50376
2000
476

UNIVERSITÉ DES SCIENCES ET TECHNOLOGIES DE LILLE

THÈSE

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DES SCIENCES ET TECHNOLOGIES DE LILLE

Discipline :
PRODUCTIQUE : AUTOMATIQUE et INFORMATIQUE INDUSTRIELLE

présentée et soutenue publiquement

le 20 décembre 2000

par

Nathalie Dangoumau

UNIVERSITE DES SC. ET TECHN. LILLE
BIBLIOTHEQUE UNIVERSITAIRE

CONTRIBUTION À LA GESTION DES MODES DES SYSTÈMES AUTOMATISÉS DE PRODUCTION

directeur de thèse :

M. E. CRAYE — Professeur à l'École Centrale de Lille

JURY

Mme M. BAYART	Examinateur	Professeur à l'Université de Lille I,
M. F. CHERIAUX	Examinateur	Ingénieur – Chercheur à EDF,
M. E. CRAYE	Directeur	Professeur à l'École Centrale de Lille
M. S. EL KHATTABI	Examinateur	Maître de conférences à l'École Centrale Lille,
M. J.-M. FAURE	Rapporteur	Professeur à l'ISMCM de Saint-Ouen,
M. J.-C. GENTINA	Examinateur	Professeur à l'École Centrale de Lille,
M. P. LADET	Rapporteur	Professeur à l'ENSIEG de Grenoble.

Table des Matières

Introduction Générale 1

Contexte &Problématique

Chapitre I 7

Introduction 7

1 Les Systèmes de Production 8

1.1 Définitions 8

1.2 Le cycle de vie 10

1.3 La flexibilité 12

1.4 La complexité 16

1.5 Les Systèmes de Production étudiés 16

2 La Sûreté de Fonctionnement 17

2.1 Caractérisation de la Sûreté de Fonctionnement 17

2.2 Les entraves 19

2.2.1 Défaillances 19

2.2.2 Défaut 20

2.2.3 Classifications des entraves 21

2.2.4 Entraves prises en compte 22

2.3 Les attributs de la SdF 22

2.3.1 Fiabilité (Reliability) : 22

2.3.2 Disponibilité (Availability) : 23

2.3.3 Maintenabilité (Maintenability) : 23

2.3.4 Sécurité (Security) : 23

2.3.5 Notre besoin de sûreté 24

2.4 Les moyens 24

2.4.1 La prévention de fautes 25

2.4.2 La tolérance aux fautes 25

2.4.3 L'élimination de fautes 25

2.4.4 La prévision de fautes 26

2.4.5 Nos objectifs 26

3 Description du contexte de contrôle commande 27

3.1 La méthodologie CASPAIM 27

3.2 La Commande 28

3.2.1 Les Gammes Logiques 28

3.2.2 Les Gammes Opératoires 29

3.2.3 Intégration au contrôle-commande 29

3.3 La Planification/Ordonnancement 30

3.3.1 La Planification 31

3.3.2 Optimisation des performances 31

3.3.3 Ordonnancement cyclique du régime permanent 31

3.3.4 Ordonnancement du régime transitoire 31

3.3.5 Intégration au contrôle-commande 32

3.4 La Surveillance 32

3.4.1 Les différents types de Surveillance 32

3.4.2 Les activités de la Surveillance 34

3.4.3 Intégration au contrôle-commande 34

3.5 La Maintenance 35

3.5.1 Les stratégies de Maintenance 35

3.5.2 Les activités de la Maintenance 36

3.5.3 Intégration au contrôle-commande 37

3.6 La Supervision 37

Conclusion 39

Chapitre II 40

Introduction 40

1 Le processus de Reconfiguration 41

1.1 Du recouvrement à la reconfiguration 41

1.1.1 Introduction au recouvrement 41

1.1.2 Différentes approches 42

1.2 La reconfiguration : Constats et propositions 51

1.3 Synthèse 54

2 De la Supervision à la Gestion des Modes 58

2.1 La Supervision 58

2.1.1 Objectifs 58

2.1.2 Le Recouvrement 59

2.1.3 Le pilotage 61

2.2 La Gestion des Modes 62

2.2.1 Gestion des Modes et contrôle-commande 62
2.2.2 Le modèle OID 64
2.2.3 Gestion des Modes et modèle OID 65

2.3 Problématique 66
2.3.1 Le nombre d'intervenants 67
2.3.2 La complexité des Systèmes de Production 67
2.3.3 Cahier des Charges 68

Conclusion 69

Proposition pour la Modélisation et la Gestion des Modes des SP

Chapitre III 71

Introduction 71

1 présentation générale 72

1.1 Objectifs et Proposition 72
1.1.1 Objectifs 72
1.1.2 Proposition 73

1.2 Outil et formalisme retenus 75
1.2.1 Outil 75
1.2.2 Formalisme 77

1.3 Proposition pour la Gestion des Modes 79
1.3.1 Première étape : la structure hiérarchique 79
1.3.2 Deuxième étape : modélisation du comportement des sous-systèmes 80

2 Proposition pour la détermination des Modes des SP 80

2.1 Les Modes et les Familles de Modes 80
2.1.1 Le GEMMA 81
2.1.2 LAN, Nantes 82

2.2 Approche par points de vue 83
2.2.1 Terminologie 84
2.2.2 Démarche proposée 85
2.2.3 Modes et Familles de Modes retenus dans notre étude 87

2.3 Exemple d'application 90

Conclusion 93

Chapitre IV 95

Introduction 95

1 Présentation 96

1.1 Les composants à modéliser 97

1.2 Structuration du Modèle de Composant 98

1.3 Démarche de conception 100

2 Conception du Modèle de Composant 103

2.1 Spécification statique et dynamique 103

2.2 La cohérence des modes 106

2.2.1 Les états compatibles 107

2.2.2 Les états trivialement incompatibles 109

2.2.3 Compatibilités liées aux états non significatifs 110

2.2.4 Les derniers états 111

2.3 Mise en œuvre de la cohérence des modes 113

2.3.1 États interdits et Interactions 114

2.3.2 Les états interdits : mécanismes 115

2.3.3 Les états transitoires et les interactions : mécanismes 116

2.3.4 Mise en œuvre 117

3 Application de la démarche de la cohérence des modes 117

3.1 Cahier des charges 117

3.2 Mise en œuvre de la cohérence des modes 119

3.3 Vérification 123

Conclusion 124

Chapitre IV 125

Introduction 125

1 Le Modèle de Fonction 126

1.1 Le MFC et le MFIE 127

1.1.1 Le Modèle Fonctionnel de Conception 127

1.1.2 Le Modèle Fonctionnel d'Implantation Élémentaire 129

1.1.3 Exemple d'application 130

1.2 Présentation du Modèle de Fonction 132

1.2.1 Son rôle 132

1.2.2 Flexibilités prises en compte 133

1.3 Sa représentation 135

1.3.1 La disponibilité 135
1.3.2 Les configurations et les versions 136
1.3.3 Son comportement 139

2 Modèle Comportemental pour la Gestion des Modes des SP. 140

2.1 Proposition 140

2.2 Liens de dépendance, points de vue et contexte 142
2.2.1 Liaison de type nécessité 142
2.2.2 Liaison de type alternative 145
2.2.3 Configurations, versions et points de vue 146

Conclusion 149

Conclusion & Perspectives 151

Annexes 154

Références 173

Introduction Générale

Contexte

A une époque où la productivité et la rentabilité prennent de plus en plus d'importance, il faut savoir produire rapidement des petites et moyennes séries de produits afin de s'adapter au marché. Dans ce contexte, l'un des objectifs est de concevoir des systèmes capables de s'adapter à des fabrications variant dans le temps par l'introduction de nouveaux produits ou le changement des objectifs de production.

Ainsi, les **Systèmes Flexibles de Production Manufacturière** (**SFPM**) sont progressivement apparus. Les SFPM sont des systèmes automatisés utilisant des ressources paramétrables et possédant des degrés de liberté, sous forme d'indéterminismes de fonctionnement, leur permettant d'ajuster la production à l'évolution de la commande.

Néanmoins, la complexité de tels systèmes nécessite de bien spécifier les besoins en production et de maîtriser leur fonctionnement. En plus d'optimiser les flux de production et de gérer les différents types de produits fabriqués, il

est nécessaire de prendre en compte les éventuelles déficiences du procédé ou de la commande. Le traitement de ces dysfonctionnements, par la connaissance de la disponibilité des ressources, permet notamment de contribuer à l'augmentation de la productivité. Ce besoin de disponibilité et également de sécurité des ressources humaines et matérielles, a rendu l'intégration des concepts de la **Sûreté de Fonctionnement** (**SdF**) incontournable.

Le projet **CASPAIM** (**C**onception **A**ssistée de **S**ystèmes de **P**roduction **A**utomatisés en **I**ndustrie **M**anufacturière), qui initialement couvrait uniquement l'aspect commande, s'est orienté vers cette intégration par l'analyse et la conception d'autres composantes tels que la Surveillance, la Maintenance et la Supervision.

Ces travaux menés au sein de l'équipe **Production Flexible Manufacturière** (**PFM**) (thème SURFEX : Sûreté de Fonctionnement et Exploitation) du **Laboratoire d'Automatique et d'Informatique industrielle de Lille** (**LAIL**) ont pour finalités de garantir les objectifs de production tout en tenant compte des différentes contraintes auquel est soumis le système. Plus particulièrement notre objectif est de connaître, évaluer, prévoir et maîtriser les défaillances des SFPM.

Problématique

Nous nous intéressons aux traitements à envisager suite à la défaillance de l'un ou plusieurs éléments constituant le système.

Une fois la défaillance détectée et diagnostiquée par la fonction de surveillance, il est nécessaire de commuter sur un autre type de fonctionnement afin de limiter le temps d'arrêt total du système. Pour envisager une telle commutation, il est nécessaire que le système comporte un certain nombre de flexibilités et qu'elles soient prises en compte dès la conception du système.

Les potentialités que représentent les flexibilités du système sont prises en compte par la fonction de Supervision. Son rôle est de gérer ces potentialités afin de garantir les objectifs de production et également la sécurité des ressources humaines et matérielles.

La problématique abordée dans ce mémoire concerne la gestion des potentialités, appelée Gestion des Modes, offertes par le système dans le cadre de leur supervision lors de défaillance.

Contribution

Une partie de notre contribution concerne la terminologique employée dans la problématique que nous étudions. Elle part du constat de la diversité des termes employés par les différents auteurs. La proposition a pour objectif de définir le processus de reconfiguration d'une façon générale et indépendamment de tout formalisme et méthode ; ceci afin de permettre aux auteurs de positionner leurs travaux les uns par aux autres.

La majeure partie de notre contribution se situe au niveau de la supervision des **Systèmes de Production** (**SP**) et concerne plus particulièrement la **Gestion des Modes**.

Notre premier apport concerne la nature des systèmes étudiés. Nous ne nous intéressons plus seulement aux SFPM caractérisés par des produits atomiques et identifiés mais aux Systèmes de Production dont l'évolution peut être caractérisée de manière discrète (au moins pour ce qui concerne des commutations dans leurs contrôles). Dans ce contexte, nous nous intéressons par exemple à des Systèmes de Production tels que les centrales nucléaires. Bien que considéré comme des systèmes continus, en raison des flux manipulés et des modèles de commandes continus, ce type de système peut brutalement commuter sur de nouveaux modèles de commandes continus. Cette commutation est alors déclenchée de façon événementielle (discrète).

Notre apport concernant la Gestion des Modes est fondé sur une démarche hiérarchique et orientée objectifs de production. La Gestion des Modes apparaît ici également comme une manière de spécifier les objectifs à atteindre au niveau de la fonction de Supervision. Une modélisation fonctionnelle permet non seulement de déterminer l'état du système mais également des sous-systèmes le constituant. Cette vision "locale" (sous-système) permet à chaque opérateur d'appréhender en permanence la connaissance de l'état de son installation quel que soit le niveau d'abstraction.

En outre, nous proposons de ne plus "regarder" l'état du système seulement sous un angle *production*. En effet, des approches méthodologiques et

l'expérience ont montré que la maintenance permet également de contribuer à l'augmentation de la productivité et de la sécurité. Il nous est alors apparu indispensable de la prendre en compte dans notre modèle. Ce dernier permet alors de caractériser l'état du système d'un point de vue production et également d'un point de vue maintenance et pour différentes familles de modes contraintes entre elles pour assurer la cohérence du système. La prise en compte de ces points de vue permettent aux opérateurs de conduite et de maintenance d'intervenir dés que cela est nécessaire.

Plan du Mémoire

Ce mémoire se décompose en cinq chapitres répartis en deux parties. La première partie qui comprend les chapitres I et II, est consacrée à la présentation du contexte de notre travail et de la problématique étudiée. Les trois derniers chapitres constituent la seconde partie qui concerne la présentation de notre proposition pour la modélisation et la gestion des modes des Systèmes de Production.

Le **Chapitre I** est consacré au cadre de nos travaux. Le domaine d'application, c'est–à-dire les Systèmes de Production, et la Sûreté de Fonctionnement sont présentés. Les principaux concepts et définitions de base sont à chaque fois abordés. Par la suite, nous décrivons la structure du contrôle-commande telle qu'elle est définie dans le projet CASPAIM. Ce premier chapitre conduit à la caractérisation de notre contexte d'étude.

Le **Chapitre II** s'intéresse au processus qui permet aux Systèmes de Production de remplir ses fonctions en dépit des fautes apparues ; et plus particulièrement au processus de reconfiguration. Cette partie vise à contribuer à l'élaboration d'une terminologie commune. Nous nous intéressons par la suite à la mise en œuvre du processus de reconfiguration. Ceci nous permet de caractériser notre problématique.

Le **Chapitre III** propose une vision globale de notre proposition pour la modélisation du comportement des Systèmes de Production d'un point de vue de leurs modes. Nous introduisons également les outils et formalismes retenus dans notre approche. Par la suite, nous abordons ce qui est la "base" de nos travaux : les modes des Systèmes de Production ; nous exposons une démarche pour leur détermination.

L'objectif du **Chapitre IV** est de présenter l'un des éléments de notre approche : le Modèle de Composant. Son rôle est de modéliser le comportement de chacun des composants élémentaires d'un Système de Production. Sa démarche de conception est détaillée

Dans le **Chapitre V**, le deuxième modèle, le Modèle de Fonction, nécessaire dans notre approche est proposé. Ce modèle permet de décrire le comportement "interne" d'un système ou sous-système fonctionnel. La dernière partie de ce chapitre montre comment les modèles précédents sont exploités dans le cadre de la Gestion des Modes des Systèmes de Production.

En conclusion générale, nous dressons un bilan des différentes propositions effectuées dans ce mémoire. Nous présentons ensuite quelques perspectives à court terme et moyen terme.

Contexte & Problématique

Cette première partie, constituée de deux chapitres, est consacrée à la présentation du contexte de notre travail et de la problématique étudiée.

L'objectif du premier chapitre est de situer le cadre de nos travaux selon trois axes : le domaine d'application, la thématique considérée et la méthodologie CASPAIM, développée au sein de notre équipe.

Dans le deuxième chapitre, l'étude du traitement de fautes, dans un contexte de tolérance aux fautes, effectuée à partir de la littérature permet de définir la problématique abordée dans ce mémoire.

Chapitre I

Sûreté et Exploitation des Systèmes de Production

INTRODUCTION

L'objectif de ce chapitre est de présenter le contexte de notre étude. D'une manière générale, ce contexte peut être caractérisé selon trois axes : le domaine d'application, la thématique considérée et par rapport à la méthodologie CASPAIM, développée au sein de notre équipe.

Dans un premier temps, nous présentons les concepts et les définitions de base qui vont permettre de définir les Systèmes de Production auxquels nous nous intéressons dans notre étude.

L'un des objectifs de l'équipe PFM est de connaître, évaluer, prévoir et maîtriser les défaillances des Systèmes de Production. Dans ce sens, la thématique Sûreté de Fonctionnement est abordée. Afin d'éviter toutes

ambiguïtés, nous définissons alors un certain nombre de termes en vigueur dans la Sûreté de Fonctionnement, ainsi que nos objectifs.

Enfin, la méthodologie CASPAIM, développée au LAIL, est présentée ; elle permettra de positionner notre étude par rapport aux travaux existants. L'objectif de cette partie est de caractériser de manière générale, d'un point de vue des objectifs et des démarches, les travaux antérieurs afin d'introduire notre problématique dans le chapitre suivant.

Ainsi, ce premier chapitre conduit à la caractérisation de notre contexte d'étude.

1 LES SYSTÈMES DE PRODUCTION

1.1 Définitions

Tout **S**ystème de **P**roduction (**SP**) 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 [Bon, 93]. Lorsque le Système de Production est fortement automatisé, c'est-à-dire très autonome, le terme **S**ystème **A**utomatisé de **P**roduction (**SAP**) est usuel. Pour notre part, nous ne faisons pas de différence entre les termes *Système de Production* et *Système Automatisé de Production*.

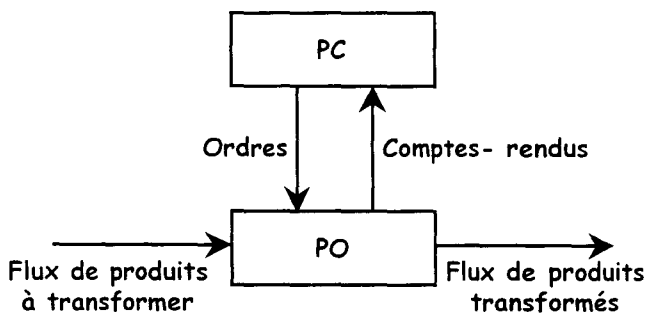


figure I-1. Schéma d'un Système de Production

En effet, les Systèmes Automatisés de Production sont définis de manière similaire aux Systèmes de Production par la norme NFX50-400 [NFX50] comme un ensemble d'éléments matériels et/ou logiciels en interaction dynamique, organisé en fonction d'une finalité : conférer une valeur ajoutée à

des flux de produits, conformément à des objectifs de production, d'exploitation et de sécurité.

D'une manière générale, les Systèmes de Production sont schématisés par trois types d'entités (*figure I-1*) :

- les **Produits** qui représentent l'ensemble des entités à transformer et des entités transformées (matières premières, énergie, des hommes dans le cas des systèmes de transport [Ver, 89], ...),
- une **Partie Opérative** (**PO**) (ou procédé) qui regroupe l'ensemble des organes physiques qui interagissent sur le produit pour lui conférer sa valeur ajoutée. Elle est constituée d'entités de transformation qui peuvent porter sur la structure du produit (usinage), leur composition (assemblage) ou sur leur position (transport). Selon la nature du flux de produits [Rak, 93], la PO peut être de trois types :
  - ✧ discrète : le produit représente une matière solide et discrète et constitue un ensemble de matière localisable individuellement,
  - ✧ continue : le produit est un flux continu de matière (câblerie, chimie, ...) ou d'énergie (production d'électricité),
  - ✧ mixte ou hybride : lorsque le processus est à la fois discret et continu ;
- une **P**artie **C**ommande (**PC**) (ou système de contrôle-commande) qui regroupe l'ensemble des moyens logiciels et matériels et les informations permettant la gestion du procédé. Elle peut être considérée comme la partie décisionnelle du SAP et comme *l'Univers de l'information* [Del, 89] dans lequel est représentée la dynamique (le comportement) désirée de la PO. Les décisions (**ordres**) portent sur les actions à mener par le procédé sur le produit. Elles sont élaborées à partir des informations (**comptes-rendus**) recueillies sur le procédé ou sur le produit.

Remarque : Dans ce mémoire, nous parlons indifféremment d'éléments, d'entités, d'équipements ou plus globalement de ressources pour désigner les éléments constituant un Système de Production.

Étant donné la diversité des équipements qui constituent les Systèmes de Production et de leurs interactions, les automaticiens ont senti le besoin de décomposer de tels systèmes en sous-systèmes. Le type du découpage permet de déterminer la structure de l'architecture du Système de Production. D'une

manière générale, nous distinguons trois types de structure [Get, 94] [Mab, 96] :

- la structure centralisée qui se caractérise par l'existence d'un système de décision unique chargé de coordonner l'ensemble des opérations des différents équipements,
- la structure distribuée, répartie ou décentralisée, qui se caractérise par la répartition des prises de décision sur chacun des équipements,
- la structure hiérarchisée qui peut être assimilée à une décentralisation verticale et structurée. Le système est décomposé en sous-systèmes de plus en plus petits.

1.2 Le cycle de vie

L'évolution d'un Système de Production est caractérisée par ce que l'on nomme son cycle de vie. Il représente les différentes étapes par lesquelles passe le Système de Production, entre le moment de la prise de décision de produire un nouvel élément pour lequel il faut concevoir ce système, et sa production effective.

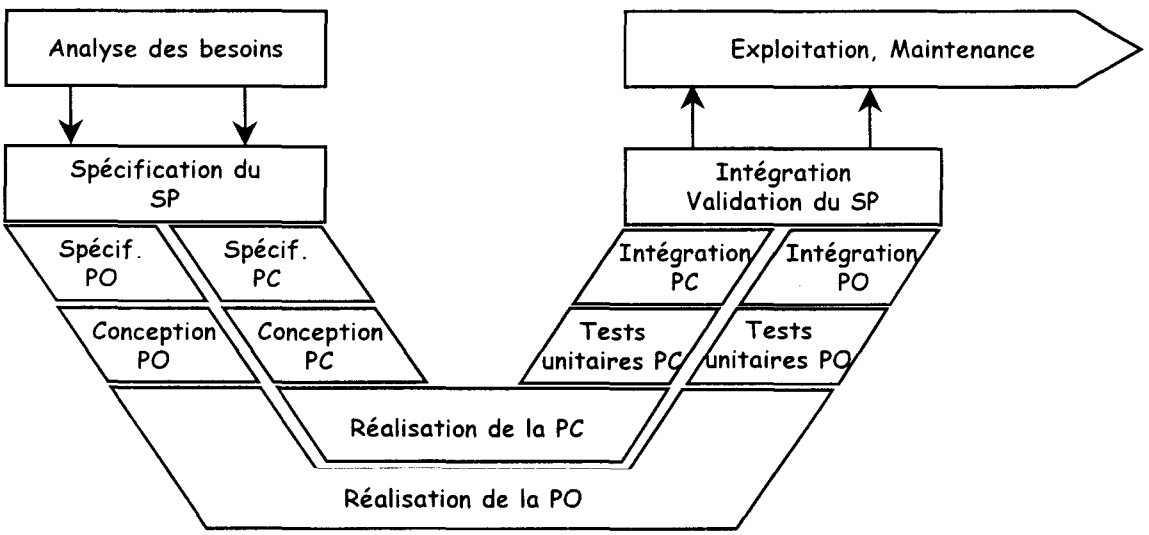


figure I-2. Cycle de vie : schéma en V

Ces étapes consistent à déterminer les objectifs du Système de Production (cahier des charges), à décrire les étapes nécessaires pour atteindre ces objectifs (spécification), à concevoir des moyens (conception) et à exploiter ces moyens (exploitation).

Dans le domaine des Systèmes de Production, le cycle dit en "V" (ou en racine carrée) est le plus utilisé (*figure I-2*). Notre but n'est pas de présenter le cycle de vie de façon détaillée mais seulement de présenter un certain nombre de notions sur lesquelles repose notre travail. La figure I-2 représente de manière générale le cycle de vie d'un Système de Production.

Ce modèle de cycle de vie décrit un enchaînement temporel des activités qui s'étendent de l'énoncé des besoins jusqu'à l'exploitation, avec les développements parallèles de la partie commande et de la partie opérative. Il fait apparaître un axe horizontal temporel et un axe vertical d'élaboration technique.

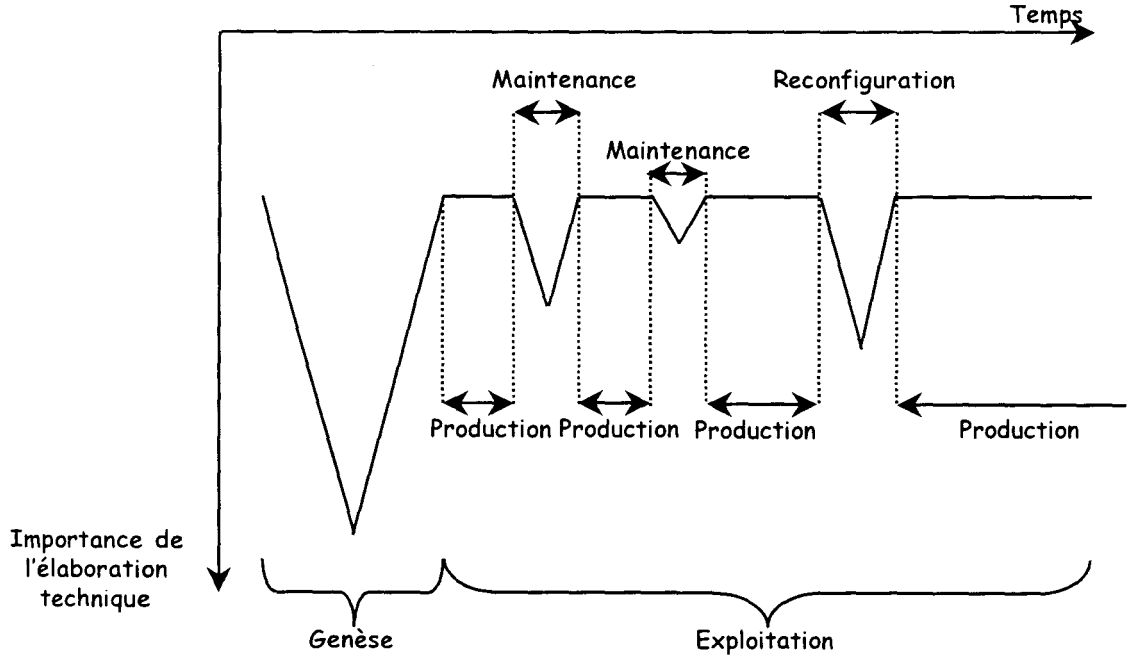


figure I-3. Cycle de vie d'un Système de Production

Ce modèle se décompose en deux parties : la première caractérise la **genèse** du Système de Production et la seconde son **exploitation**.

- la genèse, est elle-même décomposée en deux sous parties :

  - ✧ la première, la partie gauche du "V" correspond à une approche descendante et regroupe les phases de spécification et de conception du Système de Production durant lesquelles ses propriétés sont définies,

- ✧ la seconde, la partie droite du "V" correspond à une approche ascendante et représente une suite d'intégration et de tests de sous-ensembles de plus en plus complexes.

- son exploitation, elle regroupe les activités relevant de l'exploitation (production, maintenance et reconfiguration du système). Cette seconde partie est également modélisée par une succession de "V" (*figure I-3*). En effet, il est généralement nécessaire de modifier la spécification du Système de Production pour prendre en compte des oublis ou pour corriger des erreurs. En outre, l'évolution voulue (changement de production) ou subie (défaillances) de la production entraîne une reconfiguration du système. Il est à noter que les périodes de reconfiguration peuvent être incluses dans les phases de production. En effet, seule une partie du système peut être reconfigurée et l'autre continuer à produire.

Le cycle de vie d'un Système de Production peut être vu comme une hiérarchie d'alternances entre étapes de spécification et étapes de conception : la spécification définissant *ce qu'il faut faire* et la conception *comment le faire* [Bon, 93].

1.3 La flexibilité

L'augmentation de l'automatisation industrielle et la tendance vers des cycles de vie des produits de plus en plus courts ont pour conséquence de rendre la flexibilité des Systèmes de Production primordiale pour leur rentabilité. La flexibilité est considérée comme une possibilité pour un décideur de pouvoir à tout moment reconsidérer ses choix de manière à maintenir l'optimalité de sa décision [Coh, 92]. La flexibilité apparaît alors comme un moyen efficace pour améliorer la gestion des Systèmes de Production. Cette première approche laisse entrevoir le nombre de définitions possibles selon le point de vue adopté. En effet, il existe autant de définitions qu'il y a d'intervenants dans un Système de Production (économiste, responsable de production, ...) [Oko, 91]. Le point de vue qui nous intéresse dans le cadre de ces travaux est celui de l'exploitation des Systèmes de Production.

D'une manière générale, pour les industriels, le terme flexibilité est synonyme d'adaptabilité et de capacité de changement [Gus, 95]. Cette flexibilité se présente sous plusieurs formes. Dans un premier temps, il est

possible de distinguer les flexibilités **potentielles** et les flexibilités **opératoires**.

Les **flexibilités potentielles** (ou physiques) [Ers, 88] sont liées au procédé (architecture du système) et aux produits. Elles correspondent à la capacité de changement physique du système. Les principaux types de flexibilité que nous pouvons rencontrer dans les Systèmes de Production sont :

- les **ressources polyvalentes** (ou ressources multi-opérations) pouvant réaliser plusieurs types d'opérations,
- les **ressources de transformation multiples** qui correspondent au fait d'avoir une machine en plusieurs exemplaires pouvant faire les mêmes opérations. La multiplicité des ressources conduit à de la redondance (active ou passive),
- les **flexibilités du système de transport** [Cam, 97/a] ou flexibilité dans l'architecture de transport ; c'est le cas où plusieurs chemins peuvent relier deux postes de travail,
- les **flexibilités des ressources de transport** [Ohl, 95] où les ressources de transport (de type palettes ou robots par exemple) peuvent transporter soit un seul type de pièces (palettes dédiées) soit plusieurs types de pièces (palettes universelles).

Les **flexibilités opératoires** (ou décisionnelles), appelées également flexibilités des gammes, sont liées à la commande et traduisent la capacité du système à utiliser les flexibilités potentielles. De telles flexibilités permettent aux Systèmes de Production d'être facilement adaptés à des fabrications variant dans le temps par l'introduction de nouveaux produits, le changement des objectifs de production ou la déficience du procédé et/ou de la commande. En outre, elles donnent la possibilité de réaliser un type de produit d'une ou plusieurs façons différentes [Got, 93]. Dans les Systèmes de Production, ces flexibilités se présentent sous forme d'indéterminismes de fonctionnement, leurs permettant d'ajuster la production en fonction de l'évolution de la commande.

Il n'existe guère de Systèmes de Production type ou standard. Cependant, ils sont en général distingués selon les flexibilités opératoires qu'ils contiennent. Pour illustrer les différentes formes de flexibilités opératoires, considérons que les gammes opératoires qui représentent les ensembles

d'opérations nécessaires pour la réalisation du type de produit, soient modélisées par réseaux de Petri [Dav, 92].

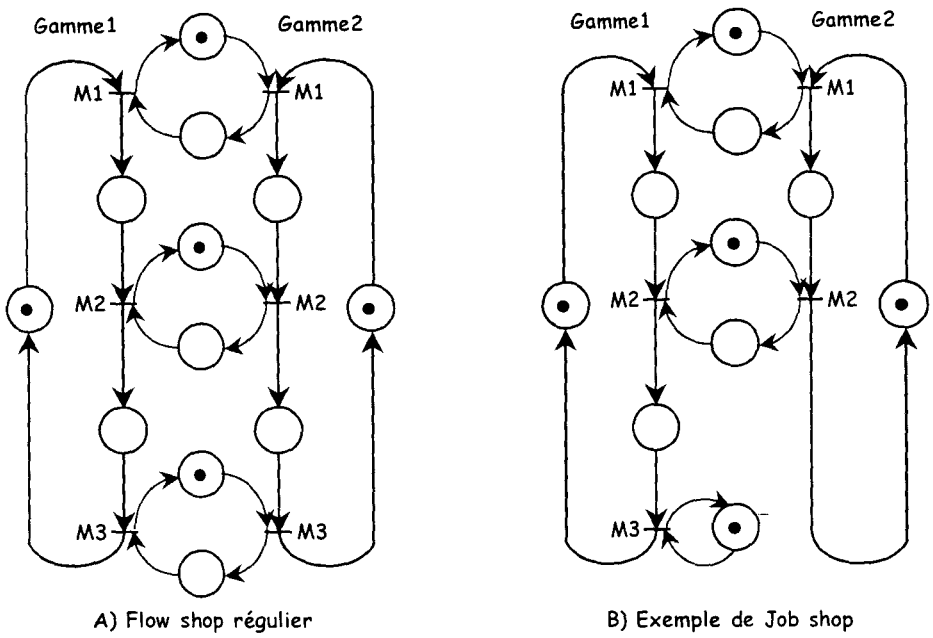


figure I-4. Flow shop régulier et Job shop.

Nous distinguons alors les Systèmes de Production dans l'ordre croissant des flexibilités contenues [Lop, 99] :

- le **Flow shop** (atelier à cheminement unique) : toutes les gammes de fabrication passent par les mêmes machines et dans le même ordre. Par exemple, la réalisation de trous dans des plaques métalliques nécessite le passage par les mêmes machines. Cette dernière demandera plus ou moins de temps pour réaliser l'opération en fonction du diamètre et de la profondeur du trou. Si les produits passent dans le même ordre sur les machines, le flow shop est dit régulier (*figure I-4-A*),
- le **Job shop** (atelier à cheminement multiple) : dans ce cas, chaque type de produit possède une gamme opératoire linéaire spécifique. Dans ce type d'atelier, il n'y a pas de flexibilité au sein des différentes gammes, seulement elles diffèrent entre elles en n'utilisant pas les mêmes machines ou dans des ordres différents (*figure I-4-B*),
- le **Job shop généralisé** : dans ce cas, les gammes sont spécifiques mais ne sont pas forcément linéaires et contiennent donc des flexibilités. Parmi les flexibilités les plus rencontrées, nous pouvons noter [Kor, 98] (*figure I-5*) :

✧ les flexibilités de permutation : c'est le cas d'une gamme qui contient deux opérations sans contrainte de précédence stricte entre les deux,

✧ les flexibilités d'affectation : dans ce cas, une opération peut être indifféremment effectuée sur au moins deux machines différentes avec des temps opératoires pouvant être également différents,

✧ les flexibilités de procédé : une gamme possède au moins deux chemins linéaires distincts pour réaliser la pièce.

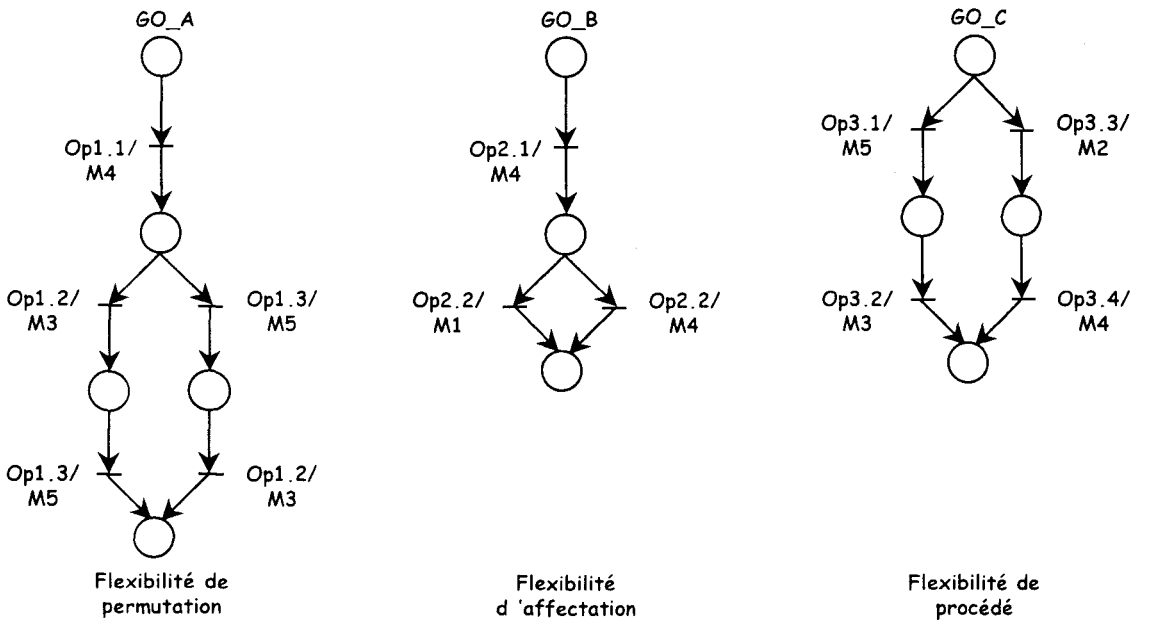


figure I-5. Illustration des flexibilités d'un Job shop généralisé

- l'**Open shop** (atelier à cheminement libre) : les pièces sont définies par un ensemble d'opérations à réaliser sans contrainte de précédence ni de gamme spécifique.

Ainsi, l'introduction du concept de flexibilité apparaît comme un moyen d'atténuer les conséquences des incertitudes de production (perturbations, défaillances, demandes variables des quantités de produits, ...) en offrant un certain nombre de possibilités. Cependant, si les flexibilités contenues dans les Systèmes de Production permettent de répondre à des exigences économiques et/ou de production, elles contribuent à l'augmentation des interactions à gérer entre les éléments du système et par conséquent à l'accroissement des risques pour les personnes et les moyens de production. De ce fait, dès la conception

des Systèmes de Production, une attention toute particulière doit être portée au concept de **sécurité**.

1.4 La complexité

De nos jours, les Systèmes de Production s'avèrent très complexes du fait de l'hétérogénéité de leurs équipements, des flexibilités qu'ils offrent et de la multitude de paramètres à contrôler. La notion de complexité fait référence au nombre et à la diversité des relations internes au système [Lus, 72]. Elle est différente de la notion de complication qui se caractérise par la présence de nombreux éléments connectés uniquement par des relations arborescentes [Lem, 91].

La diversité des technologies utilisées et la complexité, de plus en plus poussée, des Systèmes de Production font que tout système évoluant dans un environnement réel subit des perturbations qui ont pour conséquence de dévier son comportement par rapport aux objectifs de production. Ces incertitudes de production sont alors pénalisantes pour atteindre les objectifs préalablement fixés.

En outre, la complexité de tels systèmes tend à diminuer la "fiabilité" de leur fonctionnement et demande un effort assez conséquent pour améliorer leur "maintenabilité" et leur "disponibilité". Les causes des écarts (ou perturbations) n'apparaissent pas seulement en phase d'exploitation (Chapitre I, §. 1.2) ; elles sont réparties dans les diverses étapes du cycle de vie. Ces concepts de "maintenabilité" et de "disponibilité", attributs de la Sûreté de Fonctionnement, doivent alors être pris en compte dès la phase de conception.

1.5 Les Systèmes de Production étudiés

A partir de ces quelques définitions et concepts, nous pouvons maintenant préciser quels sont les Systèmes de Production qui nous intéressent et dans quel contexte.

Premièrement, la nature du procédé des Systèmes de Production retenus peut être discrète ou continue. Bien qu'initialement, nous nous sommes intéressés aux SFPM (discrets), Les exemples présents tout au long de ce mémoire concernent une centrale nucléaire (continu). Le type de l'évolution du

système nous importe plus que sa nature en raison du choix des outils de modélisation. En effet, l'aspect continu, dans le cas de la centrale nucléaire, ne dépend pas uniquement du fait que l'on manipule des flux continus. Il provient également des modèles de commande continue à base d'équations différentielles surveillant des variables évoluant elles-mêmes de façon continue, fonction des lois de la physique. Par contre, ce type de système peut brutalement commuter sur de nouveaux modèles de commandes continus. Cette commutation est déclenchée de façon événementielle (discrète) sur la base d'un franchissement d'un seuil d'une variable caractéristique. De même, dans le cas des SFPM, l'aspect discret ne correspond pas uniquement au fait que l'on manipule des produits atomiques et identifiés. Il est également lié à l'évolution du système due à la succession d'occurrences d'événements.

Ainsi, la nature du système peut être discrète ou continue. La seule condition requise est que l'évolution des systèmes étudiés puisse être représentée par un modèle à événements discrets.

Deuxièmement, la notion de flexibilité doit être présente de façon plus ou moins importante dans les systèmes étudiés. Nous montrerons, dans le paragraphe suivant, le besoin de flexibilité.

Enfin, quel que soit le système étudié, nos travaux se concentrent sur la phase d'exploitation. Cependant, les alternatives possibles offertes par les flexibilités du système doivent être prévues dès la phase de conception.

2 LA SÛRETÉ DE FONCTIONNEMENT

2.1 Caractérisation de la Sûreté de Fonctionnement

Issue des domaines aéronautique, nucléaire et spatial, la **S**ûreté **d**e **F**onctionnement (**SdF**) a été étendue aux Systèmes de Production. Également appelée science des défaillances, la Sûreté de Fonctionnement a pour objectif d'établir le degré de confiance que l'on peut attribuer à un système dans le cadre de la mission qu'il doit assurer [Zwi, 95]. Nous pouvons également citer une définition similaire issue du domaine logiciel [Lap, 95] :

> *"La Sûreté de Fonctionnement est la qualité du service que le système délivre, de telle sorte que les utilisateurs puissent lui accorder (au système) une confiance justifiée."*

Le terme service désigne le comportement du système tel qu'il est perçu par son (ou ses) utilisateur(s). Les utilisateurs peuvent être d'autres systèmes ou des ressources humaines qui interagissent avec le système considéré.

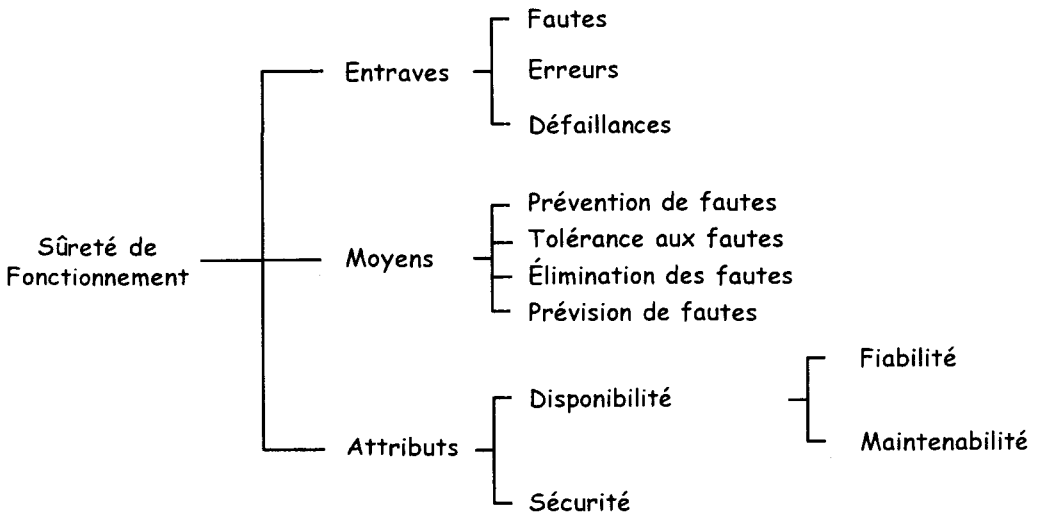


figure I-6. Arbre de la Sûreté de Fonctionnement.

Le rôle de la Sûreté de Fonctionnement consiste alors à identifier, analyser, évaluer et hiérarchiser des défaillances afin de minimiser leurs effets tout en tenant compte des contraintes de sécurité et de rentabilité [Sim, 99/a].

Comme toute science, elle possède de nombreux concepts, des grandeurs mesurables, un support mathématique, des méthodes de mesure et de prévision de ces grandeurs. Il existe dans le domaine de la Sûreté de Fonctionnement une terminologie conséquente. C'est pourquoi nous nous proposons de définir clairement quelques termes. Les notions nécessaires à la bonne compréhension de cette science peuvent être regroupées en trois classes : les **entraves**, les **moyens** et les **attributs**. La figure I-6 propose une vision générale de cette science en représentant l'arbre de la Sûreté de Fonctionnement.

2.2 Les entraves

Les entraves sont les circonstances indésirables, mais non inattendues, causes ou résultats de la non-sûreté de fonctionnement [Lap, 85]. Dans un monde idéal, un Système de Production fabriquerait des produits en toute conformité avec les caractéristiques attendues. Force est de constater que dans un environnement réel, il existe des écarts entre les caractéristiques attendues et celles effectives (Chapitre I, §. 1.4). Ces écarts peuvent être de deux natures : défaillance ou défaut.

2.2.1 Défaillances

Lorsque le système ne délivre plus la fonction pour laquelle il a été conçu : le système est alors **défaillant**. Une défaillance [CEI, 74] est définie comme :

> *"La fin de l'aptitude d'un dispositif à accomplir sa fonction requise."*

L'occurrence d'une défaillance est due à une succession d'événements qui sont la **faute** et l'**erreur**. Nous donnons les définitions et illustrons ces trois notions.

- **Faute** : c'est la cause d'une erreur. Une faute peut être définie comme un phénomène ou une imperfection présent dans le système et susceptible de générer des erreurs [Che, 99],
- **Erreur** : c'est la partie d'un système qui ne répond pas au besoin, et qui peut donc éventuellement provoquer une défaillance. Le fait qu'une erreur conduise ou non à une défaillance dépend de certains facteurs : la composition du système (existence de redondance), la définition d'une défaillance du point de vue de l'utilisateur (ce qui est considéré comme erreur pour un utilisateur peut être considérée comme une perturbation admissible par un autre utilisateur),
- **Défaillance** : elle se produit lorsque la partie erronée du système est utilisée. Elle se traduit par un comportement du système différent de celui prévu.

Illustration [Lap, 95] : Un programmeur conçoit un logiciel. Si, au cours de la réalisation, le programmeur se trompe dans une opération X, il commet

une **faute**. L'appel de cette opération (donc de la faute) donnera une **erreur**. Si elle affecte le service délivré, une **défaillance** se produira.

Certains auteurs [Lap, 85] distinguent l'erreur latente de l'erreur effective. Une faute de conception, par exemple, amène une erreur latente. Cette erreur devient effective quand une procédure d'exploitation fait intervenir la faute en cause (ceci n'est pas sans rappeler la notion de conflit structurel et effectif dans les réseaux de Petri). Toutefois, le passage d'une erreur de l'état latent à l'état effectif ne peut absolument pas être assimilé à l'apparition d'une défaillance. Il existe également des erreurs de propagation : l'erreur d'un composant peut conduire un autre composant indépendant fonctionnellement dans un état erroné [Elk, 93].

Il est à noter que, selon le point de vue où l'on se place, un même événement peut être une faute ou une défaillance. En effet, il est une défaillance pour l'étape dont le service est dévié et il est une faute pour l'étape qui se basera sur ce service dévié. Il est alors possible de dire que des défaillances se produisent à chaque étape.

La conséquence directe d'une défaillance est la **panne**. La panne est l'inaptitude d'une entité (composant ou système) à assurer une fonction requise [Vil, 88].

2.2.2 Défaut

Le système ne délivre plus la fonction avec les caractéristiques qui lui ont été spécifiées : le système présente alors un **défaut**. Un défaut [Vil, 88] est défini comme :

> *"Un écart entre une caractéristique d'un composant et la caractéristique voulue."*

Un défaut dans le système n'affecte en général pas l'aptitude du système à accomplir une fonction requise. Par conséquent, on peut constater que le défaut ne conduit pas toujours à une défaillance. Par contre, une défaillance implique systématiquement l'existence d'un défaut.

2.2.3 Classifications des entraves

Les défaillances peuvent être regroupées selon les conséquences qu'elles engendrent sur le fonctionnement de l'élément défaillant. Il existe plusieurs critères [Zwi, 95] [Tog, 92] pour les classer : rapidité, amplitude, causes, date, ampleur.

		Types de défaillance
Critères	Rapidité	Progressive, Soudaine
	Amplitude	Partielle, Complète
	Rapidité et Amplitude	Dégradation, Cataleptique
	Causes	Première, Seconde, Commande
	Date d'apparition	Précoce, D'usure
	Ampleur	Significative, Critique

figure I-7. Classifications des défaillances

Dans le cadre de la Sûreté de Fonctionnement, deux types de défaillances (*figure I-8*) sont principalement prises en compte :

- les défaillances cataleptiques : ce sont des défaillances soudaines et complètes. Il n'existe pas d'état transitoire entre l'état de fonctionnement normal et l'état de panne,
- les défaillances par dégradation : ce sont des défaillances partielles et progressives.

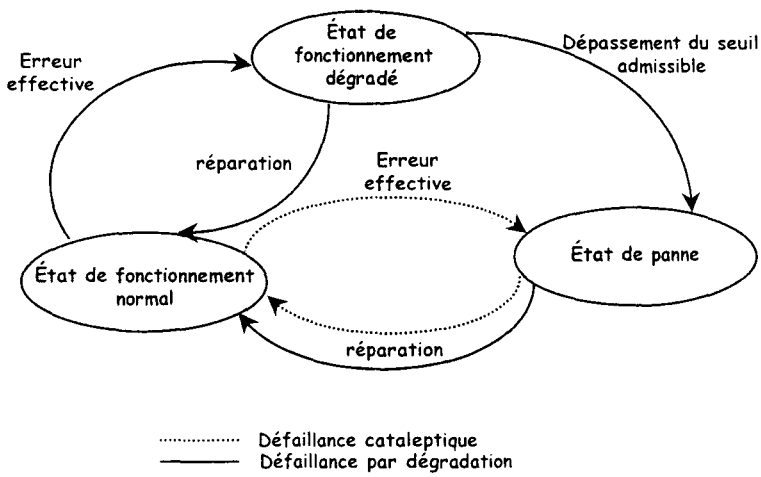


figure I-8. Défaillance par dégradation et cataleptique

Les caractéristiques temporelles de ces deux types de défaillances entraînent une manière différente de les traiter. Les défaillances cataleptiques conduisent immédiatement à l'état de panne.

Les classifications des pannes sont semblables. On distingue les pannes mineures, significatives, critiques, catastrophiques, partielles, complètes, ...

2.2.4 Entraves prises en compte

Parmi les défaillances possibles, nous ne prenons en compte que celles du procédé. En effet, nous considérons la commande comme exempte d'erreurs et conduisant toujours à l'exécution de l'ordre demandé. En outre, nous nous intéressons aux défaillances cataleptiques et également aux défaillances par dégradation. Enfin, nous excluons le cas des défaillances simultanées.

D'un point de vue terminologique, nous ne distinguons pas les termes *faute* et *erreur*. Enfin, les termes *défaillance*, *défaut*, *dysfonctionnement* et *écart* sont considérés comme équivalents.

2.3 Les attributs de la SdF

La Sûreté de Fonctionnement peut être vue selon différentes propriétés complémentaires qui permettent de définir ses **attributs** ou **mesures**. Selon les domaines d'application, l'accent pourra être mis sur une partie ou sur l'ensemble de ces attributs.

2.3.1 Fiabilité (Reliability) :

> *"La fiabilité est l'aptitude à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné" [NFX60/b].*

Au sens général, la fiabilité caractérise la confiance qu'un utilisateur accorde à un système pendant son exploitation. Cela revient à s'intéresser à la continuité du service délivré.

2.3.2 Disponibilité (Availability) :

> *"La disponibilité est l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné" [NFX60/a].*

La disponibilité peut donc être présentée comme résultant de la fiabilité du matériel (au sens large) et des conditions de sa maintenance. S'intéresser à la disponibilité d'une entité revient à savoir si cette entité est prête à fonctionner à un instant donné.

2.3.3 Maintenabilité (Maintenability) :

> *"La maintenabilité est l'aptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données avec des procédures et des moyens prescrits" [Vil, 88].*

Ainsi, suite à la défaillance d'un système, il est nécessaire de le remettre en état de marche : c'est le rôle de la maintenance. La mesure de son efficacité est appelée maintenabilité. On peut remarquer que la fiabilité et la maintenabilité sont deux notions duales, qui traduisent globalement la disponibilité d'un système.

2.3.4 Sécurité (Security) :

> *"La sécurité est l'aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques" [Zwi, 95].*

Elle résulte du comportement du système en cas de problème. Elle est caractérisée par la capacité du système à exécuter correctement les tâches pour lesquelles il est prévu, et à refuser toute action non autorisée ou incorrecte. La sécurité assure la non-occurrence de défaillances, dangereuses ou non pour les hommes ou pour le matériel. Elle concerne l'évitement de conséquences catastrophiques.

2.3.5 Notre besoin de sûreté

Selon le domaine d'application, l'accent peut être mis sur certains attributs de la Sûreté de Fonctionnement. La figure I-9 propose des exemples en terme de besoin de sûreté selon le domaine d'application considéré.

La complexité des systèmes étudiés (Chapitre I, §. 1.4) fait que la disponibilité est toujours requise bien qu'à des degrés différents selon le domaine d'application. En outre, nous avons montré que la flexibilité des systèmes étudiés (Chapitre I, §. 1.3) demande de prêter une attention toute particulière à la sécurité. Par conséquent, les concepts de disponibilité et de sécurité sont au centre des préoccupations de nos travaux.

	Systèmes à mission de sauvegarde	**Systèmes dangereux à mission unique**	**Systèmes industriels à mission prolongée**
	(systèmes de détection : d'incendie, toxique)	*(fusées, missiles,...)*	*(systèmes de production)*
Sûreté	**Fiabilité absolue** ou à défaut **Sécurité positive** (sécurité orienté vers l'alarme: très sûr mais non fiable)	**Sécurité hors mission** (ne pas exploser...) + **Fiabilité mission** (fonctionner à la demande car non réparable en mission)	**Sécurité** (des personns, des biens et de l'environnement) + **Disponibilité** (Fiabilité + maintenabilité)

figure I-9. Le besoin de sûreté [Sim, 99/a]

2.4 Les moyens

Les moyens de la Sûreté de Fonctionnement sont les méthodes et les techniques pour, d'une part conférer au système l'aptitude à délivrer le service conforme à l'accomplissement de sa fonction, c'est-à-dire fournir la Sûreté de Fonctionnement au système, et d'autre part pour donner confiance en cette aptitude, c'est-à-dire la valider [Bon, 93].

L'obtention d'un système sûr de fonctionnement passe ainsi par l'utilisation de méthodes d'analyse permettant la prévention des défaillances, leur identification et leur maîtrise.

Les moyens d'**obtention** de la Sûreté de Fonctionnement consistent en fait à éviter la création d'entraves ou à corriger les entraves lorsqu'elles ne peuvent être évitées. Ces deux types de méthodes sont la prévention de fautes et la tolérance aux fautes.

Les moyens de **validation** de la Sûreté de Fonctionnement permettent de déterminer le degré de sûreté du système conçu et donc d'indiquer s'il est possible d'avoir confiance dans l'aptitude du système à délivrer le service spécifié. Ces moyens sont l'élimination de fautes et la prévision de fautes. Nous proposons ci dessous de présenter ces différentes méthodes en nous basant sur les définitions données par Laprie [Lap, 95].

2.4.1 La prévention de fautes

Ce type de méthodes consiste à minimiser les risques de fautes lors de la conception même du système. Leur objectif est d'empêcher l'occurrence ou l'introduction de fautes. Pour cela, elle cherche à minimiser par construction les possibilités de faire des fautes, et par conséquent, diminuer le nombre de défaillances. Ceci implique généralement l'utilisation d'outils de modélisation puissants (maximum d'informations), fondés sur des formalismes stricts. Toutefois, toutes les fautes ne peuvent pas être évitées, aussi est-il nécessaire d'étudier des méthodes correctives.

2.4.2 La tolérance aux fautes

Ce type de méthodes permet au système de poursuivre sa mission en dépit de l'occurrence de défaillances. Un système tolérant aux fautes doit pouvoir remplir ses fonctions malgré des fautes pouvant affecter ses entités. La tolérance aux fautes est mise en œuvre grâce aux techniques de traitement des erreurs et des fautes. Ces traitements font appel à différents types d'actions que sont la détection, le diagnostic et le recouvrement (reprise, poursuite ou compensation). Lorsque le service initial ne peut plus être délivré, une modification de la structure du système est réalisée afin que les entités non défaillantes puissent délivrer un service acceptable : il s'agit de la reconfiguration. Ces techniques sont généralement fondées sur l'utilisation de redondances d'éléments du système.

2.4.3 L'élimination de fautes

Ce type de méthodes s'appuie sur la vérification, le diagnostic et la correction de fautes. Les techniques de vérification peuvent être, soit des méthodes statistiques (preuves, analyses), soit des méthodes dynamiques (test, exécution symbolique). Le principe consiste à générer des entrées de test (de façon déterministe ou aléatoire), d'observer les sorties de test et de décider si

les conditions de vérification sont satisfaites. L'élimination des fautes en phase d'exploitation du système est réalisée par la Maintenance (Chapitre I, §. 3.5).

2.4.4 La prévision de fautes

Ce type de méthodes consiste à évaluer, c'est-à-dire examiner et analyser les défaillances des entités et de leurs conséquences sur la Sûreté de Fonctionnement d'un système. Ces examens et analyses peuvent être, soit des évaluations ordinales (classification des défaillances), soit des évaluations probabilistes (degré de satisfaction des attributs de la Sûreté de Fonctionnement). Les méthodes les plus connues sont l'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC) pour l'évaluation ordinale et les chaînes de Markov pour l'évaluation probabiliste. Les diagrammes de fiabilité et arbres de fautes sont valables quel que soit le type d'évaluation. La quantification de l'alternance entre état correct et état incorrect permet de définir les attributs (fiabilité, disponibilité et maintenabilité) comme des mesures de la Sûreté de Fonctionnement.

2.4.5 Nos objectifs

L'obtention d'un système sûr ne peut être que le résultat d'une combinaison des différents moyens de la Sûreté de Fonctionnement. En effet, les imperfections (en raison de la nature humaine) accumulées à chaque étape du cycle de vie créent une dépendance de ces moyens. En dépit de la prévention de fautes, des erreurs surviennent. Il est alors nécessaire de procéder à l'élimination de ces fautes. Cette vérification est elle-même imparfaite d'où la nécessité de prévoir les fautes. Cependant, quelques fautes subsistent tout de même, c'est pourquoi elles doivent être traitées par la tolérance aux fautes.

Nos travaux se situent dans le cadre de la tolérance aux fautes. Notre objectif est de pouvoir assurer, en présence d'une défaillance, la continuité du service. Cette position explique pourquoi les systèmes étudiés doivent présenter un caractère flexible (Chapitre I, §. 1.5). En effet, sans aucune flexibilité (ou alternative) et en présence de défaillance, il n'est pas possible de continuer à délivrer le service attendu. Dans ce sens, une étude de la tolérance de l'architecture [Ber, 98] permet de déterminer les degrés de liberté offerts par le système et par conséquent exploitables dans le cadre de la tolérance aux fautes.

Plus particulièrement, nous nous intéressons au processus de

reconfiguration. Dans un contexte de tolérance aux fautes où l'objectif est de produire en dépit de défaillances, il est nécessaire de modifier l'organisation du Système de Production afin d'atteindre les objectifs de production fixés.

3 DESCRIPTION DU CONTEXTE DE CONTRÔLE COMMANDE

3.1 La méthodologie CASPAIM

La méthodologie CASPAIM (Conception Assistée des Systèmes de Production Automatisés en Industrie Manufacturière) a débuté dans les années 80. Elle avait pour objectif initial de prendre en charge la totalité des étapes du cycle de développement du système de commande d'un Système de Production. Le système de commande était alors décomposé en deux parties : une couche de coordination appelée commande [Bou, 88] et une couche décisionnelle [Cra, 89] appelée niveau hiérarchique.

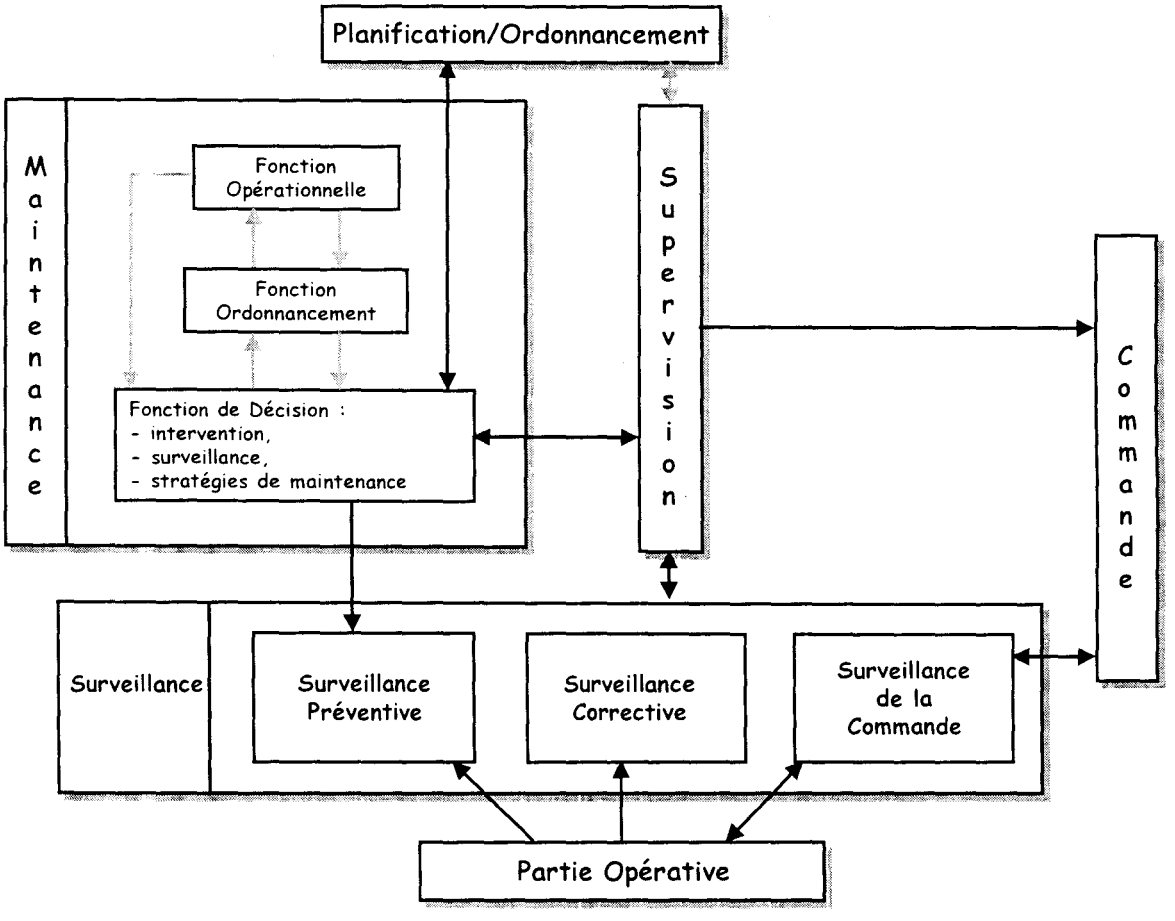


figure I-10. Intégration des fonctions du contrôle-commande

A partir de là, de nombreux travaux de recherche [Cru, 91], [Boi, 91], [Tog, 92], [Ber, 98] [Ly, 99] ont été menés afin d'affiner le niveau hiérarchique. C'est dans un souci de respect des objectifs de production qu'a été développée chacune de ces nouvelles composantes. Ces différents travaux, développés dans un cadre de conduite réactive, ont conduit à une nouvelle organisation (*figure I-10*) qui intègre maintenant les fonctions de Surveillance, Supervision et Maintenance. Il est à noter que l'intégration de ces composantes correspond à une prise en compte de la Sûreté de Fonctionnement en phase d'exploitation. En effet, chacun de ces modules contribue à améliorer la disponibilité, la fiabilité, la maintenabilité ainsi que la sécurité des Systèmes de Production.

3.2 La Commande

La Commande a pour fonction de recevoir les comptes rendus et d'envoyer les commandes aux actionneurs en assurant la coordination et le séquencement des commandes applicables au procédé. Elle ne résout pas les conflits et indéterminismes liés à la flexibilité du système. Elle est hiérarchisée en plusieurs niveaux distinguant différents types de gammes, les filtres de comportement des ressources complexes et les graphes de commande des ressources.

3.2.1 Les Gammes Logiques

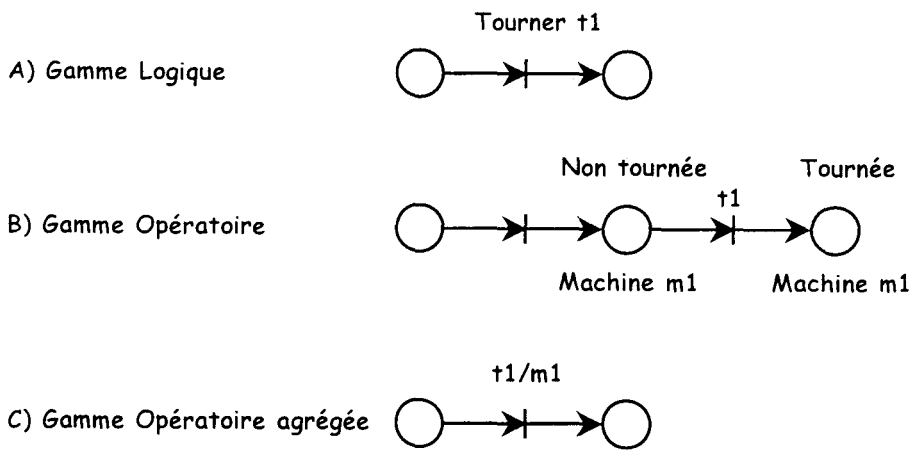


figure I-11. Illustration des différentes gammes

Dans un premier temps, les **gammes logiques** sont définies (*figure I-11-A*). Elles permettent de prendre en compte le séquencement des opérations sur

chaque type de pièce tout en tenant compte des possibilités de flexibilité dans l'ordre d'exécution [Cru, 91].

Les gammes logiques sont représentées à l'aide de réseaux de Petri ordinaires [Bra, 83] où les opérations sur les produits sont décrites par les transitions et les différents états des produits sont représentés par les places.

3.2.2 Les Gammes Opératoires

Dans un deuxième temps, les gammes logiques sont directement traduites en **gammes opératoires** (*figure I-11-B*) grâce à une prise en compte de plus en plus fine des moyens de production et de transport [Ama, 94]. Modélisées également par Réseaux de Petri, chaque état et chaque lieu sont représentés par une place et chaque opération ou changement de lieu est représenté par une transition [Cru, 91]. Cette étape est réalisée à partir des **relations d'accessibilité** [Ama, 94] inter-ressources et sur définition de **lieux caractéristiques** au sein de ces ressources. Une ressource est en relation d'accessibilité directe avec une autre si un produit peut transiter de l'une à l'autre sans passer par une ressource physique intermédiaire. Le chargement ou le déchargement d'une machine par un robot en est un exemple. Les lieux caractéristiques caractérisent des lieux physiques (emplacement de travail, de transport ou de stockage) mobiles ou non pouvant recevoir un produit. Un lieu physique est caractéristique s'il constitue un lieu de travail ou s'il est en relation d'accessibilité externe c'est-à-dire avec un lieu physique d'un autre moyen de production. Il représente soit une zone de transformation, soit une zone d'accès à une ressource. Dans un souci de lisibilité, nous utiliserons une représentation agrégée pour la gamme opératoire finale (*figure I-11-C*).

3.2.3 Intégration au contrôle-commande

La commande correspond donc à la transcription des modèles de gammes en séquences élémentaires traduisant la coordination du produit et des ressources au sein du Système de Production. Par ailleurs, la commande intègre également les modèles de commande des ressources élémentaires connectées au graphe de coordination par des requêtes génériques de type synchronisation avec accusé de réception [Huv, 94]. Les interactions de ce module avec le module de Supervision permettent de connaître les modèles de commande à activer selon la configuration retenue.

3.3 La Planification/Ordonnancement

Ce module tente de transformer une demande initiale en une commande déterministe prête à être appliquée sur le système [Gen, 00]. En effet, certains indéterminismes tels que ceux de routage peuvent subsister. Les données nécessaires à ce module sont le nombre de pièces à réaliser et les gammes opératoires correspondantes.

L'objectif d'un tel module est de lever tous les indéterminismes présents (quelles pièces produire, avec quelles quantités, quand démarrer chaque opération, ...) afin d'obtenir une commande totalement déterministe en optimisant différents critères : le temps total de production (makespan), l'en-cours du système (palettes transportant les pièces), simplicité de mise en œuvre de la commande trouvée, ...

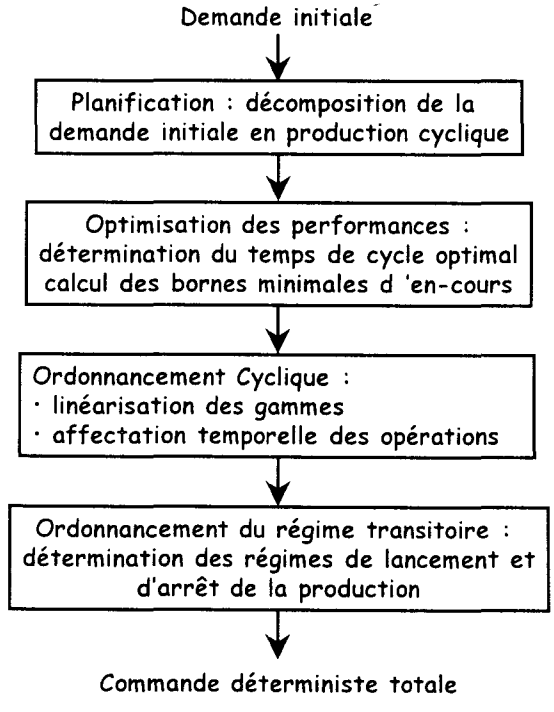


figure I-12. Décomposition en phases de la Planification et de l'Ordonnancement

Étant donné la très grande complexité du problème, ce module procède par phases (*figure I-12*) en hiérarchisant les différents critères considérés. En outre, le grand nombre de pièces à considérer a poussé le module Planification/Ordonnancement vers une commande cyclique. Ceci se traduit par une optimisation d'un nombre réduit de pièces afin d'obtenir un motif (un

cycle) à reproduire autant de fois que nécessaire pour respecter la demande initiale.

3.3.1 La Planification

Le but de la planification est de trouver la meilleure façon de décomposer la demande initiale (30 pièces d'un type A, 30 pièces d'un type B et 30 pièces d'un type C) en production cyclique (par exemple, en 30 cycles formés chacun de 1 pièce de type A, 1 de type B et 1 de type C). Dans cette étape, maximiser le flux (critère principal), minimiser la taille d'un cycle, ...[Cam, 97/b] sont les critères considérés.

3.3.2 Optimisation des performances

L'ordonnancement cyclique [Ohl, 95] permet d'optimiser la commande hors ligne pour obtenir un ordonnancement théorique optimal à appliquer sous conditions idéales et à approcher en cas de dérive. Le critère principal à optimiser dans cette phase d'évaluation est la minimisation du temps total de production. Ceci se traduit, pour une commande cyclique, par la minimisation du temps de cycle. La phase d'évaluation de performances se charge de lever les indéterminismes de gammes et de machines de transformation pour obtenir des gammes linéaires.

3.3.3 Ordonnancement cyclique du régime permanent

Une fois les gammes linéarisées, il devient possible de passer à l'**ordonnancement** proprement dit c'est-à-dire à la détermination de l'en-cours nécessaire ainsi que les dates d'exécution des opérations [Cam, 97/b]. Pour cela, l'algorithme d'ordonnancement a pour but de respecter le temps de cycle optimal (contrainte stricte) et de minimiser l'en-cours. Le résultat obtenu est une commande cyclique évoluant à débit maximal.

3.3.4 Ordonnancement du régime transitoire

Cette commande est en fait un régime permanent qui ne peut être implémenté sans un régime de lancement et d'arrêt (transitoires). Le régime permanent précédemment obtenu est défini sur un cycle. Par conséquent, il ne possède ni de date de début ni de date de fin. Il vient alors que toutes les dates contenues dans le cycle sont candidates à devenir le point d'intersection entre le transitoire de lancement et le permanent. Les travaux menés au sein de

l'équipe PFM ont permis de réduire la combinatoire du problème (en réduisant le nombre de dates à étudier) sans pour autant altérer l'optimalité de la solution de cette phase [Kor, 98].

3.3.5 Intégration au contrôle-commande

Les interactions de ce module avec les autres fonctions du contrôle-commande lui permettent de connaître les ressources disponibles pour une production donnée grâce à la fonction Maintenance. D'autre part, le résultat produit par ce module est fourni à la fonction Supervision sous forme de ratios de production et d'un échéancier concernant l'entrée et les dates dues des pièces à produire et une liste de ressources nécessaires à la production.

3.4 La Surveillance

De manière générale, l'implantation d'un module de surveillance permet de détecter les erreurs de fonctionnement, de les diagnostiquer et d'en assurer le traitement, donc de diminuer le temps de dépannage (maintenabilité). De ce fait, la surveillance contribue à augmenter la productivité par une meilleure maîtrise de la disponibilité des moyens de production. Enfin, elle contribue à la sécurité des hommes, des produits et des machines.

3.4.1 Les différents types de Surveillance

On distingue principalement deux types de surveillance : la **Surveillance de la Commande** et la **Surveillance du Procédé**.

L'objectif de la surveillance de la commande est de s'assurer que la commande émise est en parfaite adéquation avec l'état du procédé. Une telle surveillance est élaborée dans le cadre d'une surveillance réactive au niveau de la détection ce qui permet d'éviter la propagation de défaillance d'un composant vers d'autres composants. La fonction de surveillance de la commande doit être interprétée comme une fonction de sécurité [Tog, 92].

Une approche [Elk, 93], fondée principalement sur les Filtres de Commande, a été développée au sein de notre laboratoire. Le rôle des Filtres de Commande est de vérifier la compatibilité des actions transmises au procédé avec l'état de celui-ci.

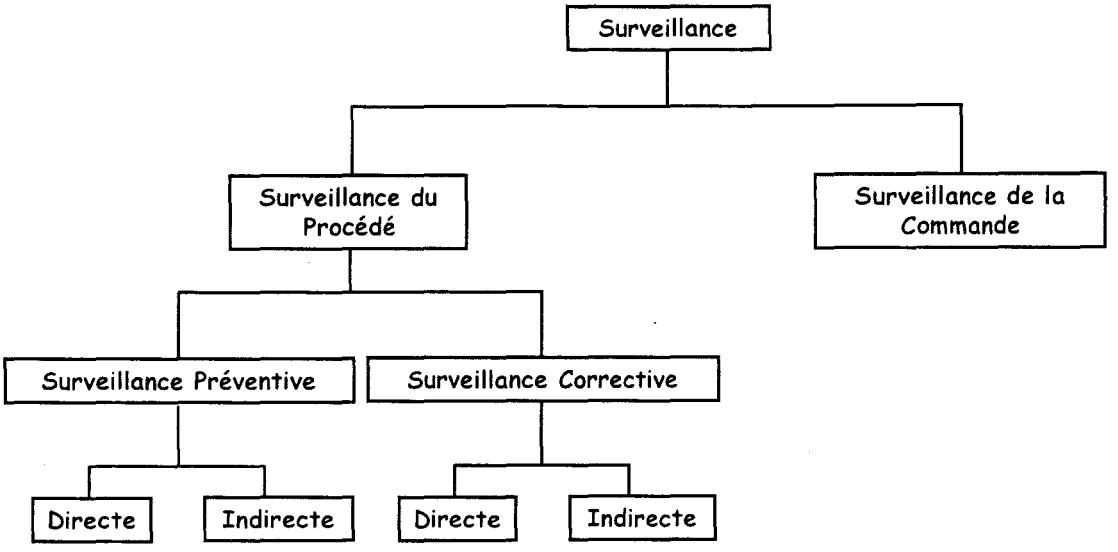


figure I-13. Les différents types de Surveillance

La surveillance du procédé peut être divisée en deux types de surveillance : la **surveillance corrective** et la **surveillance préventive** (*figure I-13*).

La surveillance corrective se situe dans le cadre de la maintenance corrective. Son objectif est de détecter et diagnostiquer les dysfonctionnements du procédé. En règle générale, la localisation de l'origine de tels dysfonctionnements conduit à des actions de maintenance corrective. Dans ce contexte, deux approches complémentaires ont été développées. La première, fondée sur le concept du Contrôle de Commandes, peut être qualifiée de surveillance corrective directe. Le rôle du Contrôle Commande est de vérifier en temps réel la réalisation des actions reçues par le procédé afin d'assurer la fiabilité du système de commande. La seconde [Tog, 92], propose une surveillance corrective indirecte du procédé en ligne. Elle s'appuie sur l'exploitation d'un modèle fonctionnel, le Graphe Fonctionnel (GF) et d'un modèle structurel.

La surveillance préventive consiste à mesurer, de manière périodique ou en continu, des paramètres décrivant au mieux l'état d'un équipement afin de déterminer le moment où il faudra intervenir. Ce type d'activité est basé sur les données réelles. La surveillance préventive peut être directe (suivi par des capteurs spécifiques) ou indirecte (analyse des effets induits sur les produits).

La surveillance préventive indirecte consiste à surveiller les ressources à partir des perturbations qu'elles engendrent sur les produits. La surveillance peut être basée sur le suivi du flux de production [Ly, 99]. Un écart entre le nombre de pièces qui rentrent et le nombre de celles qui sortent signifie qu'il y

a nécessairement une dégradation de performances du système. Elle peut être également basée sur la qualité du produit [Nab, 00]. L'approche proposée repose sur l'existence d'une corrélation entre les paramètres de qualité et les ressources dont les défaillances peuvent influer la qualité.

3.4.2 Les activités de la Surveillance

Quel que soit le type de surveillance choisie, ses principales activités sont la **détection** et le **diagnostic** des dysfonctionnements des différents éléments du Système de Production.

Le rôle de la détection est de détecter les situations de défaillance. Il est donc nécessaire de connaître toutes les situations ou défaillances conduisant à de tels états. Le problème de base soulevé par cette fonction est le choix du critère utilisé pour distinguer les situations normales des autres : dresser une liste exhaustive des défaillances paraît illusoire. C'est pourquoi on considérera que tout ce qui entraîne une déviation entre le service spécifié et le service délivré est dû à une défaillance [Cha, 95]. Les principales techniques de détection reposent sur la détection de l'écart de comportement du système réel avec celui de son modèle.

Le rôle du diagnostic est de déterminer les causes ayant entraîné une détection de la déviation du comportement. La comparaison avec le milieu médical permet de mieux appréhender la notion de symptôme et de cause [Com, 91]. L'observation des symptômes que présente un malade permet au médecin d'établir un diagnostic et donc de déterminer la cause de la maladie. La fonction diagnostic d'un module de surveillance doit, à partir de la détection d'un symptôme (situation anormale), déterminer l'élément défectueux. La principale difficulté, pour la mise en place de cette fonction, est de dresser une liste exhaustive qui permet d'établir des liens de cause à effet entre les symptômes et les causes. Ceci est d'autant plus complexe qu'un même symptôme peut apparaître pour des causes différentes. La fonction de diagnostic fait généralement appel, pour des systèmes complexes, à des techniques d'intelligence artificielle basées sur l'apprentissage et à des systèmes basés sur un modèle formel du procédé commandé.

3.4.3 Intégration au contrôle-commande

La surveillance rend possible l'accès, "en temps réel", aux informations concernant le procédé nécessaires aux autres fonctions du contrôle-commande.

C'est ainsi que la mise en place d'un module de Surveillance permet au système de valider son propre fonctionnement et de communiquer son état aux utilisateurs (les autres modules). C'est pourquoi nous considérons la surveillance comme un système informationnel alimentant en données les autres fonctions du contrôle-commande.

3.5 La Maintenance

La Maintenance consiste en un certain nombre d'activités qui permettent de mettre en œuvre des actions pour maintenir ou remettre une entité dans un état lui permettant de délivrer une fonction requise. La gestion de ces équipements est devenue un enjeu clé de la productivité et de la compétitivité des Systèmes de Production. Pour cela, la maintenance doit être capable de s'organiser afin de répondre aux contraintes de production en terme de qualité du service délivré par les équipements, et de disponibilité. Cette organisation, en phase de conception, passe par le choix d'une politique de maintenance (ou stratégie de maintenance) qui est fonction du système et des types de défaillance auxquelles elle va permettre de faire face.

3.5.1 Les stratégies de Maintenance

On distingue principalement deux politiques de maintenance : la **Maintenance Corrective** et la **Maintenance Préventive** (*figure I-14*).

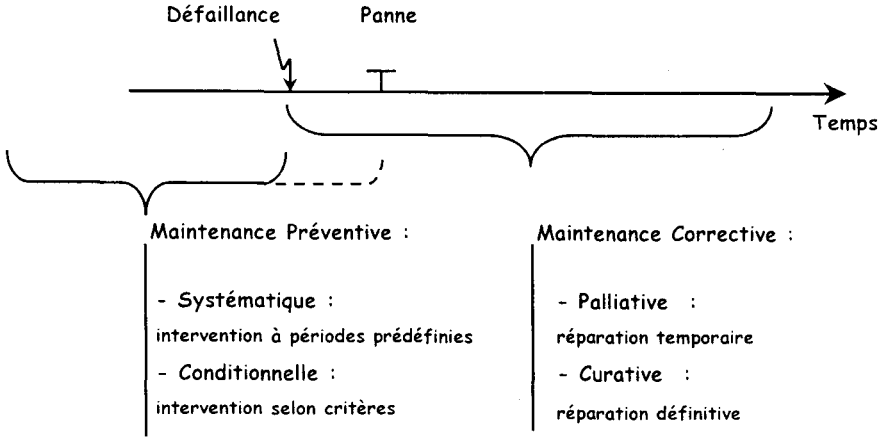


figure I-14. Les différentes stratégies de maintenance.

La Maintenance Corrective concerne les actions menées après la détection d'une défaillance et son objectif est de remettre une entité dans un état lui permettant de délivrer une fonction requise même de façon provisoire. Elle

concerne notamment les défaillances catalectiques (Chapitre I, §. 2.2.1). La Maintenance Corrective peut être divisée en deux types de maintenance : la **Maintenance Palliative** et la **Maintenance Curative** (*figure I-14*).

La Maintenance Préventive concerne les actions menées avant l'état de panne (ou même de défaillance) d'une entité (*figure I-14*). Ces interventions sont effectuées selon un échéancier préétabli (temps, nombre de cycles, ...), ou des critères prédéfinis (une information d'un capteur, une mesure, ...). On distingue principalement deux types de maintenance : la **Maintenance Préventive Systématique** et **la Maintenance Préventive Conditionnelle** (*figure I-14*).

3.5.2 Les activités de la Maintenance

Quelle que soit la politique de maintenance retenue, celle-ci sera caractérisée en phase d'exploitation par différentes activités. Elles peuvent être regroupées en trois catégories : la **surveillance**, la **maintenance** dans le sens intervention et la **gestion** (technique et administrative) (*figure I-15*).

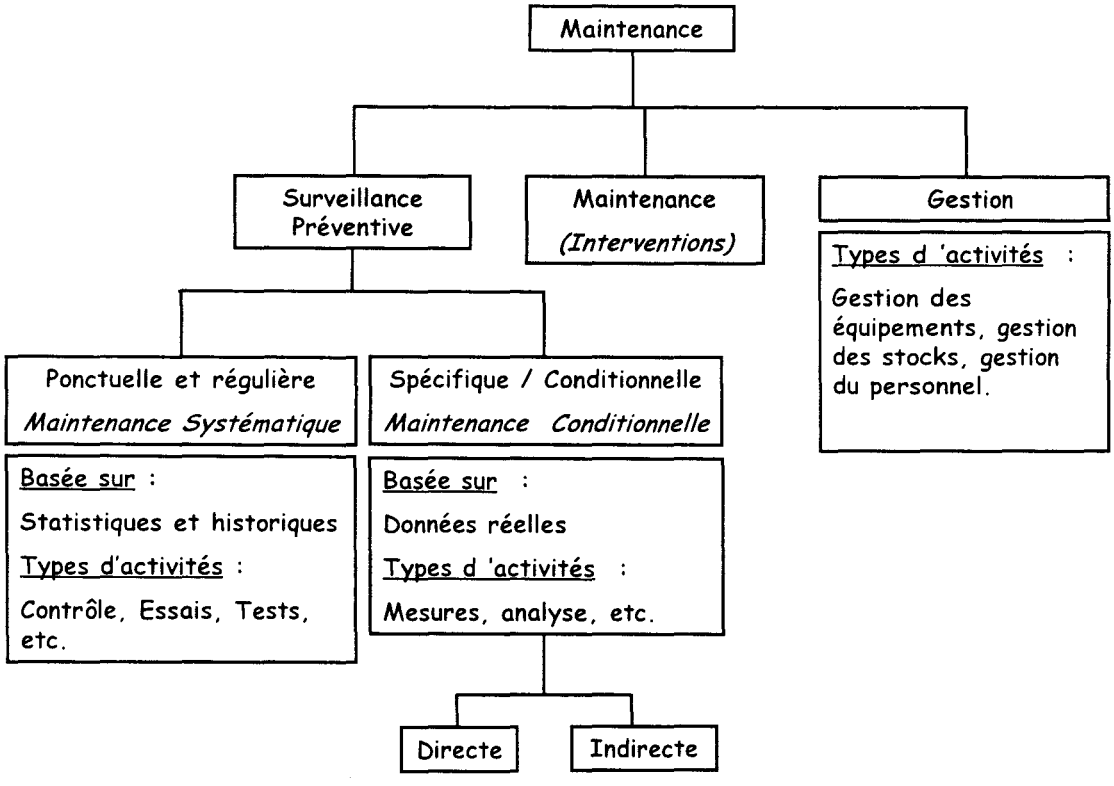


figure I-15. Les activités de la Maintenance.

Dans le cadre de la surveillance des équipements, la Maintenance comporte deux types d'activités préventives : les activités **ponctuelles et régulières**

(Maintenance Systématique) et les activités de **surveillance spécifique** ou **conditionnelle** (Maintenance Conditionnelle). La **gestion** des activités consiste à planifier et à mettre en œuvre les différentes activités de la Maintenance.

3.5.3 Intégration au contrôle-commande

D'un point de vue intra-module [Ly, 99], la fonction **Ordonnancement** du module de Maintenance (*figure I-10*) gère et planifie les ressources matérielles et humaines participant à la réalisation des opérations de Maintenance. La fonction de **Décision** a un rôle de coordination et de décision des tâches de Maintenance. Enfin, la fonction **Opérationnelle** est chargée d'effectuer les interventions selon le plan établi par la fonction Ordonnancement. Les interventions du module de Maintenance sont dues à trois types d'événements : les tâches de maintenance systématique, les résultats de la surveillance conditionnelle, les résultats de la surveillance curative.

D'un point de vue contrôle-commande, le module de Maintenance (*figure I-10*) détermine et indique aux fonctions Planification/Ordonnancement et Supervision les ressources qui sont disponibles pour une production. En outre, suivant l'échéancier des tâches de maintenance et les informations fournies par la fonction Surveillance, elle indique à la fonction Supervision quelles sont les ressources sur lesquelles elle doit intervenir et par conséquent leurs indisponibilités.

3.6 La Supervision

La Supervision contribue à l'augmentation de la disponibilité et de la sécurité des personnes et des moyens de production. C'est dans ce sens qu'elle concourt à la sûreté du système. C'est dans ce cadre de la Supervision que nous avons axé nos travaux.

La Supervision regroupe un ensemble de fonctions en interaction avec toutes les autres composantes du Système de Production, y compris la composante humaine.

La Supervision est définie par R. Isermann [Ise, 96] comme la surveillance d'un système physique et la détermination d'actions appropriées pour maintenir les opérations dans le cas de fautes. Pour nous, les objectifs de la

Supervision, dans un contexte de tolérance aux fautes, peuvent être alors résumés comme suit :

- assurer le respect des objectifs de production et des contraintes de sécurité et empêcher les dérives du système commandé,
- assurer la continuité du service lors de l'occurrence d'une défaillance.

La fonction Supervision doit être à la fois "intelligente" et réactive. En effet, les dysfonctionnements relevés par la surveillance sont pris en compte par la supervision afin de réduire les temps de non-productivité. Pour cela, elle doit être capable, connaissant l'état du système, de déterminer et mettre en œuvre des solutions afin de trouver un compromis entre les objectifs de production et ceux de la Sûreté de Fonctionnement.

En outre, la Supervision assure une aide à la conduite du système, principalement en prenant en "temps réel" les dernières décisions concernant les degrés de liberté encore présents dans la commande.

De part ces objectifs, la Supervision est au carrefour d'une multitude d'informations qu'elle doit gérer. La Supervision intervient alors pour :

- lever les derniers indéterminismes. Bien que la commande résultant de la Planification/Ordonnancement soit déterministe, il reste tout de même des indéterminismes au niveau du routage. Ce type de degré de liberté est ainsi conservé jusqu'au "dernier moment",
- paramétrer la commande séquentielle et les modèles de la surveillance compte tenu des états des ressources à activer,
- modifier, quand cela est nécessaire, la configuration de la commande et du procédé afin de répondre aux objectifs fixés.

La combinaison de ces actions fait apparaître deux types de situation :

- les situations dîtes "normales" ; elles correspondent à toutes les situations qui ont été prévues,
- les situations dîtes "anormales" ; elles correspondent à toutes les situations non prévues (par exemple suite à une défaillance).

La difficulté d'une telle fonction vient du fait qu'une fonction intelligente est très difficilement réactive [Tog, 92]. Ainsi, la Supervision sera composée de fonctions qui interviendront sur plusieurs niveaux d'une hiérarchie du procédé

calquée sur des horizons temporels différents. Ces fonctions sont appelées, au sein du LAIL : Recouvrement, Pilotage et Gestion des Modes. Le rôle de chacune de ces fonctions fait l'objet d'une partie du chapitre suivant. Notre contribution concerne la Gestion des Modes.

CONCLUSION

A une époque où la productivité et la rentabilité prennent de plus en plus d'importance, et du fait de la complexité des Systèmes de Production, il est nécessaire d'intégrer les concepts liés à la Sûreté de Fonctionnement. Le projet CASPAIM, qui initialement couvrait uniquement l'aspect commande, s'est orienté vers cette intégration par l'analyse et la conception d'autres composantes tels que la Surveillance, la Maintenance et la Supervision.

Notre objectif, à travers la Supervision, est de garantir les objectifs de production tout en tenant compte des différentes contraintes auquel est soumis le système : consignes de la Planification/Ordonnancement, de la Maintenance, de la Surveillance, de l'opérateur et des perturbations subies par le système.

Notre contribution est axée plus particulièrement sur la Gestion des Modes, fonction de la Supervision. Pour cela, nous supposons que le système étudié est représentable par un modèle à événements discrets. De part nos objectifs, nous sommes dans un contexte de tolérance aux fautes où le cas des défaillances simultanées n'est pas pris en compte. En outre, nous considérons uniquement les défaillances du procédé, la commande étant exempte d'erreurs.

A travers les définitions et les concepts présentés, ce chapitre nous a conduit à la caractérisation de notre contexte d'étude. L'étude, dans le chapitre suivant, de la chaîne de réaction de la Supervision en présence d'une défaillance, va nous permettre de préciser la problématique abordée.

Chapitre II

Du processus de Reconfiguration à la Gestion des Modes

INTRODUCTION

Dans un contexte de tolérance aux fautes (Chapitre I, § 2.4.5), il est naturel de s'intéresser au traitement qui permet au système de remplir ses fonctions en dépit des fautes apparues. L'étude du traitement de fautes va nous permettre de préciser la problématique traitée dans ce mémoire.

Dans un premier temps, après un rappel des actions à envisager pour palier une défaillance, nous nous intéressons plus particulièrement à l'une d'entre elles : la reconfiguration. A travers l'étude d'un certain nombre d'approches, notre premier objectif est de définir, d'une manière générale et indépendamment de toutes méthodes et formalismes, le principe de la reconfiguration.

Dans un deuxième temps, nous nous intéressons à la mise en œuvre d'un tel principe dans notre contexte de contrôle/commande (Chapitre I, § 3). Notre but est de définir les objectifs de la fonction de Gestion des Modes, objet de nos travaux. Ainsi, cette partie conduit à la caractérisation de notre problématique.

1 LE PROCESSUS DE RECONFIGURATION

1.1 Du recouvrement à la reconfiguration

1.1.1 Introduction au recouvrement

La notion de recouvrement est issue du domaine informatique. Elle désigne une des phases du traitement d'erreur qui permet de substituer un état exempt d'erreur à l'état erroné [Lap, 95]. Étendu aux Systèmes de Production, le recouvrement regroupe un ensemble ordonné d'actions correctives modifiant le comportement du système afin d'en accroître la sécurité et la disponibilité.

L'occurrence d'une défaillance sur le procédé déclenche, après les phases de détection et de diagnostic, la mise en œuvre d'actions de recouvrement. Ces actions modifient la partie commande en reparamétrant ses modèles. La plupart des actions sur la partie opérative se déduisent des actions menées sur la partie commande. Ces actions sont réparties en trois familles [Cra, 89], [Sah, 92] :

- le gel de la commande qui consiste à figer dans l'état certains processus de la commande ; il est alors impossible d'envoyer des ordres de la partie commande vers la partie opérative,
- la reprise qui consiste à ramener le système dans un état stable précédent l'erreur [Aus, 94],
- la reconfiguration qui consiste à modifier la structure du système. Dans ce sens, l'AFNOR [AFN, 91] définit la reconfiguration comme un processus de réorganisation physique ou logique des postes de travail en terme d'implantation ou d'allocation des produits et/ou des activités. Dans un contexte de tolérance aux fautes, la reconfiguration apparaît alors comme un moyen de faire face à une défaillance tout en maintenant le service pour lequel le système a été conçu.

Nous venons de définir les objectifs du recouvrement. Afin de pouvoir dégager les principes de sa mise en œuvre, nous nous intéressons à un certain nombre d'approches développées dans des laboratoires français. Cette liste de travaux n'est en rien une liste exhaustive.

1.1.2 Différentes approches

ASPIC - LAIL, Lille

L'objectif de l'équipe **A**nalyse et **S**urveillance des **P**rocessus **I**ndustriels **C**omplexes (**ASPIC**) du **LAIL** est de définir les différentes reconfigurations possibles suite à un ensemble de défaillances détectables et localisables.

L'approche proposée [Geh, 99] est basée sur la notion d'équipement (moteur, capteur, ...) et sur une approche ascendante. Un modèle générique, applicable à tous les niveaux d'abstraction du système, permet de modéliser le fonctionnement normal du système et de gérer les ressources défaillantes.

Le fonctionnement normal d'un équipement est décrit par un graphe états-transitions (*figure II-1*) dont les états correspondent aux modes d'utilisation [Geh, 99] de l'équipement. Les transitions, quant à elles, représentent le passage d'un mode vers un autre. Un mode d'utilisation est caractérisé par une mission (ou un ensemble de missions) correspondant à un objectif à atteindre à un instant donné et à des services qui permettent sa réalisation.

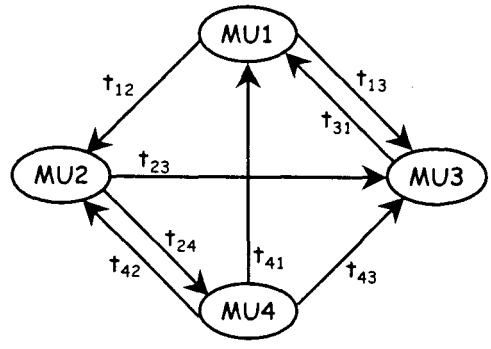


figure II-1. Graphe des Modes d'Utilisation d'un équipement

Afin que la défaillance d'une ressource n'entraîne pas systématiquement l'indisponibilité d'un service, la notion de version d'un service a été introduite. Un service est alors défini par un ensemble pré-ordonné de versions, correspondant à plusieurs traitements rendant ce service. Les ressources

utilisés pour obtenir les versions sont distincts. Un service est dit disponible s'il existe une version de ce service dont l'ensemble des ressources est non défaillant. Le choix d'une version repose alors sur la disponibilité d'une ressource c'est-à-dire sur le fait qu'elle peut être utilisée ou non. Le changement de version dans un service permet ainsi une reconfiguration appelée reconfiguration du système.

L'association du mode d'utilisation, choisi par l'utilisateur, et l'état opérationnel des ressources, subi par l'utilisateur, est appelée mode de marche. A. Bouras [Bou, 97] définit le mode de marche d'un équipement comme étant la liste des versions disponibles des services d'un mode d'utilisation. La gestion de ces modes de marche permet une reconfiguration appelée reconfiguration des objectifs du système. En effet, lorsqu'une mission d'un mode d'utilisation ne peut plus être réalisée, c'est-à-dire qu'aucune reconfiguration du système n'est possible, plusieurs cas sont envisagés pour déterminer le type de reconfiguration :

- il s'agit du mode d'utilisation courant : ses missions ne pouvant plus être poursuivies, un basculement vers un mode de repli est alors effectué,
- il ne s'agit pas du mode courant d'utilisation : tout basculement vers ce mode est alors interdit.

Ainsi, la reconfiguration du système et la reconfiguration des objectifs contribuent à la tolérance aux fautes en ne bloquant pas systématiquement le système lors de la défaillance d'une ressource [Sta, 98].

LAI, Lyon

Les travaux du **LAI** (**L**aboratoire d'**A**utomatique d'**I**ndustrielle) de Lyon ont pour objectif de garantir un service acceptable lors de l'occurrence d'une défaillance quelle que soit sa nature (humaine, logicielle ou matérielle). L'approche proposée [Nou, 97], basée sur la théorie des automates, permet de basculer d'un mode de fonctionnement nominal à un mode de fonctionnement dégradé, lors de l'apparition d'une défaillance. Cette approche introduit la notion de sécurité opérationnelle. Par définition [Nie, 92], la sécurité opérationnelle a pour objet l'assurance du fonctionnement sûr d'un système pris dans son ensemble (moyens de production, produits et opérateurs). Dans ce contexte, il est indispensable de connaître les situations de

dysfonctionnement (déduites d'une analyse des risques) ainsi que les spécifications de récupération (les compensations).

L'approche proposée consiste à adjoindre un module de surveillance à la commande par supervision. Le rôle de la surveillance est de prendre en charge la reconnaissance et la gestion des situations jugées anormales [Nou, 97]. Elle est, de ce fait, composée des fonctions de détection/observation et de compensation/recouvrement. Le principe d'une telle approche est de détecter les déviations comportementales du procédé, puis de compenser les défaillances apparues pour assurer une certaine continuité du fonctionnement du système. Les défaillances sont ici explicitement prises en compte en étant prévues et modélisées. Le fonctionnement pendant la période de compensation qui débute dès l'apparition d'une défaillance et cesse lors de la reprise, est appelé fonctionnement en mode dégradé.

L'observateur a pour rôle de suivre l'évolution du système, de détecter les déviations comportementales et d'en avertir le compensateur. Pour cette dernière fonction, l'observateur doit fournir au compensateur des informations sur la défaillance apparue et sur l'état du procédé (*figure II-2*). Rappelons qu'un même symptôme peut avoir plusieurs causes selon l'état du procédé, il en découle donc des compensations différentes suivant la défaillance et l'état du système.

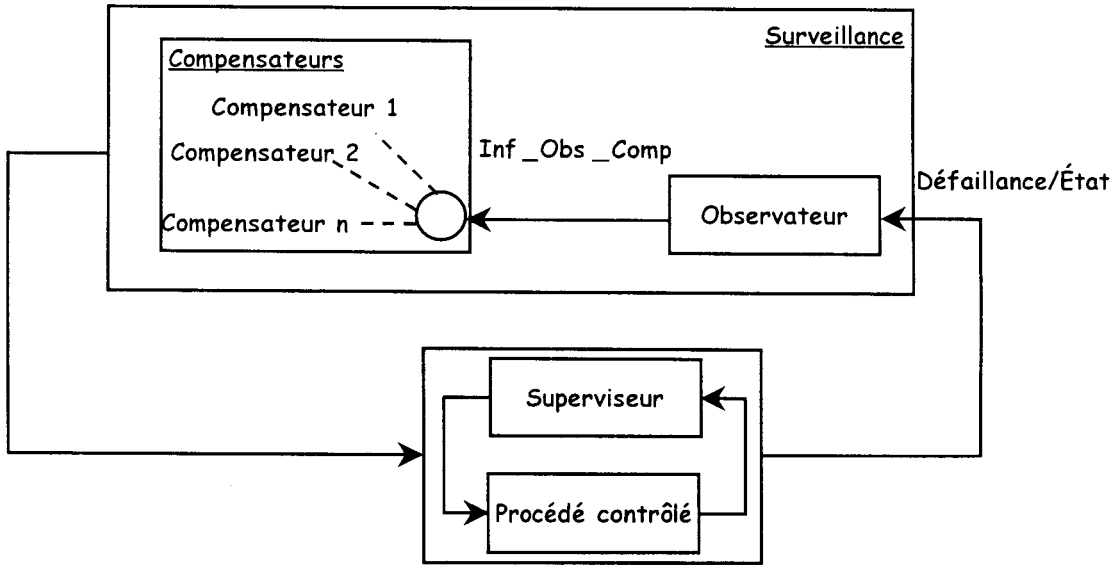


figure II-2. Schéma global du module de surveillance et du contrôle-commande

Un compensateur est un superviseur spécifique, distinct de celui dédié à la commande, qui permet d'assurer la continuité du fonctionnement du système en compensant la défaillance apparue. Lors de la commutation du superviseur nominal vers un compensateur, le superviseur nominal est figé tandis que le compensateur est activé. Après la reprise, la situation est inversée.

Une fois la phase de modélisation élaborée, la synthèse du modèle est réalisée hors ligne à l'aide du logiciel TCT basé sur les concepts de la théorie des automates. L'utilisation des approches par automates permet d'étudier la contrôlabilité des spécifications. L'implantation d'une telle approche résulte d'une traduction des observateurs et des superviseurs de compensation sous forme de grafcets.

LAMIH, Valenciennes

Les travaux de l'équipe **G**énie **I**ndustriel et **L**ogiciel (**GIL**) du **L**aboratoire d'**A**utomatique et **M**écanique **I**ndustrielles **H**umaines de Valenciennes (**LAMIH**) concernent l'exploitation des SAP. Ces travaux reposent sur une description des modes d'exploitation explicitée dans le **M**odèle d'**E**xploitation des **S**ystèmes **A**utomatisés de **P**roduction (**MESAP**). Ce modèle [Par, 92], basé sur une décomposition structurelle du SAP, met en évidence différents niveaux d'abstraction tels que le niveau de flux de pièces, le niveau composant et les niveaux applications.

La reconfiguration d'un SAP est définie par M. Dupas [Dup, 99] comme étant *une modification de son comportement dynamique (modes d'exploitation) afin qu'il maintienne les performances souhaitées.*

Le processus de réalisation d'une telle reconfiguration est décomposé en deux parties :

- la première concerne la détermination de la reconfiguration en terme de flux de pièces et est confiée à la fonction de conduite (niveau stratégique, *figure II-3*),
- la seconde concerne la mise en œuvre de la reconfiguration (de la commande et des modes d'exploitation) et est confiée au niveau exécutif (niveau tactique, *figure II-3*). L'objectif est de déterminer les états intermédiaires (états de mode d'exploitation prédéfinis) permettant d'atteindre un état objectif à partir d'un état de reprise.

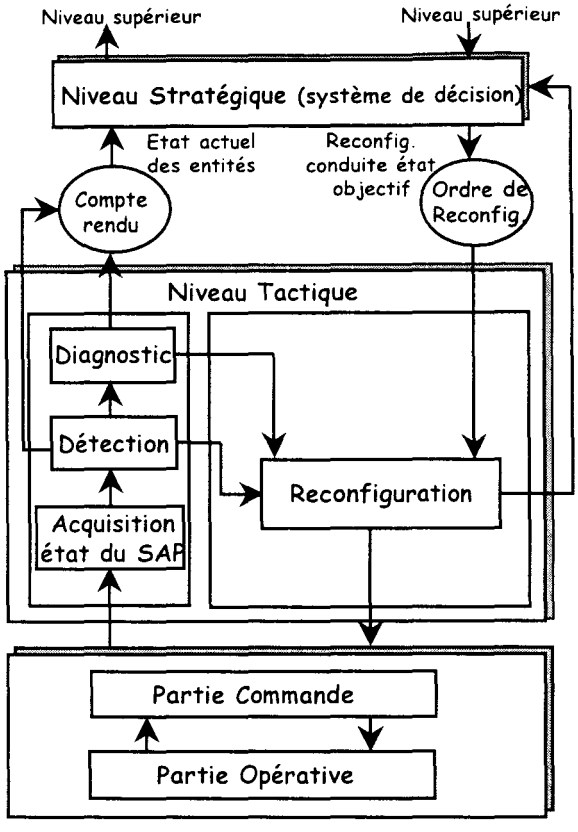


figure II-3. Interaction conduite / commande [Dup, 99]

La prise de décision concernant la détermination des actions à mener (états objectifs) est basée sur l'évaluation, au niveau conduite, de chacune des reconfigurations possibles du SAP [Roj, 96]. Ainsi, une ou plusieurs opérations de la gamme de fabrication peuvent être suspendues, des changements d'affectation des opérations peuvent être effectués. La définition des solutions repose sur des stratégies à court terme, utilisant le mode dégradé ou la réparation de la ressource défaillante, et sur des stratégies à moyen terme par la reconfiguration du système. Ainsi, la décision de la reconfiguration est fondée sur une évaluation du temps nécessaire à l'élaboration des solutions et sur une estimation du temps de production.

En ce qui concerne la mise en œuvre de la reconfiguration [Mab, 96], l'objectif en exploitation, est de proposer une méthode d'aide à la reconfiguration des SAP. En partant du principe que l'état défaillant est non prévisible, alors l'état objectif ne peut être atteint directement.

Une première étape non systématiquement automatisable est alors nécessaire pour amener le système dans un état intermédiaire E_r (état de

reprise) connu a priori. Connaissant l'état objectif défini par le niveau stratégique, c'est l'opérateur qui détermine un état intermédiaire de reprise.

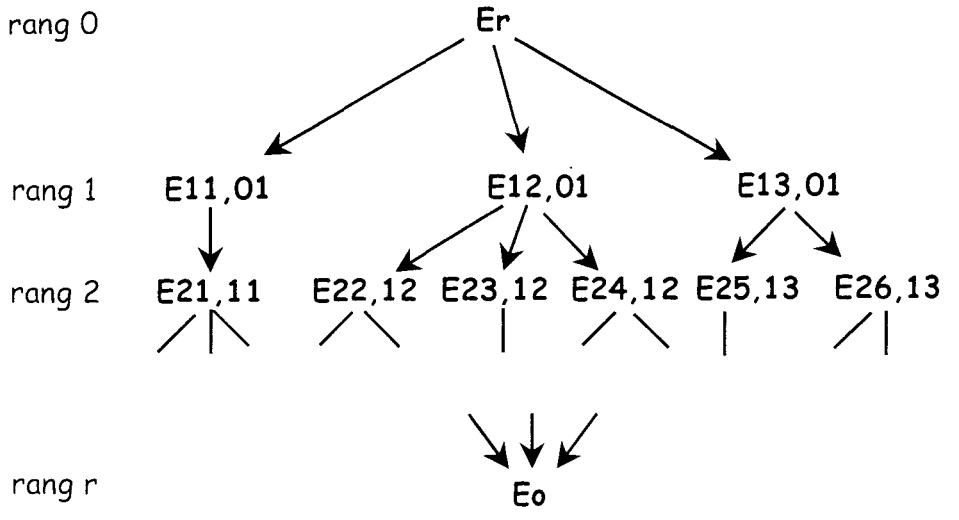


figure II-4. Structure arborescente [Mab, 96]

Une deuxième étape automatisable permet d'atteindre l'état objectif. L'ensemble des séquences d'évolution des modes d'exploitation permettant d'atteindre l'état objectif, est appelé scénario de reconfiguration. Chaque scénario concerne d'une part la reconfiguration des modes d'exploitation et d'autre part la reconfiguration de la commande. La démarche proposée, pour la reconfiguration des modes d'exploitation, a pour objectif de déterminer tous les scénarios qui permettent la reconfiguration des modes d'exploitation suite à la demande de la fonction conduite ou à l'occurrence d'un dysfonctionnement. L'idée retenue est de caractériser l'ensemble d'états de modes d'exploitation d'une entité du système par un "graphe d'états" orienté. Les nœuds du graphe représentent alors les états stables (état commandable à partir duquel la reprise est possible) et les arcs spécifient les relations d'accessibilité entre les modes. La reconfiguration d'un SAP consiste alors à parcourir un ensemble de chemins contraints entre eux (*figure II-4*). Une fois les scénarios et les modules de reprises élaborés, le choix du scénario retenu est établi suite à une évaluation par simulation. Le critère d'évaluation est le temps minimal pour reconfigurer le système.

LAAS, Toulouse

Le **L**aboratoire d'**A**nalyse et d'**A**rchitecture des **S**ystèmes (LAAS) propose initialement une approche pour la surveillance des systèmes temps réel. La

surveillance est définie comme l'ensemble des traitements temps réel concernant les défaillances du procédé [Bon, 93]. Des travaux plus récents ont conduit à développer une architecture intégrant commande et surveillance-supervision (ou surveillance active) [Zam, 97].

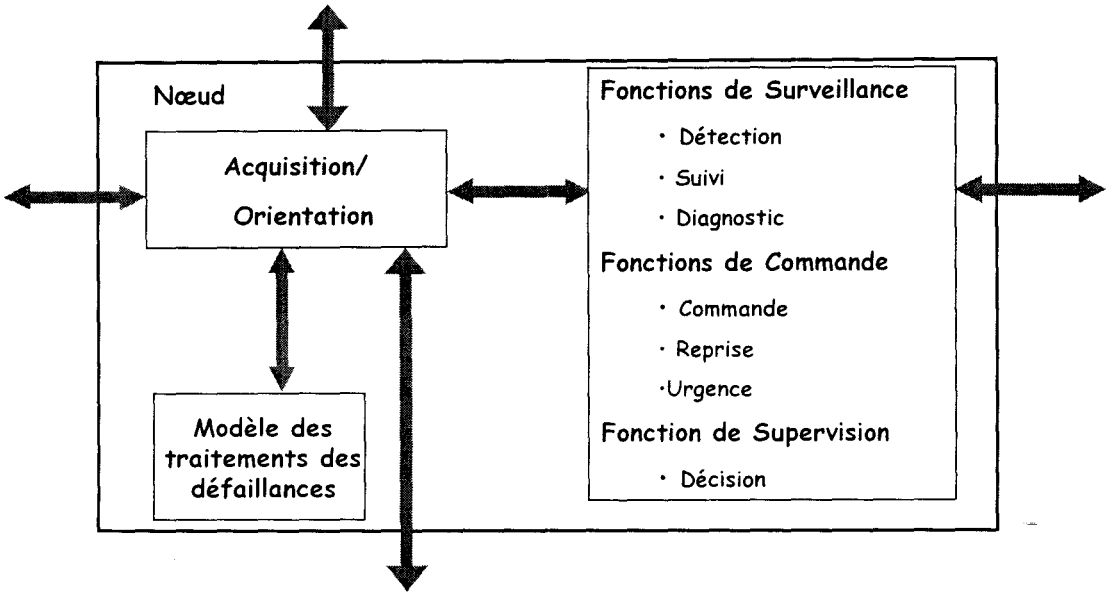


figure II-5. Module générique pour la commande, la supervision et la surveillance [Com, 00]

La structuration adoptée est modulaire et arborescente (*figure II-5*). Chaque nœud comporte les éléments suivants : un bloc d'acquisition et orientation, un modèle des traitements des défaillances et l'ensemble des fonctions de surveillance, de commande et de supervision. C'est le bloc d'acquisition et d'orientation de l'information qui gère toutes ces fonctions. Basé sur un algorithme, c'est lui qui déclenche les fonctions adéquates de surveillance, de commande et/ou de supervision [Com, 98]. Les réseaux de Petri à Objets sont employés comme moyen de spécification dans la plupart des fonctions. Un système d'information vient compléter cette architecture afin de modéliser les informations difficilement modélisables par réseaux de Petri [Cha, 95].

Les réactions d'une telle architecture dépendent des défaillances détectées et également des ressources utilisées, du type de produit fabriqué et de la politique de production spécifiée par l'utilisateur. Les réactions obtenues sont dues à la coopération de plusieurs fonctions génériques :

- le suivi, la détection et le diagnostic (partie surveillance),
- la décision (partie supervision),
- l'urgence, la reprise et la commande (partie commande).

L'activation simultanée et/ou successive de ces fonctions décrit les traitements possibles après défaillance. De cette façon, la séquence classique de surveillance (détection, diagnostic, décision et reprise) n'est plus la seule possible [Zam, 98].

Les travaux sur la fonction de reprise se sont attachés plus particulièrement à dégager les fondements de cette fonction plutôt qu'à sa mise en œuvre. Son but a été défini comme étant de déterminer et d'engager les actions permettant de ramener au mieux le Système de Production dans un état normal, tant du point de vue du potentiel productif que du respect des objectifs de production [Bon, 93]. La fonction de reprise est décomposée en deux sous-fonctions. Les étapes de détermination de l'état des entités et de construction de la séquence d'activité sont réalisées par la fonction de décision. L'étape d'application de la séquence de reprise est réalisée par la fonction de recouvrement. Les types de reprise sont fondés sur le concept d'activité. Selon le contexte, il est envisagé d'abandonner la séquence d'activités contenant l'activité défaillante, de recommencer tout ou une partie de cette séquence ou de continuer. Ces décisions font appel à des connaissances comme le classement des activités selon le caractère réversible ou non de ces dernières, le taux d'occupation des ressources, ...

PFM - LAIL, Lille

Initialement centrée autour de la commande (Chapitre I, § 3.1), l'équipe PFM s'est intéressée aux modifications subies par le système, qu'elles soient dues à une émission d'ordre ou à l'occurrence d'une panne. Cet intérêt a conduit à l'intégration d'un module de Gestion des Modes de Marche. La Gestion des Modes de Marche est définie "*comme la commande effective des machines en intégrant la modification de leurs états*" [Boi, 91]. Dans cette approche, seul l'aspect ressource du SP est pris en compte. La démarche proposée repose sur l'existence de contraintes de fonctionnement entre les ressources de production connexes. Ces contraintes entraînent des dépendances entre les modes de marche et d'arrêt de ces ressources. A partir des spécifications du système (listes des machines et des contraintes), deux

types de description sont élaborés : une représentation par "graphe d'état" et une représentation par table de contraintes.

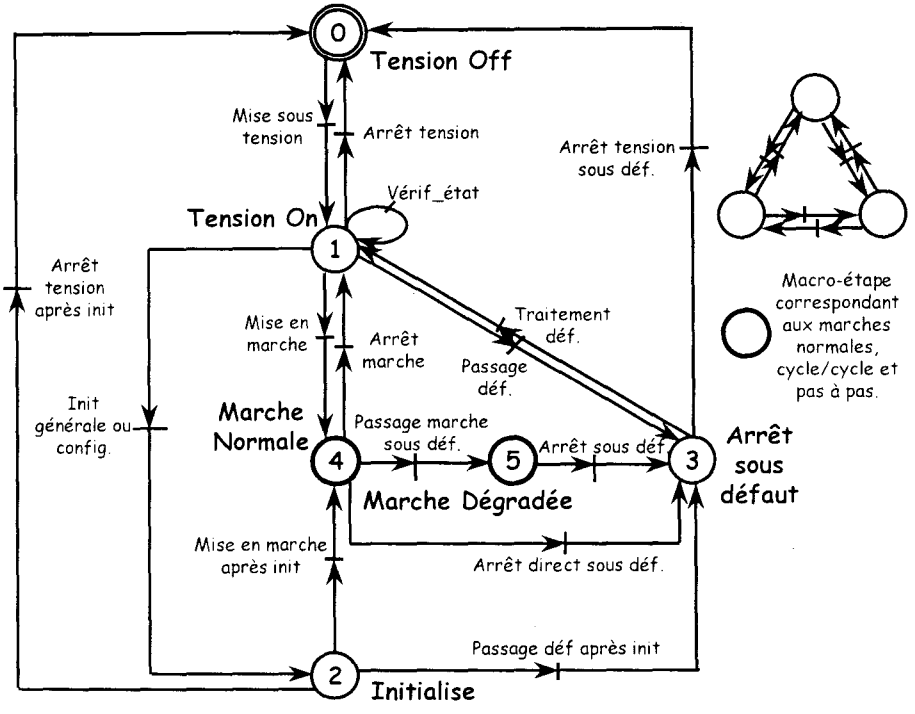


figure II-6. Graphe d'état d'une machine effective

Le principe de modélisation consiste à effectuer des regroupements de machine jusqu'à l'obtention d'un seul groupement. La démarche de modélisation, de type ascendante, est basée sur l'exploitation des contraintes de fonctionnement. Toutes ces contraintes sont représentées par une variante d'arbre "ET/OU" et transcrites dans des tables dites de contraintes. La démarche conduit à l'obtention d'une représentation structuro-fonctionnelle du système.

Dans cette approche, l'objectif est d'assurer la cohérence des commandes effectives de marche et d'arrêt des ressources de production et non la résolution des problèmes de reconfiguration des Systèmes de Production. Les systèmes experts sont utilisés pour la mise en œuvre d'une telle démarche.

Les travaux de L. Kermad [Ker 96] s'inscrivent dans la continuité de ceux de S. Bois [Boi 91]. Ils s'intéressent plus particulièrement à la gestion des modes et des configurations des SFPM. La gestion des modes y est définie comme *"la sélection d'une configuration du système qui concilie les objectifs de production d'une part et l'état courant d'autre part"*.

Ces travaux s'appuient sur une modélisation fonctionnelle par la prise en compte des opérations. La représentation utilisée est une structure arborescente appelée **COD** (**C**hargement **O**pération **D**échargement). L'introduction de la notion de configuration du système consiste à établir un lien entre les opérations du Système de Production et sa structure physique. Une configuration correspond alors à un couple (ressource, opération). Ainsi, contrairement à l'approche de S. Bois, il est possible de représenter les flexibilités d'affectation et la polyvalence de machine.

La représentation COD est employée d'une part pour représenter la structure du Système de Production et d'autre part pour représenter les gammes logiques flexibles. La traduction et l'interaction de ces arborescences permettent la mise à jour réactive de l'état de disponibilité des entités du système et la transmission des ordres de reconfiguration. Les langages synchrones graphiques sont utilisés pour la mise en œuvre d'une telle démarche.

De récents travaux [Ber, 98] ont abordé le problème de la reconfiguration des Systèmes de Production au sens large. En effet, l'objectif n'est plus seulement de gérer les ressources de production en fonction des défaillances survenues mais en tenant compte également des objectifs de production. Ces travaux ont conduit à une nouvelle structuration de la Supervision. En effet, la mise en œuvre de la reconfiguration sollicite trois fonctions : le Recouvrement, la Gestion des Modes et le Pilotage. La première a la charge de déterminer les actions à mener, les deux dernières doivent mettre en œuvre ces actions.

1.2 La reconfiguration : Constats et propositions

Afin de mettre en avant la diversité des termes employés, nous avons volontairement repris le vocabulaire utilisé par les auteurs dans les approches présentées précédemment. Ceci conduit aux constations suivantes :

- Une diversité de termes pour désigner des fonctions qui ont les mêmes objectifs. Prenons quelques exemples. La fonction de recouvrement est définie au LAAS comme une fonction qui applique les décisions déterminées par la fonction de décision. Au LAMIH, une telle fonction est appelée fonction de reconfiguration. Enfin, au LAIL, ce sont les fonctions de Gestion des Modes et de Pilotage qui ont en charge de telles actions,

- Un certain amalgame entre le nom des fonctions et les actions pour lesquelles elles sont sollicitées. L'utilisation des termes tels que reconfiguration ou recouvrement, pour désigner des fonctions du contrôle-commande, conduit à une certaine ambiguïté par rapport aux processus dans lesquelles elles interviennent.

Cette différence terminologique n'a rien de fondamental. En effet, peu importe le terme employé, l'essentiel est de savoir ce qu'il signifie. Cependant, ceci améliore la communication et la compréhension entre les différents auteurs. C'est pour contribuer à cette mise en place d'une terminologie commune que nous nous attachons dans la suite de ce paragraphe à définir un certain nombre de termes génériques. Ce travail s'inscrit dans le cadre de l'action terminologique menée par le Groupement pour la Recherche en Productique – Systèmes de Production Sûrs de Fonctionnement (GRP – SPSF). En effet, un des axes de ce groupe de travail est de dégager une terminologie commune, du moins dans un cadre d'hypothèses, permettant ainsi à chacun d'évoluer et d'être compris par la communauté.

Pour commencer, bien que le terme reconfiguration soit défini par un grand nombre d'auteurs, il ne désigne pas forcement la même chose. Nous avons vu que pour certains, il correspond aux actions (dans le sens physique du terme) qu'il est nécessaire de mener pour modifier la structure du Système de Production. Pour d'autres, il englobe une phase de calcul qui permet de déterminer les actions à mener pour modifier la structure du système en respectant un certain nombre d'objectifs ou de contraintes.

Nous introduisons ici les termes processus de reconfiguration et reconfiguration effective afin de lever une telle ambiguïté [Dan, 00/c].

Définition 1 *: Le processus de reconfiguration ("reconfiguration process")*

Le processus de reconfiguration désigne l'ensemble des actions physiques et logiques qui permettent de mettre l'ensemble du système (partie commande et partie opérative) en accord avec des objectifs quels qu'ils soient (production, sécurité).

Illustration : Considérons l'exemple d'un système de pompage constitué de trois pompes. Supposons que pour répondre aux spécifications nominales du cahier des charges, il soit nécessaire d'utiliser deux pompes sur trois. Supposons maintenant que l'une de ces deux pompes tombe en panne. Dans ce

cas précis, le processus de reconfiguration regroupe l'ensemble des actions qui vont permettre de continuer à pomper malgré la défaillance de cette pompe. Une des solutions consiste à remplacer la pompe défaillante par la troisième pompe non utilisée jusqu'à maintenant. Il est alors nécessaire "d'arrêter" la pompe défaillante et de mettre en service la troisième. L'ensemble de ces choix et de ces actions constitue le processus de reconfiguration.

Définition 2 *: La reconfiguration effective ("effective reconfiguration")*

La reconfiguration effective désigne l'ensemble des actions physiques et logiques qui modifient la structure du système d'un point de vue partie commande et d'un point de vue partie opérative.

Remarque : le terme effectif signifie ici pratique (concret) et est utilisé pour accentuer le sens du terme reconfiguration.

Notons que la reconfiguration effective est un sous-ensemble du processus de reconfiguration. Cependant, si une reconfiguration effective est due au déclenchement d'un processus de reconfiguration, nous verrons par la suite que tous les processus de reconfiguration ne conduisent pas à une reconfiguration effective.

Illustration : Dans le cas de notre système de pompage, la reconfiguration effective correspond aux actions d'arrêt et de mise en service des diverses pompes.

L'étude des différentes approches présentées précédemment montre que le processus de reconfiguration est décomposable en deux parties.

Définition 3 *: La partie décisionnelle ("decision-making part")*

La partie décisionnelle consiste à déterminer un état (ou un ensemble d'états) à partir duquel il est possible de poursuivre la production. Cet état est appelé état objectif.

Illustration : Dans notre exemple, la partie décisionnelle est celle qui décide de l'état objectif à atteindre suite à la défaillance de la pompe. Dans ce cas précis, la décision prise consiste à utiliser la troisième pompe.

Définition 4 : *La partie opérationnelle ("operational process")*

La partie opérationnelle consiste à appliquer les décisions prises par la partie décisionnelle. Elle peut être décomposée en deux sous-parties. L'une qui doit déterminer les actions à mener pour atteindre l'état objectif fixé, l'autre qui met en œuvre ces actions. La reconfiguration effective correspond alors à cette deuxième sous-partie.

Illustration : L'objectif de la partie opérationnelle est de déterminer les actions nécessaires pour que le système de pompage utilise la troisième pompe. Les actions déterminées sont l'arrêt de la pompe défectueuse et la mise en service de la troisième pompe. La partie mise en œuvre (i.e. la reconfiguration effective) correspond aux actions d'arrêt et de mise en service des diverses pompes.

	ASPIC	LAI	LAMIH	LAAS	PFM
Partie Décisionnelle			Niveau Stratégique	Décision	Recouvrement
Partie Opérationnelle	Reconfiguration	Compensation	Reconfiguration	Recouvrement	Gestion des Modes et Pilotage

figure II-7. Récapitulatif des termes employés

Chacune de ces parties, décisionnelle et opérationnelle, est mise en œuvre par une fonction ou un ensemble de fonctions. Dans la figure II-7, nous avons positionné, pour chacune des approches étudiées, le nom de la fonction correspondant à chacune des parties.

La figure II-7 met en évidence le fait que certaines approches ne comportent pas de partie décisionnelle dans la mise en œuvre du processus de reconfiguration. Ceci s'explique par le fait que l'état objectif à atteindre en cas de défaillance est prédéfini. Cet état, dépendant de la nature de la défaillance et de l'état du système, est défini dès la phase de conception.

1.3 Synthèse

Maintenant que nous avons défini un certain nombre de termes, nous nous intéressons au processus de reconfiguration. Rappelons que notre objectif est

ici de définir le principe d'un tel processus de façon générale et indépendamment de toutes méthodes et formalismes.

Après l'étude d'un certain nombre d'approches, nous pouvons dire que le processus de reconfiguration se décompose en trois traitements dont certains peuvent être simultanés [Dan, 00/c].

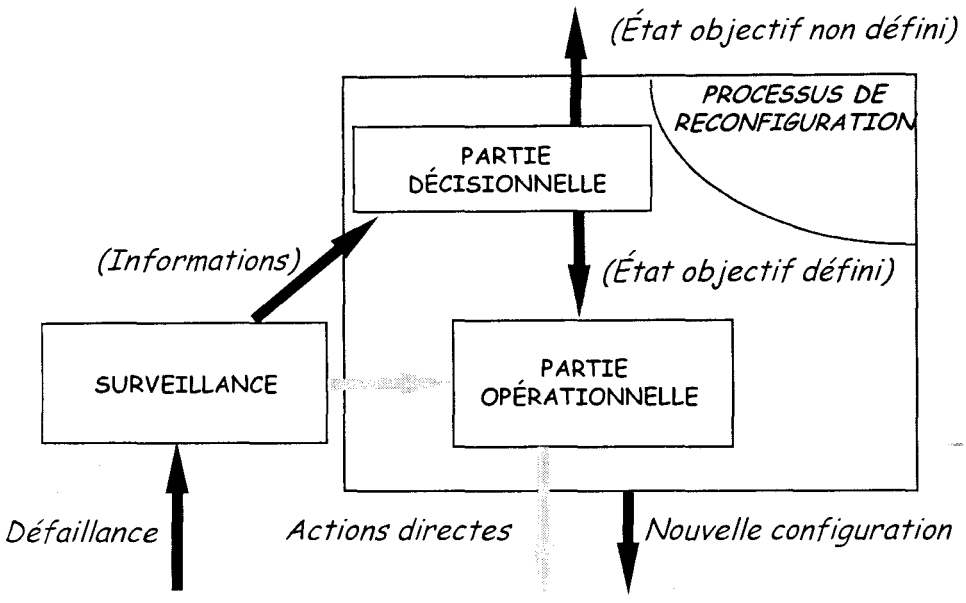


figure II-8. Principe du Processus de Reconfiguration

La première est initiée par un flux d'informations direct entre la partie opérationnelle et la surveillance (figure II-8). Elle consiste à appliquer des actions sur la partie opérative par l'intermédiaire de la partie opérationnelle. Ces actions sont considérées comme immédiates et sont à rapprocher d'actions réflexes. Elles correspondent à des procédures prédéfinies et établies selon le type de la défaillance et l'état du système. Les objectifs de ces actions peuvent être classées en deux catégories :

- les actions d'urgence : elles sont définies pour assurer la sécurité des personnes, des produits et des moyens de production. Ce type d'action est généralement déterminé pour des défaillances jugées critiques ou dangereuses, obtenues par une analyse prévisionnelle. Elles consistent à mettre le système dans un état de repli, de sécurité et ceci quel que soit l'état courant du système. Ce type d'action est présent dans toutes les approches étudiées,

- les actions de compensation : elles sont définies pour assurer la sécurité des personnes, des produits et des moyens de production et également pour assurer le maintien de la production. La solution optimale n'est pas recherchée. Ces actions correspondent souvent à un fonctionnement dégradé du système. Elles permettent de compenser momentanément la perte d'un élément. Ces actions, ou ensembles d'actions, sont également prédéterminées et leurs exécutions dépendent du type de la défaillance et de l'état du système.

L'avantage de ces actions réside dans leur réactivité. Cependant, leur limitation est due à la nécessité de les déterminer dès la phase de conception. En effet, il est nécessaire de prévoir chaque action pour une défaillance donnée dans un contexte donné. Établir une liste exhaustive des défaillances est illusoire, c'est pourquoi une analyse des risques doit être réalisée afin de déterminer les défaillances à prendre en compte. Les flèches grises de la figure II-8 représentent les premières réactions du processus de reconfiguration.

Cette première étape est provoquée par la surveillance qui déclenche également simultanément l'étape 2. En effet, quand une défaillance apparaît, elle est détectée par la surveillance qui en informe simultanément la partie décisionnelle et la partie opérationnelle.

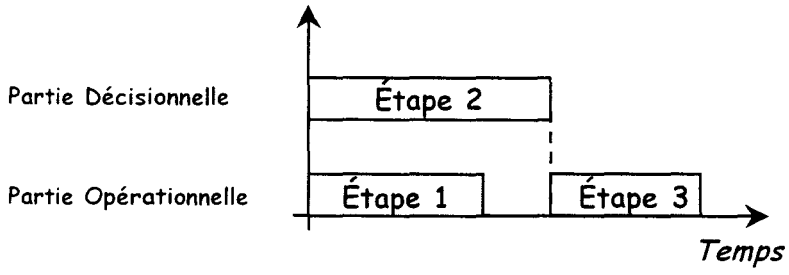


figure II-9. Les étapes du Processus de Reconfiguration

Dans le même temps (Etape 2, *figure II-9*), à partir des informations fournies sur l'état de la partie opérative et des objectifs de production, la partie décisionnelle détermine un nouvel état à atteindre afin de continuer à produire tout en respectant au mieux les consignes de production (Définition 3). Les actions résultantes peuvent être assimilées à des actions différées. La partie décisionnelle peut prendre deux types de décision [Dan, 00/c] :

- une maintenance corrective du système : qui consiste à appliquer des actions telles que l'arrêt du système global et la réparation des ressources défaillantes. Dans ce cas, aucun état objectif n'est défini. Seul un arrêt du système global est demandé et nécessaire (*figure II-8*),
- une production *tout de même* : deux solutions sont alors envisageables.
    - ✧ le premier cas consiste à utiliser la ressource défaillante malgré sa défaillance. Le fonctionnement est considéré comme non optimal mais acceptable pour continuer à produire et à respecter les objectifs imposés,
    - ✧ le deuxième cas consiste à restructurer le système par modification des ressources et/ou des objectifs. La partie opérationnelle est alors sollicitée pour mettre en œuvre une reconfiguration effective (Etape 3, *figure II-9*). Cette dernière concerne la partie commande et également la partie opérative.

Illustration : Dans le cas du système de pompage, une maintenance corrective consiste à réparer la pompe défectueuse. Nous avons vu que le choix de la production *tout de même* consiste à poursuivre le pompage en utilisant la troisième pompe. Cet exemple nous montre que chaque processus de reconfiguration ne conduit pas forcement à une reconfiguration effective. Le choix de l'utilisateur est bien évidemment fonction d'un certain nombre de paramètres tels que les objectifs de production, le temps de mise en œuvre de la reconfiguration effective, la qualité du service délivré, ...

Enfin, nous venons de voir que la troisième étape est déclenchée (Etape 3, *figure II-9*) quand un nouvel état à atteindre est défini ou l'arrêt du système global est demandé. La partie décisionnelle transmet alors son objectif à la partie opérationnelle. La partie opérationnelle a alors en charge de mettre en œuvre une séquence d'actions afin d'atteindre l'état objectif (Définition 4). Ces actions concernent la modification de la partie commande et de la partie opérative. Les flèches noires de la *figure II-8* représentent les étapes 2 et 3.

2 De la Supervision à la Gestion des Modes

2.1 La Supervision

2.1.1 Objectifs

Dans la première partie de ce chapitre, nous nous sommes attachés à décrire les réactions du contrôle-commande d'un Système de Production dans le cas d'une situation dite "anormale" (Chapitre I, § 3.6). Nous avons mis en évidence deux types de sous-systèmes : le sous-système décisionnel et le sous-système opérationnel. Dans notre cas, ces sous-systèmes correspondent à la fonction de Supervision et plus particulièrement à la fonction de Recouvrement d'une part et aux fonctions de Pilotage et de Gestion des Modes d'autre part.

Les objectifs de la Supervision consistent également, dans des situations dites "normales", à gérer les ressources nécessaires à la production et à lever tout indéterminisme et conflit de la commande (Chapitre I, § 3.6).

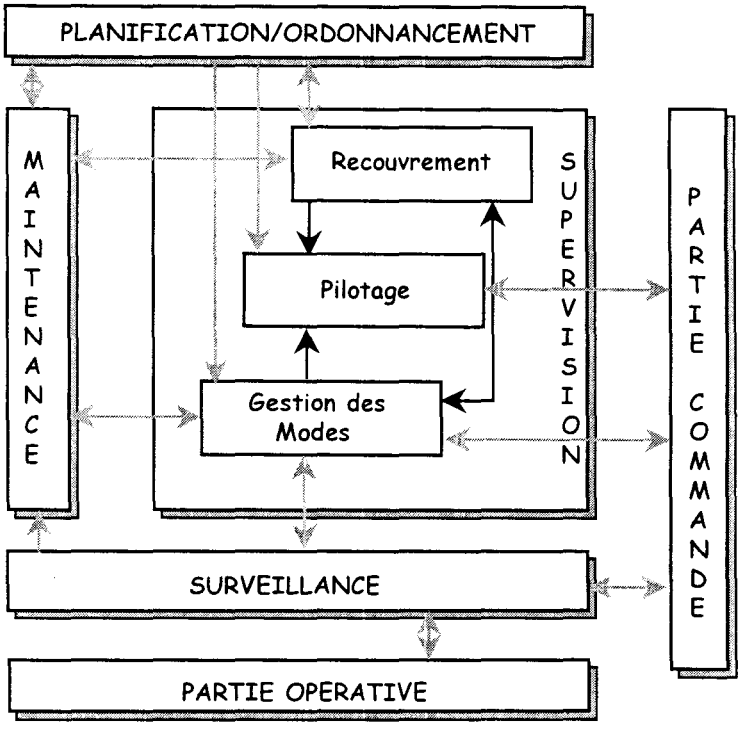


figure II-10. Intégration de la Supervision à la structure du contrôle-commande

L'ensemble de ces objectifs est atteint grâce à l'interaction des trois fonctions de la Supervision. La figure II-10 présente la structuration de la Supervision au sein du contrôle-commande. Les flèches grises représentent les échanges d'informations entre les fonctions de la Supervision et les autres fonctions du contrôle-commande. Les flèches noires indiquent les échanges d'informations au sein de la Supervision.

Les fonctions de Recouvrement et de Pilotage ont été étudiées à travers les travaux de P. Berruet [Ber, 98] et R. Tawegoum [Taw, 95]. Afin de définir les objectifs de la Gestion des Modes, objet de nos travaux, nous présentons chacune de ces fonctions dans les paragraphes suivants.

2.1.2 Le Recouvrement

Après 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. Il est à noter que cet état est différent d'un état de reprise qui consiste à placer le système dans un état correct précédent l'erreur. Lorsqu'une reconfiguration effective du système est nécessaire, les décisions à prendre concernent les pièces en cours de production et présentes dans le Système de Production et les pièces brutes à y rentrer. Les décisions à prendre consistent alors à déterminer les ressources de production et les paramètres nécessaires pour réaliser une gamme opératoire (partielle ou complète). Pour cela le Recouvrement distingue trois types de ressources de production [Ber, 98] [Tog, 00] :

- les ressources engagées en production : ce sont des ressources qui au début de l'horizon de production ont été mises en marche automatique car elles assurent au moins une opération de la Gamme Opératoire d'un des types de pièces à produire sur cette période,
- les ressources en attente : ce sont des ressources qui sont arrêtées dans un état d'attente (initialisées) et qui peuvent être mises rapidement en marche automatique en cas de besoin,
- les ressources à l'arrêt : ce sont des ressources à l'arrêt hors tension ne pouvant potentiellement assurer aucune opération de transformation dans le contexte actuel ou devant impérativement subir une opération de maintenance rendant impossible leur utilisation sur l'horizon de production.

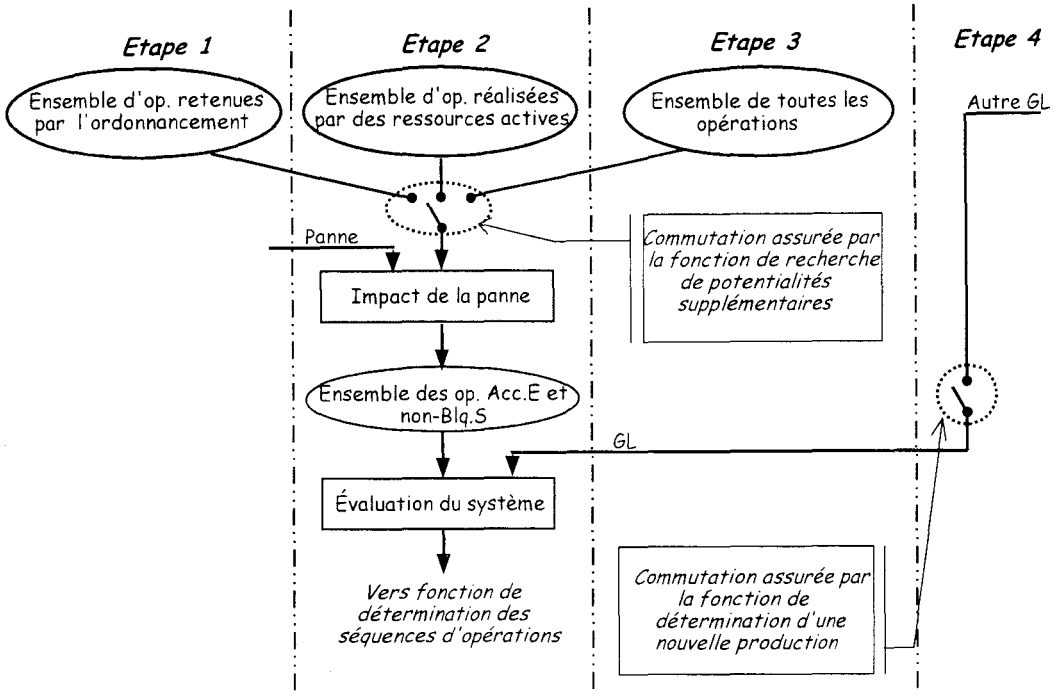


figure II-11. Recherche progressive de potentialités [Ber, 98]

Cette classification des ressources nous a amené à considérer trois types de décisions de reconfiguration effective [Ber, 99/a] :

- une reconfiguration mineure : ce type de reconfiguration effective concerne uniquement les ressources engagées en production. Elle consiste à répartir sur les ressources engagées en production et encore opérationnelles, les tâches ou opérations qui auraient dû être exécutées sur les ressources défaillantes. Une telle reconfiguration effective se traduit par la mise à l'arrêt de ressources en panne, et par un nouveau paramétrage de la commande,
- une reconfiguration significative : ce type de reconfiguration effective concerne les ressources engagées et les ressources en attente. Elle est mise en œuvre en cas d'échec d'une tentative de reconfiguration mineure. Elle consiste à faire réaliser par des ressources en attente, la charge de production des ressources défaillantes ne pouvant pas être assurée par des ressources engagées. Elles permettent également de pallier la disparition d'une fonction en sollicitant une ressource en attente,

- une reconfiguration majeure : elle considère toutes les ressources du système de production. L'idée est d'élargir le champ des possibilités en utilisant, si besoin, des ressources dont la maintenance peut être différée. En cas d'échec de cette dernière solution, il faudra que la stratégie retenue envisage de changer la production initialement retenue.

Différentes stratégies sont envisagées suivant l'état des produits, la disponibilité des ressources et les objectifs de production (*figure II-11*).

La connaissance de la disponibilité des ressources (ressources engagées, en attente, à l'arrêt) est indispensable pour le Recouvrement. En effet, l'état des ressources lui permet de déterminer les opérations encore réalisables et par conséquent de définir les nouveaux objectifs à atteindre. C'est à partir des informations fournies par la Gestion des Modes que le Recouvrement détermine la disponibilité des ressources de production.

Lorsque le Recouvrement a déterminé le type de reconfiguration effective à mettre en œuvre, il transmet cet objectif à la Gestion des Modes en lui indiquant l'état dans lequel doit être placée chaque ressource.

Il est à noter que l'approche présentée par P. Berruet ne s'attache qu'à la faisabilité opérationnelle d'une solution. En effet, l'objectif est de mettre en œuvre un ensemble de ressources délivrant des opérations, donc des fonctions, permettant de réaliser les gammes retenues par l'ordonnancement. Si cela n'est pas possible, une nouvelle gamme est considérée (Etape 4, *figure II-11*). La faisabilité apparaît comme une condition nécessaire mais pas suffisante à l'élaboration de la solution retenue. L'évaluation des performances de la solution retenue, non étudiée jusqu'à lors, fait l'objet de nouveaux travaux.

2.1.3 Le pilotage

En phase d'exploitation, le comportement des ressources de production et l'état d'avancement des produits vont conduire à des indéterminismes directionnels et à des conflits d'accès aux ressources. Ces problèmes sont liés à l'allocation simultanée d'une ressource de production à plusieurs gammes opératoires et à la gestion des indéterminismes locaux des ressources de production. Ces indéterminismes et conflits sont arbitrés par le pilotage.

L'approche dynamique [Taw, 95] se base sur un ordonnancement prévisionnel (effectué hors ligne) par la fonction de

Planification/Ordonnancement (Chapitre I, § 3.3) qui fournit les informations d'entrée (dates de début et de fin des opérations, délais, charges des machines). Lors d'une défaillance, ces données sont transmises par le Recouvrement. Les différentes étapes de transformation et de transfert des pièces sont suivies en temps réel, et l'objectif est de réagir le plus tôt possible pour maîtriser une perturbation.

La fonction de pilotage joue un rôle de régulateur de production par correction des dérives constatées en référence aux prévisions. Pour tenir les objectifs de production, le pilotage intervient sur le lancement des opérations. Il intervient également sur le lancement de produit, le routage de produit. Les décisions considérées correspondent à l'affectation réelle des produits aux machines. Un produit peut voir son affectation initiale modifiée si, le contexte de production est défavorable à l'affectation prévisionnelle. Lorsque des modifications ou des comportements inattendus surviennent, différentes actions correctives sont mises en œuvre (permutations d'opérations, consommation de marge d'opération, ...). Toutes ces actions nécessitent la connaissance de la disponibilité de chacune des ressources de production qui est fournie par la Gestion des Modes.

2.2 La Gestion des Modes

2.2.1 Gestion des Modes et contrôle-commande

La Gestion des Modes apparaît comme une fonction centrale dans la structuration du contrôle-commande (*figure II-10*). Le récapitulatif de ces interactions avec les autres fonctions du contrôle-commande nous le montre.

Relations avec la Commande :

A partir des différentes informations qui lui sont délivrées (ressources à prendre en compte, ...), la Gestion des Modes permet d'activer les graphes de commande nécessaires pour la production demandée.

Relations avec la Surveillance :

Elle permet à la Gestion des Modes la mise à jour de ses informations. En effet, dès qu'une défaillance est détectée, la Gestion des Modes en est informée. De plus, afin de ne pas surveiller inutilement certaines ressources, non engagées dans la production courante, la Gestion des Modes renseigne la

Surveillance sur celles à prendre en compte. Effectivement, seule les ressources dans un état donné (ressources engagées ou en attente) sont à surveiller. Cette information est d'autant plus importante qu'elle permet au Diagnostic de réduire son espace de recherche lors d'une défaillance.

Relations avec le Pilotage :

De manière similaire à la plupart des autres fonctions du contrôle-commande, le pilotage a besoin de connaître les ressources mises à sa disposition pour jouer son rôle de régulateur.

Relations avec le Recouvrement :

Nous avons vu précédemment que la connaissance de l'état des ressources lui permettait de définir de nouveaux objectifs à atteindre. La Gestion de Modes met en œuvre les décisions prises par cette fonction.

Relations avec la Maintenance :

La Gestion des Modes lui permet de connaître l'état des ressources de production. Cette connaissance lui est indispensable pour déclencher les actions de maintenance préventive et corrective. Pour pouvoir intervenir, la Maintenance a besoin que les ressources soient dans un état précis. La Gestion des Modes est là pour garantir qu'une ressource est bien dans l'état souhaité.

Contrairement aux fonctions précédentes, les échanges entre les fonctions de Planification/Ordonnancement et Pilotage sont unidirectionnels.

Relations avec la Planification / Ordonnancement :

Cette fonction fournit, à la Gestion des Modes, la liste et l'état des ressources qui participent initialement à la production. Ces informations sont à rapprocher de celles fournies par le Recouvrement suite à une défaillance.

Relations avec les opérateurs :

Enfin, le dernier acteur en relation avec la Gestion des Modes est l'opérateur qu'il soit un opérateur de conduite ou de maintenance. Tous les opérateurs ont besoin de connaître, à chaque instant, l'état du Système de Production et de pouvoir intervenir en le modifiant.

2.2.2 Le modèle OID

Selon l'approche systémique, tout système complexe peut se décomposer selon trois sous-systèmes [Lem, 91] : le système d'information, le système opérant et le système de décision. Ce modèle canonique (*figure II-12*) est universel et permet la modélisation de tout système complexe.

Le système opérant est constitué par l'ensemble des ressources physiques et des équipements.

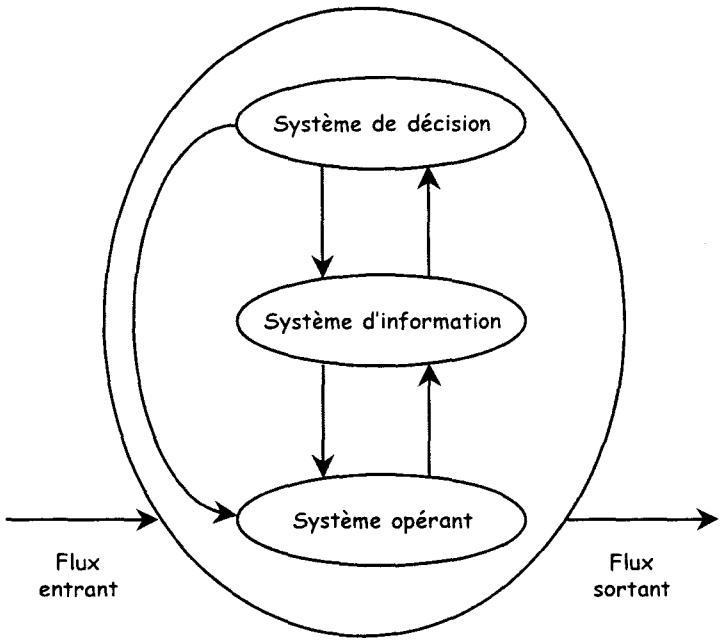


figure II-12. Modèle OID [Lem, 91]

Le système d'information enregistre les représentations des opérations du système opérant (le comportement du système complexe), les mémorise et les met à disposition du système de décision. Après avoir élaboré ses décisions d'action (les commandes), le système de décision les fait également enregistrer et mémoriser par le système d'information en les transmettant "pour action" au système opérant. Les informations proviennent soit de l'environnement du système, soit du système lui-même.

Deux critères essentiels permettent de juger le bon fonctionnement d'un système d'information [Taw, 95] :

- critère de disponibilité qui traduit l'adaptation de la fréquence des informations à la fréquence des décisions.

- critère de pertinence qui traduit la faculté de posséder une information suffisante et sans distorsion.

Les décisions prises par le système de décision sont fonction des informations fournies par le système d'information.

2.2.3 Gestion des Modes et modèle OID

Si l'on considère que la Supervision est un système complexe, la Gestion des Modes peut être alors assimilée à la fois à un système informationnel et opérationnel. Les trois sous-systèmes du modèle OID peuvent être vus comme :

- l'ensemble des fonctions de Pilotage et de Gestion des Modes représente le système opérant. Elles doivent appliquer les décisions prises par la fonction de Recouvrement (système de décision),
- la fonction de Gestion des Modes joue également le rôle de système d'information en indiquant l'état du système,
- la fonction de Recouvrement, qui apparaît comme un système de décision qui a en charge de prendre des décisions lors de l'occurrence d'une défaillance.

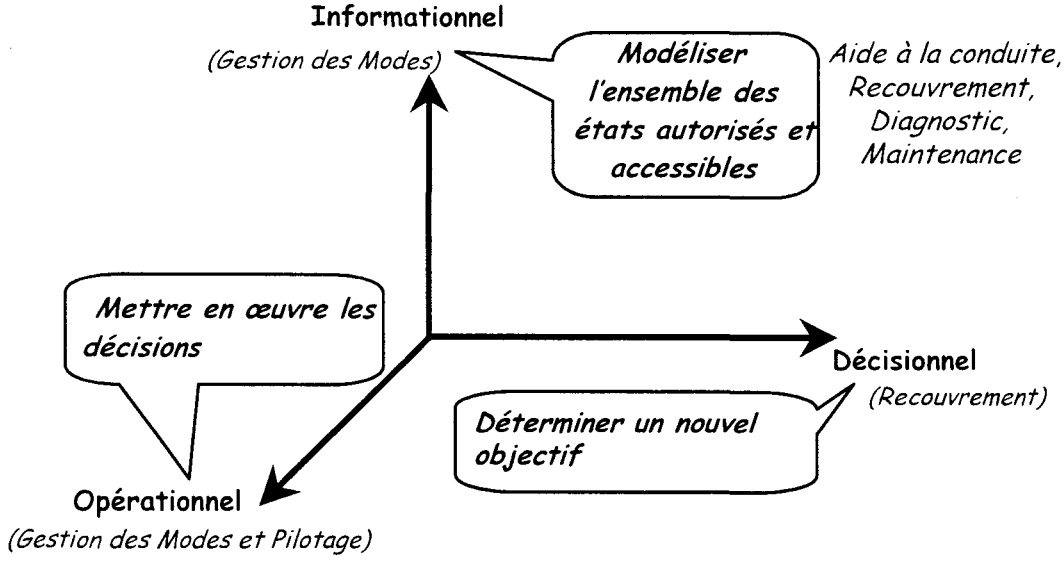


figure II-13. Projection de la Supervision sur les axes OID

Dans ce contexte la Gestion des Modes apparaît comme une fonction bidimensionnelle (*figure II-13*).

Cependant pour atteindre les objectifs fixés par les fonctions du contrôle-commande et les opérateurs, la Gestion des Modes doit tout d'abord déterminer la séquence d'action pour y parvenir. Cette situation peut être rapprochée du problème du voyageur de commerce, qui pour se déplacer d'une ville A à une ville B, étudie tous les itinéraires possibles. Le choix du chemin dépend alors d'un certain nombre de critères (le temps, le coût, ...).

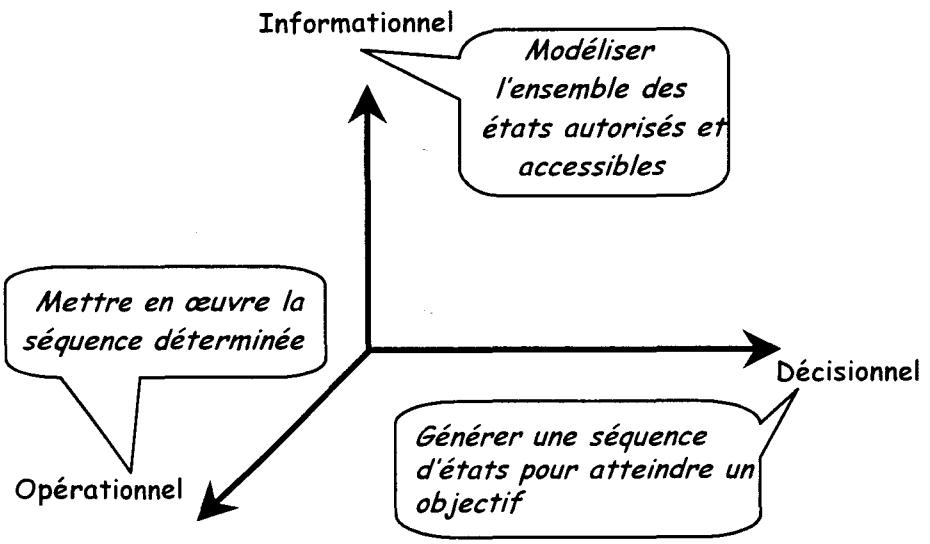


figure II-14. Projection de la Gestion des Modes sur les axes OID.

Nous pouvons alors considérer que la Gestion des Modes est elle-même un système complexe décomposable (*figure II-14*). Son sous-système décisionnel détermine la séquence d'actions (les commandes) qui va permettre de commuter de l'état courant vers un état objectif fourni par un système extérieur à la Gestion des Modes. La séquence d'actions déterminée est transmise au système d'information qui, à son tour, la communique au système opérant. Nous retrouvons bien ici les liens et fonctions des sous-systèmes décrits dans le modèle canonique OID.

2.3 Problématique

Les objectifs de la Gestion des Modes peuvent se résumer comme suit :

- modéliser, à tout instant, l'état du système et particulièrement celui des ressources,

- gérer les changements d'état du système non prévus par la partie commande. Ces changements d'état peuvent être issus soit d'une des fonctions du contrôle-commande, soit la conséquence d'une défaillance du procédé.

La difficulté d'une telle fonction provient d'une part du nombre d'intervenants avec qui elle est en rapport et d'autre part, de la complexité des Systèmes de Production qu'elle doit gérer.

2.3.1 Le nombre d'intervenants

Nous avons vu tout au long de ce chapitre que la Gestion des Modes est une source d'information pour l'ensemble des fonctions du contrôle-commande. Chacune de ces fonctions doit pouvoir y trouver les informations nécessaires pour son bon fonctionnement. Toutes ces informations concernent l'état des ressources du Système de Production. Une première approche consisterait à dire qu'il suffit de dresser la liste des informations nécessaires et de les modéliser. La difficulté réside dans l'interprétation des informations recueillies. En effet, un opérateur de conduite peut considérer qu'une ressource est à l'arrêt alors qu'un opérateur de maintenance, qui intervient sur cette même ressource, considère qu'elle est en marche manuelle pour exécuter un test. Ceci s'explique par le fait que pour le premier opérateur, cette ressource n'est pas retenue pour sa production ; par conséquent de son point de vue, elle est à l'arrêt. La perception de l'état d'une machine est alors dépendant du point de vue adopté. Il est donc nécessaire de prendre en compte et de gérer tous les points de vue spécifiés pour atteindre les objectifs de production.

Les ressources, qui constituent un Système de Production, sont en constante interaction afin de délivrer le service pour lequel le système a été conçu. Par conséquent, le changement du comportement de l'une des ressources a forcement une influence sur l'ensemble du système. Afin de toujours répondre au mieux aux objectifs de production, il est donc nécessaire que chaque intervenant connaisse l'état de chaque ressource et également l'état de l'ensemble (ou d'une partie) du Système de Production. Une vision de l'état du Système de Production, par niveau, est donc nécessaire.

2.3.2 La complexité des Systèmes de Production

Les Systèmes de Production s'avèrent très complexes du fait de l'hétérogénéité de leurs équipements, des flexibilités qu'ils offrent et de la

multitude de paramètres à contrôler. Les problèmes directement liés à l'exploitation d'un Système de Production proviennent principalement de cette complexité et du besoin de gérer différents fonctionnements selon les objectifs fixés. Ils se traduisent plus particulièrement par des incompatibilités d'états des divers équipements constituant le système et par des situations de blocage. La cohabitation de ces divers équipements conduit également à des problèmes de sécurité.

La Gestion des Modes doit alors prendre en compte un certain nombre de contraintes afin d'éviter ces problèmes.

2.3.3 Cahier des Charges

Après avoir exposé les objectifs et la problématique de la Gestion des Modes, nous pouvons dresser une liste des fonctionnalités qu'elle doit assurer.

La fonction de Gestion des Modes doit permettre de :

- Modéliser l'ensemble des états autorisés et accessibles (Modes),
  - ✧ en tenant compte du contexte de production (ce que l'on veut faire),
  - ✧ selon différents points de vue et à plusieurs niveaux,
  - ✧ en exploitant les flexibilités du système,
- Gérer le basculement d'un mode vers un autre,
  - ✧ en déterminant une séquence d'actions,
  - ✧ en vérifiant la cohérence des états et la sécurité des ressources humaines et matérielles,
  - ✧ en mettant en œuvre cette séquence.

Notre travail concerne la modélisation et de la mise en œuvre de la fonction de Gestion des Modes. Nous allons, dans la suite de ce mémoire, proposer une méthode qui permette de respecter au mieux tous ces objectifs.

CONCLUSION

A travers ce chapitre, nous avons pu mettre en avant la problématique traitée dans ce mémoire et apporter notre contribution en ce qui concerne la terminologie.

La première partie présente le processus de reconfiguration d'une façon générale et indépendamment de tout formalisme et méthode. Cette définition générale permet ainsi aux auteurs de positionner leurs travaux par rapport à ceux de la communauté déjà positionnés dans ce chapitre.

L'étude du processus de reconfiguration nous a également permis d'introduire l'objet de nos travaux : la Gestion des Modes. La deuxième partie de ce chapitre s'attache à définir le rôle de la Gestion des Modes et son intégration au sein de la supervision. Ceci nous a conduit à élaborer un cahier des charges fonctionnel de la Gestion des Modes.

Les chapitres suivants présentent les différents modèles et démarches définis en vue de la Gestion des Modes des Systèmes de Production.

Proposition pour la Modélisation et la Gestion des Modes des SP.

Cette deuxième partie du mémoire, constituée de trois chapitres, est consacrée à la présentation de notre proposition pour la modélisation et la gestion des modes des Systèmes de Production.

Dans un premier temps, afin d'avoir une vision globale de notre approche, nous la présentons de façon générale. Notre approche concernant la modélisation du comportement des Systèmes de Production d'un point de vue de leurs modes, nous proposons une démarche pour leur détermination.

Le chapitre suivant s'intéresse plus particulièrement à l'un des éléments de notre approche : le Modèle de Composant. Son objectif est de modéliser le comportement de chacun des composants d'un Système de Production tout en respectant les contraintes spécifiées par le concepteur.

Enfin, le Modèle de Fonction, dont l'objectif est de modéliser le comportement "interne" d'une fonction, est présenté dans le dernier chapitre. Le principe de construction du modèle complet et une application constituent également ce dernier chapitre.

Chapitre III

MODÉLISATION DES SYSTÈMES DE PRODUCTION

INTRODUCTION

Après avoir présenté le contexte et la problématique de notre travail, l'objectif de ce chapitre est de proposer une vision globale et générale de notre approche. Cette première présentation permet ainsi d'introduire les différents éléments qui la constituent. Chacun d'entre eux sera présenté dans les chapitres suivants.

La première partie de ce chapitre est consacrée, dans un premier temps à la présentation des différents objectifs de notre travail. Nous introduisons également les outils et formalismes retenus dans notre approche. Par la suite, nous présentons notre approche de façon générale afin de donner une vue d'ensemble aux lecteurs.

Une fois la présentation générale effectuée, nous abordons, dans la deuxième partie de ce chapitre, ce qui est la "base" de nos travaux : les modes des Systèmes de Production. Après quelques exemples issus de la littérature, nous proposons une démarche pour la détermination des modes d'un Système de Production. Les familles de modes définies et leurs états sont exploités dans les chapitres suivants.

1 PRÉSENTATION GÉNÉRALE

1.1 Objectifs et Proposition

1.1.1 Objectifs

Dans notre contexte d'étude, les objectifs de la fonction de Gestion des Modes (Chapitre II, §. 2.3.3) sont de décrire et de gérer le comportement d'un Système de Production selon différents points de vue et selon le contexte. Ceci passe d'une part par la modélisation, à tout instant, de l'état du système. La notion de mode, qui représente un regroupement d'états, intervient ici pour permettre la description ces systèmes. D'autre part, cela consiste à gérer les changements d'états du système en tenant compte des contraintes spécifiées. Le résultat attendu peut alors être assimilé à un modèle comportemental du système étudié.

Nous avons vu qu'un certain nombre de travaux s'y est intéressé. Certaines approches sont très spécifiques ([Ker, 96] : SFPM). En outre, la fonction de Gestion des Modes telle qu'elle est définie dans notre approche de contrôle-commande englobe plusieurs objectifs qui sont souvent traités, dans la littérature, de façons indépendantes ([Bil, 94] : modélisation, [Mab, 96] : aide au recouvrement,...).

L'un de nos objectifs est, bien évidemment, de proposer une méthode de modélisation qui permet de représenter le comportement d'un Système de Production tout en répondant aux exigences de la fonction de Gestion des Modes (Chapitre II, §. 2.3.3). En outre, notre but est de proposer une méthode générique utilisable pour tous les systèmes de notre domaine d'application (Chapitre I, §. 1.5).

Nous entendons par méthode la combinaison d'outils de modélisation, de règles et de démarche de construction. Les outils de modélisation correspondent aux différents modèles utilisés dans la méthode, ils sont perçus comme un moyen de représentation. L'ensemble de ces modèles constitue le modèle final. Les règles doivent, selon la démarche proposée, permettre d'atteindre l'objectif fixé. En l'occurrence, ici, elles doivent permettre de représenter la dynamique du système modélisé. En outre, elles doivent pour cela être suffisamment détaillées et explicites de telle façon qu'elles soient exploitables par tous : l'objectif étant de guider le concepteur dans la conception d'un modèle comportemental d'un Système de Production en vu de la gestion de ses modes.

La méthode proposée est alors adaptable selon le système étudié et en tenant compte des spécifications fournies par le concepteur. La diversité des systèmes existants impose cette adaptabilité.

1.1.2 Proposition

D'une manière générale, caractériser l'état d'un système permet de vérifier que son comportement est identique à celui prévu. Si c'est le cas, le système peut être considéré comme fonctionnant correctement ; en revanche si le résultat obtenu est différent de celui attendu, le fonctionnement est alors considéré comme incorrect. Cette vision trop restrictive de l'état d'un système ne peut pas être suffisante pour un Système de Production. Rappelons que l'une des particularités de ces systèmes est leur complexité notamment due à l'hétérogénéité de leurs équipements, aux flexibilités qu'ils offrent et à la multitude de paramètres à contrôler. Le fonctionnement correct ou incorrect d'un Système de Production dépend alors de chacun de ses composants et du contexte de production dans lequel ils se trouvent.

De nombreux travaux reposent sur la composition de l'état de chacun des composants d'un Système de Production pour en déterminer le modèle comportemental global du système étudié [Boi, 91], [Bil, 94], [Ker, 96],[Mab, 96]. Ils utilisent les relations entre composants, que cela soit des relations structurelles ou fonctionnelles, la composition d'automates ou des contraintes pour effectuer les regroupements successifs. La structure hiérarchique obtenue représente ainsi le comportement du système et permet de réduire la complexité du système en définissant différents sous-systèmes de plus en plus généraux jusqu'au niveau du système global. Dans ce type

d'approche, le modèle comportemental d'un Système de Production est obtenu en combinant les moyens (les composants) et en suivant une approche ascendante.

A contrario, notre proposition est basée sur une approche descendante et orientée objectifs de production.

L'idée directrice de notre méthode est que tout système doit garantir les objectifs pour lesquels il a été conçu. La caractérisation de son état dépend donc de l'atteinte ou non de ces objectifs. Partant de cette hypothèse, nous proposons de définir et de caractériser le système d'un point de vue fonctionnel. L'aspect fonctionnel se rapporte ici aux fonctions que doit délivrer le système. Une fonction est définie comme *"la réponse d'un système ou d'un composant à un stimulus donné quand il fonctionne normalement, indépendamment de l'environnement dans lequel il est sollicité"* [Tog, 96].

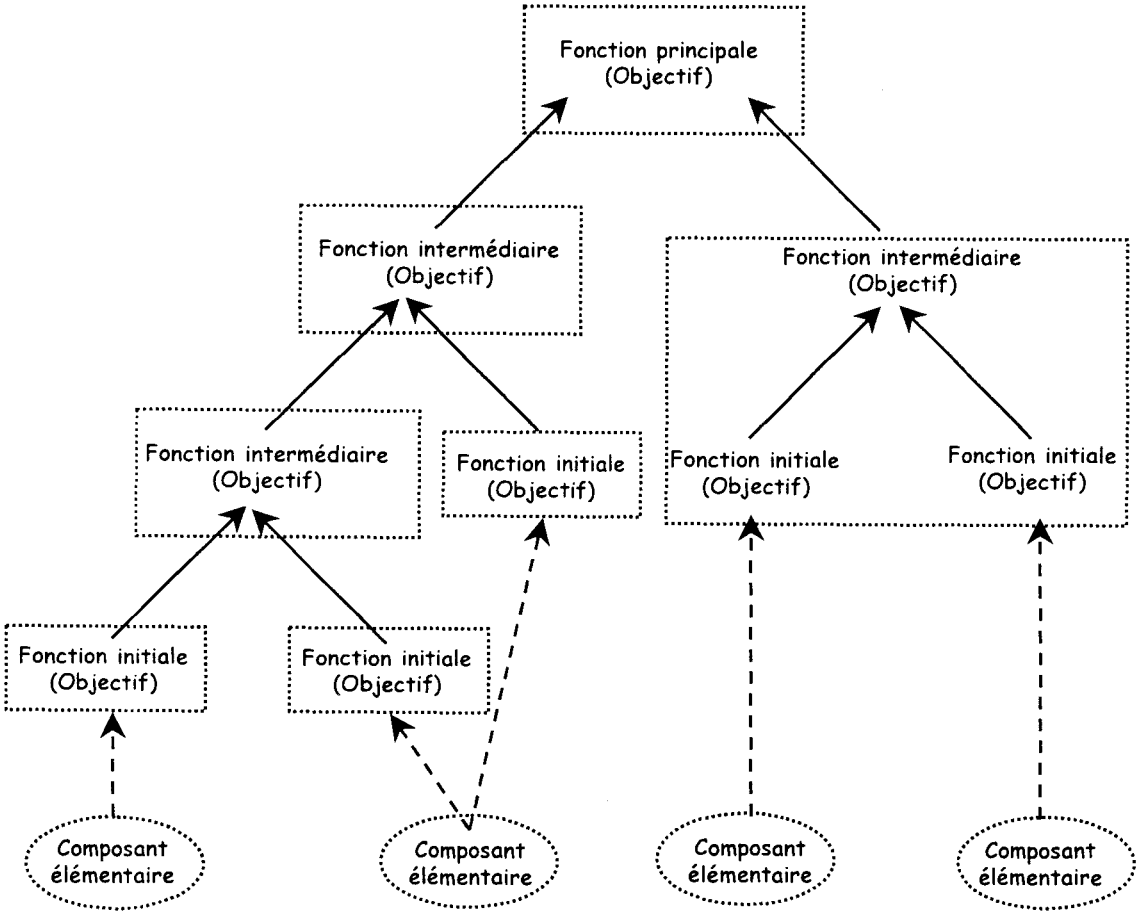


figure III-1. Proposition pour la Gestion des Modes d'un Système de Production.

Nous appelons les objectifs, pour lesquels le système a été conçu, **les objectifs principaux** ; ils correspondent aux fonctions principales que doit délivrer le système. La caractérisation de ces seuls objectifs n'est pas suffisante pour déterminer avec pertinence l'état du système du fait de sa complexité ; c'est pourquoi il est nécessaire de caractériser également les **sous-objectifs**. Ces derniers, lorsqu'ils sont atteints et combinés entre eux, permettent d'atteindre les objectifs principaux. Chacun des sous-objectifs peut être à son tour décomposé (*figure III-1*). Les sous-objectifs de plus bas niveaux sont appelés les **objectifs initiaux**. Ils correspondent à des objectifs élémentaires, c'est-à-dire dont la décomposition n'apporte aucune information pertinente pour le modèle final. Nous considérons que de tels objectifs correspondent, en général, à des fonctions délivrées par des composants élémentaires. La notion d'élémentaires dépend du système. Dans le cas d'un atelier flexible de production manufacturière, chaque ressource de transformation est considérée comme un composant élémentaire. Dans un contexte continu, une pompe peut être assimilée à un composant élémentaire.

La caractérisation de chaque objectif intermédiaire a donc une influence sur les objectifs intermédiaires de niveaux supérieur et inférieur. L'état de chacun des objectifs initiaux (de plus bas niveau) dépend notamment des composants qui sont nécessaires pour les atteindre. Il est donc indispensable de déterminer l'état de chaque composant afin de déterminer l'état des objectifs initiaux.

Notre proposition peut alors être résumée comme suit : elle consiste à caractériser l'état du système à partir de l'état des composants de base (flux d'information provenant du niveau bas), des ordres des intervenants sur le système (Opérateur de conduite, Recouvrement, Maintenance : flux d'information provenant du niveau haut) et selon un point de vue *objectif de production*.

1.2 Outil et formalisme retenus

1.2.1 Outil

La démarche proposée, pour élaborer le modèle comportemental d'un Système de Production, est fondée sur une décomposition hiérarchique. Nous avons vu qu'il s'agissait d'une décomposition d'objectifs en sous-objectifs. Un des objectifs principaux d'un Système de Production peut être, par exemple, de produire des pièces d'un type particulier. Il est donc nécessaire, d'une façon

générale, de mettre en œuvre une fonction principale "Produire" qui permet d'atteindre les objectifs de production fixés. En fait, ces objectifs correspondent aux différentes fonctions générales que doit délivrer le Système de Production. Dans de nombreux cas, pour atteindre les objectifs principaux, il est nécessaire de mettre en œuvre plusieurs fonctions. L'élaboration du niveau inférieur d'un objectif principal consiste alors à déterminer les sous-fonctions nécessaires pour réaliser cette fonction principale. Par exemple, pour la fonction "Produire", il peut être nécessaire de mettre en œuvre différentes fonctions telles que des fonctions "Transformer" et "Transporter". L'une de nos étapes de modélisation consiste alors en une décomposition hiérarchique et fonctionnelle.

La recherche d'une démarche explicite pour la conception du modèle comportemental d'un Système de Production nous a conduit à utiliser et à étendre les concepts et les formalismes utilisés pour la conception du Graphe Fonctionnel [Tog, 00]. Le Graphe Fonctionnel a été initialement conçu pour la mise en œuvre de la fonction de Diagnostic (Chapitre I, §.3.4) dans le cadre d'une approche de maintenance curative. Il permet notamment de représenter les relations de causalité entre fonctions.

Les différents concepts utilisés dans son élaboration sont la fonction, l'opération, le Lieu Caractéristique Fondamental et l'Accessibilité Directe Fondamentale. Le concept de fonction a déjà été défini c'est pourquoi nous n'y revenons pas (Chapitre III, §.1.1.2).

Une **opération** est une fonction réalisée sur un produit par une ressource compte tenu de sa situation spatiale au sein du système [Ber, 98].

Un **Lieu Caractéristique Fondamental** (LCF) correspond à une zone de transformation ou un lieu de stockage servant de zone d'entrées ou de sorties de produits du système [Ber, 00].

L'**Accessibilité Directe Fondamentale** (ADF) correspond au transfert direct d'un produit d'un lieu caractéristique vers un autre lieu caractéristique [Ber, 00].

Le Graphe Fonctionnel est obtenu après l'élaboration de différents modèles ; le Modèle Fonctionnel de Conception et le Modèle Fonctionnel d'Implantation Élémentaire. Ces derniers sont présentés dans l'annexe 1.

L'inconvénient d'un tel modèle est son impossibilité à représenter des comportements complexes. En effet, les liens de dépendance utilisés permettent de traduire tout naturellement des situations où deux fonctions sont nécessaires ("ET" logique) ou représentent une alternative ("OU" logique) pour délivrer une fonction de niveau supérieur. Par contre, ils ne permettent pas de prendre en compte le contexte courant, ni de représenter l'état d'un système ou d'un sous-système selon différents points de vue. Tous ces éléments nous ont conduit à exploiter le Graphe Fonctionnel, non comme un modèle mais plutôt comme un outil de modélisation. En effet, nous utiliserons les différentes étapes de son élaboration pour déterminer la structure hiérarchique de notre modèle. Chaque niveau (ou nœud) du modèle représentera ainsi un sous-système. Le comportement de chaque sous-système sera alors modélisé en utilisant un formalisme qui permet de répondre aux exigences de la fonction de Gestion des Modes.

1.2.2 Formalisme

Généralement, les formalismes de modélisation peuvent être classés en deux catégories selon la période où ils sont utilisés dans le cycle de vie : les formalismes de conception et les formalismes d'implémentation [Dan, 00/c]. Les formalismes de conception sont généralement caractérisés par leur capacité à permettre la validation des modèles. Dans cette catégorie, nous trouvons différents formalismes tels que ceux basés sur les automates à états finis, les réseaux de Petri, ... Le principal critère pour caractériser les formalismes d'implémentation est leur capacité à être directement utilisés sans aucune traduction dans un autre langage. Dans cette catégorie, nous trouvons tous les langages de programmation structurée (C, Ada,...) et le Grafcet.

Force est donc de constater que, pour une même approche, selon la phase du cycle de vie (conception ou implémentation) les formalismes sont souvent différents. En effet, peu de formalismes permettent la validation de modèle en phase de conception et une implémentation directe. Le problème alors est le passage de la conception à l'implémentation tout en gardant les propriétés acquises et vérifiées en phase de conception. En outre, selon les objectifs, il est nécessaire de faire appel à des formalismes bien précis qui possèdent des propriétés particulières : les StateCharts [Har, 87], l'HyperGrafcet [Dum, 99]...

Toutes ces contraintes ne font qu'argumenter le choix des auteurs d'utiliser différents formalismes.

Les Systèmes de Production, que nous prenons en compte dans cette étude (Chapitre I, §.1.5), ont la particularité d'avoir une évolution événementielle (discrète). Ces systèmes sont en interaction permanente avec leur environnement et sont composés de sous-systèmes parallèles interagissant. Le comportement global observé résulte de la coopération des sous-systèmes. La communication est alors essentielle pour assurer cette coopération. De tels systèmes peuvent être alors considérés comme des systèmes réactifs. De plus, la Gestion des Modes doit être capable de préempter des actions du système, c'est-à-dire d'interrompre un traitement avant sa fin principalement en cas d'évolution dangereuse.

Compte tenu de ces précisions et de notre démarche, nos besoins, en terme de formalisme, peuvent alors se résumer aux propriétés suivantes : la hiérarchie, le parallélisme, un fort moyen de communication, la préemption et la réactivité. En outre, la validation du comportement spécifié doit pouvoir être effectuée.

Tous ces éléments, nous ont conduit à retenir une approche synchrone [Ber, 87/a] pour la gestion des modes des Systèmes de Production. Plus particulièrement, nous avons retenu le langage synchrone Esterel et le formalisme graphique des SyncCharts.

Les langages synchrones, en particulier Esterel, permettent de prendre en compte les contraintes liées aux systèmes réactifs : le parallélisme, la communication et la préemption. Ce qui permet d'exprimer le comportement réactif de systèmes complexes. En outre, Esterel est basé sur une sémantique mathématique rigoureuse qui permet de prouver certains comportements. Enfin, le "passage à l'échelle" est possible grâce aux récents compilateurs Esterel qui font appel à des techniques performantes telles que les Binary Decision Diagrams qui supportent des systèmes de grande taille [And, 96].

Un des inconvénients d'Esterel est sa structure de programme qui s'adresse plutôt à des spécialistes en programmation.

Le formalisme des SyncCharts intègre les concepts de haut niveau des langages synchrones dans un formalisme graphique. Ceci permet une

spécification du modèle plus aisée et une traduction systématique et rigoureuse des SyncCharts en Programme Esterel [And, 96].

1.3 Proposition pour la Gestion des Modes

Nous avons déjà introduit, dans le paragraphe 1.1.2, notre proposition pour la modélisation et la Gestion des Modes d'un Système de Production. Notre objectif est ici de présenter de manière informelle les différentes étapes de notre démarche. Celle ci se décompose en deux étapes. La première consiste à déterminer la structure hiérarchique du modèle. La seconde, quant à elle, consiste à définir les sous-systèmes et à déterminer leur comportement.

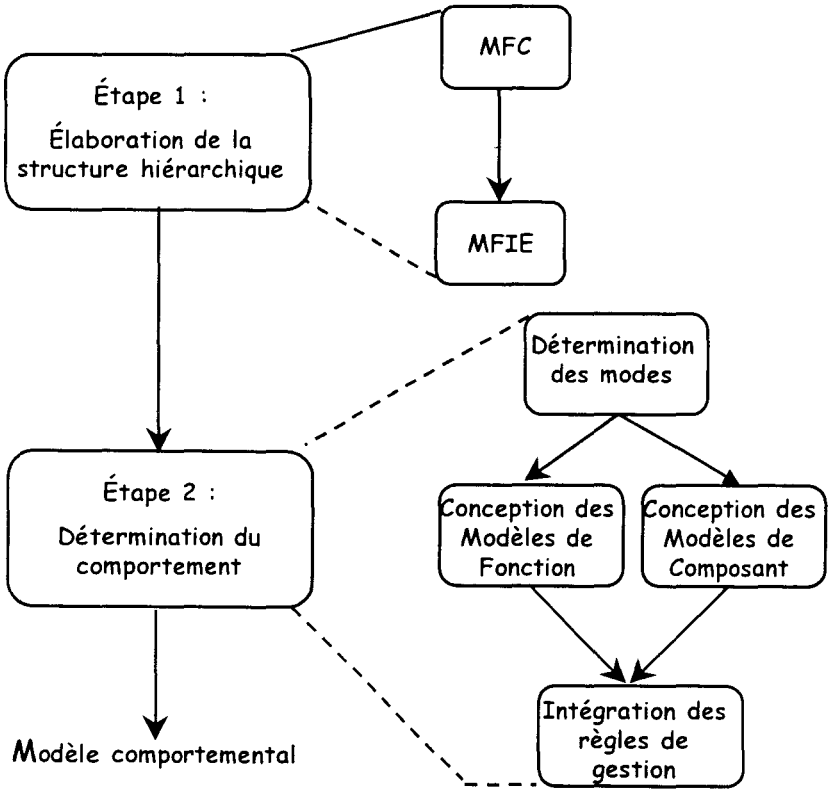


figure III-2. Démarche de construction du modèle comportemental

1.3.1 Première étape : la structure hiérarchique

La première étape (*figure III-2*) est fondée sur la décomposition hiérarchique du système. Pour cela, nous exploitons le formalisme et les modèles nécessaires à l'élaboration du Graphe Fonctionnel. Les modèles, que nous utilisons, sont le Modèle Fonctionnel de Conception et le Modèle Fonction d'Implantation Élémentaire.

La construction de ces deux modèles permet, d'une part, de déterminer la structure hiérarchique du modèle comportemental du système étudié. D'autre part, elle permet de déterminer les composants élémentaires à modéliser pour atteindre les objectifs fixés. Rappelons que ces composants sont ceux qui délivrent les fonctions initiales (Chapitre III, §.1.1.2) et qu'il est nécessaire de les modéliser afin de déterminer leur comportement et par conséquent le comportement de chacune des fonctions initiales.

1.3.2 Deuxième étape : modélisation du comportement des sous-systèmes

L'élaboration de l'étape précédente nous permet dans la deuxième étape (*figure III-2*) de définir les sous-systèmes fonctionnels qui constituent le système et leur comportement. Un système ou un sous-système fonctionnel est caractérisé par le service qu'il doit délivrer. Pour chaque système ou sous-système, il est nécessaire de lui associer un modèle comportemental afin de pourvoir déterminer constamment son état. Nous l'appelons le Modèle de Fonction (MdF). Un modèle comportemental est également associé à chaque composant élémentaire pour les mêmes raisons. Ce modèle est appelé le Modèle de Composant (MdC).

Le comportement global du système est le résultat de l'interaction de ces différents modèles. Ces interactions se traduisent par des règles de gestion qui sont définies par le concepteur et intégrées après la conception du MdF et du MdC.

2 PROPOSITION POUR LA DÉTERMINATION DES MODES DES SP

2.1 Les Modes et les Familles de Modes

Un des critères de bon fonctionnement d'un système d'information, tel que la Gestion des Modes, est la pertinence qui traduit la faculté de posséder une information suffisante (Chapitre II, §. 2.2.2). La principale difficulté est alors de modéliser le comportement du système, de façon pertinente tout en répondant aux besoins de chacun des intervenants, pour qui, ces informations sont nécessaires.

Le comportement d'un Système de Production est souvent représenté par un graphe états-transitions. Chaque nœud (état) du graphe caractérise le Système de Production à un instant donné. Les transitions modélisent le moyen de passer d'un état à un autre. Pour définir un tel graphe, il est nécessaire dans un premier temps de déterminer tous les états, regroupés sous la notion de mode, dans lequel peut se trouver le Système de Production.

S'il est vrai que la plupart des auteurs utilisent cette notion de mode pour décrire le comportement de leur système, rares sont ceux qui ont défini une méthode pour leur détermination. En effet, les modes retenus, pour la description du comportement d'un Système de Production, sont souvent le résultat de l'expérience du concepteur. Nous pouvons cependant citer deux approches qui, par leurs définitions ou par leur démarche, guide le concepteur dans la détermination des modes.

2.1.1 Le GEMMA

Le Guide d'Étude des Modes de Marches et d'Arrêts (GEMMA) [ADE, 81] propose un vocabulaire précis et un outil graphique permettant de mieux définir les Modes de Marches et d'Arrêts d'un système automatisé.

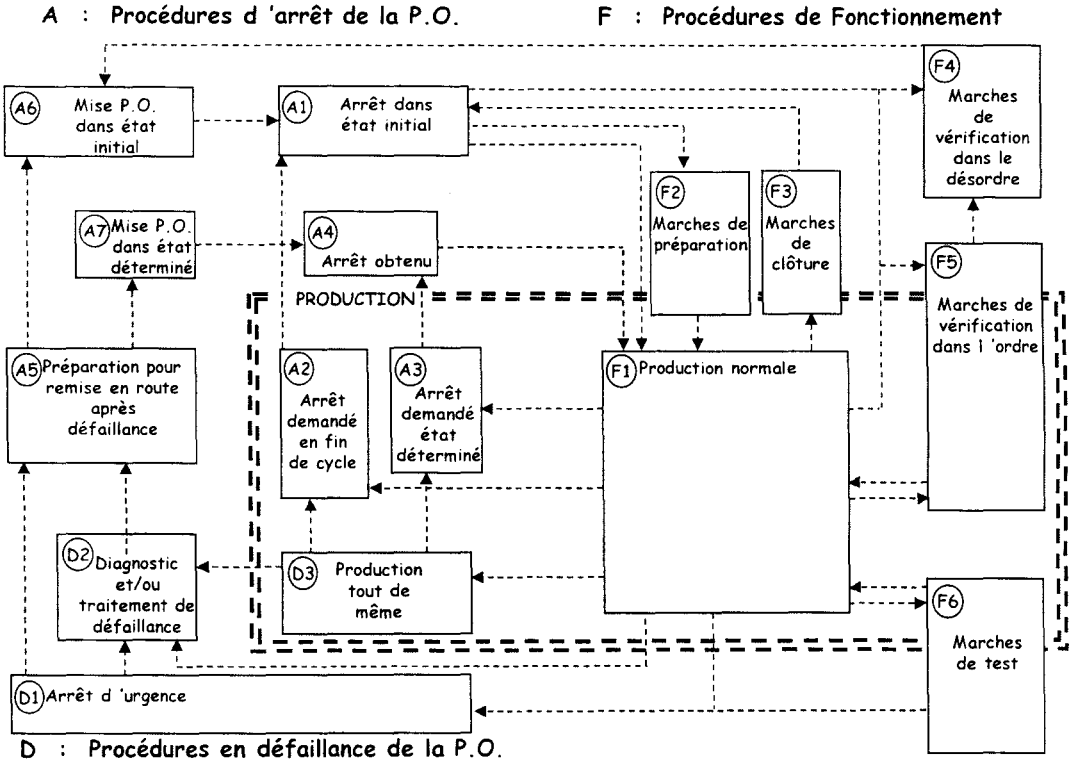


figure III-3. Le GEMMA

Cet "outil-méthode" est présenté sous forme de grille structurée en zones de "rectangles-états" (*figure III-3*). Chaque rectangle représente un état de fonctionnement ou mode de marche ou d'arrêt, unique, du système.

Les principes de base du GEMMA reposent principalement sur : les modes de marche et d'arrêt vus d'une partie commande disponible (en énergie et non défaillante), une organisation des modes en trois familles fonctionnelles et une unicité de mode.

En outre, la position de chacun des "rectangles-états" sur le guide graphique définit son appartenance à une des trois familles et le fait qu'il soit "en" ou "hors" production.

La démarche proposée consiste dans un premier temps à recenser les modes ou états de fonctionnement du système, à partir des définitions données, et dans un deuxième temps à établir les conditions de passage d'un mode à l'autre.

Ce guide, adapté à la description du comportement d'un système, présente l'avantage d'une présentation graphique et d'une définition formelle des modes de marches et d'arrêts. Cependant, sa propriété d'unicité de mode rend impossible la description de systèmes complexes.

- De plus, il est présenté comme modèle générique et directement utilisable pour lequel la démarche de sa conception n'est pas explicite. Il est donc difficile de reprendre ce modèle pour l'adapter à des systèmes complexes.

2.1.2 LAN, Nantes

L'objectif du **L**aboratoire d'**A**utomatique de **N**antes (**LAN**) est de proposer une modélisation du comportement d'un SAP du point de vue de ses modes de marche. Dans ses travaux, P. Biland [Bil, 94] met en avant le fait que la modélisation du comportement, d'un même SAP, est différente selon la fonction étudiée (commande, maintenance, ...). L'auteur propose une approche ascendante de modélisation des modes de marches, quelle que soit la fonction étudiée, qui repose sur deux types de SAP : les SAP élémentaires et les SAP composés.

- "Un SAP élémentaire est un composant du plus bas niveau de la hiérarchie d'un SAP. Il est constitué par un matériel et son logiciel de base associé. L'ensemble des SAP élémentaires constitue le niveau composant",

- "Un SAP composé est constitué par l'association de plusieurs SAP élémentaires et/ou composés".
- La démarche proposée est analogue à celle du GEMMA. Cependant, contrairement au GEMMA, qui établit une liste exhaustive des modes de marche, l'auteur propose d'effectuer une partition de l'ensemble de tous les états que peut prendre un SAP et définit comme mode de marche chacune de ces partitions.

En respectant la structure hiérarchique du SAP, les contraintes de fonctionnement, les interactions technologiques et en effectuant à chaque niveau de structuration une abstraction des niveaux inférieurs, les modes de marche de chaque niveau sont définis. Bien qu'il existe une méthodologie pour déterminer les modes d'un Système de Production, là encore l'expérience du concepteur est requise pour effectuer les partitions. En outre, la détermination des modes doit être réalisée pour chaque système étudié.

2.2 Approche par points de vue

L'approche proposée par le GEMMA présente l'avantage d'une description formelle des modes retenus. Cependant, son unicité de mode rend impossible la description de systèmes complexes. L'approche proposée par le LAN présente l'avantage de l'utilisation d'une méthodologie pour la détermination des modes d'un Système de Production. Toutefois, cette détermination des différents modes est à faire pour chaque équipement utilisé dans le système. Ceci est nécessaire puisque la méthode proposée repose sur la structure du Système de Production.

Notre objectif est de trouver un compromis entre ces deux approches en proposant :

- Une démarche qui permet de déterminer les modes d'un Système de Production et qui soit valable pour une grande majorité de systèmes,
- Une structuration des modes de telle façon que les systèmes complexes soient représentables,
- Une démarche qui prend en compte les besoins de la Gestion des Modes (gestion des différents points de vue, Chapitre II, §. 2.3.3).

2.2.1 Terminologie

Les termes état, mode et famille de modes sont couramment utilisés dans la littérature pour décrire le comportement des Systèmes de Production. Cependant, peu d'auteurs donnent une définition précise des termes employés. De manière similaire au processus de reconfiguration, ceci conduit à une certaine ambiguïté. Pour éviter ce genre de problèmes, nous rappelons ou introduisons ci-après quelques définitions.

Définition 5 *: Etat (state)*

Situation d'une ressource ou d'un élément à un instant donné [IEC61].

Définition 6 *: Mode (mode)*

Ensemble d'états caractérisant une ressource ou un ensemble de ressources selon un point de vue [Dan, 99/b]. A un instant donné, dans un mode, un seul état est actif [Tog, 96].

L'expression *point de vue* correspond ici à la vision que l'on peut avoir sur un objet selon des caractéristiques liées à ce point de vue.

Illustration : Considérons une ressource de transformation quelconque (un tour, une fraiseuse,...). Du point de vue d'un opérateur de conduite, cette ressource peut être considérée à l'arrêt alors que du point de vue d'un opérateur de maintenance, cette même ressource, au même instant, peut être considérée comme en marche manuelle par exemple. Cette différence de point de vue provient du fait que l'opérateur de conduite considère qu'une ressource est en fonctionnement lorsqu'elle est en phase de production. Le reste du temps il considère qu'elle est à l'arrêt : il ne ferra pas de distinction entre le fait que la ressource est à l'arrêt parce que c'est la fin de la journée ou parce qu'elle est en maintenance. De son point de vue, le résultat est le même : la ressource ne produit plus.

Définition 7 *: Famille de Modes (modes family)*

Ensemble de modes ou de familles de modes représentant les différents états que peut prendre une entité selon un même point de vue. Notons que le terme entité peut désigner une ressource ou un ensemble de ressources [Dan, 99/b]. A un instant donné, plusieurs modes sont simultanément actifs [Tog, 96].

Remarque : Par abus de langage, le terme état est souvent utilisé à la place du terme mode. Dans ce cas, le terme état désigne un ensemble d'états.

Afin de lever toutes ambiguïtés, nous définissons également certains termes en relation avec le cycle de vie (Chapitre I, §. 1.2). Nous nous attachons plus particulièrement à présenter les différences que nous faisons entre les termes production et exploitation.

Durant sa phase d'exploitation, le système doit respecter des objectifs pour lesquels il a été conçu : produire en quantité, en qualité et dans des délais fixés tout en assurant la sécurité des ressources humaines et matérielles. Pour atteindre ces objectifs, la phase d'exploitation est constituée d'un certain nombre d'activités. Le cycle de vie en V d'un Système de Production fait apparaître principalement deux types d'activités durant l'exploitation du système : la production et la maintenance (Chapitre I, §. 1.2). Nous considérons que les activités de reconfiguration sont incluses dans celles de production.

Nous considérons ici les activités de production comme l'ensemble des actions qui permet de donner une valeur ajoutée aux produits. La phase d'exploitation, quant à elle, est vue comme l'ensemble des activités qui contribue à atteindre les objectifs pour lequel le système a été conçu. La production apparaît alors comme un sous-ensemble de l'exploitation.

2.2.2 Démarche proposée

Notre objectif, ici, est de présenter la démarche utilisée pour déterminer les modes retenus pour décrire le comportement d'un Système de Production.

Nous avons montré que la perception de l'état d'un système dépend du point de vue adopté (Chapitre II, §. 2.3.1). La description du comportement d'un Système de Production dépend alors du point de vue choisi. C'est sur cette notion de points de vue que repose notre approche.

L'objectif de cette démarche est de déterminer les modes d'un Système de Production tout en tenant compte des besoins de la Gestion des Modes. En effet, les modes retenus doivent permettre, à chaque intervenant, y compris la fonction de Gestion des Modes, d'obtenir l'information pertinente sur le système dont il a besoin.

La démarche consiste alors à considérer l'ensemble des états que peut prendre le système comme étant l'ensemble des états caractérisant un point de vue. A partir de ce point de vue, l'ensemble est partionné en sous-ensembles caractérisant le point de vue initial.

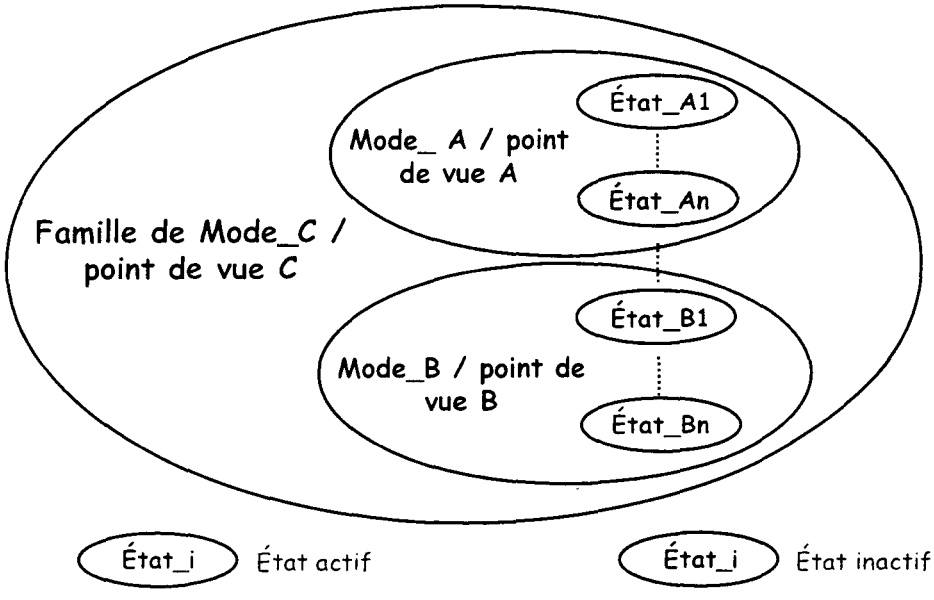


figure III-4. Partition de l'ensemble des états.

Décomposer un point de vue revient alors à se demander : à ce niveau de décomposition, quelles sont les informations (points de vue, modes) dont nous avons besoin pour caractériser le comportement du système ? Les points de vue retenus dépendent des besoins des intervenants et du contexte. La décomposition de chaque nouveau point de vue retenu est poursuivie jusqu'à l'obtention d'un point de vue non décomposable. La détermination des modes selon un point de vue est effectuée en faisant abstraction de tous les autres points de vue [Dan, 99/b]. Une telle décomposition a pour résultat une encapsulation de points de vue (*figure III-4*) qui donne naissance à des modes ou familles de modes.

Un point de vue qui ne peut plus être décomposé en sous points de vue est considéré comme étant un mode. Nous considérons qu'un point de vue qui ne peut pas être décomposé signifie que selon son point de vue, il ne correspond qu'une seule interprétation possible. Ceci correspond à la définition d'un mode dans lequel un seul état est actif à un instant donné. De manière générale, le nom des modes est identique au nom du point de vue correspondant. Une démarche ascendante permet de déterminer les modes et les familles de modes.

La démarche proposée permet de définir les familles de modes et les modes d'un système par rapport à des besoins bien précis. La dernière étape d'une telle démarche consiste alors à déterminer les états qui constituent chacun des modes retenus.

Rappelons que notre objectif est de déterminer un ensemble d'états, de modes et de familles de modes génériques permettant par la suite de décrire le comportement d'un Système de Production. Il semble cependant illusoire de déterminer tous les états correspondants à un mode donné. Là encore, la pertinence de l'information est nécessaire. Néanmoins, il est indispensable de pouvoir modéliser l'état du système, à chaque instant et selon un point de vue donné (donc pour un mode donné).

Afin d'atteindre ces objectifs, nous introduisons dans chacun des modes un état spécifique : **l'état non significatif**.

Définition 8 : *Etat non significatif (non significant state)*

Un état non significatif caractérise l'état du système par rapport à un mode donné quand les autres états de ce même mode ne le permettent pas.

Un mode peut alors être défini comme suit :

Définition 9 : *Mode*

Un mode (M) est défini comme l'union d'un ensemble d'états (E_c) caractérisant une entité selon ce mode et un état non significatif (E_{ns}). A chaque instant, un seul état de ce mode est actif.

Un ensemble Ec générique peut être déterminé à partir du GEMMA. Nous proposons dans le paragraphe suivant un ensemble Ec par mode retenu. Suivant le système, seule une partie de cet ensemble peut être prise en compte ou peut être adaptée à la situation.

2.2.3 Modes et Familles de Modes retenus dans notre étude

Nous allons maintenant appliquer cette démarche dans notre contexte de travail. Nos travaux concernent la supervision des Systèmes de Production. Le comportement à modéliser est celui du Système de Production en phase d'exploitation. Par conséquent, dans un premier temps, le premier point de vue retenu est celui de l'exploitation. Nous savons que cette phase est constituée

d'activités liées à la production et à la maintenance. Nous considérons alors que du point de vue de l'exploitation, le système peut être caractérisé selon deux points de vue : production et maintenance.

Nous nous attachons plus particulièrement à la décomposition du point de vue production. A ce niveau de description, les informations nécessaires à l'ensemble des intervenants peuvent être décomposées en deux catégories. D'une part, il y a les informations dont le système a besoin pour pouvoir évoluer (lancement de la production, type de production, ...). D'autre part, nous avons vu que les différents acteurs du système (les opérateurs et les fonctions du contrôle-commande) ont besoin d'informations sur l'état du système. Le GEMMA et ces différents besoins nous ont conduit à définir quatre points de vue pour caractériser le point de vue production. Les deux premiers, marche et arrêt, caractérisent la manière dont peut être exécutée ou arrêtée la production. Ils correspondent aux besoins du système pour pouvoir évoluer [Dan, 99/b].

Le troisième point de vue caractérise le type de fonctionnement du système par rapport au comportement attendu. Le dernier décrit l'état d'avancement de la production. Ces deux derniers points de vue répondent plus particulièrement aux besoins des acteurs du système.

Ceci nous conduit donc à différents modes. Pour chacun d'entre eux, nous définissons, à partir du GEMMA, les états qui les composent. Dans les abréviations suivantes le premier P indique qu'il s'agit du point de vue production.

- Le mode de marche (PM) : il caractérise l'autonomie du système. Les principaux états sont la marche automatique (PM-a), la marche semi-automatique (PM-s), la marche cycle par cycle (PM-c) et la marche manuelle (PM-m),
- Le mode d'arrêt (PA) : il spécifie toutes les façons dont le système peut être arrêté pour des raisons extérieures au système (par exemple la fin de la journée). Les principaux états sont l'arrêt hors tension(PA-hs), l'arrêt en fin de cycle (PA-c), l'arrêt dans l'état initial (PA-i) et l'arrêt dans un état déterminé (PA-d),

- Le mode de fonctionnement (PF) : il caractérise le type de fonctionnement du système. Les principaux états sont le fonctionnement normal (PF-n), le fonctionnement dégradé (PF-d) et le fonctionnement hors service (PF-hs). Le fonctionnement normal correspond à un fonctionnement du système qui correspond à ce qui est attendu. Le fonctionnement dégradé correspond à un dépassement de seuil fixé par le concepteur. Ces seuils peuvent être de nature fonctionnelle, temporelle ou qualitative. Le fonctionnement hors service correspond à un nouveau dépassement de seuil, fixé par le concepteur, qui ne permet plus au système de répondre à ces objectifs,
- Le mode de production (PP) : il caractérise les différentes étapes par lequel le système doit passer pour atteindre les objectifs (de sécurité, de qualité,...) pour lequel il a été conçu. Les principaux états sont la production préparatoire (PP-p), la production effective (PP-e) et la production de clôture (PP-c).

L'ensemble de ces modes constitue **la famille des modes de production** (FMP) (*production modes family*).

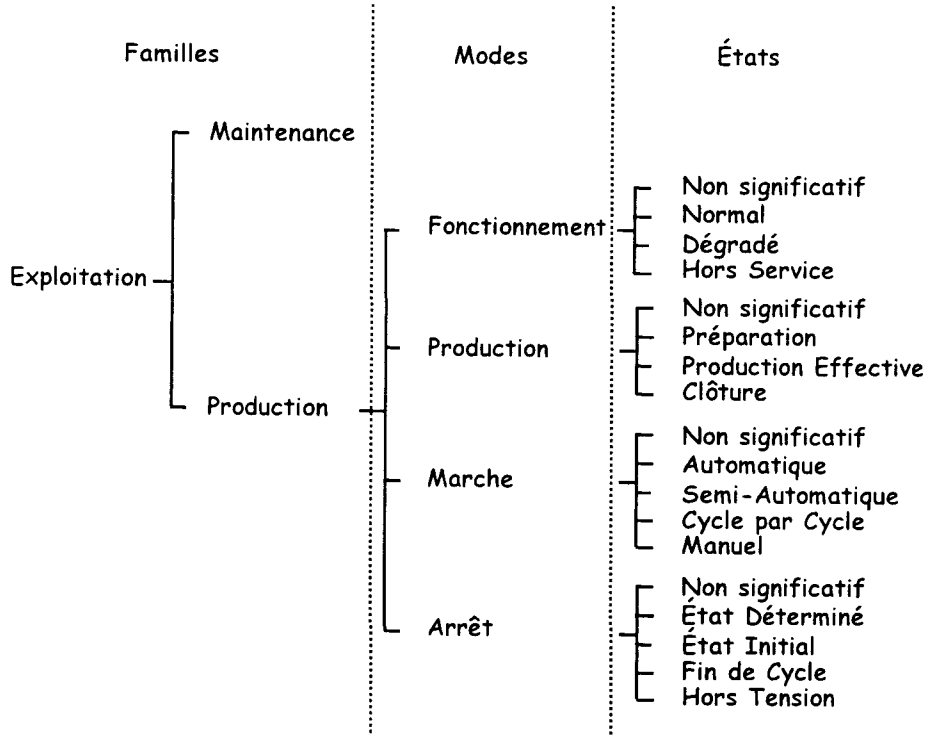


figure III-5. Les familles du mode d'exploitation : famille de production

Une démarche similaire pour le point de vue maintenance conduit à la détermination des modes et états suivants :

- Le mode de marche (MM) : la marche cycle par cycle (MM-c) et la marche manuelle (MM-m),
- Le mode d'arrêt (MA) : l'arrêt hors tension (MA-hs), l'arrêt en fin de cycle (MA-c), l'arrêt dans l'état initial (MA-i) et l'arrêt dans un état déterminé (MA-d),
- Le mode maintenance (MMa) : les différents états retenus sont l'essais (MMa-e), l'intervention (MMa-i) et l'attente (MMa-a).

L'ensemble de ces modes constitue **la famille de modes de maintenance** (FMM) (*maintenance modes family*).

La famille des modes de production et la famille des modes de maintenance constituent les familles du mode d'exploitation.

Rappelons que chaque mode est le résultat de l'union d'un ensemble d'états caractéristiques que nous venons de définir et d'un état non significatif. La figure III-5 présente l'ensemble des états et des modes de la famille de production.

Il est à noter que l'ensemble des états, modes et familles de modes proposé peut être restreint selon les besoins et les caractéristiques du système. Il semble peut probable qu'une marche cycle par cycle soit nécessaire dans le cas d'un processus continu.

De manière similaire au GEMMA, la démarche proposée consiste à recenser les modes ou états de fonctionnement du système en fonction des données fournies par le cahier des charges fonctionnelles (CdCF). Nous traitons un exemple dans le paragraphe suivant.

2.3 Exemple d'application

L'exemple que nous avons choisi de traiter, tout au long de ce mémoire, correspond à un sous-système d'une centrale nucléaire : le Système de Réfrigération Intermédiaire (SRI). Nous sommes en présence d'un Système de Production dont la nature des flux est de type continu et le type d'évolution est de nature discrète. Nous présentons ici une partie du cahier des charges fonctionnels [EDF, 99].

Le SRI a pour rôle d'assurer le refroidissement des auxiliaires de la partie conventionnelle d'une centrale nucléaire. Il est alimenté en eau déminéralisée et il fonctionne en boucle fermée. L'utilisation de réfrigérants à eau brute permet de refroidir l'eau déminéralisée passée par les échangeurs auxiliaires. Les fuites du circuit SRI seront compensées par un système d'appoint. L'eau déminéralisée sera mise en circulation par un système de pompes. Ces quelques points nous permettent de définir un schéma de principe pour le SRI (*figure III-6*).

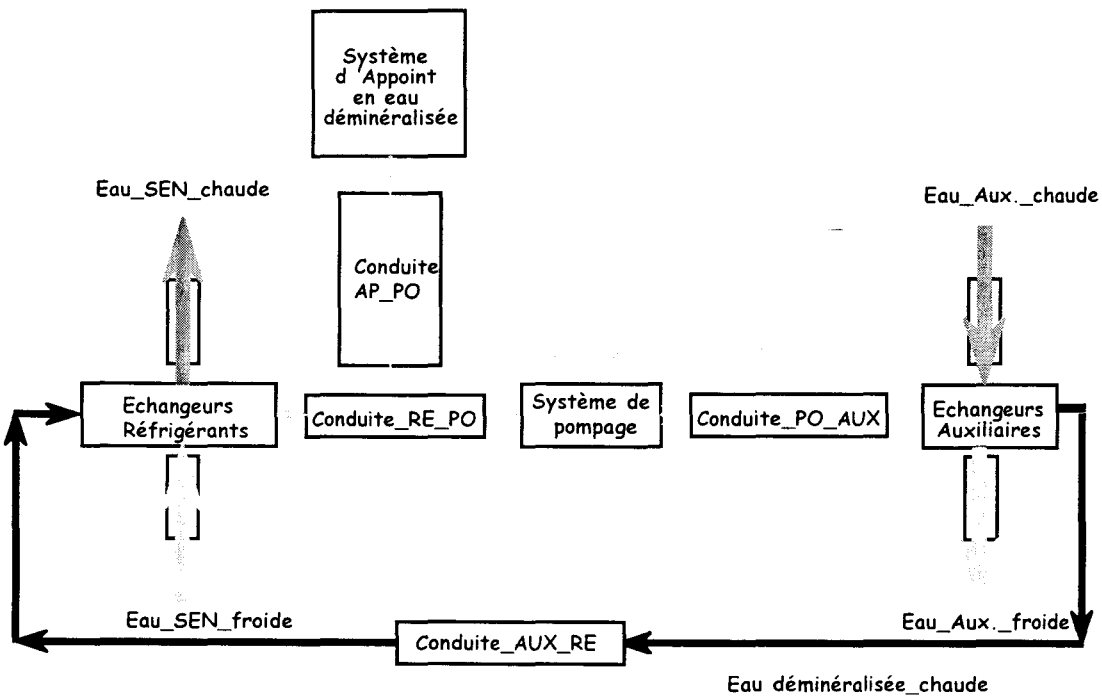


figure III-6. Schéma de principe du circuit SRI d'après les hypothèses du CdCF.

Le circuit SRI est normalement toujours en fonctionnement quelle que soit la situation de la tranche. Toutefois, en cas d'arrêt prolongé de la tranche ou en cas d'entretien du SRI, le système SRI peut être totalement arrêté, voir vidangé. Cela a pour conséquence que la température de l'eau déminéralisée du circuit SED et du circuit SRI peut descendre en hiver au-dessous d'une température fixée (température basse minimale en fonctionnement normal). Dans ce contexte, le démarrage du SRI se fait de manière à rattraper cette température minimale.

Lorsque la tranche est à l'arrêt, la température de consigne doit être maintenue par une circulation minimale pour assurer le refroidissement des auxiliaires restant en service.

Lorsque le niveau de l'eau dans le système d'appoint atteint un niveau MIN3, le système fonctionne alors en boucle ouverte et est considéré comme dégradé.

L'impossibilité pour l'opérateur de mettre en œuvre la configuration choisie pour le fonctionnement du système conduit à un fonctionnement hors service du SRI.

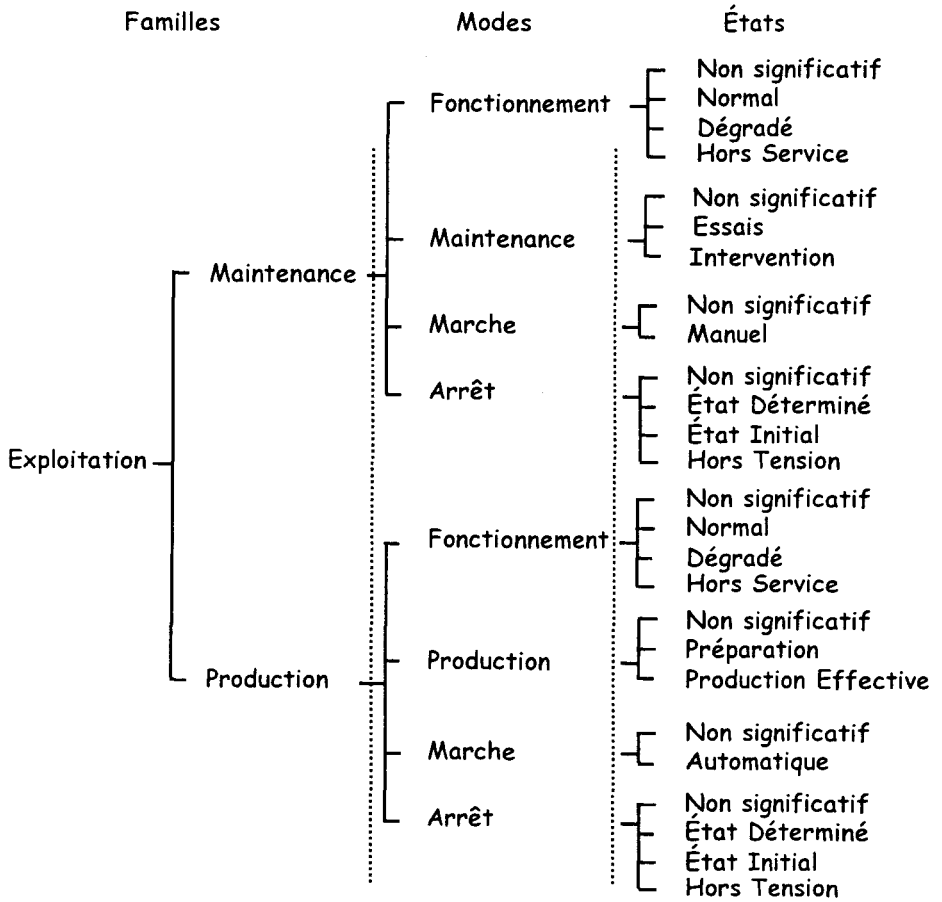


figure III-7. Familles du mode d'exploitation du SRI

A partir de ces indications, nous pouvons recenser les états, modes et familles de modes qui nous intéressent dans cet exemple :

D'un point de vue production :

- Mode de marche : la marche retenue est la marche automatique. En effet, le SRI est continuellement en fonctionnement,

- Mode d'arrêt : les arrêts pris en compte sont les arrêts dans un état déterminé, initial et hors tension. L'arrêt dans un état déterminé signifie que la tranche est arrêtée mais que la température de consigne est maintenue par une circulation minimale. L'arrêt hors tension signifie que la circulation du liquide de refroidissement est arrêtée. Il est possible d'intervenir sur le SRI pour en assurer la vidange et/ou des opérations d'entretien. L'état initial correspond à l'état du SRI dès sa mise sous tension,
- Mode de fonctionnement : les fonctionnements normal, dégradé et hors service sont pris en compte. Le passage du fonctionnement normal au fonctionnement dégradé intervient lorsque le niveau MIN3 est atteint,
- Mode de production : la préparation correspond à la phase où suite à la mise en eau, la température de l'eau déminéralisée est progressivement amenée à la température de consigne. L'état de production effective correspond à la période où la réfrigération des auxiliaires est assurée par la circulation du liquide de refroidissement et à bonne température.

D'un point de vue maintenance :

- Mode de maintenance : les états entretien et essais sont retenus. Ils correspondent respectivement à la vidange du SRI et aux opérations d'entretien des équipements du SRI.

Bien que le CdCF ne fasse pas apparaître des modes de fonctionnement, de marche et d'arrêt dans la famille de maintenance, ils sont nécessaires pour l'opérateur de maintenance pour réaliser les essais et les interventions. Les modes et les états retenus pour le circuit SRI sont représentés par la figure III-7.

CONCLUSION

A travers ce chapitre, nous avons présenté de manière générale notre approche pour la modélisation et la gestion des modes d'un Système de Production.

La première partie nous a permis, dans un premier temps, de préciser nos objectifs et d'introduire les différents outils et formalismes retenus. Dans un deuxième temps, nous avons proposé une présentation générale de notre

approche. En outre, elle met en avant les différentes entités qui constituent le modèle comportemental d'un Système de Production selon notre approche : le Modèle de Composant et le Modèle de Fonction. Le premier permet de modéliser le comportement de chacun des composants d'un Système de Production tout en respectant les contraintes spécifiées par le concepteur. Le second modélise le comportement "interne" d'une fonction.

La dernière partie de ce chapitre est consacrée à la proposition d'une démarche pour la détermination des modes d'un Système de Production. Jusqu'à lors peu de travaux explicitent la manière dont sont définis les modes d'un Système de Production. Notre proposition repose sur la notion de point de vue qui permet de caractériser une ressource selon les critères de l'observateur.

Les chapitres suivants vont présenter de façon détaillée les différents modèles nécessaires à la conception du modèle comportemental d'un Système de Production en vue de la gestion de ses modes ainsi que leurs exploitations.

Chapitre IV

LE MODÈLE DE COMPOSANT

INTRODUCTION

Dans ce chapitre nous nous intéressons au Modèle de Composant. Ce modèle est un élément indispensable dans notre approche pour, d'une part, déterminer l'état de chaque sous-système et du système global. D'autre part, il permet de mettre les composants élémentaires dans l'état fixé par l'un des intervenants du contrôle commande.

Dans un premier, nous indiquons ce que nous entendons par un *composant élémentaire* que représente le Modèle de Composant. Nous introduisons également sa structure basé sur le formalisme des SyncCharts. Enfin, sa démarche de conception est décrite de façon globale afin de donner aux lecteurs une vision globale.

Dans un deuxième temps, nous nous intéressons aux principales étapes de la démarche de conception du Modèle de Conception. Nous insisterons principalement sur l'étude de la cohérence des modes et sur sa mise en œuvre.

Enfin la dernière partie, reprendra complètement la démarche de conception à travers l'exemple du SRI introduit dans le Chapitre III, §.2.3. Ceci nous permettra, notamment de présenter des étapes de la démarche de conception non détaillée précédemment.

1 PRÉSENTATION

Nous nous intéressons ici à la partie basse du modèle comportemental ; c'est à dire au **Modèle de Composant** (**MdC**) (*figure IV-1*).

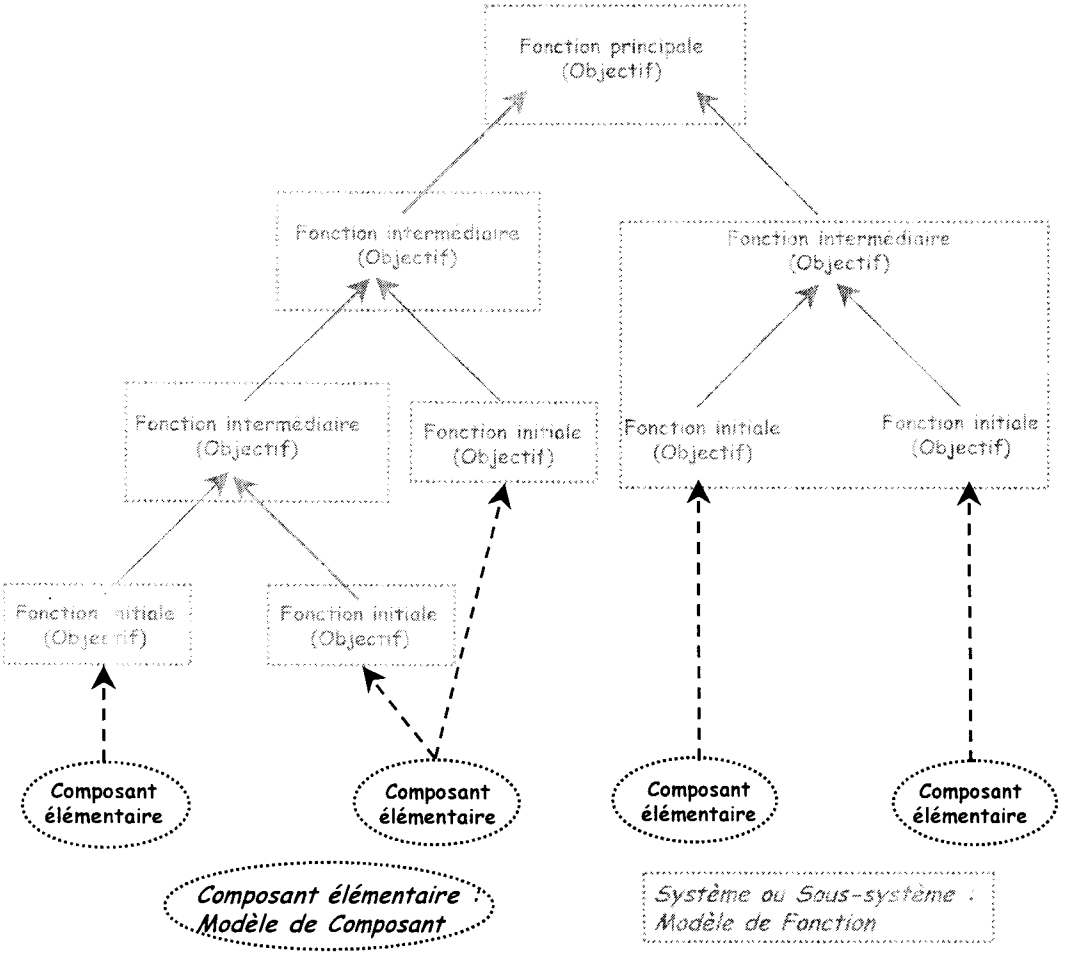


figure IV-1. Schéma d'un modèle comportemental.

Le rôle du Modèle de Composant est de modéliser le comportement d'un composant d'un point de vue de ses modes. La connaissance du comportement de

chaque composant, que nous appelons **composants élémentaires**, permet de caractériser les fonctions initiales rendues par ce composant (*figure IV-1*).

1.1 Les composants à modéliser

La notion de composant élémentaire est totalement subjective. En effet, les concepteurs de la fonction de Plannification/Ordonnancement considèrent les ressources de transformation et de transport comme des composants élémentaires du Système de Production. Un tour, par exemple, est considéré comme un composant élémentaire. Par contre, du point de vue des concepteurs de la fonction de Surveillance, le niveau élémentaire est celui des actionneurs des ressources. La broche, le fourreau de ce tour, ... sont considérés comme des composants élémentaires pour les concepteurs de la fonction de Surveillance.

La question est alors de savoir jusqu'à quel niveau de décomposition du système, il est nécessaire d'aller pour avoir suffisamment d'informations pertinentes pour la Gestion des Modes.

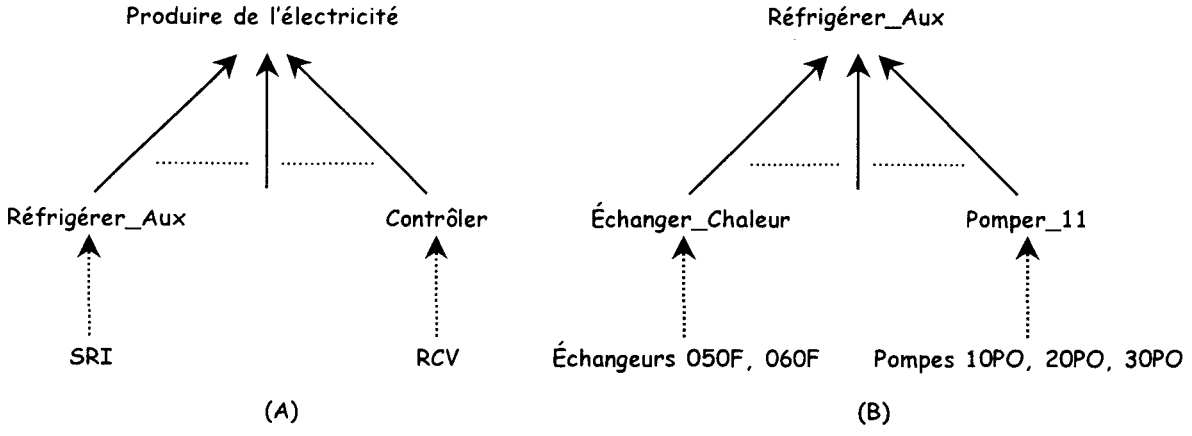


figure IV-2. Extrait des modèles comportementaux simplifiés de la centrale nucléaire et du circuit SRI.

Ce qui nous intéresse c'est de pourvoir caractériser les composants qui sont directement liés aux fonctions initiales du MFC (*Annexe 1*) du système étudié. C'est pourquoi nous considérons comme composant élémentaire toute ressource ou ensemble de ressources permettant de délivrer les fonctions initiales du MFC du système étudié. Nous ne décomposerons pas ces ressources comme cela est fait lors de la conception du Graphe Fonctionnel (*Annexe 1*).

Illustration : Prenons l'exemple d'une centrale nucléaire. La figure IV-2(A) représente un extrait du schéma, très (très) simplifié, du modèle comportemental d'une centrale nucléaire. Certaines des fonctions initiales d'un tel système sont la réfrigération des auxiliaires (fonction "**Réfrigérer_Aux**") et le contrôle chimique et volumétrique (fonction "**Contrôler**"). L'étude de la structure de la centrale nucléaire met en avant que ces fonctions sont respectivement assurées par deux circuits : le SRI et le RCV. Du point de vue de la centrale nucléaire, ils constituent des composants élémentaires.

Par contre, si le système étudié est le circuit SRI, la figure IV-2(B), qui représente de manière très simplifiée le modèle comportemental du SRI, montre que les composants élémentaires retenus sont entre autres les échangeurs 050F et 060F et les pompes 10PO, 20PO et 30PO.

Par cet exemple, nous venons de préciser ce que nous entendons par le terme *composant élémentaire*. Un composant est élémentaire par rapport à quelque chose et non pas dans l'absolu.

1.2 Structuration du Modèle de Composant

Nous avons précédemment expliqué notre choix pour le formalisme des SyncCharts (Chapitre III, §.1.2.2) avec lequel nous allons représenter le Modèle de Composant [Dan, 00/d].

Notre démarche pour la détermination des modes d'un Système de Production (Chapitre III, §.2.2.2) nous a permis de définir une liste de modes et familles de modes généraux (Chapitre III, §.2.2.3). Rappelons que la liste des états à prendre en compte dépend du système étudié. La question est alors de déterminer la structure du Modèle de Composant. Le terme structure désigne ici l'agencement du modèle SyncCharts (hiérarchie, parallélisme, ...).

Dans un premier temps, un parallèle entre les états, les modes et les familles de modes retenus, qui caractérisent le composant, et les éléments graphiques qui composent les SyncCharts, nous a permis de déterminer une ébauche du Modèle de Composant. En effet, nous avons défini :

- Les modes :

Chaque mode d'un composant est représenté par une constellation. En effet, une constellation est un ensemble d'étoiles tel qu'une et seule étoile est active à

l'intérieur d'une constellation. Cette définition est analogue à notre définition d'un mode (Chapitre III, §.2.2.1, Définition 6) dans laquelle il est spécifié que dans un mode, à un instant donné, un seul état est actif.

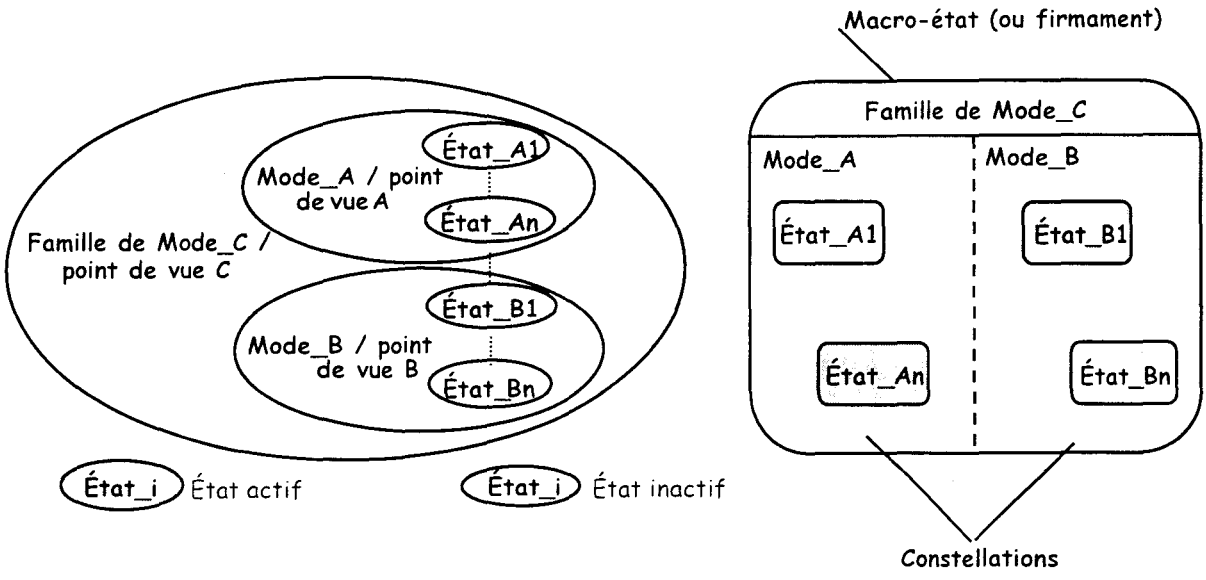


figure IV-3. Parallèle entre les modes et les éléments des SyncCharts.

- Les états :

Par conséquent, nous pouvons assimiler un état (d'un mode) à une étoile dans le formalisme des SyncCharts.

- Une famille de modes :

Enfin, une famille de modes correspond à un ensemble de modes dans lequel plusieurs modes sont simultanément actifs (Chapitre III, §.2.2.1, Définition 7). Un macro-état, dans le formalisme des SyncCharts, est constitué d'une ou plusieurs constellations en parallèles. Nous pouvons donc représenter chaque famille de modes par un macro-état (ou firmament).

La figure IV-3 illustre le parallèle entre les modes et une famille de modes et les éléments graphiques du formalisme SyncCharts. Il est à noter que le terme étoile n'apparaît pas. En effet, pour désigner les étoiles de chacune des constellations, nous devons représenter les façons de quitter chacune d'entre elles ; les transitions.

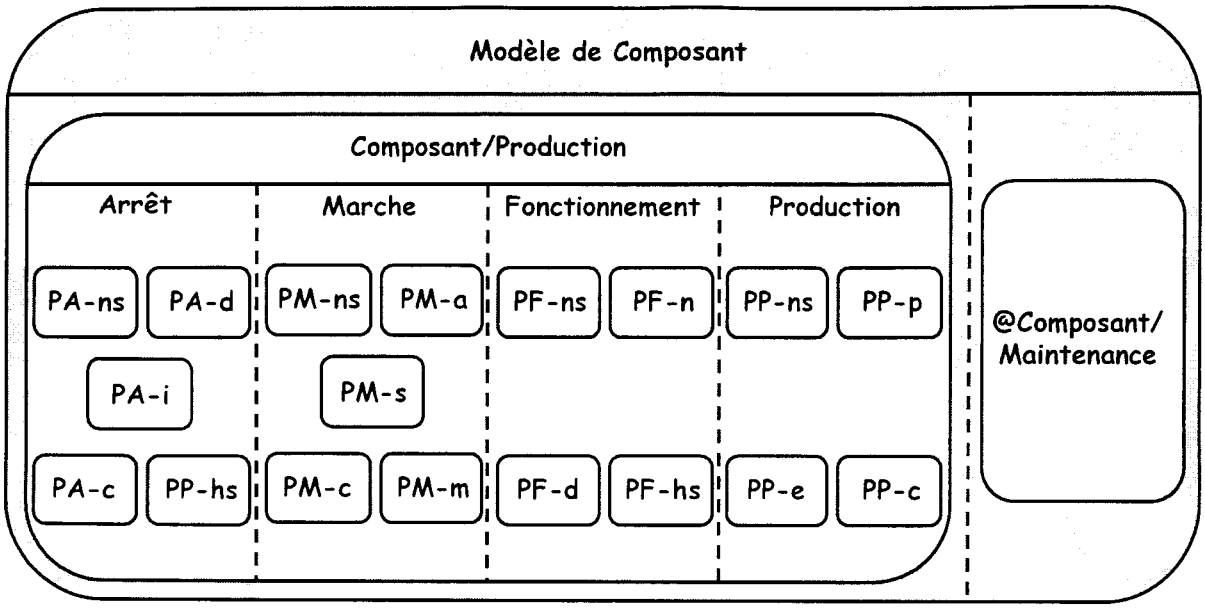


figure IV-4. Première ébauche du Modèle de Composant.

Un macro-état n'est qu'une étoile du niveau supérieur, par conséquent un Modèle de Composant est un macro-état qui, selon notre liste des familles retenues, comporte deux constellations. L'une représente le point de vue production et l'autre le point de vue maintenance. La figure IV-4 présente une ébauche du Modèle de Composant. Rappelons que le symbole "@" signifie que ce module est défini autre part.

1.3 Démarche de conception

Rappelons que l'un des nos objectifs est de proposer une méthode suffisamment détaillée et explicite de telle façon qu'elle apparaisse comme un guide pour le concepteur (Chapitre III, §.1.1.1). Pour ce faire, nous proposons de présenter, ci-après, la démarche qui nous a conduit à l'élaboration du Modèle de Composant.

Le Modèle de Composant doit modéliser le comportement d'un composant élémentaire du point de vue de ses modes. Nous avons vu que le comportement se détermine à partir des différents états que peut prendre le composant et des conditions de passage d'un état vers un autre. La définition du Modèle de Composant passe alors premièrement par la détermination de ses états et deuxièmement par la détermination des conditions de passage. Nous appelons la première étape la ***spécification de la partie statique*** et la deuxième la ***spécification de la partie dynamique***.

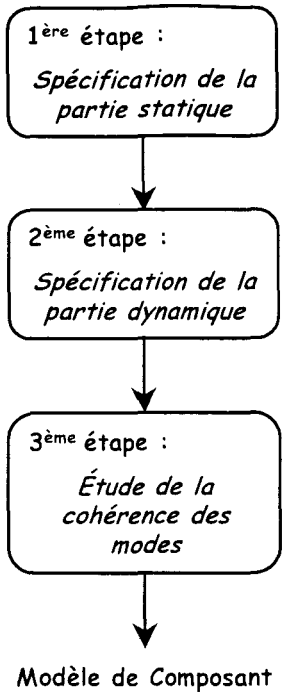


figure IV-5. Démarche de conception du Modèle de Composant.

Au niveau composant élémentaire, la gestion de ses modes consiste à assurer la ***cohérence*** de ses modes. Cette troisième étape, la plus longue, permet d'assurer la fiabilité des informations délivrées et d'assurer le respect des contraintes imposées par le concepteur.

L'un des objectifs du Modèle de Composant est de fournir des informations aux différents acteurs du contrôle commande (Chapitre III, §.2.3.1). Chaque mode fournit une information sur l'état du composant selon un point de vue. Nous avons vu que tous ces modes sont en parallèles. Cependant, ces différents modes caractérisent des états pour le même composant, il existe donc par conséquent des interactions entre eux. Ces interactions peuvent alors conduire à des situations incohérentes : il est difficile de concevoir un système qui peut se trouver à la fois en mode de production effective et en mode d'arrêt hors tension. Certaines situations sont constamment proscrites alors que d'autres le sont par le concepteur selon les stratégies de sécurité et de conduite.

Pour éviter de telles situations, il est nécessaire de déterminer quels sont les états compatibles entre eux et quelles sont les interactions existantes dans le système [Dan, 99/b].

Définition 10 *: une interaction*

Une interaction entre deux modes traduit un lien de cause à effet entre deux modes. L'occurrence d'événement conduisant à l'activation de certains états dans un mode donné implique une commutation d'états dans un autre mode.

Au niveau composant, ces interactions permettent le plus souvent d'assurer la cohérence du comportement du système suivant les spécifications du concepteur. L'activation de l'état hors service dans le mode de fonctionnement peut, par exemple, conduire à l'arrêt du système dans un état déterminé. Elles peuvent également correspondre à une spécification de conduite : la production peut débuter si et seulement si un état de marche est sélectionné.

Définition 11 *: états incompatibles*

Deux états sont dits incompatibles si l'activation simultanée de ces deux états traduit une situation sémantiquement incorrecte.

Une ressource qui ne peut être ni caractérisée d'un point de vue du mode de marche et ni du point de vue du mode d'arrêt en est un exemple. Pour de telles situations, deux solutions sont envisageables :

- L'interdiction de basculer vers une situation où ces états sont composés : Il est alors nécessaire de vérifier que de telles situations ne conduisent pas à des situations de blocage,
- Le passage transitoire par ces états composés : dans ce cas, le passage par ces états combinés interdits n'est qu'une transition vers un état stable autorisé. La mise en œuvre de ces transitoires est effectuée à partir de relation d'interaction.

Ces trois étapes (*figure IV-5*), que nous allons détailler par la suite, correspondent à notre démarche pour la conception du Modèle de Composant. C'est elle qui permettra à chaque concepteur d'adapter ce modèle au système étudié. Nous verrons que certaines parties de la démarche sont immuables quel que soit le Système de Production étudié.

2 CONCEPTION DU MODÈLE DE COMPOSANT

2.1 Spécification statique et dynamique

Cette partie repose sur la spécification des différents états que peut prendre un composant et des transitions qui permettent de passer d'un état à un autre.

Dans un souci de généricité, nous avons présenté, les modes retenus pour caractériser l'état d'un Système de Production. Nous avons montré également qu'un composant élémentaire peut être également considéré comme un Système de Production à part entière (illustration, Chapitre IV, §.1.1). Par conséquent, les modes retenus pour caractériser l'état d'un Système de Production sont les mêmes que ceux qui caractérisent un composant élémentaire. La spécification de la partie statique consiste alors à recenser les états que peut prendre le système étudié. Cette première étape correspond à ce que nous avons présenté pour le circuit SRI au §.2.3 du chapitre III.

Le Modèle de Composant ne peut décrire le comportement d'un composant que si les conditions de commutation d'un état vers un autre sont exprimées. Cette deuxième étape se déroule en deux phases.

La première consiste à définir les états initiaux du modèle. Pour que le modèle puisse être initialisé, chaque constellation doit comporter un état initial. L'état choisit par le concepteur doit représenter son état par défaut par rapport à un mode donné. Il représente également le premier état actif du modèle. La détermination de la plupart des états initiaux est principalement une question de bon sens. Il est difficile d'imaginer que l'état initial, d'un point de vue du mode de marche, soit le mode de marche automatique. Par contre, certains états initiaux peuvent être liés à l'interprétation du concepteur. En effet, du point de vue du mode de fonctionnement, le fonctionnement normal peut être considéré comme initial. En ce qui nous concerne, il nous semble difficile de caractériser initialement l'état du composant d'un point de vue mode de fonctionnement. En effet, nous considérons que le mode de fonctionnement est dépendant de l'évolution du système donc du mode de production. Or, ce dernier ne peut évoluer que s'il en a reçu l'ordre. Pour nous, l'activation initiale du modèle et donc du mode de fonctionnement n'est pas assimilée à un ordre reçu. Par conséquent l'état initial dans le mode de fonctionnement est l'état "PF-ns". L'activation de cet état permet de spécifier, qu'à l'instant donné, aucun état de

cette famille peut caractériser l'état du système du point de vue du mode de fonctionnement. Cette famille est donc caractérisée par l'état non significatif (état "PF-ns").

États	e_1			e_j		e_n
e_1						
e_i				0 ou $C_{ei,ej}$		
e_j						
e_n						

figure IV-6. Matrice des Conditions de Passage.

La deuxième phase consiste à déterminer les conditions de passage d'un état à un autre. Pour se faire, nous utilisons une ***Matrice des Conditions de Passage*** (**MCP**) où les lignes et les colonnes représentent des états. Cette représentation matricielle permet de prendre en compte toutes les possibilités au sein d'un mode. Étant donné que les modes sont en parallèles, il y a autant de matrices MCP que de modes pris en compte. $MCP^{m}_{(e_i,e_j)}$ représente la condition de passage de l'état e_i à l'état e_j (avec $e_i, e_j \in m$) dans le mode "m". Elle est construite comme suit (*figure IV-6*) :

$MCP^{m}_{(e_i,e_j)} = C_{e_i,e_j}$ s'il existe une condition C_{e_i,e_j} de passage de l'état e_i à l'état e_j,

$MCP^{m}_{(e_i,e_j)} = 0$ sinon.

La condition de passage C_{e_i,e_j} peut correspondre à l'occurrence d'un événement ou à une combinaison logique d'événements.

Illustration : $C_{e_i,e_j} = \alpha \; AND \; NOT \; \beta$ signifie que si l'état e_i est actif alors l'occurrence de "α" et l'absence de "β" désactivent l'état e_i et active l'état e_j.

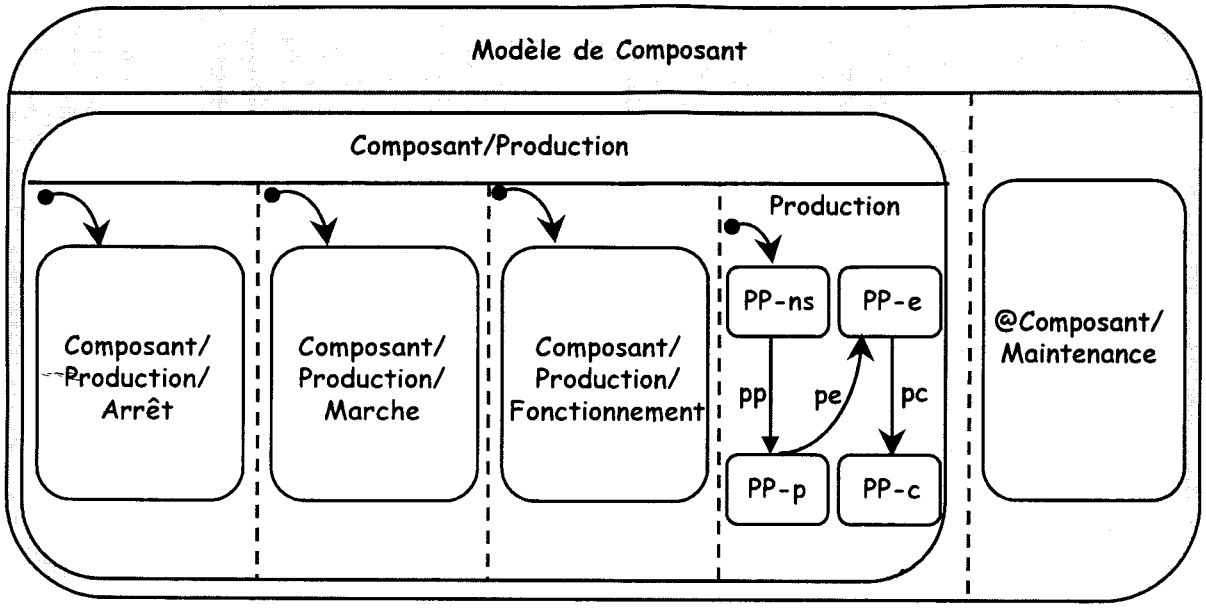


figure IV-7. Modèle de Composant : 1ere version.

Remarque : En ce qui concerne les transitions, nous considérons que tout arc reliant un état à un autre état est en fait une agrégation. La figure IV-8 illustre nos propos. Pour passer de l'état "Etat1" à l'état "Etat2" *(figure IV-8(A))*, il est nécessaire que l'événement "*état2_demandé*" soit présent. Dans la pratique cet événement correspond à un ordre émis. L'occurrence de cet événement fait basculer le système dans l'état "Etat12". Lorsque le système a atteint l'état demandé, un compte rendu est émis ("*état2_atteint*") ce qui permet de contrôler que l'ordre envoyé s'est bien exécuté. Afin de simplifier les modèles présentés, nous adoptons la représentation de la figure IV-8(B). Nous ne représentons que l'événement déclencheur et l'état atteint. Nous supposons donc que tout ordre émis s'exécute correctement.

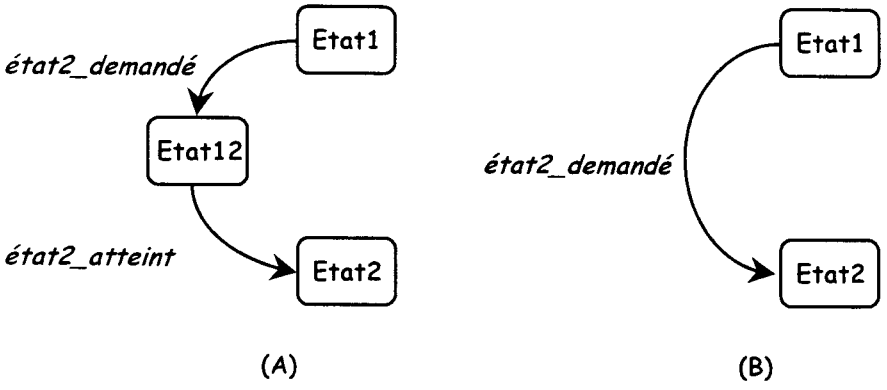


figure IV-8. Simplification de représentation.

Cas particulier : les états non significatifs

Les états non significatifs sont des états particuliers. Rappelons que ces états permettent de caractériser l'état du système par rapport à un mode donné quand les autres états de ce même mode ne le permettent pas. Cependant, à un moment ou à un autre un événement se produira permettant ainsi de caractériser le système par rapport à ce mode. Ce sont ces conditions de passage que le concepteur doit spécifier. Les conditions de passage, d'un état quelconque vers un état non significatif, seront spécifiées plus tard automatiquement en fonction des contraintes imposées par le concepteur. En effet, ces conditions n'ont pas réellement de sens physique, elles permettent principalement d'assurer la cohérence du Modèle de Composant.

Selon le composant élémentaire à modéliser, il n'existe pas toujours de condition de passage d'un état non significatif vers un état précis. Cela peut être par exemple le cas d'un système qui a toujours besoin d'une phase de production préparatoire avant la phase de production effective. Dans ce cas, aucune transition de passage est définie entre l'état non significatif ("PP-ns") et l'état production effective ("PP-e") du mode de production (*figure IV-7*).

Ces conditions de passage sont alors reportées sur le Modèle de Composant. Ceci donne une première version du Modèle de Composant (*figure IV-7*).

2.2 La cohérence des modes

Une fois le comportement attendu spécifié, il est nécessaire d'en assurer la cohérence. La phase de spécification pour la cohérence des modes repose sur l'utilisation de la ***Matrice de Cohérence des Modes*** (**MCM**) [Dan, 99/b]. Les lignes et les colonnes de cette matrice représentent des états.

$MCM\binom{m_i\ m_j}{e_{ik}\ e_{jl}}$ représente la compatibilité des états e_{ik} et e_{jl} (avec $e_{ik} \in m_i, e_{jl} \in m_j$). Elle est construite comme suit :

$MCM\binom{m_i\ m_j}{e_{ik}\ e_{jl}} = 1$ si les états e_{ik} et e_{jl} sont compatibles,

$MCM\binom{m_i\ m_j}{e_{ik}\ e_{jl}} = 0$ sinon.

		A					M					F				P			
		PA-ns	PA-ht	PA-i	PA-f	PA-d	PM-ns	PM-a	PM-s	PM-c	PM-m	PF-ns	PF-n	PF-d	PF-hs	PP-ns	PP-p	PP-e	PP-c
A	PA-ns	1	0	0	0	0													
	PA-ht		1	0	0	0													
	PA-i			1	0	0													
	PA-f				1	0													
	PA-d					1													
M	PM-ns						1	0	0	0	0								
	PM-a							1	0	0	0								
	PM-s								1	0	0								
	PM-c									1	0								
	PM-m										1								
F	PF-ns											1	0	0	0				
	PF-n												1	0	0				
	PF-d													1	0				
	PF-hs														1				
P	PP-ns															1	0	0	0
	PP-p																1	0	0
	PP-e																	1	0
	PP-c																		1

figure IV-9. Matrice de Cohérence
des Modes de la famille de production.

Rappelons que c'est le concepteur qui détermine, selon ses propres critères, si deux états sont compatibles ou incompatibles. Remplir directement la matrice MCM, selon le nombre d'états pris en compte, peut ne pas être une tâche simple. C'est pourquoi nous proposons différentes étapes pour y parvenir. Nous étudions seulement la cohérence des modes de la famille de production afin de présenter notre démarche.

2.2.1 Les états compatibles

Notre première étape consiste à déterminer les états compatibles ; du moins ceux qui le sont de façon triviale. Si nous reprenons la définition 11, nous pouvons en déduire que deux états sont compatibles si ces deux états peuvent être simultanément actifs tout en ayant une sémantique correcte. Notre première étape consiste alors à déterminer (à choisir) tous les états qui peuvent être simultanément actifs.

La détermination des autres états compatibles ou incompatibles est alors guidée, en partie, par ce premier choix. Pour illustrer cela et pour guider le concepteur dans leur détermination, nous proposons d'utiliser un schéma du type de la figure IV-10. Il représente tous les modes et états que nous avons retenus pour la caractérisation des Systèmes de Production.

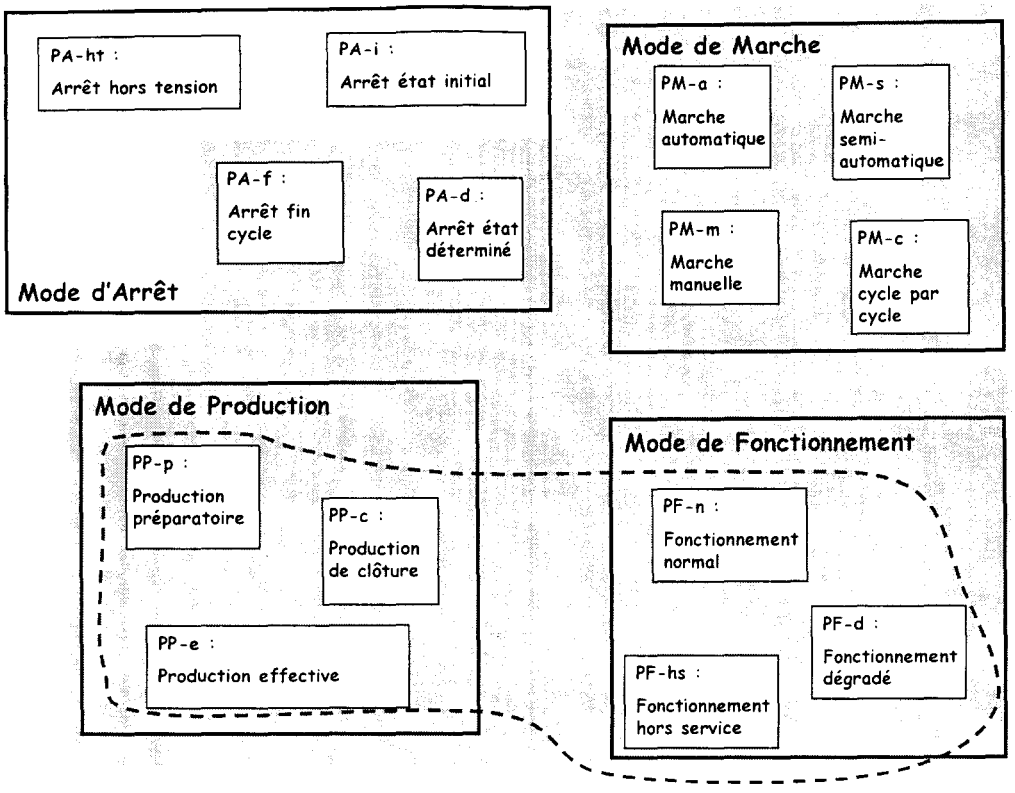


figure IV-10. Schéma des modes et des états de la famille de production.

Déterminer les états qui peuvent être simultanément actifs revient à définir une zone, que nous appelons ***zone de simultanéité*** (*figure IV-10*, en gris foncé), dans laquelle les états de deux modes différents peuvent être actifs simultanément. Certains modes peuvent partiellement faire partie de cette zone. Cela signifie que certains de leurs états peuvent être actifs avec le reste des états de la zone de simultanéité. Les limites et le nombre de zones sont définies par le concepteur. Pour certains, il peut paraître incohérent de dire que le système est à l'arrêt dans un état déterminé et simultanément en mode de production effective. Dans ce cas, le mode d'arrêt dans un état déterminé ne fera pas partie de la zone de simultanéité. Selon certains critères (sécurité, conduite, valeur ajoutée, ...), le concepteur définira quels sont les états pouvant être simultanément actifs. Réduire au maximum la zone de simultanéité ou en définir de nombreuses ne présente aucun avantage dans le cadre de notre approche. En effet, l'objectif est de pouvoir caractériser à tout moment l'état du système et selon plusieurs points de vue.

		A					M					F				P			
		PA-ns	PA-ht	PA-i	PA-f	PA-d	PM-ns	PM-a	PM-s	PM-c	PM-m	PF-ns	PF-n	PF-d	PF-hs	PP-ns	PP-p	PP-e	PP-c
A	PA-ns	1	0	0	0	0													
	PA-ht		1	0	0	0													
	PA-i			1	0	0													
	PA-f				1	0		1	1	1	1		1	1	1		1	1	1
	PA-d					1		1	1	1	1		1	1	1		1	1	1
M	PM-ns						1	0	0	0	0								
	PM-a							1	0	0	0		1	1	1		1	1	1
	PM-s								1	0	0		1	1	1		1	1	1
	PM-c									1	0		1	1	1		1	1	1
	PM-m										1		1	1	1		1	1	1
F	PF-ns											1	0	0	0				
	PF-n												1	0	0		1	1	1
	PF-d													1	0		1	1	1
	PF-hs														1		1	1	1
P	PP-ns															1	0	0	0
	PP-p																1	0	0
	PP-e																	1	0
	PP-c																		1

figure IV-11. États compatibles.

La zone de simultanéité permet de compléter en partie la matrice de compatibilité (i.e. mettre des "1") pour un certain nombre de couples (e_i, e_j) où $e_i \in m_1$ et $e_j \in m_2$, m_1 et m_2 étant deux modes différents. Le principe consiste à mettre un "1" pour chacun des couples où e_i et e_j qui appartiennent à la **même** zone de simultanéité. La figure IV-11 présente la matrice partiellement complétée à partir de la zone de simultanéité.

2.2.2 Les états trivialement incompatibles

		A					M					F				P			
		PA-ns	PA-ht	PA-i	PA-f	PA-d	PM-ns	PM-a	PM-s	PM-c	PM-m	PF-ns	PF-n	PF-d	PF-hs	PP-ns	PP-p	PP-e	PP-c
A	PA-ns	1	0	0	0	0													
	PA-ht		1	0	0	0		0	0	0	0		0	0	0		0	0	0
	PA-i			1	0	0		0	0	0	0		0	0	0		0	0	0
	PA-f				1	0		1	1	1	1		1	1	1		1	1	1
	PA-d					1		1	1	1	1		1	1	1		1	1	1
M	PM-ns						1	0	0	0	0								
	PM-a							1	0	0	0		1	1	1		1	1	1
	PM-s								1	0	0		1	1	1		1	1	1
	PM-c									1	0		1	1	1		1	1	1
	PM-m										1		1	1	1		1	1	1
F	PF-ns											1	0	0	0				
	PF-n												1	0	0		1	1	1
	PF-d													1	0		1	1	1
	PF-hs														1		1	1	1
P	PP-ns															1	0	0	0
	PP-p																1	0	0
	PP-e																	1	0
	PP-c																		1

figure IV-12. États trivialement incompatibles.

Par raisonnement inverse et à partir de la figure IV-10, il est facile de déterminer certains états incompatibles. Tous les états qui ne sont pas situés

dans la zone de simultanéité sont incompatibles avec ceux contenus par cette même zone. Leur incompatibilité se traduit par un "0" dans la matrice MCM (*figure IV-12*).

2.2.3 Compatibilités liées aux états non significatifs

Dans la zone de simultanéité

Rappelons que ces états permettent de caractériser l'état du système par rapport à un mode donné quand les autres états de ce même mode ne le permettent pas.

A partir de là, déterminer si un état "e_i" d'un mode X est compatible avec un état non significatif "e_{ns}" d'un mode Y revient à se demander : "*Est-ce qu'il est possible qu'**à un instant donné**, il ne soit pas possible de caractériser l'état du système par rapport au mode Y (i.e. activation de l'état non significatif) et que simultanément l'état "e_i" (différent de l'état non significatif) du mode X soit actif ?*". Cela n'empêche en rien que les autres états du mode Y soit également compatible avec l'état "e_i".

Considérons l'exemple des modes de marche et d'arrêt. Il est possible qu'à un instant donné, il soit impossible de caractériser l'état du système par rapport au mode d'arrêt ("PA-ns") et que simultanément l'état de marche automatique ("PM-a") soit actif. En outre, dans cet exemple, certains états du mode d'arrêt sont également compatibles avec l'état de marche automatique ("PM-a") (*figure IV-12*).

Hors de la zone de simultanéité

En ce qui concerne la compatibilité des états des modes n'appartenant pas à la zone de simultanéité avec les états non significatifs, la figure IV-10 permet d'y répondre pour certains.

En effet, prenons le cas de l'état non significatif du mode de marche ("PM-ns") et l'état hors tension du mode d'arrêt ("PA-ht"). Le premier état correspond à la non-activation des autres états de ce mode qui appartiennent tous à la zone de simultanéité. Le deuxième état n'appartient pas à cette zone. Comme à chaque instant, chaque mode possède un état actif, il est alors tout à fait possible que ces deux états ("PM-ns" et "PA-ht") soient simultanément actifs. Il en est de même

pour les états "PM-ns" et "PA-i". Dans ces deux cas nous trouverons un "1" dans la matrice MCM. Il est à noter que les états "PF-ns", "PP-ns" présentent la même compatibilité par rapport à ces états du mode d'arrêt.

2.2.4 Les derniers états

La difficulté des dernières études de la compatibilité des états repose sur le fait que ces états appartiennent à la zone de simultanéité. Par conséquent, ils peuvent, mais ce n'est pas une obligation, être simultanément actifs. En outre, rien ne dit qu'ils sont obligatoirement tous simultanément actifs au même instant. Ceci est dû à l'enchaînement de l'activation des états. En effet, il est rare qu'une même et seule consigne lance l'activation de tous les états des modes simultanément actifs. En d'autres termes, généralement, il existe différentes consignes d'activation : une consigne pour sélectionner le type de marche, une consigne pour sélectionner le lancement de la production, ... Se pose alors la question du séquencement de ces ordres. C'est ce que nous appelons ici la stratégie de conduite. Là encore, la coopération avec le concepteur est nécessaire pour connaître cette stratégie. C'est elle qui va nous permettre d'étudier les dernières compatibilités d'états.

Bien que différentes stratégies soient envisageables, nous proposons d'adopter une stratégie inspirée du GEMMA. En analysant le GEMMA, nous pouvons dire que l'état "initial" d'un système est quand il est à l'arrêt. Pour pouvoir passer en production, il est nécessaire de choisir un mode de marche. Cette sélection permet d'arriver dans la zone de production et d'être dans une famille des modes de fonctionnement, ...Ceci entraîne une notion d'ordre dans les différents modes pris en compte.

De manière similaire, afin d'assurer un comportement constamment correct du composant, nous introduisons une relation d'ordre entre les modes. Partant du mode d'arrêt, nous considérons qu'il est nécessaire d'activer un état du mode de marche pour accéder au mode de production. Lorsqu'un état du mode de marche est sélectionné alors la production peut débuter. De notre point de vue, le mode de fonctionnement est là pour caractériser l'état du système par rapport à l'état d'avancement de sa production. Par conséquent, pour nous, le mode de production et le mode de fonctionnement sont constamment simultanément actifs. Les pointillés de la figure IV-10 mettent en avant cette forte relation. L'activation du mode de production entraîne alors l'activation du mode de

fonctionnement. Ceci nous conduit également à une relation d'ordre entre modes qui s'écrit :

$PA \prec PM \prec PP \prec PF$ où $\prec$ représente la précédence.

Cette relation, qui peut être différente selon le concepteur, nous permet de compléter la MCM.

		A					M					F				P			
		PA-ns	PA-ht	PA-i	PA-f	PA-d	PM-ns	PM-a	PM-s	PM-c	PM-m	PF-ns	PF-n	PF-d	PF-hs	PP-ns	PP-p	PP-e	PP-c
A	PA-ns	1	0	0	0	0	0	1	1	1	1	0	1	1	1	0	1	1	1
	PA-ht		1	0	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0
	PA-i			1	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0
	PA-f				1	0	0	1	1	1	1	0	1	1	1	0	1	1	1
	PA-d					1	0	1	1	1	1	0	1	1	1	0	1	1	1
M	PM-ns						1	0	0	0	0	1	0	0	0	1	0	0	0
	PM-a							1	0	0	0	1	1	1	1	1	1	1	1
	PM-s								1	0	0	1	1	1	1	1	1	1	1
	PM-c									1	0	1	1	1	1	1	1	1	1
	PM-m										1	1	1	1	1	1	1	1	1
F	PF-ns											1	0	0	0	1	0	0	0
	PF-n												1	0	0	0	1	1	1
	PF-d													1	0	0	1	1	1
	PF-hs														1	0	1	1	1
P	PP-ns															1	0	0	0
	PP-p																1	0	0
	PP-e																	1	0
	PP-c																		1

figure IV-13. MCM finale.

Prenons l'exemple de l'état non significatif du mode de fonctionnement et l'état automatique du mode de marche. Dans ce cas, du fait de notre relation d'ordre, il est tout à fait possible qu'à un instant donné, aucun état du mode de fonctionnement ne soit actif (état non significatif non compris) et que simultanément l'état automatique "PM-a" du mode de marche soit actif. Ces deux états sont donc compatibles. Par contre, étant donné notre relation d'ordre, il est impossible qu'aucun état du mode de marche (activation de "PM-ns") ne soit actif et que simultanément, par exemple, l'état de production effective ne soit pas actif ("PP-e"). Par conséquent, ces deux états ("PM-ns" et "PP-e") sont incompatibles.

Ces différentes étapes permettent de guider le concepteur dans le remplissage de la Matrice de Cohérence des Modes. En outre, l'utilisation de la zone de simultanéité permet de déterminer automatiquement l'incompatibilité de certains états (les états trivialement incompatibles et les états non significatifs hors zone).

Avant de prendre en compte ces spécifications, il est nécessaire de vérifier la cohérence de la matrice MCM. La principale vérification porte la valeur des lignes et des colonnes. En effet, ce contrôle consiste à vérifier que :

$$\sum_{k=0}^{|m_i|} MCM^{(m_i, m_j)}_{(e_{ik}, e_{jl})} \neq 0 \text{ et } \sum_{l=0}^{|m_j|} MCM^{(m_i, m_j)}_{(e_{ik}, e_{jl})} \neq 0$$

Ceci permet de vérifier qu'aucun état d'un mode m_i est incompatible avec tous les autres états d'un mode m_j et inversement.

2.3 Mise en œuvre de la cohérence des modes

Cette étape consiste à rapporter les spécifications de la matrice MCM sur le modèle de composant. Elle est effectuée selon les stratégies de conduite et de sécurité imposées par le concepteur.

2.3.1 États interdits et Interactions

Les incompatibilités ou les interactions entre états se traduisent par des conditions sur les transitions entre états et par des combinaisons d'états non accessibles. Une des solutions pour traduire les incompatibilités d'états représentées par la matrice MCM consiste à faire la composition de tous les modes d'une même famille. Chaque mode correspond en fait à un automate. Les étapes suivantes consistent alors à repérer tous les états composés interdits et à supprimer toutes les transitions qui arrivent et qui partent de chacun de ces états. Une dernière étape est lors nécessaire pour "désassembler" l'automate résultant afin de reporter les modifications sur les automates de chacun des modes.

L'explosion combinatoire est souvent un problème lors de la composition d'automates et fastidieuse sans l'aide d'un outil informatique. En outre, la taille de l'automate résultant ne facilite pas la tâche du "désassemblage". C'est pourquoi, nous avons opté pour une méthode qui n'utilise pas la composition d'automates de façon "directe".

Nous avons vu que la matrice indique l'incompatibilité d'états et que celle ci peut se traduire soit par un état interdit soit par un état transitoire impliquant alors une interaction. Il à noter que le concepteur peut spécifier également dans

cette phase des interactions dont l'origine ne sont pas initialement des états incompatibles. Par exemple, considérons une ressource dont la matrice de cohérence des modes correspond à celle de la figure IV-13. Il est tout à fait possible que pour des raisons de sécurité, le concepteur décide que l'atteinte des états en production effective ("PP-e") et en fonctionnement hors service ("PF-hs") provoque une commutation vers l'état d'arrêt dans un état déterminé. Seules les commutations vers des états compatibles sont alors possibles. Le principe consiste alors à modifier la matrice en corrigeant le "1" par un "0".

Quel que soit le sens de l'incompatibilité (état transitoire ou interdit), un mécanisme de spécification doit être mis en place afin que le Modèle de Composant la prenne en compte.

2.3.2 Les états interdits : mécanismes

Les états interdits correspondent à des situations qui ne doivent pas se produire. Ceci implique que toutes commutations vers ces états doivent être interdites quelle que soit la situation.

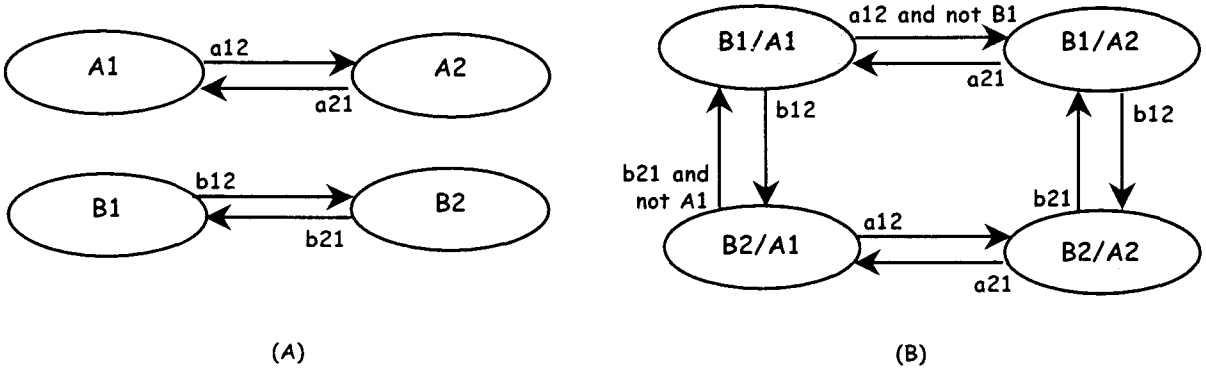


figure IV-14. Spécification des états interdits.

Considérons deux modes A et B représentés par les deux automates de la figure IV-14(A). Supposons que l'activation simultanée des états A1 et B1 soit interdite (état hachuré, figure IV-14(B)). Cette combinaison d'états est alors considérée comme un état interdit à proscrire. Afin qu'une telle situation ne se produise, il est nécessaire d'ajouter une contrainte aux conditions de passage déjà existantes. La figure IV-14(B) met en avant les conditions concernées. L'ajout des contraintes "and not A1" et "and not B1" rend ainsi impossible la commutation des modes si l'un des états "A1" ou "B1" est déjà actif. Nous utilisons ce mécanisme pour chaque état interdit.

Remarque : cet exemple illustratif montre que la spécification des états initiaux ainsi que celle des incompatibilités est importante et principalement liée au contexte de l'application concernée. Dans l'exemple précédent, en désignant les états "A1" et "B1" comme des états initiaux, il est alors incohérent d'interdire l'état "A1B1". Réciproquement, si les états "A1" et "B1" sont incompatibles alors ils ne peuvent pas être des états initiaux.

2.3.3 Les états transitoires et les interactions : mécanismes

Les états transitoires sont des états dans lesquels on peut aller mais où l'on ne peut pas rester. L'activation de tels états provoque alors une commutation vers des états compatibles.

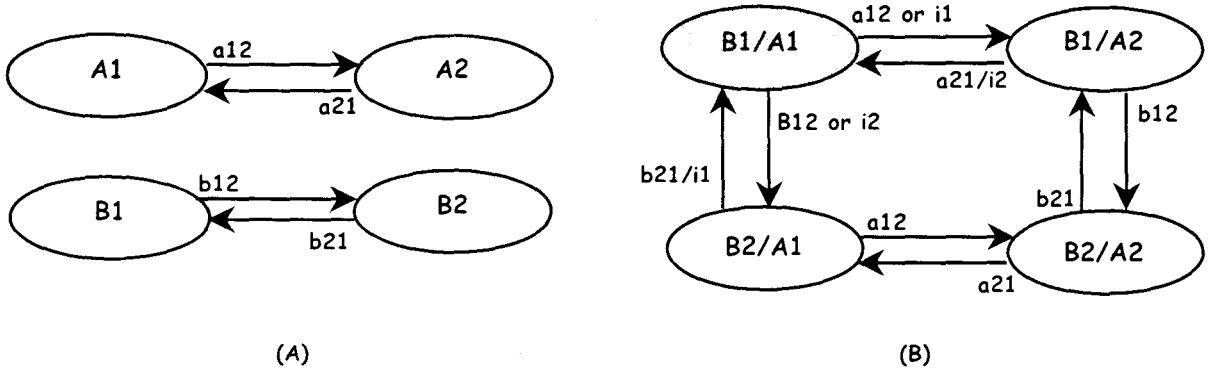


figure IV-15. Spécification des états transitoires et des interactions.

Reprenons notre exemple précédent mais considérons cette fois ci que l'activation simultanée des états A1 et B1 représente un état transitoire (état hachuré, figure IV-15 (B)).

Le mécanisme des états transitoires et des interactions consiste à provoquer un événement lorsqu'une condition de passage valide conduit vers l'état transitoire. Pour mettre en œuvre un tel mécanisme, il est alors nécessaire de déterminer vers quel état il faut commuter. Ainsi ce mécanisme permet de commuter vers un état ou un autre en fonction de l'origine de l'activation de l'état transitoire. Dans notre exemple, si la condition "b21" (respectivement "a21") est la source de l'activation, l'état "A2" (respectivement "B2") sera atteint.

Remarque : étant donné le principe synchrone adopté, la commutation de l'état "B2/A1" à l'état "B1/A2" se fait de manière instantanée.

2.3.4 Mise en œuvre

La mise en œuvre de tels mécanismes dépend d'une part du sens de l'incompatibilité (état transitoire ou interdit). D'autre part, elle dépend de la relation d'ordre des modes présentée précédemment et de la notion de priorité d'état. Prenons l'exemple de l'état hors tension du mode d'arrêt ("PA-ht") et de l'état marche automatique du mode de marche ("PM-a"). D'après la matrice de la figure IV-13, ces états sont incompatibles. Quel est alors la nature de cette incompatibilité ? Ces états sont incompatibles car leur activation simultanée n'a aucun sens. Pour savoir quelles sont les actions à mener, et donc la nature de cette incompatibilité, il faut alors se demander quelles sont les situations qui peuvent y conduire. Deux solutions sont envisageables :

- Situation 1 : l'état de marche est déjà actif et un arrêt hors tension est demandé,
- Situation 2 : l'état d'arrêt hors tension est déjà actif et une marche automatique est demandée.

Selon la situation initiale, les conséquences ne sont pas les mêmes. En effet, dans le cas de la situation1, si, par exemple, l'arrêt hors tension est considéré comme un arrêt prioritaire alors il faut absolument basculer vers cet état d'arrêt hors tension. Le mode de marche commute alors vers un état cohérent avec l'arrêt hors tension. Dans ce cas précis, seul l'état non significatif du mode de marche est compatible avec celui d'arrêt hors tension. Le mode de marche bascule alors vers l'état non significatif. Dans ce cas, la mise en œuvre correspond à une interaction.

Dans le cas de la situation 2, il semble difficile de demander une mise en marche automatique alors que l'état du système est à l'arrêt hors tension. Dans ce cas, l'ordre de mise en marche automatique n'aura aucun effet. La situation n'évoluera pas. Dans ce cas, la mise en œuvre correspond à un état interdit.

Cet exemple nous montre que pour deux états incompatibles, il peut être nécessaire de mettre en œuvre plusieurs mécanismes d'incompatibilités. En outre ces mises en œuvre dépendent de la priorité de chacun des états.

La priorité des états peut être en partie déduite de la relation d'ordre des modes. En effet, prenons l'exemple de l'état de marche automatique du mode de marche et l'état préparatoire du mode de production. Étant donné la relation

$PA \prec PM \prec PP \prec PF$ où l'opérateur "$\prec$" représente la précédence (Chapitre IV, §.2.2.4), la consigne de marche automatique est prioritaire sur la consigne de début de production. En effet, le mode de marche précédant le mode de production, il est nécessaire de spécifier un mode de marche avant de lancer la production.

Par conséquent, le mode de production ne peut commuter vers son état préparatoire ("PP-p") que si l'état non significatif du mode de marche n'est pas actif ("PM-ns", état interdit). Dans ce cas précis, nous dirons que les états du mode de marche sont plus prioritaires que les états du mode de production. Étant donné la relation forte entre le mode de production et de fonctionnement, la relation analogue existe entre le mode de marche et le mode de fonctionnement.

3 APPLICATION DE LA DÉMARCHE DE LA COHÉRENCE DES MODES

3.1 Cahier des charges

Considérons l'exemple du circuit SRI pour présenter l'enchaînement de la démarche de l'étude de la cohérence des modes. La liste des modes et états retenus est présentée par la figure III-5 (Chapitre III). Nous ne considérerons que la famille de production dans la suite de cet exemple.

États	PA-ns	PA-ht	PA-i	PA-d
PA-ns	0	aht	ai	ad
PA-ht		0	ai	
PA-i		aht	0	ad
PA-d	fin-d	aht	ai	0

figure IV-16. Matrice initiale des Conditions de Passage

A partir du cahier des charges et de la spécification de la partie statique, nous pouvons établir la matrice MCP du circuit SRI (*figure IV-16*) et en déduire l'ébauche du Modèle de Composant du SRI (*figure IV-17*).

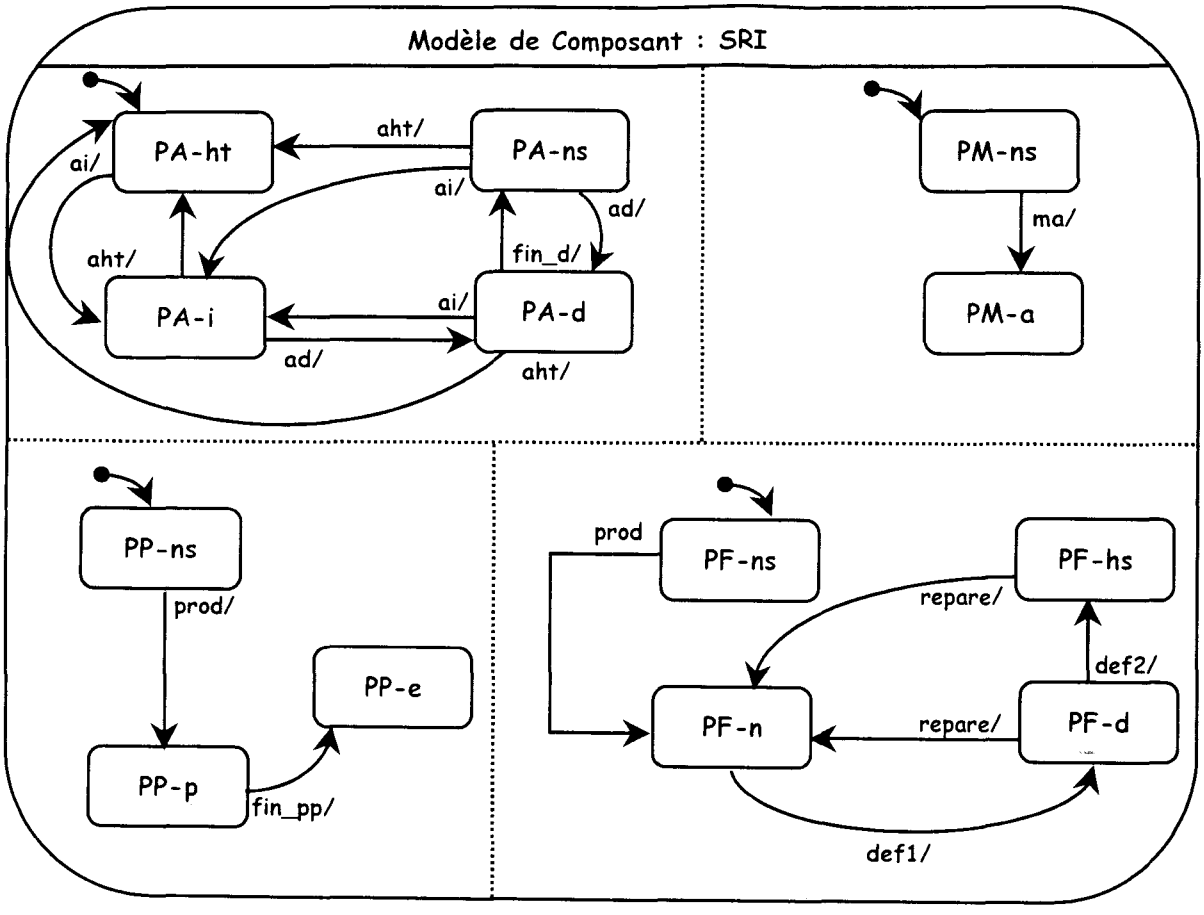


figure IV-17. Modèle de Composant du SRI : 1ère version.

Les particularités de ce modèle concernent :

- Le mode de production : une production effective (fonctionnement à plein régime) n'est possible qu'après la phase de préparatoire qui consiste à faire monter la température jusqu'à la consigne imposée,
- Le circuit SRI ne peut être en production (quel que soit l'état) qu'après la sélection d'un mode de marche et que le circuit soit dans l'état initial (pas de démarrage depuis l'état hors tension du circuit),
- Les zones de simultanéité de ce modèle sont représentées par la figure IV-18. Le mode de marche appartient simultanément aux deux zones,
- L'arrêt hors tension est l'état le plus prioritaire.

La relation d'ordre entre les modes est donnée par la relation : $PA \prec PM \prec PP \prec PF$, qui est également la relation de priorités des états lorsqu'il y a incompatibilité.

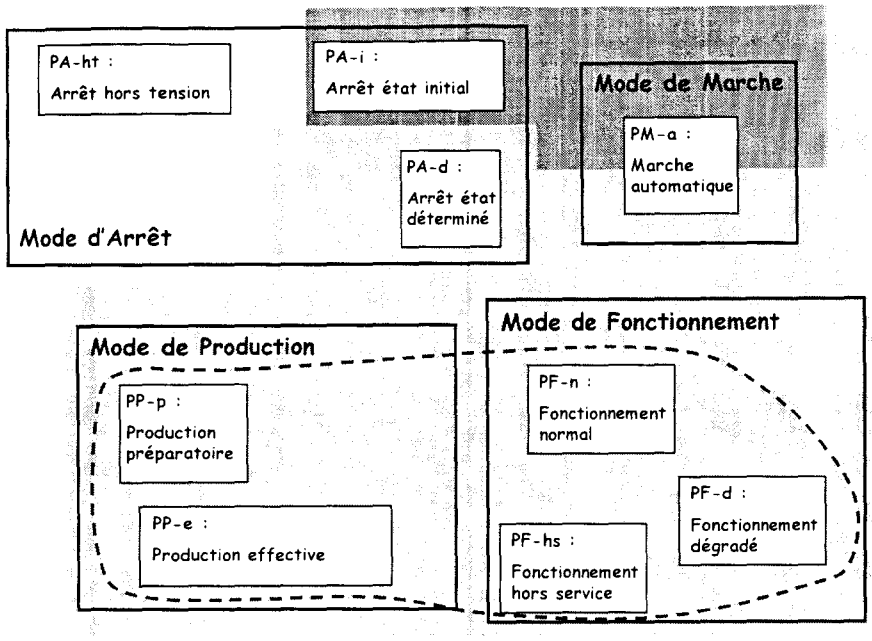


figure IV-18. Zone de simultanéité du SRI.

L'ensemble de ces spécifications permet d'obtenir la Matrice de Cohérence du circuit SRI présentée par la figure IV-19.

		A				M		F				P		
		PA-ns	PA-ht	PA-i	PA-d	PM-ns	PM-a	PF-ns	PF-n	PF-d	PF-hs	PP-ns	PP-p	PP-e
A	PA-ns	1	0	0	0	0	1	0	1	1	1	0	1	1
	PA-ht		1	0	0	1	0	1	0	0	0	1	0	0
	PA-i			1	0	1	1	1	0	0	0	1	0	0
	PA-d				1	0	1	0	1	1	1	0	1	1
M	PM-ns					1	0	1	1	1	1	1	1	1
	PM-a						1	1	1	1	1	1	1	1
F	PF-ns							1	0	0	0	1	0	0
	PF-n								1	0	0	0	1	1
	PF-d									1	0	0	1	1
	PF-hs										1	0	1	1
P	PP-ns											1	0	0
	PP-p												1	0
	PP-e													1

figure IV-19. MCM du circuit SRI.

3.2 Mise en œuvre de la cohérence des modes

L'aspect dynamique des transitions entre états et de leur cohérence est étudiée ici uniquement sous l'angle des modes d'arrêt et de marche.

La matrice de cohérence des modes fait apparaître trois états incompatibles : "PA-ns/PM-ns", "PA-d/PM-ns" et "PA-ht/PM-a".

Pour prendre en compte ces spécifications, nous "superposons" la matrice de cohérence des modes et les conditions de passage figure IV-20. Seules les conditions de passage permettant d'atteindre les états interdits nous intéressent et bien qu'elles soient représentées, les autres conditions de passage peuvent ne pas l'être. Les états incompatibles sont repérés par des hachures.

La démarche consiste alors à déterminer les conditions à rajouter pour chaque transition conduisant à un état interdit. Considérons tout d'abord l'état incompatible "PA-ns/PM-ns". Pour arriver dans cette situation deux hypothèses :

- L'état "PM-ns" est déjà actif, un événement, non défini pour l'instant, est présent : faut-il interdire cette commutation ou provoquer une interaction ? Dans le cas présent, provoquer une interaction n'a aucun sens. En effet, la mise dans un état de marche quelconque peut être dangereuse. Par conséquent, il faut interdire toutes commutations vers cet état. Pour ce faire, nous rajoutons la condition "and not PM-ns" sur tous les arcs dont la source est l'un des modes d'arrêt et la destination l'état "PA-ns". Lorsqu'il n'existe pas d'arc entre ces états, nous en rajoutons un en pointillé avec la condition "( )and not PM-ns" (*figure IV-20*). Les mécanismes d'interdictions sont surlignés par une zone grisée.
- L'état "PA-ns" est déjà actif, un événement, non défini pour l'instant, est présent. Comme pour la situation précédente provoquer une interaction n'a aucun sens. Par conséquent, nous rajoutons la condition "and not PA-ns" sur tous les arcs dont la source est l'un des modes de marche et la destination l'état "PM-ns". De manière similaire, lorsqu'il n'existe pas d'arc entre ces états, nous en rajoutons un en pointillé avec la condition "( ) and not PA-ns" (*figure IV-20*).

Considérons maintenant l'état incompatible "PA-d/PM-ns". Rappelons que l'état "PA-d" signifie que la tranche est arrêtée mais qu'une circulation minimale d'eau doit être maintenue pour assurer le refroidissement des auxiliaires restant en service. Pour atteindre cet état, il est nécessaire que le circuit SRI soit déjà en production et donc qu'un mode de marche ait été sélectionné (ce qui explique son incompatibilité avec cet état). Ceci se traduit donc d'une part, par une interdiction de commuter vers "PA-d" si "PM-ns" est actif (qui correspond à la non-sélection d'un mode de marche). D'autre part, comme pour le cas précédent,

basculer vers l'état "PA-ns" n'ayant aucun sens, une interdiction conditionnelle (en pointillé) de basculer vers "PM-ns" si "PA-d" est actif, est rajoutée.

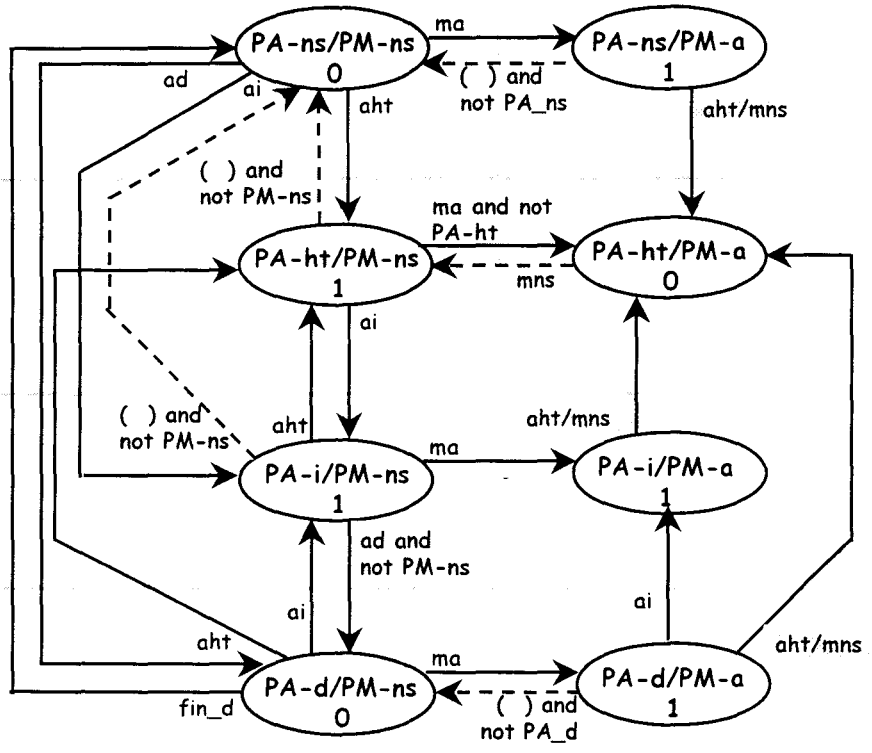


figure IV-20. Traduction des spécifications de la MCM.

Enfin, en ce qui concerne l'état ""PA-ht/PM-a", comme nous l'avons présenté dans le paragraphe 3.2.3, des mécanismes d'interdiction et d'interaction sont mis en œuvres. Les interactions sont surlignées par une zone à damiers.

États	PA-ns	PA-ht	PA-i	PA-d
PA-ns	0	aht/mns	ai/pns,fns	ad
PA-ht		0	ai	
PA-i	ans and not PM_ns	aht/mns	0	ad and not PM_ns and not PF_ns
PA-d	fin-d	aht/mns	ai/pns,fns	0

figure IV-21. Matrice des Conditions de Passage du mode d'arrêt

Tous les ajouts sur les transitions permettent également de compléter la Matrice des Conditions de Passage (*figure IV-21*).

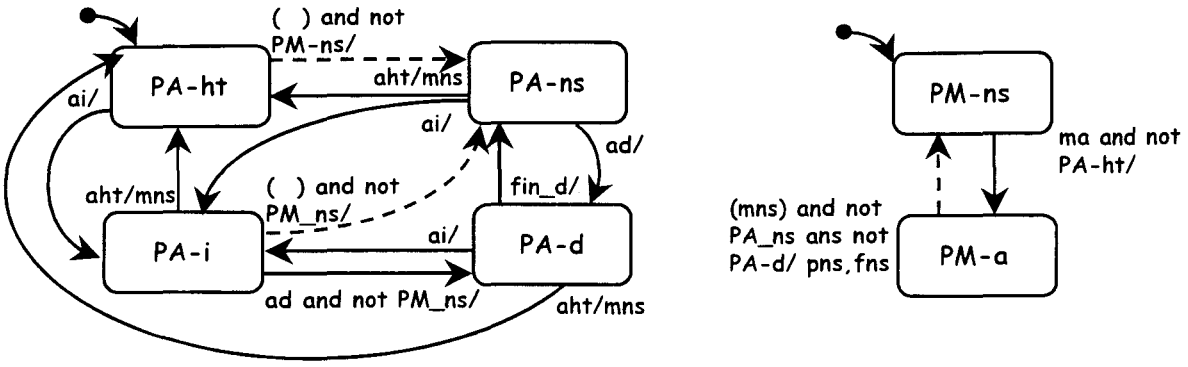


figure IV-22. Report des spécifications.

L'étape suivante consiste à extraire les conditions et arcs ajoutés pour les reporter sur le mode concerné. Dans le cas de notre exemple, une superposition des lignes permet de déterminer les ajouts à répercuter sur le mode de marche alors que les colonnes concernent le mode d'arrêt (*figure IV-22*).

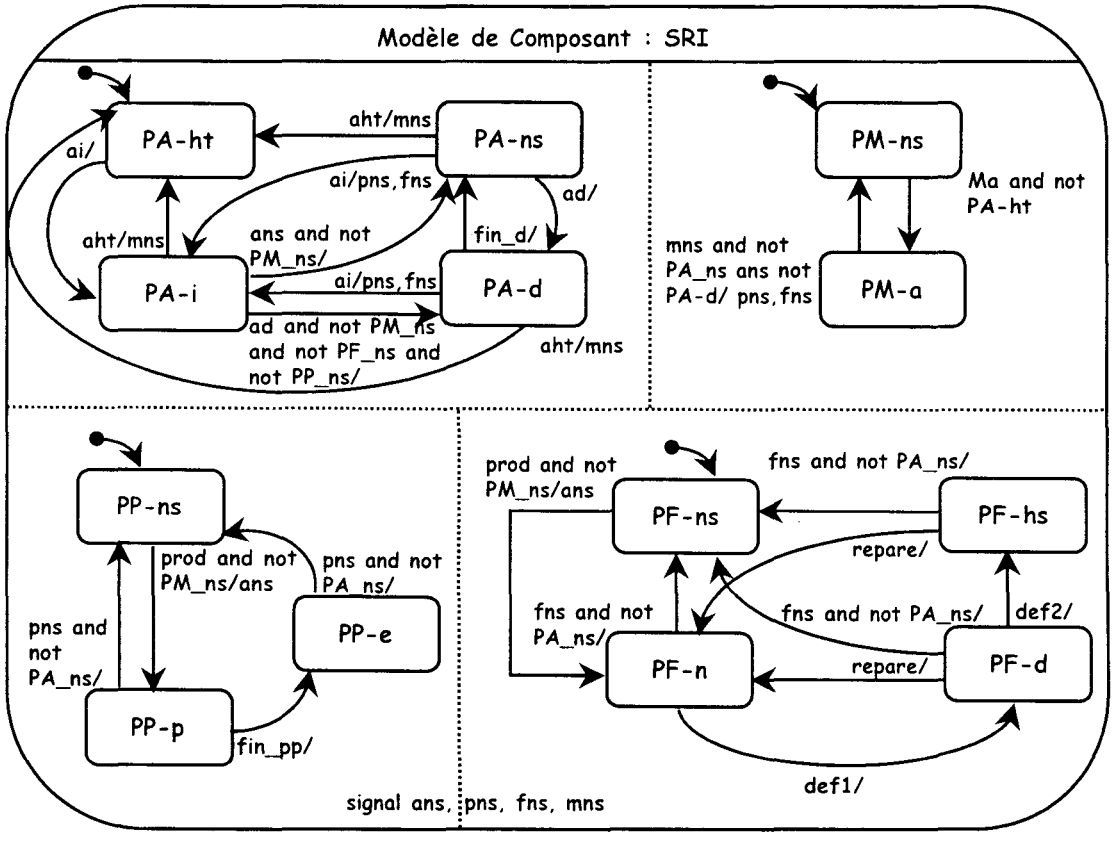


figure IV-23. Modèle de Composant du circuit SRI.

Ces différentes étapes sont à effectuer pour toutes les matrices MCM définies. Enfin une phase de simplification des conditions permet d'obtenir le modèle de composant final (figure IV-23).

Cette étape de simplification consiste à retirer tous les arcs conditionnels (en pointillés) pour lesquels aucun événement ne provoquera la commutation. Considérons la condition de passage du mode d'arrêt de l'état "PA-ns" à "PA-ht". Lors de la spécification de la cohérence des modes nous avons ajouté un arc portant comme condition "( ) and not PM–ns". La spécification de toutes les matrices n'a fait apparaître aucun événement pouvant déclencher une telle commutation. Par conséquent, cet arc est à supprimer sur le modèle final (figure IV-23). Par contre, l'arc condition "( ) and not PM–ns" entre l'état "PA-i" et "PA-ns" reste car un événement ("ans") dû à une interaction avec un autre mode provoque cette commutation. En l'occurrence c'est le passage dans l'état préparatoire du mode production qui provoque ce changement d'état.

3.3 Vérification

Après cette dernière phase de mise en œuvre, il est nécessaire de procéder à une phase de vérification du modèle obtenu. Cette phase est décomposée en deux étapes. La première consiste à vérifier les propriétés de chacun des automates modélisant un mode. La deuxième consiste à vérifier la cohérence comportementale du modèle.

La vérification des propriétés de chacun des modes est effectuée à partir des Matrices des Conditions de Passage. Elle porte principalement sur les états "puits" et sur les états non accessibles.

Elle consiste à vérifier que :

$$\sum_{i=0}^{|m|} MCP^{m}_{(e_i,e_j)} \neq 0 \text{ et } \sum_{j=0}^{|m|} MCP^{m}_{(e_i,e_j)} \neq 0$$

ce qui nous permet de vérifier pour chaque mode qu'il n'y a aucun état puit ni d'état inaccessible.

La vérification de la cohérence comportementale du modèle est réalisée grâce au compilateur Esterel. Elle consiste à vérifier qu'il n'y ait pas de problème de causalité (*Annexe 3*).

CONCLUSION

Nous venons de présenter le Modèle de Composant dont le rôle est de modéliser le comportement d'un composant élémentaire du point de vue de ses modes.

A travers la première partie de ce chapitre, nous avons défini ce que nous entendons par le terme *composant élémentaire* avant de présenter la structure du MdC et une vision globale de sa démarche de conception.

La deuxième partie est consacrée à la démarche de conception du MdC et principalement à l'étude de la cohérence des modes. Nous avons proposé deux mécanismes pour la prise en compte les spécifications imposées par le concepteur à travers la Matrice de Cohérence des Modes.

Enfin, un exemple d'application permet de montrer l'application de la démarche complète sur une famille de mode donnée.

Le Modèle de Composant est directement liée aux fonctions initiales par conséquent, la connaissance de son état permet de déterminer l'état de ces fonctions. Tout comme pour les composants élémentaires, nous proposons de déterminer, dans le chapitre suivant, un Modèle de Fonction qui permet de déterminer l'état d'un sous-système à partir des sous-systèmes de niveaux supérieur et inférieur.

Chapitre V

GESTION DES MODES DES SYSTÈMES DE PRODUCTION

INTRODUCTION

La présentation générale de notre approche, dans le chapitre III (paragraphe 1.3), a mis en avant un certain nombre modèles permettant de caractériser, à différents niveaux et selon différents points de vue, l'état du système. Après avoir détaillé le Modèle de Composant dans le chapitre IV, nous nous intéressons maintenant au Modèle de Fonction ainsi qu'aux interactions entre modèles permettent de gérer les modes d'un Système de Production.

Dans un premier temps, nous proposons quelques extensions concernant l'élaboration du Modèle Fonctionnel de Conception et du Modèle Fonctionnel d'Implémentation Élémentaire (*Annexe 1*). Nous montrons que selon l'objectif du modèle, leur démarche de conception peut être différente. Nous présentons également le rôle et la structure du Modèle de Fonction.

La décomposition hiérarchique et fonctionnelle, obtenue à partir du MFC et MFIE, fait apparaître des sous-systèmes dépendants les uns des autres. L'objectif, de la deuxième partie, est de prendre en compte ces liens de dépendance ainsi que les contraintes spécifiées par le concepteur afin de gérer les modes du système.

1 LE MODÈLE DE FONCTION

Dans le chapitre précédent, nous nous sommes intéressés au Modèle de Composant ; c'est-à-dire à la partie basse du modèle comportemental. Nous présentons maintenant l'élément de modélisation utilisé dans la partie haute du modèle comportemental : le **Modèle de Fonction** (MdF) (*figure V-1*).

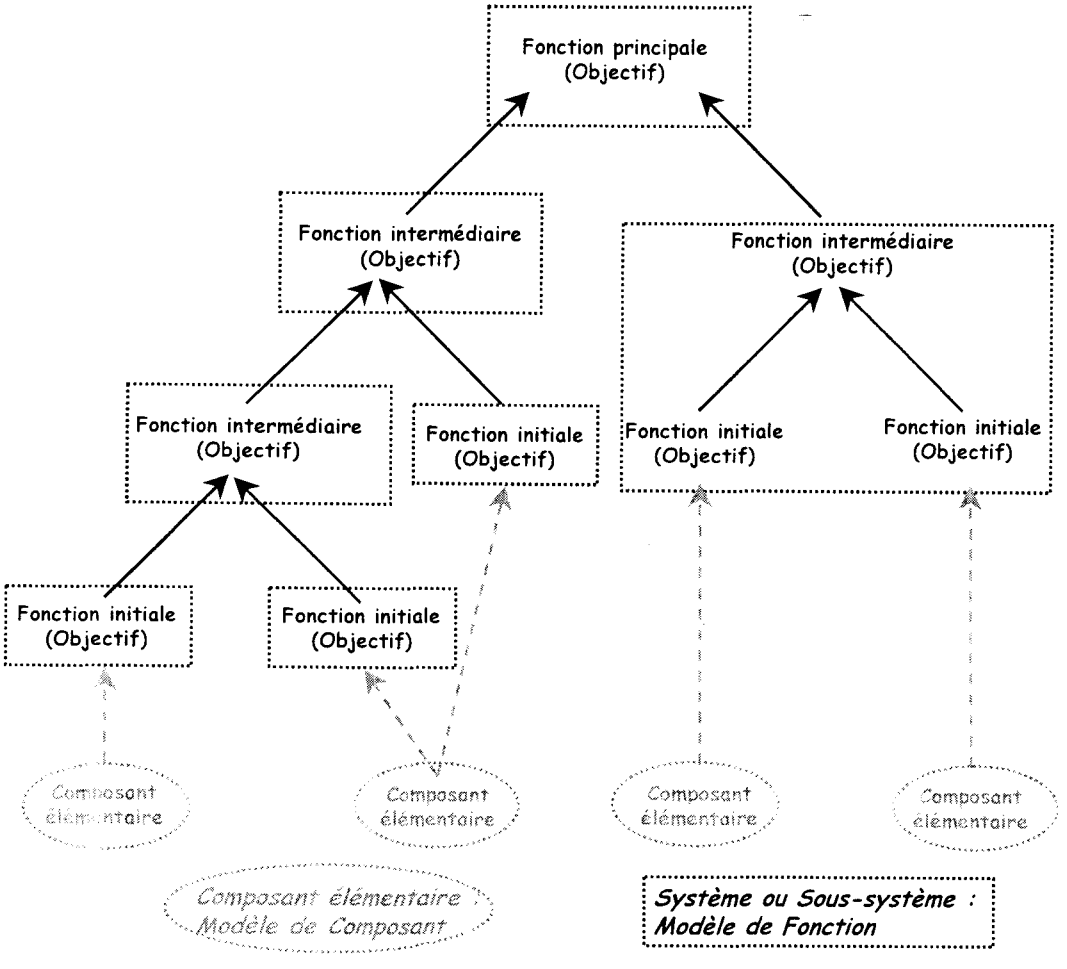


figure V-1. Schéma d'un modèle comportemental.

1.1 Le MFC et le MFIE

1.1.1 Le Modèle Fonctionnel de Conception

L'objectif du Modèle Fonctionnel de Conception (*Annexe 1*) est de permettre au concepteur de spécifier comment les fonctions principales de son système seront obtenues. Sa détermination est guidée par le cahier des charges fonctionnel.

Le résultat est un graphe dont la racine représente la fonction pour lequel le système a été conçu. Pour un même système, il peut exister plusieurs fonctions prinicpales. Les feuilles, quant à elles, représentent les fonctions initiales du système. Pour relier les fonctions initiales à la (les) fonction(s) principale(s), le concepteur établit des liens de dépendance. Il existe principalement deux types de liaison : les liaisons de type alternatives ("OU") et les liaisons de type nécessité ("ET").

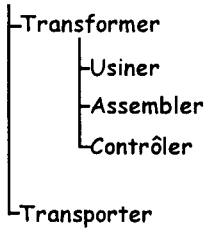


figure V-2. Classification des fonctions pour les SFPM.

Notre méthode de modélisation, orientée objectif de production, nous a conduit à modifier la démarche de conception d'un tel modèle. En effet, initialement, le principe de conception consiste à déterminer la ou (les) fonction(s) principale(s) puis de lister les fonctions nécessaires pour les obtenir. La décomposition se fait selon une classification qui porte sur la nature de la fonction (*figure V-2*).

Notre objectif est un peu différent. Il ne s'agit pas seulement de déterminer les fonctions nécessaires permettant de délivrer la fonction principale mais à définir des sous-systèmes autonomes dont l'interaction entre eux permet d'atteindre les objectifs de production fixés. Contrairement à la démarche initiale de conception du MFC, la décomposition ne se fait pas selon une classification de fonction mais selon les objectifs de production. Pour chaque objectif principal, tous les sous-objectifs (les fonctions) nécessaires, sont

définis. Le processus est réitéré jusqu'à la détermination des fonctions initiales. Cette démarche est également guidée par le CdCF.

Illustration : Considérons le cas d'un Système de Production quelconque dont la fonction principale est de fabriquer un produit P à partir de deux produits P1 et P2. La figure V-3(A) représente le MFC selon la démarche initiale et la figure V-3(B) représente le MFC selon notre démarche de conception. Les fonctions en italiques représentent les fonctions initiales. Rappelons que le symbole "+" traduit une liaison de type alternative (*Annexe 1*).

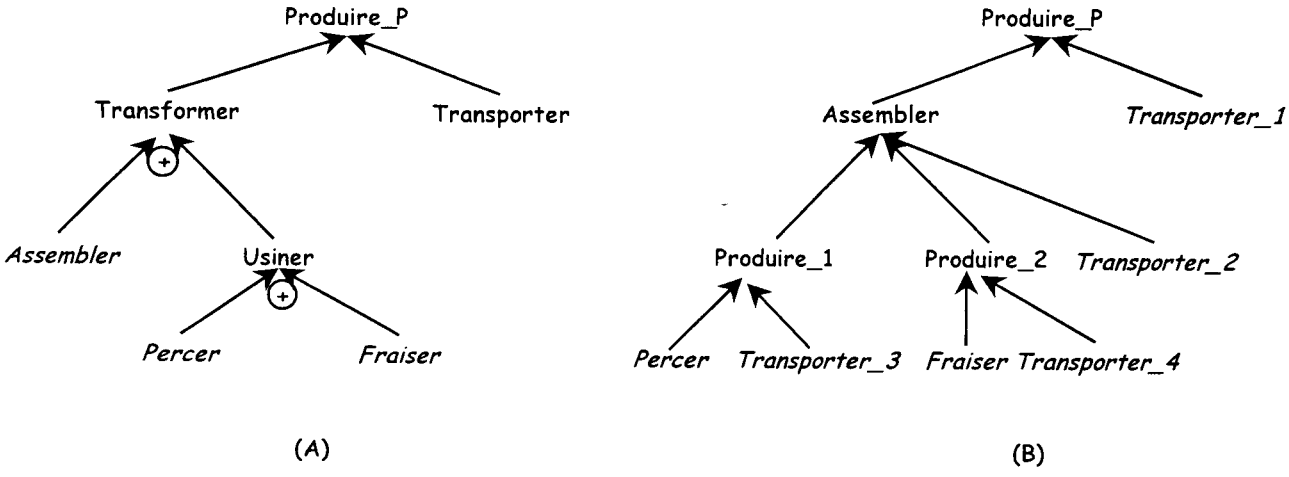


figure V-3. Comparaison des démarches de conception du MFC.

Nous pouvons remarquer que notre démarche de conception permet, notamment, d'exprimer certaines contraintes. Par exemple, dans l'illustration proposée, notre démarche met en avant qu'il faut absolument produire une pièce P1, une pièce P2 et disposer d'une fonction "Assembler" et des transferts nécessaires pour pouvoir réaliser l'assemblage. Ceci n'est pas pris en compte dans la démarche initiale.

A chaque niveau, le concepteur doit identifier les fonctions nécessaires à la réalisation de la fonction de niveau supérieur. En ce qui concerne les fonctions de transport, à ce stade de l'analyse, elles ne peuvent pas être affinées sans prendre en compte les ressources matérielles. Le rôle du MFIE est justement de spécifier les ressources en charge de la réalisation des fonctions.

1.1.2 Le Modèle Fonctionnel d'Implantation Élémentaire

Le Modèle Fonctionnel d'Implantation Élémentaire permet d'affiner les fonctions initiales en tenant compte de la structure du système. Il repose sur le concept d'opération. Compte tenu des ressources choisies par le concepteur, chacune des fonctions initiales peut être déclinée en une ou plusieurs opérations. Cela dépend de la flexibilité du système.

Initialement, le concept d'opération désigne une fonction réalisée sur un produit par une ressource. Compte tenu de notre domaine d'application, les systèmes continus et discrets, nous proposons d'étendre le concept d'opération. Nous considérons qu'une opération est une fonction réalisée sur un produit, quelle que soit sa nature, par une ressource **ou un ensemble de ressources** intervenant simultanément.

Le choix des ressources matérielles permet également d'affiner les fonctions de transport. Ce qui nous intéresse c'est de savoir quels sont les transferts qui interviennent dans la réalisation de chacun des sous-systèmes fonctionnels. Plus précisément, nous nous intéressons aux transferts entre Lieux Caractéristiques Fondamentaux (Chapitre III, §.1.2.1). Rappelons que notre objectif est de savoir si nous pouvons atteindre les objectifs de production. Les LCF sont alors suffisant dans notre cas.

Là encore, notre objectif n'est pas seulement de lister les LCF nécessaires, mais de les déterminer par rapport aux objectifs de production.

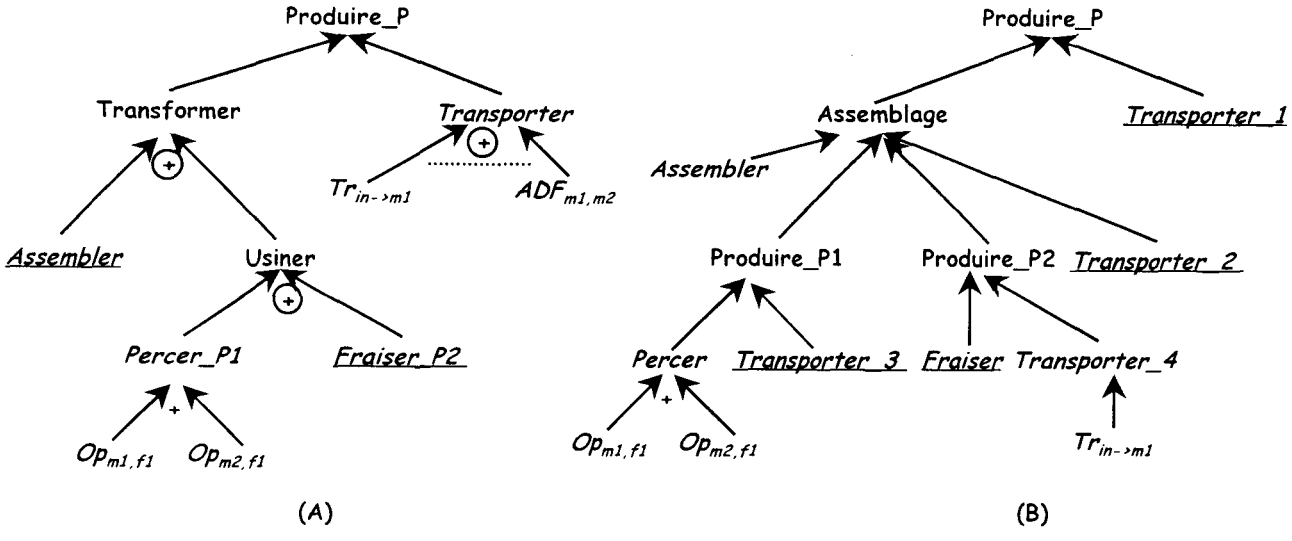


figure V-4. Comparaison des démarches de conception du MFIE.

Illustration : Si nous reprenons l'exemple précédent, nous obtenons la figure V-4(A) pour le MFIE selon la démarche initiale et la figure V-4 (B) pour le MFIE selon notre démarche de conception. Les fonctions soulignées correspondent aux fonctions non complètement développées sur le modèle.

1.1.3 Exemple d'application

Pour illustrer l'élaboration de ces modèles, nous reprenons le SRI dont une partie du cahier des charges fonctionnels a déjà été présentée (Chapitre III, §.2.3). Nous compèterons ce dernier au fur et à mesure.

Le Modèle Fonctionnel de Conception

La première étape de la conception du MFC consiste à déterminer la (ou les) fonction(s) principale(s) du système. Dans l'exemple du SRI, la fonction principale est de réfrigérer les auxiliaires de la partie conventionnelle d'une centrale nucléaire. Nous appelons cette fonction "**Réfrigérer_Aux**". Le MFC doit alors expliciter les liens de dépendance causale entre la fonction "**Réfrigérer_Aux**" et les fonctions initiales du système. Démarrant de la fonction principale, le concepteur va se demander quelles sont les fonctions nécessaires à la mise en œuvre de "**Réfrigérer_Aux**". La réponse à cette question va l'amener à déterminer que cette fonction nécessite de mettre en circulation l'eau déminéralisée (fonction "**Circuler_Dem**") et de conduire l'eau déminéralisée jusqu'aux échangeurs auxiliaires (fonction "**Conduire_1**"). De la même manière, on va étudier comment mettre en œuvre la fonction "**Circuler_Dem**". Pour cela, il faut alimenter le circuit en eau déminéralisée (fonction "**Alimenter_Dem**") et il faut vaincre les pertes de charges par le pompage de cette eau (fonction "**Pomper_Dem**"). La décomposition successive des fonctions non initiales conduit à l'élaboration du MFC. L'affinement de celui-ci est fait en étudiant les conditions de fonctionnement du système décrit par le CdCF.

Par exemple, considérons la fonction "**Pomper_1**". Selon la situation de la tranche, ces caractéristiques peuvent être différentes. Il existe en réalité trois variantes de cette fonction qui dépendent de la saison et des contraintes de production. Nous appelons ces fonctions "**Pomper_11**", "**Pomper_12**", "**Pomper_13**". La fonction "**Pomper_12**" est la plus courante. En outre, en cas de défaillance totale du système de pompage du SRI, le circuit est reconfiguré en "boucle ouverte" (l'eau déminéralisée chauffée est jetée à l'égout). Dans ce

contexte, la mise en circulation de l'eau déminéralisée est momentanément assurée par la bâche d'appoint (fonction "**Stocker_Dem**"). Elle permet ainsi la poursuite de la réfrigération du circuit pendant un certain temps. Ceci se traduit sur le modèle par une liaison de type "OU" entre les fonctions "**Pomper_Dem**" et " **Stocker_Dem**". Ceci est un exemple d'affinement du MFC.

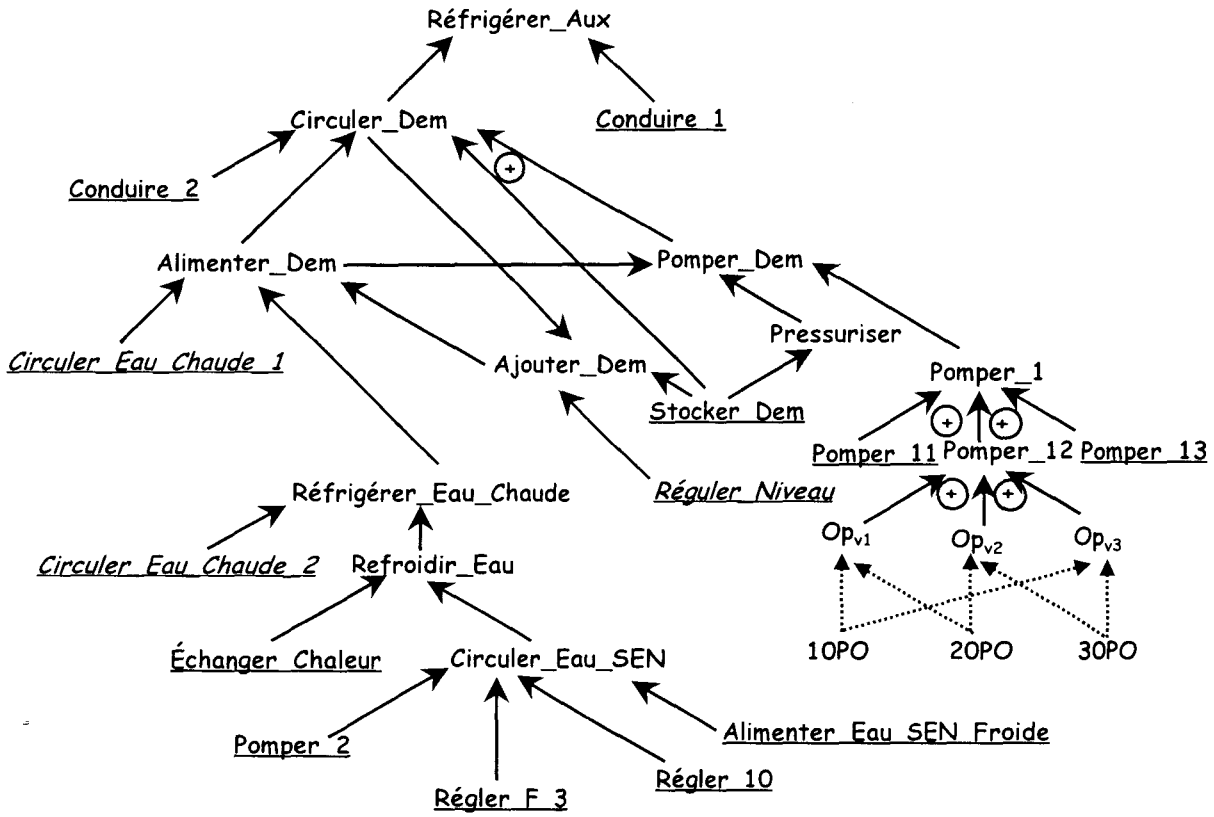


figure V-5. Extrait du Graphe Fonctionnel du SRI

Le Modèle Fonctionnel d'Implantation Élémentaire

Une fois le MFC définit, nous pouvons nous attacher à déterminer le MFIE. Pour des raisons de clarté prenons uniquement l'exemple de la fonction "**Pomper_12**". Le système possède trois pompes identiques (appelées 10PO, 20PO, 30PO). Pour répondre aux exigences de la fonction "**Pomper_12**" (et du CdCF) il est nécessaire de mettre deux pompes en service. Dans ce cas présent, nous pouvons donc dire qu'il y a trois opérations possibles pour délivrer la fonction "**Pomper_12**". Ceci se traduit sur le modèle par une liaison de type "OU" entre les opérations "Op_{v21}", "Op_{v22}", "Op_{v23}". Les fonctions "**Pomper_11**" et "**Pomper_13**" correspondent respectivement à l'utilisation d'une pompe sur les trois et à l'utilisation des trois pompes.

Un extrait du modèle fonctionnel, résultant de l'élaboration du MFC et MFIE, est présenté par la figure V-5. Les fonctions soulignées correspondent aux fonctions non complètement développées sur le modèle.

1.2 Présentation du Modèle de Fonction

1.2.1 Son rôle

Dans une approche où l'un des objectifs est de pouvoir assurer, en présence d'une défaillance, la continuité du service (Chapitre I, §.2.4.5), il est nécessaire de connaître l'état de **disponibilité** de chacune des fonctions du système. Rappelons que la disponibilité et la sécurité sont principalement au centre des préoccupations de nos travaux (Chapitre I, §.2.3.5).

Plus particulièrement, dans le cas d'une défaillance, il est également nécessaire de connaître les **alternatives** possibles afin de continuer à délivrer un service. Ces alternatives peuvent ne pas être optimales mais acceptables par rapport aux objectifs de production. La notion "d'acceptable" dépend alors d'un certain nombre de critères que peut être le temps, la qualité, ...et également de **l'état** du système ou du sous-système. Nous définissons un système ou sous-système fonctionnel comme une fonction ou un ensemble de fonctions qui délivre le même service.

Remarque : par abus de langage, nous utilisons indifféremment le terme sous-système fonctionnel et le terme fonction.

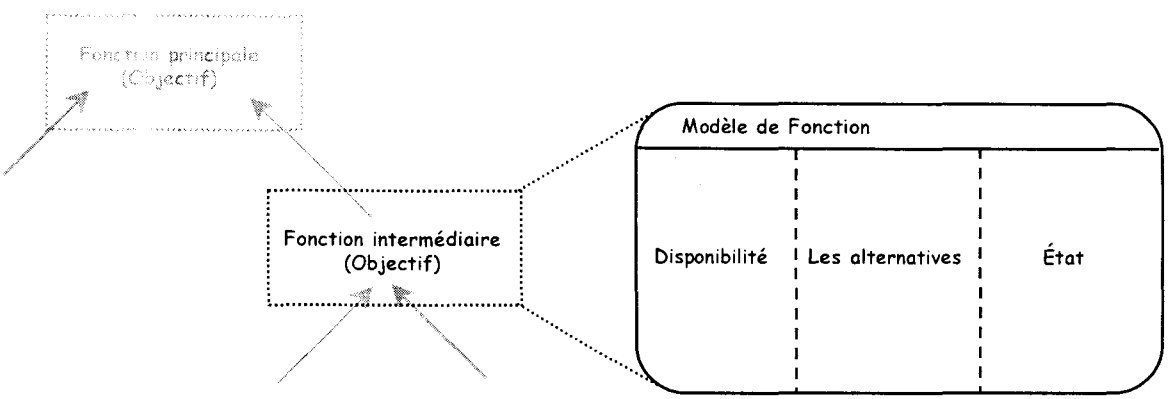


figure V-6. Modèle de Fonction d'un sous-système.

Dans la méthode que nous proposons, nous avons choisi de répondre à ces besoins (informations sur la disponibilité, les alternatives possibles et l'état du système) en procédant à un découpage en sous-systèmes fonctionnels. Un

modèle, appelé Modèle de Fonction (*figure V-6*), est associé à chaque nœud de la structure hiérarchique représentant un système ou un sous-système fonctionnel.

Le Modèle de Fonction permet de spécifier le comportement "interne" d'un système ou d'un sous-système fonctionnel. D'une part, ce modèle nous informe sur la disponibilité du système ou sous-système fonctionnel considéré. D'autre part, il prend en compte certaines flexibilités du système afin de modéliser les différentes possibilités (les alternatives) permettant de délivrer les fonctionnalités du système ou sous-système considéré et il renseigne sur son état.

La connaissance "locale" (sous-système) permet à l'opérateur de conduite d'appréhender en permanence la connaissance sur l'état de son installation quel que soit le niveau d'abstraction. Les flux d'informations, ascendants ou descendants, échangés entre les Modèles de Fonctions des différents niveaux permet de déterminer l'état du système global.

L'ensemble de ces caractéristiques permet, d'une part, à la fonction de Gestion des Modes de gérer les modes du système étudié et d'autre part de répondre aux besoins des différents intervenants du contrôle-commande (Chapitre II, §.2.3.3).

1.2.2 Flexibilités prises en compte

Les alternatives possibles, lors de la présence d'une défaillance, sont dues aux flexibilités présentes dans le système. En effet, s'il n'existe aucune flexibilité dans le système, la seule solution, dans le cas d'une défaillance, est alors de faire intervenir la maintenance corrective (Chapitre I, §.3.5.1). Pour éviter cela, la présence de flexibilités dans le système est nécessaire (Chapitre I, §.1.5).

Nous avons vu qu'il existe un grand nombre de flexibilités (Chapitre I, §.1.3). Toutes ne sont pas prises en compte par la fonction de Gestion des Modes. Nous proposons de regrouper les flexibilités considérées par la fonction de Gestion des Modes en deux grandes familles : les redondances fonctionnelles et les redondances structurelles.

Les **redondances fonctionnelles** concernent les systèmes fonctionnels (fonctions) qui peuvent être implémentées de différentes façons d'un point de vue fonctionnel.

Ce type de flexibilité est principalement lié à l'existence de différents contextes d'utilisation selon lesquels les caractéristiques du service délivré par le système ou sous-système sont différentes.

Illustration : Considérons à nouveau le circuit SRI. Nous avons vu que la fonction "**Circuler_Dem**" est obtenue à partir de la fonction "**Pomper_Dem**". En cas de défaillance totale du système de pompage du SRI, la mise en circulation de l'eau déminéralisée est momentanément assurée par la bâche d'appoint (fonction "**Stocker_Dem**"). Nous pouvons donc dire qu'il existe deux contextes d'utilisation pour la fonction "**Circuler_Dem**".

Définitions 12 : *Redondance fonctionnelle [Dan, 00/a]*

Il y a redondance fonctionnelle si une même fonction peut délivrer un service *différent* (caractéristiques différentes) selon le contexte d'utilisation.

Dans le cas de la redondance fonctionnelle, nous appelons chaque façon de délivrer la fonction une **configuration**.

Définitions 13 : *Configuration de fonction [Dan, 00/b]*

Une configuration d'une fonction correspond à une façon de délivrer cette fonction selon des caractéristiques données. Une fonction possède une ou plusieurs configurations. La commutation d'une configuration à une autre peut-être automatique ou manuelle selon les spécifications du concepteur.

Illustration : Dans le cas du système de pompage, la fonction associée est une fonction "Pomper". Étant donné l'existence des deux contextes d'utilisation, la fonction "Pomper" est constituée de deux configurations correspondant au contexte "Été" et au contexte "Hiver".

La **redondance structurelle** concerne les systèmes fonctionnels (fonctions) qui peuvent être mis en œuvre de différentes façons d'un point de vue structurel. Elle correspond à des situations où plusieurs composants élémentaires, délivrant le même service, peuvent être utiliser indifféremment pour implémenter un même service.

Définitions 14 : *Redondance structurelle [Dan, 00/a]*

Il y a redondance structurelle si plusieurs composants peuvent être utilisés pour mettre en œuvre une même fonction.

Dans le cas de redondance structurelle, nous appelons chaque façon de mettre en œuvre la fonction une **version**.

Définitions 15 : *Version de fonction [Dan, 99/a]*

Une version de fonction décrit une séquence de sollicitation des ressources afin de réaliser cette fonction. Toutes les ressources d'une version sont sollicitées.

Illustration : Considérons que, dans le cas du système de pompage, il existe trois pompes identiques qui peuvent délivrer le service de pompage lorsque la configuration "Été" est sélectionnée. Il existe alors trois versions de la fonction "Pomper" dans la configuration "Été".

1.3 Sa représentation

De manière analogue au Modèle de Composant (Chapitre IV), le formalisme des SyncCharts est utilisé pour la représentation du Modèle de Fonction. Ce dernier est représenté par un macro-état constitué de trois constellations (*Annexe 3*). Chacune d'entre-elles représente soit la disponibilité du sous-système fonctionnel, soit le contexte d'utilisation (les configurations) ou soit l'état du sous-système considéré au sens des modes tels que nous les avons définis dans les chapitres précédents.

1.3.1 La disponibilité

A chaque instant, la disponibilité d'une fonction est modélisée par deux états : "Disponible" et "Indisponible" (*figure V-7*).

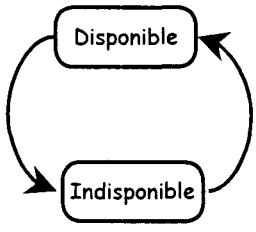


figure V-7. Disponibilité d'une fonction

L'activation du premier état signifie que le sous-système est prêt à fonctionner ou qu'il est opérationnel à cet instant donné. L'activation du second état indique que le sous-système fonctionnel n'est pas opérationnel à cet instant précis.

La disponibilité d'une fonction dépend de la disponibilité des configurations de cette fonction et par conséquent de la disponibilité de leurs versions.

Définitions 16 *: Disponibilité d'une fonction [Dan, 00/d]*

Une fonction est disponible *si et seulement si au moins* une configuration est disponible.

Remarque : Étant donné que la disponibilité d'une fonction dépend de la disponibilité de ses configurations, les états "Disponible" et "Indisponible" ne sont pas obligatoires dans le Modèle de Fonction. En effet, seule la connaissance de la disponibilité des configurations et de leurs versions est nécessaire pour en déduire celle de la fonction. Cependant, ces états permettent aux différents intervenants (opérateurs de conduite, recouvrement,...) de connaître rapidement l'état de disponibilité d'une fonction.

1.3.2 Les configurations et les versions

La seconde composante du Modèle de Fonction représente les différentes configurations possibles (et leurs versions) pour le système considéré.

Elle est composée au moins d'un état et au plus d'autant d'états que de configurations existantes. Vient s'ajouter à cela un état spécifique appelé l'état "C_Out". Cet état spécifique représente le fait qu'aucune configuration peut être exécutée. Atteindre cet état spécifique rend la fonction indisponible ; ceci entraîne la commutation de l'état "Disponible" vers l'état "Indisponible".

L'ensemble des configurations d'une fonction "F" est défini par :

$$Conf(F) = \{C_out\} \cup \{Conf_{i \in \{1..N_F\}}\} \Big/ \begin{array}{l} F \text{ est une fonction} \\ Conf_i \text{ est la configuration } i \text{ de la fonction } F \\ N_F \text{ est le nombre de configurations existantes pour } F \end{array}$$

L'activation de l'une des configurations est possible grâce à un sélecteur "S" qui permet à l'opérateur de choisir une configuration (*Annexe 2*). Le changement de configuration peut être automatique ou manuel selon les spécifications du concepteur. Les commutations entre configurations se représentent par des transitions.

Définitions 17 *: Disponibilité d'une configuration [Dan, 00/d]*

Une configuration est disponible *si et seulement si au moins* une version est disponible.

De manière similaire, dans le cas de redondance structurelle, une configuration contient au moins un état et au plus autant d'états que de versions possibles pour cette configuration. Vient s'ajouter à cela un état spécifique appelé l'état "V_Out$_i$". Cet état spécifique représente le fait qu'aucune version peut être exécutée dans la configuration *i*. Atteindre cet état spécifique rend la configuration indisponible. Par ailleurs, s'il n'y a plus de configuration disponible alors il y a commutation vers l'état "C_Out".

L'ensemble des versions d'une configuration *i* est défini par :

$$Conf_i = \{V_out_i\} \cup \{V_{ij}\} / j \in \{1..M_i\} \left| \begin{array}{l} M_i \text{ est le nombre de versions de la configuration } i \\ V_{ij} \text{ est la version } j \text{ de la configuration } i \end{array} \right.$$

Tout comme pour les configurations, le changement de versions peut être automatique ou manuel selon les spécifications du concepteur. Les commutations entre versions se représentent par des transitions.

Nous avons vu qu'une version est définie comme une séquence de sollicitation des ressources (*Définition 15*).

Une version *ij* d'une configuration *i* est alors définie par :

$$V_{ij} = \{Out_{ijj}\} \cup \{S_{ijl}\} / l \in \{1..K_{ij}\} \left| \begin{array}{l} K_{ij} \text{ est le nombre d'états de la version j de la configuration i} \\ S_{ijl} \text{ est l'état l de la version j de la configuration i} \end{array} \right.$$

Nous pouvons dire que les configurations et les versions représentent des alternatives. Une configuration est la traduction d'une alternative entre fonctions alors qu'une version correspond à une alternative entre une fonction

et des opérations. Leur détermination est alors directement possible à partir du MFIE.

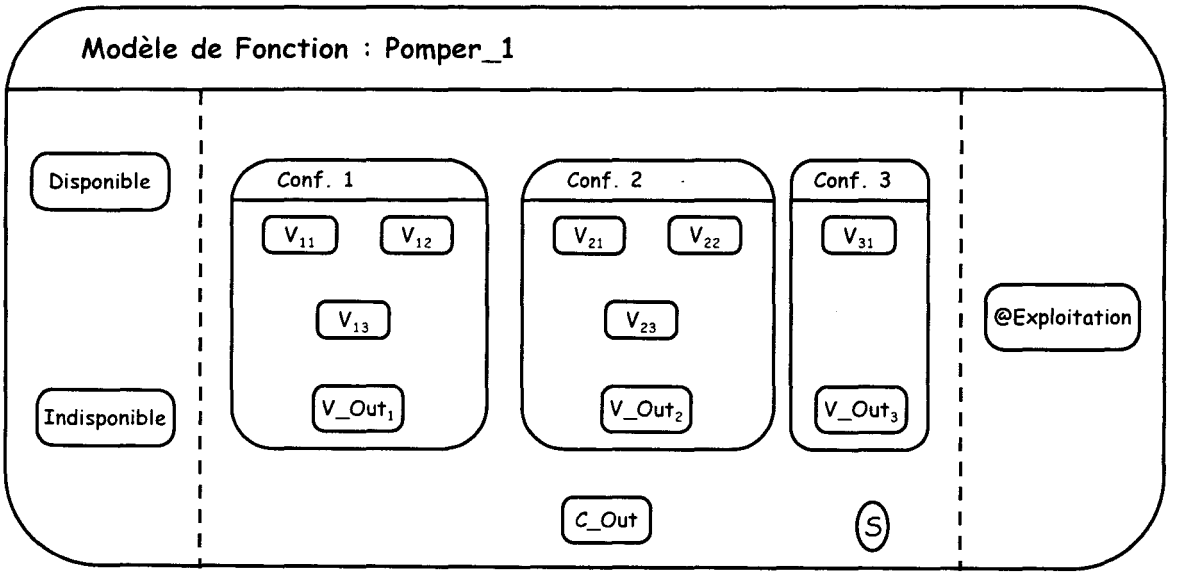


figure V-8. Modèle de Fonction de "Pomper_1"

Illustration : Les fonctions "Pomper_11", "Pomper_12" et "Pomper_13" de la figure V-5 représentent trois variantes de la fonction "Pomper_1" qui dépendent de la saison et des contraintes de production. Elles correspondent donc à trois configurations possibles (respectivement "Conf.1", "Conf.2" et "Conf.3") de délivrer la fonction "Pomper_1".

Le modèle de la figure V-5 fait également apparaître qu'il existe, pour la configuration correspondant à la fonction "Pomper_12" (i.e. "Conf.2"), trois opérations possibles ("Op_{v21}", "Op_{v22}" et "Op_{v23}") ; il existe donc trois versions possibles "v_{21}", "v_{22}", "v_{23}". Chacune de ces versions correspond au démarrage et l'arrêt des pompes adéquates (*figure V-9*). Cette flexibilité d'affectation des ressources est possible grâce à l'existence des trois pompes identiques.

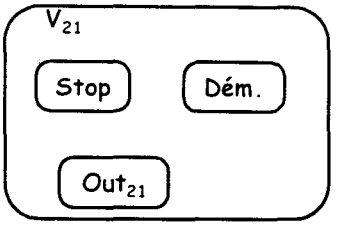


figure V-9. Version v_{21} de la configuration 2 de la fonction "Pomper_1".

Le Modèle de Fonction correspondant au sous-système "Pomper_1" est donné par la figure V-8. Pour plus de clarté, les transitions ne sont pas représentées et la partie exploitation n'est pas développée.

1.3.3 Son comportement

Nous avons vu dans le chapitre III que le comportement des Systèmes de Production est décrit en utilisant la notion de *mode*. Nous avons également proposé une démarche (Chapitre III, §.2.2.2) qui permet de déterminer les modes et familles de modes retenus pour décrire le comportement d'un Système de Production.

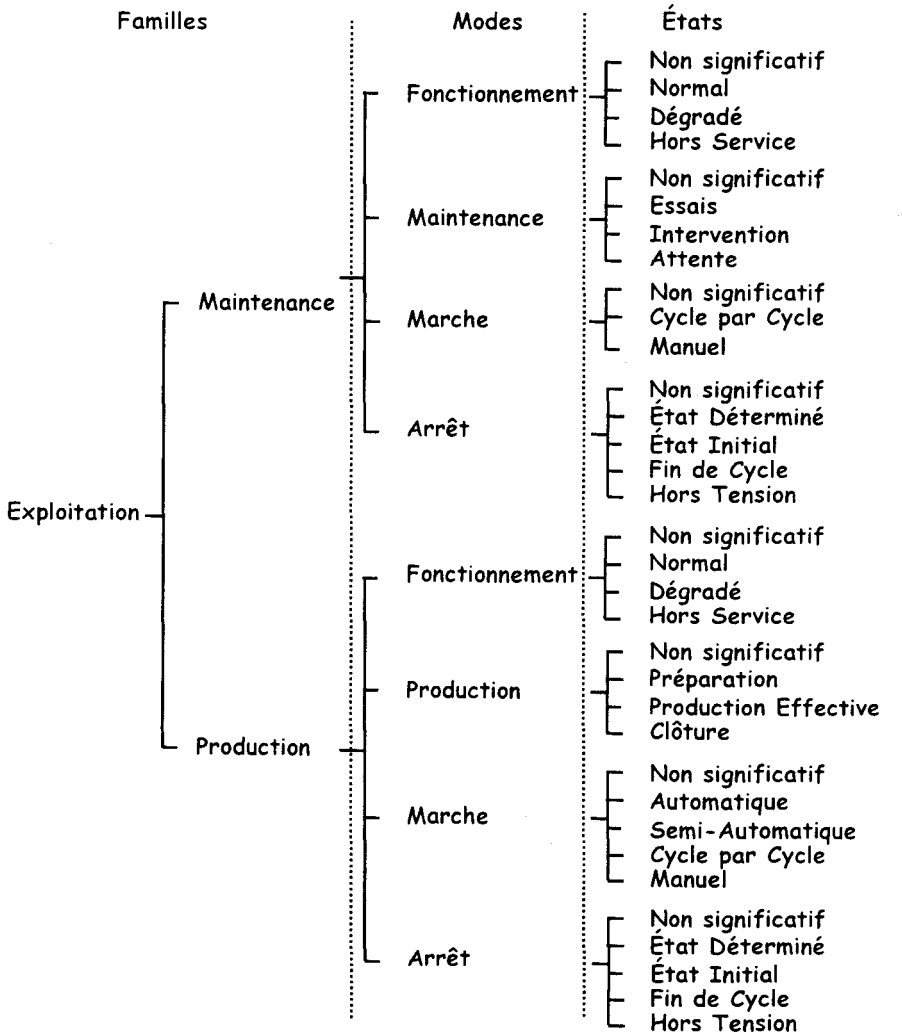


figure V-10. Les familles du mode d'exploitation.

La démarche proposée permet de déterminer les modes d'un Système de Production tout en tenant compte des objectifs de la Gestion des Modes. Ils permettent notamment, à chaque intervenant, d'obtenir les informations sur le

système dont il a besoin. Nous avons, par la suite, appliqué cette démarche à notre contexte de travail ce qui nous a permis de déterminer un ensemble générique de familles et de modes (*figure V-10*). Rappelons que la liste des états à prendre en compte dépend du système étudié.

Nous avons déjà utilisé cette liste de familles de modes et de modes pour représenter le comportement des composants élémentaires constituant le système. Nous proposons ici d'utiliser le même principe pour représenter le comportement des sous-systèmes fonctionnels.

La troisième composante du Modèle de Fonction est constituée par les mêmes constellations que le Modèle de Composant.

2 MODÈLE COMPORTEMENTAL POUR LA GESTION DES MODES DES SP.

2.1 Proposition

Nous avons vu que l'un des rôles du Modèle de Fonction est de modéliser le comportement "interne" d'une fonction. Pour ce faire, il est notamment constitué des mêmes constellations (états) que le Modèle de Composant. Les différentes familles de modes et les modes retenus permettent de modéliser le comportement d'une fonction selon plusieurs points de vue. Rappelons que l'un des objectifs finaux est de pouvoir caractériser l'état de chaque sous-système (vision locale) et du système (vision globale) (Chapitre II, §.2.3.3).

L'état de chaque fonction intermédiaire a une influence sur les fonctions de niveaux inférieurs et sur celle du niveau supérieur. Au niveau le plus bas, des interactions ont lieu entre les fonctions initiales et les composants élémentaires. Ces échanges sont bidirectionnels. L'occurrence d'une défaillance sur un composant élémentaire a forcément une influence sur l'état de la fonction initiale qu'il délivre. Inversement, la sélection d'une configuration et d'une version entraîne la sollicitation d'un composant élémentaire qui contribue à sa réalisation.

La modélisation fonctionnelle utilisée, à travers le MFC et le MFIE, nous a permis après quelques modifications concernant la démarche de conception, de déterminer des sous-systèmes liés par des relations de dépendance. Elle met

en avant deux types de liaison ; les liaisons de type nécessité et celles de type alternative. Ces liaisons vont nous permettre une première évaluation de l'état de chacun des sous-systèmes et du système.

Nous proposons ensuite de déterminer l'état d'une fonction, d'une part, selon la nature de la liaison et également selon le point de vue adopté et selon le contexte. Dans le cadre de ces travaux, les points de vue retenus sont le point de vue *production* et le point de vue *maintenance* (Chapitre III, §.2.2.3).

Rappelons que d'un point de vue production, l'objectif est de pouvoir atteindre les objectifs fixés ; "peu importe" les moyens utilisés. En revanche, l'objectif du point de vue de la maintenance est d'assurer le bon fonctionnement du système. Un changement d'état peut alors ne pas avoir les mêmes conséquences du point de vue production et du point de vue maintenance.

Illustration : Considérons le système de pompage décrit précédemment par la fonction "Pomper_1". Nous avons vu que, dans la configuration 2, cette fonction de pompage peut être implémentée de trois façons différentes (trois opérations). Considérons que la version v_{21} est active et qu'une défaillance apparaisse sur l'une des pompes utilisées dans cette version (état hors service). D'un point de vue production, cela peut n'avoir aucune influence sur l'état de la fonction pomper si un changement de version est effectué. Le système de pompage sera toujours considéré comme dans un état de fonctionnement normal ; les objectifs fixés continuent d'être atteints mais d'une façon différente. Par contre d'un point de maintenance, qu'il y ait changement de version ou pas, la fonction pomper sera considérée comme en fonctionnement dégradé. Elle peut continuer à délivrer son service, par contre, il y a eu perte d'une fonctionnalité. La maintenance en est avertie ce qui lui permet d'intervenir avant que le système de pompage ne soit complètement hors service.

Nous proposons dans un premier temps de déterminer l'influence des liens sur le comportement des fonctions. Par la suite, nous nous intéressons à l'influence du contexte sur l'état des fonctions.

Les propositions faites par la suite concernent uniquement la famille des modes de fonctionnement. Bien qu'il soit possible de tenir un raisonnement similaire pour les autres familles de modes, nous considérons qu'il peut exister

différentes règles de calcul d'état selon la nature du système, les objectifs fixés (respect de la sécurité, qualité,...) et le concepteur, pour proposer une solution valable quel que soit le système.

La première évaluation, selon la nature des liaisons, et la prise en compte du contexte et des points de vue vont nous permettre de déterminer l'état de chacun des sous-systèmes et du système global du point de vue des modes de fonctionnement.

2.2 Liens de dépendance, points de vue et contexte

2.2.1 Liaison de type nécessité

Les liaisons de type nécessité ("ET") modélisent l'obligation que chacune des sous-fonctions soit opérationnelle pour la mise en œuvre de la fonction mère.

ET		S1		
		N	D	HS
S2	N	N	D	HS
	D	D	D	HS
	HS	HS	HS	HS

figure V-11.Calcul d'état dans le cas du "ET"

Dans ce cas, lorsqu'une des sous-fonctions change d'états cela influe obligatoirement sur l'état de la fonction mère (*figure V-11*). Nous considérons qu'il suffit qu'une seule fonction ou composant se trouve dans l'état dégradé ou hors service pour estimer la fonction mère dans l'état dégradé ou hors service. Les autres sous-fonctions ne sont par contre pas affectées par ce changement d'état.

Illustration : Considérons l'exemple du SRI pour illustrer nos propos. La figure V-12 représente un extrait de son modèle fonctionnel.

Nous nous intéressons plus particulièrement à la fonction "Pomper_1". Afin de simplifier le modèle, seules sont représentées les parties configuration et modes de fonctionnement d'un point de vue production et d'un point de vue maintenance dans les Modèles de Fonction.

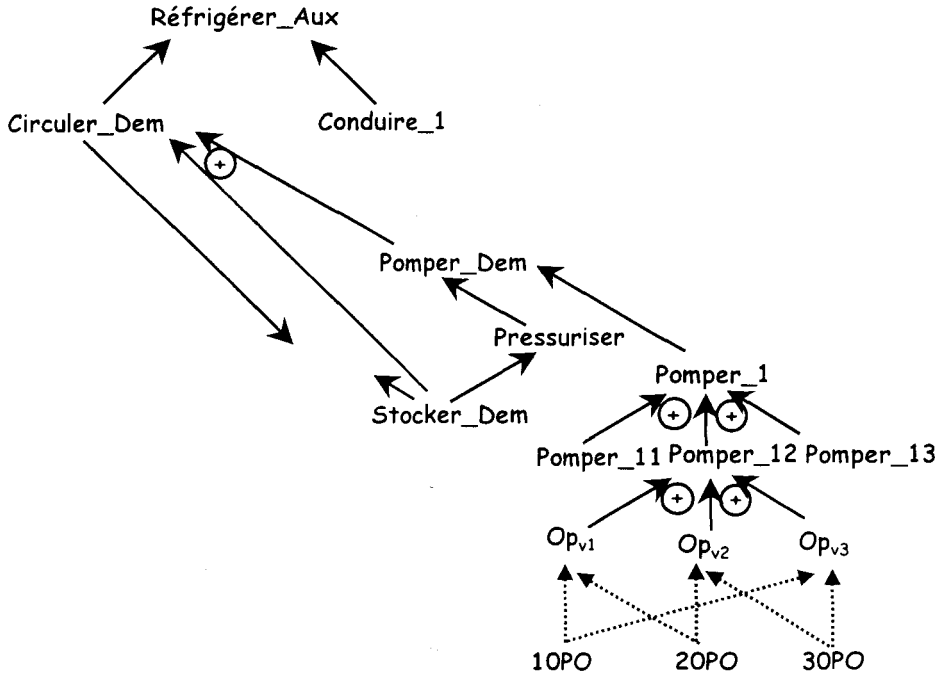


figure V-12. Extrait du Graphe Fonctionnel du SRI

D'après le modèle fonctionnel de la figure V-12, il existe trois variantes de la fonction "Pomper_1" ; ceci est représenté par les trois configurations (Conf.1, Conf.2 et Conf.3) sur la figure V-13.

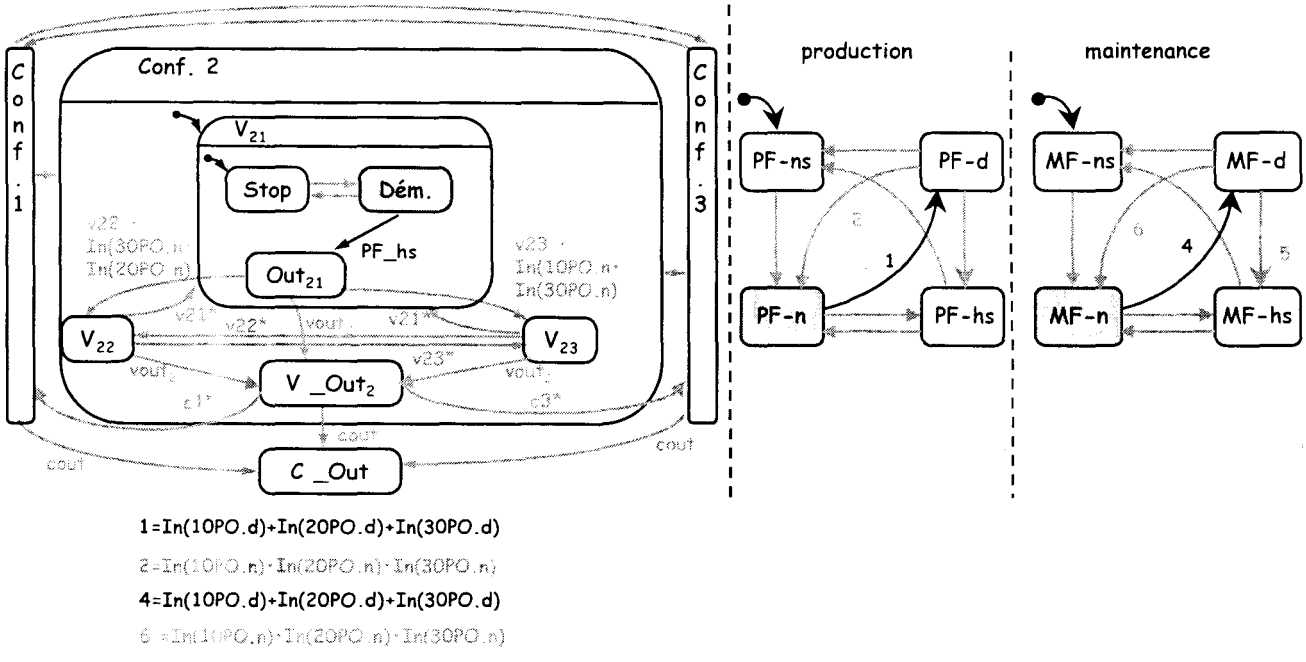


figure V-13. Modèle de Fonction de "Pomper_1" dans la situation initiale

Rappelons que dans la configuration "Conf.1", le service délivré correspond à celui délivré par une pompe. Étant donné que le SRI dispose de trois pompes

identiques (10PO, 20PO, 30PO) pour implémenter cette fonction, il existe trois versions dans cette configuration. La configuration "Conf.2" correspond à l'utilisation de deux pompes. Là aussi, il existe trois versions dans cette configuration qui correspondent à l'utilisation de (10PO, 20PO) ou (20PO, 30PO) ou (10PO, 30PO). Enfin la configuration "Conf.3" correspond à l'utilisation simultanée des trois pompes. Il n'existe alors qu'une seule version dans cette configuration. Chaque version consiste à démarrer et arrêter les différentes pompes.

Considérons que le changement de configuration et de version est manuel. L'opérateur a à sa disposition un ensemble de commutateurs lui permettant de faire ses choix. Les commutateurs du type "c*i*" permettent de sélectionner la configuration *i*. Les commutateurs du type "v*ij*" permettent de sélectionner la version *ij*.

Pour illustrer l'interaction entre les différents modèles, nous supposons que la situation courante est décrite par la figure V-13. La configuration "Conf.2" est active. La version v_{21} est sélectionnée. Les pompes 10PO et 20PO sont démarrées. Le système de pompage représenté par le modèle de fonction de la figure V-14 est en mode de fonctionnement normal d'un point de vue production et maintenance.

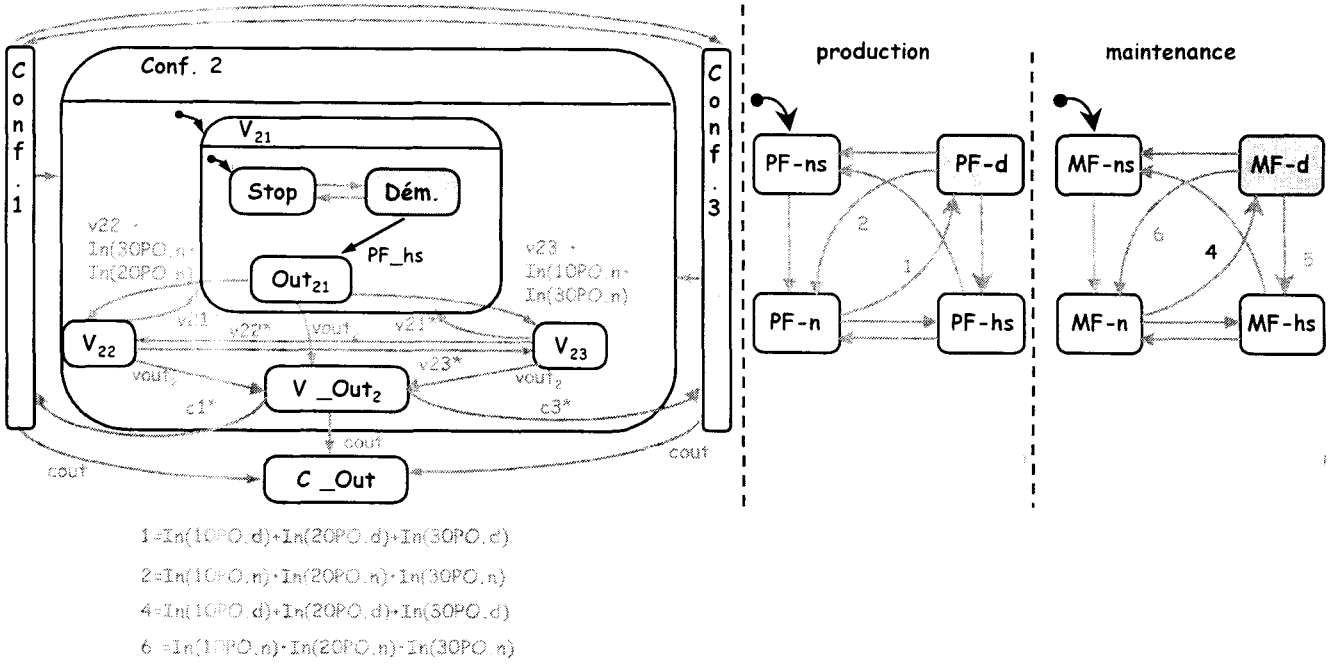


figure V-14. Influence d'une liaison de type nécessité.

Pour illustrer les liaisons de type nécessité, considérons plus particulièrement l'exemple de la version v_{21} qui sollicite les pompes 10PO et 20PO. Ceci est représenté par un lien de type nécessité sur le Graphe Fonctionnel de la figure V-13. Supposons qu'une défaillance apparaisse sur la pompe 10PO qui fait commuter son modèle de composant de l'état de fonctionnement normal à l'état de fonctionnement dégradé. Ceci conduit la fonction "Pomper_1" dans un état de fonctionnement dégradé en raison de la liaison de type nécessité (*figure V-14*).

2.2.2 Liaison de type alternative

Les liaisons de type alternatives ("OU") modélisent la possibilité du choix de la mise œuvre d'une fonction. Elles sont différenciées des liaisons de type "ET" par le symbole "⊕".

OU		S1		
		N	D	HS
S2	N	N	N	N
	D	N	D	D
	HS	N	D	HS

figure V-15. Calcul d'état dans le cas du "OU"

Dans ce cas, il faut que toutes les sous-fonctions changent d'états pour que la fonction mère change d'état (*figure V-15*). Nous considérons qu'il faut que toutes les sous-fonctions se trouvent dans l'état dégradé ou hors service pour estimer la fonction mère respectivement dans l'état dégradé ou hors service du point de vue des modes de fonctionnement.

Illustration : Reprenons notre illustration précédente. Considérons maintenant la configuration 2. Celle-ci peut être mise en œuvre par trois versions représentées par une liaison de type alternative sur la figure V-12. Initialement, nous avons considéré que la version v_{21} était active. Supposons que suite à la première défaillance sur la pompe 10PO, une deuxième défaillance se produit rendant la version v_{21} inutilisable et activant l'état "V_Out_2". L'atteinte de l'état "V_Out_2" va provoquer une commutation entre version, dépendant de la présélection de la version "suivante" (v22 ou v23) effectuée par l'opérateur.

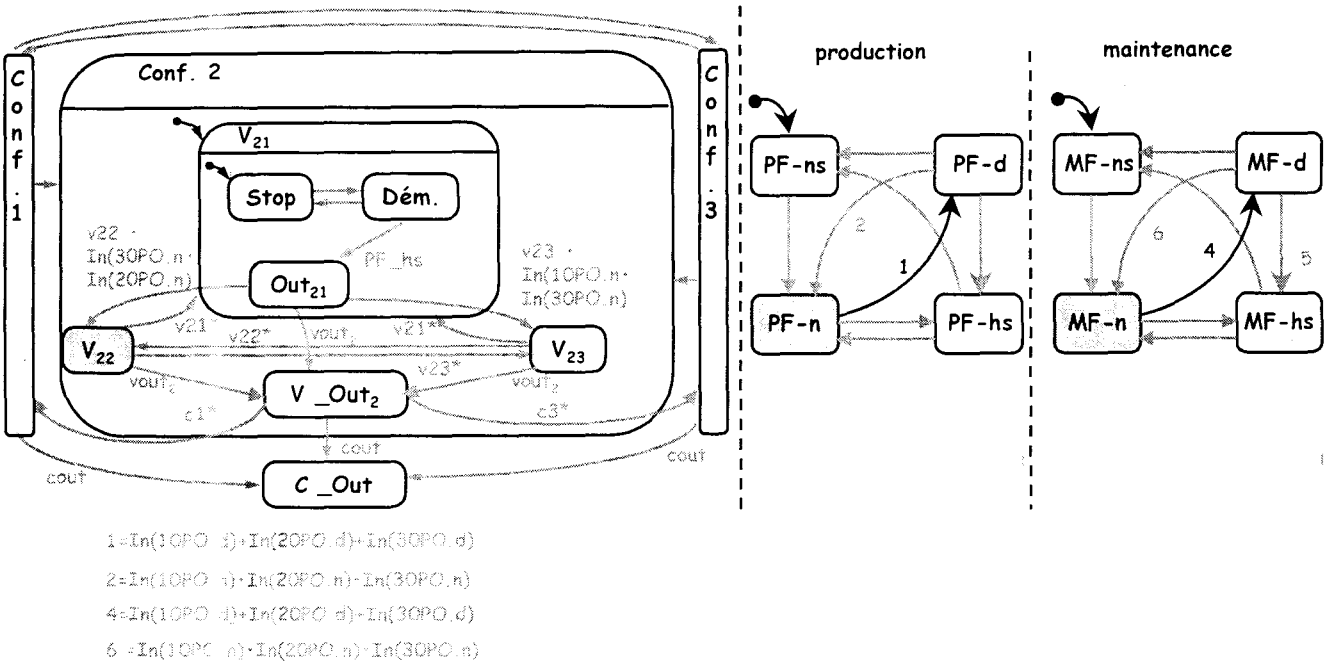


figure V-16. Influence d'une liaison de type alternative.

Nous considérons que c'est la version v_{22} qui est choisie. "L'entrée" dans la version v_{22}, si elle est disponible (i.e. les ressources ne sont pas dans un état de fonctionnement hors service) va provoquer une nouvelle commutation de l'état de fonctionnement dégradé vers l'état de fonctionnement normal (*figure V-16*). Bien que la pompe 10PO soit hors service et la version v_{21} soit inutilisable, le mode de fonctionnement n'est pas considéré comme hors service en raison de la liaison de type alternative (i.e. commutation vers la version v_{22}).

2.2.3 Configurations, versions et points de vue

Nous avons défini, dans les paragraphes précédents, les règles qui permettent de déterminer l'état d'une fonction mère à partir de ses sous-fonctions en ne tenant compte que de la nature des liens.

Nous avons montré que, selon le point de vue adopté et le contexte d'utilisation (i.e. la configuration et la version), le résultat de calcul d'état peut être différent (Chapitre V, §.2.1). La prise en compte du contexte et du point de vue adopté consiste alors à conditionner les résultats définis précédemment.

Point de vue production

Selon le point de vue production, la commutation d'un état vers un autre est étroitement liée à l'origine de cette commutation ; en particulier, il faut que l'entité (sous-système ou composant élémentaire) affectée par un changement

d'état interviennent dans la conduite du système pour qu'une répercussion soit déclenchée aux différents niveaux d'abstraction.

La prise en compte du contexte du point de vue production peut alors se transcrire sur les transitions entre états par l'expression générale suivante : $Contexte(v_i) \bullet (expression(et/ou)$ pour chacune des versions vi.

Point de vue maintenance

Du point de vue maintenance, la commutation d'un état vers un autre est indépendante du contexte courant. En effet, étant donné que de ce point de vue, l'objectif est d'assurer le maintien des moyens de production, toutes les informations concernant un changement d'état d'un sous-système doivent être prises en compte.

Contrairement au point de vue production, la prise en compte du contexte du point de vue de maintenance ne nécessite aucun ajout concernant les transitions entre états.

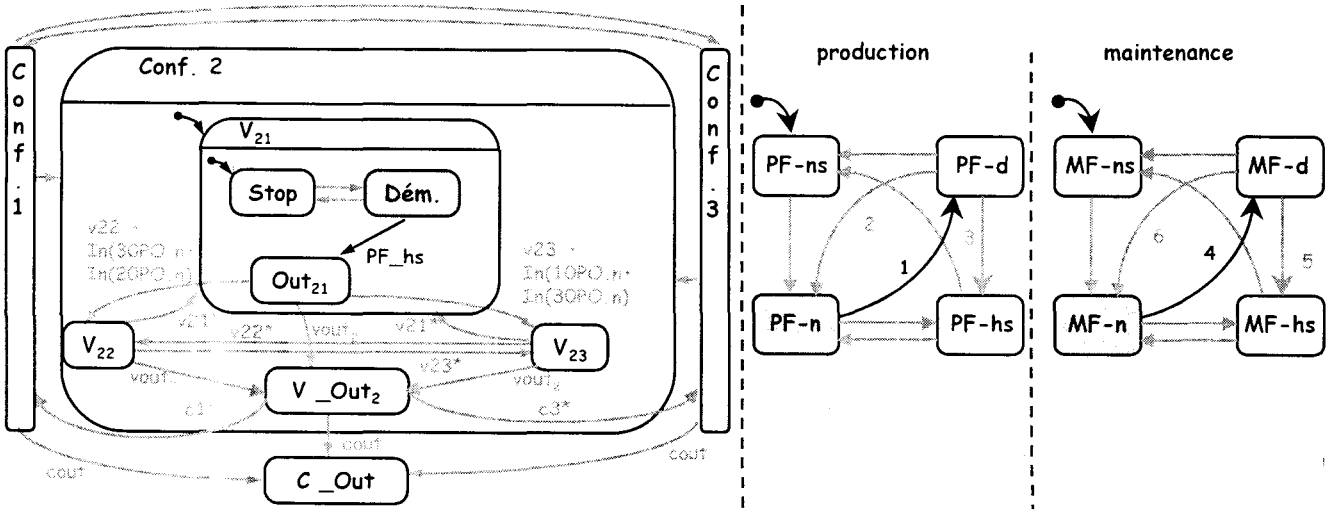


figure V-17. Situation initiale.

Illustration : Repartons de notre situation initiale (*figure V-17*). Supposons que dans ce contexte précis, une défaillance apparaisse sur la pompe 30PO et qu'elle fasse basculer le modèle du composant de cette pompe de l'état de

fonctionnement normal à l'état de fonctionnement dégradé. Comme la pompe 30PO n'est pas utilisé dans la configuration "Conf.2" version *v21* de la fonction "Pomper_1", cela n'a aucune influence sur le point de vue production de son Modèle de Fonction. Par contre, d'un point de vue maintenance, le contexte (la version) n'étant pris en compte puisque l'on souhaite signaler la perte d'une fonctionnalité, la fonction "Pomper_1" commute de l'état de fonctionnement normal à l'état de fonctionnement dégradé (arc 4, *figure V-17*). Cette nouvelle situation est représentée par figure V-18.

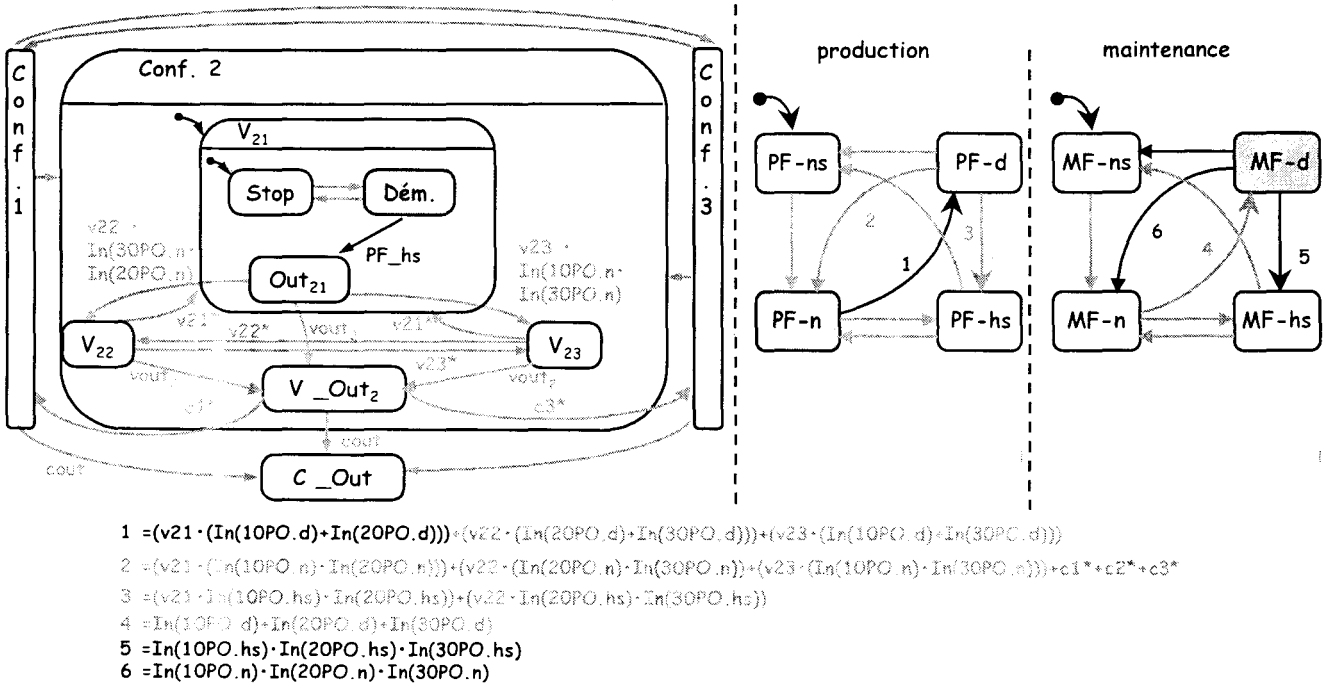


figure V-18. Situation après la défaillance de 30PO

Considérons maintenant que deux défaillances apparaissent successivement sur chacune des pompes 10PO et 20PO. Les premières font commuter le Modèle de Composant de chacune des pompes de l'état de fonctionnement normal à l'état de fonctionnement dégradé. Les secondes font commuter le Modèle de Composant de chacune des pompes de l'état de fonctionnement dégradé à l'état de fonctionnement hors service. Cette fois-ci, ce nouveau changement a pour conséquence de faire commuter le modèle de fonction selon les deux points de vue ; production et maintenance.

Du point de vue production, dans un premier temps, le modèle de fonction commute de l'état de fonctionnement normal vers l'état de fonctionnement dégradé puis de cet état vers l'état de fonctionnement hors service.

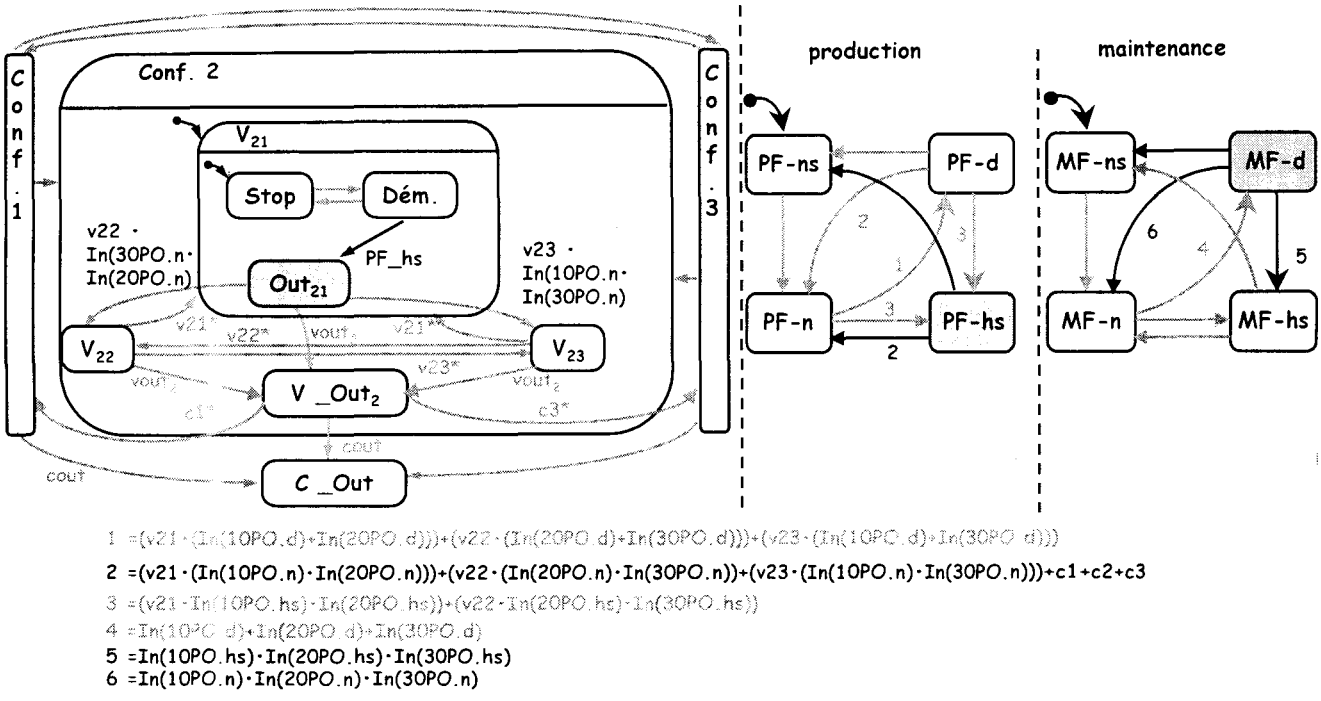


figure V-19. Situation après les défaillances de 10PO et 20PO.

Dans cette situation, la seule évolution possible est un changement de configuration. En effet, étant donné que les pompes 10PO et 20PO sont dans un état de fonctionnement hors service, il est impossible de changer de version. En outre, une commutation vers la configuration "Conf.3" conduirai à la même situation que la figure V-19 puisque cette configuration utilise les pompes 10PO et 20PO. Nous pouvons remarquer que nous aurions pu interdire cette commutation en ajoutant un test de l'état des pompes sur la transition entre "Conf.2" et "Conf.3".

La seule véritable alternative, pour l'opérateur, réside dans l'utilisation de la configuration "Conf.1" qui n'utilise qu'une seule pompe.

CONCLUSION

Cette dernière partie du mémoire a permis de présenter le Modèle de Fonction dont le rôle est de décrire le comportement "interne" d'un système fonctionnel. Il est, en effet, indispensable de pouvoir caractériser chaque sous-système afin de déterminer l'état global du système. Ce modèle permet de définir l'état de disponibilité, le contexte courant et le comportement de chacun des sous-systèmes. Ces informations permettent notamment de répondre aux exigences de chacun des intervenants du contrôle-commande.

A travers l'exemple du SRI, nous avons illustré notre principe de prise en compte du contexte d'utilisation et des points de vue pour déterminer l'état de fonctionnement de chacun des sous-systèmes.

Ce principe de prise en compte du contexte et des points de vue peut être étendu à toutes les familles des modes d'exploitation. Il revient à chaque concepteur de définir ses tables de calcul d'état selon ses propres critères.

Conclusion & Perspectives

En conclusion, nous dressons un bilan des apports de ce mémoire, puis, nous présentons les perspectives et nouvelles directions de recherche que nous proposons.

Conclusion

Les travaux présentés au cours de ce mémoire concernent les traitements à envisager suite à la défaillance de l'un ou plusieurs éléments constituant les Systèmes de Production.

Le **Chapitre I** a permis de présenter le contexte de ces travaux. Ainsi, nous nous sommes attachés à préciser le type des systèmes étudiés. Nous avons retenu tous les Systèmes de Production dont la nature de l'évolution peut être représentée par un modèle discret. Ces travaux s'inscrivent également dans un contexte de tolérance aux fautes où l'objectif est de continuer à délivrer le service souhaité lors de l'occurrence de défaillances. Enfin, nous avons présenté le projet CASPAIM dans lequel s'intègrent ces travaux.

Le **Chapitre II** a mis en avant un manque de terminologie commune en ce concerne le processus de reconfiguration. Suite à l'étude d'un certain nombre d'approches sur le processus de reconfiguration, nous avons proposé des définitions pour des termes donnés en français et en anglais. Il est clair que ceci ne représente qu'une première proposition que certains termes sont amenés à évoluer, notamment en fonction des points de vue des autres auteurs. L'étude du processus de reconfiguration nous a également conduit à présenter notre problématique : la Gestion des Modes.

Le **Chapitre III** présente d'une part notre proposition pour la Gestion des Modes d'une manière générale. Il met en avant l'utilisation de différents modèles ; le Modèle de Composant et le Modèle de Fonction. Il présente également notre première contribution en proposant une démarche pour la détermination des modes d'un Système de Production. L'originalité de cette démarche repose sur la prise en compte de différents points de vue concernés par l'exploitation des Systèmes de Production. Elle nous a permis de déterminer un ensemble de familles de modes et de modes pour décrire le comportement des Systèmes de Production. Cette démarche de conception, ainsi que les suivantes, est illustrée à travers un exemple du système continu dont l'évolution est de nature discrète.

Le **Chapitre IV** est consacré à l'élaboration du Modèle de Composant dont le rôle est de modéliser le comportement des composants élémentaires. Pour ce faire, nous avons introduit la notion de compatibilité des modes. L'objectif est de déterminer la cohérence des états d'un mode par rapport à ceux d'un autre mode. La compatibilité des modes est effectuée en fonction des contraintes imposées par le concepteur. Des mécanismes pour la prise en compte des incompatibilités sont proposés et illustrés. Les limites du Modèle de Composant concernent principalement l'automatisation de sa démarche de conception et sa validation. Dans ce sens, nous proposerons dans les perspectives quelques pistes de recherche.

Le **Chapitre V** est consacré d'une part à la présentation du Modèle de Fonction et d'autre part aux interactions existant entre les différents modèles. Le Modèle de Fonction permet de déterminer l'état "interne" d'un système ou sous-système. Afin de répondre aux besoins des différents intervenants du contrôle-commande, ce modèle renseigne sur la disponibilité, sur la configuration utilisée, et celles possibles, et enfin sur l'état du système ou sous-système d'un point de vue ses modes. L'influence des modèles de niveau

supérieur et inférieur ainsi que la prise en compte du contexte est ensuite abordée pour finalement déterminer l'état du système ou de chaque sous-système. Les limites de ces propositions concernent la formalisation de la prise en compte du contexte et des points de vue ce qui, pour l'instant, rend impossible toute vérification de la structure du modèle obtenu. Là encore, nous proposons dans les perspectives quelques pistes de recherche.

Perspectives

En premier lieu, les perspectives à court terme concernent la mise en œuvre des différentes phases sous formes d'applications informatiques. En effet, il reste dans ce domaine à automatiser, dans un premier temps, les mises en œuvres des mécanismes d'interaction et d'interdiction qui traduisent les incompatibilités entre états. L'automatisation de l'ensemble de la démarche, de la spécification des conditions de passage à la spécification de chacun des modèles est ensuite à effectuer.

Dans un second temps, il nous semble intéressant d'étudier l'influence du type de préemption utilisé. Bien que les SyncCharts proposent différents types de préemption, nous n'avons jusque là utilisé que la préemption dite forte.

A plus long terme, l'objectif est la formalisation et l'étude des propriétés de la commutation dynamique des modes d'un Système de Production. Plusieurs pistes sont à prendre en compte.

La première consiste à étudier l'impact du choix d'un formalisme ou d'un langage de spécification pour la modélisation des modes d'un SP. La comparaison de différents formalismes ou langages de spécification doit permettre de valider ou invalider le formalisme retenu jusqu'à lors,

La seconde consiste, à partir du formalisme ou du langage de spécification retenu, à déterminer des propriétés structurelles des modèles proposés. Enfin, la détermination de ces propriétés permettrait de développer des outils pour valider le comportement global des modèles construits.

Annexes

Annexe 1

LE GRAPHE FONCTIONNEL

1 PRÉSENTATION

1.1 objectifs

Le Graphe Fonctionnel (GF) est un modèle fonctionnel initialement destiné à développer des algorithmes pour la fonction de Diagnostic. Il permet notamment de représenter les relations de causalité entre fonctions.

Les différents concepts utilisés dans son élaboration sont la **fonction**, **l'opération**, le **Lieu Caractéristique Fondamental** et **l'Accessibilité Directe Fondamentale**.

Une **fonction** est définie comme la réponse d'un système ou d'un composant à un stimulus donné quand il fonctionne normalement, indépendamment de l'environnement dans lequel il est sollicité [Tog, 96].

Une **opération** est une fonction réalisée sur un produit par une ressource compte tenu de sa situation spatiale au sein du système [Ber, 98].

Les fonctions sont définies au niveau du système alors que les opérations sont définies au niveau des ressources. Une opération met en œuvre une fonction.

Un **Lieu Caractéristique Fondamental** (LCF) correspond à une zone de transformation ou un lieu de stockage servant de zone d'entrées ou de sorties de produits du système [Ber, 99/a].

L'**Accessibilité Directe Fondamentale** (ADF) correspond au transfert direct d'un produit d'un lieu caractéristique vers un autre lieu caractéristique [Ber, 00].

Le GF est en fait le résultat de la combinaison de plusieurs modèles : le Modèle de Conception (MFC) et le Modèle Fonctionnel d'Implantation Élémentaire (MFIE) [Tog, 00].

1.2 Modèle Fonctionnel de Conception

L'objectif du Modèle Fonctionnel de Conception (*figure A1-1*) est de permettre au concepteur de spécifier comment les fonctions principales de son système seront obtenues. Il repose sur le concept de fonction. Sa détermination est guidée par le cahier des charges fonctionnel. La première étape consiste à identifier les objectifs initiaux du système. Ceci conduit à identifier les **fonctions principales** du système. Une approche descendante permet d'identifier les **fonctions initiales** du système.

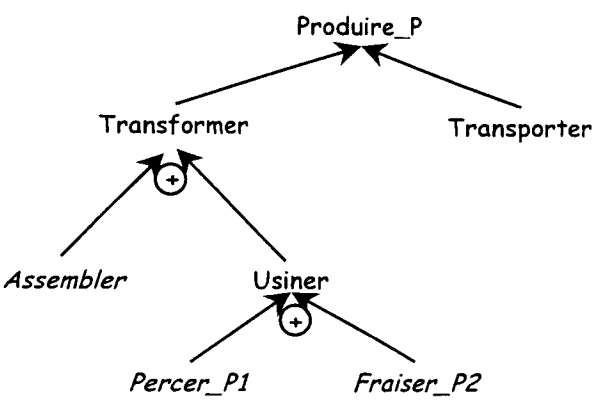


figure A1-1. Exemple de MFC

Dans le cas des SFPM, par exemple, nous pouvons considérer qu'une de ses fonctions est "usiner". Il peut, selon le système étudié et le CdCF, exister différentes façons d'usiner (par exemple : "Percer_P1" et "Fraiser_P2"). L'analyse descendante est donc poursuivie. Elle est stoppée lorsque les fonctions ne sont plus décomposables sans tenir compte de la structure physique du système. Ce sont les fonctions initiales du système. Pour relier les fonctions initiales à la fonction principale, le concepteur établit des liens de dépendances. Il existe principalement deux types de liaison : les liaisons de type alternatives (ou) et les liaisons de type nécessité (et).

1.3 Modèle Fonctionnel d'Implantation Élémentaire

Le Modèle Fonctionnel d'Implantation Élémentaire (*figure A1-2*) permet d'affiner les fonctions initiales en tenant compte de la structure du système. Il repose sur le concept d'opération. Compte tenu des ressources choisies par le concepteur, chacune des fonctions initiales peut être déclinée en une ou plusieurs opérations. Cela dépend de la flexibilité du système. Imaginons une fonction "Percer_P1" d'un Système de Production qui comporte deux fraiseuses identiques (redondance). Nous avons dans ce cas deux opérations possibles ($Op_{m1,f1}$, $Op_{m2,f1}$) pour mettre en œuvre la fonction "Percer_P1" (*figure A1-2).*

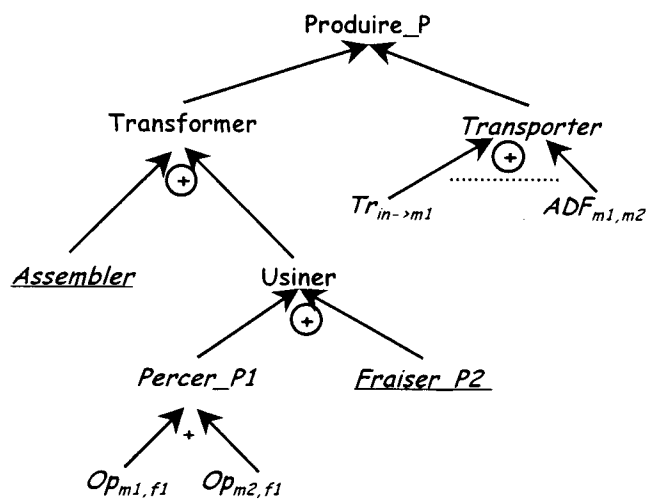


figure A1-2. Exemple de MFIE

Le Graphe Fonctionnel s'obtient principalement par la juxtaposition du MFC, du MFIE et de l'affinement des opérations. Ce dernier point consiste à relier le modèle fonctionnel de chaque ressource à chacune des opérations.

2 EXEMPLE

Pour illustrer une telle démarche, reprenons l'exemple du circuit SRI développé et dont une partie du cahier des charges fonctionnels est présenté dans le chapitre III (§.2.3). Nous compèterons ce dernier au fur et à mesure.

Le Modèle Fonctionnel de Conception

La première étape de la conception du MFC consiste à déterminer la (ou les) fonction(s) principale(s) du système. Dans l'exemple du SRI, la fonction principale est de réfrigérer les auxiliaires de la partie conventionnelle d'une centrale nucléaire. Nous appelons cette fonction "**Réfrigérer_Aux**". Le MFC doit alors expliciter les liens de dépendance causale entre la fonction "**Réfrigérer_Aux**" et les fonctions initiales du système. Démarrant de la fonction principale, le concepteur va se demander quelles sont les fonctions nécessaires à la mise en œuvre de "**Réfrigérer_Aux**". La réponse à cette question va l'amener à déterminer que cette fonction nécessite de mettre en circulation l'eau déminéralisée (fonction "**Circuler_Dem**") et de conduire l'eau déminéralisée jusqu'aux échangeurs auxiliaires (fonction "**Conduire_1**"). De la même manière, on va étudier comment mettre en œuvre la fonction "**Circuler_Dem**". Pour cela, il faut alimenter le circuit en eau déminéralisée (fonction "**Alimenter_Dem**") et il faut vaincre les pertes de charges par le pompage de cette eau (fonction "**Pomper_Dem**"). La décomposition successive des fonctions non initiales conduit à l'élaboration du MFC. L'affinement de celui-ci est fait en étudiant les conditions de fonctionnement du système décrit par le CdCF.

Par exemple, considérons la fonction "**Pomper_1**". Selon la situation de la tranche, ces caractéristiques peuvent être différentes. Il existe en réalité trois variantes de cette fonction qui dépendent de la saison et des contraintes de production. Nous appelons ces fonctions "**Pomper_11**", "**Pomper_12**", "**Pomper_13**". La fonction "**Pomper_12**" est la plus courante. En outre, en cas de défaillance totale du système de pompage du SRI, le circuit est reconfiguré en "boucle ouverte" (l'eau déminéralisée chauffée est jetée à l'égout). Dans ce contexte, la mise en circulation de l'eau déminéralisée est momentanément assurée par la bâche d'appoint (fonction "**Stocker_Dem**"). Elle permet ainsi la poursuite de la réfrigération du circuit pendant un certain temps. Ceci se traduit sur le modèle par une liaison de type "OU" entre les fonctions

"**Pomper_Dem**" et " **Stocker_Dem**". Ceci est un exemple d'affinement du MFC.

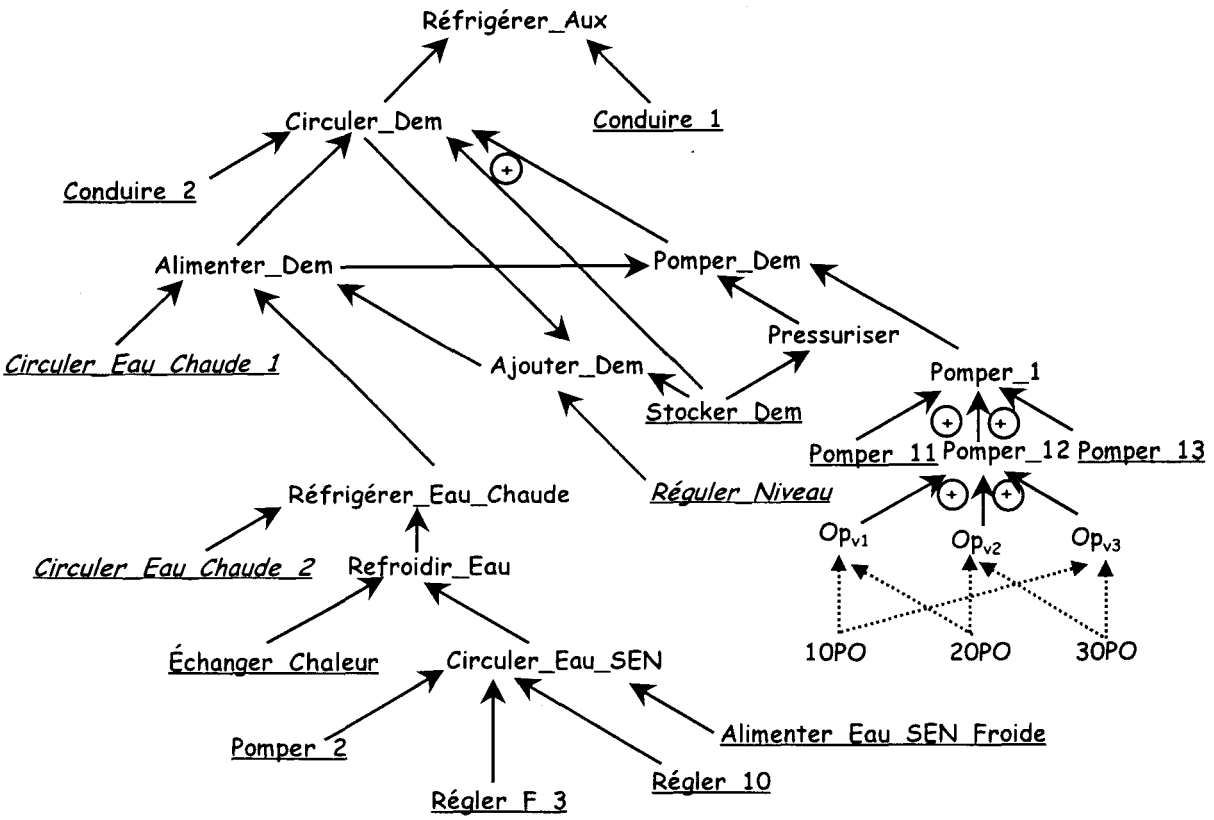


figure A1-3. Extrait du Graphe Fonctionnel du SRI

Le Modèle Fonctionnel d'Implantation Élémentaire

Une fois le MFC définit, nous pouvons nous attacher à déterminer le MFIE. Pour des raisons de clarté prenons uniquement l'exemple de la fonction "**Pomper_12**". Le système possède trois pompes identiques (appelées 10PO, 20PO, 30PO). Pour répondre aux exigences de la fonction "**Pomper_12**" (et du CdCF) il est nécessaire de mettre deux pompes en service. Dans ce cas présent, nous pouvons donc dire qu'il y a trois opérations possibles pour délivrer la fonction "**Pomper_12**". Ceci se traduit sur le modèle par une liaison de type "OU" entre les opérations "Op_{v21}", "Op_{v22}", "Op_{v23}". Les fonctions "**Pomper_11**" et "**Pomper_13**" correspondent respectivement à l'utilisation d'une pompe sur les trois et à l'utilisation des trois pompes.

Un extrait du modèle fonctionnel, résultant de l'élaboration du MFC et MFIE, est présenté par la figure A1-3. Les fonctions soulignées correspondent aux fonctions non complètement développées sur le modèle.

Annexe 2

LES STATECHARTS

1 PRÉSENTATION

StateChart est un formalisme graphique de spécification développé par D. Harel en 1987 [Har, 87]. Il est destiné à la description comportementale des systèmes complexes. Ce formalisme est présenté comme une extension des automates à états finis et de leur mode de représentation (les diagrammes états-transitions) [Har, 87]. Les principales extensions portent sur trois notions fondamentales :

- La hiérarchisation des états (la profondeur) : permet de décomposer un état (appelé super état ou état pères) en sous-états (ou états fils),
- L'expression du parallélisme (l'orthogonalité) : permet de décrire l'activation simultanée de plusieurs sous-états,
- La communication par diffusion (Broadcasting-communication) : signifie que les événements sont connus de tous au même instant.

Ce modèle est fréquemment caractérisé par la formule :

StateCharts = Diagramme d'états + hiérarchie + parallélisme + communication

2 SYNTAXE

Un StateChart est un graphe dont les sommets représentent les états du système, et les arcs les transitions entre états (*figure A2-1*). Les arcs sont étiquetés par l'événement déclencheur de la transition. Les états sont symbolisés par des rectangles à coins arrondis.

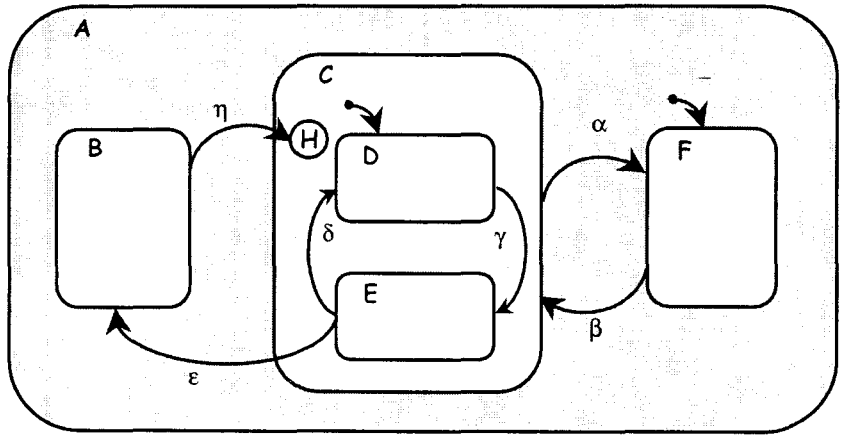


figure A2-1. Exemple de StateChart

2.1 Entrer dans un état

Il existe différentes manières d'activer un état : par défaut, par historique, directement, par sélection ou par condition.

2.1.1 Par défaut

L'entrée par défaut permet de savoir quel est le sous-état à activer initialement. Ce type d'entrée est représenté par une flèche pointée symbolisée par : ↘. La notion d'état par défaut (initial) a été introduite afin de déconnecter un état de son environnement. Ce mécanisme illustré par la figure A2-1 montre que le symbole flèche pointée arrivant sur le sous-état "F" désigne l'état initial entre "B", "C" et "F". A l'intérieur de l'état "C", l'état initial "D" est spécifié par le même formalisme.

2.1.2 Directement, par sélection ou par condition

Ces différents types d'entrée permettent d'activer un état particulier. L'entrée directe est représentée par une flèche qui va directement de l'état source vers l'état objectif.

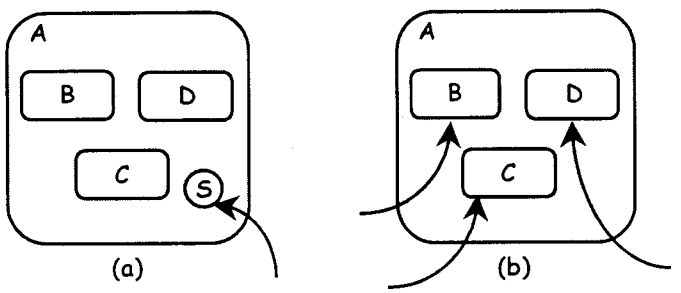


figure A2-2. Entrée par Sélection

L'entrée par sélection et par condition permet d'activer un sous-état spécifique sur l'occurrence d'un événement particulier (par sélection) et/ou une condition (par condition). Ce type d'entrée est représenté respectivement par un "S" et un "C" placé dans un cercle. Elles permettent de réduire le nombre d'arcs qui entrent dans un état. La figure A2-2(a) est équivalente à la figure A2-2(b).

2.1.3 Par historique

La notion d'historique permet de réactiver le dernier état actif du groupement. Elle est symbolisée par un arc se terminant sur un cercle contenant la lettre "H" (*figure A2-1*). Il est ainsi possible de mémoriser l'état. Cette notion pourrait être d'une grande utilité en cas de reprise.

2.2 Sortir d'un état

Pour sortir d'un état, il est nécessaire de franchir une transition dont la source est l'état lui-même ou l'un de ces sous-états. Pour sortir de l'état "C" (*figure A2-1*), il est nécessaire que l'événement "α" ou "ε" se produise.

3 LES EXTENSIONS

La hiérarchie, l'orthogonalité et la communication sont les principales extensions proposées. La hiérarchisation et l'orthogonalité permettent notamment de gagner en lisibilité.

3.1 La hiérarchie

Le concept de hiérarchie introduit les notions d'abstraction et d'affinement nécessaires aux approches structurées. Elles permettent la description de système de taille et de complexité importantes en évitant la rapide multiplication des états. La figure A2-3 illustre ce concept de hiérarchie. Le passage de la figure A2-3(b) à la figure A2-3(a) représente l'abstraction. Le passage de la figure A2-3(b) à la figure A2-3(c) représente l'affinement.

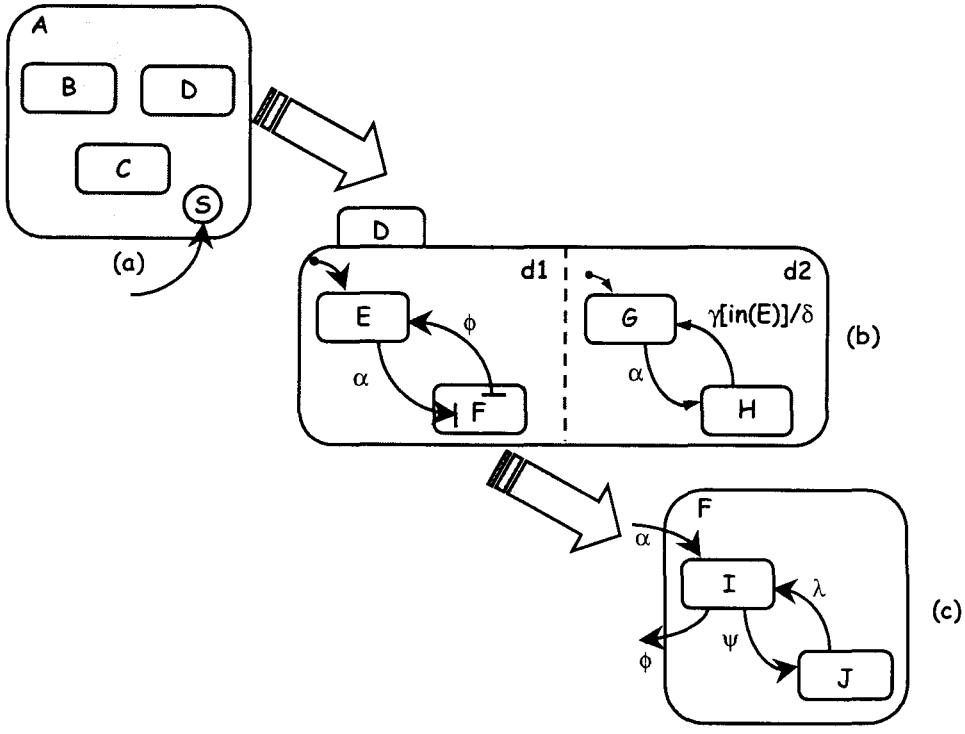


figure A2-3. Notions d'abstraction et d'affinement

Les StateCharts offrent deux possibilités de constructions. La première de type **OU** permet de spécifier des états exclusifs d'un même StateChart. C'est le cas du StateChart "F" (*figure A2-3(c)*) où seul le sous-état I ou le sous-état J peut-être actif. L'autre construction (orthogonale) permet de mettre en

évidence l'aspect parallèle de l'application : construction de type ET (*figure A2-3(b)*).

3.2 Le parallélisme

Le StateChart "D" de la (*figure A2-3(b)*) indique que le sous-état d1 et le sous-état d2 sont en parallèles. Ces sous-états sont alors dits orthogonaux. Le parallélisme est symbolisé par les pointillés scindant un groupement d'états en deux. Ce qui engendre une non-connexité des ensembles d'états. Chacun des sous-états possède un et un seul état actif à un instant donné. Les sous-états d1 et d2 forment implicitement l'état D du niveau supérieur.

Il est possible de synchroniser l'évolution de sous-états. Dans la figure A2-3(b), il est nécessaire que le sous-états "E" soit actif ("in(E)")pour qu'il puisse y avoir basculement du sous-état "H" vers "G" (à condition que l'événement "γ" soit présent).

3.3 La communication

Le passage d'un état à l'autre se fait par les événements qui étiquettent les arcs. Quand un état est actif, et un événement étiquetant un arc sortant de cet état est présent, l'état actif après franchissement est l'état pointé par ce même arc. Les transitions d'un StateChart sont donc considérées comme de la préemption forte. Dès que la transition est validée (i.e. occurrence de l'événement), l'état source est immédiatement désactivé ainsi que tous ces sous-états.

L'évolution d'un StateChart est définie par une sémantique associée aux transitions qui prend la forme suivante : événement(s)[condition(s)]/action(s).

L'évolution d'un diagramme StateChart est donc conditionnée par les événements engendrés par son environnement : entrées. Un événement présent est vu de la même manière à tout niveau de description : diffusion instantanée. Les actions activées par les transitions sont vues comme des sorties et deviennent simultanément des entrées pour d'autres StateCharts. La dualité événement/action permet de synchroniser des processus parallèles : une action émise est considérée comme un événement (réaction en chaîne).

Annexe 3

APPROCHE SYNCHRONE

1 ESTEREL

Esterel se définit comme un *"langage impératif parallèle qui a une sémantique mathématiquement bien définie et une réalisation complète"* [Ber, 87/b]. Cette sémantique [Ber, 96] permet d'appliquer des méthodes de vérification formelles.

Ses opérateurs sont similaires à ceux des langages impératifs classiques : la séquence (;), l'assignation (:=), les expressions conditionnelles (if...then...else, ...), le parallélisme (| |), la communication par diffusion (emit S) et des mécanismes d'interruptions. Il possède également des mécanismes temporels avec des instructions telles que les déclencheurs, les chiens de garde et les boucles temporelles [Ber, 99/b].

L'élément de base de la programmation Esterel est l'événement, défini comme l'émission ou la réception simultanée d'un ou plusieurs signaux. Les

signaux émis au même instant sont combinés et diffusés à tous les modules Esterel (broadcasting-communication). Un signal peut être porteur d'une valeur, il est alors dit valué. Un signal non valué est dit pur. La notion de temps fait abstraction du temps physique. Chaque signal reconnu définit une unité de temps. Il est possible d'exprimer deux types de relations entre les signaux. Le premier sert à exprimer une exclusion entre deux signaux. Ceci implique que la simultanéité des signaux est impossible. Cette relation est symbolisée par un #. Le second type de relation permet de spécifier la simultanéité "unilatérale" de deux signaux. Cette relation est symbolisée par un ⇒. L'expression S1⇒S2 signifie que l'apparition de S1 implique l'apparition de S2 et non l'inverse. L'exemple le plus connu est celui des minutes et des secondes : minute⇒seconde.

2 SYNCHARTS

2.1 Présentation

SynCharts est l'acronyme de *Synchronous Charts*. Ils sont fortement inspirés des StateCharts de D. Harel [Har, 87] et de ARGOS. Les principaux apports proposés par ce modèle graphique concernent la préemption et la sémantique utilisée. En outre, il est basé sur le paradigme synchrone. Ce dernier repose sur cinq hypothèses de base [And, 96] :

- Le système interagit avec son environnement par l'intermédiaire de signaux d'entrée et de signaux de sorties,
- Tous les signaux d'entrée et de sortie sont perçus simultanément,
- Il n'y a pas de temps physique mais des instants logiques,
- Les opérations internes se font, vu de l'extérieur, en un temps nul. Les signaux de sortie sont alors synchrones à ceux d'entrée,
- Tous les signaux sont simultanément émis.

Tout comme les StateCharts, les SynCharts permettent de représenter le comportement réactif de systèmes complexes. Ils proposent une structure hiérarchique par encapsulation d'états, l'orthogonalité et la préemption. Une des particularités des SynCharts est de proposer trois sortes de préemption : la faible, la forte et la suspension. Une autre particularité repose sur la

traduction directe de chaque modèle SynCharts en un programme ESTEREL équivalent. Ceci donne la possibilité d'utiliser les vérifications comportementales offertes par ESTEREL et le dote d'une sémantique mathématique bien définie.

2.2 Syntaxe

Le modèle SynCharts possède une syntaxe graphique proche de celles des StateCharts. Cette syntaxe graphique est articulée autour de l'*étoile*. Chaque étoile peut alors faire elle-même partie d'une *constellation* qui est à son tour une constituante d'un *macro-état*. Un macro-état n'est en fait qu'une étoile de niveau supérieur.

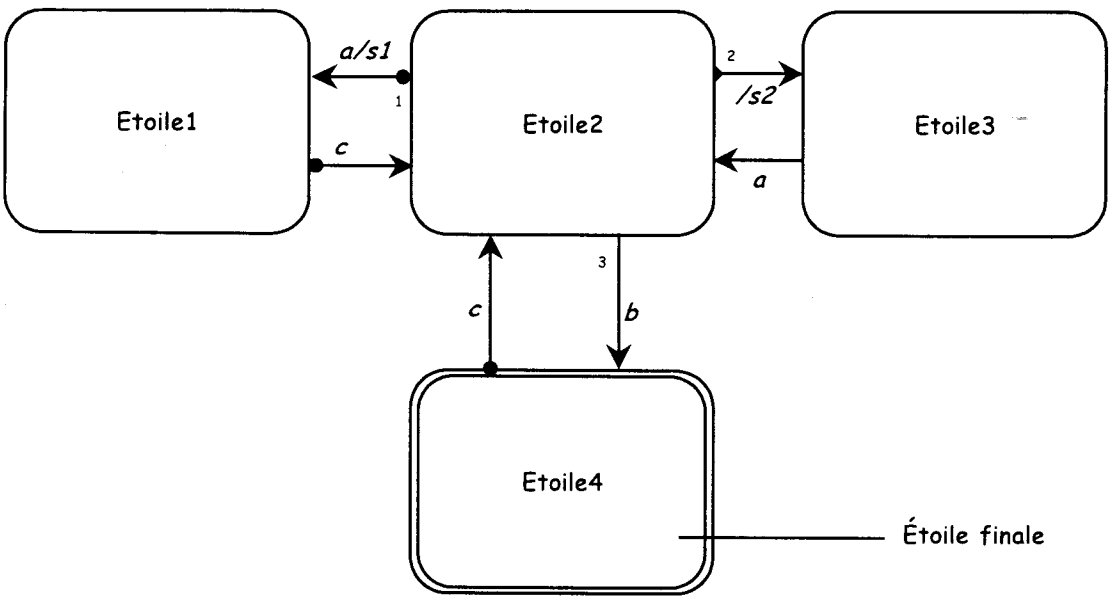


figure A3-1. Une constellation

Une constellation

Une constellation (*figure A3-1*) est un ensemble d'étoiles tel qu'une seule étoile est active à l'intérieur d'une constellation [And, 98].

L'étoile

Une étoile (*figure A3-2(b)*) est plus qu'un état : c'est un état et les façons de le quitter [And, 97]. Les arcs d'avortement issus d'un état constituent les rayons de l'étoile. Chaque rayon reçoit une priorité ce qui rend déterministe le

modèle dans le cas ou plusieurs événements permettant de sortir de l'étoile sont simultanément actifs.

Une étoile particulière, entouré une fois supplémentaire, permet de spécifier un état final (*figure A3-1*). Lorsque cet état est atteint, la tâche imputée à la constellation est terminée.

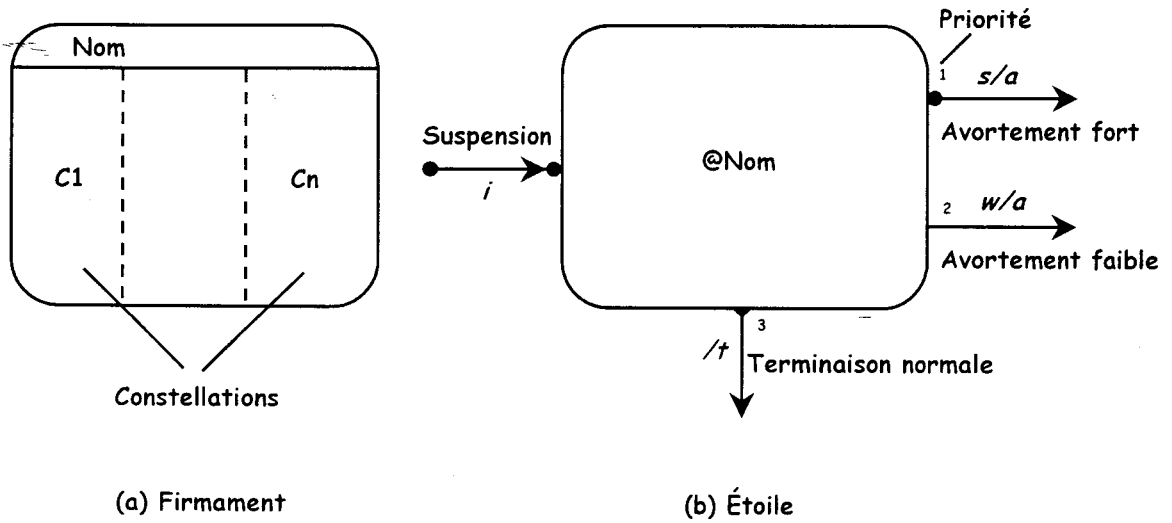


figure A3-2. Macro-état et Étoile

Un macro-état ou firmament

Un macro-état (*figure A3-2(a)*) est constitué d'une ou plusieurs constellations en parallèle. A un autre niveau hiérarchique, il correspond à une étoile possédant plusieurs constellations en son sein.

Les arcs

Les arcs sont étiquetés de la façon suivante :

Trigger[condition]/effect

- Trigger : représente une expression booléenne qui porte sur la présence des signaux,
- Condition : représente un prédicat pouvant faire intervenir des valeurs de signaux,
- Effect : une liste de signaux, éventuellement valués, à émettre lors de la transition.

Ces différents champs sont optionnels. En effet, si aucun trigger n'est spécifié, le trigger par défaut est *Tick*, un signal prédéfini présent à chaque instant. " T [?T > Time]/a" est un exemple d'étiquette. Elle déclenche la transition sur l'occurrence du signal "T", si la valeur de ce signal est supérieure à la constante "Time" et émet le signal "a". "/b" signifie qu'à un temps logique "Tick", la transition est déclenchée sans aucune occurrence d'événement et de condition et émet le signal "b".

2.3 Les différentes formes de préemption

Il existe différentes façons de sortir d'une étoile ou d'un macro-état (*figure A3-2(b)*) :

- Terminaison normale : Lorsque toutes les composantes d'un macro-état sont dans un état dit final (représenté par double cercle), alors il y a instantanément terminaison finale. La terminaison normale se caractérise par le fait qu'il n'y pas de trigger. Une telle terminaison est représentée par une flèche simple ayant un triangle rouge pour base,
- Avortement : Il met définitivement fin à l'exécution des tâches d'une étoile ou d'un macro-état. On distingue deux formes :
    - ✧ L'avortement fort interdit toute exécution de l'étoile ou du macro-état préempté, dans l'instant de la préemption. Il est représenté par une flèche simple ayant pour base un rond rouge,
    - ✧ L'avortement faible laisse terminer l'exécution de l'instant. Il se représente par une flèche simple.
- La suspension : La tâche en court est suspendu tant que le signal inhibiteur est présent. Le résultat est comparable à un figeage. Elle se représente par une flèche simple ayant pour base un rond noir et se terminant par un rond rouge.

3 PARADOXES ET INDÉTERMINISMES DES

La littérature met l'accent sur certains paradoxes et indéterminismes qui peuvent être rencontrés dans une spécification SyncCharts et les langages synchrones. Ils sont liés à une erreur de conception qui va à l'encontre de l'hypothèse de synchronisme.

present *a* then emit *c* else emit *b* end

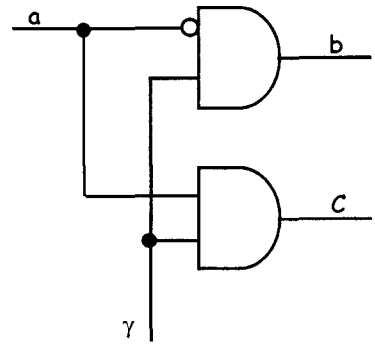
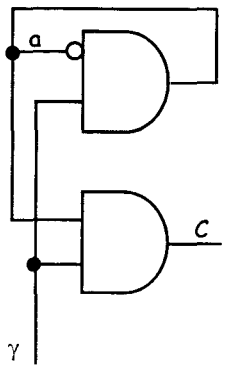


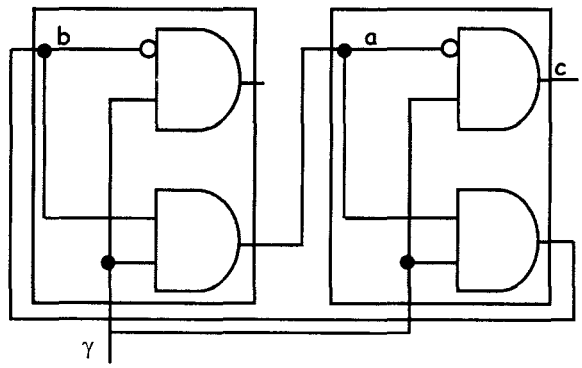
figure A3-3. Équivalence d'un programme Esterel en un circuit

Tout programme Esterel (donc tout SyncCharts) a une équivalence en un circuit qui manifeste le même comportement d'un point de vue des entrées et des sorties. Ceci est possible grâce à l'algorithme du compilateur Esterel. Les exemples sont donnés par C. André [And, 96]. La figure A3-3 représente l'équivalence entre un programme Esterel et un circuit. Les signaux "b" et "c" sont des sorties , le signal "a" est une entrée, "γ" est un contrôleur de ligne. Nous utilisons cette équivalence pour présenter les paradoxes rencontrés.



signal *a*
present *a* then emit *c* else emit *a* end
end signal

(A)



signal *a, b* in
present *a* then emit *b* else emit c end
||
present b then emit *a* end
end signal

(B)

figure A3-4. Non-réactivité et Indéterminisme

L'hypothèse synchrone concerne l'association événement/action portée par les arcs pour laquelle l'événement et l'action sont considérés comme simultanés. La diffusion instantanée des signaux permet d'écrire des

programmes syntaxiquement corrects mais sémantiquement incorrects. En effet, pour être correct (au sens Esterel), tout programme doit être déterministe et réactif. Un programme est réactif s'il fournit une sortie précise pour chaque entrée. Un programme est déterministe s'il fournit seulement une sortie pour chaque entrée.

Il existe une dépendance entre le signal A et le signal B lorsque la connaissance de l'état (présent ou absent) de A est nécessaire pour connaître de l'état B. Par transitivité, on peut avoir un cycle dit statique. Une dépendance induit un ordre d'évaluation à respecter.

Le circuit représenté par la figure A3-4 (A) est cyclique. La sortie dépend de l'entrée. De plus, nous pouvons montrer que ce programme est non réactif en utilisant les deux équations du système : $a = \gamma \bullet \overline{a}$ et $c = \gamma \bullet a$. Si $\gamma = 0$ alors $a = c = 0$. Par contre si $\gamma = 1$ alors il n'y a pas de solution pour que $a = \overline{a}$. Ce programme est non réactive car à l'entrée $\gamma = 1$ il ne donne aucune sortie précise.

Il est facile de montrer de façon similaire que le programme de la figure A3-4 (B) est indéterministe. Il représente deux composants qui sont en parallèles. Lorsque $\gamma = 1$ il y a deux solutions : soit $a = b = 0$ et $c = 1$, soit $a = b = 1$ et $c = 0$. Ce programme est non déterministe puisque pour l'entrée $\gamma = 1$, il donne deux solutions.

Les cycles statiques, la non réactivité et l'indéterminisme sont plus souvent appelés des **problèmes de causalité**.

```
present I then
        present O1 then O2 end
else
        present O2 then O1 end
end present
```

figure A3-5. Faux cycle statique

Cependant, les cycles statiques ne sont pas forcément de véritables cycles de causalité. En effet, la figure A3-5 présente un programme qui comporte un cycle statique mais qui en est en réalité un faux cycle statique. Il y a bien dépendance entre les signaux O1 et O2. Comme cette dépendance est transitive, nous sommes en présence d'un cycle statique. Cependant, au cours

de l'exécution, une seule branche du programme ne pourra être exécutée selon la valeur de I. Il n'y aura donc pas d'indéterminisme sur l'ordre de l'évaluation.

Pour déterminer les cycles statiques le compilateur fait une mise à plat de l'ensemble des états. Ceci lui permet de trouver tous les cycles. Il sait "casser" ces cycles statiques en tenant compte du contexte comme nous venons de le décrire précédemment. Si les cycles résistent, le programme est alors rejeté en provoquant une erreur de cycle de causalité.

Les cycles statiques ne sont donc pas important dans notre approche. Il le sont lorsque les programmes sont utilisés pour concevoir des circuits électronique : certains logiciels de conception de carte ne supportent pas les cycles.

Par contre, afin de garantir un comportement de notre modèle, il est indispensable qu'il n'ait pas de problème de causalité. Le compilateur Esterel permet de faire cette vérification.

Références

Références

[ADE, 81] ADEPA,

"GEMMA, Guide d'Etude des Modes de Marches et d'Arrêts", Productior Automatisé, ADEPA, 1981.

[AFN, 91] AFNOR,

"Organisation et gestion de la production industrielle - Concepts fondamentaux (la gestion de production", Norme NF X 50-310, décembre 1991.

[Ama, 94] S. AMAR,

"Systèmes automatisés et flexibles de production manufacturière : Méthodol de conception du système de coordination par prototypage orienté objet d partie procédé", Thèse de doctorat, Université des Sciences et Technologie Lille, avril 1994.

[And, 96] C. ANDRE,

"Representation and Analysis of Reactive Behaviors: A Synchronous Appr IEEE-SMC, Computational Engineering in System Applications, CESA'96, 1996, pp. 19-29.

[And, 97] C. ANDRE,

"SynCharts : un formalisme graphique pour systèmes réactifs complexes", ELISA'97, Journées d'étude sur les logiciels pour le traitement de l'image, du signal et de l'automatique, Nancy, 25-26 mars 1997.

[And, 98] C. ANDRE, H. BOUFAÏED, S. DISSOUBRAY,

"SynCharts : un modèle graphique synchrone pour systèmes réactifs complexes", RTS'98, Real-Time Systems, Paris, 14-16 janvier, pp. 175-193.

[Aus, 94] C. AUSFELDER,

"Contribution à la conception d'un système de conduite pour les systèmes flexibles de production manufacturière : modélisation et validation de la commande", Thèse de doctorat, Université des Sciences et Technologies de Lille, mars 1994.

[Bas, 97] A. BASSAND,

"Proposition d'un Modèle de Données de Référence pour la Conception des Systèmes de Supervision", Thèse de doctorat, École Normale Supérieure de Cachan, janvier 1997.

[Ber, 96] G. BERRY,

"The Constructive Semantics of Pure Esterel", Draft version 2, Centre de Mathématiques Appliquées, Ecole des Mines de Paris, May 1996.

[Ber, 87/a] G. BERRY, P. COURRONE, G. GOUTHIER,

"Programmation Synchrone des Systèmes Réactifs : le langage ESTEREL", TSI, Vol. 6, n° 4, 1987, pp. 305-315.

[Ber, 87/b] G. BERRY, G. GOUTHIER,

"Le langage synchrone Esterel : Conception, Sémantique, Impléméentation", Ecole des Mines, Sophia-Antipolis, France, 1987.

[Ber, 98] P. BERRUET,

"Contribution au recouvrement des systèmes flexibles de production manufacturière : analyse de la tolérance et reconfiguration", Thèse de doctorat, Université des Sciences et Technologies de Lille, décembre 1998.

[Ber, 99/a] P. BERRUET, A. TOGUYENI, E. CRAYE,

"Considering parts in progress in a reconfiguration procedure for FMS",3rd IMACS/IEEE International Multiconference, Circuits, Systems, Communications and Computers (CSCC'99), Athènes (Grèce), Juillet 1999.

[Ber, 00] P. BERRUET, A. TOGUYENI, E. CRAYE,

"Modèles et algorithmes pour la surveillance/supervision", Édition Hermès (A paraître).

[Ber, 99/b] G. BERRY,

"The Esterel v5 Language Primer", version 5.21 release 2.0, Centre de Mathématiques Appliquées, Ecole des Mines de Paris, April 1999.

[Bil, 94] P. BILAND,

"Modélisation des modes de marche d'un système automatisé de production", Thèse de doctorat, École Centrale de Nantes, février 1994.

[Boi, 91] S. BOIS,

"Intégration de la gestion des modes de marche dans le pilotage d'un système automatisé de production", Thèse de doctorat, Université des Sciences et Technologies de Lille, novembre 1991.

[Bon, 93] A. de BONNEVAL,

"Mécanismes de reprise dans les systèmes de commande à événements discrets", Thèse de doctorat, Université Paul Sabatier, Toulouse, septembre 1993.

[Bou, 97] A. BOURAS,

"Contribution à la conception d'architectures réparties : modèles génériques et interopérabilité d'instruments intelligents", Thèse de doctorat, Université des Sciences et Technologies de Lille, juillet 1997.

[Bou, 88] J.-P. BOUREY,

"Structuration de la partie procédurale du système de commande de cellules flexibles dans l'industrie manufacturière", Thèse de doctorat, Université des Sciences et Technologies de Lille, mars 1988.

[Bra, 83] G. W. BRAMS,

"Réseaux de Petri : Théorie et Pratique", Tome 1 : Théorie et analyse, Éditions Massons, Paris, 1983.

[Cam, 97/a] H. CAMUS *et al.*

"Projet EOWYN" Mars 1997, 20 pages. Note Interne NI/97/1, L.A.I.L., 1997.

[Cam, 97/b] H. CAMUS,

"Conduite des Systèmes Flexibles de Production Manufacturière par composition des régimes permanents cycliques : modélisation et évaluation de performance à l'aide des Réseaux de Petri", Thèse de doctorat, Université des Sciences et Technologies de Lille, mai 1997.

[CEI, 74] Commission Électronique Internationale,

"Liste des termes de base, définitions et mathématiques applicables à la fiabilité", référence 271, 1974.

[Cha, 95] A. CHAILLET-SUBIAS,

"Approche multi modèles pour la commande et la surveillance en temps réel des systèmes à événements discrets", Thèse de doctorat, Université Paul Sabatier de Toulouse, décembre 1995.

[Che, 99] P. CHEVOCHOT, I. PUAUT,

"Tolérance aux fautes dans les systèmes répartis temps réel strict", Technique et Science Informatiques, Volume 18, n° 8, 1999, pp. 837-870.

[Coh, 92] P. COHENDET, P. LLERENA et B. MUTEL,

Chapitre "Flexibilité et mise en cohérence des données de production", dans "Les nouvelles rationalisations de la production", pp. 25-41, G. de Terssac et P. Dubois, Cépaduès Éditions, 1992.

[Com, 91] M. COMBACAU,

"Commande et surveillance des systèmes à événements discrets complexes : application aux ateliers flexibles", Thèse de doctorat, Université Paul Sabatier de Toulouse, décembre 1991.

[Com, 98] M. COMBACAU, E. ZAMAÏ, A. CHAILLET-SUBIAS,

"Monitoring Strategies as Control Structure of Monitoring Architectures Based on Discrete Event System Applications", Nabeul-Hammamet, Tunisia, April 1998.

[Com, 00] M. COMBACAU, P. BERRUET, E. ZAMAÏ et al

"Supervision and Monitoring of Production Systems", Seconde Conférence Management et Conduite en Production et Logistique, MCPL'2000, Grenoble, juillet 2000.

[Cra, 89] E. CRAYE,

"De la modélisation à l'implantation automatisée de la commande hiérarchisée de cellules de production flexibles dans l'industrie manufacturière", Thèse de doctorat, Université des sciences et technologies de Lille, janvier 1989.

[Cru, 91] D. CRUETTE,

"Méthodologie de conception des systèmes complexes à événements discrets: Application à la conception et à la validation hiérarchisée de la commande de cellules flexibles de production dans l'industrie manufacturière", Thèse de doctorat, Université des Sciences et Technologies de Lille 1, février 1991.

[Dan, 99/a] N. DANGOUMAU, S. EL KHATTABI, E. CRAYE,

"Modèle de fonction en vue de la gestion des modes des systèmes flexibles de production", JDA'99, Nancy, 21 - 23 septembre 1999, pp.313-316.

[Dan, 99/b] N. DANGOUMAU, S. EL KHATTABI, E. CRAYE,
"Design and Management of Flexible Manufacturing System's modes", Advanced Computer Systems (ACS'99), Szczecin (POLAND), November 1999, pp. 417-422.

[Dan, 00/a] N. DANGOUMAU, A.K.A. TOGUYENI, S. EL KHATTABI, E. CRAYE,
"The design of an alarm processing system based on functional and behavioral modeling", IMACS World Congress 2000, Lausanne (Switzerland), August 2000.

[Dan, 00/b] N. DANGOUMAU, A.K.A. TOGUYENI, S. EL KHATTABI, E. CRAYE,
"Modes Management for Automated Production Systems", WAC'2000, Seventh International Symposium on Manufacturing with Applications (ISOMA), Maui (Hawaii), June 2000.

[Dan, 00/c] N. DANGOUMAU, A.K.A. TOGUYENI, M. DUPAS, E. CRAYE,
"Reconfiguration Process For Automated Production Systems", MCPL'2000, Grenoble, Juillet 2000.

[Dan, 00/d] N. DANGOUMAU, A.K.A. TOGUYENI, E. CRAYE,
"Functional and Behavioral modeling for Dependability in Automated Production Systems". Journal of Systems and Control Engineering, soumis.

[Dav, 92] R. DAVID et H. ALLA,
"Du grafcet aux réseaux de Petri", Édition Hermes, 1992.

[Del, 89] J.-L. DELCUVELLERIE,
"Ingénierie des systèmes d'automatisation de production : connaissances en conception des architectures de systèmes informatisés d'automatisation et outil d'analyse de la robustesse aux défaillances d'architectures réparties", Thèse de doctorat, Institut National Polytechnique de Lorraine, Nancy, mars 1989.

[Dum, 99] J.-J. DUMERY,
"Un langage de spécification pour la conception structurée de la commande des systèmes à événements discrets", Thèse de doctorat, École Centrale de Paris, décembre 1999.

[Dup, 99] M. DUPAS, Y. SALLEZ, T. BERGER, R. SOENEN,
"Reconfiguration des systèmes automatisés de production", 3° Congrès International de Génie Industriel, Montréal (Canada), 1999, vol. 3, pp. 2007- 2012.

[EDF, 99] E. CRAYE, N. DANGOUMAU *et al.*,
"Analyse du SRI et filtrage d'alarmes", Rapport de fin de contrat EDF Réf P31/BO2970/EP885, 1999.

[Elk, 93] S. EL KHATTABI,

"Intégration de la surveillance de bas niveau dans la conception des systèmes à événements discrets : application aux systèmes de production flexibles", Thèse de doctorat, Université des Sciences et Technologies de Lille, septembre 1993.

[Ers, 88] J. ERSCHLER et G. de TERSSAC,

"Flexibilité et rôle de l'opérateur humain dans l'automatisation intégrée de production", Rapport LAAS, Toulouse, mars 88.

[Geh, 99] A. -L. GEHIN, M. STAROSWIECKI,

"Modèle de description d'un système automatisé tolérant aux fautes.", MSR'99, pp. 101-110.

[Gen, 00] J.-C. GENTINA, O. KORBAA,

"De l'apport spécifique des réseaux de Petri temporisés à l'optimisation de performances des SFPM en fonctionnement cyclique et à l'ordonnancement cyclique de la production". CIFA'2000 Conférence Internationale Francophone d'Automatique, Lille (France), pp214-223, juillet 2000.

[Get, 94] E. GETAN,

"Une contribution à la productique : modélisation de données pour la maintenance intégrée des systèmes automatisés de production", Thèse de doctorat, École Centrale de Paris, décembre 1994.

[Got, 93] GOThA,

"Les problèmes d'ordonnancement", Recherche opérationnelle, vol. 27, n° 1, 1993, pp. 77-150.

[Gus, 95] S.-O. GUSTAVSSON,

"Flexible Manufacturing Systems: An Investigation For Research And Applications", Flexible Manufacturing Systems: Recent Developments, Elsevier (A. Raouf, M. Ben-Daya ed.), 1995, pp. 3-44.

[Har, 87] D. HAREL,

"StatCharts: a visual formalism for complex system", Science Computer Program, June 87, Vol. 8, n° 3, pp. 514-530.

[Huv, 94] B. HUVENOIT,

"De la conception à l'implantation de la commande modulaire et hiérarchisée de systèmes flexibles de production manufacturière", Thèse de doctorat, Université des Sciences et Technologies de Lille, octobre 1994.

[IEC61] IEC 61512-1,

"Batch Control – Part 1: Models and Terminology", International Standard IEC/CEI 61512-1, 1997.

[Ise, 96] R. ISERMANN, P. BALLE,

"Trends in the application of model based fault detection and diagnosis of technical processes", 13th IFAC World Congress, San Francisco, USA, 30 June – 5 July 1996.

[Ker, 96] L. KERMAD,

"Contribution à la supervision et à la gestion des modes et des configurations des systèmes flexibles de production manufacturière", Thèse de doctorat, Université des Sciences et Technologies de Lille, janvier 96.

[Kor, 98] O. KORBAA,

"Commande cyclique des systèmes flexibles de production manufacturière à l'aide des réseaux de Petri : de la planification à l'ordonnancement des régimes transitoires", Thèse de doctorat, Université des Sciences et Technologies de Lille, 9 juillet 1998.

[Lap, 85] J.C. LAPRIE,

"Sûreté de fonctionnement des systèmes informatiques et tolérance aux fautes : concepts de base", Technique et Science Informatiques (TSI), Vol. 4, No. 5, pp. 419-429.

[Lap, 95] J.C. LAPRIE et al,

"Guide de la sûreté de fonctionnement", Cépadues-Editions, Toulouse, mai 1995.

[Lem 91] J.L. LE MOIGNE,

"La modélisation des systèmes complexes", édition . Dunod, Paris, 1991.

[Lop, 99] P. LOPEZ,

"L'Ordonnancement", Collection Gestion, Édition ECONOMICA, Paris, 1999.

[Lus, 72] B. LUSSATO,

"Modèles cybernétiques, hommes, entreprises", Tome1, "Introduction critique aux théories des organisations", Édition Dunod, Paris, 1972.

[Ly, 99] F. LY,

"Contribution par la surveillance prédictive indirecte à l'optimisation de la maintenance dans les systèmes flexibles de production manufacturière", Thèse de doctorat, Université des Sciences et Technologies de Lille, mai 1999.

[Mab, 96] M. MABROUK,

"Proposition d'une méthode et d'un outil d'aide à la reconfiguration des systèmes automatisés de production", Thèse de doctorat, Université de Valenciennes et du Hainaut-Cambrésis, 28 mai 1996.

[Nab, 00] L. NABLI,
"Surveillance préventive conditionnelle prévisionnelle indirecte d'une unité de filature textile : approche par qualité", Thèse de doctorat, Université des Sciences et Technologies de Lille, avril 2000.

[NFX50] NFX50-400,
"Management des systèmes. Référentiel cadre", AFNOR, Citée par [Bas, 97].

[NFX60/a] NFX60-010,
"Maintenance – Vocabulaire de maintenance et de gestion des biens durables", AFNOR, juin 1984.

[NFX60/b] NFX60-500,
"Terminologie relative à la Fiabilité – Maintenabilité –Disponibilité", AFNOR, juin 1984.

[Nie, 92] E. NIEL, A. JUTARD,
"Contribution à la formalisation de la Sécurité Opérationnelle", Revue d'Automatique et de Productique Appliquée, Vol. 5, N° 2, 1992, pp. 57-64.

[Nou, 97] M. NOURELFATH,
"Extension de la théorie de la supervision à la surveillance et à la commande des systèmes à événements discrets : Application à la sécurité opérationnelle des systèmes de production", Thèse de Doctorat, LAI, Lyon, juillet 1997.

[Ohl, 95] H. OHL,
"Fonctionnements répétitifs de systèmes flexibles de production manufacturière : analyse et optimisation des performances à l'aide des Réseaux de Petri", Thèse de doctorat, Université des Sciences et Technologies de Lille, octobre 1995.

[Oko, 91] U. OKONGWU et M. CASTAGNE,
"Analyse de la flexibilité de la chaîne logistique de l'entreprise : une approche systémique et pragmatique", 3ème Congrès International – Le Génie Industriel, pp. 593-603, Tours (France), mars 1991.

[Par, 92] T. PARAYRE,
"Vers une méthode d'exploitation des systèmes automatisés de production", Thèse de doctorat, Université de Valenciennes et du Hainaut-Cambrésis, mars 1992.

[Rak, 93] M.P. RAKOTOSON,
"Synthèse des caractéristiques et technique de développement de la commande des systèmes dis-continus : application aux systèmes de production flexible Batchs", Thèse de doctorat, Université des Sciences et Technologies de Lille, juillet 1993.

[Roj 96] J. ROJAS RAMIREZ,

"Etude des modes de marche des systèmes automatisés de production pour la définition des stratégies de conduite", Thèse de doctorat, Université de Valenciennes et du Hainaut Cambrésis, janvier 1996.

[Sah, 92] A.E.K. SAHRAOUI,

"An approach for monitoring discrete event systems", AFCET APII, Vol. 26, N° 2, 1992, pp. 91-106.

[Sim, 99/a] Z. SIMEU-ABAZI,

"Sûreté de Fonctionnement des Systèmes de Production", École d'été de Grenoble, session 20, 6-10 septembre 1999.

[Sim, 99/b] Simulog,

"Esterel Studio: Tutorial and Reference Manual", Simulog, 1999.

[Sta 98] STAROSWIECKI M., GEHIN A.L.

"Analysis of system reconfigurbility using generic component models", International Conference on Control'98,Swansea (GB), September 1-4, 1998, pp. 1157-1162.

[Taw, 95] R. TAWEGOUM,

"Contrôle temps réel du déroulement des opérations dans les systèmes de production flexibles", Thèse de doctorat, Université des Sciences et Technologies de Lille, 25 avril 1995.

[Tog, 92] A.K.A. TOGUYENI,

"Surveillance et diagnostic en ligne dans les ateliers flexibles de l'industrie manufacturière", Thèse de doctorat, Université des Sciences et Technologies de Lille, 12 novembre 1992.

[Tog, 96] A.K.A. TOGUYENI, S. ELKHATTABI, E. CRAYE,

"Functional and/or Structural approach for the Supervision of Flexible Manufacturing Systems", CESA'96 IMACS, 9-13 july 1996, Symp. on Discrete Event and Manufacturing Systems, pp. 716-721.

[Tog, 00] A.K.A. TOGUYENI,

"Contribution à la sûreté de fonctionnement des systèmes flexibles de production manufacturière", Habilitation à Diriger des Recherches, Université des Sciences et Technologies de Lille, 2000.

[Ver, 89] C. VERLINDE

"Contribution à l'étude des architectures de systèmes automatisés", Thèse de doctorat, Institut National Polytechnique de Lorraine, Nancy, 1989. Citée par [Bon, 93].

[Vil, 88] A. VILLEMEUR,

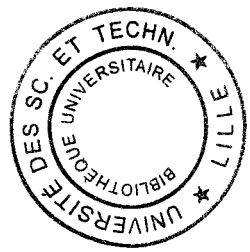
"Sûreté de fonctionnement des systèmes industriels", Éditions Eyrolles, Paris, 1998.

[Zam, 97] E. ZAMAÏ,

"Architecture de Surveillance-Commande pour les Systèmes à Événements Discrets Complexes", Thèse de doctorat, Université Paul Sabatier de Toulouse, septembre 1997.

[Zam, 98] E. ZAMAÏ, M. COMBACAU, A. CHAILLET-SUBIAS,

"Models and Strategies for Monitoring of Flexible Manufacturing Systems", 9th Symposium on Information Control in Manufacturing, Nancy-Metz, France, June 1998, pp. 365-370,

[Zwi, 95] G. ZWINGELSTEIN,

"Diagnostic des défaillances : théorie et pratique pour les systèmes industriels", Traité des Nouvelles Technologies, Éditions Hermes, 1995.