1	1	<R, Dt, Sv, Dg, Rp, Ug>
431	1	1	1	1	0	1	0	1	1	<R, P, Dt, Sv, Dg, Rp, Ug>
461	1	0	1	1	0	0	1	1	1	<R, Dt, Sv, Dc, Rp, Ug>
463	1	1	1	1	0	0	1	1	1	<R, P, Dt, Sv, Dc, Rp, Ug>

FIG. 2.1: *Les activités de référence actualisées.*

cours d'exécution (Méndez et al. [2000a]). Comme nous avons pu déjà l'évoquer dans le chapitre 1 de cette partie, en situation d'urgence, la fonction détection devra être "plus tolérante" aux défaillances mineures, mais rester toujours aussi vigilante pour toute défaillance dénotant un caractère dangereux à la fois pour l'opérateur humain et le procédé lui-même.

La modification de la liste de contraintes ayant été réalisée, nous nous proposons maintenant de tenter d'apporter une solution au problème des indéterminismes des définitions de certaines activités de référence.

2.2.2 Prise en compte du GEMMA pour le Modèle de Référence

Le modèle de référence reste dans certains cas assez imprécis quant à la définition de certaines de ces activités ; nous en avons donné un exemple frappant dans le chapitre 1 de cette partie. Un tel problème se doit d'être résolu pour assurer la fiabilité de l'approche proposée dans un cadre réel. En effet, en présence de problèmes nécessitant des prises de décision, l'état réel du système de commande, de surveillance et de supervision doit être parfaitement connu. Si tel n'est pas le cas, deux cas de figures peuvent se présenter : soit un retard dans la prise de décision, soit une mauvaise prise de décision ; dans tous les cas, les conséquences peuvent être catastrophiques.

Comme nous avons pu le démontrer dans le précédent chapitre, nous avons proposé de résoudre cet indéterminisme par la prise en compte d'un nouvel élément au sein des n-uplets qui modélisent les activités de référence. Ce nouvel élément est le GEMMA que nous avons présenté dans l'état de l'art réalisé dans la partie I de ce mémoire.

La prise en compte des modes du GEMMA au sein de l'approche pouvait être abordée de deux manières différentes : soit par l'ajout de 17 colonnes (modes) supplémentaires dans la table de vérité proposée par E. Zamaï et l'établissement de contraintes de réduction, soit par la répartition des 98 activités de référence au sein de chacun des modes du GEMMA accompagné de la définition d'une liste de contraintes rejetant ou non l'activité au sein du mode (Méndez et al. [2000b]). Étant donné la complexité inhérente à la manipulation d'une table de vérité à 26 entrées (9+17), notre choix s'est naturellement porté sur la deuxième solution. De plus, ce choix nous permet d'ores et déjà de fixer l'idée qu'au sein d'un mode plusieurs traitements de défaillances peuvent être proposés en fonction des besoins de l'industriel.

La première phase de l'élaboration du modèle de référence étendu consiste donc à répartir les 31 activités de référence dans chacun des 17 modes du GEMMA. Ceci nous a conduit à déterminer 527 activités différentes. Fort heureusement, toutes ces activités ne sont pas compatibles avec tous les modes. Par exemple, une activité de référence dont l'élément urgence est associé, est incompatible avec un mode de production normale. Afin de systématiser le rejet des relations activités/modes incompatibles, nous avons défini une nouvelle liste de contraintes. Nous avons défini ces contraintes en respectant les deux niveaux d'abstraction proposés dans le GEMMA (Familles de modes et modes).

P.C. Hors Énergie : la ressource physique n'est pas alimentée. Seule l'activité de référence minimale (<>) doit être intégrée dans ce mode. Elle est interdite dans tous les autres modes.

Procédures de Fonctionnement : les modes de cette famille sont caractérisés pour décrire les états requis pour produire. Ces modes sont la préparation, la vérification, et la production. Nous proposons donc en premier lieu les deux contraintes suivantes :

- les activités de référence qui contiennent l'élément reprise seront exclues de cette famille. En effet, les activités qui contiennent cet élément représentent des situations pour lesquelles des procédures de reprise sont lancées afin de ramener la ressource vers un état normal. Il s'agit donc de l'aboutissement d'un traitement de défaillance, ce qui n'est pas compatible avec cette famille de modes ;
- exclusion des activités qui contiennent l'élément urgence. Ces activités représentent des situations où des procédures d'urgence sont déclenchées. Pour des raisons semblables à celles exposées précédemment, ces activités sont incompatibles avec cette famille de modes.

En deuxième lieu, nous proposons d'autres contraintes associées plus précisément à chacun des modes de cette famille :

- Mode F1 (Production Normale) : ce mode caractérise la transformation normale d'un produit. Toutes les activités de référence intégrant la fonction de commande doivent être naturellement réparties au sein de ce mode.
- Modes F2 et F3 (Marches de préparation et marches de clôture) : ces modes caractérisent l'application de séquences de commandes particulières permettant d'amener la ressource soit dans un état à partir duquel elle pourra produire normalement ou bien être arrêtée. Quel que soit l'un de ces modes, toute activité de référence intégrant la fonction commande devra lui être associée.

- Mode F4 (Vérification dans le désordre) : ce mode représente les traditionnelles vérifications des fonctions de base de la ressource. Pour cette raison, ce mode est souvent appelé "mode manuel". Nous proposons de rejeter toutes les activités de référence qui intègrent la fonction commande afin d'éviter tout conflit décisionnel entre les ordres émis via les pupitres de commande (opérateur humain) et ceux pouvant être émis par le système de commande automatisé.
- Modes F5 et F6 (Marches de vérification dans l'ordre et marches de test) : il s'agit ici d'appliquer des séquences de commande pré-définies par le constructeur de la ressource physique afin de vérifier et tester son fonctionnement nominal. Pour cette raison, toute activité de référence s'appuyant sur la fonction commande doit être prise en compte dans ces modes.

Procédures d'arrêt P.O. : cette famille caractérise des modes où la ressource est à l'arrêt (initial, avant de commencer un cycle de production ou intermédiaire (mode A1), en pause au cours d'un cycle de production (mode A4) ou bien en arrêt pour cause de défaillance (mode A5)). Dans cette famille sont également inclus les modes qui conduisent à ces états d'arrêt de la ressource. Compte tenu de ces remarques générales, nous proposons que toutes les activités de référence qui associent l'élément urgence soient rejetées.

Ensuite, nous avons fourni d'autres contraintes spécifiques à chacun des modes de cette famille :

- Mode A1 (Arrêt dans l'état initial) : la ressource est à l'arrêt, prête à commencer un cycle de production.
  1. puisque la ressource est à l'arrêt, aucune fonction de la classe commande au sens GRP-ASSF (commande, reprise et urgence (Combacau et al. [2000])) ne doit être associée à une activité de référence. Les activités de référence présentant ce profil doivent donc être rejetées ;
  2. dans un arrêt à l'état initial, toute ressource doit être libérée de toute présence éventuelle d'un produit. En conséquence, nous rejetons toutes les activités de référence qui intègrent le produit dans le n-uplet.
- Modes A2 et A3 (Arrêt demandé en fin de cycle et Arrêt demandé dans état déterminé) : dans ces cas, il est évident que toutes les activités qui associent la fonction commande doivent être retenues. En revanche, les activités intégrant la fonction reprise devront être rejetées pour la simple et bonne raison que A2 et A3 appartiennent aux fonctionnements normaux!
- Mode A4 (Arrêt obtenu) : la ressource a été arrêtée dans un état différent de l'initial. Elle est prête pour continuer le cycle de production. Pour ce mode, nous retiendrons que toute activité associant les fonctions de la classe commande (commande, reprise et urgence) devront être rejetées.
- Modes A5, A6 et A7 (Préparation pour mise en route après défaillance, Mise P.O. dans l'état initial et Mise P.O. dans état déterminé) : ces modes représentent l'exécution de séquences de reprise. Le mode A5 applique les séquences de reprise pour résorber la défaillance tandis que les modes A6 et A7 appliquent les séquences complémentaires en préliminaire au retour en fonctionnement normal. Il va de soi que toutes les activités de références réparties dans ces trois modes devront intégrer la fonction reprise dans le n-uplet qui les caractérise.

Procédures de Défaillance : cette famille, composée de trois modes, regroupe les activités chargées d'appliquer les procédures d'urgence (mode D1), de diagnostiquer

et d'élaborer les séquences de reprise (mode D2) et d'appliquer les marches forcées (mode D3).

- Mode D1 (Arrêt d'urgence) : ce mode représente la mise en sécurité des ressources suite à l'occurrence d'une défaillance pouvant mettre en danger l'intégrité des opérateurs ou de la ressource. Il est donc évident que les activités à associer à ce mode doivent intégrer au moins la fonction urgence.
- Mode D2 (Diagnostic et/ou traitement de défaillances) : dans ce mode la ressource est arrêtée afin d'autoriser un diagnostic. Les conclusions obtenues doivent ensuite permettre d'envisager les actions correctives requises. Fort de ce constat, plusieurs contraintes ont été définies :
  1. la fonction commande ne doit bien entendu pas appartenir au n-uplet qui caractérise l'activité ;
  2. les fonctions diagnostic ou décision doivent être associées au n-uplet au vu des objectifs affichés de ce mode ;
  3. la fonction reprise ne peut pas être associée aux activités de ce mode car elles sont justement en cours d'élaboration ;
  4. la fonction urgence doit être également bannie des activités de ce mode.
- Mode D3 (Production tout de même) : lorsque l'on souhaite garantir un certain niveau de productivité, souvent au détriment de la qualité d'ailleurs, il peut être fort utile de faire appel à des modes de fonctionnements dégradés, forcés ou encore appelés "production tout de même". Au sein de ces modes, certaines défaillances peuvent être tolérées ou tout simplement ignorées. En conséquence, la fonction commande doit bien évidemment être associée à toutes les activités de référence appartenant à ce mode. En revanche, les fonctions urgence et reprise devront être rejetées des activités associées à ce mode.

L'application de toutes ces contraintes nous a amené à étendre encore le nombre des activités de référence, le faisant désormais passer de 31 à 98.

En premier lieu, cette extension nous a permis de résoudre les problèmes d'indéterminisme des définitions associées aux activités de référence. En effet, l'activité $\langle R, Dt, Sv, Cd\rangle$ que nous avions présentée dans la troisième section du chapitre 1 est désormais décomposée en huit activités distinctes : $\langle F1, R, Dt, Sv, Cd\rangle$, $\langle F2, R, Dt, Sv, Cd\rangle$, $\langle F3, R, Dt, Sv, Cd\rangle$, $\langle F5, R, Dt, Sv, Cd\rangle$, $\langle F6, R, Dt, Sv, Cd\rangle$, $\langle A2, R, Dt, Sv, Cd\rangle$, $\langle A3, R, Dt, Sv, Cd\rangle$, $\langle D3, R, Dt, Sv, Cd\rangle$.

En second lieu, l'extension du modèle ouvre maintenant de nouvelles perspectives en termes de traitements de surveillance et de supervision. D'ailleurs, afin de mieux appréhender les perspectives offertes par une telle extension, nous proposons au lecteur de se reporter à l'annexe 1 qui décrit chacune des 98 activités de référence.

L'analyse des définitions données pour chaque mode nous permet d'identifier deux grandes zones. La première correspond aux modes que nous pouvons utiliser pendant un processus de production normal : A1 (arrêt initial), A2 (arrêt demandé en fin de cycle), A3 (Arrêt demandé dans état déterminé), A4 (Arrêt obtenu), F1 (Production normale); F2 (Marches de préparation), F3 (Marches de clôture), F4 (Marches de vérification dans le désordre), F5 (Marche de vérification dans l'ordre) et F6 (Marche de test). La deuxième zone correspond à la partie du GEMMA qui doit être exploitée en phase de traitement de défaillances. Cette zone est représentée par les modes : D1 (Arrêt d'urgence), D2 (Diagnostic et/ou traitement de défaillance), D3 (Production tout de même), A5 (Préparation pour remise en route après défaillance), A6 (Mise P.0. dans état initial) et A7 (Mise P.O. dans état déterminé).

Tel que l'avait annoncé E. Zamaï dans ses travaux, la surveillance et la supervision des procédés industriels n'est pas aussi simple qu'une boucle réactive enchaînant détection, diagnostic, décision et reprise. Nous montrons aujourd'hui encore que ce ne sont pas 31 activités de référence qui doivent être considérées, mais 98. La richesse du modèle obtenu à ce jour laisse présager la naissance de nouvelles stratégies, plus fines encore, plus adaptées au terrain.

Cependant, avant d'aller plus avant dans ce concept de stratégie, il est nécessaire d'achever la conception du modèle de référence étendu, en s'intéressant maintenant aux enchaînements entre ces 98 activités. C'est ce que nous nous proposons de faire dans le paragraphe suivant.

2.2.3 Spécification des nouvelles transitions de référence

Compte tenu de l'existence de 98 activités de référence, l'ensemble des transitions observables entre ces activités est de 8190 (nombre d'arrangements de 2 activités parmi les 98; $A_2^{98} = 98 \times 97 = 8190$). Fort heureusement, tous ces enchaînements ne doivent pas être utilisés.

En effet, dans Zamaï [1997], il a été montré que certaines de ces transitions ne représentent pas une étape d'un traitement de défaillance : par exemple, passer d'une activité de commande à une activité de décision. En effet, une activité de diagnostic, au moins, doit être intercalée entre ces deux phases car identifier la défaillance est nécessaire avant de pouvoir décider d'un traitement correctif. De manière à rejeter toutes les transitions qui ne représentent pas un processus de surveillance, le système de surveillance, commande et supervision a été étudié sous l'aspect d'association et de dissociation des 9 éléments, ressources, produit et fonctions de surveillance, commande et supervision. L'association d'un élément a été défini comme étant son apparition dans le n-uplet modélisant l'activité de référence. La dissociation concerne la disparition d'un élément. 9 éléments peuvent être associés ou dissociés, 18 cas ont été étudiés. Pour chacun de ces cas, la démarche a amené l'auteur à étudier quels autres éléments devaient être associés ou dissociés simultanément. Par exemple, l'association de la fonction reprise s'accompagne toujours de la dissociation de la fonction commande. Si tel n'était pas le cas, deux éléments distincts pourraient être amenés à envoyer des ordres contradictoires vers le sous-système commandé.

Cependant, afin d'être conforme à l'hypothèse que nous avons formulée dans le paragraphe 2 de ce chapitre :

"La fonction détection doit être toujours associée à une activité de référence",

nous proposons donc de réviser dans un premier temps les deux contraintes liées à l'association et à la dissociation de la fonction urgence. Ainsi, la contrainte d'association de la fonction urgence se réduit maintenant à : **l'association de l'urgence sera liée à celle du diagnostic ou à celle de la décision.** Celle liée à la dissociation de la fonction urgence est supprimée. Elle imposait en effet la "ré-association" de la fonction détection qui avait été rejetée lors de l'association de la fonction urgence.

Nous retenons ensuite les 14 autres cas qui sont exposés dans les travaux de Zamaï [1997]. Pour des raisons de concision, ils ne seront pas décrits à nouveau ici.

Cependant, l'intégration des modes de marche ayant largement étendu l'espace des activités de référence, il est désormais nécessaire de spécifier d'autres nouvelles contraintes

liées cette fois à la commutation possible entre modes.

En effet, prenons l'exemple suivant : supposons la représentation de l'évolution d'une ressource qui passe d'une phase de fin de marche de préparation à une production normale. Dans ce cas, seul l'élément mode doit varier sans que les autres éléments n'en soient affectés : $< F2, R, P, Dt, Sv, Cd > \rightarrowtail < F1, R, P, Dt, Sv, Cd >$. Il faut en effet interdire tout autre commutation entre ces deux modes car elles traduiraient forcément le passage en traitement de défaillance, ce qui n'est pas compatible avec ces modes. Ainsi, le passage de $< F2, R, P, Dt, Sv, Cd > \rightarrowtail < F1, R, P, Dt, Sv, Cd, Dg >$ doit donc être interdit.

De manière à éliminer les commutations interdites entre modes et à autoriser celles utilisables, nous proposons un ensemble de contraintes supplémentaires. Ces contraintes vont porter sur des relations étroites existant entre les événements qui sont à l'origine des commutations de mode du système physique considéré. 17 modes de marches et d'arrêts étant proposés dans le GEMMA, $17*17 = 289$ commutations devraient être étudiées. Afin de réduire cette étude, nous nous sommes appuyés sur les extensions du GEMMA proposées par MORENO (Moreno et Peulot [1997]) concernant les commutations utilisables entre modes. Fort de cette base de connaissances et des 17 contraintes qui conditionnent les enchaînements utilisables des fonctions de surveillance, commande et supervision, nous avons pu restreindre notre analyse à 17 commutations correspondant aux 17 modes de marches et d'arrêts atteignables.

Remarque 1 : notons que les événements que nous utilisons (commutation vers un mode) n'ont pas de réalité. Ils ne sont utilisés ici que pour nous aider à décrire de manière exhaustive les processus de commutation de référence.

Remarque 2 : les contraintes proposées ci-après proposent d'associer et/ou de dissocier des fonctions de surveillance, commande et supervision selon la commutation de mode considérée. Nous tenons à préciser qu'il va de soi que si l'activité d'origine (avant la commutation) intègre déjà l'élément à associer, la contrainte n'aura aucun effet.

---

1. **Événements liés à la commutation vers le mode HS (Hors Service) :** une commutation vers ce mode conduit à la dissociation de toutes les fonctions de surveillance du n-uplet modélisant l'activité de référence.

2. **Événements liés à la commutation vers le mode F1 (Fonctionnement normal) :** une commutation vers ce mode doit conduire uniquement à l'association de la fonction commande afin de produire en fonctionnement normal.

3. **Événements liés à la commutation vers le mode F2 (Marche de préparation) :** la commutation vers le mode F2 doit conduire à l'association de la fonction commande. En effet, la marche de préparation consiste à lancer une séquence de commande pour réaliser les opérations préliminaires à toutes phases de production normale.

4. **Événements liés à la commutation vers le mode F3 (Marche de clôture) :** aucune fonction supplémentaire ne doit être associée. La marche de clôture témoigne d'une coloration particulière de la séquence de commande en cours d'exécution.

5. **Événements liés à la commutation vers le mode F4 (Marches de vérification dans le désordre) :** la fonction commande doit être dissociée puisque les séquences opératoires exécutées dans ce mode correspondent à des opérations lancées manuellement depuis le pupitre de contrôle sans respecter un ordre particulier.

6. **Événements liés à la commutation vers le mode F5 (Marche de vérification dans l'ordre) :** la fonction commande doit être associée afin de vérifier le fonctionnement de la ressource.

7. **Événements liés à la commutation vers le mode F6 (Marches de test) :** pour les mêmes raisons évoquées pour le mode F5, si la fonction commande n'est pas déjà associée, elle doit l'être lors de cette commutation.

8. **Événements liés à la commutation vers le mode A1 (Arrêt dans l'état initial) :** une commutation vers ce mode doit bien évidemment s'accompagner de la dissociation de la fonction commande ou de la fonction reprise.

9. **Événements liés à la commutation vers le mode A2 (Arrêt demandé en fin de cycle) :** cette commutation de mode n'entraîne pas d'association et/ou de dissocaition des fonctions de surveillance, commande ou supervision. Il s'agit ici aussi d'une représentation plus fine de la nature de la séquence de commande en cours d'exécution.

10. **Événements liés à la commutation vers le mode A3 (Arrêt demandé dans état déterminé) :** cette commutation de mode n'entraîne pas d'association et/ou de dissociation des fonctions de surveillance, commande ou supervision pour les mêmes raisons que celles évoquées précédemment.

11. **Événements liés à la commutation vers le mode A4 (Arrêt obtenu) :** une commutation vers ce mode doit s'accompagner de la dissociation de la fonction commande ou de la fonction reprise puisque l'arrêt de la ressource est désormais effectif.

12. **Événements liés à la commutation vers le mode A5 (Préparation pour remise en route après défaillance) :** cette commutation doit bien entendu s'accompagner de l'association de la fonction reprise.

13. **Événements liés à la commutation vers le mode A6 (Mise P.O. dans état initial) :** la commutation vers ce mode ne provoque pas d'association de nouvelles fonctions. Il s'agit ici encore d'une représentation plus détaillée de la nature de la séquence de commande en cours d'exécution.

14. **Événements liés à la commutation vers le mode A7 (Mise P.O. dans état déterminé) :** cette commutation de mode n'entraîne pas d'association et/ou de dissociation des fonctions de surveillance, commande ou supervision pour les mêmes raisons que celles évoquées pour A6.

15. **Événements liés à la commutation vers le mode D1 (Arrêt d'urgence) :** le passage vers ce mode entraîne forcément l'association de la fonction urgence.

16. **Événements liés à la commutation vers le mode D2 (Diagnostic et/ou traitement de défaillance) :** le passage vers ce mode entraîne la dissociation de la fonction commande et l'association de la fonction diagnostic. Dans ce mode, la commande de la ressource est arrêtée pendant la recherche des causes de la défaillance détectée.

17. **Événements liées à la commutation vers le mode D3 (Production tout de même) :** la fonction diagnostic doit être associée lors de cette commutation afin de mieux surveiller l'état réel du procédé.

L'application de cet ensemble de contraintes nous permet de définir un ensemble de 1171 évolutions possibles entre les 98 activités de référence. Afin de ne pas alourdir cette section, nous ne les présentons pas ici. Cependant toutes ces évolutions peuvent être consultées dans l'annexe 2.

Ce modèle de référence peut être vu comme une superposition de plans (cf. Figure 2.2), chacun proposant un niveau d'abstraction différent : une vue mode, une vue activités de référence (au sens (Zamaï [1997]) et enfin une vue fonctions de surveillance, commande et supervision.

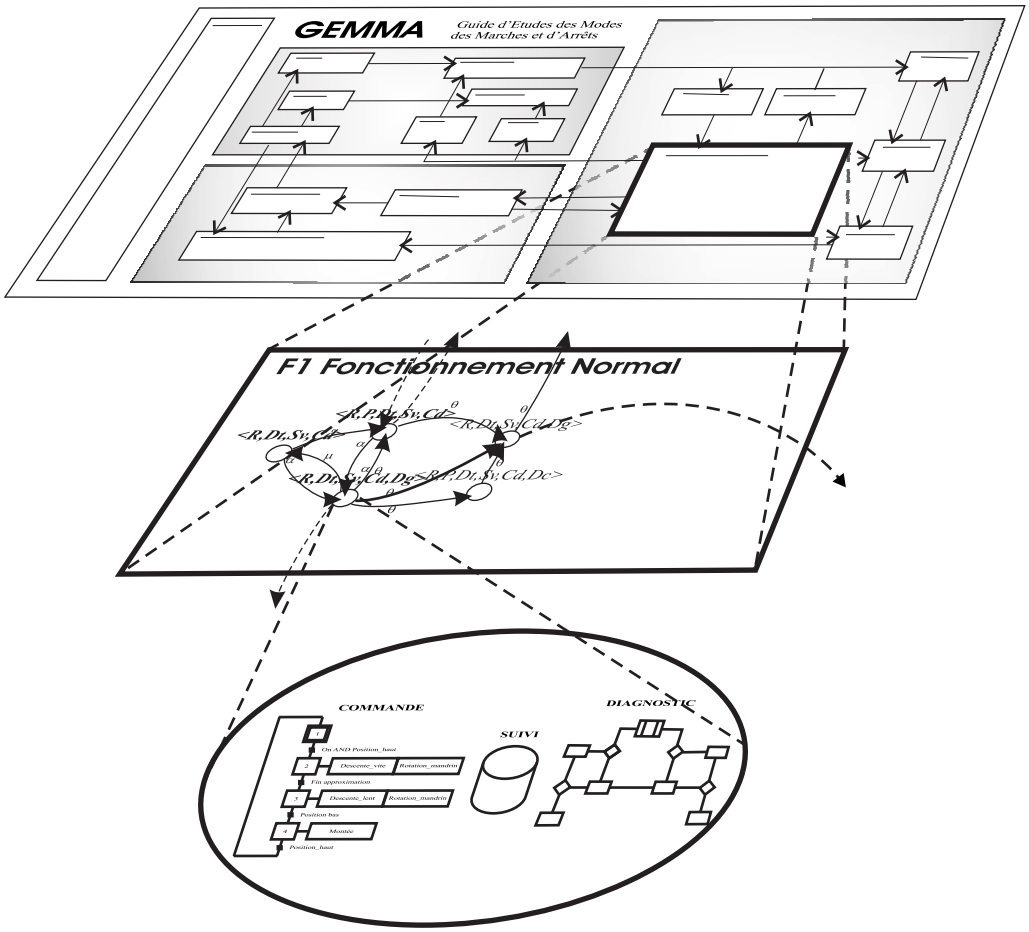

FIG. 2.2: *Niveaux d'abstraction du Modèle de Référence pour la Surveillance, Commande et Supervision.*

2.3 Conclusion

Au travers de ce chapitre, nous avons proposé une extension significative du modèle de référence proposé dans les travaux de Zamaï [1997]. Cette extension s'appuie essentiellement sur l'intégration des modes de marches et d'arrêts au sein du modèle de référence original. Cette intégration nous a amené à spécifier deux catégories de contraintes : l'une dédiée à rejeter les activités qui ne représentent pas de réalité au sens de la surveillance, la commande et la supervision, l'autre destinée à interdire certaines commutations entre activités de référence.

L'application de ces contraintes ainsi que celles proposées dans Zamaï [1997], nous

ont permis de spécifier un nouveau modèle de référence basé sur 98 activités et 1171 transitions élémentaires. Ce modèle de référence est désormais déterministe d'un point de vue des définitions associées à ces activités et se prête davantage à une exploitation réelle en entreprise.

Cependant, avant d'étudier comment ce modèle peut être exploité en entreprise, il est nécessaire de sélectionner "le bon" outil de modélisation. C'est ce que nous nous proposons de faire au chapitre suivant.

Chapitre 3

Formalisation du modèle de référence étendu

3.1 Introduction

Pour une seule ressource considérée, le modèle de référence peut être naturellement représenté sous la forme d'une machine à états. Puisque plusieurs ressources doivent être considérées au sein d'un atelier de production, plusieurs machines à états en parallèle seraient nécessaires ou bien un Réseau de Petri à Objets (RdPO) (Zamaï [1997]). C'est ce dernier outil que E. Zamaï a sélectionné dans le cadre de ses travaux.

Cependant, considérer plusieurs ressources au sein d'un seul et même modèle nuit à sa lisibilité. En effet, étudier le cheminement du jeton (modélisant dans le cadre des RdPO l'activité en cours) n'est pas des plus simples, que ce soit pour le ou les concepteurs de la stratégie de surveillance, commande et supervision, ou pour les opérateurs humains chargés de l'exploitation. Pour ces raisons, nous proposons dans le cadre de nos travaux de nous appuyer maintenant sur les concepts de la théorie des langages et automates (Hopcroft et Ullman [1978]).

Dans ce but, ce chapitre a été structuré autour de deux paragraphes. Dans le premier, nous présentons brièvement le formalisme utilisé dans la théorie des langages et automates. Ensuite, nous utilisons ce formalisme pour décrire le nouveau modèle de référence sous la forme d'un automate.

3.2 La théorie des langages et automates

La théorie des langages et automates est utilisée principalement pour étudier le comportement logique d'un système et vérifier certaines propriétés d'exactitude et de cohérence (Bucci et al. [1995]). Dans cette théorie, le point de départ est la possibilité d'associer un ensemble d'événements à tout système à événements discrets. De cette façon, l'ensemble d'événements est défini comme un "alphabet" d'un langage et les séquences d'événements correspondent alors aux "mots" de ce langage.

Un automate est un modèle mathématique défini par :

$$M = (Q, \Sigma, \delta, q_0, Q_m)$$

où:

- Q = ensemble fini d'états,
- Σ = alphabet,
- δ = fonction de transition,
- q_0 = état initial,
- Q_m = ensemble d'états marqués.

Un automate est représenté par un graphe orienté (graphe état-transition, Figure 3.1). Dans cette représentation, les nœuds correspondent aux états du système et les arcs orientés aux transitions entre ces états. Les étiquettes définissent les événements qui provoquent les changements entre les états. Le nœud marqué avec une flèche représente l'état initial (q_0) et ceux marqués avec un double-cercle correspondent aux états marqués. L'automate représenté dans l'exemple correspond à un système capable de reconnaître un nombre pair de "a" et un nombre pair de "b".

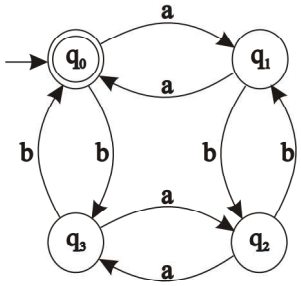

FIG. 3.1: *Exemple d'un système modélisé par un automate.*

Parmi les propriétés qui peuvent être vérifiées par un automate, nous pouvons citer :

Atteignabilité : cette propriété sert à vérifier s'il existe un chemin, à partir de l'état initial, qui nous amène à l'état marqué (état objectif). Par exemple, nous pouvons utiliser ce formalisme pour définir le comportement d'un système de production (normal et anormal) à partir des événements qui peuvent se produire. De cette façon, nous pouvons identifier les séquences d'événements qui nous amènent à des situations de défaillance (ensemble d'états marqués égal aux états du fonctionnement anormal). Ainsi l'identification de ces séquences et des événements qui conduisent à ces états permet d'anticiper des actions préventives pour éviter d'atteindre ces états ou de développer des actions correctives pour les résoudre.

Réinitialisabilité : cette propriété sert à vérifier si une fois que l'état initial a été quitté, il est possible d'y revenir. Ceci permet par exemple de vérifier s'il existe des chemins qui conduisent à nouveau dans l'état initial après l'occurrence d'une situation de défaillance et, si c'est le cas, quels sont les événements qui provoquent ce retour.

Blocage : cette propriété sert à vérifier la cohérence du système. L'apparition d'un blocage correspond à une situation à partir de laquelle le système ne peut plus évoluer. Par exemple, dans la modélisation d'un système de production, cette propriété peut être utilisée pour identifier les situations de défaillance qui empêchent le système d'évoluer.

3.3 Modélisation du modèle de référence selon la théorie des langages et automates

Pour une ressource considérée, le modèle de référence peut donc être représenté par une machine à états finis définie par :

$$G =< X, \Sigma, \delta, x_o, X_m >$$

X correspond à l'ensemble d'états du modèle. Σ correspond à l'ensemble d'événements qui provoquent les évolutions dans le modèle de référence. Il caractérise donc l'alphabet d'événements. δ définit la fonction de transition et x_0 l'état initial. L'ensemble d'états marqué (X_m) contient un seul élément. Cet élément ou état est égal à l'état initial. Il est défini par l'état qui représente la ressource en repos.

L'ensemble d'états est défini par :

$$X = \{x_1, x_2, ..., x_n : n = 98\}$$

Chaque état x_i représente une activité de référence. Il est représenté par le n-uplet suivant :

$$x_i =< m, P, Dt, Sv, Cd, Dg, Dc, Rp, Ug >$$

$P, Dt, Sv, Cd, Dg, Dc, Rp, Ug \in \{actif, inactif\}$,

$m \in M, M = \{HS, F1, F2, F3, F4, F5, F6, A1, A2, A3, A4, A5, A6, A7, D1, D2, D3\} =$ mode de marche ou d'arrêt,

avec :
P=Produit, Dt=Détection, Sv=Suivi, Cd=Commande, Dg=Diagnostic, Dc=Décision, Rp=Reprise, Ug=Urgence

L'ensemble des états X du modèle de référence est organisé selon deux sous-ensembles distincts : celui représentant le sous-ensemble des états appartenant à la famille des fonctionnements normaux (X_n), l'autre caractérisant le sous-ensemble des états utilisables pour traiter une défaillance de la partie opérative (X_t).

$$X = \{x_{HS}\} \cup X_n \cup X_t$$

Les états correspondant à chaque sous-ensemble sont identifiés par l'élément mode du n-uplet.

$M = \{x_{HS}\} \cup M_n \cup M_t$

$\{x_{HS}\} = \langle HS, R\rangle =$ état Hors-Service. Aucune opération de surveillance est possible. Pour cette raison nous le considérons à part.

$M_n = \{F1, F2, F3, F4, F5, F6, A1, A2, A3, A4\}$ (Modes du fonctionnement normal)
$M_t = \{D1, D2, D3, A5, A6, A7\}$ (Modes à utiliser pendant les traitements de défaillance)

Ainsi, les sous-ensembles des états de fonctionnement normal et des traitements de défaillance sont définis par :
$X_n = \{x_0 \cup x \in X : x(m) \in M_n\}$
$X_t = \{x \in X : x(m) \in M_t\}$ (États des traitements de défaillance)

L'alphabet d'événement Σ définit l'ensemble des signaux qui provoquent une évolution dans le modèle. Ces événements correspondent aux différentes informations reçues et émises par les fonctions de surveillance, commande et supervision. A partir d'une étude de ces informations déjà faite dans les travaux de Zamaï et al. [1998b], nous avons proposé l'alphabet suivant :

$\Sigma = \{\alpha, \beta, \gamma, \eta, \mu, \theta, \omega, \tau, \phi\}$ = alphabet d'événements

où :

α = Requête de commande, β = Requête de diagnostic, γ = Requête de reprise, η = Requête d'urgence, μ = Résultat de commande, θ = Résultat de détection, ω = Résultat de diagnostic, τ = Résultat de reprise, ϕ = Résultat d'urgence.

La fonction de transition δ nous permet alors de caractériser les évolutions qui existent au sein du modèle de référence. Elles définissent les conditions nécessaires pour évoluer d'un état à un autre suite à l'occurrence d'un de ces événements. La fonction de transition est caractérisée par l'expression :

$$\delta = X \times \Sigma \rightarrow X$$

que nous avons considérée sous l'aspect de trois autres fonctions de transition : δ_n, δ_s et δ_t

δ_n caractérise les évolutions qui existent au sein de la zone de fonctionnement normal. Elle représente donc les passages qui vont d'un état de fonctionnement normal à un autre état de fonctionnement normal suite à l'occurrence d'un événement :

$$\delta_n : X_n \times \Sigma \rightarrow X_n$$

δ_s contient les évolutions qui permettent de passer de la zone de fonctionnement normal vers la zone de traitements de défaillances. Ces passages correspondent aux déclenchements des traitements de défaillance :

$$\delta_s : X_n \times \Sigma \rightarrow X_t$$

Finalement, δ_t représente les évolutions qui existent à l'intérieur de la zone de traitement de défaillances ainsi que les évolutions qui conduisent à nouveau vers les états du fonctionnement normal :

$$\delta_t : X_t \times \Sigma \rightarrow X$$

Enfin, dans notre modèle, nous considérerons comme état initial la ressource à l'arrêt défini par $x_0 = \langle A1, R, Dt, Sv \rangle$.

En résumé, le nouveau modèle de référence que nous proposons représente 98 activités de référence et 1171 façons de les enchaîner en respectant les contraintes d'utilisation des fonctions de commande, surveillance et supervision. La représentation d'un tel modèle étant relativement conséquente, nous n'en avons représenté ici qu'un extrait (Figure 3.2).

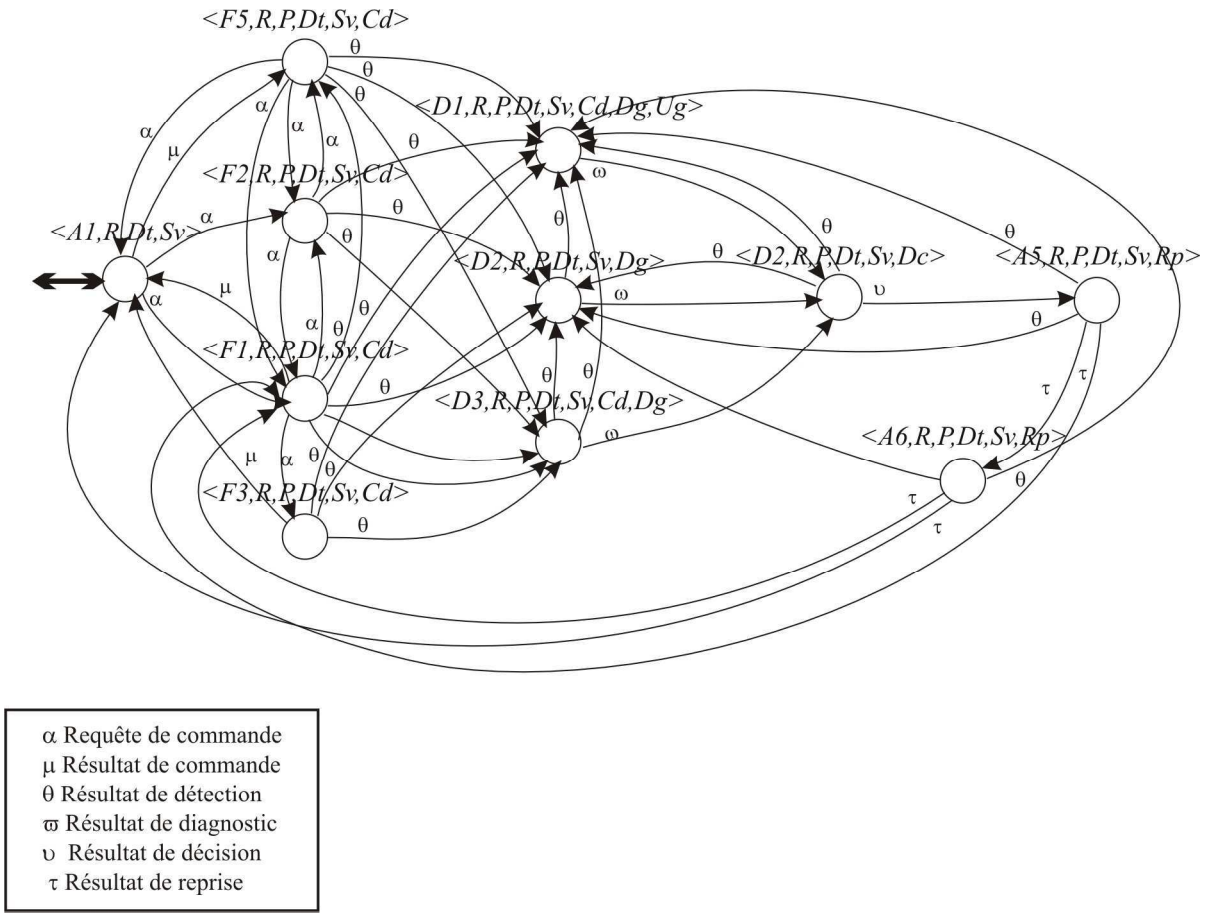

FIG. 3.2: *Extrait du Modèle de Référence pour la Surveillance-Commande et Supervision.*

3.4 Conclusion

Dans ce chapitre, nous nous sommes employés à formaliser le nouveau modèle de référence. Nous avons tout d'abord exposé brièvement les raisons du changement de formalisme (passage d'une représentation RdPO à une représentation automate). Ensuite, après avoir exposées les bases de la théorie des langages et automates, nous les avons appliquées à notre cas d'étude. Au final, nous détenons, pour une ressource considérée au sein d'un nœud de la structure hiérarchique et modulaire, une machine à états finis dont la structure de contrôle est parfaitement générique. Cet automate compte actuellement 98 états et 1171 façons de les enchaîner. Le modèle de référence pour la surveillance, la commande et la supervision a donc été fortement étendu par rapport à celui proposé dans le cadre des travaux (Zamaï [1997]). Ces états sont désormais déterministes d'un point de vue définition, et les traitements de surveillance correspondants sont à ce jour plus fins.

Cependant, disposer d'un tel "dictionnaire" de la surveillance, commande et supervision des ressources physiques d'une entreprise, ne sert à rien sans une méthode permettant d'en "déduire" efficacement une loi de surveillance, commande et supervision. C'est ce que nous nous proposons d'apporter dans la partie suivante de notre mémoire de thèse.

Troisième partie

Synthèse de lois de surveillance

Chapitre 1

Problématique de la synthèse de lois de surveillance

1.1 Introduction

La partie précédente nous a amené à spécifier le modèle de référence étendu pour la surveillance, la commande et la supervision. Comme nous avons pu le constater, ce modèle représente toutes les façons de surveiller, de commander et de superviser les ressources d'un procédé industriel. Dans cette partie, nous nous proposons de mettre au point une technique de synthèse de lois de surveillance basée sur l'exploitation de ce modèle ; l'idée directrice est ainsi de donner un cadre formel à la génération de lois de surveillance en parfaite adéquation avec les besoins des industriels.

Dans cet objectif, nous avons consacré la première section de ce chapitre à la présentation du principe de base de la synthèse proposé à l'origine dans le domaine du continu. Ceci nous permettra de mettre en exergue les éléments essentiels nécessaires à la génération d'une loi : l'expression d'un cahier des charges (propriétés recherchées de la loi), un modèle du comportement du système que nous souhaitons contraindre à ces propriétés, et enfin une méthode de synthèse.

La deuxième section aura pour but de présenter différents moyens d'expression d'un cahier des charges en fonction du domaine continu ou discret.

Fort de ces moyens d'expression, le troisième paragraphe du chapitre aura pour vocation de définir les propriétés que nous devons rechercher pour concevoir une loi de surveillance. Comme nous le verrons, les moyens d'expression de ces propriétés sont assez hétérogènes ce qui laissera présager de l'utilisation conjointe de plusieurs techniques de synthèse.

Enfin, le quatrième paragraphe s'attachera à éclaircir deux concepts fondamentaux à l'origine du choix des techniques de synthèse. Ce paragraphe constituera la charnière de notre troisième partie.

1.2 L'origine de la synthèse

Afin de mieux comprendre la démarche que nous proposons, nous souhaitons faire ici une légère "pause" sous la forme d'une présentation simplifiée de la synthèse en automa-

tique continue.

Dans ce domaine, un système est décrit comme étant un dispositif isolé, soumis aux lois de la physique, de la chimie, de la biologie, de l'économie, etc., caractérisé par certaines grandeurs et placé dans un environnement (Gentil et Zamaï [2002]).

Les grandeurs caractéristiques de ce système sont des variables et des paramètres. Les entrées caractérisent l'effet de l'environnement sur le système. Les sorties caractérisent l'effet du système sur l'environnement. Ainsi, les entrées sont souvent des produits bruts ou de l'énergie et sont classées selon deux catégories : actions et perturbations. Les actions sont maîtrisables par l'utilisateur ; elles serviront de commande, ou grandeur réglante ; les perturbations sont non maîtrisables par l'utilisateur mais parfois mesurables. Les sorties sont en général des produits finis, transformés, dont on spécifie la qualité et/ou la quantité (grandeur réglée) (Figure 1.1). La relation entre les entrées et les sorties fait souvent intervenir le temps (système dynamique)(Faurre et Robin [1984]).

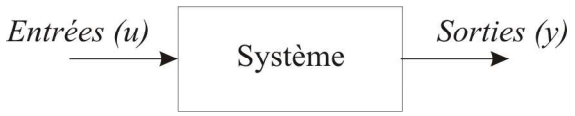

FIG. 1.1: *Diagramme fonctionnel d'un système dynamique*

Pour commander un système, il est nécessaire de connaître précisément son fonctionnement, traduit par un modèle mathématique qui indique comment varient les sorties sous l'effet des entrées. Le modèle du système exprime la relation de cause à effet entre les commandes, les perturbations et les variables à réguler. Un système dynamique est décrit grâce aux lois fondamentales des diverses disciplines (par exemple les lois fondamentales de la mécanique ou de l'électricité), qui prennent la forme d'équations différentielles, de fonctions de transfert, etc.

Le moyen généralement utilisé pour commander un procédé est la boucle de commande (boucle d'asservissement, boucle de régulation) : l'action à appliquer est calculée automatiquement par le système de commande (correcteur, régulateur), en fonction d'informations sur la valeur désirée pour la mesure (consigne, référence) et sa valeur réelle (sortie, mesure) (Figure 1.2).

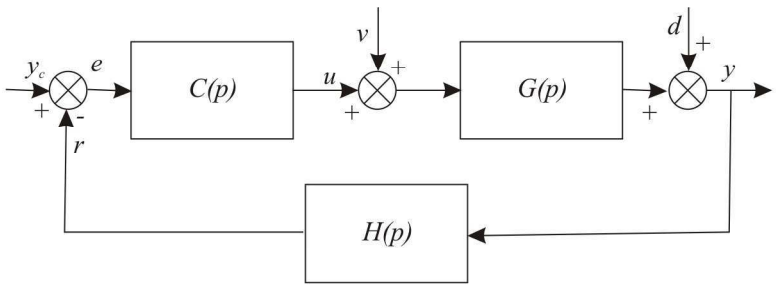

FIG. 1.2: *Exemple d'une boucle de commande*

L'automatique est donc la science qui fournit les outils théoriques pour concevoir et mettre en œuvre les commandes automatiques de systèmes.

Dans le domaine de l'automatique continue, établir une loi de commande fait donc partie des techniques désormais bien connues et maîtrisées. Aussi, de nombreux outils/techniques sont proposés tels que le réglage fréquentiel, le placement de pôles, etc., pour spécifier des lois de commande respectant des critères tels que la stabilité, la précision, le temps de réponse, etc.

En tout cas, et ce quelle que soit la technique retenue, les méthodes conventionnelles de synthèse de lois de commande partent toutes des mêmes hypothèses :

- identifier le modèle du fonctionnement normal du procédé,
- spécifier le cahier des charges du système de commande sous la forme de critères (temps de réponse, stabilité, etc.),
- sélectionner le "bon" outil de synthèse.

Dans le cadre de nos travaux de recherche, la démarche originale que nous avons retenue pour concevoir des lois de surveillance s'appuie sur une démarche proche de la synthèse de correcteurs (automatique continue) pour lesquels par exemple les critères marge de phase, marge de gain doivent être réglés afin d'obtenir à partir du modèle de comportement du système à commander, la loi de commande.

Ainsi, partant du modèle de référence que nous avons obtenu par identification des besoins de la surveillance, commande et supervision, nous nous proposons en premier lieu de mettre au point une méthode de réglage de critères (i.e. réglage de la marge de phase à 45ø pour assurer la stabilité du système) adaptés à nos besoins. En second lieu, et fort de ces réglages, nous nous proposons ensuite de concevoir une démarche d'intégration de ces critères afin de générer une loi de surveillance respectant au mieux l'ensemble des critères proposés.

Même si nous pouvons considérer que la démarche retenue est claire et simple, il n'en demeure pas moins que déterminer quels critères doivent être considérés d'une part et quelle technique de synthèse doit être retenue ou conçue d'autre part, reste cependant difficile comme vont en témoigner les paragraphes suivants.

1.3 Les moyens d'expression d'un cahier des charges

Rechercher et mettre par écrit les propriétés que doit satisfaire un système commandé revient à rédiger un cahier de charges (Delfieu et Sahraoui [1994]). Celui-ci est donc utilisé pour exprimer les besoins des utilisateurs du système. La rédaction de ce document est la première étape du cycle de vie d'un système (Figure 2.4, page 35).

L'expression de ce cahier des charges dépend entièrement du niveau de commande considéré de ce système (continu/discret).

Ainsi, dans le domaine de l'automatique continue, le système de commande (régulateur) devra façonner la réponse du procédé à une consigne donnée de manière à obtenir ou à préserver un système stable en boucle fermée, en réduisant les effets des perturbations et des bruits de mesure (Tona [2000]). Pour concevoir un tel régulateur, une liste de critères d'analyse est généralement fournie par les automaticiens du continu. Ces critères permettent de régler le comportement dynamique et stationnaire, la stabilité nominale et la robustesse du futur système de commande. En fait, ces critères d'analyse sont répartis en deux grandes classes : les quantificateurs de performance temporelle et les quantificateurs de performance fréquentielle. Dans le cadre de la première catégorie, et si nous

prenons l'exemple classique d'un asservissement de position et d'une consigne de type échelon, quatre critères devront être étudiés : temps de montée, temps de réponse, dépassement maximal et rapport de décroissance. Une fois ces critères établis, l'automatique continue met à disposition tout un ensemble de techniques et outils de synthèses de lois de commande comme par exemple le placement de pôles, le réglage fréquentiel d'un système dynamique linéaire, le réglage temporel, les correcteurs numériques RST, etc. Les outils couramment utilisés sont par exemple les diagrammes de Bode, de Nyquist ou encore de Black (Foulard et al. [1997]).

Dans le domaine de l'automatique des systèmes à événements discrets, la rédaction du cahier des charges est d'une autre nature. Prenons l'exemple simple de la commande d'un dispositif de manutention à aiguillage (Figure 1.3) (Combacau [1991]). D'un point de vue physique, à partir du point A, un chariot peut se diriger à droite ou à gauche. Spécifier ici un cahier des charges de commande consiste à fixer un chemin : par exemple, aller de A vers B. Cette propriété est généralement appelée une contrainte que l'on souhaite imposer au procédé. Ici, la contrainte traduit un simple séquencement obligatoire. Pour

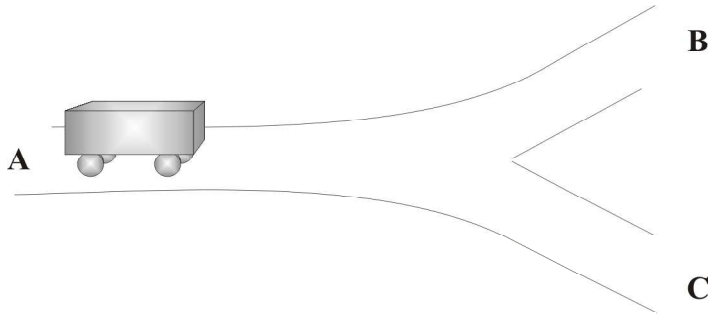

FIG. 1.3: *Système d'aiguillage*

d'autres types de procédés, il en sera généralement de même ; on cherchera par exemple à interdire le convoyage simultané de deux types de produits différents (contrainte d'exclusion mutuelle), à imposer des démarrages en parallèle de certaines opérations de commande comme par exemple les opérations de lubrification pendant l'usinage (contrainte de parallélisme d'exécution, etc.). Bien entendu, comme pour l'automatique continue, de nombreuses techniques et outils sont proposés par les automaticiens du discret afin de nous aider à intégrer ces contraintes et ainsi en synthétiser une loi de commande adaptée : GEMMA (ADEPA [1981]), travaux de l'EXERA (EXERA et Gimélec [1999]), approche du LURPA (Lampérière-Couffin [1998]; Couffin et al. [2000]), approche Ramadge et Wonham (Ramadge et Wonham [1987]), approche LAI (Niel et al. [1996]), approche LISA (Ferrier [1999]), etc. La plupart de ces travaux ayant été détaillés dans la première partie de ce mémoire, nous ne les reprendrons pas ici.

Cette section nous a donc permis de mettre en évidence les différents moyens d'expression d'un cahier des charges dans deux domaines connexes, l'automatique continue et l'automatique discrète. Nous avons pu ainsi constater que les propriétés recherchées dans le domaine de la commande des systèmes à événements discrets sont assez différentes de celles retenues en automatique continue ; dans le premier cas, les propriétés prennent la forme de contraintes qui sont imposées, dans l'autre la forme de critères intégrés dans le processus de production. Comme nous le verrons dans la dernière section de ce chapitre, ces deux moyens d'expression vont jouer un rôle essentiel dans le cadre de nos travaux de recherche. Compte tenu de ces moyens d'expression, nous nous proposons maintenant de les utiliser afin de spécifier les propriétés qui doivent être recherchées lorsqu'il s'agit de synthétiser une loi de surveillance.

1.4 Les propriétés recherchées pour la synthèse de lois de surveillance

Comme nous l'avons vu, pour une phase d'exploitation, spécifier une loi de commande d'un système quelconque revient tout d'abord à fixer les propriétés qu'il doit respecter. Dans ce paragraphe, nous présentons un ensemble non exhaustif de propriétés que doit au moins respecter un système de surveillance, commande et supervision. Ces propriétés sont organisées selon cinq niveaux : la spécification des modes de marches et d'arrêts inhérents à la ressource considérée, la définition des normes législatives auxquelles toute entreprise doit adhérer en fonction des machines, outils et produits qu'elle manipule, la spécification des intérêts des industriels, le réglage des priorités entre ces normes et intérêts industriels, et enfin le degré de récursivité acceptable des traitements de surveillance, commande et supervision.

1.4.1 Les modes de marches et d'arrêts

Lors de l'acquisition et de l'installation d'une ressource physique telle qu'un centre d'usinage à grande vitesse, un convoyeur, etc., au sein d'un atelier, des documents techniques spécifiant entre autre les modes de marches et d'arrêts requis en fonctionnement normal sont fournis. Par exemple, certains fours nécessitent une phase de montée en température avant de pouvoir passer en mode de production normale. C'est le cas également pour les vérins double effets dont les chambres doivent tout d'abord être équilibrées en pression afin d'éviter les classiques claquages au démarrage.

Nous proposons donc en premier lieu que l'utilisateur du système de surveillance, commande et supervision spécifie l'ensemble des modes des marches et d'arrêts inhérents à la ressource physique considérée, et ce, uniquement pour les modes appartement à la famille du fonctionnement normal. Retenons également que cette étape est systématique et simple puisqu'il s'agit uniquement de reporter les préconisations rédigées dans les cahiers techniques fournis.

Les autres modes témoignant d'un traitement de défaillance, nous allons voir dans ce qui suit qu'ils ne peuvent pas être directement spécifiés sous la forme de rejet ou non d'un mode de marche. D'autres propriétés doivent être spécifiées et retenues.

1.4.2 Les normes législatives

Toute entreprise est soumise au respect d'un ensemble de normes et de lois dictées par des organismes gouvernementaux afin d'assurer l'intégrité des opérateurs humains et le respect de l'environnement. Ces normes sont incontournables et doivent être respectées tout au long des processus de production que ce soit en fonctionnement normal ou anormal. C'est dans ce sens que des organismes tels que l'Association Française pour la Normalisation, la Communauté Économique Européenne, le Code du Travail en France, etc. ont établi des directives, des textes législatifs (lois), des textes réglementaires (décrets) et des normes pour protéger les opérateurs humains qui participent dans les processus de transformation et la population civile en général. Toute transgression de ces lois, décrets et/ou normes implique directement la responsabilité civile et pénale de l'entreprise (Sourisse et Boudillon [1996]).

Il en va de même pour le respect de l'environnement. Ainsi, des organismes tels que le Ministère de l'Environnement Français, l'Organisation Mondiale pour la Santé et aussi

la Communauté Économique Européenne ont voté des lois visant à préserver ce secteur (IFEN [1998]).

Les termes *sécurité* et *écologie* sont précisés ci-après :

sécurité : " aptitude d'une machine à accomplir sa fonction, à être transportée, installée, mise au point, entretenue, démontée et mise au rebut dans les conditions d'utilisation normales sans causer de lésion ou d'atteinte à la santé ". Cette définition est issue de la norme européenne EN 292 (Sourisse et Boudillon [1996]).

écologie : les principaux risques technologiques du point de vue strictement environnemental sont, selon la nature des produits et de l'activité, les pollutions de l'air, de l'eau ou encore des sols. En France, la loi pour la protection de l'environnement (issue de la loi du 19 juillet 1976 relative aux installations classées pour la protection de l'environnement) impose des politiques de prévention en termes d'environnement et des plans d'intervention permettant de maîtriser les conséquences en cas d'accident (MEFI [1999]).

Les normes de sécurité et d'écologie sont incontournables, et elles doivent être respectées quel que soit le mode de fonctionnement de la ressource considérée. Ces exigences dépendent bien entendu de la nature des ressources utilisées et des produits transformés. Par exemple, les exigences en termes de sécurité et d'environnement ne seront pas les mêmes pour la surveillance, commande et supervision d'un réacteur d'une centrale nucléaire et d'un convoyeur à bande transportant des canettes.

Contrairement aux propriétés liées au choix des modes de marches et d'arrêts, spécifier l'adhésion à une norme ne se réduit pas à une formulation du type : "OUI" ou "NON". Comme nous le verrons dans le chapitre 2 de cette partie, cette spécification s'apparente plus à un réglage de critère (phase/gain) en automatique continue.

1.4.3 Les besoins internes de l'entreprise

En terme de surveillance, les intérêts des industriels sont souvent ignorés. La plupart des approches du domaine proposent uniquement des solutions restrictives dédiées à la prise en compte de la sécurité, voire parfois de l'écologie et en ignorant les intérêts propres aux entreprises tels que la productivité, la qualité, les délais de production, etc. (Zamaï et al. [1998b]).

Cependant ces besoins ne peuvent continuer à être ignorés, d'autant plus qu'aujourd'hui les marges de manœuvre pour améliorer la productivité d'une entreprise sont faibles : les ateliers sont déjà optimisés du point de vue de leur implantation géographique sur site, jusqu'à la commande optimale des ressources physiques en passant par la logistique ou encore l'ordonnancement. Au moins deux paramètres peuvent encore être optimisés : d'une part la communication (standardisation des réseaux d'entreprise et des informations échangées) de l'entreprise afin d'améliorer la réactivité face à des situations imprévues, d'autre part les techniques permettant de garantir un retour en fonctionnement normal optimal suite à une défaillance de la partie opérative.

Dans le cadre de l'approche que nous proposons, nous avons essentiellement travaillé sur deux de ces besoins internes industriels, à savoir la productivité et la qualité. Bien entendu, d'autres pourront être pris en compte. Insistons sur le fait que notre but n'est pas de fournir une liste exhaustive de toutes les propriétés internes que doit rechercher une entreprise, mais uniquement d'en proposer quelques unes d'essentielles et de montrer

comment elles peuvent être prises en compte pour synthétiser une loi de surveillance (Méndez et al. [2001]).

Productivité : se mesure par le rapport entre le volume de production réalisé et la quantité (ou la valeur) des facteurs humains et matériels mis en œuvre. Au niveau de l'entreprise, elle correspond au moyen le plus sûr pour augmenter le profit (Pourcel [1986]).

Qualité : quelle serait votre réaction si, pour un produit, vous n'étiez pas livré à temps ? ou si l'installation de votre produit à domicile était négligée ? ou encore si le mode de financement accordé à l'achat était défaillant ? C'est à travers ces notions que l'on peut définir l'Assurance de la Qualité. Il s'agit donc de définir un "ensemble approprié de dispositions préétablies et systématiques nécessaires pour donner la confiance appropriée en ce qu'un produit ou service satisfera aux exigences données relatives à la qualité (norme NFX 50 120)". Ces dispositions ce déclinent généralement selon trois principes : "ce qu'ils voulaient, quand ils le voulaient, au prix convenu" (AFNOR [1995b]).

Comme nous le verrons dans le chapitre suivant, ces deux propriétés ne peuvent pas non plus être considérées comme des paramètres "tout ou rien". Il peut par exemple être particulièrement judicieux d'imposer un niveau de qualité important au détriment parfois de la productivité lorsque des défaillances se produisent.

1.4.4 Les priorités normes/besoins internes

Donner le moyen de fixer des niveaux de qualité et de productivité, ou de prendre en compte les normes imposées par la législation c'est aussi prendre le risque "de tout vouloir". Par exemple, pourquoi ne pas fixer : "je veux une productivité maximale, avec une qualité de fabrication de très haut niveau, tout en respectant bien entendu les normes portant sur la sécurité et la préservation de l'environnement". Nous conviendrons bien entendu que des priorités entre ces critères doivent être établies afin d'éviter tout échec de synthèse de lois de surveillance. Comme nous le verrons par la suite, nous serons amenés à imposer, dans la démarche de rédaction du cahier des charges, des priorités entre les normes et les besoins internes de l'entreprise, et laisserons une marge de flexibilité à la discrétion de l'industriel quant aux priorités à fixer au sein de chacune de ces deux classes de propriétés.

1.4.5 La récursivité des traitements de défaillance

Lorsqu'une défaillance significative est détectée, un traitement de surveillance-supervision est généralement déclenché. Cependant, ce traitement ne peut pas toujours garantir un retour en fonctionnement normal. C'est le cas par exemple lors de l'exécution d'une séquence de reprise où d'autres défaillances peuvent survenir : *l'occurrence d'un accident est souvent associé à une défaillance, mais la réparation d'une simple défaillance peut parfois aussi être à l'origine d'un accident* (Sourisse et Boudillon [1996]).

Ainsi, le cycle *production normale* → *détection de défaillance* → *élaboration d'un diagnostic* → *prise de décision* → *application de la séquence de reprise* → *détection de défaillance ...* (Figure 1.4) risque de ne plus avoir de fin. Il faut alors envisager des conditions d'exploitation supplémentaires qui permettent de faire face à ces situations.

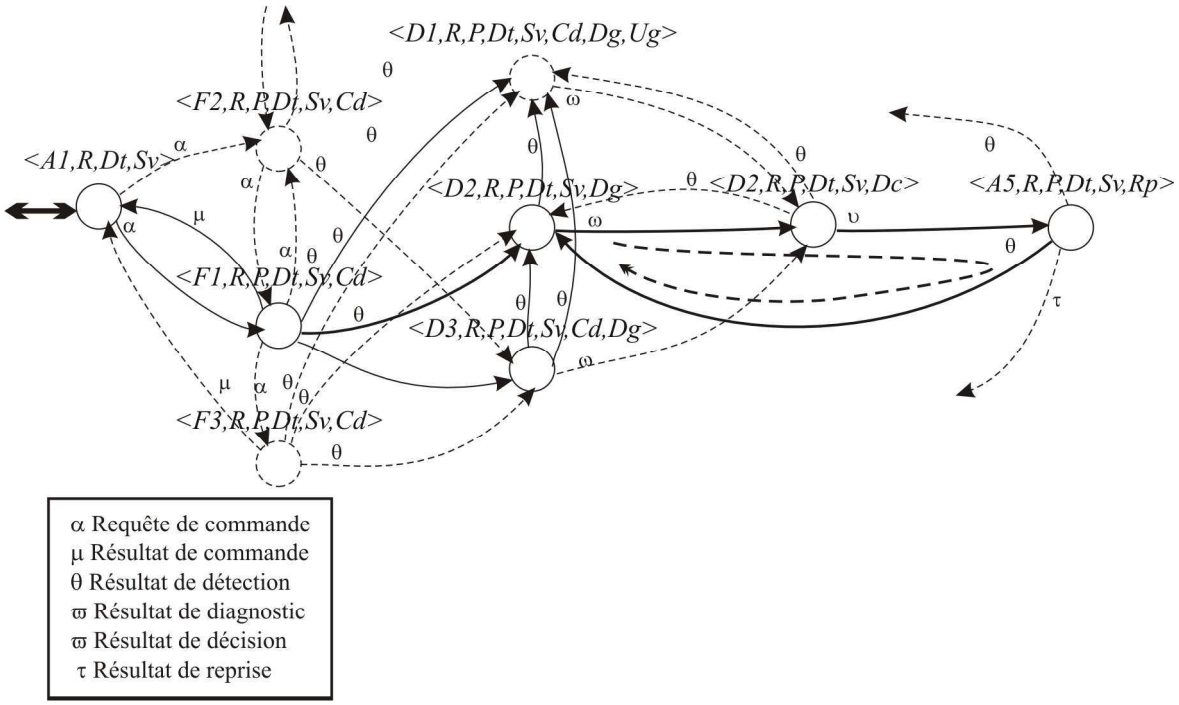

FIG. 1.4: *Illustration du problème de récursivité des traitements de surveillance*

Nous proposons donc d'intégrer le réglage de cette propriété dans le cahier des charges pour la synthèse de lois de surveillance. Il s'agira notamment de spécifier les niveaux de récursivité acceptables des traitements de surveillance. Bien entendu, toute transgression devra se conclure par un arrêt d'urgence de la ressource incriminée avec appel à un service de maintenance (Française [1973]).

Jusqu'à présent, nous avons dressé une liste de cinq classes de propriétés qui doivent être prises en compte dans la phase de spécification des propriétés pour la synthèse de lois de surveillance. La question qui se pose désormais, c'est comment intégrer ces propriétés au sein du modèle de référence afin d'en déduire la loi de surveillance correspondante ? Devons-nous recourir à une technique de synthèse issue du domaine de l'automatique continue ? Pouvons-nous plus simplement nous appuyer sur les techniques de synthèse issues de la théorie de la supervision sur la base de la théorie des automates ? Ou bien devons-nous mettre au point une nouvelle technique de synthèse adaptée à nos besoins ?

Afin de répondre à toutes ces questions, ce qui fera d'ailleurs l'objet du chapitre 3 de cette partie, nous nous proposons préalablement de revenir sur les deux concepts fondamentaux à la base des techniques de synthèse couramment utilisées de nos jours. Il s'agit des concepts de *critère* et de *contrainte*.

1.5 Démarche pour la synthèse de lois de surveillance

Tout au long de ce chapitre nous avons discuté des différents moyens d'expression d'un cahier des charges pour la synthèse de lois de commande aussi bien dans le domaine du continu que du discret. Cette étude a mis en valeur deux concepts majeurs (*critère* et *contrainte*) à partir desquels découlent les techniques de synthèses appropriées. Afin de mieux discerner ces deux termes et mieux évaluer leur impact sur notre problématique, nous nous proposons de donner leurs définitions respectives :

Contrainte : terme général désignant tout élément susceptible de conditionner la réali-

sation des tâches, et leur position dans le temps : contraintes logiques, contraintes de charges, contraintes de dates, contraintes de ressources (Larousse [2002]).

Critère : norme ou règle par laquelle il est possible d'établir un ordre ou un classement des alternatives, soit pour mesurer les degrés relatifs d'efficacité en vue de la satisfaction d'objectifs, soit pour évaluer les résultats des programmes (Larousse [2002]).

Comme nous l'avons vu plus haut, ce concept de *critère* est généralement utilisé en automatique continue pour spécifier des propriétés telles que le respect d'un temps de réponse, la stabilité, la précision, la maîtrise du régime transitoire, etc. Imaginons par exemple un ascenseur (après tout, tout système est par nature continu!) (Gentil et Zamaï [2002]). Lorsque l'on appuie sur le bouton de l'étage n, il faut un certain temps pour y arriver. Ce temps ne doit pas être trop long (satisfaction du client), mais pas trop court non plus (confort du client). On ne veut pas d'oscillations à l'arrivée. On ne veut pas arrêter l'ascenseur à plus de 1 cm de la hauteur de l'étage souhaité. Bien sûr, d'autres considérations rentrent en ligne de compte comme sa robustesse (l'ascenseur doit fonctionner à vide comme à pleine charge, donc avec un paramètre de masse variable). D'un point de vue synthèse du contrôleur qui doit commander cet ascenseur, on cherchera par exemple à améliorer la stabilité du processus en agissant sur la phase afin de la rendre positive autour de la fréquence de coupure du processus en boucle ouverte (Figure 1.5). Pendant longtemps, ce type de correcteur a suffi au réglage de la majorité des installations, une modification simple de la synthèse permettant de traiter les systèmes à retard. Toutefois, les procédés devenant plus complexes, des algorithmes de commande avancée ont vu le jour. Quoi qu'il en soit, l'intégration de tels critères s'appuie sur des modèles mathématiques décrivant le fonctionnement normal de référence du système à commander.

Le concept de *contrainte* prend quant à lui plutôt sa place dans le domaine de l'automatique discontinue (Figure 1.5). Comme nous avons pu le décrire précédemment dans ce chapitre, il est utilisé pour spécifier des propriétés comme des exclusions mutuelles, des séquencements obligatoires, des parallélisme d'exécution, etc. En effet, la définition d'une contrainte revient à définir les propriétés autorisées et/ou interdites par rapport au niveau décisionnel considéré (i.e. commande locale, coordination, ordonnancement temps réel, etc.) et au fonctionnement physique du système que nous souhaitons commander : *il y a deux pompes, appelées "pompe1" et "pompe2". Les deux pompes ne fonctionnent jamais en même temps, on utilise l'une ou l'autre* (Roussel [1994]). Ceci est caractéristique d'une exclusion mutuelle de l'activité de ces deux pompes, alors que physiquement, ces deux activités peuvent être lancées simultanément. D'autres propriétés que l'exclusion mutuelle peuvent être spécifiées comme par exemple des séquencements obligatoires. Si nous reprenons le cas du four cité plus haut, les documentations techniques d'utilisation de ce four impose de lancer une marche de préparation avant d'envisager son utilisation pour une production normale. Ainsi, lorsque l'on possède une représentation discrète du fonctionnement normal du système que l'on souhaite commander, intégrer ces contraintes revient alors tout simplement à **autoriser** ou **inhiber** les évolutions correspondantes. Il en résulte ainsi la génération d'une loi de commande respectant l'ensemble des contraintes spécifiées. Ici aussi, au même titre que dans le domaine de l'automatique continue, les contraintes spécifiées peuvent être prises en compte car le modèle représentant le fonctionnement normal de référence du système à commander s'y prête parfaitement.

Compte tenu de cette prise de recul sur les moyens d'expression d'un cahier des charges et des besoins caractérisés dans le paragraphe 3 de ce chapitre, force est de constater que le cahier des charges de notre approche de synthèse de lois de surveillance s'appuie sur les deux concepts de **critère** et de **contrainte**. En effet, comme nous l'avons mentionné, nous avons besoin d'exprimer les **contraintes** portant sur les modes de marches et d'arrêts autorisés et/ou interdits, de spécifier des **critères** de productivité envisagée par l'entreprise

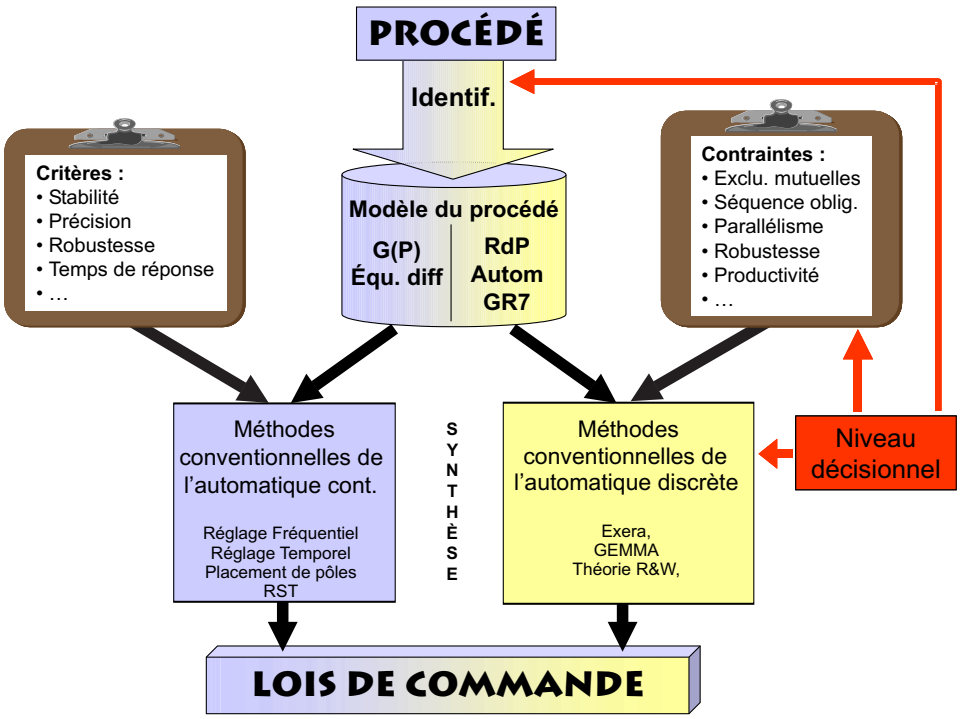

FIG. 1.5: *Principes de la synthèse en discret et continu*

au même titre que ceux pour la qualité, la sécurité ou encore l'environnement, etc. Cependant, bien que deux types de spécifications ont été reconnus nécessaires, il n'en demeure pas moins que le modèle caractérisant le fonctionnement normal de référence de la surveillance, commande et supervision se prête davantage à la prise en compte de contraintes que de critères.

Toute la difficulté de la synthèse de lois de surveillance se situe dans ce paradoxe. D'un côté, nous disposons d'un modèle de référence propre au domaine de l'automatique discrète, et, d'un autre côté, nous disposons à la fois de critères et de contraintes de spécification. Compte tenu de cette problématique, au moins deux solutions peuvent être envisagées : soit développer une technique permettant d'intégrer directement les critères au sein d'un modèle appartenant au mode du discret, soit encore proposer une technique permettant de traduire les critères sous la forme de contraintes, puis d'appliquer une technique conventionnelle de synthèse de l'automatique discrète (Figure 1.6).

1.6 Conclusion

Au travers de ce chapitre, nous avons progressivement campé la problématique de la synthèse de lois de surveillance. En premier lieu, nous avons tout naturellement présenté les origines de la synthèse. Comme nous avons pu le dire, et ce quel que soit le domaine considéré, la synthèse s'appuie sur trois piliers : un modèle de référence représentant le fonctionnement du système, un cahier des charges des propriétés que l'on souhaite donner au système et enfin une technique d'intégration de ces propriétés pour en déduire une loi. Le premier de ces piliers ayant été présenté dans la partie II de notre mémoire, nous nous sommes principalement intéressés ici à décrire les différentes propriétés qu'il faut rechercher pour synthétiser une loi de surveillance. Précisons cependant que l'ensemble des propriétés que nous avons cité n'est pas exhaustif, d'autres propriétés peuvent bien entendu être ajoutées et prises en compte au gré des besoins de l'industriel. Cependant,

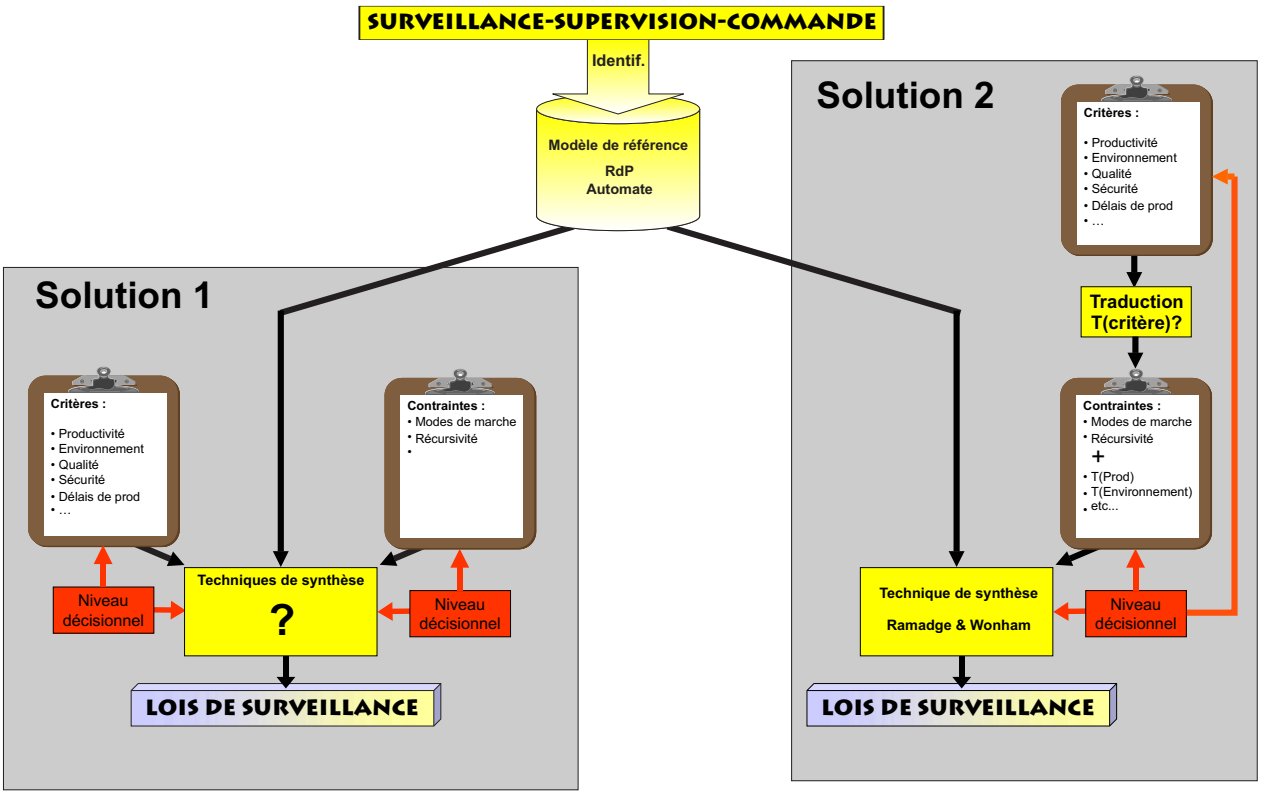

FIG. 1.6: *Problématique de la synthèse de lois de surveillance*

tendre vers l'exhaustivité des propriétés n'était pas notre but. Il s'agissait plutôt de mettre en exergue les différentes classes de ces propriétés. Ainsi, nous avons montré que deux classes de propriétés devaient être prises en compte : les critères et les contraintes. Fort de ce constat, nous avons terminé ce chapitre par la présentation de la problématique de la synthèse de lois de surveillance. Cette problématique naît justement de la nécessité d'intégrer deux classes de propriétés dont l'une n'est pas forcément compatible avec la classe de modèle que nous manipulons.

Les deux chapitres suivants vont désormais s'attacher à présenter la méthode de synthèse de lois de surveillance que nous proposons.

Chapitre 2

Fondements de la synthèse de lois de surveillance

2.1 Introduction

Dans le chapitre précédent, nous avons présenté la problématique générale de la synthèse de lois de surveillance. Ainsi, nous avons tout d'abord spécifié l'ensemble minimal des propriétés qu'il fallait rechercher pour synthétiser convenablement une loi de surveillance adaptée à la fois au produit transformé, aux machines/outils de transformation (ressources), à la politique de production de l'entreprise (productivité, qualité, etc.) et aux normes législatives en vigueur (sécurité, écologie). Nous avons également mis en évidence la nécessité d'intégrer ces différentes propriétés aux modèles de référence proposé dans la partie II. Cette intégration peut être envisagée selon deux techniques distinctes. La première consiste à concevoir des méthodes de synthèse appropriées aux différentes classes de propriétés recherchées (critères, contraintes), la seconde propose de traduire tout d'abord les critères sous la forme de contraintes afin de proposer une seule technique de synthèse. Dans le cadre des travaux que nous avons mené, nous avons choisi de développer la solution 1 pour des raisons de compatibilité assez évidentes entre la structure même du modèle de référence et les propriétés recherchées. Nous tenons cependant à attirer l'attention du lecteur sur le fait que nous ne rejetons pas actuellement la solution 2. Comme nous le préciserons plus loin dans les perspectives de ces travaux, l'étude de la "traduction" critères $\rightarrowtail$ contraintes devra tôt ou tard être menée.

Compte tenu de la solution de synthèse générale de lois de surveillance que nous préconisons dans nos travaux, nous nous proposons dans ce chapitre de dresser les fondements d'une telle approche. Ainsi, en premier lieu, nous mènerons une analyse des propriétés du modèle de référence. De cette analyse, nous mettrons en évidence le rôle partiel de la synthèse de lois de surveillance. Fort de ce constat, nous pourrons alors mettre en relation directe les propriétés recherchées avec la structure même du modèle de référence. Après quoi, nous terminerons ce chapitre par une mise en place des pré-requis à la synthèse de lois de surveillance que nous proposons dans le chapitre suivant.

2.2 Analyse des propriétés du modèle de référence

Dans ce paragraphe, nous allons nous intéresser à l'analyse des propriétés du modèle de référence pour la surveillance, la commande et la supervision. Ceci est nécessaire pour

au moins deux raisons. Premièrement, il n'est pas envisageable de baser notre méthode de synthèse de lois de surveillance sur un modèle de référence identifié qui ne vérifie pas les "bonnes" propriétés (au moins sans blocage et ré-initialisable). Deuxièmement, si ce modèle de référence se veut représenter toutes les façons de surveiller, commander et superviser une ressource physique, alors ce modèle doit forcément être indéterministe structurellement parlant. Pour cette raison, une analyse structurelle doit être également menée afin de montrer l'indéterminisme inhérent au modèle. Comme nous le verrons par la suite, synthétiser une loi de surveillance, c'est en partie rendre le modèle de référence déterministe.

2.2.1 Blocage

L'existence d'un état absorbant indique que si cet état est atteint, il devient alors impossible d'évoluer au sein du modèle. L'existence de tels blocages dans le modèle de référence ne peut être bien entendu toléré. Imaginons, ne serait-ce qu'un instant, le modèle bloqué dans un état de production normale suite à l'occurrence d'un résultat de détection caractérisant la transgression d'une contrainte physique!

L'absence d'états absorbants dans un automate est défini par (Bellot et Sakarovitch [1998]) :

Soit $M = \langle X, \Sigma, \delta, x_0, x_m \rangle$

où

X = ensemble d'états,
Σ = alphabet d'événements (transitions),
δ = conditions de transition,
x_0 = état initial,
x_m = état marqué.

L'automate M contient des états absorbants si :

$$\exists x \in X \mid (x, \sigma, x) \forall \sigma \in \Sigma$$

Cette expression indique que s'il existe des états où l'occurrence d'un événement quelconque ne provoque aucun changement d'état, alors ces états sont des états absorbants.

Dans notre cas, la table de transitions donnée dans l'annexe 1 nous montre que tous les états du modèle de référence conduisent au moins à un autre état à partir de l'occurrence d'un événement. Il n'y a donc pas d'états puits. Le modèle de référence est donc exempt de blocages.

2.2.2 Ré-initialisabilité

Nous allons rechercher ici s'il existe au moins un chemin qui partant de l'état initial $< A1, R, Dt, Sv >$, nous ramène dans cet état. Pour ce faire, nous allons nous appuyer sur la théorie du langage automate.

Définition : soit u une séquence d'événements (mot) générée par un automate :

$$u = \sigma_1\sigma_2...\sigma_n(\sigma_i \in \Sigma, n \geq 1)$$

u est une séquence reconnue (ou acceptée) par l'automate si $(x_0, u, x_m) \in \delta^*$.

Le *langage reconnu*, noté $Rec(M^*)$ est l'ensemble de toutes les séquences reconnues par l'automate, c'est-à-dire :

$$Rec(M^*) = \{u \in \Sigma^* \mid (x_0, u, x_m) \in \delta^*\}$$

Le langage généré par l'automate représente le modèle de référence et donc le comportement que peut avoir le système de surveillance, commande et supervision (Sampath et al. [1998]).

Comme nous l'avons spécifié dans la partie II de notre mémoire, l'automate correspondant au modèle de référence est défini par son état initial égal à l'état final. Cet état correspond à l'activité $< A1, R, Dt, Sv >$ (machine dans l'arrêt initial).

L'application de l'algorithme de Mac Naughton et Yamada (Séébold [1999]) nous permet d'obtenir le langage généré par le modèle de référence.

On note $W_{s,P,t}$ l'ensemble de tous les mots $u \in M^*$ tels que u est étiqueté d'un chemin menant de s à t et n'utilisant pas d'autres états que ceux de P comme états intermédiaires : $Rec(M^*) = \bigcup_{s=t=x_o} W_{s,P,t}$.

$W_{1,4,1} = \alpha, \mu$

$W_{1,\{10,4\},1} = \alpha, \alpha, \mu$

$W_{1,\{10,4,16\},1} = \alpha, \alpha, \alpha, \mu$

$W_{1,\{4,91,94,73\},1} = \alpha, \theta, \omega\nu, \tau$

$W_{1,\{4,81,85,87,73\},1} = \alpha, \theta, \omega\nu, \tau$

$W...$

Les trois premières situations caractérisent des évolutions qui se déroulent pendant une production normale. La première représente le passage de l'arrêt initial vers la production normale et ensuite le retour vers l'arrêt initial.

Le deuxième cas représente une séquence de production normale avec le déclenchement préliminaire d'une marche de préparation.

Le troisième cas traduit une production normale qui s'appuie sur une marche de préparation et une marche de clôture.

Les deux autres exemples représentent le déclenchement d'un traitement de défaillance suite à l'occurrence d'une défaillance au cours d'une production normale.

Ces séquences nous permettent de vérifier que partant de l'état initial, il existe au moins un chemin qui ramène le système de surveillance, commande et supervision de retour à cet état initial. Donc, la propriété de ré-initialisabilité est vérifiée.

2.2.3 Indéterminismes du modèle de référence

Nous avons donné plus haut une hypothèse un peu forte qui mérite d'être approfondie ici. En effet, nous avons annoncé le fait que le modèle de référence doit être forcément indéterministe car il représente l'ensemble des façons de surveiller, commander et superviser une ressource physique. Pour s'en convaincre, étudions de plus près le comportement de notre modèle de référence.

2.2.3.1 Mise en évidence

Un automate fini $Aut =< X, \Sigma, \delta, x_0, x_m >$ est déterministe si (Séébold [1999]) :

– pour tout état x et tout événement σ, $card\{x' \in X \mid (x, \sigma, x') \in \delta\} \leq 1$.

En d'autres termes, **un automate fini est déterministe si d'un même état, ne peuvent jamais être issues deux transitions différentes étiquetées par le même événement**.

La première propriété est vérifiée dans la définition du modèle de référence donnée dans la partie II de ce mémoire :

$$x_0 =< A1, R, Dt, Sv >$$

Pour la vérification de la deuxième propriété, nous nous proposons de nous reporter à la table des transitions du modèle de référence. Compte tenu de sa taille, nous n'en présentons ici qu'un extrait (Figure 2.1).

Dans cette table, nous pouvons remarquer que les possibilités d'évolutions ne sont pas uniques à partir de plusieurs états. Par exemple, à partir de l'état 1 ($< A1, R, Dt, Sv >$), l'occurrence de l'événement *requête de commande* (α) nous donne la possibilité de suivre quatre chemins différents. A partir d'un arrêt initial, nous pouvons soit lancer une marche de préparation, soit une marche de vérification, soit une marche de test, soit encore basculer directement en production normale. Le modèle de référence n'est donc pas déterministe. Dans le cadre du fonctionnement normal d'une ressource physique, et compte tenu des différents modes de marche inhérents à cette famille de comportements, ceci se comprend aisément.

Étudions maintenant l'existence de ces indéterminismes structuraux en présence de défaillances de la partie opérative.

2.2.3.2 Indéterminismes et traitements de défaillances

L'objectif d'une loi de surveillance est de spécifier clairement quel est le traitement de défaillance qui doit être lancé suite à l'occurrence d'une défaillance, le tout en respectant

Activité	Etat	α	β	γ	η	μ	θ	ω	υ	τ	ϕ	ψ	ON
<HS>	0												40
<A1,R,Dt,Sv>	1	{4,10,28,34}	2		79		{79,91}						
<A1,R,Dt,Sv,Dg>	2	{6,12,30,36}			79		{79,91}	3					
<A1,R,Dt,Sv,Dc>	3	{8,14,32,38}			83		{83,93}		{1,79,91}				
<F1,R,Dt,Sv,Cd>	4	{16,22,28,34,43,49}	6		81	40	{81,81,97}					5	
<F1,R,P,Dt,Sv,Cd>	5	{17,23,29,35,44,50}	7		82	40	{82,92,98}					4	
<F1,R,Dt,Sv,Cd,Dg>	6	{18,24,30,36,45,50}			81	41	{81,81,97}	8				7	
<F1,R,P,Dt,Sv,Cd,Dg>	7	{19,25,31,37,46,51}			82	41	{82,92,98}	9				6	
<F1,R,Dt,Sv,Cd,Dc>	8	{20,26,32,38,47,52}			85	42	{85,93,99}		{4,81,91}			9	
<F1,R,P,Dt,Sv,Cd,Dc>	9	{21,27,33,39,48,53}			86	42	{86,96,100}		{5,82,92}			8	
<F2,R,Dt,Sv,Cd>	10	{4,28,34}	12		81		{81,81,97}					11	
<F2,R,P,Dt,Sv,Cd>	11	{5,29,35}	13		82		{82,92,98}					10	
<F2,R,Dt,Sv,Cd,Dg>	12	{6,30,36}			81		{81,81,97}	14				13	
<F2,R,P,Dt,Sv,Cd,Dg>	13	{7,31,37}			82		{82,92,98}	15				12	
<F2,R,Dt,Sv,Cd,Dc>	14	{8,32,38}			85		{85,93,99}		{10,81,91}			15	
<F2,R,P,Dt,Sv,Cd,Dc>	15	{9,33,39}			86		{86,96,100}		{11,82,92}			14	
<F3,R,Dt,Sv,Cd>	16		18		81	40	{81,91}					17	
<F3,R,P,Dt,Sv,Cd>	17		19		82	40	{82,92}					16	
<F3,R,Dt,Sv,Cd,Dg>	18				81	41	{81,91}	20				19	
<F3,R,P,Dt,Sv,Cd,Dg>	19				82	41	{82,92}	21				18	
<F3,R,Dt,Sv,Cd,Dc>	20				85	42	{85,93}		{16,81,91}			21	
<F3,R,P,Dt,Sv,Cd,Dc>	21				86	42	{86,94}		{17,82,92}			20	

α	=	*Requête de commande*
β	=	*Requête de diagnostic*
γ	=	*Requête de reprise*
η	=	*Requête d'urgence*
μ	=	*Résultat de commande*
θ	=	*Résultat de détection*
ω	=	*Résultat de diagnostic*
υ	=	*Résultat de décision*
τ	=	*Résultat de reprise*
ϕ	=	*Résultat d'urgence*
ψ	=	*Détection de produit*
ON	=	*Mise en tension de la ressource*

FIG. 2.1: *Extrait de la table de transitions du modèle de référence*

les propriétés énumérées dans le premier chapitre de cette partie.

Dans le modèle de référence, le dysfonctionnement d'une ressource est caractérisé par l'occurrence de l'événement *résultat de détection* (θ). Cet événement est à la base du déclenchement d'un processus de traitement de défaillance. Puisque nous avons prétendu proposer des processus de traitements adaptés aux besoins des entreprises, il serait normal de mettre en évidence qu'à partir d'une activité de référence, plusieurs transitions conditionnées par l'événement "résultat de détection" sont en conflits structuraux (Valette [2001]).

Pour ce faire, nous nous sommes appuyés sur la même table de transitions évoquée plus haut. Au sein de cette table, nous nous sommes uniquement intéressés à l'événement *résultat de détection* (θ).

L'analyse effectuée sur cette table a révélé les propriétés suivantes :

- quelle que soit l'activité de référence considérée, il existe un maximum de **trois** transitions, conditionnées par l'événement *résultat de détection* (θ), conflictuelles (Figure 2.2).

- compte tenu du fait que ces transitions conduisent à des activités de référence différentes impliquant les fonctions diagnostic et/ou urgence, **trois** déclenchements de traitements distincts de défaillance peuvent donc être recensés :

  1. la première évolution est caractérisée par la désactivation de la fonction commande au profit de la fonction diagnostic. Ceci correspond au déclenchement d'un traitement "classique" de défaillances (Zamaï [1997]).
  2. la deuxième évolution témoigne de l'intervention simultanée des fonctions urgence et diagnostic. Ceci traduit le déclenchement d'une procédure d'urgence.

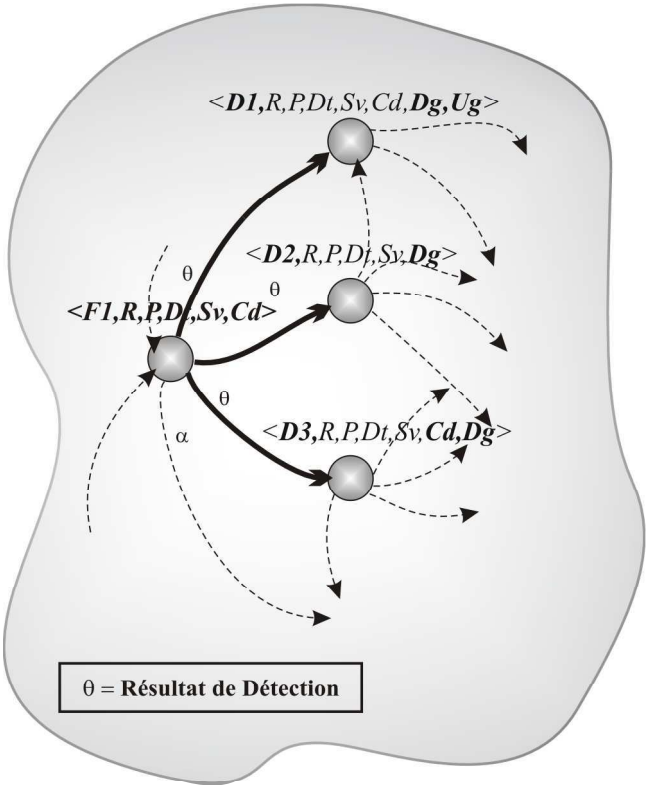

FIG. 2.2: *Indéterminismes provoqués pour l'événement* "résultat de détection"

3. la troisième évolution illustre l'appel à la fonction diagnostic alors que la ressource est toujours commandée. Cette situation correspond parfaitement à une production forcée où le diagnostic est lancé pour chercher les causes de la défaillance mais le processus de transformation continue.

Comme le lecteur pourra le constater dans la table des transitions présentée en annexe à ce mémoire, d'autres transitions sont en conflit structurel. Il s'agit notamment des transitions conditionnées par l'événement "résultat de décision". Ceci préfigure le fait que plusieurs types de résultats de décision peuvent être générés (remise en cause de la décision prise au niveau supérieur, appel à un service de maintenance, "tout va bien", on continue la production...). Bien entendu, le modèle de référence prévoit plusieurs processus pour traiter convenablement les différents résultats de décision. Dans le cadre de nos travaux, nous n'avons pas pris en compte les autres conflits structuraux du modèle. Cependant, comme nous allons le voir dans la suite de ce document, la méthode de synthèse proposée pourra être adaptée simplement afin de prendre en compte ces autres conflits structuraux.

Cette analyse basée sur la recherche des indéterminismes structuraux en fonctionnement normal et anormal est capitale. Elle met en exergue un point d'entrée dans le modèle de référence pour envisager une démarche de synthèse de lois de surveillance. En effet, synthétiser doit permettre en premier lieu de résoudre ces indéterminismes. Et, **résoudre ces indéterminismes, c'est aussi déterminer une technique permettant d'instancier l'événement générique "résultat de détection"** par un événement de la même famille en rapport direct avec la ressource considérée et les différentes propriétés données dans le chapitre précédent. Nous nous proposons de détailler cette proposition dans le paragraphe suivant.

2.3 Corrélation entre les propriétés recherchées et le modèle de référence

Dans le cadre de ce paragraphe, nous allons montrer que les indéterminismes inhérents au modèle de référence, à la fois en fonctionnement normal et anormal, peuvent être résolus par la prise en compte de chacune des propriétés proposées dans le chapitre 1 de cette partie. La méthode de résolution sera quant à elle détaillée dans le dernier chapitre de cette partie.

2.3.1 Les modes de marches et d'arrêts

Selon l'article R 233 105 du code de travail (AFNOR [1995a]), toute ressource physique est soumise à des règles opératoires fixées généralement par les notices d'utilisation livrées avec ces machines/outils. Ces dernières détaillent les instructions pour l'exploitation normale de la ressource, les limites d'utilisation, les procédures de maintenance, les MTBF (Mean Time Between Failure), etc.

Parmi ces règles d'utilisation, la spécification des modes de production normale est une donnée capitale pour l'exploitation de la ressource physique. Cette spécification conseille par exemple quant aux passages obligatoires en marches de vérification, de clôture, de test, etc.

Comme nous avons pu le montrer plus haut, quelles que soient les deux zones du modèle de référence (fonctionnement normal / traitements de défaillance), le modèle présente des indéterminismes structuraux (équivalents à des conflits de transitions dans un réseau de Petri (Valette [2001])). Dans le cadre de la prise en compte des modes de marches et d'arrêts liés au fonctionnement normal d'une ressource, nous allons ici nous intéresser à la première zone de ce modèle de référence.

Dans cette zone du modèle de référence, les indéterminismes sont caractérisés par les transitions conditionnées par l'événement *requête de commande* (α). Chaque évolution traduit le lancement d'une nouvelle phase de production normale à partir de l'activité courante. La figure 2.3 montre ce cas. Dans cette figure, l'état caractérisé par l'uplet

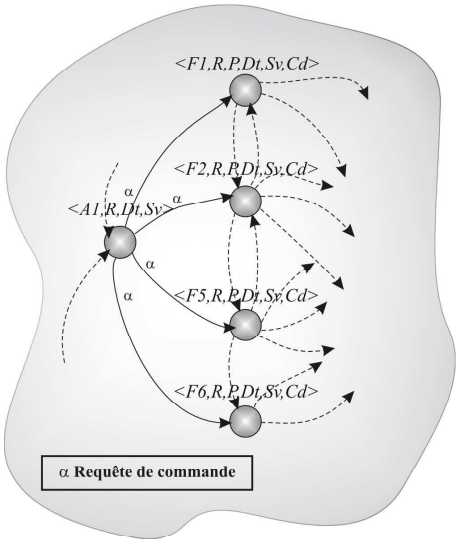

FIG. 2.3: *Exemple d'indéterminismes en production normale.*

$< A1, R, Dt, Sv, >$ désigne une ressource se trouvant dans un arrêt initial. *À* partir de cet

état, le modèle de référence nous offre quatre possibilités d'évolutions sous un fonctionnement normal :

- le passage à l'uplet $< F1, R, Dt, Sv, Cd >$ qui correspond au lancement immédiat d'une production normale,
- le passage à l'uplet $< F2, R, Dt, Sv, Cd >$ traduisant le lancement d'une marche de préparation avant de commencer la production normale,
- l'évolution vers l'uplet $< F5, R, Dt, Sv, Cd >$ qui sert à lancer une marche de vérification dans l'ordre,
- la transition conduisant à l'état $< F6, R, Dt, Sv, Cd >$ pour lancer une marche de test.

Le choix dépendra des caractéristiques techniques de la ressource et des intérêts de l'utilisateur. Ainsi, si nous travaillons avec le cas du four, l'évolution nécessaire correspond au passage de l'activité $< A1, R, Dt, Sv, >$ vers l'activité $< F2, R, Dt, Sv, Cd >$. Tel que nous l'avons signalé, cette évolution permet de préparer le four pour qu'il puisse accomplir ses objectifs. La préparation consiste à lancer une séquence pour réaliser le préchauffage du four. La spécification des modes du fonctionnement normal permet donc de résoudre ces indéterminismes par rejet des activités n'intégrant pas ces modes.

2.3.2 La récursivité

Le langage reconnu obtenu par le générateur de langage représenté par le modèle de référence contient un grand nombre de fermetures itératives (L^*). Les fermetures itératives sont des cycles répétitifs qui traduisent la possibilité d'appliquer une même séquence plusieurs fois. En effet, le modèle de référence ne limite à aucun moment l'exécution des séquences répétitives ; les cycles peuvent donc être exécutés indéfiniment.

Les séquences répétitives qui se trouvent dans la zone de fonctionnement normal indiquent qu'une séquence de production normale peut être lancée autant de fois que l'utilisateur le souhaite. Ceci dépendra donc des modèles de commande qui seront exécutés par la fonction commande. Si nous prenons pour hypothèse que ces modèles de commande sont correctement spécifiés, il n'y a aucune raison de restreindre la loi de surveillance à la limitation du nombre de répétitions d'une séquence de production normale.

En revanche, dans la zone de traitement des défaillances, ne pas contraindre ces structures répétitives, c'est prendre le risque de continuellement traiter une défaillance détectée au cours d'un autre traitement de défaillance, détectée à son tour durant un autre processus, etc. Ceci peut donc avoir des conséquences fâcheuses pour certaines des propriétés qui doivent être recherchées, comme par exemple la productivité ou encore la sécurité.

Par exemple, dans la figure (Fig. 1.4) de cette même partie, la séquence $\{\alpha(\theta\omega)^*\nu\tau\}$ indique que les événements $(\theta\omega)$ peuvent se répéter indéfiniment si une défaillance survient au moment d'exécuter une reprise. Dans la réalité, un opérateur humain expérimenté ne tolérera jamais un tel fonctionnement. Il envisagera sans doute une autre manière de réagir, comme par exemple appliquer un arrêt d'urgence.

La limitation de ces structures répétitives est à la charge de l'entreprise et se formalise de la façon suivante :

$$\forall L \| L_1^* \subset Let L_1^* \in X_t, L_1^* \rightarrow n(L_1)$$

avec $n =$ nombre maximum de répétitions autorisées d'un traitement de défaillance.

2.3.3 Les critères Productivité, Qualité, Sécurité et Écologie

Jusqu'à présent, nous avons étudié les corrélations existant entre le modèle de référence et les contraintes des modes de marches et de récursivité. Maintenant, nous nous proposons de tenter de mettre en évidence le lien qui unit les critères Productivité, Qualité, Sécurité et Écologie et le modèle de référence.

L'analyse structurelle menée plus haut a montré le caractère indéterministe du modèle de référence, à la fois en fonctionnement normal et anormal. En fonctionnement normal, prendre en compte les quatre critères proposés revient à respecter les modes de marches et d'arrêts issus des documentations techniques associées à la ressource, mais également à spécifier et à concevoir des lois de commande adaptées (hors cadre de notre étude).

Reste donc maintenant à déterminer si ces mêmes critères peuvent avoir un impact majeur quant à la résolution des indéterminismes en présence de défaillances. Nous rappelons ici que dans le cadre de ces travaux, nous ne nous intéresserons qu'aux indéterminismes de transitions conditionnées par l'événement "résultat de détection" (θ).

D'après le modèle de référence, l'occurrence d'un tel événement traduit généralement le déclenchement d'un processus de traitement de défaillances. Ces processus ont été caractérisés par trois traitements distincts que sont les traitements classiques, les traitements d'urgence ou encore les traitements de type production forcée. Rappelons qu'un traitement classique modélise le fait que le système de commande est bloqué suite à l'occurrence d'une défaillance et que les fonctions diagnostic, décision et reprise seront successivement déclenchées pour corriger les effets de la défaillance. Un traitement d'urgence est caractérisé quant à lui par le déclenchement de la fonction urgence afin d'appliquer des procédures prioritaires sur la commande. En parallèle, un processus diagnostic, décision et reprise est généralement lancé. Enfin, un traitement de type production forcée tolère ou absorbe l'occurrence de certaines défaillances tout en surveillant "de plus près" la ressource concernée. Ceci se fait en déclenchant la fonction de surveillance appelée diagnostic.

Choisir hors ligne ou en ligne le type de traitement de défaillance (choix d'un chemin dans le modèle de référence) qui doit être déclenché suite à l'occurrence d'un événement "résultat de détection" revient à évaluer non seulement le **coût** de ce chemin pour l'ensemble des critères proposés, mais aussi à évaluer l'impact de la défaillance détectée pour chacun des critères. Il va en effet de soi que pour une ressource considérée, lancer un traitement d'urgence revient à pénaliser la productivité de l'entreprise au profit de la sécurité des hommes et des machines. En revanche, accepter une production forcée peut à court terme préserver la productivité, et ce, peut être au détriment de la qualité.

D'autre part, savoir évaluer le coût d'un traitement de défaillance pour chacun des critères proposés n'est pas suffisant pour "décider" quel chemin prendre lors de l'occurrence de la défaillance. Il est aussi nécessaire de pouvoir évaluer le coût du "résultat de détection". Par exemple, savoir caractériser le fait qu'une ressource se trouve dans un état incompatible avec le respect de sa structure physique (sur-course d'un bras de robot par exemple), c'est en partie décider du traitement correctif qu'il faut appliquer.

Cependant, pour chaque ressource considérée, dresser une liste exhaustive des défaillances qui peuvent survenir au cours d'un cycle de production ne peut pas toujours être envisagé ; la complexité est généralement incompatible avec l'exhaustivité. Pour cette raison, notre approche doit s'appuyer sur une technique de détection générique et indépendante de la complexité du procédé surveillé, commandé et supervisé. L'événement "résultat de détection" doit être affiné afin de le rendre exploitable pour la synthèse de lois de surveillance. Ici, synthétiser reviendra à choisir un chemin en fonction du niveau d'interprétation de l'événement "résultat de détection".

L'approche (Combacau [1991]) propose une telle solution. Elle s'appuie sur une hypothèse simple et efficace : **"tout ce qui n'est pas normal est forcément anormal"**!

2.4 Pré-requis à la synthèse

2.4.1 Approche générique de détection

Notre approche a adopté les techniques de détection de défaillances du procédé proposées dans (Combacau [1991]).

Remarque : pour des raisons de concision, nous ne reprendrons pas ici tous les détails de l'approche mais ne retiendrons uniquement que les principes généraux et les définitions des symptômes proposées par l'auteur. Pour plus de détails, nous convions bien entendu le lecteur à se reporter à (Combacau [1991]).

L'approche garantit la détection de toute déviation de comportement au moyen de quatre symptômes[1] parfaitement génériques et donc indépendants du procédé considéré.

Dans cette approche, deux techniques d'analyse des défaillances sont considérées : une analyse comportementale et une analyse temporelle.

2.4.1.1 Analyse comportementale : symptômes 1 et 2

Comme nous avons pu le constater dans la première partie de ce mémoire, l'approche (Combacau [1991]) s'appuie sur l'exploitation conjointe de deux modèles. Le premier représente l'ensemble des possibilités offertes par le procédé (modèle des états utilisables), le deuxième spécifie les contraintes de commande qui doivent être imposées au procédé (modèle des états autorisés).

Le mécanisme développé pour la détection des défaillances caractérisées par les symptômes 1 et 2 est basé sur l'étude de l'impact de comptes rendus sur les modèles du procédé et de commande. Ces comptes rendus sont renvoyés par le sous-système commandé en réponse à une requête de commande.

Lorsqu'une requête de commande est envoyée vers le sous-système commandé, le système de détection se met en attente du compte rendu correspondant spécifié dans le modèle de commande. Lorsque ce dernier arrive, il est naturellement comparé à celui attendu par le modèle de commande. Ainsi, trois situations distinctes peuvent être caractérisées :

- le compte rendu traduit une évolution possible du modèle de commande. Dans ce cas, la fonction détection ne caractérise bien entendu aucun symptôme de défaillance.

- le compte rendu est rejeté par le modèle de commande mais traduit cependant une évolution du modèle de référence. La fonction détection caractérise alors un symptôme **S1**. Ce dernier représente le fait que le sous-système commandé n'a pas réalisé ce qu'on lui a dit de faire, mais n'a cependant pas transgressé de contraintes matérielles. De plus, l'état réel du sous-système est connu puisque représenté dans le modèle du procédé.

1. un symptôme de défaillance est l'événement ou l'ensemble de données au travers desquels le système de détection identifie le passage du procédé dans un fonctionnement anormal (SPSF et al. [1999])

– le compte rendu ne traduit aucune évolution possible, ni dans le modèle de commande, ni dans le modèle du procédé. La fonction détection caractérise alors un symptôme **S2**. Ce dernier indique que non seulement le sous-système n'a pas fait ce qu'on lui a demandé, mais que de surcroît il a transgressé une ou plusieurs contraintes matérielles. Le sous-système commandé n'est donc plus représenté par les modèles de commande et de référence.

2.4.1.2 Analyse temporelle : symptômes 3 et 4

Bien entendu, l'exploitation conjointe de ces deux modèles ne permet pas de caractériser toutes les défaillances de la partie opérative comme par exemple l'absence de comptes rendus suite à l'emission d'une requête de commande. Ce peut être le cas par exemple lorsqu'un capteur est hors service. Afin de prendre en compte ces problèmes, l'auteur a proposé d'intégrer aux modèles de commande et de procédé des mécanismes de chiens de garde. Dans le cadre de la détection des défaillances issues du sous-système commandé, ces mécanismes s'appuient ici sur l'exploitation de deux dates critiques fournies par l'ordonnancement : la date de fin au plus tôt et la date de fin au plus tard d'une opération de commande. Compte tenu de la fenêtre temporelle d'estimation de fin d'opération de commande bornée par ces deux dates, deux symptômes distincts peuvent être caractérisés :

– occurrence du compte rendu avant la date de fin au plus tôt. Dans ce cas, la fonction de détection caractérisera un symptôme de type 3 (**S3**).

– absence de réception du compte rendu. Ceci est systématiquement détecté par le chien de garde basé sur la date de fin au plus tard de l'opération de commande. Dans ce cas, la fonction détection proposée par l'auteur caractérise un symptôme de type 4 (**S4**). Ici, l'état du procédé ne peut donc plus être précisément représenté.

Comme nous pouvons le constater, cette approche puise sa force du caractère générique, systématique et exhaustif de la méthode de détection retenue.

L'intégration de cette méthode de détection au sein de notre approche, revient à instancier l'événement "résultat de détection" porté sur les transitions du modèle de référence par l'une ou plusieurs des quatre symboles génériques S1, S2, S3 et/ou S4.

La problématique actuelle revient donc à se poser la question : comment instancier l'événement "résultat de détection" par le ou les bons symptômes? C'est ce que nous nous proposons d'étudier dans le paragraphe suivant.

2.4.2 Impact des symptômes de défaillances sur les propriétés recherchées

Comme nous avons pu le noter dans les paragraphes précédents, deux concepts fondamentaux sont à retenir pour la synthèse de lois de surveillance. En premier lieu, trois points de départ de traitements de défaillances ont pu être mis en évidence quel que soit l'état considéré du modèle de référence. L'application de l'un de ces traitements a un impact évident sur chacun des critères proposés. En second lieu, la déclinaison de l'événement "résultat de détection" en quatre symptômes distincts, génériques et bien définis laisse aussi entrevoir une possibilité d'évaluation de l'impact du symptôme détecté sur chacun des critères retenus. Retenir une même échelle d'évaluation commune pour les symptômes de défaillances et pour les traitements de défaillance (chemins dans le modèle

de référence) reviendrait donc à établir un lien de cause à effet entre ces deux concepts. Ce serait donc apporter une solution à la problématique de l'instanciation des événements "résultats de détection" portés sur certaines transitions du modèle de référence et donc en partie à la problématique de la synthèse de lois de surveillance.

Dans ce qui suit, nous allons nous attacher à identifier cette échelle d'évaluation. Pour ce faire, nous nous sommes tout d'abord appuyés sur les travaux et les normes caractérisant chacun des critères retenus, puis nous nous sommes attachés à déterminer et à proposer une échelle commune d'évaluation des conséquences des symptômes de défaillances et des coûts d'un traitement de défaillance.

2.4.2.1 Échelles d'évaluation connues

Les premiers travaux qui ont porté sur l'évaluation de l'impact d'une défaillance ont été fait au profit de la sécurité puis de l'écologie. La notion de risque ou de criticité y a été définie comme étant la mesure d'un danger exprimé en fonction de l'occurrence d'un événement indésirable (probabilité, fréquence) et d'une mesure de ses effets ou de ses conséquences. Un danger est une situation dont les conséquences peuvent nuire à l'homme (blessure ou mort de personnes), à la société (perte de production, perte financière, etc.) ou à l'environnement (dégradation du milieu naturel et animal, pollution). Pour la sécurité, une échelle de risque est souvent associée au danger afin de pouvoir classer les défaillances en niveaux de criticité. Si l'on considère l'incidence d'une défaillance sur l'intégrité des opérateurs humains (sécurité) et sur la mission de l'équipement (sûreté) évaluée dans la publication CEI 271 (Sourisse et Boudillon [1996]), on distingue quatre niveaux de gravité :

- Niveau 1 - gravité mineure : conséquences négligeables sur la mission,
- Niveau 2 - gravité significative : interruption de la mission et gêne sur les intervenants,
- Niveau 3 - gravité critique : mise en jeu de la sécurité. Dégradations importantes et conséquences à terme,
- Niveau 4 - gravité catastrophique : mise en jeu de la survie ou accident corporel.

Dans le cadre de l'environnement, le BARPI [2] du Ministère de l'environnement a mis au point une *échelle de gravité* qui en compte six (IFEN [1998]) :

- Niveau 1 : ce niveau est décrit comme une anomalie sans conséquences pour l'environnement,
- Niveau 2 : incident. Fait inhabituel, petit obstacle sans conséquences pour l'environnement,
- Niveau 3 : accident sérieux. Risque de pollution dans la zone de travail avec danger pour les opérateurs humains,
- Niveau 4 : accident plus sérieux encore mais sans conséquences hors du site de production,
- Niveau 5 : accident sérieux avec conséquences hors du site de production,

2. BARPI - Bureau d'Analyse des Risques et Pollutions Industriels

– Niveaux 6 : accident majeur. Les conséquences de pollution s'étendent à plusieurs kilomètres du site de production.

En revanche, pour les deux autres critères de productivité et de qualité, il n'existe pas à notre connaissance de véritables échelles d'évaluation normalisées de l'impact de défaillances.

Pour la productivité par exemple, l'impact d'une défaillance est uniquement évalué a posteriori par le calcul de la différence entre les volumes de production prévus par les plans de production et ceux réellement obtenus.

Il en va de même pour le critère *qualité*, où la qualité de la fabrication est évaluée a posteriori par une mesure de l'adéquation entre le cahier des charges qualité (ce que le client voulait, à la date spécifiée, au prix convenu) et le produit effectivement fabriqué.

2.4.2.2 Proposition d'une échelle d'évaluation commune

Dans le cadre de notre approche, nous avons proposé de prendre en compte au moins quatre critères (Productivité, Qualité, Écologie, Sécurité) afin de synthétiser des lois de surveillance adaptées. Comme nous avons pu le voir, synthétiser revient en partie à instancier les transitions du modèle de référence conditionnées par l'événement "résultat de détection" par le ou les bons symptômes de défaillance. Cela laisse donc supposer qu'à partir d'une activité de référence comme $< F1, R, P, Dt, Sv, Cd >$, l'occurrence de l'événement "S1" conduise le système vers un traitement classique de défaillance et "S2 ou S4" vers un traitement d'urgence. Afin d'instancier correctement les transitions du modèle avec les symptômes répondant au respect des quatre critères retenus, il est nécessaire de retenir une seule et même échelle d'évaluation. Il n'est en effet pas envisageable de considérer qu'une défaillance peut avoir des conséquences de niveau 3 sur le plan sécurité et écologie alors que ces deux niveaux ne sont pas identiques pris séparément.

Compte tenu de la bonne maîtrise de la grille associée à la sécurité dans le milieu industriel, notre proposition consiste à l'étendre aux trois autres critères. De plus, nous proposons l'intégration d'un cinquième niveau d'évaluation. Ce niveau correspond au niveau 0 et caractérisera des défaillances non significatives. Une défaillance peut en effet n'avoir aucune conséquence sur un critère considéré. Par exemple, si un procédé de fabrication manipule ni produit ni ressource présentant un risque pour l'environnement, il est bien évident qu'aucun symptôme de défaillance aura des effets sur le critère écologie.

Pour chacun des quatre critères recherchés pour la synthèse de lois de surveillance, nous proposons ci-après un ensemble de quatre grilles d'évaluation de l'impact de symptômes de défaillances. Pour le critère sécurité, la grille utilisée reste égale à celle proposée dans la publication CEI 271 (page 104). Nous proposons seulement d'ajouter à cette échelle le cinquième niveau, Non-significatif :

– **Sécurité**
  – Non-significatif : la défaillance n'a pas de conséquence sur la sécurité,
  – Niveau 1 - gravité mineure : conséquences négligeables sur la mission,
  – Niveau 2 - gravité significative : interruption de la mission et gêne sur les intervenants,
  – Niveau 3 - gravité critique : mise en jeu de la intégrité des opérateurs. Dégradations importantes et conséquences à terme,
  – Niveau 4 - gravité catastrophique : mise en jeu de la survie ou accident corporel.

Pour les trois autres critères, les échelles d'évaluation proposées sont :

- **Écologie**
  - Non-significatif : pas de conséquences polluantes sur l'environnement,
  - Mineur : les niveaux de pollution provoqués par la défaillance sont au-dessous des niveaux établis par les organismes protecteurs de l'environnement,
  - Significatif : les conséquences de la défaillance conduisent à des dégradations graves latentes en interne à l'entreprise,
  - Critique : pollution effective au sein de l'entreprise avec risque de propagation externe,
  - Catastrophique : les conséquences de pollution s'étendent à plusieurs kilomètres du site de production.
- **Productivité**
  - Non-significatif : pas de conséquences sur les volumes de production,
  - Mineur : légère réduction des volumes de production sans remise en cause des objectifs,
  - Significatif : remise en cause de l'objectif de production fixé,
  - Critique : non seulement l'objectif de production ne pourra être atteint, mais la rentabilité de l'entreprise est mise en cause,
  - Catastrophique : la productivité va être quasiment réduite à zéro.
- **Qualité**
  - Non-significatif : pas de conséquence sur la qualité des produits (ISO [2000]),
  - Mineur : légère transgression des contraintes de qualité fixées. Les niveaux qui seront obtenus resteront cependant dans des marges acceptables,
  - Significatif : le niveau de qualité ne pourra pas être accepté, mais la pièce pourra être réparée et mise à niveau en but de chaîne de production,
  - Critique : le produit est non conforme aux exigences du cahier des charges, il ne peut pas être entièrement récupéré, seul un sous-ensemble du produit peut être re-introduit (toujours en adéquation avec la qualité fixée) en amont de la chaîne de production,
  - Catastrophique : aucune adéquation entre le cahier des charges et le produit qui sera obtenu. De surcroît, aucun des constituants du produit ne répond aux exigences qualitatives, ils ne pourront donc pas être directement récupérés.

Remarque : l'analyse de la propriété permettant de régler les priorités entre critères a été volontairement exclue de ce chapitre. Elle ne peut en effet être détaillée qu'après obtention d'un modèle intermédiaire intégrant déjà les quatre critères retenus. Pour cette raison, cette propriété sera examinée dans le cadre du chapitre suivant.

2.5 Conclusion

Dans le cadre de ce chapitre, nous avons développé et posé les fondations de notre approche de synthèse. Pour ce faire, nous avons tout d'abord analysé les propriétés structurelles du modèle de référence établi dans la partie II de ce mémoire. Cette analyse a mis en exergue le caractère indéterministe du modèle. Ces indéterminismes sont liés aux différentes possibilités offertes par le modèle de référence pour surveiller, commander et superviser une ressource considérée. Dans une démarche de synthèse, nous avons alors montré que synthétiser revenait en partie à instancier le modèle de référence afin de le rendre déterministe. Cette résolution s'appuie non seulement sur l'intégration des modes des marches et d'arrêts en fonctionnement normal mais aussi sur l'intégration des quatre critères (Productivité, Qualité, Sécurité et Écologie) lors du déclenchement d'un traitement de défaillance. Pour chacun de ces points, nous avons proposé des démarches pour la synthèse en partant de l'inhibition des activités de référence qui n'appartiennent pas aux modes recherchés jusqu'à l'évaluation de symptômes de défaillances génériques sur la base de quatre échelles d'évaluation.

A ce stade de l'étude, tous les éléments sont disponibles pour proposer notre démarche de synthèse de lois de surveillance. C'est ce que nous nous proposons d'établir dans le chapitre suivant.

Chapitre 3

Synthèse de lois de surveillance

3.1 Introduction

Dans les chapitres précédents, nous avons dressé les fondations de notre approche de synthèse de lois de surveillance. Ces dernières se déclinent sous la forme d'un modèle de référence dont la structure de contrôle est générique et indéterministe, d'une liste de propriétés qui doivent être recherchées, et d'un ensemble de corrélations mettant en relation directe les propriétés retenues et la structure même du modèle de référence. D'autre part, nous avons également émis une hypothèse de travail qui restreint notre démarche de synthèse à la résolution des indéterminismes conditionnés par le "résultat d'une détection".

Dans le cadre de ce chapitre, nous nous proposons d'exposer le point de vue technique de cette approche de synthèse de lois de surveillance.

Dans ce but, ce chapitre a été structuré autour de cinq paragraphes. Le premier paragraphe s'attache à présenter la démarche générale de synthèse que nous proposons. Nous mettons en évidence la nécessité de procéder par intégration successive des propriétés recherchées. Ceci nécessite bien entendu le recours à plusieurs techniques de synthèse, quatre pour être exact. Aussi, les quatre autres paragraphes exposent chacune de ces quatre techniques. La première permet de prendre en compte les modes de marches et d'arrêts liés à l'utilisation normale d'une ressource considérée. La seconde montre comment des critères tels que la productivité, la qualité, la sécurité ou encore l'écologie peuvent être intégrés au sein du modèle de référence. La troisième technique traite du réglage des priorités entre les critères retenus, et la quatrième détaille la prise en compte de la récursivité des traitements de défaillances.

3.2 Démarche générale

La méthode de synthèse proposée revient à raffiner successivement le modèle de référence proposé dans la partie II (Méndez et al. [2002a]). Cette démarche générale retenue dans le cadre de notre approche est entièrement schématisée dans la Figure 3.1. Comme le montre cette figure, nous allons progressivement intégrer chacune des propriétés présentées dans les deux chapitres précédents au sein du modèle. L'intégration progressive a pour effet de contraindre le modèle et donc le "réduire" au fur et à mesure jusqu'à obtenir une loi de surveillance déterministe respectant chacune des propriétés fixées. Chacune des étapes proposées dans cette figure correspond à la synthèse d'une loi respectant la

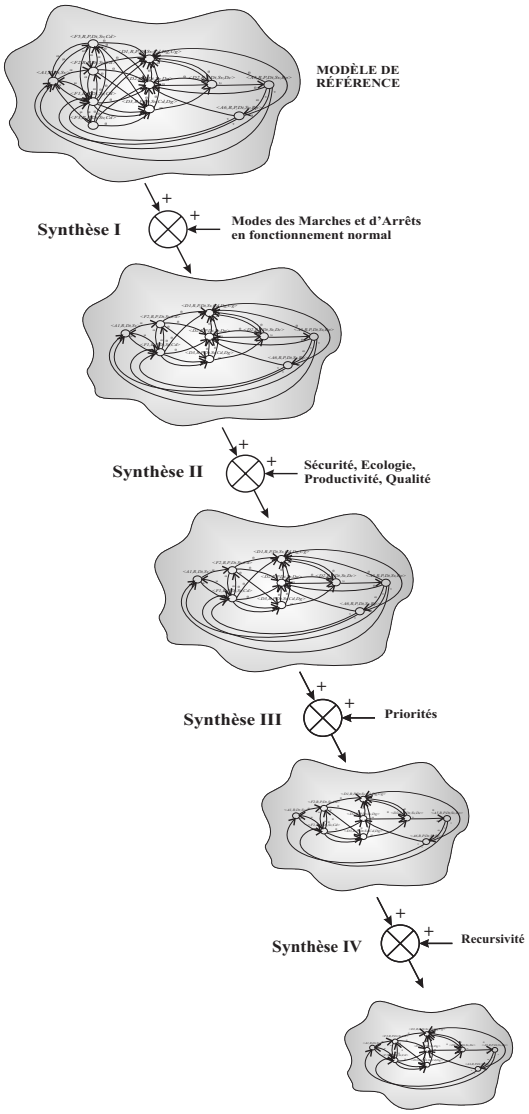

FIG. 3.1: *Démarche proposée pour la synthèse de lois de surveillance*

propriété considérée. Ces étapes sont rappelées ci-après :

Intégration des modes des marches et d'arrêts : il s'agit ici de rejeter les modes des marches et d'arrêts qui n'appartiennent pas au fonctionnement normal en fonction des fiches techniques de la ressource considérée.

Intégration des critères : quelles que soient les activités de référence restantes, il s'agit ici d'instancier toutes les transitions conditionnées par l'événement "résultat de détection" par le ou les bons symptômes de défaillance (S1, S2, S3 et/ou S4). Pour cela, deux évaluations sont demandées au concepteur de la loi de surveillance. En premier lieu, et à partir de toutes les activités de référence, il faut évaluer le coût de chacun des trois traitements de défaillance (production forcée, traitement classique et traitement d'urgence) par rapport à chacun des quatre critères retenus (Productivité, Écologie, Sécurité et Qualité). Une deuxième évaluation doit ensuite porter sur chacun des quatre symptômes de défaillances détectables à partir de chacune des activités de référence restantes. Dans cette étape, synthétiser revient à projeter les symptômes sur les transitions concernées en suivant le "vecteur" d'évaluation.

Réglage des priorités : en cas de conflits non résolus entre les transitions conditionnées par les symptômes de défaillances, il s'agit de les résoudre en considérant des priorités

données par le concepteur. Il va de soi que les critères "Sécurité et Écologie" devront toujours avoir la priorité sur la "Productivité et la Qualité".

Réglage de la récursivité : afin d'éviter des cycles infinis dans les traitements de défaillances suite à l'occurrence répétitive de défaillances, il s'agit ici de fixer ou de régler le nombre de fois qu'un traitement de défaillance peut être lancé.

Nous nous proposons désormais de présenter plus en détail chacune de ces étapes de synthèse.

3.3 Synthèse I : intégration des modes de marches et d'arrêts

Comme nous avons pu l'évoquer dans le chapitre précédent, nous allons rechercher ici une technique permettant de rejeter systématiquement les activités de référence qui ne sont pas en adéquation avec les modes de marches et d'arrêt du fonctionnement normal (F1 à F6 et A1 à A4) spécifiés par le concepteur. Par exemple, rejeter toutes les activités appartenant à la famille "marche de préparation" revient à amputer le modèle de référence de 6 activités de référence et 79 transitions.

Notre proposition consiste à utiliser le GEMMA réduit aux modes du fonctionnement normal sous sa forme graphique (Figure 3.2). A partir de ce graphe, nous demandons

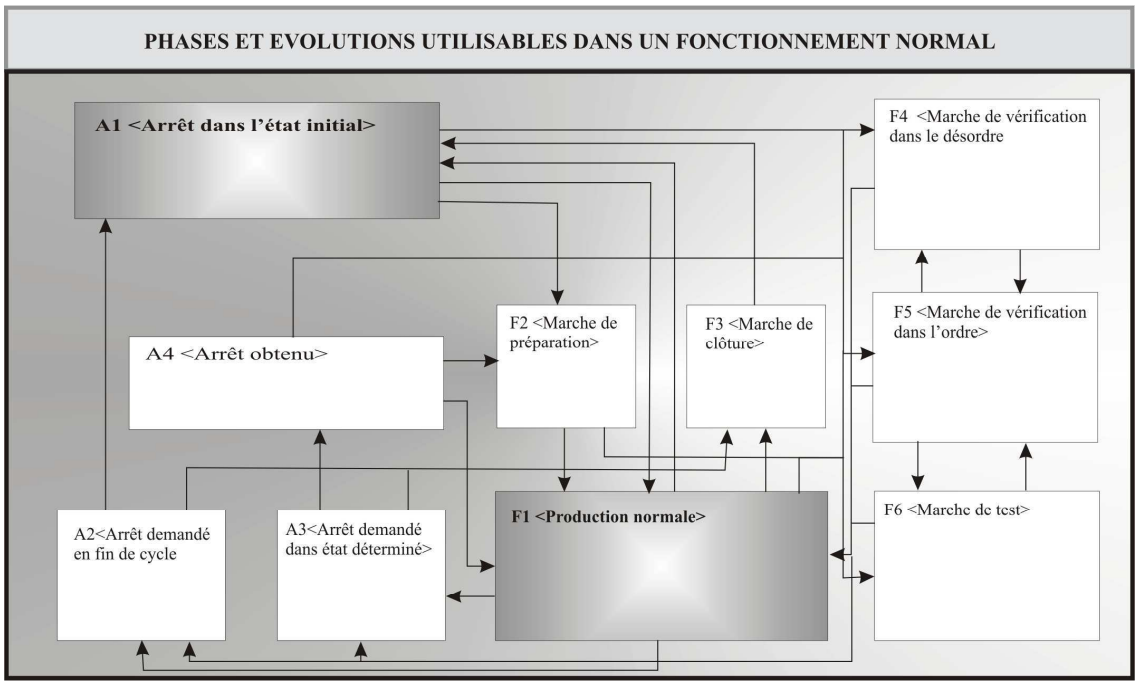

FIG. 3.2: *GEMMA réduit aux modes du fonctionnement normal*

au concepteur de la loi de surveillance d'appliquer une démarche classique d'utilisation du GEMMA. Il s'agit de marquer (éliminer) les modes incompatibles avec la ressource considérée et de sélectionner les commutations autorisées (Figure 3.3). Dans cette figure, nous montrons un exemple d'application de cette démarche pour une ressource de type *four industriel*. Pour cette ressource, le fonctionnement normal est caractérisé par les modes et les commutations suivants : *arrêt initial* → *marche de préparation* → *production normale* → *arrêt initial*.

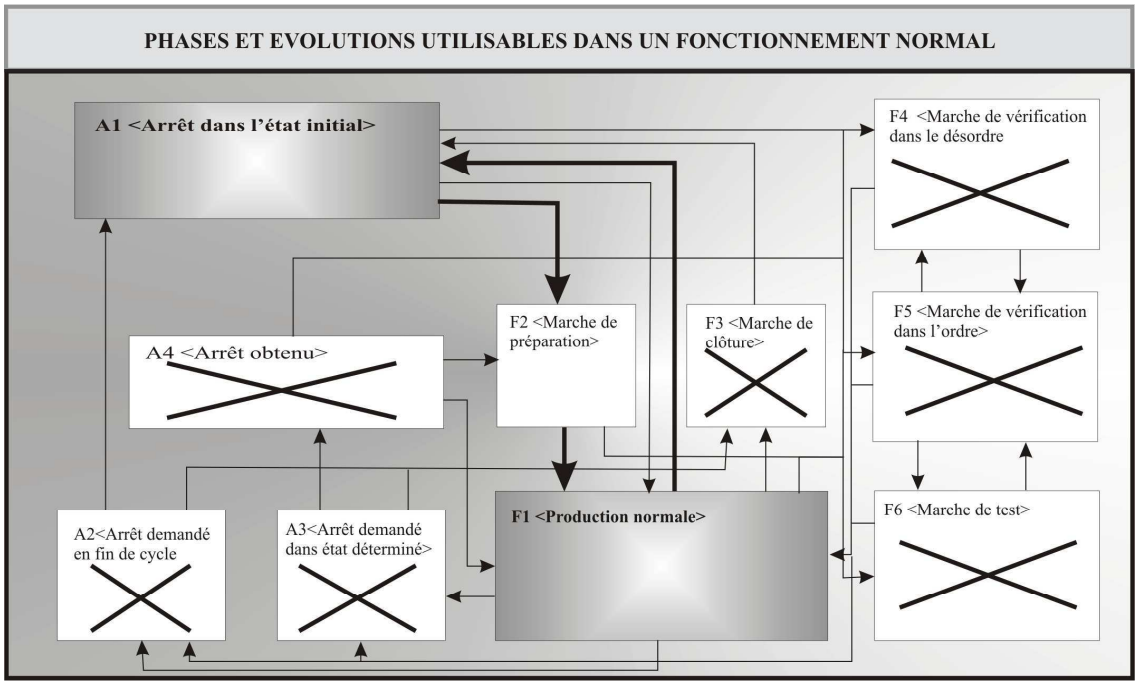

FIG. 3.3: *Exemple d'utilisation du GEMMA réduit*

D'un point de vue technique, nous avons considéré une représentation matricielle G_n de ce GEMMA réduit aux modes M_n= $A1, A2, A3, A4, F1, F2, F3, F4, F5, F6$.

$$G_n = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Dans cette matrice, les lignes et les colonnes représentent les dix modes considérés (M_n). Les 0 et les 1 caractérisent l'existence d'une commutation de référence ou non.

Par exemple, l'impossibilité de commuter d'une production normale (F1) à une marche de préparation (F2) est indiquée par $G_n(5,6) = 0$. La possibilité de passer du mode A1 (arrêt normal) à une phase de production normale (F1) est définie par $G_n(1,5) = 1$.

Rejeter des modes appartenant à M_n au sein de cette matrice G_n, revient à mettre à zéro tous les éléments de la ligne et de la colonne correspondante. Rejeter ensuite les commutations incompatibles revient à mettre à 0 le 1 correspondant dans G_n.

Notons alors G'_n la matrice répondant aux exigences. La première phase de synthèse

revient alors à appliquer la projection $P : \delta_n(x, \sigma) \rightarrow x'$ suivante :

$$P(\delta(x,\sigma)) = \begin{cases} \delta(x,\sigma) \text{ si } G'_n(i,j) = 1, x(m) = M_n(i), x'(m) = M_n(j) \\ \delta(x,\varepsilon) \text{ si } G'_n(i,j) = 0, x(m) = M_n(i), x'(m) = M_n(j) \\ \delta(x,\varepsilon) \text{ si } G'_n(i,j) = 0, x(m) = M_n(j) \end{cases}$$

où

- ε représente le mot vide et caractérise l'inhibition d'une évolution dans le modèle de référence (Sampath et al. [1996]),
- $\Sigma = \{\alpha, \beta, \gamma, \eta, \mu, \theta, \omega\}$ (cf. chapitre 3, partie II).

Cette projection revient à étudier toutes les transitions du modèle de référence réduit à $X_n = \{x_0 \cup x \in X : x(m) \in M_n\}$. Pour chacune de ces transitions, l'événement la conditionnant est conservé (σ) ou remplacé par ε selon que la commutation est autorisée ou non dans G'_n. La figure 3.4 donne un aperçu de la démarche proposée.

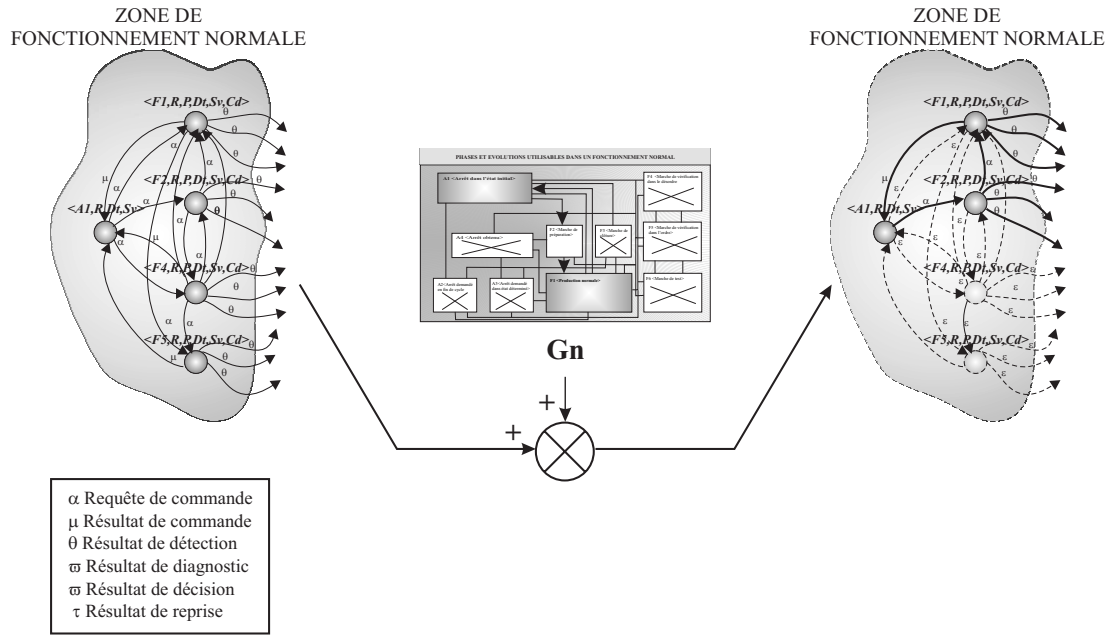

FIG. 3.4: *Principe de la synthèse I*

3.4 Synthèse II : intégration des critères

L'objectif de cette synthèse, que nous qualifions de "synthèse II", consiste, d'une part, à instancier convenablement chacune des transitions du modèle de référence conditionnées par l'événement "résultat de détection" par le ou les "bons" symptômes de défaillance, et d'autre part à résoudre les indéterminismes. Comme nous l'avons déjà démontré, il ne s'agit pas que le système de surveillance, commande et supervision reste bloqué sur l'occurrence d'une défaillance. Un choix de traitement doit être impérativement fait!

La démarche que nous proposons consiste à évaluer l'impact sur chacun des critères retenus, d'une part des symptômes de défaillances S1, S2, S3 et S4 et d'autre part des trois traitements de défaillances utilisables. Ces évaluations faites, la démarche consiste alors à projeter les symptômes sur les transitions marquant le début d'un nouveau traitement de défaillance.

D'un point de vue pratique, nous proposons au concepteur de la loi de surveillance de compléter deux grilles qui mettent en relation impacts/traitements et symptômes/impacts ; nous associons au terme *impact* l'ensemble des niveaux de gravité proposés dans le chapitre précédent (i.e. mineur, significatif, critique et catastrophique). Comme nous le préciserons plus loin, le niveau non-significatif n'a pas à être pris en compte de manière explicite.

La première grille est donc caractérisée par trois lignes et quatre colonnes. Chaque ligne correspond à un traitement de défaillance. La première ligne illustre une production forcée (PF), la deuxième représente un traitement classique de défaillances (TC) et la troisième caractérise un traitement d'urgence (TU). Les colonnes représentent les quatre niveaux de gravité. Ainsi, la première colonne est associée au niveau *mineur*, la seconde au niveau *significatif*, la troisième au niveau *critique* et la dernière colonne au niveau *catastrophique* (Figure 3.5).

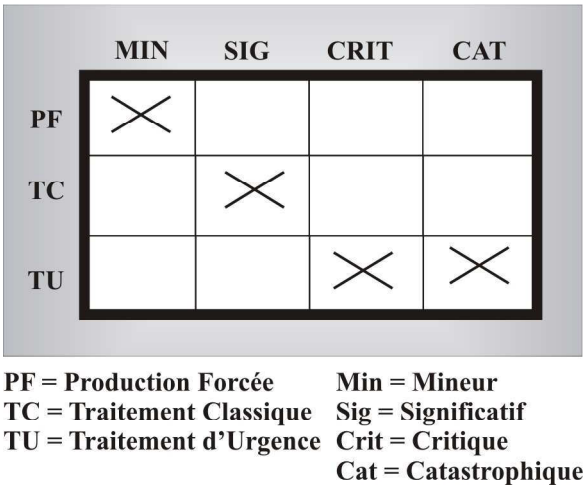

FIG. 3.5: *Première grille d'évaluation*

Pour une ressource considérée et pour les quatre critères retenus (Productivité, Qualité, Écologie et Sécurité), quatre versions de cette grille doivent être remplies. La méthode préconisée pour remplir ces grilles consiste à répondre à la question suivante : *pour le critère X et pour un symptôme de défaillance de gravité Y, quel traitement de défaillance faut-il appliquer ?* Pour cela, le concepteur doit s'appuyer **impérativement** sur les définitions données à la fois pour les critères, les symptômes, les niveaux de gravité et les traitements de défaillances. Compte tenu de cette définition de l'évaluation impact/traitement, il est clair que le niveau non-significatif ne présente pas de sens. En effet, si un symptôme est considéré non-significatif, aucun traitement est nécessaire.

La deuxième grille met en relation les symptômes de défaillance avec leurs niveaux de gravité. Le niveau non-significatif ayant été rejeté pour la première grille, il devient également ici obsolète. Lorsqu'un symptôme sera considéré comme tel, aucune croix ne sera marquée dans la colonne correspondante. Cette grille a donc une taille de quatre lignes par quatre colonnes. A chaque ligne est associé un niveau de gravité ; à chaque colonne est affecté un symptôme de défaillance (Figure 3.6).

Pour une ressource considérée, 16 modes des marches et d'arrêts peuvent être considé-

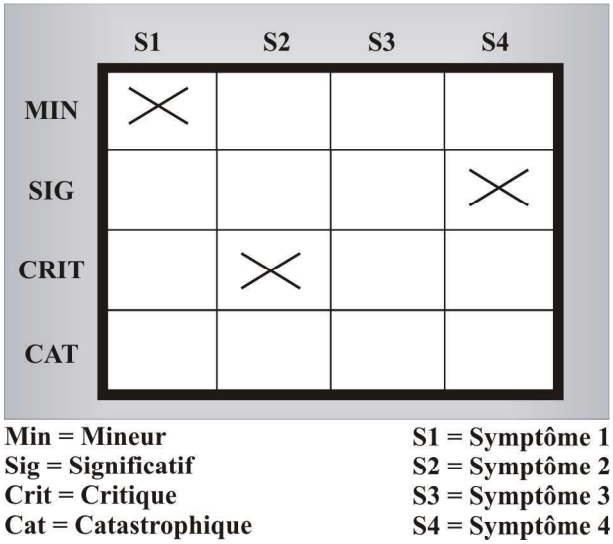

FIG. 3.6: *Deuxième grille d'évaluation*

rés. Pour chacun de ces 16 modes et chacun des quatre critères proposés, un symptôme de défaillance doit être évalué. Aussi, pour un mode, quatre versions de cette grille devront être complétées. Au total, un maximum inatteignable de $16 \times 4 = 64$ grilles pourront être complétées. En effet, certains modes sont exclusifs entre eux. La méthode préconisée pour remplir ces grilles est cependant générique et consiste à répondre à la question suivante : *pour le mode Z et pour le critère X quel est le niveau de gravité du symptôme de défaillance W ?* Pour cela, le concepteur doit également s'appuyer **impérativement** sur les définitions données à la fois pour les critères, les symptômes et les niveaux de gravité.

Au final, le concepteur pourra être amené à compléter dans le pire des cas $4+64 = 68$ grilles.

Une fois ce travail effectué, la phase de projection des symptômes de défaillance sur les transitions du modèle de référence réduit peut être démarrée.

D'un point de vue pratique, une étape de mise en forme des grilles complétée doit être faite. Il s'agit simplement de les représenter sous la forme de matrices comme le montre la figure 3.7 pour la grille de type impacts/traitements. La matrice associée est appelée

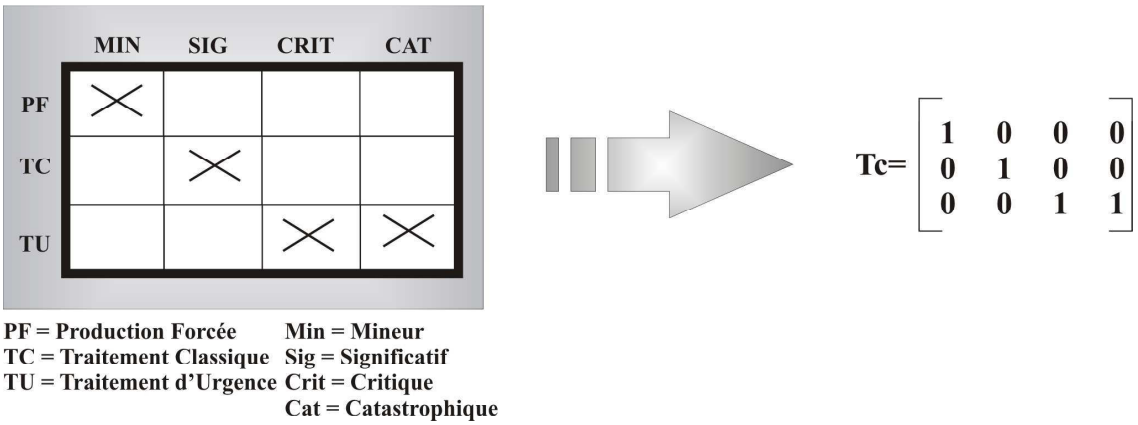

FIG. 3.7: *Exemple de représentation matricielle d'une grille d'évaluation de type impacts/traitements*

T_c, où c représente l'un des quatre critères retenus. Naturellement, les lignes représentent les traitements de défaillances et les colonnes les niveaux de gravité associés.

Le même principe est adopté pour la grille symptômes/impacts. La matrice est ici appelée S_{mc} où m représente l'un des 16 modes de marche et d'arrêt et c le critère évalué. Les lignes de la matrice représentent les niveaux de gravité associés aux symptômes de défaillance (colonnes). La figure 3.8 donne un exemple de ce type de matrice pour un mode de *production normale (F1)* et pour le critère *productivité (p)*. Bien entendu, et

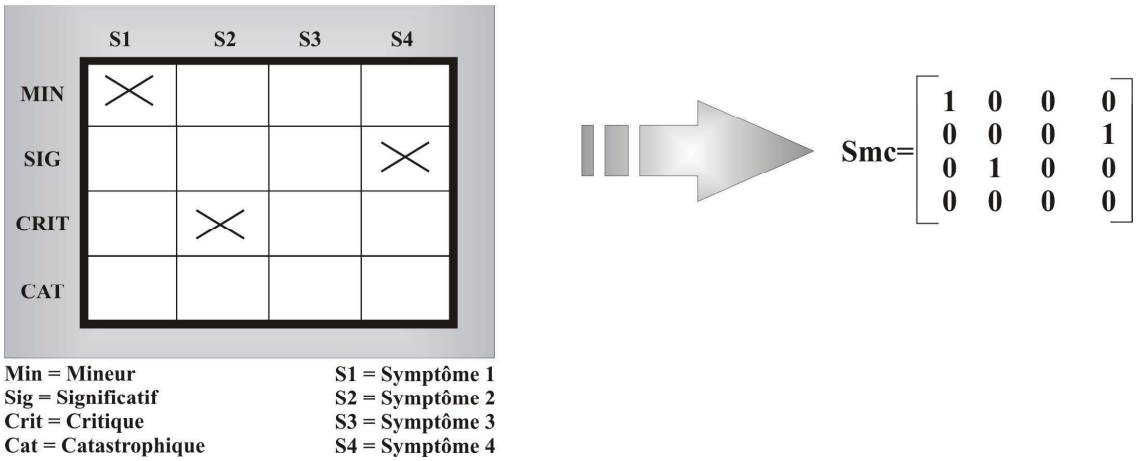

FIG. 3.8: *Exemple de représentation matricielle d'une grille d'évaluation de type symptômes/impacts*

pour des raisons déjà évoquées, si le niveau de gravité associé au symptôme de défaillance est considéré comme *non-significatif* pour le mode et le critère analysé, la colonne associée au symptôme doit rester vide.

La première étape de projection consiste à faire correspondre un symptôme avec le traitement adapté. Cela revient à faire le produit $T_c \times S_{mc}$. Afin de restituer la condition qui doit être portée sur la transition correspondante, une multiplication par le vecteur $C = \begin{pmatrix} S1 \\ S2 \\ S3 \\ S4 \end{pmatrix}$ est requise.

Le vecteur obtenu est nommé TS_{mc} où c représente un des quatre critères et m le mode de marche ou d'arrêt considéré. La figure (3.9) donne un exemple de ce vecteur.

Étant donné que 64 matrices maximum de type S_{mc} peuvent être complétées, 64 vecteurs de type TS_{mc} seront générés. Il est clair qu'une projection des 64 vecteurs obtenus pourrait être envisagée pour instancier les transitions du modèle de référence réduit. Cependant, des conflits peuvent exister entre ces vecteurs ; un conflit est caractérisé ici par le partage d'un même symptôme par plusieurs traitements de défaillance. En effet, un symptôme S1 peut avoir été mis en relation directe avec une production forcée pour un critère *productivité* et un traitement d'urgence pour un critère *sécurité*. Dans le cadre de cette approche et pour des raisons de simplification de la méthode retenue, nous avons opté pour la résolution de ces conflits préalablement à l'instantiation du modèle de référence. Pour faire face à ces conflits, nous proposons un réglage des priorités entre les quatre critères retenus.

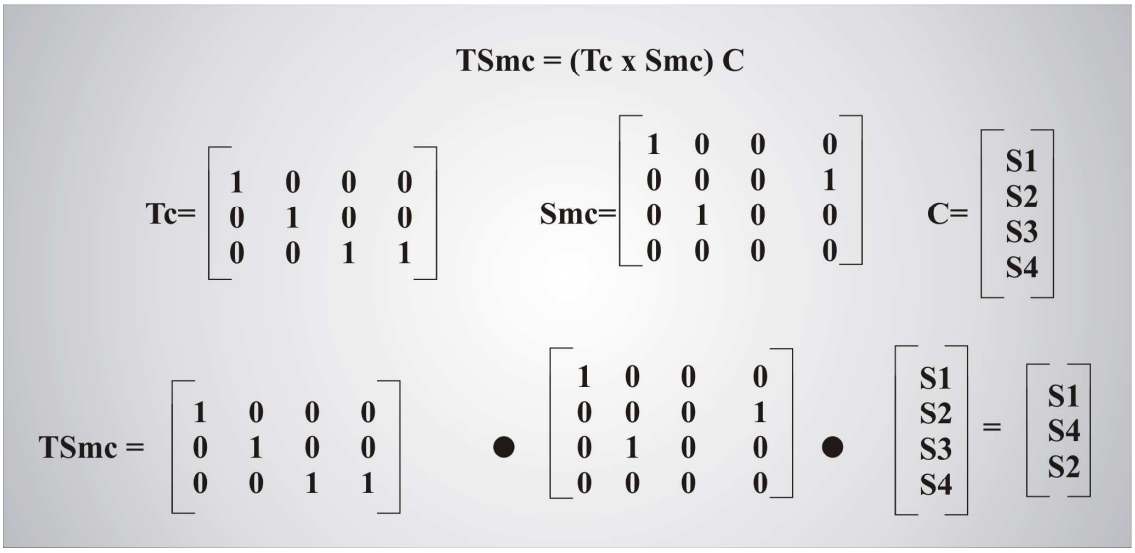

FIG. 3.9: *Vecteur relation symptômes/traitements*

3.5 Synthèse III : réglage des priorités

Nous nous proposons ici de définir une technique permettant pour chaque mode considéré de l'application, de synthétiser un seul vecteur de type TS_{mc} à partir des quatre générés suite à l'application de la synthèse II.

Pour ce faire, nous proposons préalablement au concepteur de régler les niveaux de priorité entre les quatre critères. Cependant, il est difficile de ne pas considérer, et ce quelle que soit l'entreprise visée, que les normes législatives (sécurité et écologie) doivent être plus prioritaires que les besoins internes déclinés sous la forme de productivité et qualité. Pour cette raison, nous proposons deux groupes de critères pour lesquels nous réduisons la liberté du concepteur au réglage des priorités ($<$, $>$ ou $\equiv$) à l'intérieur de ces groupes. Bien entendu, étant donné que nous offrons la possibilité au concepteur, au sein d'un groupe, d'utiliser l'opérateur $\equiv$, des conflits pourront subsister. En effet, il peut tout à fait être envisagé de considérer productivité et qualité comme étant d'importance équivalente. Si tel est le cas, seul le concepteur sera habilité à résoudre ces conflits résiduels.

Le premier groupe, que nous appellerons "Groupe A ($G_{m,A}$)", correspond aux critères de sécurité et d'écologie ; le second, nommée "Groupe B ($G_{m,B}$)" intègre quant à lui les critères de productivité et de qualité.

Ainsi, pour un mode de marche ou d'arrêt considéré, $G_{m,A}$ (respectivement $G_{m,B}$) représente deux vecteurs TS_{mc} où $c \in$ {Sécurité, Écologie} (respectivement $c \in$ {Productivité, Qualité}.

Notons $P_{m,A}$, $P_{m,B}$ et P_m les vecteurs solutions obtenus après prise en compte des priorités fixées dans chacun des groupes.

Notons $niv \in$ {max, min, équi} le niveau de priorité affecté à chacun des vecteurs du groupe A (respectivement B) et $P1_{m,A,niv}$ et $P2_{m,A,niv}$ (respectivement $P1_{m,B,niv}$ et $P2_{m,B,niv}$) ces vecteurs.

Compte tenu, qu'au sein d'un groupe, le concepteur peut rendre un critère plus important que l'autre ($P1_{m,A,max} > P2_{m,A,min}$), ou non ($P1_{m,A,equiv} \equiv P2_{m,A,equiv}$), nous obtenons l'algorithme de synthèse des vecteurs suivant :

Soit $N(P)$ une fonction renvoyant le niveau de priorité (min, max, equiv) du vecteur P.

Soit $F(X,Y)$ une fonction capable d'extraire du vecteur X les éléments de Y.

ALGORITHME

POUR chaque mode "m" de la ressource considérée FAIRE
  POUR g = A $\longrightarrow$ B FAIRE
    DEBUT
      SI $N(P2_{m,g,niv}) > N(P1_{m,g,niv})$ FAIRE $P1_{m,g,niv} = F(P1_{m,g,niv}, P2_{m,g,niv})$
      SINON SI $N(P1_{m,g,niv}) > N(P2_{m,g,niv})$ FAIRE $P2_{m,g,niv} = F(P2_{m,g,niv}, P1_{m,g,niv})$
      $P_{m,g} = P1_{m,g,niv} + P2_{m,g,niv}$
    FIN
  FINPOUR
  $P_{m,B} = F(P_{m,B}, P_{m,A})$ /* groupe A toujours prioritaire sur B */
  $P_m = P_{m,A} + P_{m,B}$
FINPOUR

L'application de cet algorithme pour chacun des modes considérés revient à produire m vecteurs de taille 3×1 mettant en relation symptômes et traitements de défaillances. La ligne 1 du vecteur correspond à la production forcée, la ligne 2 au traitement classique et la ligne 3 au traitement d'urgence.

L'instanciation des transitions conditionnées par l'événement "résultat de détection" du modèle de référence réduit peut alors être envisagée par simples projections des symptômes contenus dans les vecteurs en fonction des traitements cibles. Ces projections sont définies par $P : \delta_n(x,\sigma) \rightarrow x' \cdot P_m$ de la façon suivante :

$$P(\delta(x,\sigma)) = \begin{cases} \delta(x,\sigma) \cdot P_m(1,1) \text{ si } P_m(1,1) \neq 0, x(m) = \text{ mode}, x'(m) = D3 \\ \delta(x,\varepsilon) \text{ si } P_m(1,1) = 0, x(m) = \text{ mode}, x'(m) = D3 \\ \delta(x,\sigma) \cdot P_m(2,1) \text{ si } P_m(2,1) \neq 0, x(m) = \text{ mode}, x'(m) = D2 \\ \delta(x,\varepsilon) \text{ si } P_m(2,1) = 0, x(m) = \text{ mode}, x'(m) = D2 \\ \delta(x,\sigma) \cdot P_m(3,1) \text{ si } P_m(3,1) \neq 0, x(m) = \text{ mode}, x'(m) = D1 \\ \delta(x,\varepsilon) \text{ si } P_m(3,1) = 0, x(m) = \text{ mode}, x'(m) = D1 \end{cases}$$

Le mot vide ε est ici aussi utilisé pour inhiber le déclenchement des traitements de défaillance qui ne sont pas en adéquation avec les critères recherchés.

L'application d'un tel mécanisme de projection permet de synthétiser un nouveau modèle qui respecte désormais les propriétés suivantes : modes de marches et d'arrêts en fonctionnement normal, critères de productivité, qualité, sécurité et écologie et finalement les priorités entre ces critères. Ce modèle est défini par le générateur de langages M' suivant :

$M' = \{X', \Sigma, \delta', x_0, x_m\}$
$M' \subset M$
$X' \subset X$
$\delta' \subset \delta$

L'état initial du générateur de langages est égal à l'état $(< A1, R, Dt, Sv >)$.

Comme nous avons pu le remarquer plus haut, lorsque le concepteur ne fixe pas de priorités au sein d'un groupe de critères, il prend le risque de ne pas résoudre tous les conflits au sein du modèle de référence réduit. Afin de résoudre ces conflits, il est nécessaire de lancer une seconde phase de recherche de conflits structuraux dans le modèle et de demander au concepteur, pour chacun de ces conflits, de les résoudre.

Le modèle obtenu par synthèses successives est désormais déterministe vis à vis des transitions de type "résultat de détection". Cependant, il n'en demeure pas moins qu'il ne peut être qualifié de loi de surveillance. En effet, une loi de surveillance ne correspond pas uniquement à une réduction du modèle de référence. Il s'agit en effet maintenant de fixer des niveaux de tolérance aux défaillances répétitives afin de limiter le nombre de bouclages d'un traitement de défaillance sur lui-même. C'est ce que nous nous proposons de traiter dans le paragraphe suivant.

3.6 Synthèse IV : réglage de la récursivité

Cette quatrième étape de synthèse est la dernière de la liste. Si nous faisons abstraction des autres indéterminismes liés aux autres événements de type "résultat de diagnostic", "résultat de décision", etc., le modèle obtenu suite à cette étape doit correspondre à la loi de surveillance respectant chacune des propriétés recherchées.

Afin de limiter la profondeur d'appel à un même traitement de défaillance, deux étapes doivent être envisagées. En premier lieu, il s'agit de localiser les boucles répétitives contenues dans le modèle de référence réduit. En deuxième lieu, il s'agit de les limiter.

Pour ce faire, nous nous sommes appuyés sur le langage généré par l'automate.

Le langage reconnu par M' est défini par $\Psi(s)$. Il est composé par l'ensemble des traces non nulles qui conduisent à nouveau à l'état initial (égal à l'état marqué). Il est défini par :

$\Psi(s) = \{s \in M' | (x_0, s) \rightarrow x_m, |s| > 0\}$

L'ensemble $\Psi(s)$ est composé de séquences répétitives. Dans cet ensemble, nous pouvons distinguer deux types d'évolutions principales :

- $\Psi(s) = \Psi(s_n) \cup \Psi(s_t)$
- $\Psi(s_n) = \{s \in M' | (x_0, s) \rightarrow x_m, |s| > 0, \theta \notin s\}$
- $\Psi(s_t) = \{s \in M' | (x_0, s) \rightarrow x_m, |s| > 0, \theta \in s\}$

Le premier ensemble caractérise les évolutions qui se déroulent en fonctionnement normal. L'exclusion de l'événement θ indique que nous ne considérons pas dans cet ensemble les séquences qui prennent en compte les dysfonctionnements. Le deuxième ensemble est le complément du premier. Il s'agit des séquences qui représentent les traitements de défaillances et qui conduisent à nouveau vers une des activités appartenant au fonctionnement normal.

Afin de rejeter de toutes les boucles de surveillances tout appel infini au même traitement de défaillance, nous proposons de limiter le nombre de séquences itératives contenues dans $\Psi(s_t)$, hormis celles qui concernent les traitements d'urgence. En effet, limiter l'exécution répétitive d'une séquence d'urgence, c'est prendre le risque de perdre tout ou partie du procédé. En conséquence, nous proposons la procédure suivante :

- soit n le nombre maximum autorisé pour la répétition d'un même traitement de

défaillance. Soit s_i^* une fermeture itérative contenue dans $\Psi(s_t)$ provoqué par l'occurrence d'un nouveau événement θ. Soit $x_i^* = x_1, x_2, ..x_n | x_i \in X'$ l'ensemble d'états visités suite à l'exécution de la séquence s_i.

Les séquences s_i^* sont limités dans le nombre d'exécutions si et seulement si les états visités par la séquence ne sont pas contenus dans le mode des traitements d'urgence (D1). Cette limitation est faite en autorisant l'exécution de ces séquences un nombre maximum n pour ensuite forcer l'application d'un traitement d'urgence. Ce forçage est fait avec l'inclusion d'une nouvelle séquence $s_(i)'$ avec le passage au traitement d'urgence pour qu'il soit appliquée après avoir atteint le nombre maximum d'appels autorisés.

$s_i^* \rightarrow n(s_i) | s_i^* \in \Psi(s_t), D1 \notin x_i^*(m)$
$s_i = s_i' - \theta + \theta' \mid \delta(x_n, \theta) = x', x'(m) = D1$
$\Psi(s_t) = \Psi(s_t) - s_i^* + n(s_i) + s_i'$

3.7 Conclusion

Dans ce chapitre, nous avons présenté notre approche de synthèse de lois de surveillance. La technique proposée est parfaitement générique et donc applicable à toute ressource/produit, à la condition bien entendu de disposer de toutes les fiches techniques les concernant. D'un point de vue utilisation, la technique de synthèse se décline en quatre phases de raffinement du modèle de référence. La première permet au concepteur d'intégrer les propriétés liées aux modes de marches et d'arrêts du fonctionnement normal. Ici, la technique retenue reprend celle proposée déjà par le GEMMA. Une extension est cependant faite afin de pouvoir l'adapter à la classe de modèle que nous utilisons. La deuxième technique permet au concepteur d'injecter dans le modèle quatre critères qui ont des conséquences directes sur le choix des traitements de défaillances qu'il faut déclencher en fonction du type de symptôme détecté. Ces quatre critères représentent à la fois le point de vue de la législation (Sécurité et Écologie) et le point de vue de l'entreprise (Productivité et Qualité). Bien entendu, comme nous avons pu déjà en faire la remarque, d'autres critères peuvent être pris en compte en fonction de l'entreprise considérée. Mais rappelons que l'objectif essentiel de notre approche est de démontrer d'une part la nécessité de synthétiser des lois de surveillance respectant des propriétés, d'autre part d'établir les différentes classes de propriétés de la problématique, et enfin de montrer la faisabilité d'une telle synthèse. Si d'autres propriétés doivent être prises en compte, l'approche générale proposée peut être facilement étendue. La troisième étape de synthèse permet quant à elle de prendre en compte les priorités que doit établir le concepteur au sein de deux groupes de critères. Nous avons en effet volontairement imposé que les critères de Sécurité et d'Écologie soient toujours plus prioritaires que la Productivité et la Qualité. Au sein d'un groupe, nous avons cependant montré les limites d'une telle marge de flexibilité laissée au concepteur. Si ce dernier ne classe pas, par exemple "*je considère que la productivité est aussi importante que la qualité*", des conflits structuraux peuvent alors subsister dans le modèle de référence réduit. La résolution de ces conflits risque alors d'être laborieuse, étant donné que le concepteur aura à les passer tous en revue. Enfin, la quatrième technique permet de contraindre les cycles infinis utilisables dans le modèle de référence réduit. Il est en effet inimaginable d'accepter de traiter indéfiniment de la même façon l'occurrence répétitive d'une même défaillance au cours de l'application d'un seul traitement.

La suite de ce mémoire est entièrement consacrée à une application de notre approche de synthèse de lois de surveillance sur un exemple inspiré d'une installation réelle, la plate-forme de recherche SAPHIR du Laboratoire d'Automatique de Grenoble.

Quatrième partie

Exemple d'application

Chapitre 1

Présentation de la plate-forme de recherche SAPHIR

1.1 Introduction

Dans cette partie, nous avons souhaité développer un exemple d'application de notre approche de synthèse de lois de surveillance sur la base du procédé pilote SAPHIR du Laboratoire d'Automatique de Grenoble. Ce choix nous a semblé judicieux pour plusieurs raisons. Premièrement, cette plate-forme de test et de validation est exclusivement dédiée à la recherche. Deuxièmement, elle est localisée dans le laboratoire où nous avons mené nos travaux de recherche. Elle est donc facilement accessible. Troisièmement, et comme nous allons le voir dans le premier chapitre de cette partie, SAPHIR se prête particulièrement bien à l'étude des défaillances du procédé. Elle met à disposition à la fois des capteurs de surveillance et de commande permettant de valider tout type d'approche de surveillance (surveillance intégrée, séparée ou mixte), elle permet d'illustrer les phénomènes de propagation de défaillances, elle offre un terrain propice à l'étude des stratégies de surveillance en mettant à disposition des ressources physiques hétérogènes. Enfin, sa structure opérationnelle autorise l'étude de différents types d'architectures décisionnelles en partant des architectures purement hiérarchiques jusqu'aux structures entièrement distribuées en passant par les architectures mixtes.

Dans le cadre de ce premier chapitre, nous allons donc plus particulièrement nous intéresser à la présentation de la plate-forme de recherche SAPHIR. Le premier paragraphe s'attachera à donner les caractéristiques techniques essentielles de la plate-forme. Il s'agira notamment d'en présenter le cahier des charges général, la partie opérative, la partie commande et enfin l'architecture opérationnelle retenue dans le cadre de cet exemple d'application. Après quoi, nous présenterons l'adéquation de SAPHIR à l'étude, le test et la validation d'approches de surveillance, commande et supervision.

Remarque : la plupart des informations présentées ici sont extraites des documents Zamaï et al. [2000] et Zamaï [2001]. Pour plus d'informations, le lecteur peut se reporter au site WEB http://www-lag.ensieg.inpg.fr/saphir.

1.2 Caractéristiques techniques

1.2.1 Cahier des charges

D'un point de vue technique, la plate-forme de recherche SAPHIR est dédiée à l'assemblage d'arbres à cames (Figure 1.1). Le magasin rotatif de huit emplacements peut

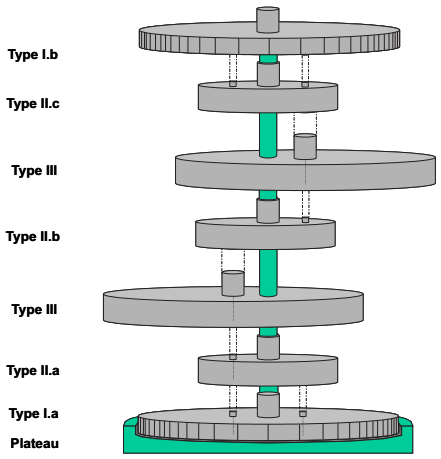

FIG. 1.1: *Exemple d'arbre à câmes*

accueillir six types de pièces différentes. Ces pièces sont identifiées par pesage. Suite à cette identification, elles sont dirigées vers un portique de tri via un convoyeur central. Selon le type de pièce identifié, le portique oriente la pièce vers les convoyeurs gauche ou droit qui font également office de stocks intermédiaires. En sortie de ces deux convoyeurs, deux postes de positionnement permettent d'indexer les pièces afin que le robot manipulateur puisse les prendre convenablement. Ce dernier peut réaliser en parallèle huit arbres à cames par superposition des pièces. Un opérateur humain est chargé d'approvisionner le magasin de pièces ; un autre doit vider le poste d'assemblage rotatif. Enfin, une caméra sert à la surveillance à distance du procédé.

1.2.2 La partie opérative

La partie opérative de SAPHIR est constituée de huit éléments (Figure 1.2). Chacun de ces éléments est détaillé dans les paragraphes suivants.

1.2.2.1 Le magasin rotatif

Le magasin de pièces est réalisé sur la base d'un plateau de 300mm de diamètre. Chacun des huit emplacements peut accueillir indifféremment tous les types de pièces (Figure 1.1) grâce aux deux gabarits, l'un de largeur 33mm, l'autre de 66mm. D'un point de vue motorisation, un moteur pas à pas 100/200 pas par tour assure la mise en rotation du magasin via une démultiplication par courroie crantée de rapport 6,6. Une précision de positionnement de 0,7mm est ainsi atteinte. Un capteur inductif assure l'indexation du plateau, et un capteur à réflexion permet de détecter la présence de pièce sur les emplacements prévus à cet effet. Un vérin pneumatique double effet doté de deux capteurs magnétiques assure la poussée des pièces sur le poste de pesée.

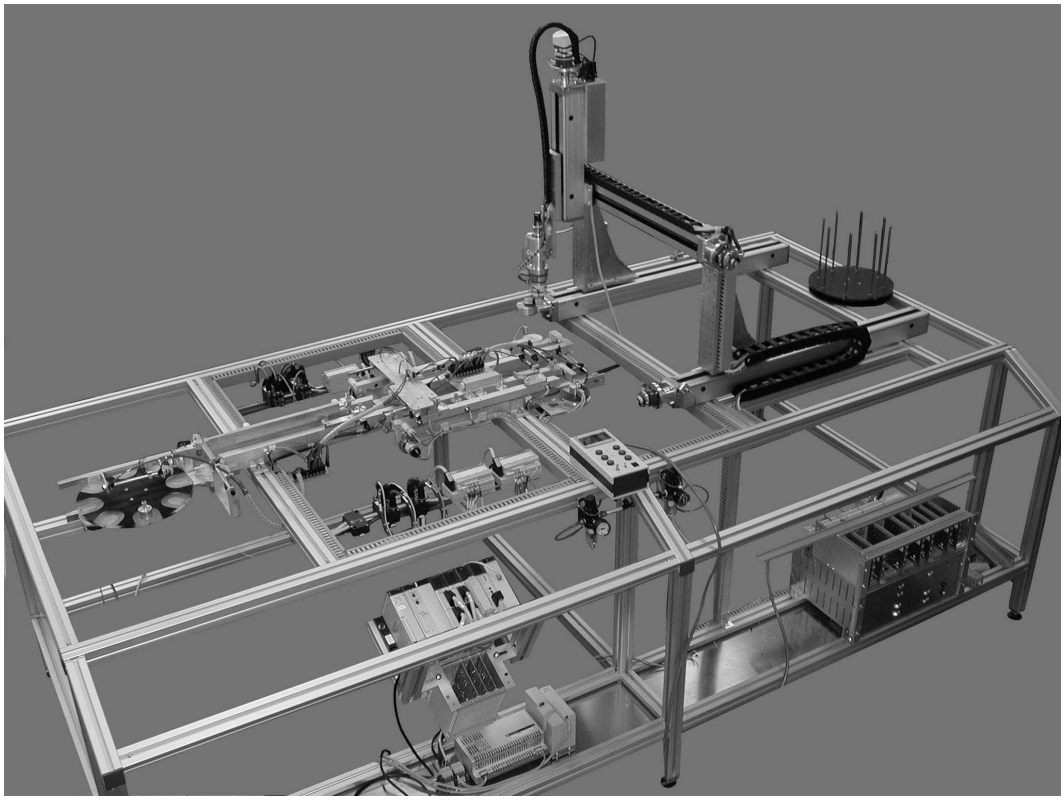

FIG. 1.2: *Partie opérative de la plate-forme SAPHIR*

1.2.2.2 Le poste de pesée

Le poste de pesée est constitué d'une jauge de contrainte permettant la pesée de pièces allant de 20g à 5Kg. Afin d'assurer la poussée de la pièce pesée sur le convoyeur central, un vérin pneumatique double effet équipé de deux capteurs magnétiques a été mis à disposition.

1.2.2.3 Le système de manutention

Le système de manutention est constitué de trois convoyeurs à bande (un central, deux latéraux). Une courroie crantée industrielle de longueur 65cm assure le convoyage des pièces. Elle est entraînée par un moteur à courant continu équipé d'un réducteur. Ce moteur est commandé via une carte de commande autorisant à la fois des changements de sens de rotation mais également des modifications de la vitesse de rotation. La vitesse max a été fixée à 10cm/s. De plus, cette carte interdit tout changement de sens de rotation sans passer par une vitesse nulle ; ceci afin de préserver les engrenages du réducteur. D'un point de vue capture d'informations, quatre capteurs ont été requis. Le premier atteste de la présence d'une pièce en entrée des convoyeurs. Le deuxième témoigne d'une saturation du système de convoyage. Le troisième permet de détecter la présence d'une pièce en face de l'ancrage limitant ainsi le nombre de pièces en phase de tri ou de positionnement. Le dernier capteur indique la présence d'une pièce en fin de convoyage. Les ancrages sont quant à eux réalisés au moyen de vérins simples effets. Afin de détecter les pièces qui doivent être rebutées, deux capteurs photo-barrages ont été placés sur les convoyeurs latéraux.

1.2.2.4 Le poste de tri

Le portique a été réalisé autour d'un dispositif de trois vérins pneumatiques double effets. Deux de ces vérins sont dédiés à l'évacuation des pièces soit sur le convoyeur de droite soit sur celui de gauche, le dernier est chargé de positionner les deux autres devant la pièce à évacuer. L'ensemble est fixé sur un plateau monté sur paliers autorisant des déplacements longitudinaux sans frottement.

1.2.2.5 Les postes de positionnement

Le même dispositif réalisé pour le magasin rotatif a été retenu. Un capteur inductif permet de positionner correctement le poste de positionnement en sortie des convoyeurs latéraux, un autre de détecter la présence d'une pièce à positionner, un troisième de positionner correctement la pièce avec un angle de prise connu pour le robot d'assemblage.

1.2.2.6 Le robot d'assemblage

Ce robot (Figure 1.3) est basé sur une structure axes vis à bille de type positionneurs à guidage linéaire. Chacun des quatre axes a été équipé d'un moteur pas à pas (100/200 pas

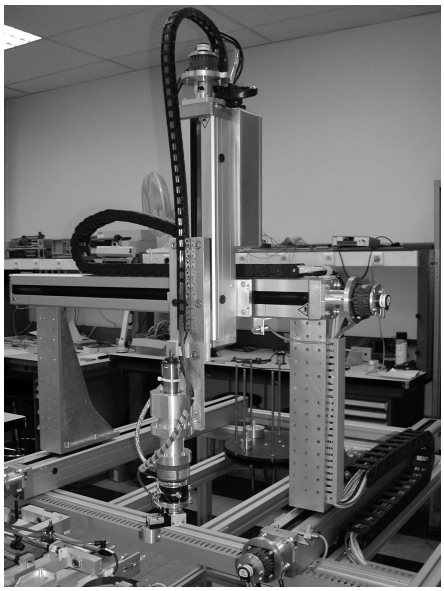

FIG. 1.3: *Le robot d'assemblage*

par tour). Compte tenu de la démultiplication inhérente à la vis à bille (1 tour correspond à un déplacement de 5mm) et de la configuration du moteur en 200 pas par tour, une précision de 0,025mm peut être atteinte. Chacun des moteurs est équipé d'un codeur incrémental 200 pas par tour afin de s'assurer de leur bon fonctionnement (essentiellement surveillance de la synchronisation des axes X1 et X2). Afin d'éviter toute sur-course, chaque axe est équipé de part et d'autre de capteurs secs TOR. Ces capteurs sont sérialisés et entraînent une coupure matérielle de la consigne des moteurs. En ce qui concerne le degré de liberté R, un moteur à courant continu équipé d'un réducteur planétaire à jeu limité a été sélectionné afin de garantir précision, stabilité et couple. Ce moteur est également équipé d'un codeur absolu 12 bits afin d'assurer son asservissement de position via une carte d'asservissement. Afin de réduire le câblage qui doit être ramené vers le PC de pilotage du Robot (i.e. 12 fils ne serait-ce que pour le codeur absolu), un dispositif

basé sur un micro-contrôleur 89C52 chargé de sérialiser les 12 bits renvoyés par le codeur absolu est implanté. L'outil associé au moteur à courant continu assure la prise des cames et entretoises. Il s'agit d'une pince (Figure 1.4) asymétrique compliante offrant à la fois les services de prise, de palpage pour des tests de qualité mais également la détection de collision ou de problème d'insertion. Le dispositif de fermeture et d'ouverture des mors de la pince est assuré par un vérin pneumatique rotatif double effet. Ce vérin est fixé sur

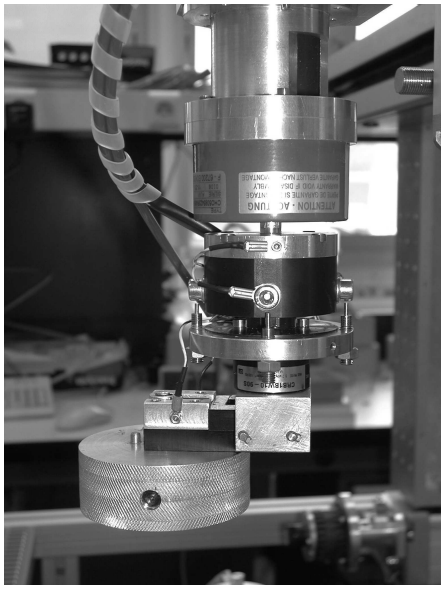

FIG. 1.4: *Détails de la pince*

un socle qui accueille en périphérie les quatre détecteurs de compliance, et au centre le capteur de sécurité prévu en cas de choc violent. Ce socle est monté sur quatre cylinblocs caoutchouc qui lui donnent la compliance requise.

1.2.2.7 Le poste d'assemblage

Cette partie opérative est la copie du magasin de pièces (Figure 1.1, page 126). Pour cette raison, nous ne la détaillerons pas à nouveau ici.

1.2.2.8 Le poste de video surveillance

Le poste de vidéo surveillance est basé sur l'exploitation d'une caméra vidéo haute résolution commandable en zoom, en mouvements horizontaux et verticaux via une liaison série.

1.2.3 La partie commande

La commande locale de ce procédé pilote est répartie sur quatre postes : le magasin rotatif et le système de pesée, les systèmes de convoyage, de tri et de positionnement, le robot et le poste d'assemblage, et enfin la caméra de vidéo surveillance. Ils sont chacun commandés par un PC équipé du noyau multi-tâches temps réel VxWorks, le système de convoyage, de tri et de positionnement par un automate programmable de type TSX PREMIUM, et la caméra par une architecture de type PC équipée du noyau LINUX. Le détail de chacun de ces quatre nœuds de commande locale est donné ci-après.

1.2.3.1 Commande : magasin et pesée

Ce nœud de commande est supporté par un PC Pentium I. Afin de le connecter avec le procédé qu'il doit commander, une carte d'acquisition analogique lui a été insérée. En sus de l'acquisition du signal analogique issu de la jauge de contrainte, cette dernière met également à disposition seize entrées et sorties TOR permettant la commande des deux vérins en fonction des signaux émis par les quatre capteurs magnétiques. Une carte de communication 3COM/Etherlink III permet la communication Ethernet/TCP-IP avec les autres nœuds de commande de l'architecture.

1.2.3.2 Commande : convoyeurs, tri et positionnement

Ce nœud de commande est supporté dans un automate programmable de dernière génération. Il a la charge de s'interfacer avec 26 capteurs TOR (inductifs et photo-barrages), 15 électro-vannes TOR (pré-actionneurs des vérins), 3 cartes de commandes des moteurs à courant continu (0-10V), et 2 cartes de commande des moteurs pas à pas. De plus, comme tout autre nœud de commande locale, il doit pouvoir communiquer avec le reste de l'architecture via le réseau Ethernet sur le protocole TCP-IP. Pour toutes ces raisons, l'automate a été enrichi de cinq cartes coupleurs capable de gérer 64 E/S TOR, 4 sorties analogiques, un bus de terrain ASI, et la communication Ethernet/TCP-IP.

1.2.3.3 Commande : robot et poste assemblage

Ce nœud est abrité par un PC Pentium III. Il a la charge de s'interfacer avec 3 cartes de commande des moteurs pas à pas (réglage de la direction, de l'activation et de la vitesse des moteurs X1/X2, Y et Z) soit 9 sorties TOR, la consigne d'angle à destination de la carte d'asservissement du moteur à courant continu assurant la rotation de la pince, soit 1 sortie analogique, 1 vérin rotatif double effet (ouverture pince, fermeture pince) soit 2 sorties TOR, 1 carte de commande du moteur pas à pas du poste d'assemblage, soit une sortie TOR (activation/désactivation), 27 entrées TOR (4 capteurs de référence, 8 capteurs de sur-course d'axes, 1 capteur de détection de choc violent de la pince, 4 capteurs de compliance, 4 codeurs incrémentaux donnant sens et pas soit 8 entrées TOR, 1 bouton Auto/Manu, 1 capteur de positionnement du plateau d'assemblage), 1 entrée liaison série pour acquérir la position angulaire de la pince. Dans ce but, le PC a été enrichi de 4 cartes de couplage capables de gérer 32 E/S TOR, 12 compteurs, 1 sortie analogique et la communication Ethernet/TCP-IP.

1.2.3.4 Commande caméra de vidéo surveillance

Ce nœud est mis en œuvre sur la base d'une architecture de type PC 486. Il s'interface avec une liaison série pour la commande des mouvements de la caméra, une entrée vidéo pour l'acquisition du signal vidéo renvoyée par la caméra, le réseau Ethernet/TCP-IP pour communiquer avec le reste de l'architecture.

1.3 Architecture opérationnelle

D'un point de vue architecture opérationnelle, les quatre nœuds de commande communiquent par une liaison Ethernet-TCP/IP. Dans une configuration de pilotage hiérarchisée,

ils sont connectés à deux PC de coordination via le même type de réseau. Enfin, un niveau trois de commande assure la connexion entre l'ordonnancement et le pilotage temps réel (Figure 1.5). Dans une configuration distribuée, ces quatres éléments peuvent être direc-

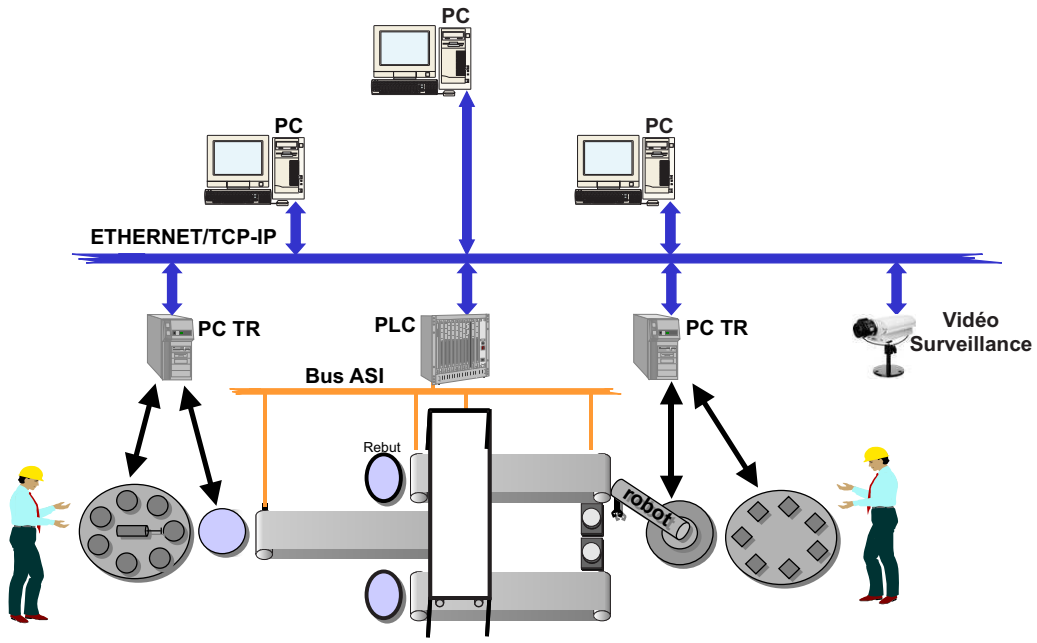

FIG. 1.5: *Architecture opérationnelle de la plate-forme SAPHIR*

tement connectés entre eux via le réseau Ethernet. Dans le cadre de notre étude, nous avons retenu la solution de pilotage hiérarchisé (Zamaï et al. [1997]).

1.4 Adéquation à l'étude de la surveillance et de la supervision

Avant d'évaluer notre approche de synthèse de lois de surveillance, il est nécessaire de s'assurer que la plate-forme SAPHIR se prête bien à l'étude de défaillances du procédé. Pour ce faire, nous nous proposons de mener une analyse des défaillances détectables sur ce procédé. Bien entendu, il n'est pas question d'en dresser une liste exhaustive, le procédé est trop complexe (nombre d'entrées/sorties trop important) pour cela.

Le problème de la surveillance temps réel auquel nous allons nous intéresser ici est celui de la surveillance des défaillances du procédé. Une défaillance du procédé est caractérisée par une évolution du système commandé qui diffère de l'évolution spécifiée (consigne). Analysons au travers d'exemples simples les trois cas de figure pouvant se présenter :

1. le capteur de type jauge de contrainte dont les connexions sont endommagées ne transmettra généralement plus une mesure correcte correspondant au poids réel de la pièce pesée. Un défaut de cette nature pourra alors provoquer des "qui pro quo" des pièces mal identifiées,

2. un jeu anormal au niveau des planétaires d'un réducteur associé à un moteur asservi en position peut conduire à une instabilité du système,

3. l'absence de pièces dans le magasin d'entrée ou dans le stock intermédiaire à disposition du robot provoquera immanquablement le blocage de l'un de ces postes.

Par extension, ces trois cas de figure peuvent s'appliquer à tous les capteurs de commande, actionneurs, pré-actionneurs et stocks de SAPHIR.

De plus, en sus des capteurs de commande, SAPHIR a été doté de capteurs de surveillance dédiés à la surveillance des parties opératives dites sensibles telles que le robot. Ces capteurs (sur-course axes, compliance pince) n'ont aucune utilité pour la commande mais permettent de satisfaire les règles de sécurité de base pour la préservation du matériel et des opérateurs humains.

Enfin, afin de mettre en évidence la problématique classique de la propagation de défaillances (Chaillet-Subias et al. [1997]), une erreur de conception mécanique a été volontairement introduite au niveau du convoyeur central. En effet, ce dernier offre une largeur de bande de convoyage exactement égale à deux fois la largeur d'une entretoise. Ainsi, et ce de manière parfaitement aléatoire, deux entretoises peuvent se doubler en amont de l'ancrage pièces. En bout de chaîne, le robot peut être amené à assembler une mauvaise pièce.

Remarque : tous les vérins simple effet sont utilisés à des fins d'ancrage. Les pièces viennent donc buter contre ces vérins forçant ainsi sur leur axe en risquant de les tordre ou bien de comprimer exagérément leur joint torique. Le MTBF de ces vérins sera donc sérieusement réduit.

En tout état de cause, SAPHIR se prête bien à l'étude de la surveillance, de la commande et de la supervision.

1.5 Conclusion

Dans ce chapitre nous avons présenté la plate-forme de recherche SAPHIR du Laboratoire d'Automatique de Grenoble sur laquelle nous allons évaluer notre technique de synthèse de lois de surveillance. Afin de mieux préparer la phase de recherche de propriétés dédiées à SAPHIR, nous avons détaillé ses caractéristiques techniques à la fois d'un point de vue procédé et commande. Nous avons ensuite présenté son architecture décisionnelle. Enfin, nous avons mené une étude de l'adéquation de SAPHIR à nos besoins, la surveillance et la supervision des défaillances du procédé.

Compte tenu de la complexité de l'ensemble du procédé SAPHIR et de l'objectif visé, la validation de notre approche, nous n'envisageons pas dans le cadre de ce mémoire de l'appliquer sur tout le procédé ; seule une partie opérative sera sélectionnée pour la démonstration. Étant donné la richesse offerte par le robot d'assemblage, à la fois en terme de défaillances, de normes de sécurité, de capacité de test de qualité d'assemblages (capteurs de palpage), nous nous proposons de nous appuyer sur cet élément pour valider notre approche. C'est ce que nous nous proposons de faire dans les deux chapitres suivants.

Chapitre 2

Propriétés recherchées

2.1 Introduction

Dans le cadre de ce chapitre, nous nous proposons de rédiger le cahier des charges pour la synthèse d'une loi de surveillance dédiée à la commande, surveillance et supervision du robot CHARLY de la plate-forme SAPHIR. Dans cet objectif, nous allons donc naturellement structurer ce cahier des charges autour des sept propriétés proposées dans la partie III de notre mémoire.

2.2 Modes de marches et d'arrêts

En sus des modes incontournables A1 (arrêt initial) et F1 (production normale), il est nécessaire de retenir le mode F2 (marche de préparation). Ceci s'explique simplement compte tenu de l'instrumentation des axes du robot. Les moteurs pas à pas étant munis de codeurs incrémentaux, ils ne renvoient pas une image absolue de la position du moteur. Une phase d'initialisation avant production normale est donc nécessaire pour faire le "HOME" du robot.

L'ensemble des modes de marches et d'arrêts que nous recherchons en fonctionnement normal se limite donc ici à : A1, F1 et F2 avec les commutations $A1 \rightarrowtail F2 \rightarrowtail F1 \rightarrowtail A1$ (cf. Figure 2.1).

2.3 Réglage des quatre critères

Dans le cadre de notre exemple d'application, et en prenant en compte que nous considérons seulement trois modes pour le fonctionnement normal, le nombre de grilles que nous devons remplir est de 40 : 4 grilles de type impacts/traitements + $(9 * 4) = 36$ grilles de type symptômes/impacts.

Afin de ne pas alourdir ce paragraphe, nous ne présenterons ici dans le détail que la spécification des quatre grilles impacts/traitements et des quatre grilles symptômes/impacts affectées au mode de production normale ($F1$). Les 28 autres grilles peuvent être consultées en Annexe 3.

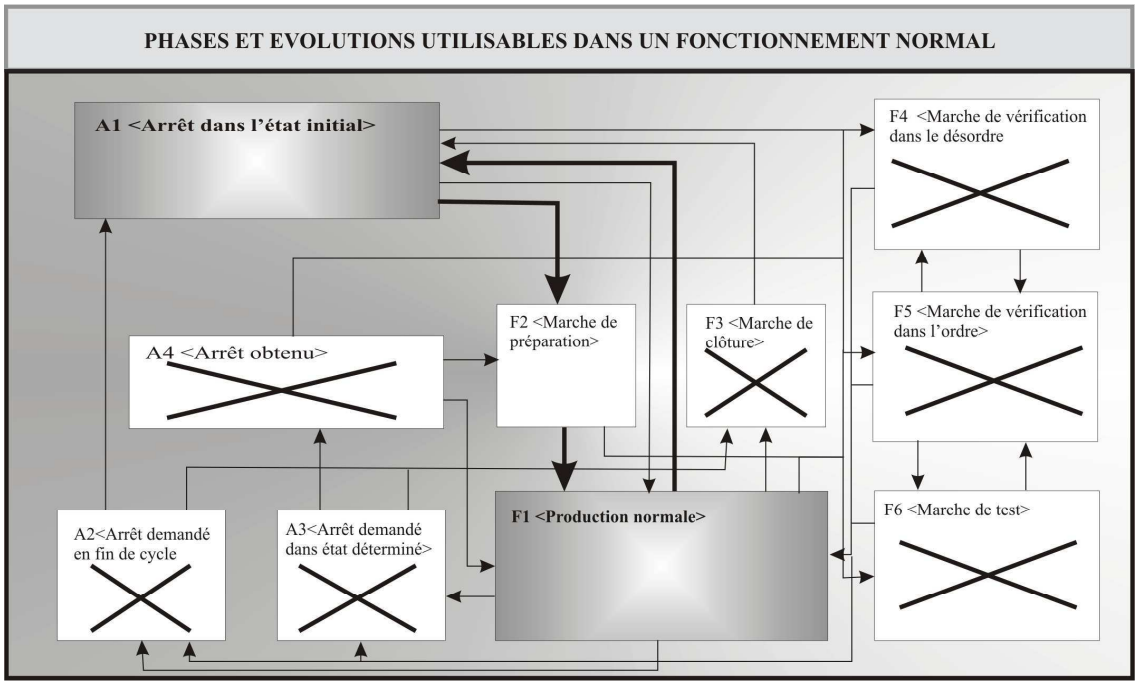

FIG. 2.1: *Les modes gardés pour le robot Charly*

2.4 Normes législatives

Dans le cadre de ce paragraphe nous allons nous intéresser à la spécification des propriétés législatives (sécurité et écologie) qui doivent être recherchées.

2.4.1 Grilles impacts/traitements

2.4.1.1 Sécurité

Les normes AFNOR dictées pour ce type de ressource (robot) en matière de sécurité imposent le déclenchement de procédures d'urgence en présence de défaillances au moins significatives afin de garantir l'intégrité du personnel et des machines AFNOR [1995a]. Pour un symptôme de défaillance mineur, nous imposons le déclenchement d'un traitement

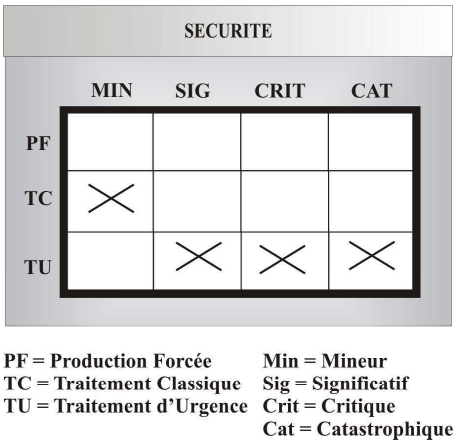

FIG. 2.2: *Sécurité: grille d'évaluation impacts/traitements*

classique. Pour ce type de matériel, une production forcée ne peut en effet qu'être rejetée

(cf. Figure 2.2).

2.4.1.2 Écologie

L'écologie n'ayant aucun écho au niveau de la plate-forme SAPHIR, tout symptôme de défaillance sera considéré ici comme non-significatif. Aucun traitement de défaillance ne devra être déclenché du point de vue de ce critère (cf. Figure 2.3).

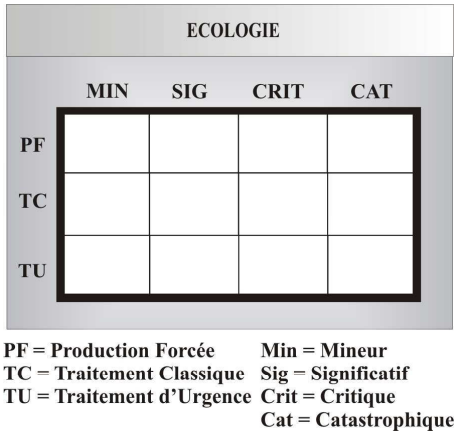

FIG. 2.3: *Écologie : grille d'évaluation impacts/traitements*

2.4.2 Grilles symptômes/impacts

2.4.2.1 Sécurité

Dans la phase de production normale, nous pouvons considérer l'occurrence d'un symptôme 1 comme mineur. En effet, ce symptôme indique uniquement une transgression d'une contrainte de commande et non une contrainte physique. En revanche, dans le cas de l'occurrence d'un symptôme 2, nous pouvons être assuré de la transgression d'une contrainte physique du procédé. Pour cette raison, ce symptôme sera considéré comme critique sur le plan de la sécurité. En ce qui concerne l'évaluation des symptômes temporels 2 et 3, une analyse plus fine de l'interfaçage du système de commande du robot avec ses capteurs/actionneurs est requise. La commande des moteurs pas à pas des axes X, Y et Z consiste à activer leurs cartes de commande respectives et à charger le nombre de pas correspondant au déplacement désiré au sein d'un des registres de la carte compteur ; le codeur incrémental associé au moteur pas à pas est connecté bien entendu à la carte compteur. Si, pour des raisons diverses, comme par exemple la défaillance du circuit anti-rebond de la carte compteur, ou plus simplement du codeur lui-même (axe de rotation tordu), davantage de signaux sont pris en compte par la carte compteur, cette dernière risque donc plus rapidement que prévu de générer un compte rendu de fin de commande. Ceci est caractéristique d'un symptôme 3. Dans ce cas précis, ce type de symptôme traduit forcément la perte totale ou partielle de la localisation précise de l'axe correspondant. Ceci est donc caractérisé d'un point de vue sécurité comme critique. Le symptôme 4, qui caractérise l'absence totale de réponse dans le temps prévu, peut quant à lui traduire des blocages éventuels des axes, des pannes de capteur, etc. Compte tenu des conséquences immédiates de ce type de symptôme, nous considérerons aussi l'occurrence de S4 comme critique (cf. Figure 2.4).

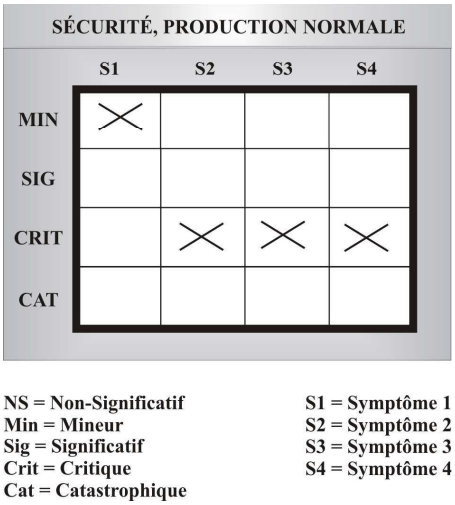

FIG. 2.4: *F1, Sécurité : grille d'évaluation symptômes/impacts*

2.4.2.2 Écologie

Pour les mêmes raisons que celles évoquées plus haut, cette évaluation ne se prête pas au procédé considéré (cf. Figure 2.5).

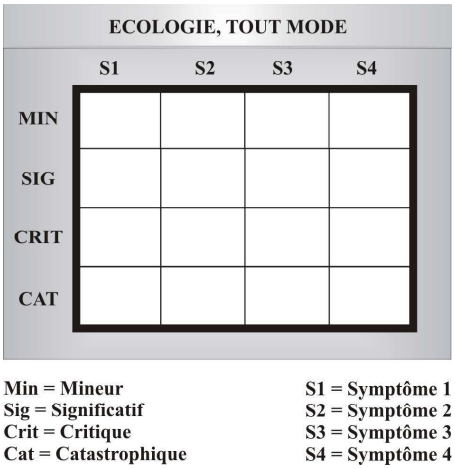

FIG. 2.5: *F1, Écologie : grille d'évaluation symptômes/impacts*

2.5 Besoins internes

Dans le cadre de ce paragraphe nous allons nous intéresser à la spécification des propriétés internes que nous souhaitons intégrer (productivité et qualité).

2.5.1 Grilles impacts/traitements

2.5.1.1 Productivité

La difficulté ici est de fixer la limite à partir de laquelle nous pouvons considérer que la productivité du robot est remise en cause. Compte tenu des définitions données

pour chacun des niveaux de gravité, nous considérons ici atteindre cette limite pour un symptôme de défaillance jugé catastrophique. Pour tout autre impact (mineur, significatif ou critique), nous souhaitons maintenir une production forcée (cf. Figure 2.6).

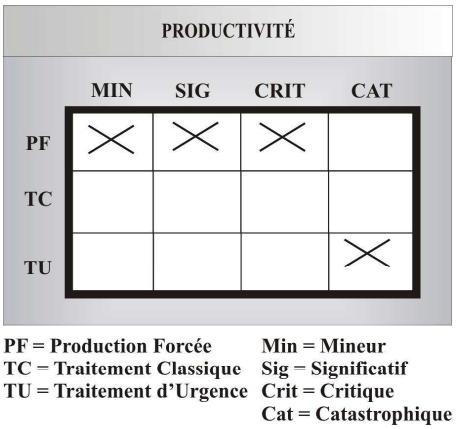

FIG. 2.6: *Productivité : grille d'évaluation impacts/traitements*

2.5.1.2 Qualité

Comme nous avons pu le constater au niveau de la définition associée à ce critère, garantir un niveau de qualité revient à respecter trois principes : "ce qu'ils voulaient, quand ils le voulaient, au prix convenu". Dans le cadre de cet exemple, nous restreindrons la qualité aux deux premiers principes. Nous proposons donc dans ce cas la grille d'évaluation de la figure 2.7.

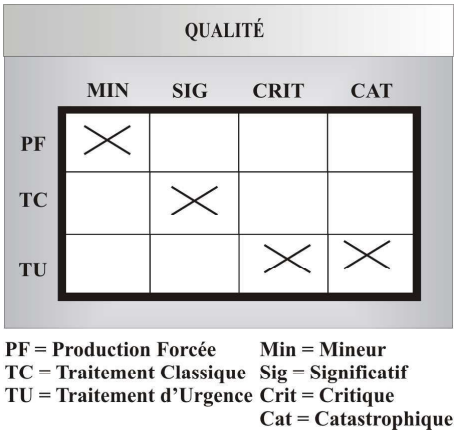

FIG. 2.7: *Qualité : grille d'évaluation impacts/traitements*

2.5.2 Grilles symptômes/impacts

2.5.2.1 Productivité

Bien qu'un symptôme S1 caractérise un blocage du système de commande, il n'en demeure pas moins qu'il indique également que le procédé est toujours dans un état utilisable. Aussi, même s'il a des conséquences directement à court terme sur la productivité, il témoigne également de la possibilité de reprendre la production assez simplement

connaissant l'état réel du procédé. Nous considérons pour cette raison que le symptôme S1 est mineur. En revanche, un symptôme S2 caractérisant une transgression physique du procédé, la productivité est remise en cause, non seulement à court terme mais probable-

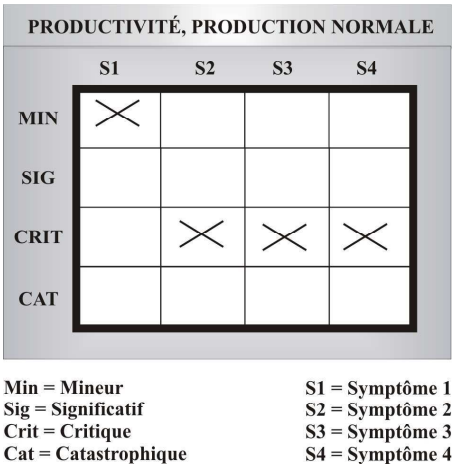

FIG. 2.8: *F1, Productivité : grille d'évaluation symptômes/impacts*

ment à moyen voire même long terme. Une intervention manuelle devra sans doute être envisagée. Compte tenu de ce constat, nous évaluons ce symptôme comme critique. Les symptôme 3 et 4 seront également considérés comme critiques pour les mêmes raisons. Une intervention manuelle devra sans doute être envisagée pour contrôler l'état des cartes compteurs, des codeurs incrémentaux, etc. Ceci occasionnera donc des pertes importantes en terme de productivité (cf. Figure 2.8).

2.5.2.2 Qualité

Même si un symptôme 1 ne met pas directement en cause la qualité d'un assemblage (emboîtement juste des cames et entretoises), il n'en demeure pas moins qu'il remet forcément un minimum en cause les délais de livraisons. Pour cette raison, nous le considérerons comme mineur. Tous les autres symptômes seront évalués comme critique (cf. Figure 2.9).

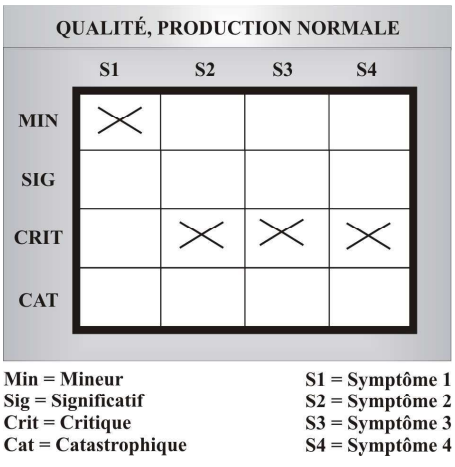

FIG. 2.9: *F1, Qualité : grille d'évaluation symptômes/impacts*

2.6 Priorités

Tout d'abord, la méthode impose une priorité entre les critères législatifs et internes. Il reste donc à définir les priorités d'une part entre la sécurité et l'écologie et d'autre part entre la productivité et la qualité. Or, les risques écologiques sont inexistants pour notre procédé. Nous avons donc donné par défaut la plus haute priorité à la sécurité. Enfin, nous avons choisi de privilégier la productivité vis à vis de la qualité.

2.7 Récursivité

Il s'agit ici de déterminer le nombre maximal de traitements de défaillance consécutifs acceptable. Dans le cadre des fonctionnalités offertes par le robot (assemblage d'arbres à cames), la majorité des défaillances qui peuvent être détectées proviendrons d'une incapacité à assembler les cames et/ou les entretoise sur l'axe d'assemblage. Ce problème peut avoir trois origines : axe d'assemblage tordu, mauvaise coordonnées de prise et/ou de pose (mauvaise phase d'apprentissage), erreur de pesée. Dans tous les cas, nous estimons que détecter consécutivement trois fois le même symptôme de défaillance au cours de l'application d'un seul traitement de défaillances doit conduire à un changement de tactique.

2.8 Conclusion

Dans ce chapitre, nous avons rédigé le cahier des charges pour la synthèse de la loi de surveillance adaptée à la ressource CHARLY de la plate-forme SAPHIR. Pour ce faire, nous nous sommes appuyés sur le canevas proposé dans le chapitre 2 de la partie III. Ainsi, nous avons caractérisé l'espace des modes de marches et d'arrêts appartenant au fonctionnement normal, nous avons ensuite réglé l'ensemble des quatre critères retenus sur la base de 40 grilles d'évaluation, nous avons ensuite fixé les priorités entre les critères de productivité et de qualité d'une part et entre les critères de sécurité et d'écologie d'autre part. Nous avons enfin terminé ce chapitre par la détermination du niveau de récursivité acceptable en présence de défaillances répétitives.

Le chapitre suivant est entièrement dédié à l'application de notre démarche de synthèse sur la base du cahier des charges que nous venons d'établir.

Chapitre 3

Synthèse de la loi de surveillance

3.1 Introduction

Dans le cadre de ce dernier chapitre, nous nous proposons d'appliquer la technique de synthèse détaillée dans la partie III de notre mémoire. Cette dernière va être mise en œuvre sur la base du cahier des charges proposé au le chapitre précédent.

Dans cet objectif, nous avons structuré ce chapitre autour de trois paragraphes. Compte tenu de la taille du modèle de référence qu'il faut manipuler, et afin d'alléger la présentation des résultats, le premier paragraphe pose des hypothèses de travail permettant de réduire la taille du modèle à manipuler. Le deuxième paragraphe s'attache quant à lui à appliquer point par point la technique de synthèse progressive que nous avons développée. Le dernier paragraphe est dédié à la vérification de l'adéquation du modèle de surveillance obtenu par rapport au cahier des charges fixé.

3.2 Hypothèses de travail

La représentation graphique complète du modèle de référence modélisé par un automate de 98 états et 1171 transitions n'est bien entendu pas envisageable dans le cadre de ce mémoire. Pour cette raison, et en veillant à ne pas altérer la démonstration par l'exemple, nous baserons notre application uniquement sur un extrait du modèle de référence.

Ce modèle (Figure 3.1) représente un sous-ensemble d'états et de transitions du modèle de référence complet.

L'ensemble des modes retenu pour la présentation de l'exemple d'application sont :

- $A1$ = Arrêt initial
- $F1$ = Fonctionnement normal
- $F2$ = Marche de préparation
- $F3$ = Marche de clôture
- $F5$ = Marche de vérification dans l'ordre
- $D1$ = Arrêt d'urgence

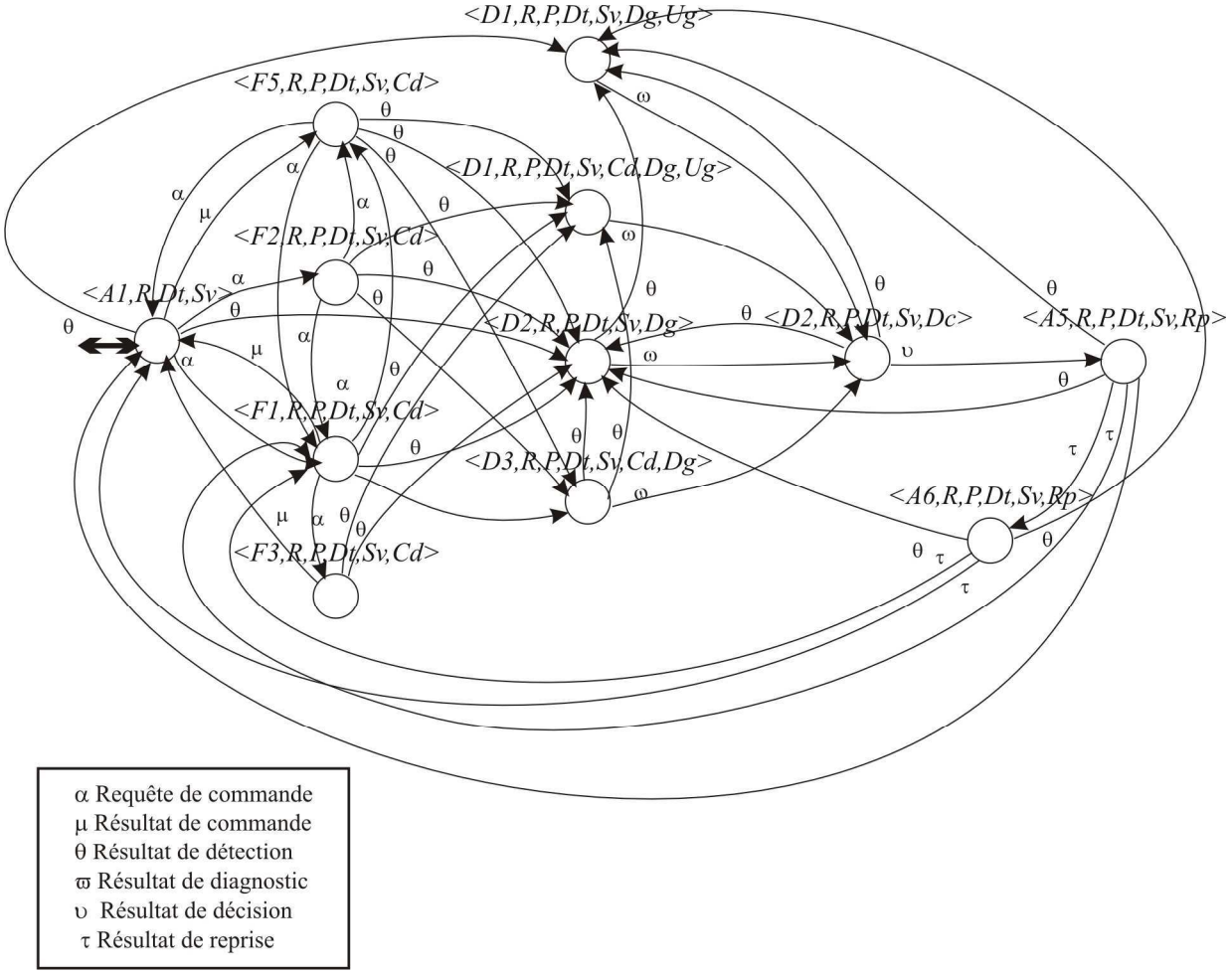

FIG. 3.1: *Extrait du Modèle de référence.*

- $D2$ = Diagnostic et/ou traitement de défaillances
- $D3$ = Production tout de même
- $A5$ = Préparation pour remise en route après défaillance
- $A6$ = Mise P.O. dans l'état initial

tel que :

$Mn = \{A1, F1, F2, F3, F5\}$
$Mt = \{D1, D2, D3; A5, A6\}$

L'extrait du modèle de référence que nous allons utiliser est ainsi défini par :

$Mr = \{X, \Sigma, \delta, x_0, x_m\}$

X représente l'ensemble des activités de l'extrait du modèle de référence et est structuré autour des deux sous-ensembles Xn et Xt. Le premier sous-ensemble représente les états utilisables associés aux modes du fonctionnement normal Mn ; le deuxième aux modes caractérisant un traitement de défaillance Mt. Σ représente l'ensemble des événements qui peuvent se produire au cours d'un fonctionnement normal. δ caractérise la fonction de transition, x_0 l'état initial et x_m l'état marqué.

Le modèle de référence volontairement réduit pour les besoins de l'exemple ayant été présenté, nous nous proposons maintenant d'appliquer notre démarche de synthèse.

3.3 Synthèse

Conformément à la technique de synthèse progressive proposée dans le chapitre 3 de la partie IV, nous allons progressivement raffiner le modèle de référence réduit en y intégrant successivement les quatre ensembles de propriétés qu'il faut au moins rechercher pour générer une loi de surveillance. A chacun de ces ensembles vont être appliqués les quatre techniques de synthèse appropriées.

3.3.1 Synthèse I

L'objectif de la synthèse I est de rejeter au sein du modèle de référence l'ensemble des activités et transitions qui ne correspondent pas au cahier des charges délimitant le contexte du fonctionnement normal du robot CHARLY. Ce cahier des charges établi dans le chapitre précédent stipule d'une part que seuls les modes A1 (arrêt dans l'état initial), F1 (Fonctionnement normal) et F2 (marche de préparation) doivent être conservés et que d'autre part seules les séquences $A1 \rightarrowtail F2 \rightarrowtail F1 \rightarrowtail A1$ doivent être retenues.

Aussi, partant de la matrice G_n, et en rejetant l'ensemble des modes indésirables et les transitions les liant, nous obtenons naturellement la matrice G'_n.

$$G_n = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$G'_n = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

La mise en forme matricielle autorise alors la première phase de projection sur le modèle de référence. Ceci a pour effet de rejeter les activités non-autorisées.

$$P(\delta_n(x, x') \rightarrow \sigma$$

$P(\delta_n(x, x'); x = \langle A1, R, Dt, Sv\rangle, x' = \langle F1, R, P, Dt, Sv, Cd\rangle;$
$G'_n(1, 2), G'_n(A1, F1) = 0 \rightarrow \varepsilon$

$P(\delta_n(x, x'); x = \langle A1, R, Dt, Sv\rangle, x' = \langle F2, R, P, Dt, Sv, Cd\rangle;$
$G'_n(1, 3), G'_n(A1, F2) = 1 \rightarrow \sigma$

$P(\delta_n(x, x'); x = \langle A1, R, Dt, Sv\rangle, x' = \langle F5, R, P, Dt, Sv, Cd\rangle;$
$G'_n(1, 5), G'_n(A1, F5) = 0 \rightarrow \varepsilon$

$P(\delta_n(x,x'); x = \langle F1, R, P, Dt, Sv, Cd\rangle, x' = \langle A1, R, Dt, Sv, Cd\rangle;$
$G'_n(2,1), G'_n(F1, A1) = 1 \rightarrow \sigma$

$P(\delta_n(x,x'); x = \langle F1, R, P, Dt, Sv, Cd\rangle, x' = \langle F3, R, P, Dt, Sv, Cd\rangle;$
$G'_n(2,4), G'_n(F1, F3) = 0 \rightarrow \varepsilon$

$P(\delta_n(x,x'); x = \langle F1, R, P, Dt, Sv, Cd\rangle, x' = \langle F5, R, P, Dt, Sv, Cd\rangle;$
$G'_n(2,5), G'_n(F1, F5) = 0 \rightarrow \varepsilon$

$P(\delta_n(x,x'); x = \langle F2, R, P, Dt, Sv, Cd\rangle, x' = \langle F1, R, P, Dt, Sv, Cd\rangle;$
$G'_n(3,2), G'_n(F2, F1) = 1 \rightarrow \sigma$

$P(\delta_n(x,x'); x = \langle F1, R, P, Dt, Sv, Cd\rangle, x' = \langle F5, R, P, Dt, Sv, Cd\rangle;$
$G'_n(3,5), G'_n(F1, F5) = 0 \rightarrow \varepsilon$

$P(\delta_n(x,x'); x = \langle F3, R, P, Dt, Sv, Cd\rangle, x' = \langle A1, R, Dt, Sv, Cd\rangle;$
$G'_n(4,1), G'_n(F3, A1) = 0 \rightarrow \varepsilon$

$P(\delta_n(x,x'); x = \langle F5, R, P, Dt, Sv, Cd\rangle, x' = \langle A1, R, Dt, Sv, Cd\rangle;$
$G'_n(5,1), G'_n(F5, A1) = 0 \rightarrow \varepsilon$

$P(\delta_n(x,x'); x = \langle F5, R, P, Dt, Sv, Cd\rangle, x' = \langle F1, R, P, Dt, Sv, Cd\rangle;$
$G'_n(5,1), G'_n(F5, F1) = 1 \rightarrow \varepsilon$

La deuxième phase de projection permet d'effacer les transitions non autorisées :

$$P(\delta_s(x,x') \rightarrow \sigma$$

Dans un souci de concision, seules les évolutions qui doivent être inhibées sont présentées ici. Les évolutions autorisées suite à cette projection sont représentées intégralement dans la figure 3.2.

$P(\delta_s(x,x'); x = \langle F3, R, Dt, Sv, Cd\rangle, x' = \langle D1, R, P, Dt, Sv, Cd, Dg, Ug\rangle;$
$P(\delta_s(F3, D1) \rightarrow \varepsilon$

$P(\delta_s(x,x');$
$x = \langle F3, R, Dt, Sv, Cd\rangle, x' = \langle D2, R, P, Dt, Sv, Dg\rangle;$
$P(\delta_s(F3, D2) \rightarrow \varepsilon$

$P(\delta_s(x,x'); x = \langle F5, R, Dt, Sv, Cd\rangle, x' = \langle D1, R, P, Dt, Sv, Cd, Dg, Ug\rangle;$
$P(\delta_s(F5, D1) \rightarrow \varepsilon$

$P(\delta_s(x,x'); x = \langle F5, R, Dt, Sv, Cd\rangle, x' = \langle D2, R, P, Dt, Sv, Dg\rangle;$
$P(\delta_s(F5, D2) \rightarrow \varepsilon$

$P(\delta_s(x,x'); x = \langle F5, R, Dt, Sv, Cd\rangle, x' = \langle D3, R, P, Dt, Sv, Cd, Dg\rangle;$
$P(\delta_s(F5, D3) \rightarrow \varepsilon$

Cette première phase de synthèse nous a permis de réduire la zone de travail au sein du modèle de référence. Ce dernier est désormais réduit aux activités et transitions autorisées en phase de fonctionnement normal. Les autres activités et transitions correspondant aux modes de traitements de défaillances sont quant à elles conservées (Figure 3.2).

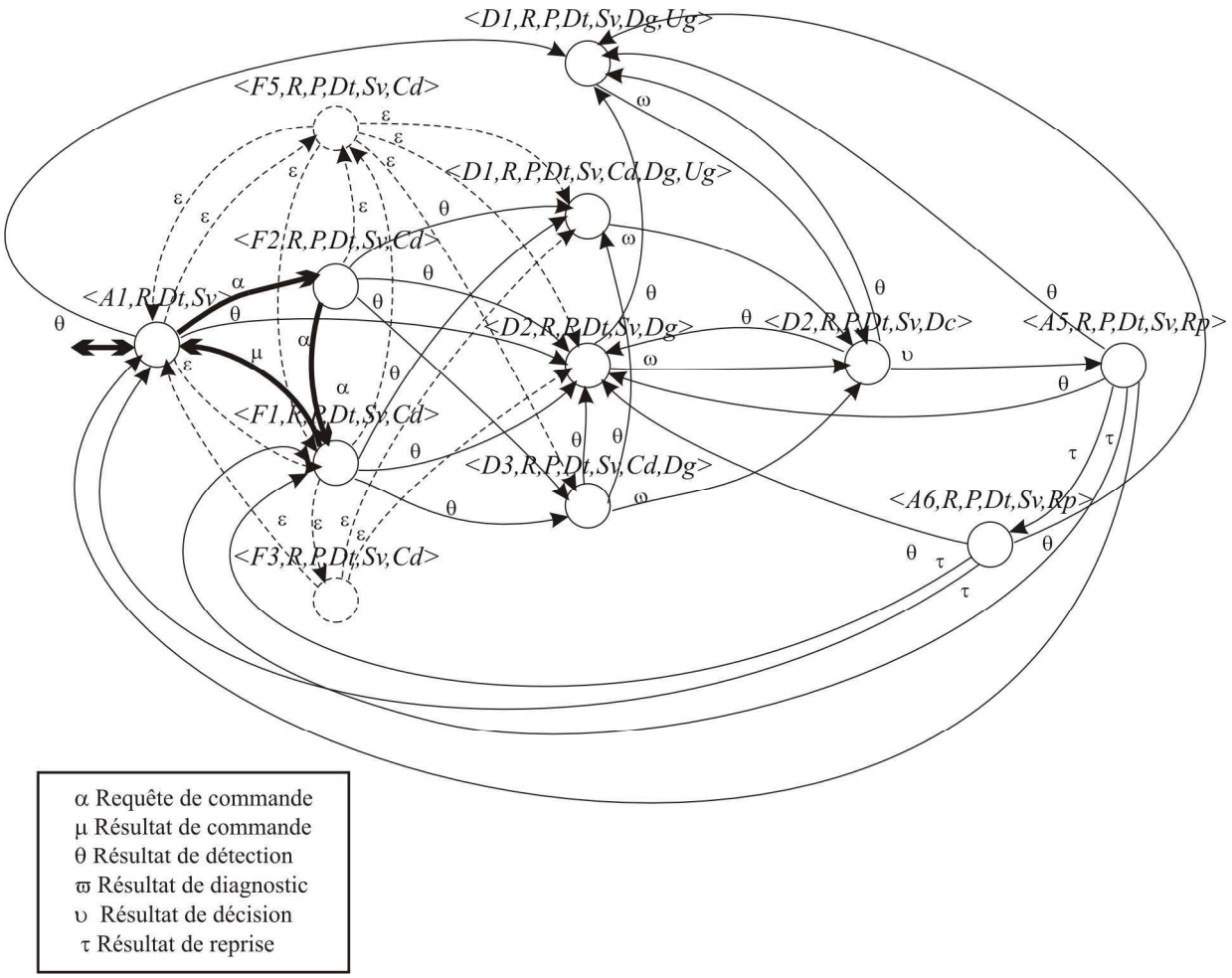

FIG. 3.2: *Résultats de la phase de synthèse I.*

3.3.2 Synthèse II

L'objectif de la phase de synthèse II est d'assigner à chaque traitement de défaillances le ou les "bons" symptômes de défaillance susceptibles de le déclencher. Pour ce faire, nous nous appuyons sur le cahier des charges spécifié sous la forme de grilles d'évaluation et décrit dans le chapitre précédent. La mise en relation traitement/symptôme est alors réalisée comme suit :

$$TS_{mc} = (T_c \times S_{mc})C$$

Ainsi, pour le mode $A1$ (arrêt initial) et selon le point de vue de la sécurité (s), les symptômes de défaillances qui doivent déclencher les traitements adéquats (Annexe 2) sont obtenus par :

$$TS_{A1,s} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} S1 \\ S2 \\ S3 \\ S4 \end{pmatrix} = \begin{pmatrix} 0 \\ S1 + S3 \\ S2 + S4 \end{pmatrix}$$

Pour le mode $A1$ (arrêt initial) et selon le point de vue de la productivité (p), nous obtenons :

$$TS_{A1,P} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} S1 \\ S2 \\ S3 \\ S4 \end{pmatrix} = \begin{pmatrix} S1+S2+S3+S4 \\ 0 \\ 0 \end{pmatrix}$$

Étant donné que pour les points de vue *écologie* (e) et *qualité* (q) dans le mode $A1$ l'occurrence de défaillances a été jugé comme non-significative, les matrices TS correspondantes sont forcément nulles :

$$TS_{A1,e} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}; TS_{A1,q} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix};$$

L'application de la même procédure pour les deux autres modes $F2$ et $F1$ selon les quatre points de vue sécurité, écologie, productivité et qualité nous conduit aux résultats suivants :

$$TS_{F2,s} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} S1 \\ S2 \\ S3 \\ S4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ S1+S2+S3+S4 \end{pmatrix}$$

$$TS_{F2,e} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} S1 \\ S2 \\ S3 \\ S4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$TS_{F2,p} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} S1 \\ S2 \\ S3 \\ S4 \end{pmatrix} = \begin{pmatrix} S1+S2+S3+S4 \\ 0 \\ 0 \end{pmatrix}$$

$$TS_{F2,q} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} S1 \\ S2 \\ S3 \\ S4 \end{pmatrix} = \begin{pmatrix} 0 \\ S1+S2+S3+S4 \\ 0 \end{pmatrix}$$

$$TS_{F1,s} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} S1 \\ S2 \\ S3 \\ S4 \end{pmatrix} = \begin{pmatrix} 0 \\ S1 \\ S2+S3+S4 \end{pmatrix}$$

$$TS_{F1,e} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} S1 \\ S2 \\ S3 \\ S4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$TS_{F1,p} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} S1 \\ S2 \\ S3 \\ S4 \end{pmatrix} = \begin{pmatrix} S1+S2+S3+S4 \\ 0 \\ 0 \end{pmatrix}$$

$$TS_{F1,q} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} S1 \\ S2 \\ S3 \\ S4 \end{pmatrix} = \begin{pmatrix} S1 \\ 0 \\ S2+S3+S4 \end{pmatrix}$$

Bien entendu, l'application de cette démarche doit également être réalisée pour tous les autres modes n'appartenant pas à la famille fonctionnement normal ; dans notre exemple $Mt = \{D1, D2, D3, A5, A6\}$. Cependant, alourdir ce paragraphe avec le calcul de toutes les autres matrices TS ne présente que peu d'intérêt. Pour cette raison, nous ne les avons pas présentées ici.

Bien que la méthode proposée dans le chapitre 3 de la partie III rejette la phase de projection des résultats obtenus après la prise en compte des priorités entre critères, nous avons souhaité cependant donner un aperçu graphique des quatre modèles obtenus correspondant aux quatre points de vue : Sécurité, Écologie, Productivité et Qualité (Figure 3.3).

Ceci nous permet de montrer graphiquement les problèmes liés au recouvrement de ces quatre modèles. En effet, des conflits apparaissent. Nous pouvons en effet remarquer qu'à partir de l'activité $< F1, R, P, Dt, Sv, Cd >$, l'événement (S2 + S3 + S4) conduit à l'activité $< D1, R, P, Dt, Sv, Cd, Dg, Ug >$ dans le modèle associé au critère Sécurité, alors que l'événement (S1 + S2 + S3 + S4) conduit à l'activité $< D3, R, P, Dt, Sv, Cd, Dg >$ au sein du modèle affecté au critère Productivité. La condition de transition $S2+S3+S4$ préfigure donc un conflit structurel effectif. Une phase de réglage de priorité doit donc être envisagée. Il s'agit de mettre en place la phase de synthèse III.

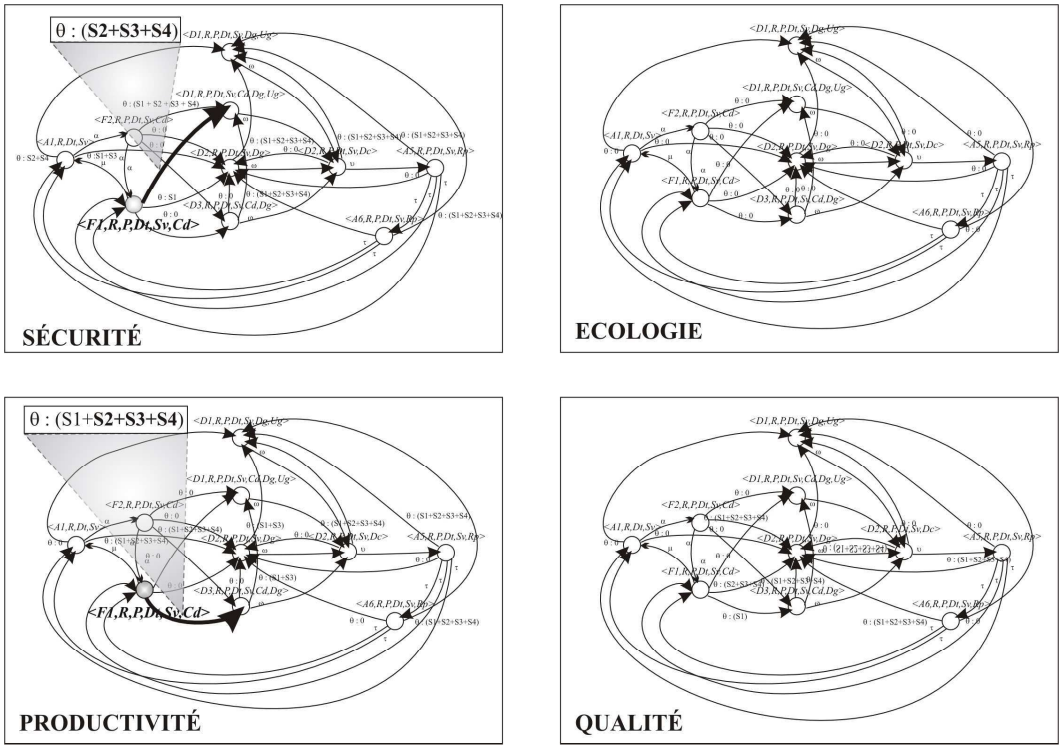

FIG. 3.3: *Projection des matrices TS sur l'extrait du modèle de référence*

3.3.3 Synthèse III

Dans le cadre de cette troisième étape de synthèse, nous allons chercher à résoudre les conflits structuraux liés aux conditions de transitions étiquetées par l'événement θ (*résultat de détection*).

Pour ce faire, nous allons reprendre les priorités entre les critères établis dans le chapitre précédent, les formaliser selon les principes donnés dans le chapitre 3 de la partie III et agir directement sur l'ensemble des matrices TS obtenues précédemment.

$P_{m,A} = \{P1_{m,A}, P2_{m,A}\} =$ { Sécurité, Écologie }
$P_{m,B} = \{P1_{m,B}, P2_{m,B}\} =$ { Productivité, Qualité }
$P1_{m,A,max}, P2_{m,A,min}$
$P1_{m,B,max}, P2_{m,B,min}$

Compte tenu que le critère Écologie ne présente aucun intérêt en ce qui concerne le procédé considéré, le réglage des priorités entre Sécurité et Écologie est simplifiée dans le groupe A.

Dans un souci de concision, nous ne présentons ici que les résultats de cet algorithme pour le mode $F1$:

Les vecteurs symptômes/transitions (TS) sont tout d'abord assignés à l'ensemble des vecteurs P :

$$P_{F1,A} = \{P1_{F1,A,max}, P2_{F1,A,min}\} = \{TS_{F1,s}, TS_{F1,e}\} = \begin{pmatrix} 0 \\ S1 \\ S2+S3+S4 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

L'application de la fonction F permet ensuite d'extraire du vecteur $P1_{F1,A,max}$ les éléments de $P2_{F1,A,min}$.

$$P1_{F1,A,max} > P2_{F1,A,min} \text{ ALORS } P2_{F1,A,min} = F(P1_{F1,A,max}, P2_{F1,A,min}) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

La somme entre les deux vecteurs $P1_{F1,A,max}$ et $P2_{F1,A,min}$ permet alors de déterminer le vecteur solution $P_{F1,A}$:

$$P_{F1,A} = P1_{F1,A,max} + P2_{F1,A,min} = \begin{pmatrix} 0 \\ S1 \\ S2+S3+S4 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ S1 \\ S2+S3+S4 \end{pmatrix}$$

Ce vecteur indique, pour le mode F1 et sur les plans sécurité et écologie, qu'aucun symptôme de défaillance ne peut conduire au déclenchement d'un traitement de type production forcée alors que l'occurrence d'un symptôme S1 doit aboutir au lancement d'un traitement classique (TC) et celle des symptômes S2, S3 et S4 conduiront à un traitement d'urgence (TU).

L'application de la même procédure au groupe B conduit à la construction du vecteur solution suivant :

$$P_{F1,B} = P1_{F1,B,max} + P2_{F1,B,min} = \begin{pmatrix} S1+S2+S3+S4 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} =$$

$$\begin{pmatrix} S1+S2+S3+S4 \\ 0 \\ 0 \end{pmatrix}$$

Le groupe A étant toujours prioritaire sur B, le vecteur solution final s'obtient en appliquant la fonction F à $P_{F1,B}$ et $P_{F1,A}$:

$$F(P_{F1,B}, P_{F1,A}) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

puis en sommant les vecteurs $P_{F1,B}$ et $P_{F1,A}$:

$$P_{F1} = P_{F1,A} + P_{F1,B} = \begin{pmatrix} 0 \\ S1 \\ S2+S3+S4 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ S1 \\ S2+S3+S4 \end{pmatrix}$$

Une projection des tous les vecteurs solutions de type P_m permet alors d'instancier l'extrait du modèle de référence en garantissant le déterminisme structurel des transitions conditionnées par les événements de type symptôme.

Remarque : bien entendu, comme nous l'avons déjà signalé dans la partie précédente, si aucune priorité n'est fixée dans le cahier des charges au sein des groupes A et B, un risque subsiste quant à la non résolution des indéterminismes. Si tel était le cas, et comme nous l'avons précisé, le concepteur devra alors passer en revue chacun des indéterminismes et les résoudre localement.

Pour le mode de marche $F1$, la projection $P : \delta(x, x') \rightarrow \sigma \cdot P_m$ donne le résultat suivant :

$$P_m(1,1) = 0; x(m) = F1, x'(m) = D3 \rightarrow \varepsilon; P_m(1,2) = S1; x(m) = F1, x'(m) = D2 \rightarrow \sigma \cdot P_m(1,1) = \theta \cdot \{S1\}; P_m(1,3) = S2 + S3 + S4; x(m) = F1, x'(m) = D1 \rightarrow \sigma \cdot P_m(1,1) = \theta \cdot \{S2, S3, S4\};$$

Les autres résultats peuvent être consultés au sein de la figure 3.4.

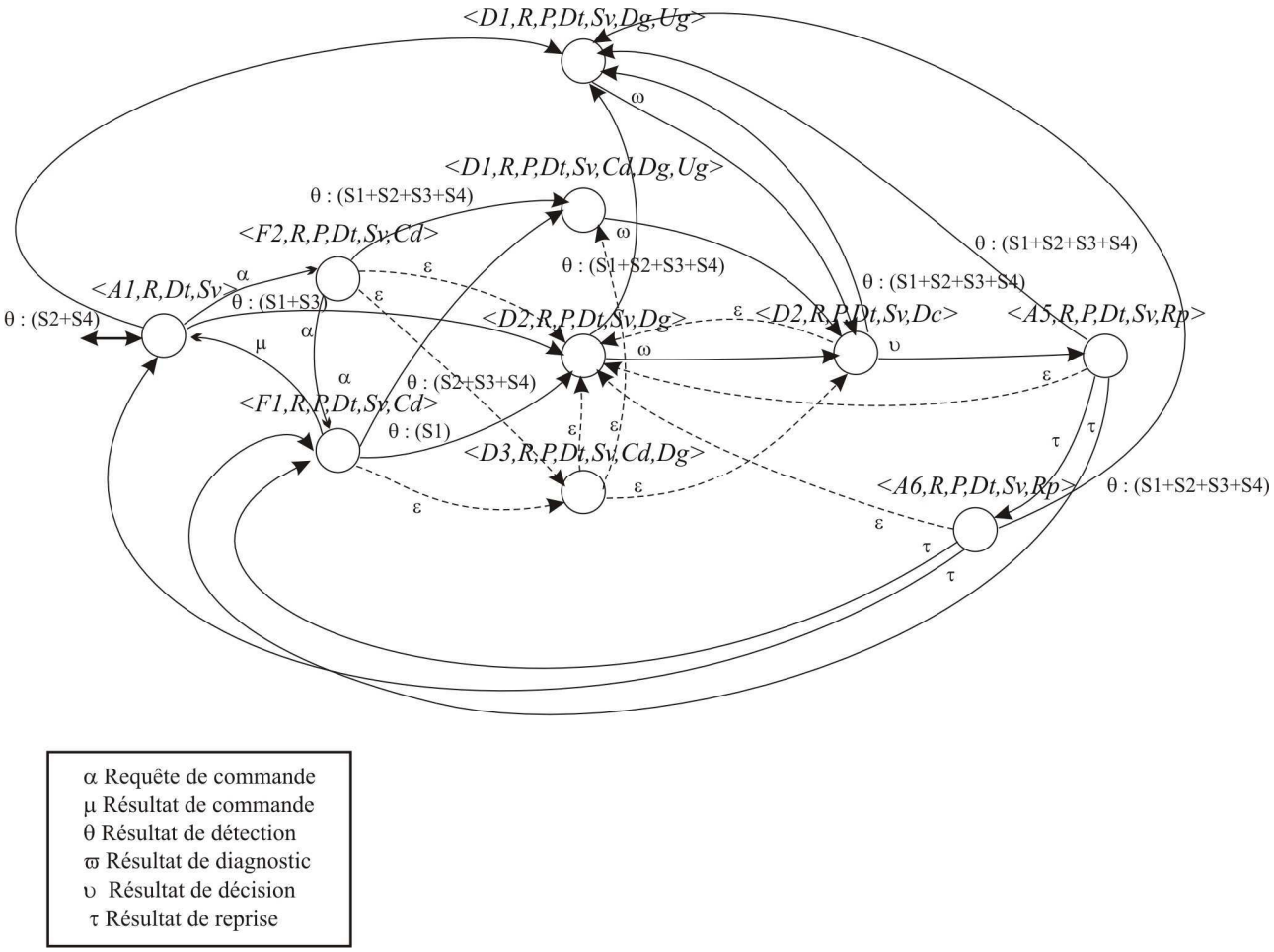

FIG. 3.4: *Modèle synthétisé en phase III*

Le modèle étant désormais déterministe sur le plan décisionnel, à savoir le choix de déclenchement d'un traitement de défaillance adapté non seulement aux symptômes détectés, au mode dans lequel ils ont été détectés, et aux critères retenus, nous pouvons maintenant envisager d'appliquer la phase de synthèse IV pour obtenir enfin la loi de surveillance du robot CHARLY.

3.3.4 Synthèse IV

Au niveau du cahier des charges localisé à cette étape de synthèse, nous avons estimé que détecter consécutivement trois fois le même symptôme de défaillance doit conduire à un changement de tactique.

Afin d'intégrer cette propriété, nous devons tout d'abord nous assurer qu'il existe bien au sein du modèle obtenu en phase de synthèse III des cycles infinis.

La figure 3.5 donne une image de la table des transitions déduite du modèle obtenu en phase III.

				θ						
		α	μ	θ1	θ2	θ3	θ4	ω	υ	τ
<A1,R,DT,Sv>	1	2		6	4	6	6			
<F2,R,P,Dt,Sv,Cd>	2	3		5	5	5	5			
<F1,R,P,Dt,Sv,Cd>	3		1	6	5	5	5			
<D1,R,P,Dt,Sv,Dg,Ug>	4							7		
<D1,R,P,Dt,Sv,Cd,Dg,Ug>	5							7		
<D2,R,P,Dt,Sv,Dg>	6			4	4	4	4	7		
<D2,R,P,Dt,Sv,Dc>	7			4	4	4	4		8	
<A5,R,P,Dt,Sv,Rp>	8			4	4	4	4			{1,3,9}
<A6,R,P,Dt,Sv,Rp>	9			4	4	4	4			{1,3}

α	Requête de commande
μ	Résultat de commande
θ1	Résultat de détection avec symptôme de défaillance 1
θ2	Résultat de détection avec symptôme de défaillance 2
θ3	Résultat de détection avec symptôme de défaillance 3
θ4	Résultat de détection avec symptôme de défaillance 4
ω	Résultat de diagnostic
υ	Résultat de décision
τ	Résultat de reprise

FIG. 3.5: *Table des transitions*

A partir de cette table, et en appliquant l'algorithme de Mac Naughton et Yamada (Séébold [1999]), nous obtenons le langage reconnu par l'automate suivant :

$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}; L(Mr') = W_{1,s,1} \mid |s| > 0$

$X =$ Ensemble des activités du modèle tel que
$1 =< A1, R, DT, Sv >$
$2 =< F2, R, P, Dt, Sv, Cd >$
$3 =< F1, R, P, Dt, Sv, Cd >$
$4 =< D1, R, P, Dt, Sv, Dg, Ug >$
$5 =< D1, R, P, Dt, Sv, Cd, Dg, Ug >$
$6 =< D2, R, P, Dt, Sv, Dg >$
$7 =< D2, R, P, Dt, Sv, Dc >$
$8 =< A5, R, P, Dt, Sv, Rp >$
$9 =< A6, R, P, Dt, Sv, Rp >$

$L(Mr') =$ Langage reconnu par le modèle. Il est composé de l'ensemble des séquences s qui partent de l'état initial (1) et qui y reviennent avec une longueur non nulle.

$W_{1,\{2,3\}1} = \{\alpha, \alpha, \mu\}$
$W_{1,\{2,5,7,3\}1} = \{\alpha, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \mu\}$
$W_{1,\{2,5,7,8\}1} = \{\alpha, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau\}$
$W_{1,\{2,5,7,8,3\}1} = \{\alpha, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau, \mu\}$
$W_{1,\{2,5,7,8,9\}1} = \{\alpha, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau, \tau\}$
$W_{1,\{2,5,7,8,9,3\}1} = \{\alpha, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau, \tau, \mu\}$
$W_{1,\{2,5,7,4,7,3\}1} = \{\alpha, \theta\{S1, S2, S3, S4\}, \omega, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \mu\}$
$W_{1,\{2,5,7,4,7,8\}1} = \{\alpha, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau\}$
$W_{1,\{2,5,7,4,7,8,3\}1} = \{\alpha, \theta\{S1, S2, S3, S4\}, \omega, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau, \mu\}$
$W_{1,\{2,5,7,4,7,8,9\}1} = \{\alpha, \theta\{S1, S2, S3, S4\}, \omega, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau, \tau\}$
$W_{1,\{2,5,7,4,7,8,9,3\}1} = \{\alpha, \theta\{S1, S2, S3, S4\}, \omega, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau, \tau, \mu\}$
$W_{1,\{2,3,5,7,3\}1} = \{\alpha, \alpha, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \mu\}$
$W_{1,\{2,3,5,7,8\}1} = \{\alpha, \alpha, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau\}$

$W_{1,\{2,3,5,7,8,3\}1} = \{\alpha, \alpha, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau, \mu\}$
$W_{1,\{2,3,5,7,8,9\}1} = \{\alpha, \alpha, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau, \tau\}$
$W_{1,\{2,3,5,7,8,9,3\}1} = \{\alpha, \alpha, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau, \tau, \mu\}$
$W_{1,\{2,3,5,7,4,7,3\}1} = \{\alpha, \alpha, \theta\{S1, S2, S3, S4\}, \omega, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \mu\}$
$W_{1,\{2,3,5,7,8\}1} = \{\alpha, \alpha, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau\}$
$W_{1,\{2,3,5,7,4,7,8,3\}1} = \{\alpha, \alpha, \theta\{S1, S2, S3, S4\}, \omega, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau, \mu\}$
$W_{1,\{2,3,5,7,4,7,8,9\}1} = \{\alpha, \alpha, \theta\{S1, S2, S3, S4\}, \omega, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau, \tau\}$
$W_{1,\{2,3,5,7,,4,7,8,9,3\}1} = \{\alpha, \theta\{S1, S2, S3, S4\}, \omega, \alpha, \theta\{S1, S2, S3, S4\}, \omega, \upsilon, \tau, \tau, \mu\}$
$W_{1,\{4,7,3\}1} = \{\theta\{S2\}, \omega, \upsilon, \mu\}$
$W_{1,\{4,7,8\}1} = \{\theta\{S2\}, \omega, \upsilon, \tau\}$
$W_{1,\{4,7,8,3\}1} = \{\theta\{S2\}, \omega, \upsilon, \tau, \mu\}$
$W_{1,\{4,7,8,9\}1} = \{\theta\{S2\}, \omega, \upsilon, \tau, \tau\}$
$W_{1,\{4,7,8,9,3\}1} = \{\theta\{S2, \}, \omega, \upsilon, \tau, \tau, \mu\}$
$W_{1,\{6,4,7,3\}1} = \{\theta\{S1 + S3 + S4\}, \theta\{S1 + S2 + S3 + S4\}, \omega, \upsilon, \mu\}$
$W_{1,\{6,4,7,8\}1} = \{\theta\{S1 + S3 + S4\}, \theta\{S1 + S2 + S3 + S4\}, \omega, \upsilon, \tau\}$
$W_{1,\{6,4,7,8,3\}1} = \{\theta\{S1 + S3 + S4\}, \theta\{S1 + S2 + S3 + S4\}, \omega, \upsilon, \tau, \mu\}$
$W_{1,\{6,4,7,8,9\}1} = \{\theta\{S1 + S3 + S4\}, \theta\{S1 + S2 + S3 + S4\}, \omega, \upsilon, \tau, \tau\}$
$W_{1,\{6,4,7,8,9,3\}1} = \{\theta\{S1 + S3 + S4\}, \theta\{S1 + S2 + S3 + S4\}, \omega, \upsilon, \tau, \tau, \mu\}$
$W_{1,\{2,3,6,4,7,3\}1} = \{\alpha, \alpha, \theta\{S1\}, \theta\{S1 + S2 + S3 + S4\}, \omega, \upsilon, \mu\}$
$W_{1,\{2,3,6,4,7,8\}1} = \{\alpha, \alpha, \theta\{S1\}, \theta\{S1 + S2 + S3 + S4\}, \omega, \upsilon, \tau\}$
$W_{1,\{2,3,6,4,7,8,3\}1} = \{\alpha, \alpha, \theta\{S1\}, \theta\{S1 + S2 + S3 + S4\}, \omega, \upsilon, \tau, \mu\}$
$W_{1,\{2,3,6,4,7,8,9\}1} = \{\alpha, \alpha, \theta\{S1\}, \theta\{S1 + S2 + S3 + S4\}, \omega, \upsilon, \tau, \tau\}$
$W_{1,\{2,3,6,4,7,8,9,3\}1} = \{\theta\{S1 + S3 + S4\}, \theta\{S1 + S2 + S3 + S4\}, \omega, \upsilon, \tau, \tau, \mu\}$

La partie du langage reconnu qui correspond au fonctionnement normal est défini par :

$L(Mr') = \{s \in L(Mr') | \theta \notin s\} = \{\alpha, \alpha, \mu\}$

Chacune des autres évolutions correspond à un traitement de défaillances différent. Nous pouvons remarquer que quelle que soit l'occurrence d'un symptôme de défaillance au cours d'un traitement de défaillance, il provoque le déclenchement d'un traitement d'urgence. En conséquence, il n'y a aucun risque que le système de surveillance, commande et supervision basé sur ce modèle se retrouve dans un cycle infini. Quoiqu'il se passe au cours d'un traitement de défaillance, une procédure d'urgence sera lancée.

Dans ce cas précis, le modèle obtenu en phase de synthèse III est donc la loi de surveillance du robot CHARLY de la plate-forme SAPHIR (Figure 3.6).

3.4 Vérification

Cette section est dédiée à la vérification de l'adéquation du modèle obtenu par rapport au cahier des charges que nous nous sommes fixé.

Notons cependant que l'objectif n'est pas ici de mener une vérification formelle de l'adéquation de la loi avec le cahier des charges, ceci sort en effet largement du cadre de l'étude. Nous nous proposons simplement de vérifier "à la main" quelques propriétés qui doivent être contenues, de manière implicite dans la loi générée.

En premier lieu, les aspects modes de marche et d'arrêt imposés en fonctionnement normal (A1, F1 et F2) sont respectés. Seuls trois activités liées à ces modes ont subsisté à la première étape de synthèse, il s'agit de $< A1, R, Dt, Sv >$, $< F1, R, P, Dt, Sv, Cd >$ et $< F2, R, P, Dt, Sv, Cd >$.

Sur le plan du respect des critères de sécurité, écologie, productivité et qualité, nous

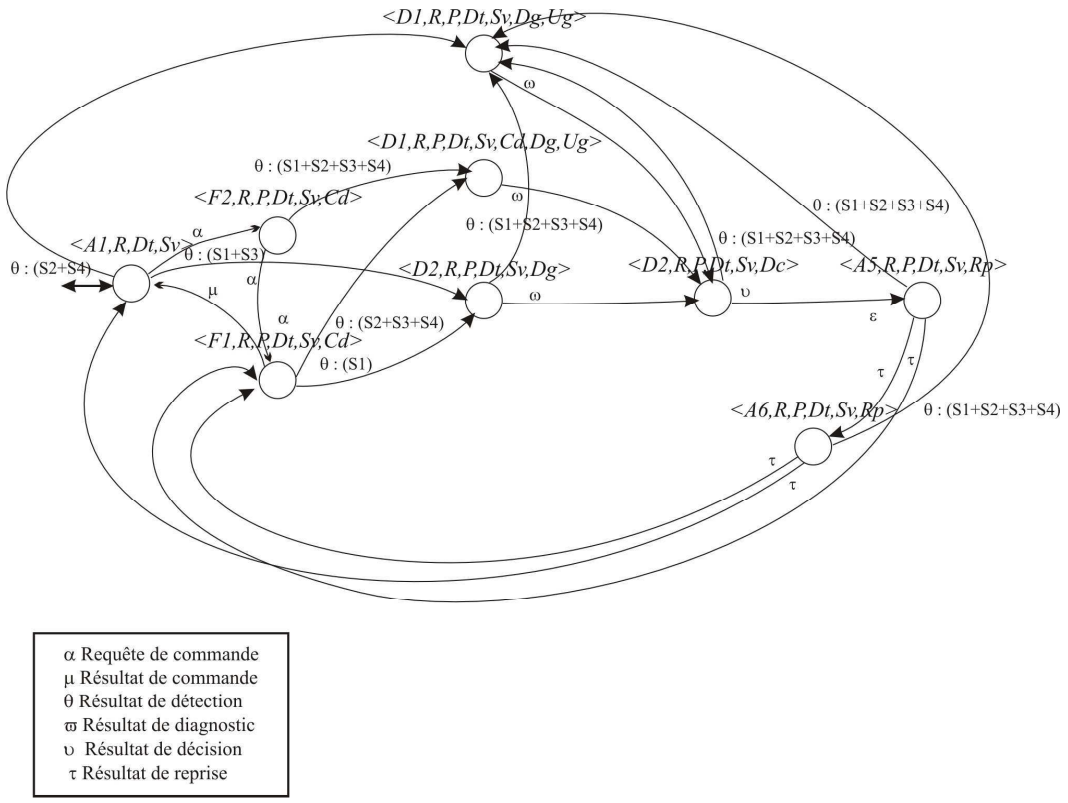

FIG. 3.6: *Loi de surveillance dédiée au robot "Charly"*

pouvons remarquer par exemple qu'à partir d'une activité appartenant au fonctionnement normal, il n'est pas possible de lancer une production forcée. Ceci respecte bien le cahier des charges qui doit être appliqué à une telle ressource. Quelle que soit la gravité de la défaillance détectée, il ne faut surtout pas continuer à produire au risque de casser le matériel (la pince est un outil de précision très fragile) ou de mettre en danger un opérateur humain. Le point de vue de la productivité a bien été mis "de côté", au profit de la sécurité.

Enfin, sur le plan de la récursivité, nous avons déjà pu montrer que le modèle obtenu ne présentait pas de cycles infinis à partir d'un état du fonctionnement anormal. Tout événement du type "résultat de détection" conduit dans notre cas à l'application d'une procédure d'urgence. La propriété imposée dans le cadre de cette synthèse IV est, de fait, amplement satisfaite.

3.5 Conclusion

L'exemple que nous venons de développer dans cette partie est basé sur la synthèse d'une loi de surveillance du robot d'assemblage de la plate-forme SAPHIR du Laboratoire d'Automatique de Grenoble.

Il s'est notamment agit de démontrer à la fois la pertinence du cadre de rédaction du cahier des charges proposé et de l'applicabilité de la méthode de synthèse mise en place.

Dans ce but, nous nous sommes appuyés sur un modèle de référence allégé pour l'occasion. La manipulation du modèle complet n'était en effet pas envisageable pour des raisons évidentes (98 activités et plus de 1100 transitions). Cependant, nous avons montré que cette réduction n'altérait d'aucune façon la démonstration.

Du point de vue de la spécification des propriétés qu'il faut rechercher pour synthétiser une loi de surveillance, nous avons pu constater l'intérêt du cadre rédactionnel très structuré que nous proposons. Le concepteur doit en quelque sorte "remplir des cases" avec le support de définitions et de documents techniques très ciblés. Ceci présente un avantage certain en terme de fermeture de contexte ; ceci permet d'ailleurs de garantir par la suite le bon déroulement de la synthèse. Cependant, nous devons noter que le niveau d'expertise du concepteur prend une place capitale au cours de cette phase de spécification. En effet, les aspects d'évaluation, bien que documentés et guidés, se prêtent mal à une formalisation totale. Enfin, dans l'état actuel, force est de constater que les différentes phases de spécification, bien que parfaitement génériques d'une ressource à l'autre, peuvent paraître fastidieuses voire même peu abordables pour un non-initié. Pour cette raison, il faudra à court terme envisager de concevoir une interface logicielle d'assistance à la saisie du cahier des charges.

Du point de vue de la technique de synthèse proposée, l'exemple nous a conduit pas à pas à suivre la démarche jusqu'à l'obtention de la loi de surveillance du robot. La méthode sélectionnée a consisté à mettre en relation progressivement l'ensemble de propriétés recherchées avec la structure même du modèle de référence. Ainsi, nous avons successivement mis en forme les différentes propriétés recherchées sous les formes matricielles spécifiques préconisées et avons ensuite appliqué les projections de ces matrices sur la structure du modèle de référence. L'application de cette méthode a montré essentiellement son caractère systématique et son efficacité, ce qui laisse à penser que son informatisation à court terme ne devrait pas poser de problèmes majeurs.

Enfin, nous avons mené une vérification succincte "à la main" de l'adéquation entre les propriétés recherchées et la loi de surveillance obtenue. Bien que non exhaustive, cette vérification à pu mettre en évidence qu'un sous-ensemble de propriétés étaient respectées par la loi. Bien entendu, le recours à des outils de vérification formelle doit être envisagé, mais ceci sort largement du cadre de ces travaux.

Conclusion générale

Conclusion générale

Les travaux que nous avons présentés dans ce document traitent de la surveillance, de la commande et de la supervision des procédés industriels complexes. Ils font suite à ceux déjà réalisés [Combacau, 1991] [Zamaï, 1997].

La contribution de nos travaux est l'élaboration d'une technique de synthèse de lois de surveillance adaptée non seulement aux besoins de l'entreprise, mais aussi à la ressource considérée et aux normes législatives en vigueur.

Pour ce faire, nous avons tout d'abord proposé une définition des concepts et des mécanismes nécessaires à la conception de traitements de défaillances adaptés non seulement au procédé considéré mais également aux produits manipulés, au contexte de production, aux exigences économiques des entreprises, aux contraintes législatives imposées sous la forme de normes de qualité, d'écologie ou encore de sécurité imposées par les gouvernements. Cette analyse a conduit à l'identification d'un modèle de référence générique de tous les traitements de défaillances utilisables en entreprise pour la supervision, la surveillance et la commande de procédés industriels. Ce modèle compte à ce jour 98 états et plus de 1100 processus élémentaires les liant. Ceci a ouvert des perspectives fort intéressantes quant aux moyens qu'il est possible de mettre en œuvre pour superviser et surveiller correctement une installation industrielle.

Nous avons ensuite proposé une démarche de génération semi-automatique de traitements de défaillances en adéquation avec les différentes exigences des industriels. Cette démarche s'appuie sur une méthode proche de la synthèse de correcteurs (automatique continue) pour lesquels par exemple les critères marge de phase, marge de gain doivent être réglés afin d'obtenir à partir du modèle de comportement du système à commander, la loi de commande.

Partant du modèle de référence établi, nous avons proposé une méthode de réglage de critères (i.e. réglage de la marge de phase à 45^0 pour garantir la stabilité du système en boucle fermée) tels que l'impact (mineur, significatif, critique et catastrophique) de symptômes de défaillance génériques sur les plans écologique, économique, qualitatif ou sécuritaire. Cette démarche, véritablement novatrice dans le domaine, a donné lieu à des résultats significatifs.

Enfin, comme nous l'avons souligné dans les deux dernières parties de ce mémoire, l'opérateur trouve naturellement sa place dans notre approche. Il est en effet le seul à détenir le niveau d'expertise suffisant pour évaluer par exemple l'impact des symptômes de défaillances selon les critères de productivité, qualité, sécurité ou encore écologie. La démarche générale proposée dans le cadre de ce mémoire offre donc un cadre de conception assistée des lois de surveillance.

Au terme de ces travaux, plusieurs axes de recherche se dégagent pour envisager, du point de vue des perspectives, de prolonger l'étude menée pendant ces trois ans.

A court terme, quatre axes d'investigations peuvent être envisagés :

- Premièrement, une étude peut être entreprise afin de fournir les outils nécessaires à la validation et à la vérification des lois de surveillance générées par rapport aux propriétés recherchées. Pour ce faire, les travaux réalisés par (Lampérière-Couffin [1998]) devront être analysés finement.
- Deuxièmement, et d'un point de vue plus technique, une réalisation informatique complète de l'approche de synthèse s'impose en intégrant les aspects validation et vérification.
- Troisièmement, une validation à échelle réelle pourra ensuite être envisagée sur la base du superviseur proposé dans les travaux de E. Zamaï. Ce superviseur est actuellement en cours de développement au sein du Laboratoire d'Automatique de Grenoble et devrait voir le jour d'ici quelques mois. Son installation au sein de l'architecture de pilotage de la plate-forme SAPHIR permettra donc de valider différentes lois de surveillance répondant à différentes variantes des sept propriétés qui doivent être recherchées.
- Enfin, nous avons dans la partie III de ce mémoire émis l'hypothèse que deux solutions de synthèse pouvaient être proposées : soit développer une technique permettant d'intégrer directement les critères au sein d'un modèle appartenant au monde du discret, soit encore proposer une technique permettant de traduire les critères sous la forme de contraintes puis d'appliquer une technique conventionnelle de synthèse de l'automatique discrète. Dans le cadre de ces travaux, nous avons opté pour la première solution. Il n'en demeure pas moins que la seconde solution devrait être également étudiée.

A moyen terme, nous pouvons mettre en évidence quatre orientations de recherche possibles.

- Premièrement, il est possible d'envisager d'étudier la résolution des autres indéterminismes structuraux du modèle. En effet, nous avons émis l'hypothèse dès la partie III de ce mémoire, que nous ne nous intéresserons qu'aux indéterminismes de transitions conditionnées par l'événement "résultat de détection" (θ). Pourtant, d'autres transitions sont conflictuelles, notamment celles conditionnées par les événements "résultat de décision", "résultat de reprise", etc. Pour chacun de ces événements, le même travail que celui mené dans le cadre de cette thèse devra être réalisé afin de proposer rapidement une technique complète de synthèse de lois de surveillance. Cependant, l'issue de ce travail est conditionné par la connaissance exacte des algorithmes qui régissent les différentes fonctions concernées. Aussi, au même titre que pour la fonction détection, des algorithmes génériques devront être étudiés et sélectionnés dans la littérature, ou à défaut établis, pour identifier clairement les différents niveaux des résultats générés. Une évaluation de ces résultats pourra alors être envisagée, afin de résoudre les autres conflits du modèle de référence.
- Une deuxième étude pourrait s'intéresser à l'interaction de plusieurs lois de surveillance associées à des produits simultanément associés à la même ressource. La résolution des conflits entre ces lois en serait le principal centre d'intérêt.
- Troisièmement, au sein d'un nœud de surveillance, commande et supervision comment considérer dans notre approche l'interaction de plusieurs lois de surveillance ? Une étude des incohérences décisionnelles inter-lois de surveillance pourrait être menée afin d'envisager une démarche de synthèse non-plus spécifique à une ressource, mais à plusieurs ressources physiques.

- Quatrièmement, une étude identique pourrait être menée quant aux conflits décisionnels qui peuvent exister entre deux lois de surveillance générées à des niveaux décisionnels différents. En effet, comment considérer une loi d'un nœud de coordination de niveau I imposant une production forcée, alors qu'une des loi du niveau inférieur intègre des normes sécuritaires sévères (i.e. robotique) imposant des arrêts d'urgence en présence de défaillances significatives ?

- Enfin, on pourrait encore s'intéresser à l'analyse détaillée des recouvrements décisionnels existant entre une loi de surveillance et les fonctions mêmes de surveillance, commande et supervision. En effet, chacune de ces fonctions intègre une part de décision qui peut par exemple entrer en conflit avec la loi de surveillance synthétisée.

Par ailleurs, à plus long terme, il faudrait envisager l'étude de la pertinence de l'approche proposée dans des contextes de natures différentes, comme par exemple l'automobile, l'aéronautique, les services hospitaliers, etc.

Bibliographie

Bibliographie

ADEPA. *Le GEMMA, Guide d'Etude des Modes de Marches et d'Arrêts.* Adepa, Agence de la Productique, 17 rue Perier, 92120 Montrouge, 1981.

AFNOR. Norme nf en61-120 - sites de production comprenant des robots manipulateurs industriels - prévention des accidents d'origine mécanique. Technical report, Association Française de Normalisation, 1995a.

AFNOR. Norme nf x50-125 - qualité - management de la qualité et assurance de la qualité - vocabulaire - termes complémentaires. Technical report, Association Française de Normalisation, 1995b.

S. Ben Ahmed, M. Moalla, et M. Courvoisier. Approche multimodèles pour la commande des ateliers flexibles. *RAIRO-APII, Journal Européen des Systèmes Automatisés*, 30: 1201–1232, 1996.

D. Alligier. Réalisation dŠun superviseur de commande et de surveillance pour le pilotage temps réel des systèmes flexibles de production manufacturière. Technical report, Centre Universitaire d'Education et de Formation des Adultes, Grenoble, France, 2001.

B. Bako. *Mise en œuvre et simulation du niveau coordination de la commande des ateliers flexibles: une approche mixte réseaux de Petri et systèmes de règles.* PhD thesis, Université Paul Sabatier, Toulouse, Octobre 1990.

T. Belkadi. Réalisation et intégration de commande de cellule flexible. Projet de mastère production automatisée, ENIT, Septembre 1989.

P. Bellot et J. Sakarovitch. *Logique et automates.* Ellipses, France, 1998.

P. Berruet. *Contribution au recouvrement des systèmes flexibles de production manufacturières: analyse de la tolérance et reconfiguration.* PhD thesis, Université de Lille, Décembre 1998.

P. Berruet, A. Toguyeni, et E. Craye. Considering parts in progress in a reconfiguration procedure for fms. Dans *3rd IMACS/IEEE International Multiconference, Circuits, Systems, Communications and Computers (CSCC'99)*, Athènes, Grece, Juillet 1999.

J.C. Billaut. *Prise en Compte des Ressources Multiples et des Temps de Préparation dans les Problèmes d'Ordonnancement en Temps Réel.* PhD thesis, Université Paul Sabatier, Toulouse, Décembre 1993.

M. Blanchard. *Comprendre, maîtriser et appliquer le grafcet.* Cepadues, 1979.

C. Briand. Vers une plus grande flexibilité du pilotage des systèmes de production. *Modélisation des Systèmes Réactifs, Hermes*, pages pp.277–286, Mars 1999.

G. Bucci, M. Campanai, et P. Nesi. Tools for specifying real-time systems. *Real-Time Systems*, 8:117–172, 1995.

S. Chafik. *Proposition d'une structure de contrôle par supervision hiérarchique et distribuée : application à la coordination.* PhD thesis, Institut National des Sciences Appliquées de Lyon, 22 décembre 2000.

S. Chafik et E. Niel. Hierarchical descentralized solutions of supervisory control. Dans *3rd MATHMOD*, volume 2, pages 787–790, Vienna, Austria, February 2000.

A. Chaillet. *Approche multi modèles pour la commande et la surveillance en temps réel des systèmes à événements discrets.* PhD thesis, Université Paul Sabatier, Toulouse, Décembre 1995.

A. Chaillet-Subias et M. Courvoisier. An architecture and its mechanism for real-time control and monitoring of discrete events systems. Dans *IMACS Multiconference, Computational Engineering in Systems Applications, CESA'96*, Lille, France, Juillet 1996.

A. Chaillet-Subias, E. Zamaï, et M. Combacau. Information flow in a control and monitoring architecture. Dans *IEEE International Symposium on Industrial Electronics*, Guimarães, Portugal, Juillet 1997.

F. Charbonnier, B.A. Brandin, H. Alla, et C. Foulard. Commande par supervision d'un atelier flexible. *Revue d'Automatique et Productique Appliquée*, 7 (5):491–507, octobre, 1994.

M. Combacau. *Commande et surveillance des systèmes à événements discrets complexes : application aux ateliers flexibles.* PhD thesis, Université Paul Sabatier, Toulouse, Décembre 1991.

M. Combacau, P. Berruet, E. Zamaï, P. Charbonnaud, et A. Khatab. Supervision and monitoring of production systems. Dans *Second Conférence on Management and Control of Production and Logistics (MCPL'2000)*, Grenoble, France, 5-8 juillet 2000.

F. Couffin, S. Lamperiere, E. Hospital, et J.M. Faure. Reutilisation d'un modele de reference en genie automatique - application a l'integration des activites de conception des systemes automatises de production. *JESA - AFCET - CNRS*, 34 (1):35–62, Fevrier 2000.

D. Cruette. *Méthodologie de conception des systèmes complexes à événements discrets: application à la conception et à la validation hierarchisée de la commande de cellules flexibles de production dans l'industrie manufacturière.* Thèse de doctorat, Université de Lille, Février 1991.

N. Dangoumau. *Contribution à la gestion des modes des systèmes automatisés de Production.* PhD thesis, Université des Sciences et Technologies de Lille, Lille, Décembre 2000.

N. Dangoumau, A.K.A. Toguyeni, et S. El Khattabi end E. Craye. Modes management for automated production systems. Dans *International Symposium on Manufacturing with Applications (ISOMA)*, Maoui, Hawaii, june 2000.

R. David et H. Halla. *Du Grafcet aux réseaux de Petri.* Hermes, Paris, France, 1992.

A. de Bonneval. *Mécanismes de Reprise dans les Systèmes de Commande à Evénements Discrets.* Thèse de doctorat, Université Paul Sabatier, Toulouse, Septembre 1993.

A. de Bonneval, M. Combacau, et M. Courvoisier. Rôle de l'opérateur humain dans une boucle de surveillance automatique de systèmes à événements discrets. Dans *Canadian Conference and Exhibition on Industrial Automation*, Montreal, Canada, Juin 1992.

D. Delfieu. *Expression et validation de contraintes temporelles pour la spécification des systèmes réactifs*. PhD thesis, Université Paul Sabatier de Toulouse, Toulouse, France, janvier 1995.

D. Delfieu et A.E.K. Sahraoui. Expression and validation of timing constraints and integration in software specification methods. Dans *IEEE Workshop on Real-Time Application*, pages 63–68, Washington USA, 21-22 Juillet 1994.

J. Erschler. Flexibilité et autonomie dans les systèmes de production. Dans *1er Congrès Biennal de l'AFCET*, pages 13–18, Versailles,France, 8-10 Juin 1993.

P. Esquirol et P.Lopez. *L'ordonnancement*. Economica. Collection Gestion, 1999.

EXERA et Gimélec. *Guide pratique de spécification de la conduite des systèmes de production. Méthode DEMIOPS*. Association des exploitants d'equipements de Mesure, de regulation et d'automatisme (EXERA) et Groupement des industries de l'equipement électrique, du contrôle-commande et des services associés (Gimélec), 1999.

P. Faurre et M. Robin. *Eléments d'automatique*. Dunod, Saint Etienne, France, 1984.

J.-L. Ferrier. De quelques approches de la commande basée sur les réseaux de petri, notes de cours sed. Technical report, Laboratoire d'Ingénierie des Systèmes Automatisés (LISA), 1999.

C. Foulard, J.-M. Flaus, et M. Jacomino. *Automatique pour les classes préparatoires*. Hermes, Paris, France, juin 1997.

J.-P. Frachet, S. Lamperière, et J.M. Faure. The hyperfinite signal: application to the modelling of discrete event systems behavior. Dans *CESA'96 : IEEE-IMACS Multiconference Cumputational Engineering in Systems Applications. Symposium on Discrete Events ans Manufacturing Systems*, pages 584–589, Lille,France, 9-12 juillet 1996a.

J.-P. Frachet, S. Lamperière, et J.M. Faure. Le signal hyperfini : application à la modélisation du comportement des systèmes à événements discrets. Dans *AFCET'96 : Modélisation des systèmes réactifs*, pages 335–342, Brest,France, 28-29 mars 1996b.

République Française. Code du travail. chapitre 3 : Sécurité. *Journal Officiel*, 3 janvier 1973.

S. Gentil et E. Zamaï. *Techniques de l'Ingénieur en Informatique Industrielle*, chapter principes des chaînes de régulation. Techniques de l'ingénieur, décembre 2002.

GREPA. *Le grafcet : de nouveaux concepts*. Cepadues, 1985.

S. Hammami, I. Tnazefti, M. Moala, et A. Chaillet. Designing control and diagnosis for flexible manufacturing systems as a multi-agent system using blackboard and object petri nets. Dans *4th INRIA/IEEE Symposium on Emerging Technologies and Factory Automation, ETFA'95*, Paris, France, Octobre 1995.

G. Hetreux. *Structures de Décision Multi-Niveaux pour la Planification de la Production : Robustesse et Cohérence des Décisions*. PhD thesis, Université Paul Sabatier, Toulouse, Décembre 1996.

L. E. Holoway et B. H. Krogh. Fault detection and diagnosis in manufacturing systems: a behavioral model approach. Dans *IEEE International Conference on Computer Integrated Manufacturing*, Mai 1990.

J. Hopcroft et J. Ullman. *Introduction to automata theoty, languages end computation.* Addison Wesley, Reading, MA, 1978.

B. Huvenoit. *De la conception à l'implémentation de la commande modulaire et hiérarchisée des systèmes flexibles de production manufacturière.* PhD thesis, Université de Lille 1, Octobre 1994.

Institut Français de l'Environnement IFEN. *Indicateurs de Performance environnementale de la France, édition 1996-1997.* Editions Lavoisier TEC and DOC, 1998.

International Organization for Standardization ISO. *ISO 9000:2000 Quality management systems – Fundamentals and vocabulary.* ISO Normalisation, 2000.

A. Jones. A multi-layer/multi-level control architecture for computer integrated manufacturing systems. Dans *IEEE Int. Symp. on Intelligent Control*, Albany, NY, Septembre 1989.

O. Kamach, S. Chafik, L. Pietrac, et E. Niel. Representation of a reactive system with different models. Dans *Soumis à 2002 IEEE International Conference on Systems, Man and Cybertetics (SMC'02)*, Hammamet, Tunisia, 6-9 octobre 2002.

A. Khatab. *Contrôle et contrôle stabilisant des systèmes à événements discrets : application au recouvrement des défaillances.* PhD thesis, Institut National des Sciences Appliquées de Lyon, 18 décembre 2000.

S. El Khattabi. *Intégration de la Surveillance de Bas Niveau dans la Conception des Systèmes à Evénements Discrets : Application aux Systèmes de Production Flexibles.* PhD thesis, Université des Sciences et Technologies de Lille, Septembre 1993.

S. Lampérière-Couffin. *De la vérification des cahiers des charges de systèmes à événements discrets à la validation des spécifications décrits en Grafcet.* PhD thesis, École Normale Supérieur de Cachan, Cachan , France, Janvier 1998.

Larousse. *Petit Larousse illustré 2002.* Larousse, Paris, France, janvier 2002.

F. Laroussinie. *Logique temporelle avec passé pour la spécification et la vérification des sytèmes réactifs.* PhD thesis, Institut National Polytechnique de Grenoble, Novembre 1994.

P. Lopez. *Analyse énergétique pour l'ordonnancement de tâches sous contraintes de temps et de ressources.* PhD thesis, Université Paul Sabatier, Toulouse, Septembre 1991.

M. Mabrouk, Y. Sallez, et R. Soenen. Toward a tool for aiding reconfiguration of production automated systems. Dans *IMACS Multiconference, Computational Engineering in Systems Applications, CESA'96*, Lille, France, Juillet 1996.

M.Combacau, M. Da Silveira, et A.Boufaied. Prognosis and recovery evaluation in flexible manufacturing systems supervision. Dans *International Conference on Industrial Engineering and Production Management (IEPM'2001)*, Quebec, Canada, 20-23 Août 2001.

M.Combacau, E. Zamaï, et A. Chaillet-Subias. Monitoring strategies as control structures of monitoring architectures based on discrete event systems. Dans *Computational Engineeroig in System Applications (CESA 1998)*, Nabeul-Hammamet, TUNISIE, 1-4 Avril 1998.

Ministère de l'Économie des Finances et de l'Industrie MEFI. *100 normes clés pour la France de l'an 2000.* Editions de l'Industrie, 1999.

H. Méndez, D. Alligier, E. Zamaï, et B. Descotes-Genon. Supervisory monitoring and control for manufacturing processes. Dans *IFAC SAFEPROCESS 2000*, Budapest, Hongrie, 14-16 juin 2000a.

H. Méndez, E. Zamaï, et B. Descotes-Genon. Supervisory monitoring and control of complex discrete event systems. Dans *Second Conférence on Management and Control of Production and Logistics (MCPL'2000)*, pages 327–332, Grenoble, France, 5-8 juillet 2000b.

H. Méndez, E. Zamaï, et B. Descotes-Genon. Integration of economical, ecological, safety and quality constraints in the design of monitoring strategies. Dans *10th IFAC Symposium on Information Control Problems in Manufacturing (INCOM 2001)*, Vienne, Autriche, 20-22 septembre 2001.

H. Méndez, E. Zamaï, et B. Descotes-Genon. Design of monitoring strategies. Dans *2002 IEEE Conference on Systems; Man and Cybernetics (SMC'02)*, Hammammet, Tunisia, 6-9 octobre (à apparaître) 2002a.

H. Méndez, E. Zamaï, et B. Descotes-Genon. Synthesis of a reference model for the design of monitoring strategies. Dans *2002 Japan-USA Symposium on Flexible Automation (2002 JUSFA)*, Hiroshima, Japon, 15-17 juillet 2002b.

S. Moreno et E. Peulot. *le GEMMA - Guide d'Etude des Modes de Marches et d'Arrêts*. Educalivre, Paris, France, Septembre 1997.

E. Niel, L. Pietrac, et L. Regimbal. Advantages and drawbacks of the logic program synthesis using supervisory control theory. Dans *10th IFAC Symposium on information Control Problems in Manufacturing (INCOM 2001)*, Vienna, Austria, 20-22 september 2001.

E. Niel, N. Rezg, M. Nourelfath, et S. Boukohbza. Supervisory control in the context of operational safety reactivity. Dans *IMACS Multiconference, Computational Engineering in Systems Applications, CESA'96*, Lille, France, Juillet 1996.

M. Nourelfath et E. Niel. Contribution à la surveillance des systèmes automatisés de production. *Journal Européen des Systèmes Automatisés (JESA)-Automatique, Productique et Informatique Industrielle*, 14 (2-3):105–124, Avril 2000.

P-J. O'Grady, Y. Kim, et R-E. Young. A hierarchical approach to concurrent engineering systems. *Computer Integrated Manufacturing*, 7:152–162, 1994.

T. Parayre. *Le MESAP : vers une Méthodologie d'Exploitation des Systèmes Automatisés de Production*. PhD thesis, Université de Valenciennes et du Hainaut Cambresis, 1992.

C. Pourcel. *Systèmes automatisés de production*. Cepandues - Editions, Toulouse, France, Décembre 1986.

J.P. Ramadge et W.M. Wonham. Supervisory control of class of discrete event processes. *SIAM J. Control and Optimization*, 25, Janvier 1987.

P. Ramadge et W. Wohanm. The control of discrete event systems. *Proceedings of the IEEE*, 77(1):81–97, 1989.

L. Regimbal. Applicabilité de la théorie de contrôle par supervision : proposition d'une approche d'implantation décentralisée. Technical report, Conservatoire National des Arts et Metiers, Lyon, France, 2002.

J.-M. Roussel. *Analyse de Grafcets par génération logique de l'automate equivalent.* PhD thesis, Ecole Normale Supérieure de Cachan, décembre 1994.

A. E. K. Sahraoui. *Sur la surveillance des ateliers flexibles.* PhD thesis, Université Paul Sabatier, Toulouse, Octobre 1987.

M. Sampath, S. Lafortune, et D. Teneketzis. Active diagnosis of discrete-event systems. *IEEE Transaction on automatic control*, 43 (7):908–928, july 1998.

M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, et D. Teneketzis. Failure diagnosis using discrete-event models. *IEEE Transaction on control systems technology*, 4 (2):105–124, March 1996.

P. Sarri. *Stabilisation optimale des systèmes à événements discrets à structure vectorielle : application à la sécurité opérationnelle des systèmes de production.* PhD thesis, Institut National des Sciences Appliquées de Lyon, 20 janvier 1999.

P. Séébold. *Théorie des automates.* Viubert, Cahors, France, 1999.

C. Sourisse et L. Boudillon. *La sécurité des machines automatisées, Tome 1.* Groupe Schneider, 1996.

SPSF, M. Combacau, P. Berruet, P. Charbonnaud, et A. Khatab. Réflexions sur la terminologie surveillance - supervision. Technical report, Systèmes de Production Sûrs de Fonctionnement, 1999.

R. Tawegoum. *Contrôle Temps Réel du Déroulement des Opérations dans les Systèmes de Production Flexibles.* PhD thesis, Université des Sciences et Technologies de Lille, Avril 1995.

A-K-A. Toguyeni. *Surveillance et Diagnostic en Ligne dans les Systèmes Flexibles de l'Industrie Manufacturière.* PhD thesis, Université de Lille I, Novembre 1992.

A-K-A. Toguyeni, S. El Kahttabi, et E. Craye. Functional and/or structural approach for the supervision of flexible manufactuirng systems. Dans *IMACS Multiconference, Computational Engineering in Systems Applications, CESA'96*, Lille, France, Juillet 1996.

P. Tona. *Conception de systèmes de commande avancée par calculateur : méthodologie et applications.* PhD thesis, Institut National Polytechnique de Grenoble, Janvier 2000.

R. Valette. Petri Nets for Control and Monitoring: Specification, Verification, Implementation. Dans *Analysis and Design of Event-Driven Operations in Process Systems*, Imperial College, Centre for Process Systems Engineering, London, Avril 1995.

R. Valette. Les réseaux de petri. notes des cours, Septembre 2001.

C. Verlinde. *Contribution à l'étude des architectures de systèmes automatisés.* PhD thesis, Institut National Polytechnique de Lorraine, NANCY, 1989.

VIDAL. *VIDAL 2002, Le Dictionnaire.* VIDAL, Paris, France, 2002.

E. Zamaï. *Architecture de Surveillance-Commande pour les Systèmes à Evénements Discrets Complexes.* PhD thesis, Université Paul Sabatier, Toulouse, Septembre 1997.

E. Zamaï, A. Chaillet-Subias, et M. Combacau. An architecture for control and monitoring of discrete event systems. *Computers in Industry, Elsevier*, 36:95–100, 1998a.

E. Zamaï, A. Chaillet-Subias, M. Combacau, et A. de Bonneval. A hierarchical structure for control of discrete events systems and monitoring of process failures. *Studies in Informatics and Control*, 6, Number 1:7–15, 1997.

E. Zamaï, M. Combacau, et A. Chaillet-Subias. Models for monitoring and control of discrete events systems. Dans *9th Symposium on Information Control in Manufacturing*, Nancy-Metz, France, Juin 1998b.

Eric Zamaï. Intégration et développement de nouvelles technologies pour le pilotage et la supervision temps réel d'ateliers manufacturiers. Technical report, Laboratoire d'Automatique de Grenoble (LAG), 2001.

Eric Zamaï, Zdeneck Hanzalek, et Mireille Jacomino. Hardware and software prototype for supervision, monitoring and control structure. poster, 5-8 juillet 2000.

J. Zaytoon, J.-J. Lesage, L. Marce, J.-M. Faure, et P. Lhoste. Vérification et validation du grafcet. *Journal Européen des Systèmes Automatisés, AFCET/Hermes*, 31 (4):713–740, 1997.

Annexes

Annexe 1 : liste des activités de référence

Nous présentons au sein de cette annexe l'ensemble des 98 activités de référence reconnues utilisables, structurées autour des 17 modes de marches et d'arrêts. La notation proposée par E. Zamaï dans sa thèse a été étendue pour prendre en compte l'élément nouveau (mode) :

Mode $= HS, F1, F2, F3, F4, F5, F6, A1, A2, A3, A4, A5, A6, A7, D1, D2, D3,$

Ressource $= R,$

Produit $= P,$

Détection $= Dt,$

Suivi $= Sv,$

Commande $= Cd,$

Diagnostic $= Dg,$

Décision $= Dc,$

Reprise $= Rp,$

Urgence $= Ug.$

- Mode HS; P.C. Hors énergie (Hors service):
  - <> Aucun élément de surveillance n'est actif, le système se trouve hors service.
- Mode F1 (Fonctionnement normal) :
  - $< F1, R, P, Dt, Sv, Cd >$: production optimale qui caractérise la transformation normale d'un produit,
  - $< F1, R, Dt, Sv, Cd >$: les capteurs de présence produit n'étant pas toujours disponibles, cette activité représente également une production optimale sans prendre en compte le produit.
  - $< F1, R, P, Dt, Sv, Cd, Dg >$: puisque le système reste en mode F1, le diagnostic ne travaille évidemment pas sur une défaillance locale à la ressource. Cette activité modélise donc forcément un diagnostic détaillé en réponse à une requête de diagnostic (phénomène classique d'une propagation de défaillance). Nous noterons au passage que la prise en compte du mode résout le problème d'indéterminisme de l'activité $< R, P, Dt, Sv, Cd, Dg >$ proposée dans le modèle de référence de Zamaï [1997].

- $< F1, R, Dt, Sv, Cd, Dg >$: situation similaire à la précédente sans que le produit ne soit associé à la ressource.
- $< F1, R, P, Dt, Sv, Cd, Dc >$: cette activité est la suite logique de $< F1, R, P, Dt, Sv, Cd, Dg >$. Suite au résultat de diagnostic, une décision est prise.
- $< F1, R, Dt, Sv, Cd, Dc >$: même signification que l'activité précédente sans considérer ici le produit transformé.

- Mode F2 (Marche de préparation) :
  - $< F2, R, P, Dt, Sv, Cd >$: le système de commande prépare la ressource à une production normale. La présence du produit est nécessaire à cette marche.
  - $< F2, R, Dt, Sv, Cd >$: même caractéristique que l'activité précédente mis à part le fait que le produit n'est pas requis pour exécuter la marche de préparation.
  - $< F2, R, P, Dt, Sv, Cd, Dg >$: activité $< F2, R, P, Dt, Sv, Cd >$ répondant de surcroît à une requête de diagnostic du niveau supérieur.
  - $< F2, R, Dt, Sv, Cd, Dg >$: idem sans le produit,
  - $< F2, R, P, Dt, Sv, Cd, Dc >$: prise de décision faisant suite au résultat de diagnostic élaboré au cours de l'activité $< F2, R, P, Dt, Sv, Cd, Dg >$.
  - $< F2, R, Dt, Sv, Cd, Dc >$: idem, mais le produit n'est pas considéré.

- Mode F3 (Marche de clôture) :
  - $< F3, R, P, Dt, Sv, Cd >$: la marche de clôture est exécutée par le système de commande (nettoyage de la ressource, retrait du produit transformé, etc.).
  - $< F3, R, Dt, Sv, Cd >$: idem activité précédente, le produit étant désormais retiré.
  - $< F3, R, P, Dt, Sv, Cd, Dg >$: en sus de la marche de clôture, un diagnostic est lancé en réponse à une requête de niveau supérieur.
  - $< F3, R, Dt, Sv, Cd, Dg >$: idem sans le produit.
  - $< F3, R, P, Dt, Sv, Cd, Dc >$: une décision est prise suite au résultat de diagnostic délivré durant l'activité $< F3, R, P, Dt, Sv, Cd, Dg >$.
  - $< F3, R, Dt, Sv, Cd, Dc >$: idem sans le produit.

- Mode F4 (Marche de vérification dans le désordre) :
  - $< F4, R, P, Dt, Sv >$: même si la vérification est exécutée par un opérateur humain via un pupitre de contrôle, il n'en demeure pas moins qu'il faut surveiller (Dt, Sv) la ressource afin de parer à toute défaillance.
  - $< F4, R, Dt, Sv >$: idem sans le produit.
  - $< F4, R, P, Dt, Sv, Dg >$: même en phase de vérification manuelle, le niveau supérieur peut toujours émettre une requête de diagnostic détaillé (Chaillet [1995]).
  - $< F4, R, Dt, Sv, Dg >$: idem, sans le produit.
  - $< F4, R, P, Dt, Sv, Dc >$: toujours en phase de vérification manuelle, la fonction décision analyse les résultats délivrés par le diagnostic.
  - $< F4, R, Dt, Sv, Dc >$: idem sans le produit.

- Mode F5 (Marche de vérification dans l'ordre) :
  - $< F5, R, P, Dt, Sv, Cd >$: ici, la vérification est réalisée en mode automatique à travers le système de commande. Notons qu'un produit est requis pour exécuter cette vérification.
  - $< F5, R, Dt, Sv, Cd >$: idem, sans que le produit soit nécessaire.
  - $< F5, R, P, Dt, Sv, Cd, Dg >$: cas classique d'un diagnostic détaillé lancé en parallèle à la marche de vérification dans l'ordre.
  - $< F5, R, Dt, Sv, Cd, Dg >$: idem, sans le produit.
  - $< F5, R, P, Dt, Sv, Cd, Dc >$: la décision analyse les résultats du diagnostic délivrés au cours de l'activité $< F5, R, P, Dt, Sv, Cd, Dg >$.
  - $< F5, R, Dt, Sv, Cd, Dc >$: idem sans le produit.
- Mode F6 (Marche de test) :
  - $< F6, R, P, Dt, Sv, Cd >$: le système de commande exécute les séquences classiques de réglages et/ou étalonnages périodiques. Le produit est requis pour faire ces réglages.
  - $< F6, R, Dt, Sv, Cd >$: idem, mais le produit n'est pas nécessaire à l'opération de réglage.
  - $< F6, R, P, Dt, Sv, Cd, Dg >$: cas désormais classique d'un diagnostic détaillé lancé en parallèle avec la phase de test.
  - $< F6, R, Dt, Sv, Cd, Dg >$: pendant de l'activité précédente, sans le produit.
  - $< F6, R, P, Dt, Sv, Cd, Dc >$: une décision fait suite au résultat de diagnostic fourni au cours de l'activité $< F6, R, P, Dt, Sv, Cd, Dg >$.
  - $< F6, R, Dt, Sv, Cd, Dc >$: idem sans le produit.
- Mode A1 (Arrêt dans l'état initial) :
  - $< A1, R, Dt, Sv >$: cette activité est qualifiée comme "activité minimale de surveillance-commande-supervision". *Cette terminologie véhicule bien le sens de cette activité. La situation exprimée par cette activité correspond à la non exploitation des services offerts par la ressource considérée. Toutefois, ce n'est pas parce que cette ressource physique n'est pas exploitée qu'aucune évolution n'est observable. Si un opérateur est amené à intervenir sur cette ressource, cette dernière risque d'évoluer en entraînant le déclenchement intempestif des capteurs qui lui sont associés. Le même cas de figure peut se présenter, par exemple, suite à une collision entre deux chariots, l'un commandé, l'autre non. Ainsi le système de surveillance/commande doit être capable de détecter d'éventuelles évolutions et de représenter au mieux l'occurrence de ces événements grâce à la fonction suivi"* (Zamaï [1997]).
  - $< A1, R, Dt, Sv, Dg >$: un diagnostic, demandé par le niveau supérieur est en cours d'exécution.
  - $< A1, R, Dt, Sv, Dc >$: une décision est en train d'être prise afin d'interpréter les résultats obtenus pendant la phase de diagnostic.
- Mode A2 (Arrêt demandé en fin de cycle) :
  - $< A2, R, P, Dt, Sv, Cd >$: un arrêt dans l'état initial a été demandé. Le système de commande tente d'atteindre cet objectif.
  - $< A2, R, Dt, Sv, Cd >$: idem, sans le produit.

- $< A2, R, P, Dt, Sv, Cd, Dg >$: cas classique de l'exécution d'un diagnostic détaillé faisant suite à une requête du niveau supérieur.
- $< A2, R, Dt, Sv, Cd, Dg >$: idem, sans le produit.
- $< A2, R, P, Dt, Sv, Cd, Dc >$: une prise de décision fait suite aux résultats de diagnostic délivrés au cours de l'activité $< A2, R, P, Dt, Sv, Cd, Dg >$.
- $< A2, R, Dt, Sv, Cd, Dc >$: idem, sans le produit.

- Mode A3 (Arrêt demandé dans état déterminé) :
  - $< A3, R, P, Dt, Sv, Cd >$: le système de commande place la ressource dans un état d'arrêt déterminé. Un produit est en cours de transformation.
  - $< A3, R, Dt, Sv, Cd >$: idem, sans le produit.
  - $< A3, R, P, Dt, Sv, Cd, Dg >$: en parallèle à la mise à l'arrêt, un diagnostic détaillé est en cours d'exécution. Cela ne veut donc pas dire que la ressource est en situation de défaillance!
  - $< A3, R, Dt, Sv, Cd, Dg >$: idem, sans le produit.
  - $< A3, R, P, Dt, Sv, Cd, Dc >$: une prise de décision fait suite au résultat de diagnostic élaboré au cours de l'activité $< A3, R, P, Dt, Sv, Cd, Dg >$.
  - $< A3, R, Dt, Sv, Cd, Dc >$: idem, sans le produit.

- Mode A4 (Arrêt obtenu) :
  - $< A4, R, P, Dt, Sv >$: la ressource est à l'arrêt dans un état différent de celui initial. Un produit est associé à la machine.
  - $< A4, R, Dt, Sv >$: idem, sans le produit.
  - $< A4, R, P, Dt, Sv, Dg >$: le système de surveillance-commande-supervision répond à une demande de diagnostic détaillé alors que la ressource est à l'arrêt.
  - $< A4, R, Dt, Sv, Dg >$: idem, sans le produit.
  - $< A4, R, P, Dt, Sv, Dc >$: prise de décision suite à un diagnostic détaillé, le tout en phase d'arrêt de la ressource.
  - $< A4, R, Dt, Sv, Dc >$: idem, sans le produit.

- Mode A5 (Préparation pour remise en route après défaillance) :
  - $< A5, R, P, Dt, Sv, Rp >$: une séquence de reprise est en cours d'exécution afin de ramener la ressource dans un état de reprise.
  - $< A5, R, Dt, Sv, Rp >$: idem, sans le produit.
  - $< A5, R, P, Dt, Sv, Dg, Rp >$: cas classique d'un diagnostic détaillé demandé par le niveau supérieur.
  - $< A5, R, Dt, Sv, Dg, Rp >$: idem, sans le produit.
  - $< A5, R, P, Dt, Sv, Dc, Rp >$: prise de décision faisant suite aux résultats de diagnostic générés durant l'activité $< A5, R, P, Dt, Sv, Dg, Rp >$
  - $< A5, R, Dt, Sv, Dc, Rp >$: idem, sans le produit.

- Mode A6 (Mise P.O. dans état initial) :
  - $< A6, R, P, Dt, Sv, Rp >$: fin de séquence de reprise nécessitant des réglages particuliers avant de déclarer la ressource "apte au service".
  - $< A6, R, Dt, Sv, Rp >$: idem, sans le produit.

- $< A6, R, P, Dt, Sv, Dg, Rp >$: cas classique d'un diagnostic détaillé demandé par le niveau supérieur.
- $< A6, R, Dt, Sv, Dg, Rp >$: idem, sans le produit.
- $< A6, R, P, Dt, Sv, Dc, Rp >$: une prise de décision est lancée en réponse aux résultats de diagnostic élaborés durant l'activité $< A6, R, P, Dt, Sv, Dg, Rp >$.
- $< A6, R, Dt, Sv, Dc, Rp >$: idem, sans le produit.

- Mode A7 (Mise P.O. dans état déterminé) :
  - $< A7, R, P, Dt, Sv, Rp >$: la fonction reprise est en train d'exécuter des opérations supplémentaires afin de mettre la ressource dans un état spécifique avant d'autoriser une éventuelle poursuite de la production.
  - $< A7, R, Dt, Sv, Rp >$: idem, sans le produit.
  - $< A7, R, P, Dt, Sv, Dg, Rp >$: un diagnostic détaillé est demandé par le niveau supérieur alors que la ressource est en cours de reprise.
  - $< A7, R, Dt, Sv, Dg, Rp >$: idem, sans le produit.
  - $< A7, R, P, Dt, Sv, Dc, Rp >$: prise de décision faisant suite à la génération d'un résultat de diagnostic.
  - $< A7, R, Dt, Sv, Dc, Rp >$: idem, sans le produit.

- Mode D1 (Arrêt d'urgence) :
  - $< D1, R, P, Dt, Sv, Dg, Ug >$: exécution d'une séquence d'urgence afin d'assurer l'intégrité des opérateurs et/ou de la ressource. Le diagnostic est lancé en parallèle (Zamaï et al. [1998b]) afin d'optimiser le traitement de la défaillance. Nous noterons, que la ressource n'était pas en cours d'utilisation lors de l'occurrence de la défaillance.
  - $< D1, R, Dt, Sv, Dg, Ug >$: idem, sans le produit.
  - $< D1, R, P, Dt, Sv, Dc, Ug >$: exécution de la fonction décision suite à l'obtention de résultats de diagnostic élaborés durant l'activité $< D1, R, P, Dt, Sv, Dg, Ug >$.
  - $< D1, R, Dt, Sv, Dc, Ug >$: idem, sans le produit.
  - $< D1, R, P, Dt, Sv, Cd, Dg, Ug >$: suite à l'occurrence d'une défaillance critique (sur-course par exemple) au cours d'une séquence de commande, une procédure d'urgence prioritaire est lancée.
  - $< D1, R, Dt, Sv, Cd, Dg, Ug >$: idem, sans le produit.
  - $< D1, R, P, Dt, Sv, Cd, Dc, Ug >$: une prise de décision est en cours faisant suite au diagnostic élaboré au cours de l'activité $< D1, R, P, Dt, Sv, Cd, Dg, Ug >$.
  - $< D1, R, Dt, Sv, Cd, Dc, Ug >$: idem, sans le produit.
  - $< D1, R, P, Dt, Sv, Dg, Rp, Ug >$: exécution d'une procédure d'urgence suite à l'occurrence d'une défaillance détectée au cours d'une séquence de reprise. Le diagnostic est bien entendu également lancé afin d'optimiser la phase de retour en fonctionnement normal.
  - $< D1, R, Dt, Sv, Dg, Rp, Ug >$: idem, sans le produit.
  - $< D1, R, P, Dt, Sv, Dc, Rp, Ug >$: une prise de décision est en cours pour envisager une reprise de la reprise en cours. Dans le modèle de référence, nous nous refusons de limiter ce type de récursivité. Ceci fait partie de la stratégie qu'aura à mettre en oeuvre l'industriel.

  - $< D1, R, Dt, Sv, Dc, Rp, Ug >$: idem, sans le produit.

- Mode D2 (Diagnostic et ou traitement des défaillances) :
  - $< D2, R, P, Dt, Sv, Dg >$: ceci correspond à l'activité classique de diagnostic d'une défaillance alors que le système de commande est bloqué.
  - $< D2, R, Dt, Sv, Dg >$: idem, sans le produit.
  - $< D2, R, P, Dt, Sv, Dc >$: prise de décision classique suite à l'élaboration d'un résultat de diagnostic au cours de l'activité $< D2, R, Dt, Sv, Dg >$.
  - $< D2, R, Dt, Sv, Dc >$: idem, sans le produit.

- Mode D3 (Production forcée) :
  - $< D3, R, P, Dt, Sv, Cd, Dg >$: cette activité est la plus caractéristique d'une production forcée. Elle indique clairement que le système de commande continue à réaliser son service alors que la fonction diagnostic "surveille de plus prés" la ressource.
  - $< D3, R, Dt, Sv, Cd, Dg >$: idem, sans le produit.
  - $< D3, R, P, Dt, Sv, Cd, Dc >$: une décision est prise ("en fait, tout va bien!", ou bien "il y avait bien un problème!") faisant suite au résultat de diagnostic généré au cours de l'activité $< D3, R, P, Dt, Sv, Cd, Dg >$.
  - $< D3, R, Dt, Sv, Cd, Dc >$: idem, sans le produit.
  - $< D3, R, P, Dt, Sv, Cd >$: il a été décidé d'ignorer les défaillances détectées. La production se poursuit, mais cette fois en marche forcée. La fonction détection devra donc tolérer certaines défaillances afin d'éviter le phénomène classique de déclenchement d'alarmes en cascade.
  - $< D3, R, Dt, Sv, Cd >$: idem, sans le produit.

Annexe 2 : liste des processus de référence

Le lecteur trouvera dans cette annexe la table de transitions qui représente l'ensemble des évolutions utilisables contenues dans le Modèle de Référence pour la supervision, la surveillance et la commande. Dans cette table, chaque ligne est associée à une activité de référence et les colonnes représentent les événements susceptibles de se produire. L'intersection ligne/colonne indique l'ensemble des états atteignables à partir d'une activité de référence et pour l'occurrence d'un événement.

α		= *Requête de commande*
β		= *Requête de diagnostic*
γ		= *Requête de reprise*
η		= *Requête d'urgence*
μ		= *Résultat de commande*
θ		= *Résultat de détection*
ω		= *Résultat de diagnostic*
υ		= *Résultat de décision*
τ		= *Résultat de reprise*
ϕ		= *Résultat d'urgence*
ψ		= *Détection de produit*
ON		= *Mise en tension de la ressource*

Activité	Etat	α	β	γ	η	μ	θ	ω	υ	τ	ϕ	ψ	ON
<HS,R>	0												37
<F1,R,Dt,Sv,Cd>	1	{13,25,31,40,46}	3	88	78	37	{78,88,94}					2	
<F1,R,P,Dt,Sv,Cd>	2	{14,26,32,41,47}	4	89	79	37	{79,89,95}					1	
<F1,R,Dt,Sv,Cd,Dg>	3	{15,27,33,42,47}		88	78	38	{78,88,94}	5				4	
<F1,R,P,Dt,Sv,Cd,Dg>	4	{16,28,34,43,48}		89	79	38	{79,89,95}	6				3	
<F1,R,Dt,Sv,Cd,Dc>	5	{17,29,35,44,49}		90	82	39	{82,90,96}		1			6	
<F1,R,P,Dt,Sv,Cd,Dc>	6	{18,30,36,45,50}		91	83	39	{83,91,97}		2			5	
<F2,R,Dt,Sv,Cd>	7	{1,25,31}	9	88	78		{78,88,94}					8	
<F2,R,P,Dt,Sv,Cd>	8	{2,26,32}	10	89	79		{79,89,95}					7	
<F2,R,Dt,Sv,Cd,Dg>	9	{3,27,33}		88	78		{78,88,94}	11				10	
<F2,R,P,Dt,Sv,Cd,Dg>	10	{4,28,34}		89	79		{79,89,95}	12				9	
<F2,R,Dt,Sv,Cd,Dc>	11	{5,29,35}		90	82		{82,90,96}		7			12	
<F2,R,P,Dt,Sv,Cd,Dc>	12	{6,30,36}		91	83		{83,91,97}		8			11	
<F3,R,Dt,Sv,Cd>	13		15	88	78	37	{78,88}					14	
<F3,R,P,Dt,Sv,Cd>	14		16	89	79	37	{79,89}					13	
<F3,R,Dt,Sv,Cd,Dg>	15			88	78	38	{78,88}	17				16	
<F3,R,P,Dt,Sv,Cd,Dg>	16			89	79	38	{79,89}	18				15	
<F3,R,Dt,Sv,Cd,Dc>	17			90	82	39	{80,90}		13			18	
<F3,R,P,Dt,Sv,Cd,Dc>	18			91	83	39	{81,91}		14			17	
<F4,R,Dt,Sv>	19	{1,25,31}	21	88	78	37	{76,88}					20	
<F4,R,P,Dt,Sv>	20	{2,26,32}	22	89	79	37	{77,89}					19	
<F4,R,Dt,Sv,Dg>	21	{3,27,33}		88	78	38	{76,88}	23				22	
<F4,R,P,Dt,Sv,Dg>	22	{4,28,34}		89	79	38	{77,89}	24				21	
<F4,R,Dt,Sv,Dc>	23	{5,29,35}		90	82	39	{78,90}		19			24	
<F4,R,P,Dt,Sv,Dc>	24	{6,30,36}		91	83	39	{79,91}		20			23	
<F5,R,Dt,Sv,Cd>	25	{1,13,19,31,40,46}	27	88	78	37	{78,88}					26	
<F5,R,P,Dt,Sv,Cd>	26	{2,14,20,32,41,47}	28	89	79	37	{79,89}					25	
<F5,R,Dt,Sv,Cd,Dg>	27	{3,15,21,33,42,48}		88	78	38	{78,88}	29				28	
<F5,R,P,Dt,Sv,Cd,Dg>	28	{4,16,22,34,43,49}		89	79	38	{79,89}	30				27	
<F5,R,Dt,Sv,Cd,Dc>	29	{5,17,23,35,44,49}		90	82	39	{82,90}		25			30	
<F5,R,P,Dt,Sv,Cd,Dc>	30	{6,18,24,36,45,50}		91	83	39	{83,91}		26			29	
<F6,R,Dt,Sv,Cd>	31	{1,13,19,25,40,46}	33	88	78	37	{78,88}					32	
<F6,R,P,Dt,Sv,Cd>	32	{2,14,20,26,41,47}	34	89	79	37	{79,89}					31	
<F6,R,Dt,Sv,Cd,Dg>	33	{3,15,21,27,42,48}		88	78	38	{78,88}	35				34	
<F6,R,P,Dt,Sv,Cd,Dg>	34	{4,16,22,28,43,49}		89	79	38	{79,89}	36				33	
<F6,R,Dt,Sv,Cd,Dc>	35	{5,17,23,29,44,49}		90	82	39	{82,90}		31			36	
<F6,R,P,Dt,Sv,Cd,Dc>	36	{6,18,24,30,45,50}		91	83	39	{83,91}		32			35	

Activité	Etat	α	β	γ	η	μ	θ	ω	υ	τ	ϕ	ψ	ON
<A1,R,Dt,Sv>	37	{1,2,7,8,19,20,25,26,31,32,}	38	88	76		{76,88}						
<A1,R,Dt,Sv,Dg>	38	{3,4,9,10,21,22,27,28,33,34}		88	76		{76,88}	39					
<A1,R,Dt,Sv,Dc>	39	{5,6,11,12,23,24,29,30,35,36}		90	80		{80,90}		37				
<A2,R,Dt,Sv,Cd>	40	13	42	88	78	37	{78,88}					41	
<A2,R,P,Dt,Sv,Cd>	41	14	43	89	79	37	{79,89}					40	
<A2,R,Dt,Sv,Cd,Dg>	42	15		88	78	38	{78,88}	44				43	
<A2,R,P,Dt,Sv,Cd,Dg>	43	16		89	79	38	{79,89}	45				42	
<A2,R,Dt,Sv,Cd,Dc>	44	17		90	82	39	{82,90}		40			45	
<A2,R,P,Dt,Sv,Cd,Dc>	45	18		91	83	39	{83,91}		41			44	
<A3,R,Dt,Sv,Cd>	46	13	48	88	78	52	{78,88}					47	
<A3,R,P,Dt,Sv,Cd>	47	14	49	89	79	53	{79,89}					46	
<A3,R,Dt,Sv,Cd,Dg>	48	15		88	78	54	{78,88}	50				49	
<A3,R,P,Dt,Sv,Cd,Dg>	49	16		89	79	55	{79,89}	51				48	
<A3,R,Dt,Sv,Cd,Dc>	50	17		90	82	56	{82,90}		46			51	
<A3,R,P,Dt,Sv,Cd,Dc>	51	18		91	83	57	{83,91}		47			50	
<A4,R,Dt,Sv>	52	{1,19,25,31}	54	88	76		{76,88}					53	
<A4,R,P,Dt,Sv>	53	{2,20,26,32}	55	89	77		{77,89}					52	
<A4,R,Dt,Sv,Dg>	54	{3,21,27,33}		88	76		{76,88}	56				56	
<A4,R,P,Dt,Sv,Dg>	55	{4,22,28,34}		89	77		{77,89}	57				55	
<A4,R,Dt,Sv,Dc>	56	{5,23,29,35}		90	80		{78,90}		52			58	
<A4,R,P,Dt,Sv,Dc>	57	{6,24,30,36}		91	81		{79,91}		53			57	
<A5,R,Dt,Sv,Rp>	58		60		84		{84,88}			{1,7,19,25,31,64,70}		59	
<A5,R,P,DT,Sv,Rp>	59		61		85		{85,89}			{2,8,20,26,32,65,71}		58	
<A5,R,Dt,Sv,Dg,Rp>	60				84		{84,88}	62		{3,9,21,27,33,66,72}		61	
<A5,R,P,DT,Sv,Dg,Rp>	61				85		{85,89}	63		{4,10,22,28,34,67,73}		60	
<A5,R,Dt,Sv,Dc,Rp>	62				86		{86,90}		58	{5,11,23,29,35,68,74}		63	
<A5,R,P,Dt,Sv,Dc,Rp>	63				87		{87,91}		59	{6,12,24,30,36,69,75}		62	
<A6,R,Dt,Sv,Rp>	64		66		84		{84,88}			{37,84,88}		65	
<A6,R,P,DT,Sv,Rp>	65		67		85		{85,89}			{37,85,89}		64	
<A6,R,Dt,Sv,Dg,Rp>	66				84		{84,88}	68		{38,84,88}		67	
<A6,R,P,DT,Sv,Dg,Rp>	67				85		{85,89}	69		{38,85,89}		66	
<A6,R,Dt,Sv,Dc,Rp>	68				86		{86,90}		64	{39,86,90}		69	
<A6,R,P,Dt,Sv,Dc,Rp>	69				87		{87,91}		65	{40,87,91}		68	
<A7,R,Dt,Sv,Rp>	70		72		84		{84,88}			{52,84,88}		71	
<A7,R,P,DT,Sv,Rp>	71		73		85		{85,89}			{53,85,89}		70	
<A7,R,Dt,Sv,Dg,Rp>	72				84		{84,88}	74		{54,84,88}		73	
<A7,R,P,DT,Sv,Dg,Rp>	73				85		{85,89}	75		{55,85,89}		72	
<A7,R,Dt,Sv,Dc,Rp>	74				86		{86,90}		70	{56,86,90}		75	
<A7,R,P,Dt,Sv,Dc,Rp>	75				87		{87,91}		71	{57,87,91}		74	
<D1,R,Dt,Sv,Dg,Ug>	76							80				77	
<D1,R,P,Dt,Sv,Dg,Ug>	77							81				76	
<D1,R,Dt,Sv,Cd,Dg,Ug>	78							82			88	79	
<D1,R,P,Dt,Sv,Cd,Dg,Ug>	79							83			89	78	
<D1,R,Dt,Sv,Dc,Ug>	80						76		62		90	81	
<D1,R,P,Dt,Sv,Dc,Ug>	81						77		63		91	80	
<D1,R,Dt,Sv,Cd,Dc,Ug>	82						78				90	83	
<D1,R,P,Dt,Sv,Cd,Dc,Ug>	83						79				91	82	
<D1,R,Dt,Sv,Dg,Rp,Ug>	84							86	60	86	88	85	
<D1,R,P,Dt,Sv,Dg,Rp,Ug>	85							87	61	87	89	84	
<D1,R,Dt,Sv,Dc,Rp,Ug>	86						84		84	80	90	87	
<D1,R,P,Dt,Sv,Dc,Rp,Ug>	87						85		85	81	91	86	
<D2,R,Dt,Sv,Dg>	88				76		76	90				89	
<D2,R,P,Dt,Sv,Dg>	89				77		77	91				88	
<D2,R,Dt,Sv,Dc>	90				80		80		{20,26,32,38,58}			91	
<D2,R,P,Dt,Sv,Dc>	91				81		81		{19,25,31,37,59}			90	
<D3,R,Dt,Sv,Cd>	92		94	88	78	{25,31,37,41,46,}	{78,88}					93	
<D3,R,P,Dt,Sv,Cd>	93		95	89	79	{26,32,37,42,47,}	{79,89}					92	
<D3,R,Dt,Sv,Cd,Dg>	94			88	78		{78,88}	96				95	
<D3,R,P,Dt,Sv,Cd,Dg>	95			89	79		{79,89}	97				94	
<D3,R,Dt,Sv,Cd,Dc>	96			90	82		{82,90}		{1,19,25,31,41,46,58,92}			97	
<D3,R,P,Dt,Sv,Cd,Dc>	97			91	83		{83,91}		{2,20,26,32,42,47,59,93}			96	

FIG. 3.7: *Table de transitions correspondante au Modèle de Référence pour la Supervision, La surveillance et la Commande*

Exemple d'application : grilles d'évaluation complémentaires

Cette annexe présente l'ensemble de toutes les autres grilles d'évaluation qui concerne la rédaction du cahier des charges pour la synthèse d'une loi de surveillance appliquée au robot CHARLY de la plate-forme SAPHIR. Cette annexe fait ici figure de complément au chapitre 2 de la partie IV de ce mémoire. Les grilles présentées correspondent à l'évaluation des symptômes de défaillances pour les modes *Arrêt initial (A1), Marches de préparation (F2), Arrêt d'urgence (D1), Mode de diagnostic et/ou traitement de défaillances (D2), Production tout de même (D3), Préparation pour remise en route après défaillance (A5) et Mise P.O. dans l'état initial (A6)* et pour les critères sécurité, productivité et qualité. Nous noterons que les évaluations portant sur le critère *écologie* ne sont pas présentées ici car ce critère ne trouve aucun écho dans le contexte particulier de la plate-forme SAPHIR.

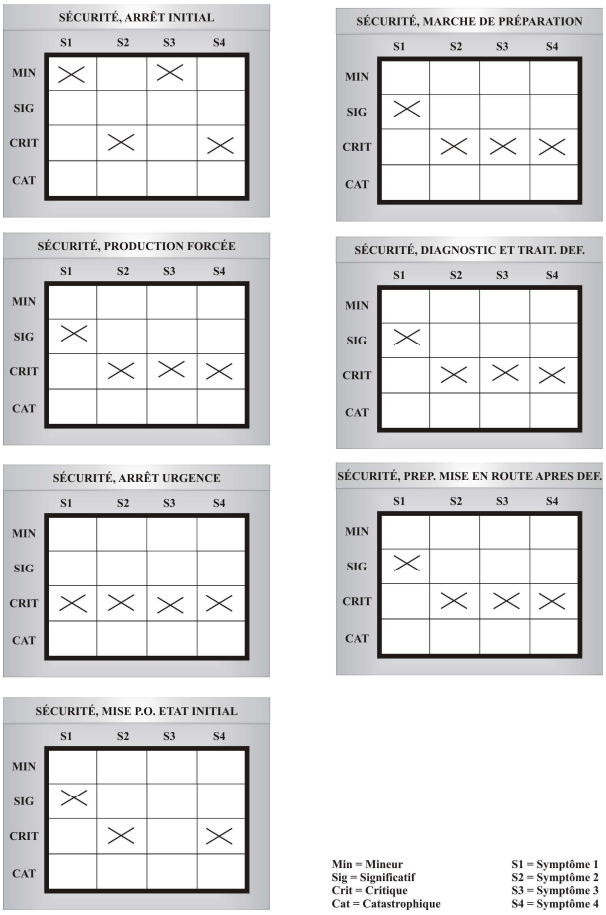

FIG. 3.8: *Grilles d'évaluation des symptômes de défaillance pour le critère* sécurité

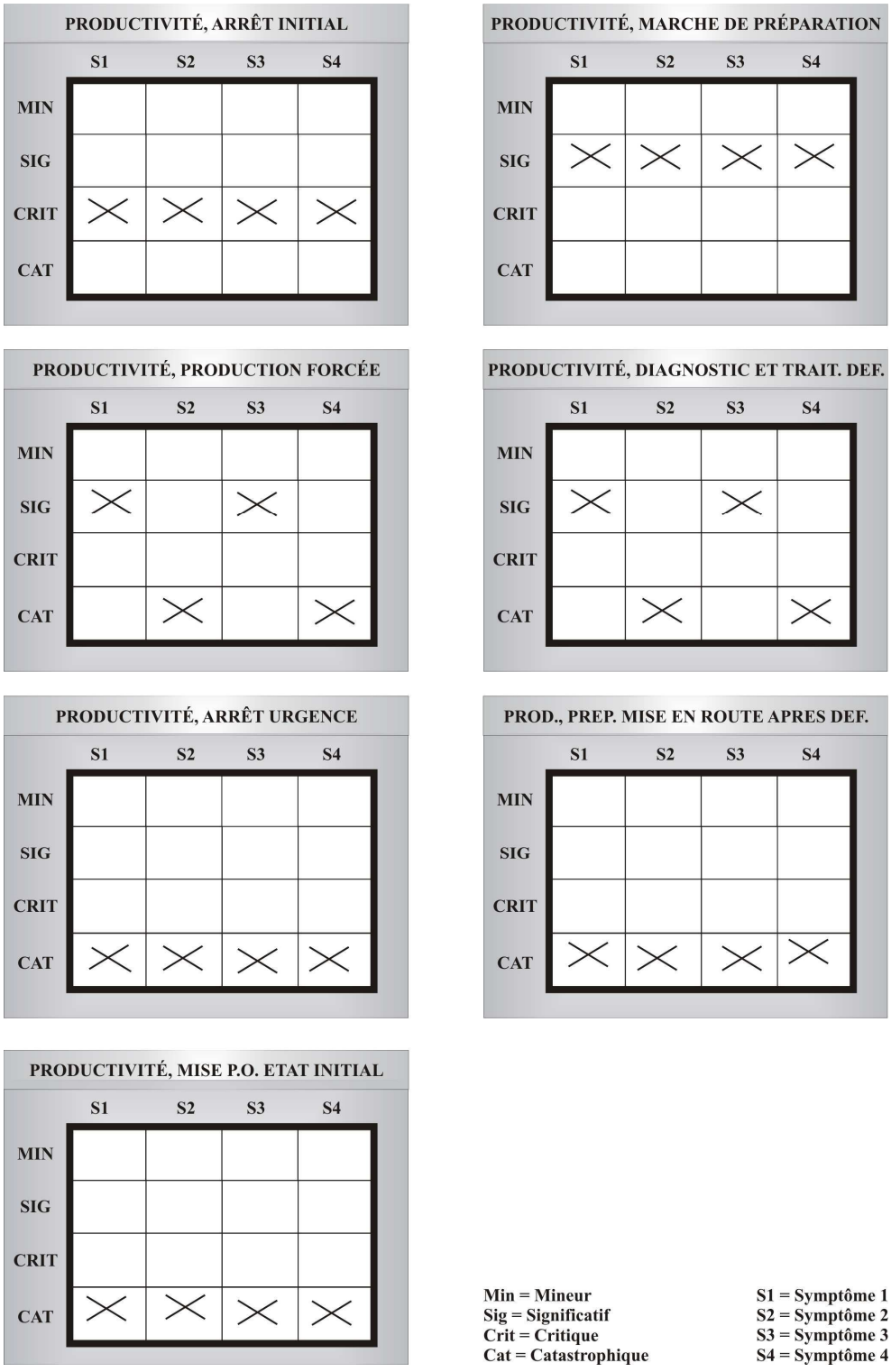

FIG. 3.9: *Grilles d'évaluation des symptômes de défaillance pour le critère* productivité

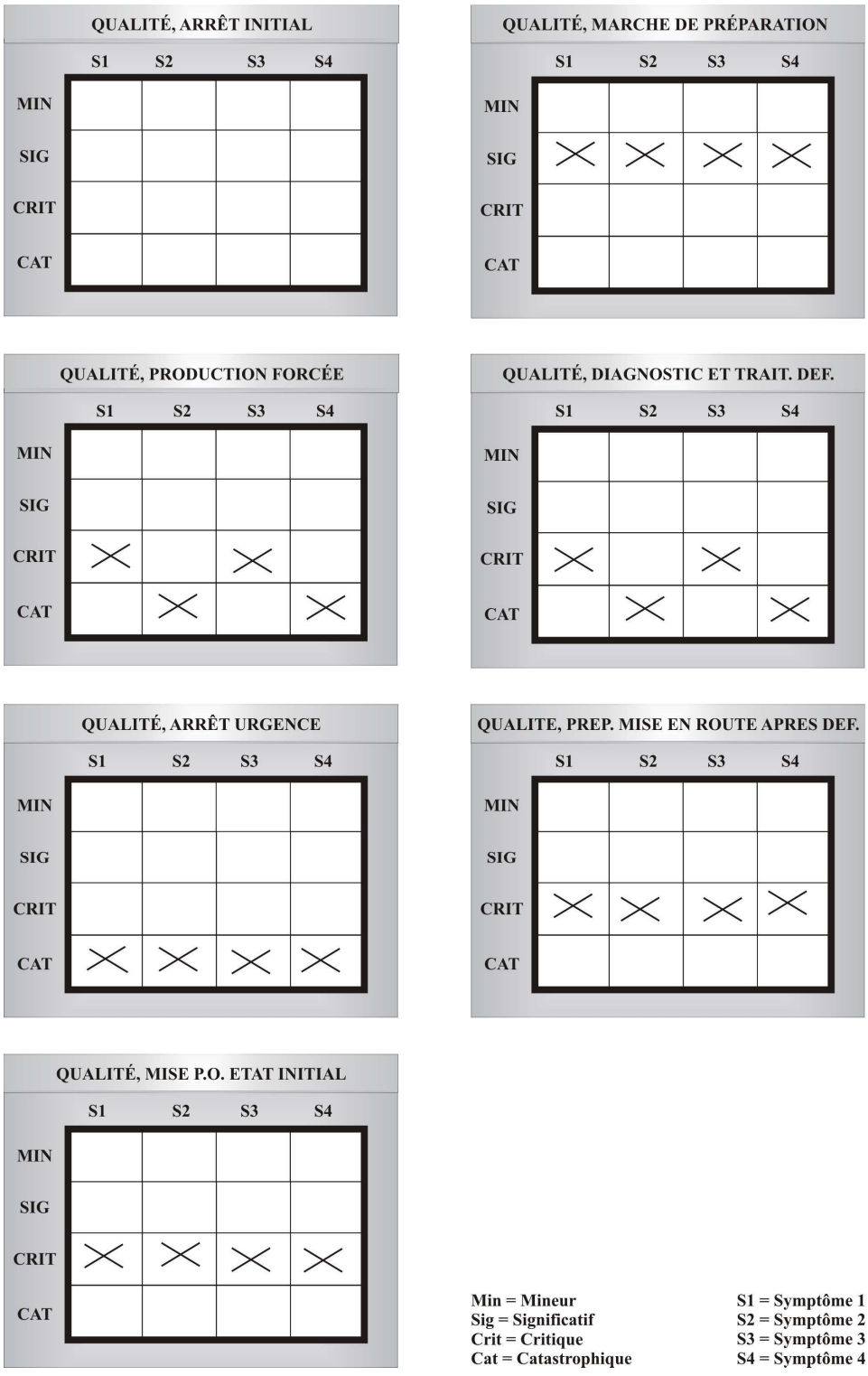

FIG. 3.10: *Grilles d'évaluation des symptômes de défaillance pour le critère* qualité

Synthèse de lois de surveillance pour les procédés industriels complexes

Résumé :

Le travail présenté dans ce mémoire s'inscrit dans le domaine de la supervision des systèmes automatisés de production. Il traite plus particulièrement de la synthèse de lois de surveillance adaptées aux exigences des entreprises. La loi de surveillance est obtenue à partir d'un modèle de référence pour la supervision, la commande et la surveillance. Ce dernier fournit l'ensemble exhaustif de tous les traitements de supervision, de commande et de surveillance qui peuvent être appliqués en situation de défaillances au cours d'un cycle de production et ce, quel que soit le système de production considéré. La méthode de synthèse proposée s'appuie sur une démarche proche de la synthèse de correcteurs en automatique continue. Elle revient à raffiner successivement le modèle de référence par intégration progressive d'un ensemble de quatre propriétés qui doivent être recherchées. Ces propriétés, la sécurité, l'écologie, la qualité et la productivité sont à évaluer par le concepteur au moyen de grilles mettant en relation l'impact de quatre symptômes de défaillances sur l'ensemble des propriétés recherchées et ce, en fonction de la ressource physique considérée.

Un exemple d'application basé sur un processus manufacturier réel, la plate-forme de recherche en productique SAPHIR du Laboratoire d'Automatique de Grenoble, illustre les apports de notre approche. Ces derniers se déclinent en terme de flexibilité des traitements proposés, de systématisation de la méthode proposée et de respect des propriétés recherchées.

Mots-clés : Supervision, Surveillance, Commande, Modes de Marches et d'Arrêts, Lois de Surveillance, Systèmes Automatisés de Production, Systèmes à Événements Discrets.

Synthesis of monitoring laws for complexe industrial processes

Abstract: This work deals with the supervision of manufacturing systems. It is mainly directed towards the synthesis of monitoring laws adapted to the industrial requirements. The monitoring law is obtained from a Supervision, Monitoring and Control Reference Model that contains the set of supervision, control and monitoring treatments that can be applied in failure situations for any manufacturing system. The synthesis method proposed is based on a process close to the one used to synthesizing self-compensating devices in the automatic control for continuous systems. This method consists in a successive refining of the reference model with a progressive integration of a set of four properties. Those properties, security, ecology, quality, and productivity must be evaluated by the user by using a set of grids establishing a relationship between the impact of four failure symptoms with the set of properties to be reached. This evaluation is related to the physical resource.

An application example based on a real manufacturing process, the SAPHIR research platform on production systems of the Laboratory of Automatics and Control of Grenoble shows the contribution of this approach. The results show the advantages of this approach characterized by flexibility in the failure treatments proposed, by a systematization of the method proposed and by the respect of the expected properties.

Keywords: Supervision, Monitoring, Control, Operating Modes, Monitoring Laws, Manufacturing Systems, Discrete Event Systems.