UVHC
Université de Valenciennes
et du Hainaut Cambrésis

LAMIH
Laboratoire d'Automatique
et de Mécanique
Industrielles et Humaines

N° d'ordre : 98 - 34

THÈSE

présentée à

l'Université de Valenciennes et du Hainaut Cambrésis

pour obtenir le titre de

DOCTEUR

Spécialité

Automatique Industrielle et Humaine

par

Laurent GRUDZIEN

Maître ès Sciences et Techniques

Contribution à l'intégration de la sûreté de fonctionnement au sein d'une démarche de conception multimétiers

Soutenue le 07 Janvier 1999 devant la commission d'examen :

M. DUBUISSON Bernard	**Rapporteur**
M. BERTRAND Jean-Claude	**Rapporteur**
M. PRUNET François	**Examinateur**
M. TAHON Christian	**Examinateur**
M. LIGERON Jean-Claude	**Examinateur**
M. SOENEN René	**Directeur de thèse**

UVHC
Université de Valenciennes
et du Hainaut Cambrésis

LAMIH
Laboratoire d'Automatique
et de Mécanique
Industrielles et Humaines

N° d'ordre : 98 - 34

THÈSE

présentée à

l'Université de Valenciennes et du Hainaut Cambrésis

pour obtenir le titre de

DOCTEUR

Spécialité

Automatique Industrielle et Humaine

par

Laurent GRUDZIEN

Maître ès Sciences et Techniques

Contribution à l'intégration de la sûreté de fonctionnement au sein d'une démarche de conception multimétiers

Soutenue le 07 Janvier 1999 devant la commission d'examen :

M. DUBUISSON Bernard	**Rapporteur**
M. BERTRAND Jean-Claude	**Rapporteur**
M. PRUNET François	**Examinateur**
M. TAHON Christian	**Examinateur**
M. LIGERON Jean-Claude	**Examinateur**
M. SOENEN René	**Directeur de thèse**

À ma muse

À mes parents

REMERCIEMENTS

Les travaux présentés dans ce mémoire ont été réalisés au Laboratoire d'Automatique et de Mécanique Industrielles et Humaines de l'Université de Valenciennes et du Hainaut-Cambrésis, au sein du groupe de recherches en Génie Industriel et Logiciel dirigé par le professeur René SOENEN.

Je tiens à lui exprimer toute ma gratitude pour m'avoir accueilli dans ce laboratoire, pour m'avoir guidé dans mes recherches ainsi que pour la confiance qu'il m'a témoignée.

Je remercie vivement Monsieur Bernard DUBUISSON, Professeur à l'Université de Technologie de Compiègne et Monsieur Jean-Claude BERTRAND, Professeur à l'Université d'Aix-Marseille pour avoir accepté d'être les rapporteurs de ce travail.

Mes remerciements vont également à Monsieur François PRUNET, Professeur à l'Université de Montpellier et Monsieur Christian TAHON, Professeur à l'Université de Valenciennes qui ont accepté d'examiner les travaux présentés dans ce mémoire.

Je remercie également Monsieur Jean-Claude LIGERON, PDG de la société LIGERON SA, d'avoir accepté de prendre part à ce jury et d'examiner ces travaux.

Je tiens aussi à adresser *A very special thanks* à Pierre, pour le temps qu'il a consacré à me lire (cela n'a pas été facile), à me corriger (cela a été très long) et surtout à me conseiller afin d'améliorer la qualité de ce mémoire. Je fais par ailleurs toutes mes excuses à Jacqueline pour lui avoir tant monopolisé son gentil mari.

Je ne peux oublier tous les membres de ma famille, mes amis qui ont fait preuve de beaucoup de patience et qui m'ont toujours soutenu. Un merci tout particulier à Christophe qui, en plus de cela, a accepté de me relire.

Mes remerciements vont enfin à tous les membres du laboratoire et plus particulièrement à ceux de " l'équipe du bas ", pour leurs encouragements et pour la bonne humeur qu'ils ont su entretenir dans le bureau.

TABLE DES MATIÈRES

CHAPITRE 2 : MODÈLE DE PRODUIT

CHAPITRE 3 : PROCESSUS DE CONCEPTION

CHAPITRE 4 : SPÉCIFICATION DU SYSTÈME D'AIDE À LA CONCEPTION DE SYSTÈMES SÛRS

CHAPITRE 5 : VALIDATION DE LA DÉMARCHE

TABLE DES MATIÈRES DES ANNEXES

INTRODUCTION GÉNÉRALE

Dans les systèmes de production actuels constitués d'éléments de plus en plus automatisés, sophistiqués et multitechnologies, les dysfonctionnements potentiels sont nombreux et extrêmement variés. De plus, certains d'entre eux peuvent entraîner des conséquences graves sur les plans humain, technologique et/ou économique. Il convient par conséquent de prévenir ces dysfonctionnements ou, au moins, d'en réduire les effets. Cet objectif peut être obtenu par la mise en place d'une politique de maîtrise des risques adaptée au contexte d'exploitation de chaque système de production.

Cette politique a pour but tout d'abord, d'identifier les risques (humains, technologiques, économiques) pouvant être associés à chaque dysfonctionnement potentiel, de les évaluer ensuite et enfin, de les éliminer sinon de les réduire à un niveau jugé acceptable. La dernière phase passe par la définition et la mise en oeuvre d'actions (préventives ou correctives) tout au long du cycle de vie du système.

Selon les domaines industriels, les techniques utilisées pour identifier, analyser, évaluer et, éventuellement, réduire les risques sont regroupées sous des termes différents. Cependant, le terme qui émerge actuellement est celui de Sûreté de fonctionnement. Celle-ci est définie comme *la propriété d'un produit, telle que ses utilisateurs peuvent accorder une confiance justifiée dans le service qu'il leur délivre* /Norme NF X60-500/. Elle est plus généralement appelée Science des défaillances et intègre dans une même démarche les aspects fiabilité, maintenabilité, disponibilité et sécurité. Elle intervient à la fois au niveau du produit fini et en phase de conception des systèmes. Dans ce cadre, elle cherche à mettre en évidence les meilleurs compromis sécurité — fiabilité et disponibilité — productivité, conduisant alors à des systèmes à la fois non dangereux et rentables.

Les travaux présentés dans ce mémoire de thèse s'intègrent dans cette problématique. Ils visent à intégrer, au sein d'une démarche de spécification et de conception développée au laboratoire, le concept de sûreté de fonctionnement. A partir d'exigences définies par le client dans son cahier des charges, l'objectif des travaux est d'aboutir à un produit qui soit sûr de fonctionnement par la mise en oeuvre entre autres de moyens de surveillance et de diagnostic de défaillances.

Pour présenter notre contribution, ce mémoire s'articule autour de cinq chapitres.

Le premier chapitre concerne "la conception de systèmes sûrs". Il présente en cela les deux aspects essentiels du cadre de nos travaux : la conception et la sûreté de fonctionnement.

La partie "conception" consiste en une présentation de la démarche de spécification et de conception développée au laboratoire. Nous verrons qu'elle intègre deux notions importantes : le modèle de produit et le processus de conception.

La partie "sûreté de fonctionnement" vise à expliciter les différentes notions qu'elle intègre ainsi que les différentes méthodes permettant son évaluation. L'objectif du chapitre est de retenir les méthodes qui nous permettront d'évaluer la sûreté de fonctionnement dans le cadre de cette démarche de conception.

Dans le second chapitre, nous décrivons le modèle de produit associé à la démarche de conception. Cette description se fait d'un point de vue "Exploitation" par la présentation des différents concepts que nous intégrons au modèle pour concevoir un système sûr de fonctionnement. Pour cela, nous donnons pour chacun des cinq niveaux de représentation du modèle de produit, les différents concepts relatifs à la sûreté de fonctionnement que nous avons identifiés. Nous intégrons ainsi au modèle de produit un autre point de vue dont l'objectif est de rendre sûr le système conçu lors de son exploitation.

L'instanciation des concepts du modèle de produit se fait au travers du processus de conception présenté dans le cadre du troisième chapitre. Ainsi, nous décrivons tout d'abord le méta-modèle d'élaboration des concepts qui, par l'intermédiaire de différentes questions, permet de définir les opérations conduisant à l'instanciation d'un concept d'un niveau de représentation donné. Nous présentons ensuite le modèle d'élaboration des concepts associé à chaque niveau de représentation c'est-à-dire les opérations nécessaires à l'instanciation des concepts dédiés à la sûreté de fonctionnement, que nous avons intégrés au modèle de produit.

Le processus de conception tel qu'il a été défini, est non monotone c'est-à-dire que les concepts ne sont pas instanciés dans l'ordre dans lequel ils sont présentés dans ce mémoire. De même, il n'est pas également nécessaire de mettre en oeuvre tous les concepts d'un niveau de représentation donné pour passer à un autre niveau.

Dans le quatrième chapitre, nous spécifions l'environnement informatique permettant de représenter les concepts et les modèles décrits dans les chapitres précédents. Nous décrivons par la technique de modélisation par objet OMT (Object Modelling Technique), la structure de données associée à l'outil informatique d'aide à la conception de système sûr. Nous présenterons auparavant les différentes caractéristiques de cette méthode.

Afin d'évaluer et de valider nos propositions, nous présentons, dans le cinquième chapitre, différents scénarios de conception appliqués à un exemple concret. L'objectif de ce chapitre est, d'une part, d'illustrer la non monotonie du processus de conception et d'autre part, de montrer que la sûreté de fonctionnement est prise en compte dans la démarche de spécification et de conception développée au laboratoire.

CHAPITRE 1

CONCEPTION DE SYSTEMES SÛRS

INTRODUCTION

Pour être compétitive et s'adapter à un marché toujours plus concurrentiel, toute entreprise doit disposer d'un outil de production lui assurant une productivité maximale, au moindre coût de production et lui permettant de fabriquer des produits de bonne qualité. L'obtention de telles performances passe nécessairement par une automatisation et une optimisation technique des équipements, débouchant sur l'utilisation de techniques très sophistiquées et complexes. Le moindre dysfonctionnement peut avoir dans ces conditions des conséquences critiques voire catastrophiques.

Dans ce contexte, la sûreté de fonctionnement est devenue aujourd'hui un véritable enjeu car elle joue un rôle important dans la maîtrise des risques qu'ils soient économiques, humains ou environnementaux. Les caractéristiques de sûreté de fonctionnement qu'un système devra respecter lors de son exploitation sont spécifiées dès sa conception .

Dans ce chapitre, nous allons présenter le domaine de la sûreté de fonctionnement. Après une brève présentation des moyens permettant d'obtenir les caractéristiques de sûreté de fonc-tionnement, nous décrivons dans la seconde partie le cadre général dans lequel s'intègrent nos travaux : la conception. Après une courte description des méthodes existantes, nous décrivons la démarche de conception qui a été élaborée au sein du laboratoire.

Nous présentons dans la troisième partie du chapitre la sûreté de fonctionnement. Cette présentation s'articulera autour de deux points : la description des caractéristiques de sûreté de fonctionnement et les méthodes d'analyse de cette sûreté.

La quatrième partie du chapitre concernera les méthodes d'évaluation de la sûreté de fonctionnement, tant qualitatives que quantitatives.

1. Obtention des caractéristiques de sûreté de fonctionnement

Il est aujourd'hui fréquent de voir apparaître dans les cahiers des charges pour la conception d'un système les caractéristiques relatives à sa fiabilité, sa disponibilité ou sa sécurité. Elles s'expriment de façon quantitative (95 % de disponibilité, 0 accident) ou de façon qualitative (système fiable, réparable). Afin de s'approcher le plus possible voire d'atteindre ces contraintes, les concepteurs ont à leur disposition quatre solutions principales :

— choisir des solutions plus fiables ;

— mettre en redondance les fonctions ou les éléments jugés à risque ;

— mettre en place une politique de maintenance appropriée ;

— proposer une solution hybride mêlant plusieurs des solutions précédentes.

1.1. Choix de solutions plus fiables

Une première possibilité qui s'offre aux concepteurs pour aboutir à des systèmes sûrs de fonctionnement, est de choisir des solutions plus fiables que celles proposées ou utilisées dans des conceptions antérieures (technologies éprouvées, composants dont le taux de défaillance est faible). Ces choix peuvent se faire sur la base d'expériences passées ayant donné entière satisfaction (retour d'expérience) ou par interrogation de banques de données de fiabilité.

Cette solution est privilégiée lorsque l'on souhaite disposer de produits homogènes, constitués des mêmes éléments que l'on connaît et maîtrise. Elle peut également être choisie lorsque l'on peut mettre en place un composant dont le rapport coût / efficacité est supérieur au composant choisi initialement. Enfin, des problèmes d'accessibilité pour intervention

nécessitée par une défaillance peuvent également être une raison du choix de la mise en place de composants plus fiables.

1.2. Mise en redondance

Mettre en redondance des fonctions ou des éléments consiste à utiliser, pour un même service, plusieurs composants ou modules strictement identiques ou à reporter la tâche sur un autre processus disponible donnant des résultats semblables malgré une technologie parfois différente. On distingue à ce niveau :

— la redondance active où tous les moyens utilisés pour assurer le service considéré fonctionnent simultanément ;

— la redondance passive où la défaillance du composant principal peut être supplée par des composants en réserve ;

— la redondance m/n où l'on exige qu'au moins m composants parmi les n placés en parallèle soient non défaillants pour que le système fonctionne.

Cette mise en redondance a pour objectif d'améliorer la sûreté de fonctionnement des systèmes. Le choix de l'utilisation de plusieurs éléments en parallèle pour réaliser une même fonction doit se faire dès la conception du système afin de prendre en considération les problèmes de commande (pour mettre en fonctionnement le composant de secours),de dimensionnement et autres. Il est donc important de déceler les fonctions ou les composants susceptibles de mettre en cause la mission du système et de prévoir alors leur redondance.

Cette solution est à privilégier lorsque la sécurité (des biens et/ou des personnes) est en jeu. Les conséquences financières liées à la défaillance du composant principal peuvent alors être largement supérieures au coût du composant à mettre en redondance. Le choix du type de redondance sera fonction : des risques encourus en cas de défaillance, de la fonction que le composant remplit dans le système global, des moyens de détection de défaillances qu'il est possible de mettre en œuvre, ...

Si cette opération n'est pas possible (coût, topologie insuffisante ou incompatible, ...), la mise en place d'une politique de maintenance appropriée s'avère alors nécessaire.

1.3. La maintenance

La maintenance regroupe /AFNOR 94/ *toutes les activités destinées à maintenir ou à rétablir un bien dans un état ou dans des conditions données de sûreté de fonctionnement, pour accomplir une fonction requise.* Ces activités sont une combinaison d'activités techniques, administratives et de management. Maintenir c'est donc effectuer, au coût global optimum, des opérations qui permettent de conserver le potentiel du matériel pour assurer la continuité et la qualité de service. Une politique de maintenance est essentiellement basée sur quatre types de stratégies /SOURIS 90/ : la maintenance corrective, la maintenance préventive systématique, la maintenance préventive conditionnelle /MOBLEY 92//BOULENGER 88/ et la maintenance améliorative.

Sur les éléments à risques, une politique de maintenance préventive systématique pourra être mise en place afin de les remplacer par des composants neufs. Pour d'autres, c'est une maintenance préventive conditionnelle qui sera préférée et mise en place afin de ne changer que les éléments effectivement dégradés ou défaillants pour ainsi réduire les coûts. Il est nécessaire pour cela que la dégradation de ces éléments puisse être caractérisée par un ou plusieurs paramètres d'une part, et que, des moyens de surveillance et de diagnostic soient mis en place sur le système d'autre part ; ceci afin de détecter les dégradations et diagnostiquer leurs origines. Ceci doit être mis en œuvre dès la conception afin de définir les paramètres à surveiller, prévoir les capteurs et leurs emplacements. Nos travaux de recherche s'inscrivent dans ce cadre.

Cette solution sera envisagée lorsque la défaillance (ou la dégradation) des composants peut être suivie par des techniques particulières (maintenance conditionnelle) dont le coût est inférieur à celui d'un composant redondant. Elle peut également être utilisée pour des composants dont la défaillance n'entraîne pas de risque pour la sécurité (humaine et matérielle). Elle sera privilégiée lorsque le remplacement du composant défaillant peut être effectué rapidement et si son coût de défaillance est faible.

Nous allons dans ce qui suit présenter succinctement les méthodes de conception que l'on trouve dans la littérature, avant de décrire plus précisément celle proposée par le laboratoire et dans laquelle s'intègrent nos travaux.

2. La conception

2.1. Les approches de conception

Deux approches de conception peuvent être distinguées dans la littérature /JACQUET 98/. La première dite Axiomatique /SUH 90//YOSHIKAWA 89/ est basée sur la définition de plusieurs domaines (client, fonctionnel, physique, ...) et d'axiomes devant permettre une bonne conception.

La seconde approche dite Algorithmique /PAHL 84/ se compose d'un ensemble de phases (spécification, conception détaillée, ...) et d'étapes visant à définir progressivement le système à concevoir.

Même si l'approche axiomatique a l'avantage de fixer le cadre du travail, elle ne précise malheureusement pas comment agir au sein de ce cadre. Quant à l'approche algorithmique, son organisation séquentielle ainsi que son manque de précision sur les différentes étapes composant chacune des phases font qu'elle va à l'encontre des concepts définis par l'ingénierie simultanée.

De plus, ces deux approches ne prennent pas en compte les aspects *conception pour l'exploitation* et notamment les concepts relatifs à la maintenance. Or, ces concepts prennent aujourd'hui de plus en plus d'importance dans la phase de conception, dans le but de réduire le coût global de possession d'un produit.

Pour résoudre ces problèmes, une démarche de conception a été développée au sein du laboratoire. Celle-ci est "localement algorithmique" non monotone et comporte une composante axiomatique. Cette démarche fait référence à deux aspects : Modèle de produit et Processus de conception. Elle fait l'objet du paragraphe suivant.

2.2. Modèle de produit et processus de conception

Ces deux notions ont été définies par /KRAUSE 93/. Le modèle de produit consiste en une accumulation logique de toutes les informations qui sont en rapport avec le produit durant son cycle de vie. Le processus de conception est communément représenté comme le travail nécessaire au développement du produit ou comme le processus de modélisation du produit faisant référence à un ensemble de fonctions (technique, gestion) nécessaires à la transformation de l'idée initiale en produit final. Nous entendons par produit tout système devant rendre un service.

La démarche proposée au laboratoire est assez similaire. En ce qui concerne le premier aspect, celui-ci prend en compte la modélisation du produit au cours de la conception par l'intermédiaire du modèle du produit. Celui-ci est décrit par cinq niveaux de modélisation. Ils traduisent le passage depuis l'expression d'un besoin (cahier des charges client) jusqu'à sa

solution matérielle (produit). Chaque niveau fait référence à un ensemble d'entités ou concepts permettant de modéliser les différents aspects du produit.

Le second aspect explicite quant à lui la dynamique qui existe entre chaque niveau de modélisation du produit à travers le processus de conception. Il fera l'objet du troisième chapitre.

Nous allons maintenant décrire les cinq niveaux de modélisation qui composent la démarche.

2.3. Présentation des différents niveaux de modélisation

Les cinq niveaux de modélisation du modèle de produit (Figure 1) représentent une partie des informations indispensables à la définition du modèle de produit. Ces informations sont générées au cours du processus de conception. Ainsi, quelque soit le processus de conception adopté, les concepts associés à chaque niveau de modélisation devront être renseignés à un moment ou à un autre. Les niveaux de modélisation qui ont été identifiés sont présentés dans les paragraphes ci-dessous.

2.3.1. Niveau Représentation des besoins

Ce niveau permet de modéliser, de façon formelle, les besoins du client. Ces besoins sont transcrits, exprimés sous forme littérale, en un ensemble d'exigences (fonctions) spécifiant, d'une part, les services que le système doit satisfaire, et d'autre part, un ensemble de contraintes (fonctions) que celui-ci doit respecter. Ces exigences sont exprimées de sorte que leur cohérence soit validée. Ce niveau a donc pour objectif de définir les différentes fonctions (service, contraintes) que le système doit remplir. Les modèles utilisés sont généralement ceux issus de l'Analyse de la valeur.

C'est à ce niveau que sont également définies les exigences de sûreté de fonctionnement du système. Celles-ci regroupent les caractéristiques de fiabilité, de maintenabilité, de disponibilité (conjonction des deux caractéristiques précédentes) et de sécurité. Elles peuvent s'exprimer de façon qualitative ou quantitative.

2.3.2. Niveau Représentation des exigences fonctionnelles

Ce niveau a pour objectif de modéliser l'ensemble des solutions susceptibles de répondre à chaque service tout en respectant les contraintes ou limites spécifiées par le client. Aucune solution ne doit être écartée *a priori*, tous les moyens permettant de satisfaire le besoin doivent être recensés. Ce niveau de modélisation permet en définitive de décrire, de façon synthétique, les comportements (chaînes de fonctions) que le système pourra adopter pour accomplir sa mission. Les différents principes (fluidique, magnétique, ...) susceptibles de permettre leur mise en œuvre sont également définis. Nous obtenons alors des chaînes de fonctions opératoires.

La définition des chaînes opératoires et des principes retenus pour leur mise en oeuvre, met en évidence les modes de fonctionnement normaux et anormaux du système. Il convient alors de définir des moyens permettant de détecter et d'effectuer le diagnostic d'origine de ces fonctionnements anormaux ou de contrôler la normalité du fonctionnement. C'est également à ce niveau que les moyens (au sens fonction) de mise en état de sécurité du système, lorsqu'un fonctionnement anormal survient, sont à définir.

2.3.3. Niveau Représentation technologique

Ce niveau décrit la structure technologique du système à concevoir. Il permet de représenter le système par l'intégration des points de vue des différents acteurs de la conception (automaticien, mécanicien, futurs exploitants, ...). Pour cela, certains aspects comporte-

mentaux (nominal, dégradé, défaillant, ...), modes d'exploitation (redondance, sécurité, ...) doivent être pris en compte.

A ce niveau, certaines solutions ont été définitivement rejetées. Il est alors possible d'affiner les moyens de détection et de diagnostic et les dispositifs de sécurité à mettre en œuvre. Il est aussi nécessaire de focaliser l'étude sur des éléments jugés plus importants que d'autres pour le système et sur lesquels la fiabilité, la sécurité (mise en redondance de fonction) et la maintenabilité seront à privilégier. Des contraintes concernant la modularité, la mise en place de technologies maîtrisées plutôt que de technologies nouvelles, ... peuvent être définies à ce niveau.

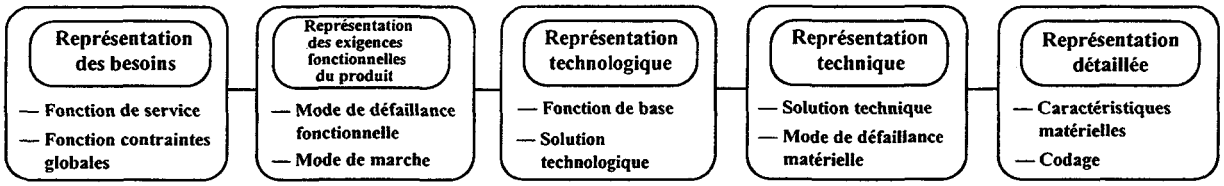

Figure 1 : Modèle de produit

2.3.4. Niveau Représentation technique

A ce niveau, l'objectif est de modéliser la structure technique du système. Les aspects dimensionnement et techniques de réalisation y sont considérés.

Nous définissons à ce niveau les différents composants matériels susceptibles de répondre aux besoins exprimés. Nous disposons alors d'informations sur leur taux de défaillance nous permettant d'élaborer les modèles mathématiques de fiabilité, de maintenabilité et de sécurité. Nous pouvons ainsi vérifier *a priori* que les exigences exprimées au niveau représentation des besoins sont satisfaites. Des contraintes concernant l'utilisation de composants standards plutôt que de prototypes peuvent être définies. Des procédures de maintenance préventive sur certains des éléments jugés sensibles peuvent également être précisées à ce stade. En cas de non-respect des exigences de sûreté, il sera nécessaire de remplacer les composants choisis par d'autres plus fiables qui nous permettront d'atteindre ces objectifs.

2.3.5. Niveau Représentation détaillée

Ce dernier niveau permet d'aboutir aux spécifications détaillées du système (la morphologie, les schémas de câblage de l'installation, le codage ...).

La structure finale du produit est définie au terme de cette étape. Les caractéristiques de sûreté du système sont vérifiées (en terme de fiabilité et de sécurité). Les moyens permettant d'assurer une maintenabilité suffisante ont été définis (gamme de démontage-remontage, dispositif de détection et de diagnostic de défaillance, procédures de maintenance préventive, ...).

Chacun de ces niveaux de représentation est commun à chaque acteur de la conception. Pour notre part, notre contribution se situe au niveau de la *conception pour l'exploitation* et plus particulièrement la *maintenance*. Nous cherchons à définir, dès ce stade, les moyens à mettre en place qui permettront de garantir les critères de sûreté de fonctionnement définis dans le cahier des charges du client. Ces moyens concernent surtout la surveillance et le diagnostic des défaillances des systèmes de production. Avant de définir les concepts propres à ces activités qui feront l'objet du second chapitre, nous allons tout d'abord définir ce qu'est la sûreté de fonctionnement et présenter les méthodes qui permettent de la caractériser.

3. Le domaine de la sûreté de fonctionnement

Pour faire face à la concurrence, toute entreprise doit se doter de produits (systèmes) très performants. Pour atteindre une telle qualité, ils peuvent être automatisés et intégrer différentes technologies ce qui augmente leur complexité. Il est pourtant nécessaire de maîtriser cette complexité /MOREAU 95/ et faire en sorte que les systèmes soient sûrs de fonctionnement, que les délais et les coûts quant à eux soient réduits. Pour atteindre de tels objectifs, il faut :

— minimiser les arrêts non prévus (pannes) par une amélioration de la fiabilité ;

— minimiser les temps d'intervention par la prise en compte de critères de maintenabilité ;

— accroître la disponibilité, concept recouvrant celui de fiabilité et de maintenabilité. C'est le rapport du temps pendant lequel le système peut être exploité sur le temps total ;

— mettre le système dans un état de sécurité en cas de panne (" failsafe") ;

— pouvoir exploiter le système en marche dégradée.

Il faut par conséquent chercher à obtenir un système qui soit sûr de fonctionnement c'est-à-dire /LEROY 92/ un système qui réalise la mission pour laquelle il a été conçu, sans incident mettant sa rentabilité en question et sans accident mettant la sécurité en jeu. Il est donc important de définir, dès l'élaboration du cahier des charges, les caractéristiques de sûreté de fonctionnement auxquelles le système devra répondre. Celles-ci sont donc définies dès le niveau représentation des besoins de la démarche de conception. Il conviendra ensuite de s'assurer que celles-ci sont bien respectées aux autres niveaux de modélisation.

3.1. Le concept de sûreté de fonctionnement

Le concept de sûreté de fonctionnement est associé à la notion de risque, laquelle peut être considérée comme une entité à deux dimensions : probabilité d'occurrence d'un événement redouté d'une part et gravité de ses conséquences d'autre part. Cette notion générale permet de caractériser aussi bien des événements catastrophiques mettant en cause la sécurité (faible probabilité d'occurrence, forte conséquence), que des événements mettant en cause la production des installations (forte probabilité d'occurrence, faible conséquence).

On peut donc exprimer le risque sous la forme :

$$R = f(Pr , G)$$

généralement écrite

$$R = Pr \times G$$

où Pr représente la probabilité (ou fréquence) d'apparition de la défaillance du système et G l'importance (ou la gravité) des conséquences du dysfonctionnement considéré. Ainsi, selon les objectifs visés (fiabilité, maintenabilité, disponibilité ou sécurité, les quatre caractéristiques de la sûreté de fonctionnement), l'étude peut prendre alors une direction différente qui ne doit pas conduire à négliger les autres axes de recherche : améliorer un aspect c'est parfois risquer d'en détériorer un autre et les systèmes obtenus peuvent alors être à l'opposé de ce que l'on souhaitait au départ. Ainsi, il est indispensable de traiter ces différents aspects simultanément afin de trouver des compromis en particulier entre sécurité/fiabilité d'une part et disponibilité/productivité d'autre part. Il convient donc de disposer de méthodes et d'outils permettant de contribuer à l'obtention de ces compromis.

Nous présentons, dans le paragraphe suivant, la démarche visant à atteindre ces objectifs.

3.2. L'analyse de la sûreté de fonctionnement des systèmes techniques

Une analyse de la sûreté de fonctionnement d'un système matériel se décompose en quatre phases principales successives /LEROY 92/ /VILLEMEUR 88/(Figure 2). L'objectif de cette analyse est de rechercher la probabilité d'occurrence ainsi que la gravité des conséquences des événements redoutés au niveau du système à concevoir. Nous décrivons ci-dessous chacune de ces phases tout en les positionnant par rapport aux cinq niveaux de représentation du modèle de produit présenté au paragraphe 2.3.

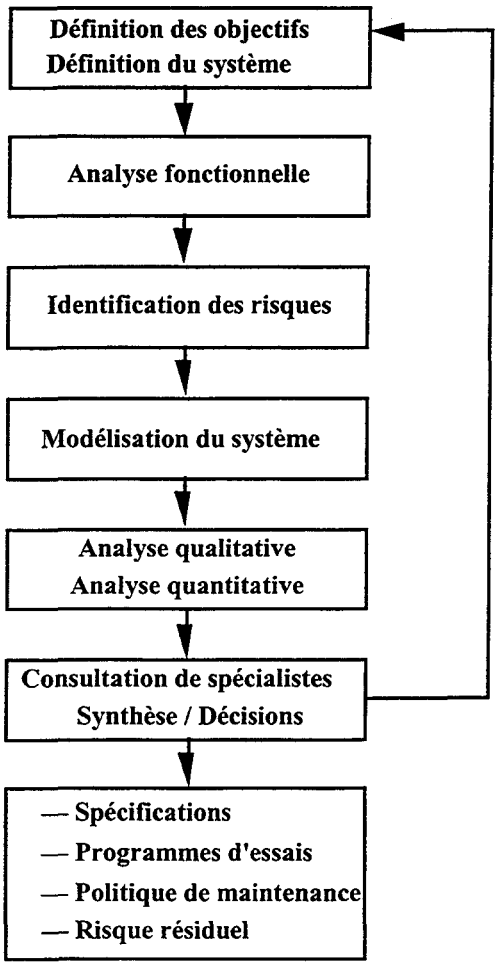

Figure 2 : Principales phases de l'analyse de sûreté de fonctionnement /LEROY 92/

3.2.1. Définition des objectifs

Les objectifs de l'étude, qui peuvent varier selon le paramètre à évaluer (fiabilité, disponibilité, productivité, ...), le type de système à étudier, l'étape de la conception ou encore le niveau de détail désiré, doivent être définis précisément de même que le seront le système à étudier et son environnement. Cette première phase se situe au niveau représentation du besoin.

3.2.2. Analyse fonctionnelle

Les méthodes d'analyse fonctionnelle /FADIER 90/ permettent de décrire les caractéristiques d'un système et les fonctions qu'on en attend. Elles apportent ainsi une aide importante pour la compréhension et la description synthétique des modes de fonctionnement nominaux du système étudié. Cette phase très importante dans une analyse de sûreté de fonctionnement est associée au niveau représentation des exigences fonctionnelles du besoin. La définition des fonctions opératoires est le résultat de cette phase.

A partir de ces informations, une analyse des risques peut être menée. Elle vise, par l'utilisation d'une ou de plusieurs méthodes, à rechercher les événements susceptibles de contrarier les objectifs fixés. Chacune des méthodes a pour objectif de rechercher la gravité de chacun des événements redoutés identifiés ainsi que de quantifier leur probabilité ou fréquence d'apparition. Nous présentons, dans le paragraphe suivant, les méthodes les plus couramment utilisées.

3.2.3. Identification des risques

C'est au regard des objectifs fixés que se fera l'identification des risques potentiels du système. Les méthodes utilisées procèdent d'une démarche inductive (partant d'une cause quelconque, elles cherchent à mettre en évidence les effets sur le système étudié) ou d'une démarche déductive (elles partent d'un effet pour essayer de remonter à ses causes). Elles s'appuient sur une décomposition du système en sous-systèmes, fonctions, composants ..., à partir de laquelle les éléments dangereux, les déviations ou les défaillances dangereuses sont identifiés afin de déterminer les conséquences sur le système lui-même et/ou sur les systèmes adjacents. Elles cherchent aussi à vérifier que pour chaque risque potentiel mis en évidence, les moyens de détection appropriés sont en place. Les principales méthodes d'analyse prévisionnelle de la sûreté de fonctionnement sont :

— l'Analyse des Modes de Défaillance et de leurs Effets (AMDE). L'AMDE /VILLEMEUR 88/ est une méthode inductive d'analyse des causes et des effets des défaillances d'un système. Elle a pour objectifs l'évaluation des effets de chaque mode de défaillance des composants d'un système sur ses différentes fonctions et l'identification des modes de défaillance ayant des effets importants sur la disponibilité, la fiabilité, la maintenabilité ou la sécurité de ce système. Les résultats de l'analyse sont généralement présentés sous la forme d'un tableau à colonnes (voir Tableau 1). Les trois notions, mode, cause et mécanisme de défaillance, sont trois composantes essentielles pour la mise en œuvre de l'analyse AMDE. Une extension courante de l'AMDE est l'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC). Elle consiste à ajouter à l'analyse précédente, une analyse de criticité qui a pour but d'évaluer, pour chaque mode de défaillance, le couple (gravité, fréquence d'apparition). La méthode AMDE(C) qui fait l'objet d'une normalisation internationale /AFNOR 88/ est devenue réglementaire dans les études de sécurité de nombreux secteurs de l'industrie. En outre, ses caractéristiques générales permettent sa mise en œuvre aux différents stades de la conception, de la réalisation ou de l'exploitation des systèmes.

Identification du composant (Repères, désignation, type, lieu)	Fonction s États	Mode de défaillance	Causes possibles d'une défaillance (internes ou externes)	Effets sur le système	Effets sur les systèmes externes	Moyens de détection	Fréquence des inspections ou essais	Observations

Tableau 1 : Exemple de tableau AMDE /VILLEMEUR 88/

Les principales améliorations apportées récemment à la méthode AMDEC sont :

- l'élaboration de méthodologies /KARA-ZAITRI 93/ pour la modélisation des relations cause-mode-effet des défaillances (notamment pour les modes de défaillance à causes multiples) ainsi que le calcul et la classification des indices de criticité (indices locaux ou globaux) ;

- l'adaptation de la méthode au diagnostic /SUHNER 92/ par ajout de notions comme les tests de détection (attribués à chaque mode et/ou cause de défaillance) ou les stratégies de diagnostic qui visent à hiérarchiser les moyens et les tests de détection selon différents critères (complexité de la technologie utilisée, accessibilité aux composants, ...). L'AMDEC orientée diagnostic doit permettre, par la suite, de générer automatiquement les connaissances profondes (structurelles et fonctionnelles) et les connais-

sances de surface (empiriques) nécessaires à l'élaboration de la base de connaissances d'un système d'aide au diagnostic. Finalement, une démarche de type AMDEC est un point de passage obligé au début de n'importe quelle analyse de risque, soit parce qu'elle constitue l'analyse elle-même, soit parce qu'elle est utilisée pour comprendre le fonctionnement du système ;

— la méthode de l'arbre de défaillance (MAD) /LIMNIOS 91/ ou arbre des causes (MAC) est une démarche déductive ayant pour objectifs la recherche de l'ensemble des événements ou combinaison d'événements élémentaires conduisant à un événement redouté. L'évaluation de la probabilité d'occurrence de l'événement redouté se fait à partir de celle de ses événements élémentaires. Mais l'étude de certains systèmes complexes peut conduire à des arbres de grande taille, difficile à traiter même avec un programme informatique. De plus, il n'est pas toujours possible d'identifier des séquences de défaillances menant à un événement indésirable ;

— la méthode de l'arbre des conséquences (MACQ) /VILLEMEUR 88/ est une démarche inductive permettant de définir et d'évaluer qualitativement et quantitativement des séquences d'événements conduisants à des conséquences jugées inacceptables. Cette méthode ne permet pas de justifier l'exhaustivité des événements initiateurs et nécessite généralement l'utilisation d'autres méthodes pour l'analyse des événements génériques ;

— la méthode du diagramme causes-conséquences (MDCC) /VILLEMEUR 88/ qui combine les principes des deux méthodes précédentes, permet d'identifier simultanément les causes et les conséquences d'un événement initiateur tout en mettant en évidence leurs dépendances. Elle semble cependant difficilement utilisable pour un ensemble complexe de systèmes élémentaires car l'analyse quantitative combine les méthodes de l'arbre des causes et de l'arbre des conséquences ;

— la méthode du diagramme de succès (MDS) /VILLEMEUR 88/ modélise le fonctionnement de systèmes non réparables en représentant leurs composants ou leurs fonctions par des blocs et en recherchant les liens entre ces blocs. Elle vise à identifier les combinaisons de défaillance compromettant leur fonctionnement et de calculer leur fiabilité (ou disponibilité). Malheureusement, elle n'est pas adaptée à l'analyse de relations complexes entre effets et causes des défaillances.

D'autres méthodes peuvent aussi être utilisées. Il s'agit notamment de l'Analyse Préliminaire des Risques (APR), de la méthode HAzard and OPerability Study (HAZOP), de la méthode de la Table de Vérité (MTV) ou encore de la méthode des Combinaisons de Pannes Résumées (MCPR) /VILLEMEUR 88/. Le tableau 2 ci-après présente ces méthodes en les comparant en fonction de la démarche utilisée, du type d'évaluation, de l'événement de départ de l'analyse, du type et de la forme d'expression des résultats.

3.2.4. Résultats issus de l'analyse de la sûreté de fonctionnement

Cette quatrième et dernière phase consiste à utiliser le modèle pour en tirer les résultats désirés sous la forme d'une analyse qualitative et/ou quantitative selon les méthodes mises en oeuvre auparavant. A partir du modèle et de données statistiques sur les événements susceptibles d'apparaître, des traitements et des calculs peuvent être entrepris nécessitant souvent l'emploi de logiciels appropriés.

Critères Méthodes	Type de démarche	Type d'évaluation	Entités de départ	Type de résultats	Formalisme utilisé	Liens entre les méthodes Amont	Aval
APR	inductive	qualitative	éléments dangereux	répertoire des situations dangereuses	tableaux	Analyse fonctionnel.	AMDE HAZOP
AMDEC	inductive	qualitative et semi-quantitative	modes de défaillance composants	répertoire des modes de défaillance	tableaux et grilles	Anal. fonct. et/ou APR	Méthodes ACQ, AD ou DCC
HAZOP	inductive	qualitative	paramètres mesurables du système	répertoire des déviations	tableaux	APR	MAD MDCC
MACQ	inductive	qualitative et semi-quantitative	événement initiateur	séquences d'événements inacceptables	arbre binaire	Anal. fonct. MDS	MAD Graphe de Markov
MAD	déductive	mixte	événement redouté	coupes minimales, prob. d'occur.	arbre logique combinatoire	Méthodes inductives	Graphe de Markov
MDCC	mixte	mixte	événement initiateur ou critique	séquences d'événem. inacceptables coupes min.	arbre binaire, diag. logique combinatoire	AMDE	/
MDS	/	quantitative	fonctions ou composants	coupes min. et paramètres de sûreté	diagrammes (blocs)	Analyse fonction.	/

Tableau 2 : Comparaison des méthodes d'analyse de sûreté de fonctionnement /FADIER 90/

3.3. Les caractéristiques de sûreté de fonctionnement

La détermination des caractéristiques de sûreté peut être faite lorsque les composants du système sont connus. Dans le cadre de la démarche de conception proposée, ils n'apparaissent seulement qu'à partir du niveau représentation technique. Ce n'est donc qu'à ce niveau que nous allons pouvoir contrôler que les composants choisis vérifient bien les objectifs de sûreté de fonctionnement définis dans le cahier des charges.

Avant de présenter les modèles mathématiques permettant de calculer les caractéristiques de sûreté de fonctionnement, nous allons faire quelques rappels.

3.3.1. Concept de défaillance

Une entité mise en marche à la date t = 0 tombera certainement en panne à un instant T non connu *a priori*.

On désigne par $\lambda(t)$ la densité de probabilité conditionnelle de défaillance. C'est la probabilité de défaillance d'une entité dans l'intervalle dt, sachant qu'elle a vécu jusqu'à t. La probabilité pour que l'entité soit défaillante entre t et t+dt vaut :

$$f(t)dt = R(t).\lambda(t)dt$$

$$\lambda(t) = \frac{1}{R(t)}\left[-\frac{dR(t)}{dt}\right]$$

Les observations faites à l'issue de tests ou en phase d'exploitation de l'équipement ont montré que de nombreuses entités présentent un taux de défaillance dont l'allure en fonction du temps est une courbe dite "en baignoire ". Trois zones peuvent être distinguées sur cette courbe (voir figure 3) :

— les défaillances précoces ou de jeunesse apparaissent au début de la vie d'un dispositif, durant la période pendant laquelle le taux de défaillance λ décroît rapidement. Cela

correspond aux périodes de déverminage pour les composants électroniques et de rodage pour les systèmes mécaniques ;

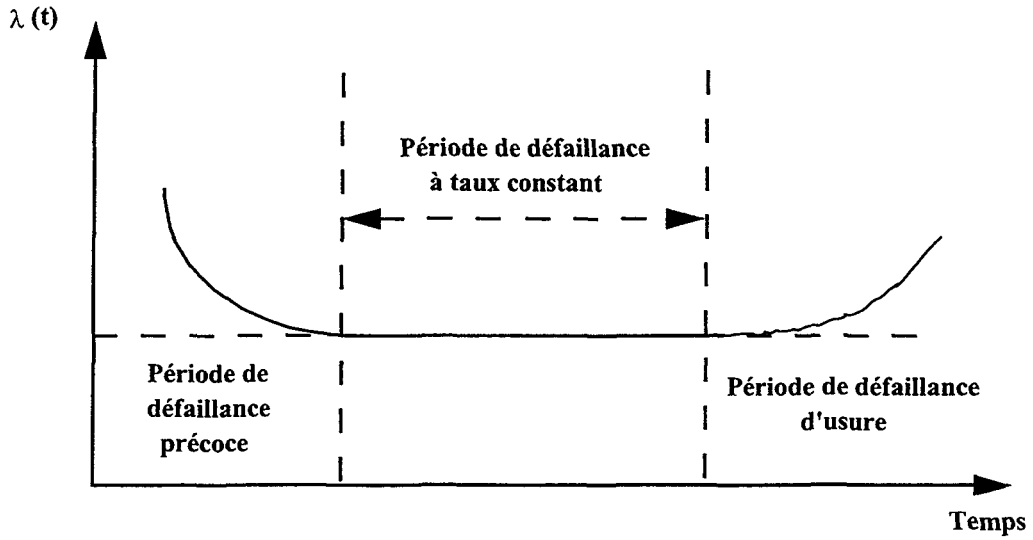

Figure 3 : Évolution du taux de défaillance (courbe dite en baignoire)

— les défaillances à taux constant surviennent durant la période de vie utile (λ sensiblement constant). Les défaillances apparaissent ici de façon aléatoire ;

— les défaillances d'usure apparaissent à la fin de la vie d'un dispositif, durant la période pendant laquelle le taux de défaillance λ croit rapidement. Elles sont liées aux modes de vieillissement et de dégradation des dispositifs.

Après ces quelques rappels, nous allons maintenant définir les concepts de fiabilité, de maintenabilité, de disponibilité et de sécurité. Les définitions issues de la norme française NF X60-500 des termes présentés ci-dessous, sont données dans le glossaire. Nous nous attachons ici à les définir d'un point de vue mathématique.

3.3.2. La fiabilité /BON 95/

Elle se définit comme la probabilité pour qu'une entité accomplisse une fonction requise, dans des conditions données, pendant un intervalle de temps donné [0,t].

$$R(t) = Prob\ (E\ non\ défaillante\ sur\ la\ durée\ [0,t])$$

Plusieurs types de fiabilité peuvent être distingués :

— la *fiabilité opérationnelle* obtenue à partir de l'exploitation du retour d'expérience. Elle est déduite de l'analyse d'entités identiques ayant été soumises aux mêmes conditions opérationnelles ;

— la *fiabilité prévisionnelle* correspondant à la fiabilité future d'un système connaissant les fiabilités de ses composants. Elle est estimée en phase de conception de façon théorique (banques de données) ou de façon expérimentale (essais). Ainsi, suivant la disposition des différents composants, nous obtenons :

$$R = \prod_{i=1}^{n} P[E_i] = \prod_{i=1}^{n} R_i \qquad \text{pour des éléments en série}$$

$$R = 1 - \prod_{i=1}^{n} P[E_i] = 1 - \prod_{i=1}^{n} (1 - R_i) \qquad \text{pour des éléments en parallèle}$$

L'évaluation de la fiabilité est mesurée le plus souvent par :

— le *temps moyen de fonctionnement avant la première défaillance* (Mean operating Time To Failure) qui est l'espérance mathématique du temps de fonctionnement avant la première défaillance

$$MTTF = E(T) = m = \int_0^{\infty} (1 - F(u))du = \int_0^{\infty} R(u)du$$

— le *temps moyen de fonctionnement entre défaillances* (Mean operating Time Between Failures) qui correspond à l'espérance mathématique du temps de fonctionnement entre défaillances

$$MTBF = \int_{-\infty}^{+\infty} t.f(t)dt = \int_0^{+\infty} R(t)dt$$

3.3.3. La maintenabilité

Elle se définit /Norme NF X60-500/ pour une entité utilisée dans des conditions données d'utilisation, comme la probabilité pour qu'une opération donnée de maintenance puisse être effectuée sur un intervalle de temps donné (0, t), lorsque la maintenance est assurée dans des conditions données et avec l'utilisation de procédures et de moyens prescrits, soit :

$$M(t) = Prob \text{ (la maintenance de E est achevée au temps t)}$$

ou

$$M(t) = \Pr ob(T_R < t)$$

avec T_R = temps de réparation

En notant g(t) la densité de probabilité du temps de réparation, on peut alors mettre M(t) sous la forme :

$$M(t) = \int_0^t g(t)dt$$

Le taux de remise en service ou taux de réparation μ(t) peut être exprimé sous la forme :

$$\mu(t) = \frac{1}{1 - M(t)} \times \frac{dM(t)}{dt} = \frac{g(t)}{1 - M(t)}$$

Nous pouvons associer à la maintenabilité le *temps moyen avant remise en service* (Mean Time To Restoration) qui représente l'espérance mathématique du temps avant remise en service (ou temps d'indisponibilité après défaillance). Ce temps se définit mathématiquement par :

$$MTTR = \int_{-\infty}^{+\infty} t.g(t)dt = \int_0^{+\infty} (1 - M(t))dt$$

3.3.4. La disponibilité (instantanée)

Elle peut être définie /Norme NF X60-500/ comme la probabilité pour qu'une entité soit en état de disponibilité dans des conditions données à un instant donné en supposant que la fourniture des moyens extérieurs nécessaires soit assurée.

$$A(t) = Prob\ (E\ non\ défaillante\ à\ l'instant\ t)$$

Pour augmenter la disponibilité d'une entité, il faut réduire le nombre de ses arrêts et notamment ceux ayant pour origine une défaillance (fiabilité) mais également réduire le temps passé à les corriger (maintenabilité).

Dans le cas où l'entité est non réparable, la disponibilité A(t) est égale à sa fiabilité R(t). Si nous observons cette entité en période de vie utile (zone à λ constant sur la courbe en baignoire présentée figure 3), A(t) et R(t) suivent une loi exponentielle :

$$A(t) = R(t) = e^{-\lambda t}$$

Cette hypothèse est généralement faite en vue de simplifier les calculs.

Dans le cas où l'entité est réparable, et en supposant les taux de défaillance et de réparation constants, la disponibilité a pour expression :

$$A(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}$$ si l'entité était disponible à t = 0

ou

$$A(t) = \frac{\mu}{\lambda+\mu}\left(1 - e^{-(\lambda+\mu)t}\right)$$ si l'entité n'était pas disponible à t = 0

Nous pouvons associer à cette caractéristique le *temps moyen de disponibilité* (Mean Up Time), espérance mathématique du temps de disponibilité ainsi que le *temps moyen entre défaillances* (Mean Time Between Failures), espérance mathématique du temps entre défaillances. Pour de nombreux systèmes, la différence entre le MTTF et le MTBF est très faible. Ainsi, on considère :

$$MTTF \approx MTBF = \int_0^{+\infty} R(t)\,dt$$

3.3.5. La sécurité

C'est l'aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques /VILLEMEUR 88/. Elle peut également être définie /DESROCHES 95/ comme l'absence de circonstances (nuisances potentielles) pouvant occasionner des dommages sur le système et son environnement.

La sécurité est généralement mesurée par la probabilité qu'une entité E évite de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques. L'aptitude contraire sera dénommée " insécurité".

Sécurité et risque sont deux notions étroitement liées. En sécurité des systèmes, le risque relatif à un événement redouté survenant pendant une activité dangereuse est défini par deux paramètres :

— la possibilité d'occurrence de l'événement redouté (probabilité des causes) ;

— la gravité des conséquences qui, en final, correspondent à des morts, des blessures graves, destruction, échec d'une mission ...

3.3.6. Synthèse

Les résultats obtenus par cette analyse de la sûreté de fonctionnement sont divers et variés : paramètres probabilistes liés à la sécurité ou à l'économie de l'installation (taux de disponibilité, MTBF, MTTR, ...), mise en évidence des paramètres prépondérants vis-à-vis du risque envisagé (chemins critiques), évaluation de plusieurs conceptions possibles ... Tous ces résultats sont finalement des éléments d'aide à la décision qui permettent d'établir les spécifications des composants les plus sensibles, les programmes d'essais pour les composants nouveaux, les stratégies de maintenance à mettre en place ou encore le niveau de risque du système et/ou de ses éléments.

La définition de ces caractéristiques de sûreté passe par l'utilisation de méthodes d'évaluation. Nous allons décrire ces méthodes dans le paragraphe suivant.

4. Évaluation des caractéristiques de sûreté

L'évaluation des caractéristiques de sûreté de fonctionnement d'un système peut se faire par l'utilisation de différentes méthodes. Nous pouvons les regrouper en deux grandes classes : les approches *a priori* et les approches *a posteriori*.

4.1. Les approches *a priori*

Lors de la conception d'un système, un certain nombre d'éléments ne sont pas complètement définis. Ce sont par exemple les conditions réelles dans lesquelles le système sera exploité ou ses défaillances internes. Pour faire face à ce type de problème, deux types de démarches peuvent être distingués : la démarche déterministe et la démarche probabiliste.

4.1.1. La démarche déterministe

Cette première démarche s'appuie sur un ensemble de connaissances, à la fois théoriques et expérimentales, des phénomènes physico-chimiques ainsi que sur l'expérience accumulée par l'exploitation de systèmes semblables. A partir de scénarios d'événements conduisant à un événement redouté (incident ou accident), les analystes doivent porter un jugement sur la vraisemblance de ces scénarios. Le repérage des scénarios envisagés, basé sur l'expérience et sur l'imagination des analystes, représente une étape essentielle puisqu'elle conditionne en grande partie la sûreté du futur système.

Le dilemme dans la prise de décision réside dans /DESROCHES 95/ :

— la prise en compte d'un scénario dont l'occurrence est *a priori* peu probable pendant la durée de vie du système et qui pénalise la conception par l'introduction de contraintes supplémentaires (techniques, économiques ou opérationnelles) ;

— la non prise en compte d'un scénario dont l'occurrence est, *a priori*, peu vraisemblable pendant la durée de vie du système et dont on accepte plus ou moins consciemment les conséquences. Cette décision ne pénalise pas la conception mais peut entraîner des surcoûts en exploitation.

Nous pouvons donc constater que la démarche déterministe est d'un maniement relativement simple. Mais sa difficulté majeure réside dans le choix du scénario de référence, base pour toute la démarche. C'est pourquoi la démarche probabiliste est parfois utilisée.

4.1.2. La démarche probabiliste

Cette démarche se décompose en deux étapes principales. Dans la première, une analyse qualitative du système est menée dans le but de recenser de façon exhaustive, l'ensemble des

défaillances pouvant l'affecter. On cherche dans le même temps à établir les conséquences qu'elles pourraient avoir à la fois sur le système lui-même et sur son environnement. Dans la seconde étape, l'analyste va s'attacher à donner à chacun des scénarios d'événements possibles, une probabilité d'occurrence. Au moyen d'un critère de décision (combinant à la fois probabilité d'occurrence et conséquence des événements), la démarche probabiliste se propose de définir les actions correctives optimales pour faire face à l'ensemble des scénarios retenus.

La démarche probabiliste n'exclut *a priori* aucun scénario. Par contre, le choix du critère de décision est difficile, l'attribution de probabilité d'occurrence à certains événements peut s'avérer délicate, et la démarche est d'un maniement plutôt lourd.

La tendance actuelle cherche donc à utiliser de façon conjointe les démarches déterministe et probabiliste /VILLEMEUR 88/. A la relative simplicité de la première s'ajoutent la recherche, l'obtention et la garantie d'un niveau minimal de sûreté de fonctionnement données par la seconde .

Cependant, des sources d'incertitudes demeurent concernant la prise en compte ou non de tous les scénarios et sur l'attribution de certaines probabilités d'occurrence. Pour remédier à cela, l'utilisation de méthodes basées sur l'intégration du retour d'expérience s'avère nécessaire.

4.2. Les approches *a posteriori*

Ces approches consistent à analyser les incidents ou les accidents (événements redoutés) "immédiatement" après leur apparition. Ils peuvent correspondre à des scénarios identifiés comme indésirables ou à des situations que l'on n'avait pas imaginé. L'ensemble de ces approches est regroupé sous le terme plus général de retour d'expérience. Ces approches ont pour objectif d'analyser des événements tels que :

a) *la défaillance*

C'est la cessation de l'aptitude d'un dispositif à accomplir une fonction requise.

La défiabilté F(t) (Failure ou Fault en anglais) peut être définie comme la probabilité d'apparition d'un défaut au moins dans l'intervalle de temps [0, t]. F(t) représente la proportion d'éléments défaillants à un instant t pour un échantillon donné.

$$F(t) = Prob(E \text{ soit défaillante } [0,t])$$

Une entité connaît donc une défaillance lorsqu'elle n'est plus en mesure de remplir sa (ou ses) fonction(s). Après une défaillance, une entité est en état de panne.

Différents types de défaillance sont distingués suivant leur rapidité de manifestation, leurs causes, leurs conséquences ... Ils peuvent également être caractérisés par la combinaison de ces différents concepts. La figure 4 ci-dessous montre une classification des défaillances suivant différents critères.

Une défaillance est le passage d'un état (fonctionnement) à un autre (panne). Une panne est donc un état.

b) *la panne*

C'est l'inaptitude d'une entité à accomplir une fonction requise. Après apparition d'une défaillance, on considère que l'entité est en panne ; une panne résulte toujours d'une défaillance.

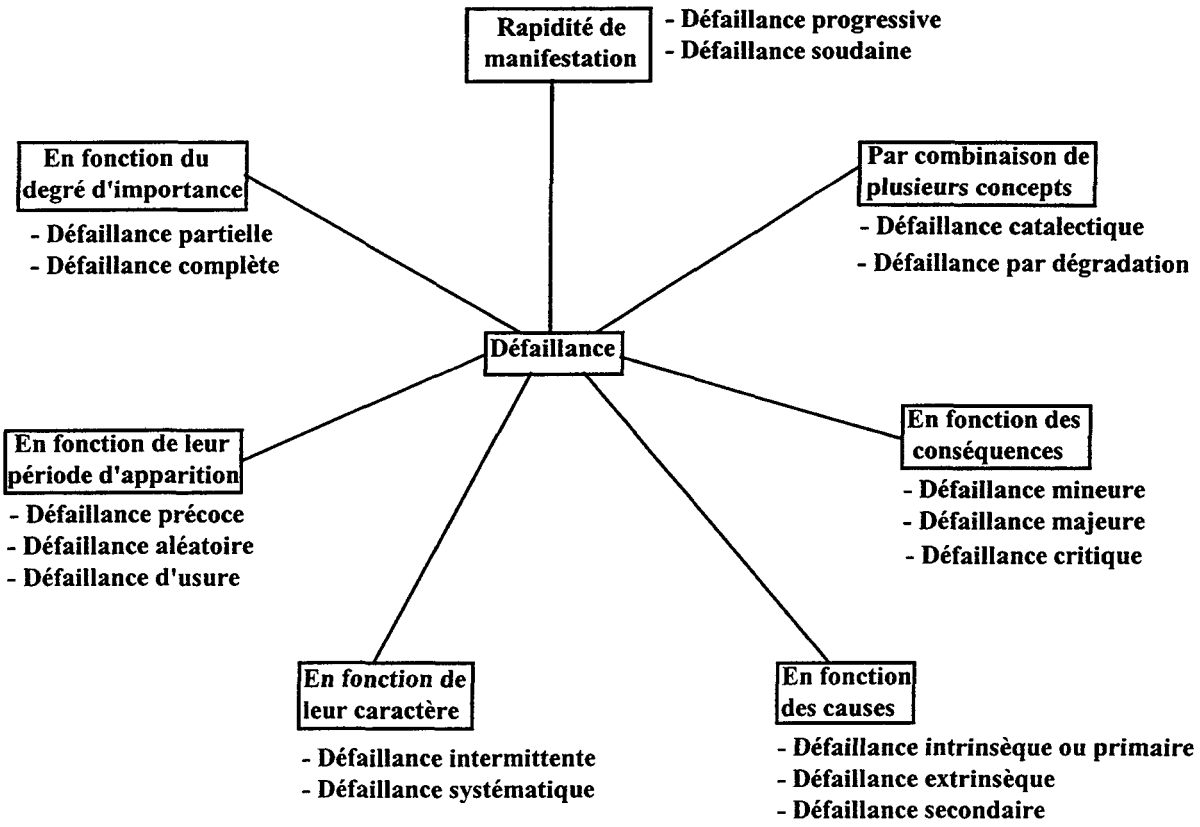

Figure 4 : Classification des défaillances /BTE 92/

c) *le défaut*

Le concept de défaut est important dans les opérations de surveillance et de maintenance. On considère comme un défaut tout écart entre la caractéristique observée sur le dispositif (système, composant) et la caractéristique de référence lorsque celui-ci est en dehors des spécifications.

Une défaillance conduit à un défaut puisqu'il existe un écart entre la caractéristique constatée et la caractéristique spécifiée. Inversement, un défaut n'induit pas nécessairement une défaillance. En effet, le système peut très bien conserver son aptitude à assurer sa mission principale si les défauts affectant les sous-systèmes et composants n'ont pas d'impacts significatifs sur la mission principale.

d) *la dégradation*

Une dégradation /ZWINGELSTEIN 96/ est l'état d'un ensemble qui présente :

— une perte de performances d'une des fonctions assurées par cet ensemble ;

— un sous-ensemble détérioré voire défaillant mais sans conséquence fonctionnelle sur cet ensemble.

Dans le cas d'une évolution monotone /CORAZZA 75/, la dérive ou la dégradation déplace la valeur des paramètres toujours dans le même sens et peut être décrite dans le cas le plus général par une expression polynomiale du type :

$$Y(t) = B_0 + B_1\, t + \ldots\ldots + B_n\, t^n$$

avec B_i : coefficients positifs (négatifs) constants à valeurs distribuées ;
t : temps.

Dans le cas d'une évolution non monotone, deux classes de mécanismes peuvent être distinguées :

— les mécanismes d'évolution déterministe décrits, comme dans le cas précédent, par une expression polynomiale à coefficients quelconques ;

— les mécanismes d'évolution aléatoire décrits par leurs propriétés stochastiques (fonction de corrélation).

e) *le mode de défaillance*

C'est l'effet par lequel une défaillance est observée.

Le mode de défaillance est relatif à une fonction. Il s'exprime par la manière ou la façon dont un élément ou un composant vient à ne plus remplir sa fonction. Les modes de défaillance peuvent également être définis comme les effets de causes de défaillance d'autres composants sur les fonctions du composant étudié. Ils se définissent donc relativement aux effets sur le composant ou aux fonctions de celui-ci /VILLEMEUR 88/.

Les modes de défaillance sont définis pour un certain état de fonctionnement du composant et du système ; la considération d'un autre état de fonctionnement du système peut entraîner la modification des modes de défaillance définis précédemment.

Nous pouvons citer, à titre d'exemples, les modes de défaillance suivant : blocage, grippage, rupture, court-circuit, ...

f) *la cause de défaillance*

Ce sont les circonstances liées à la conception, la fabrication ou l'emploi et qui ont entraînées la défaillance.

Les principales causes de défaillance se distinguent suivant qu'elles sont propres au système ou dues à l'environnement. Dans le premier cas, elles comprennent les détériorations d'origine mécanique (rupture, endommagement, baisse de performances) et les détériorations d'origine électrique. Dans le second cas, elles regroupent les défauts de fabrication, les défauts de mise en œuvre et de maintenance ainsi que les conditions ambiantes et climatiques.

g) *le mécanisme de défaillance*

Il est défini comme un processus physique, chimique ou autre ayant entraîné une défaillance.

Ces processus entraînent alors un certain endommagement du matériel. Celui-ci se manifeste suivant différentes formes selon le type de processus. Les dommages envisagés /ARINC 95//FRANCOIS 93/ peuvent être :

- ceux survenant de façon quasi-instantanée suite à l'apparition simultanée de facteurs défavorables (déformation excessive, rupture brutale ...) ;
- ceux résultant de l'accumulation des sollicitations dans le temps (fatigue, fissuration, corrosion ...). Ces endommagements apparaissent à la suite de performances mécanique, électrique ou thermique incorrectes.

Deux grandes familles d'approches *a posteriori* peuvent être distinguées pour le traitement des données de défaillance : les méthodes fréquentielles et les méthodes bayésiennes /LANNOY 94/ /PROCACCIA 92/.

4.2.1. Les méthodes fréquentielles de traitement des données de défaillances

Les méthodes fréquentielles de traitement des données de défaillances sont principalement utilisées lorsque le nombre de données d'essais ou de retour d'expérience est suffisamment important. Ces méthodes permettent, à partir des observations de défaillance soit de vérifier qu'un échantillon suit une loi de distribution postulée, soit de déterminer les paramètres d'une distribution supposée représenter les observations. Les principales lois utilisées sont la loi exponentielle, la loi de Weibull (à deux ou trois paramètres), la loi normale, la loi log-normale et la loi Gamma.

Mais les échantillons de données permettant le calcul des temps entre défaillances sont rarement complets. D'autres méthodes sont alors utilisées afin de prendre en compte cette incomplétude des informations. On distingue alors les méthodes non paramétriques et les méthodes paramétriques.

4.2.1.1. Les méthodes non paramétriques

Les méthodes que l'on retrouve couramment dans la littérature et qui appartiennent à cette classe sont la méthode de Wayne-Nelson, la méthode de " Johnson " ou des rangs médians, la méthode " life table " ou méthode actuarielle et enfin l'estimateur de Kaplan-Meier ou " Product limit ". Mais seul ce dernier considéré comme l'estimateur le plus cohérent de la fonction de survie R(t) fait référence.

Ainsi, en posant d_j le nombre de défaillances au temps t_j et r_j le nombre de dispositifs soumis à risque à t_j, on a :

$$R(t_i) = \prod_{j=1}^{i} (1 - \frac{d_i}{r_j})$$

Le lecteur intéressé trouvera une présentation plus complète de ces méthodes dans /LANNOY 94/.

4.2.1.2. Les méthodes paramétriques

Le problème qui se pose est celui du choix d'un modèle *a priori* afin d'ajuster un modèle paramétrique sur les données de survie. La loi exponentielle peut être utilisée pour cela mais en général le modèle choisi est celui de la loi de Weibull. Celle-ci offre en effet l'avantage de pouvoir décrire alternativement les trois phases de vie d'un matériel (jeunesse, vie utile, vieillesse). Nous distinguons la loi de Weibull à deux paramètres qui s'écrit sous la forme :

$$R(t) = \exp\left(-\left(\frac{t}{\eta}\right)^{\beta}\right)$$

ainsi que la loi de Weibull à trois paramètres qui s'écrit :

$$R(t) = \exp\left(-\left(\frac{t-\gamma}{\eta}\right)^{\beta}\right)$$

avec β paramètre de forme associé à la cinétique du processus observé;

η paramètre d'échelle;

γ paramètre de position représentant le décalage qui existe entre le début de l'observation et le début du processus observé (usure, fatigue, ...).

Cette loi offre de plus l'avantage de couvrir ou d'approcher d'autres lois pour des valeurs particulières de β : la loi exponentielle pour $\beta=1$ et la loi normale pour $\beta=3,6$.

Ensuite, la méthode du maximum de vraisemblance est appliquée. Celle-ci permet de déterminer un estimateur des paramètres de la distribution.

4.2.1.3. Synthèse

De nombreux événements présentent la singularité d'être unique. Aussi, la notion de fréquence ne permettra pas d'établir leur probabilité d'occurrence. Des modifications peuvent également intervenir sur le matériel ou sur son fonctionnement. Tout ceci peut donc influer sur les conditions d'occurrence des événements. Pour remédier à ces différents problèmes et compenser les limites actuelles de ces méthodes fréquentielles, celles-ci sont aujourd'hui complétées par les méthodes bayésiennes qui apportent une réponse à ces problèmes.

4.2.2. Inférence bayésienne pour le calcul des probabilités de survie /PROCACCIA 92/

L'estimation de la "mesure d'occurrence" d'un événement (parmi toutes les éventualités) peut être faite :

— en calculant sa fréquence par une méthode classique ;

— par un calcul intégrant des données complémentaires à celles des méthodes classiques qui proviennent de différentes sources (avis d'experts, résultats d'études similaires ...).

Cette dernière méthode permet d'obtenir la probabilité *a posteriori* à partir d'avis *a priori*. Elle constitue le point de départ des méthodes bayésiennes. La démarche bayésienne, contrairement à la démarche fréquentielle, peut être utilisée lorsque les données d'observations sont rares ou " polluées ". L'introduction d'information non mesurée (et/ou non mesurable) est une des bases des méthodes bayésiennes.

4.2.2.1. Application dans le domaine discret

Soit (H_i) une suite de n événements indépendants et complémentaires susceptibles d'entraîner l'apparition d'un événement E. On note :

— $Pr(H_i)$ la probabilité *a priori* d'occurrence de l'événement H_i ;

— $Pr(E/H_i)$ la probabilité de réalisation de l'événement E sachant que l'événement H_i s'est réalisé ;

— $Pr(H_i/E)$ la probabilité *a posteriori* d'occurrence de l'événement H_i sachant que l'événement E s'est réalisé. En fait, c'est la probabilité que E s'étant produit, la cause en soit H_i.

Ces trois types de probabilité apparaissent dans la formule suivante :

$$\Pr(H_i / E) = \frac{\Pr(H_i).\Pr(E / H_i)}{\Pr(E)} = \frac{\Pr(H_i).\Pr(E / H_i)}{\sum_j \Pr(H_j).\Pr(E / H_j)}$$

Ainsi, si un événement E a plusieurs causes *a priori* possibles H_i de probabilité (ou hypothèses) respectives $Pr(H_i)$, alors si E est observé, la probabilité que la cause en soit H_i est exprimée par la formule ci-dessus dite formule de BAYES. L'interprétation est donc la suivante : un événement E est nécessairement produit par l'une ou l'autre des causes (ou hypothèses) incompatibles $H_1, H_2, ..., H_n$.

4.2.2.2. Application dans le domaine continu

Soient X et Y deux variables aléatoires réelles liées à la réalisation des événements E et H. Soient :

— h(x,y) la densité de probabilité du couple (X,Y) ;

— g(y) la densité marginale (*a priori*) de Y ;

— f(x/y) la densité conditionnelle de X sachant Y.

La formule de BAYES de la densité de probabilité conditionnelle (*a posteriori*) de Y sachant X s'écrit :

$$g(y/x) = \frac{g(y).f(x/y)}{\int_{\Delta} g(t).f(x/t)}$$

où ? est le domaine de définition de Y.

Ainsi, si l'on cherche à estimer un paramètre de fiabilité θ, la démarche bayésienne s'appuie sur une information complémentaire *a priori* apportée par le jugement d'expert ou par une autre expérience passée g(θ) et une information *a priori* remise à jour par les quelques observations du retour d'expérience récent (vraisemblance) $L(x_i/\theta)$. Nous obtenons alors, grâce à l'utilisation du théorème de Bayes, une densité de probabilité conditionnelle *a posteriori* du (des) paramètre(s) de fiabilité recherché(s) $f(\theta/x_i)$:

$$f(\theta/x_i) = \frac{g(\theta).L(x_i/\theta)}{\int_{D} g(\theta).L(x_i/\theta)d\theta}$$

avec :

$L(x_1....x_n/\theta) \equiv f(x_1/\theta).....f(x_n/\theta)$ la fonction de vraisemblance de l'échantillon observé sachant le paramètre θ : c'est une densité de probabilité conditionnelle ;

g(θ) la probabilité *a priori* de θ : elle est déterminée avant d'avoir observé les informations x. Cette probabilité représente le degré de croyance que l'on a sur le paramètre θ avant les expériences.

Même si l'approche bayésienne permet de prendre en compte des événements tels que des modifications, des maintenances (corrective et préventive sur les composants), des avis d'experts, ... sa mise en œuvre pose cependant quelques difficultés. Parmi celles-ci, citons /LANNOY 95/ :

— la détermination de la loi *a priori* qui n'est pas toujours aisée ;

— le processus d'itération qui peut être difficile ;

— la loi *a priori* et la vraisemblance qui ont la même importance en l'absence de pondération.

4.3. Conclusion

Quelles qu'elles soient, les approches utilisées pour déterminer les caractéristiques de sûreté de fonctionnement d'un système ne peuvent prendre en compte tous les phénomènes et événements pouvant survenir au cours de la vie du système. Les conditions d'utilisation et d'environnement étant également différentes d'un équipement à un autre, il n'est pas toujours

facile de profiter du retour d'expérience acquis sur des équipements identiques. Il n'est pas toujours possible d'éliminer certaines défaillances, au mieux certains de leurs effets pourront être réduits.

Nous constatons donc qu'il est nécessaire de mettre en place des moyens permettant de remédier à cela tels que des moyens de détection et de diagnostic de défaillances. Ceux-ci nous permettront de déceler, au plus tôt l'apparition de situations dangereuses, de diagnostiquer leur origine, et de mettre le système dans un état de sécurité (pour l'opérateur sur l'équipement mais également pour celui qui réalisera l'intervention de maintenance). Toutes ces opérations contribueront au maintien des caractéristiques de sûreté du système à un niveau acceptable. Ces différentes activités constituent notre problématique de recherche.

CONCLUSION

Toute entreprise cherche à disposer de façon maximale des produits qu'elle acquiert pour, à son tour, fabriquer des produits de qualité. Dans ce contexte, la sûreté de fonctionnement des systèmes est devenue aujourd'hui un enjeu majeur. La complexité des nouveaux équipements nécessite en effet de rechercher, dès leur conception, les défaillances pouvant les affecter, de les hiérarchiser et de les corriger suivant les effets qu'elles peuvent avoir. En ce qui concerne les défaillances pour lesquelles des actions correctives ne peuvent être trouvées, il convient de minimiser leurs effets en mettant en œuvre des moyens de surveillance ou en place une politique de maintenance préventive.

Dans ce chapitre, nous avons tout d'abord présenté le domaine de la conception. Nous avons vu que les méthodes actuelles ne répondaient que partiellement au problème de la conception d'un système. Dans un second temps, nous avons décrit la démarche de conception élaborée au sein du laboratoire. Cette démarche regroupe différents acteurs de la conception (automaticien, mécanicien,...).

Pour notre part, notre contribution se situe au niveau de la conception pour l'exploitation. A partir de la définition des exigences de sûreté de fonctionnement au niveau représentation du besoin, nous menons une analyse de la sûreté de fonctionnement du système à concevoir au niveau représentation des exigences fonctionnelles du besoin. Cette analyse vise à déterminer les différents événements pouvant contrarier le respect des objectifs de sûreté demandés par le client. La méthode que nous utilisons dans ce cadre d'analyse prévisionnelle de la sûreté de fonctionnement est la méthode AMDE. En effet, par une recherche exhaustive des défaillances pouvant affecter un équipement (défaillances fonctionnelles et défaillances matérielles), elle propose des éléments de réponse concernant la mise en place de moyens de détection ou d'actions correctives. Elle peut être mise en œuvre aux niveaux représentation des exigences fonctionnelles du besoin et représentation technique. De plus, elle permet également de fournir des éléments au personnel intervenant lors de la recherche de composants défectueux (aide au diagnostic) et peut être facilement enrichie au fur et à mesure de l'exploitation du bien. Pour toutes ces raisons, nous utilisons donc la méthode AMDE dans nos travaux afin de pouvoir disposer d'un certain nombre d'éléments pour la mise en place de moyens de surveillance et d'aide au diagnostic des défaillances des systèmes de production.

Quant aux modèles mathématiques, ils ont été étudiés dans le but d'évaluer *a priori* les caractéristiques de sûreté de fonctionnement du système à concevoir (fiabilité, maintenabilité, disponibilité et sécurité). Ces modèles peuvent être utilisés et mis en œuvre au niveau représentation technique c'est-à-dire lorsque les composants constituant le produit à concevoir sont connus.

Dans le chapitre suivant, nous allons présenter les différents concepts dédiés à la conception pour l'exploitation que nous avons identifiés à chacun des niveaux de représentation du modèle de produit. Ceux-ci doivent permettre de fournir une aide à la définition des moyens de détection et de diagnostic des défaillances afin de garantir les

exigences de sûreté définies dans le cahier des charges. Le chapitre 3 sera quant à lui consacré au processus de conception c'est-à-dire aux méthodes permettant d'instancier les différents concepts du modèle de produit.

CHAPITRE 2

LE MODELE DE PRODUIT

INTRODUCTION

Concevoir un système qui soit sûr de fonctionnement est aujourd'hui une contrainte figurant dans tout cahier des charges client. Afin de la prendre en compte, nous avons présenté dans le chapitre précédent, la démarche de conception développée au laboratoire. Nous avons vu qu'elle se compose d'un modèle de produit et d'un processus de conception. Le modèle de produit, objet de ce chapitre, est constitué de cinq niveaux de représentation où l'aspect *sûreté de fonctionnement* apparaît dès le premier niveau. En charge ensuite aux différents acteurs de la conception de faire en sorte que ces exigences soient respectées.

Nous allons dans ce chapitre présenter comment l'aspect Exploitation et plus particulièrement la maintenance avec ses composantes surveillance et diagnostic, est intégré dans cette démarche afin de garantir les exigences de sûreté de fonctionnement.

Le modèle de système (produit) défini dans le premier chapitre est caractérisé par différents niveaux de représentation et par un certain nombre de concepts ou d'entités propres à chaque niveau de représentation et à chacun des acteurs de la conception. Les différents concepts que nous avons retenus pour l'aspect exploitation et plus particulièrement pour la sûreté de fonctionnement et la maintenance, sont présentés dans les paragraphes suivants.

Ainsi, nous allons pour chacun des cinq niveaux de représentation du modèle de produit, présenter les différents concepts qui ont été identifiés dans le cadre de cette problématique. Nous précisons également pour chacun d'eux leurs objectifs et les différents modèles susceptibles de les représenter.

1. Le niveau Représentation des besoins

Ce niveau de représentation vise à définir les fonctions auxquelles devra répondre le produit tout en respectant un certain nombre de contraintes. C'est pourquoi les concepts de "Fonction de service" et "Fonction de contraintes globales" ont été proposés /JACQUET 98/. Le concept "Fonction de service" est défini /JACQUET 98/ comme *une fonction correspondant à un service ou à une mission que le produit est supposé rendre*. Quant au concept "Fonction contrainte globale", c'est *une fonction modélisant les limites ou contraintes devant être satisfaites par l'ensemble des fonctions du produit.* Nous considérons la sûreté de fonctionnement comme une composante des fonctions contraintes globales et le produit doit respecter cette contrainte.

Ainsi, un produit peut s'exprimer comme un doublet :

$$P = < FS , Cg >$$

avec P : produit à concevoir

FS : ensemble des fonctions de service

Cg : ensemble des contraintes globales

On peut définir Cg comme un ensemble de caractéristiques auxquelles on attribue une valeur :

$$Cg = (\{ Caract.1, Valeur1\} ; \{Caract.2, Valeur2\} ; ..... ; \{Caract.N, ValeurN\})$$

Chacune de ces caractéristiques est perçue comme une contrainte par les différents intervenants de la conception, contraintes qu'ils se devront de respecter à chacun des niveaux de représentation du modèle de produit. Ces caractéristiques peuvent également être perçues comme des objectifs à atteindre au niveau des performances du produit.

Dans le cadre de la modélisation du produit, nous nous limiterons à une seule contrainte globale : la sûreté de fonctionnement. D'où $Cg = SdF$.

Nous définissons ce concept de sûreté de fonctionnement par un quadruplet :

$$SdF = \{R,A,M,S\}$$

avec R : caractéristique de fiabilité du produit

A : caractéristique de disponibilité du produit (qui dépend de R et de M)

M : caractéristique de maintenabilité du produit

S : caractéristique de sécurité du produit

Ces caractéristiques, relatives au comportement que devra avoir le système en exploitation, vont être propagées à chacun des niveaux de représentation du modèle de produit. Elles s'exprimeront par exemple sous la forme de MTBF, de probabilité de défaillance, ... Le respect de cette contrainte (ou objectif) de sûreté de fonctionnement se fera par l'utilisation de composants fiables (faible taux de défaillance), de mise en redondance, de mise en place de politiques de maintenance préventive, mais également par la définition et la mise en œuvre de moyens de surveillance et de diagnostic afin de déceler toute situation anormale. Ces différentes solutions seront analysées, évaluées et généralisées à chacune des étapes du processus de conception. Les solutions retenues seront quant à elles caractérisées aux différents niveaux de représentation du modèle de produit.

2. Niveau Représentation des exigences fonctionnelles du produit

Le comportement nominal que doit adopter le système pour accomplir sa mission ainsi que les principes nécessaires à sa mise en œuvre sont déterminés à ce niveau. Les solutions proposées pour chacun des services identifiés doivent répondre aux contraintes et aux limites spécifiées par le client. Pour cela, trois concepts ont été définis /JACQUET 98/ : "Chaîne opératoire", "Principe opératoire", "Solution de principe par fonction de service".

Le premier concept modélise les opérations indispensables à la définition du comportement que le système doit adopter pour remplir le service requis. Le second précise les principes (électrique, mécanique, fluidique, ...) susceptibles de supporter chaque opération définie à l'aide du premier concept. Le dernier concept modélise les solutions conceptuelles aptes à remplir chaque service. Il correspond à l'association des différents principes supportant chacune des fonctions opératoires.

Le passage des fonctions de service aux fonctions opératoires se fait par l'intermédiaire d'une transformation T telle que :

avec : FS : ensemble des fonctions de service fsk

Fo_{ij} : fonction opératoire de niveau 1 ($i = 0, j = 0$)

T : opérateur de transformation

Nous pouvons alors, par rapport à cette formulation, définir les contraintes globales Cg comme une restriction dans l'ensemble des valeurs admissibles par les différentes fonctions opératoires /GRUDZIEN 97/. On note donc :

$$T_{|Cg}(fsk) = T(fsk)$$

la restriction de T à Cg.

De la même façon, on peut définir un opérateur de transformation permettant de passer des fonctions opératoires de premier niveau aux fonctions opératoires de niveaux inférieurs jusqu'aux fonctions opératoires élémentaires. On aboutit alors à une chaîne opératoire du même type que celle représentée sur la figure 1 de la page suivante. Cet opérateur de transformation peut s'exprimer de la façon suivante :

$$Foij_{i=0} \xrightarrow{tr} Foij_{i,j>0}$$

Les contraintes globales non satisfaites par les fonctions opératoires de premier niveau peuvent être définies comme une restriction dans l'ensemble des contraintes globales pour les fonctions opératoires de niveaux inférieurs. Ainsi, on note :

$$tr_{|Co}(foij) = tr(foij)$$

la restriction de tr à Co

avec Co : ensemble des contraintes globales non encore satisfaites

$Co \subseteq Cg$

Comme nous l'avons dit précédemment, la chaîne opératoire est constituée de plusieurs fonctions opératoires ayant chacune un fonctionnement nominal et des caractéristiques relatives à leur comportement (MTBF, probabilité de défaillance, ...). Ces caractéristiques peuvent être obtenues à partir d'un retour d'expérience acquis sur des éléments similaires ou être calculées aux niveaux de représentation suivants (à partir de données constructeur par exemple). Les concepts que nous avons identifiés visent à associer au modèle de produit les paramètres, les données, ... permettant d'évaluer *a priori* la sûreté de fonctionnement, les besoins en éléments redondants, les fonctions nécessaires à la surveillance et au diagnostic de défaillance du système, ...

Dans ce but, le premier concept que nous intégrons au modèle de produit est le concept "Mode de défaillance fonctionnelle". Il est décrit ci-dessous.

2.1. Le concept " Mode de défaillance fonctionnelle "

A ce niveau de représentation, lorsque l'ensemble de la chaîne opératoire a été défini, l'ingénieriste en charge de l'évaluation de la sûreté de fonctionnement peut commencer son étude. Il peut tout d'abord contribuer au choix des principes à retenir pour supporter les opérations à réaliser en fonction des exigences de sûreté à respecter.

La chaîne opératoire nominale (figure 1) constitue le fonctionnement normal attendu du système. Dans le cadre de nos travaux, nous allons nous intéresser aux comportements anormaux ou alternatifs de cette chaîne et des fonctions opératoires qui la composent.

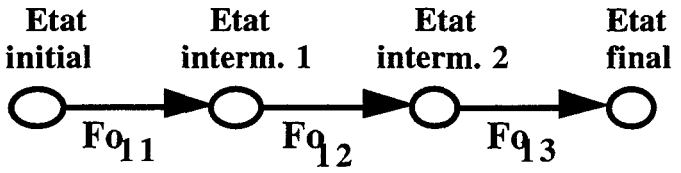

Figure 1 : Exemple de chaîne opératoire

Ainsi, à partir de la chaîne opératoire nominale, l'ingénieriste en charge de l'évaluation de la sûreté de fonctionnement va définir et lister les différents modes de défaillance susceptibles d'apparaître et proposer ensuite des alternatives (redondance, maintenance, ...) pour pallier à ces éventuels dysfonctionnements. Les deux notions de modes de défaillance et de modes de marche doivent pour cela être introduites au modèle de produit, en charge ensuite au(x) concepteur(s) de les mettre en oeuvre ou non.

2.1.1. Définition des fonctionnements anormaux

La description des différents fonctionnements anormaux que le système pourra avoir lors de son exploitation commence à ce niveau de représentation. Ne disposant ici que de fonctions opératoires, les modes de défaillance susceptibles d'apparaître seront des modes de défaillance fonctionnelle.

Cette définition des modes de défaillance vise à proposer au concepteur des moyens pour l'aider à identifier au sein de la chaîne opératoire les fonctions opératoires "sensibles" c'est-à-dire supposées à risque pour la réalisation de la mission du système.

Pour chacune des fonctions de la chaîne opératoire, quatre modes de défaillance sont proposés /CUENCA 92/ :

— *pas de fonction* : la fonction n'est pas présente lorsqu'elle doit être activée. On parle alors d'indisponibilité de la fonction ;

— *perte de fonction* : la fonction active disparaît à la suite d'une défaillance. On parle ici de non fiabilité (défiabilité) ;

— *fonction dégradée* : la fonction est réalisée à des performances non nominales. Le risque lié à l'apparition de ce mode réside dans le fait qu'il peut entraîner des erreurs opératoires pouvant avoir des conséquences très importantes (sécurité humaine et matérielle) ;

— *fonction intempestive* : la fonction se réalise à un moment autre que celui où elle est attendue ou entraîne des effets différents de ceux attendus. Là aussi l'aspect sécurité humaine et matérielle est à prendre en compte.

Le modèle de représentation proposé pour modéliser ce concept est le tableau d'Analyse des Modes de Défaillance et de leurs Effets (AMDE). Comme nous nous intéressons à des défaillances de fonctions (fonctions opératoires), nous établissons donc une AMDE fonctionnelle dont un exemple est donné Tableau 1.

La liste des différents modes de défaillance associés à chacune des fonctions opératoires donne au concepteur une évaluation qualitative de la sûreté de fonctionnement de la solution proposée. Pour en avoir une évaluation quantitative, il sera d'abord nécessaire de passer par les autres niveaux de représentation afin de connaître les éléments matériels composant les fonctions opératoires. On disposera ainsi d'informations relatives à la sûreté de fonctionnement (MTBF, probabilité de défaillance, ...) concernant chacun de ces composants. On pourra alors évaluer la fiabilité de la fonction opératoire considérée en fonction de la fiabilité de chacun de ses constituants.

Fonction	Modes de défaillance	Causes	Effets
Déplacer le composant	Déplacement non réalisé	Internes ou externes à la fonction	Composant non déplacé
	Déplacement interrompu en fonctionnement		Composant n'arrive pas au point de déchargement
	Déplacement intermittent		Composant déplacé de façon intermittente

Tableau 1 : Exemple d'AMDE fonctionnelle

Nous pouvons exprimer sous une forme algébrique les différentes informations contenues dans ce tableau.

2.1.2. Expression algébrique du concept " Mode de défaillance fonctionnelle "

En posant :

$Mof = \{m1,m2,m3,m4\}$ = l'ensemble des modes de défaillance fonctionnelle

$Card(Mof) = 4$

avec m1 = perte de la fonction
m2 = pas de fonction
m3 = fonction dégradée
m4 = fonction intempestive

Caf = l'ensemble des causes

Eff = l'ensemble des effets

On peut définir une relation de défaillance fonctionnelle comme :

$$Rd(fq_i) \subseteq (\phi(Mo_f) \times \phi(Ca_f) \times \phi(Ef_f))$$

avec Rd (fo_{ij}) : relation de défaillance fonctionnelle associée à fo_{ij}
Ø : ensemble des partitions
x : produit cartésien
fo_{ij} : fonction opératoire de niveau i et de rang j

De même, on peut dire pour chaque fonction opératoire que :

$\exists m_1 \in Mo$ tel que :

$$m_1 \ (Foij) \longrightarrow \neg R$$

$\exists m_2 \in Mo$ tel que :

$$m_2 \text{ (Foij)} \longrightarrow \neg A$$

$\exists m_3 \in Mo$ tel que :

$$m_3 \text{ (Foij)} \longrightarrow \neg S$$

$\exists m_4 \in Mo$ tel que :

$$m_4 \text{ (Foij)} \longrightarrow \neg S$$

L'identification *a priori* de ces différents modes de défaillance va faire apparaître au niveau de la chaîne opératoire nominale de nouveaux états pour chacune des fonctions opératoires (défaillant, dégradé, intempestif, pas de fonction). Dans le cadre de la conception de systèmes sûrs et en fonction des exigences de sûreté qui auront été exprimées par le client, il va être nécessaire d'introduire des modes de secours (redondance), de sécurité, de maintenance, ... Ces modes vont avoir pour objet de contrer l'apparition des modes de défaillance qui auront été identifiés précédemment. Ces séquences alternatives vont constituer les différents modes de marche du système à concevoir. C'est un autre concept que nous intégrons au modèle de produit. Il permet d'étendre et d'enrichir le modèle de comportement associé au produit. Nous allons le présenter dans le paragraphe suivant.

2.2. Le concept " Mode de marche "

La définition des états dans lesquels peut se trouver un système suite à l'apparition d'une défaillance ou d'une dégradation, va mettre en avant les modes d'exploitation qu'il va être nécessaire de prendre en compte et d'intégrer dans les phases suivantes de la conception (mode de secours, arrêt d'urgence, marche de test, ...). En fonction des exigences de sûreté de fonctionnement à respecter, des procédures visant à contourner certains fonctionnements anormaux de la fonction fo_{ij} peuvent être mises en oeuvre. Elles vont avoir pour objectif d'activer des éléments en redondance, de lancer des ordres d'arrêt pour réparation ou laisser le système dans son état présent si les risques encourus sont jugés mineurs. La nécessité de définir ce type de procédures peut être mise en évidence au niveau représentation technique (paragraphe 4.2.2.). En effet, la définition des modes de défaillance des composants peut conduire à identifier des actions à mettre en oeuvre pour contrer ces modes. La définition d'alternatives au fonctionnement normal de la fonction opératoire considérée en est une.

Nous allons présenter, dans le paragraphe suivant, les différents modes d'exploitation que l'on peut rencontrer lors de l'utilisation d'un système.

2.2.1. Les modes de marche d'un système

Tout système est conçu dans l'objectif de rendre un service à son utilisateur. Afin que celui-ci soit rendu de la meilleure façon possible, il est parfois nécessaire de mettre en oeuvre certaines procédures. Elles caractérisent les différents modes d'exploitation (de marche) du système. Nous pouvons classer ces modes de marche (modes ou états qu'un système peut atteindre) en trois familles distinctes /ADEPA 81/ :

— les modes de fonctionnement nominaux ;

— les modes d'arrêt ;

— les modes de défaillance.

Dans la première famille sont regroupés tous les modes de fonctionnement normal, de marches de préparation, de vérification, de test et de clôture entreprises avant ou après que le service soit (ait été) rendu.

La seconde comprend tous les modes conduisant à un arrêt du système pour des raisons extérieures. Les modes suivants y sont distingués : arrêt en état initial, arrêt en fin de cycle, arrêt dans un état déterminé, préparation à la remise en service après défaillance.

Dans la troisième famille sont inclus tous les modes conduisant à la perte du service (arrêt du système) suite à l'apparition d'une défaillance. On y trouve les modes suivants : arrêt d'urgence pour stopper le service s'il engendre des risques (matériels, humains, environnementaux), diagnostic et/ou traitement des défaillances, rendre le service tout de même.

Ces différents modes de marche sont traduits dans le GEMMA (Guide d'Étude des Modes de Marche et d'Arrêt) /ADEPA 81/ comme dans /BILAND 94/ par des états.

A titre d'exemple, nous pouvons donner, dans le cadre de l'étude des systèmes flexibles de production manufacturière, les modes suivants /KERMAD 96/ :

— les modes de marche : automatique, cycle par cycle ou pas à pas ;

— les modes d'arrêt : hors tension, en fin de cycle, dans un état déterminé ;

— les modes de fonctionnement : normal, dégradé ou hors service ;

— les modes d'exploitation ou d'utilisation : test, production, maintenance ;

— les modes opératoires qui spécifient le type d'opérations effectuées sur le produit.

On peut enrichir ce GEMMA par l'utilisation du modèle de comportement proposé par /BILAND 94/. Il modélise, selon différents points de vue (fonction commande, fonction maintenance, fonction conduite), le comportement des systèmes automatisés de production. Il intègre pour cela, au niveau de son modèle, des informations qui permettront :

— à la fonction commande, de contrôler l'effet d'un ordre donné au système ;

— à la fonction maintenance, d'être informée sur l'état de panne du système et d'enclencher alors des procédures de reconfiguration ou de maintenance ;

— à la fonction conduite, d'allumer par exemple un voyant pour prévenir l'opérateur de l'état de panne du système.

L'ensemble de ces informations vise à améliorer la sûreté de fonctionnement du système.

Il introduit de plus la notion de temporisateur qui, activé par la fonction commande, doit permettre de détecter la panne du système si une information de bonne exécution de l'ordre n'est pas renvoyée dans un temps donné.

Cette notion de temporisateur peut s'avérer intéressante dans le cadre de l'étude du comportement de la chaîne opératoire. En effet, en associant des temps d'exécution aux fonctions opératoires, on pourra, par diverses simulations, déceler les éventuels points faibles de la chaîne et mettre alors en place des moyens ou des procédures pour les éliminer. A partir de là, des modèles de comportement plus complexes peuvent être mis en oeuvre. Ils permettront par exemple, de simuler des mouvements d'ensembles, des déplacements d'éléments, des parties opératives de systèmes (à l'aide de l'outil SIMAC de la société Prosyst par exemple), ...

Dans le cadre de notre problématique, les modes sur lesquels va se focaliser notre étude sont relatifs au fonctionnement du système. Il est en effet important, dans le cadre de la sûreté de fonctionnement, de connaître d'une part le fonctionnement normal du système et d'autre

part, les fonctionnements anormaux, dégradés, qu'il peut avoir suite à l'apparition d'une défaillance ou d'une dégradation d'un ou de plusieurs de ses constituants.

2.2.2. Modèle de représentation associé à ce concept

Le modèle de représentation associé à ce concept est, comme pour la chaîne opératoire nominale (fonctionnement normal), le graphe d'état. Les états recensés associés aux objectifs de sûreté de fonctionnement à atteindre vont faire apparaître la nécessité de mettre en place des moyens de surveillance, de redondance, ou de maintenance. Le choix entre ces différentes solutions sera également lié au type du mode de défaillance et donc au type d'événements qu'il engendre (non fiabilité, indisponibilité, non sécurité).

A partir des modes de défaillance, l'étude aboutit à la modification de la chaîne opératoire nominale. De nouveaux états lui sont associés comme le montre la figure 2 ci-après. Des modes de marche représentant les états vers lesquels on veut alors conduire le système afin de respecter les exigences de sûreté demandées par le client sont de ce fait introduits. Des actions visant à mettre en redondance des fonctions de la chaîne opératoire (voire la chaîne opératoire complète) ou des actions proposant d'instrumenter cette chaîne ou quelques unes de ses fonctions opératoires dans le cadre de la surveillance, sont alors proposées.

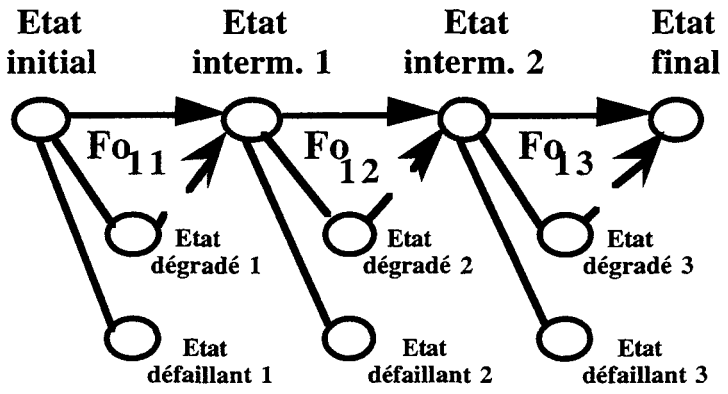

Figure 2 : Traduction des AMDE dans la chaîne opératoire

Ce concept de mode de marche permet d'introduire au niveau de la chaîne opératoire des alternatives au comportement nominal lorsque des défaillances ou des dégradations apparaissent. Nous donnons dans le paragraphe suivant une représentation algébrique de ce concept.

2.2.3. Expression algébrique du concept " Mode de marche "

Il a été défini, pour l'ensemble des fonctions opératoires, un ensemble $\emptyset_{Eo}$ des états φ_{eo} du flux d'entrée des fo_{ij} avec i, j > 0 et un ensemble $\emptyset_{So}$ des états φ_{so} du flux de sortie de ces mêmes fo_{ij}.

Par rapport au graphe de la figure 2, nous pouvons entre autres ajouter deux autres ensembles :

— un ensemble $\emptyset_{deg}$ des états dégradés φ_{deg} du flux de sortie des fo_{ij} caractérisant une baisse des performances de la fonction fo_{ij} ;

— un ensemble $\emptyset_{déf}$ des états défaillants $\varphi_{déf}$ du flux de sortie des fo_{ij} caractérisant une perte de la fonction fo_{ij}.

On peut donc définir le concept " Mode de marche " comme étant un opérateur qui à un flux d'entrée des fo_{ij} associe un flux de sortie définissant l'état vers lequel on veut mener le système. Nous définissons cet opérateur comme suit :

$$MM : \{\emptyset_{Efoij}\} \longrightarrow \{\emptyset_{Sfoij}\}$$
$$\varphi_{efoij} \xmapsto{mm} \varphi_{sfoij}$$

avec : $\{\emptyset Efoij\}$: ensemble des états $\varphi efoij$ du flux d'entrée des fo_{ij}

$\{\emptyset Sfoij\} = \{\emptyset deg, \emptyset déf, \emptyset test, ...\}$= ensemble des états $\varphi foij$ anormaux du flux de sortie des fo_{ij}

MM : ensemble des modes de marche "mm" tel que :

$$\forall mm \in MM$$
$$mm(\varphi_{efoij}) = \varphi_{sfoij}$$

Pour une fonction opératoire donnée, le passage du flux d'entrée au flux de sortie se fait par l'intermédiaire d'une opération " o " associée à la fonction opératoire. Dans le cas où cette opération n'est pas effectuée dans des conditions " normales ", le flux de sortie n'est alors pas celui attendu, d'où l'apparition de modes de fonctionnement anormaux.

L'objectif de ce niveau représentation des exigences fonctionnelles est de lister les modes de défaillance des fonctions opératoires (flux de sortie autre que celui attendu) et de recenser les procédures qui peuvent être mises en place pour contourner ces modes de défaillance et obtenir le flux de sortie souhaité (modes de marche).

Pour déceler au plus tôt ces modes de défaillance (comportement non nominal du produit) et basculer sur le mode de marche le plus approprié (secours, redondance, arrêt pour maintenance, ...), il convient de mettre en oeuvre des moyens de surveillance et de diagnostic dont l'objectif sera de garantir la sûreté de fonctionnement du produit. La définition de ces moyens s'effectue au niveau de représentation suivant, le niveau technologique.

3. Niveau Représentation technologique

Ce niveau permet de représenter la structure technologique du système d'un point de vue fonctionnel. Cette structure est définie par l'intégration des points de vue des différents métiers de la conception (automatique, mécanique, maintenance, ...).

A cet effet sont dégagées différentes fonctions de base propres à chaque métier et visant à mener une conception simultanée du produit. C'est donc un concept commun à chacun des concepteurs mais spécifique à leur métier (point de vue).

Dans le cadre de la conception de systèmes sûrs, les fonctions de base que nous avons identifiées sont dédiées à l'exploitation future du produit à concevoir. A partir de l'étude menée au niveau précédent (identification *a priori* des défaillances possibles, proposition d'alternatives pour les contrer), ces fonctions ont pour objectif de déceler la présence d'une défaillance ou d'une dégradation (fonctionnement anormal du système) puis de corriger ce fonctionnement en basculant par exemple le système (de façon automatique ou manuelle) vers un mode de fonctionnement plus approprié (redondance, arrêt dans une position sécuritaire, arrêt pour maintenance). Nous allons décrire, dans le paragraphe suivant, le concept " Fonction de base " qui permet de représenter les activités décrites précédemment.

3.1. Le concept " Fonction de base "

A partir des informations produites par le niveau précédent (chaîne opératoire notamment), chacun des acteurs étudie de façon concourante le produit à concevoir. Il décrit pour cela chacune des fonctions opératoires de plus bas niveau (élémentaires) à l'aide de fonctions de base dédiées métier.

Une fonction de base /JACQUET 98/ *permet d'assurer, de façon autonome et spécifique à un métier, une fonction particulière du produit. On peut, par exemple, distinguer les fonctions de base de la mécanique, de l'automatique, de l'exploitation, ...*

Le passage des fonctions opératoires de bas niveau aux fonctions de base se fait par l'intermédiaire d'une transformation Tr_{FB} telle que :

$$Fo_{nk} \xrightarrow{Tr_{FB}} FB$$

avec Fo_{nk} : fonction opératoire de plus bas niveau (élémentaire)

FB : ensemble des fonctions de base décrivant Fo_{nk}

Tr_{FB} : opérateur de conception au niveau technologique

Une fonction opératoire élémentaire est donc réalisée à partir d'une ou de plusieurs fonctions de base qui peuvent être de natures mécanique, automatique ou exploitation.

Algébriquement, le concept " Fonction de base " peut s'exprimer ainsi :

$$FB = FBa \cup FBm \cup FBe$$

FB = ensemble des fonctions de base décrivant les fonctions opératoires élémentaires

FBa = ensemble des fonctions de base "fba_k" de type Automatique

FBm = ensemble des fonctions de base "fbm_k" de type Mécanique

FBe = ensemble des fonctions de base "fbe_k" de type Exploitation

Ces fonctions de base ont pour objectif d'apporter des solutions aux problèmes que les concepteurs ont à résoudre par l'utilisation de modèles, de méthodes et d'outils spécifiques à leur domaine. L'ensemble des fonctions de base permet alors de décrire, d'un point de vue technologique, le support qui sera associé à chacune des fonctions opératoires tout en répondant aux besoins spécifiés par le client.

Nous allons, dans les paragraphes suivants, décrire les fonctions de base associées à chacun des métiers de la conception que nous prenons en considération, et plus particulièrement celles dédiées Exploitation.

3.1.1. Fonctions de base dédiées Mécanique

L'objectif du mécanicien est de définir la structure mécanique du produit à concevoir. Pour cela, différentes fonctions de base sont utilisées dans l'objectif de décrire, d'un point de vue cinématique, chacune des fonctions opératoires. L'ensemble de ces fonctions de base "mécanique" constituera la solution mécanique répondant au besoin. Ainsi, des fonctions de base de type "Liaison complète", "Guidage en translation", "Guidage en rotation", "Guidage

hélicoïdal", "Guidage en translation et en rotation",... peuvent être distinguées /COCQUEBERT 90/.

Parallèlement à cette étude, l'automaticien spécifie quant à lui ses fonctions de base.

3.1.2. Fonctions de base dédiées Automatique

L'automaticien va spécifier pour sa part la structure et les algorithmes de commande à associer aux différentes fonctions de base définies par le mécanicien (dans le cas où celles-ci sont commandables). Il spécifie également l'architecture et les algorithmes de commande du système complet (c'est-à-dire l'ensemble de la chaîne opératoire). Pour cela, il peut faire appel à des fonctions de base telles que /JACQUET 98/ "Communiquer entre composants matériels", "Dialoguer avec l'opérateur", "Coordonner", "Commander", "Contrôler", ...

Quant à l'aspect "conception pour l'exploitation", les fonctions de base associées sont présentées au paragraphe suivant.

3.1.3. Fonctions de base dédiées Exploitation

Les fonctions de base Exploitation utilisées par le maintenicien visent à caractériser le produit (système) en vue de son exploitation future. Le maintenicien doit définir comment déceler un fonctionnement anormal du système et proposer alors les moyens de maintenir ou de contrer ce mode de fonctionnement. Ces activités peuvent être réalisées de façons différentes (maintenance, reconfiguration) mais sont directement liées aux fonctionnalités que doit posséder un système de surveillance /BRUNET 92/.

En effet, la surveillance /CASSAR 94/ s'inscrit dans un processus global de conduite et de supervision d'un système et vise, à partir des informations disponibles sur son état de fonctionnement (commandes, mesures et, éventuellement, modèles de comportement), à détecter, à localiser et à diagnostiquer les défaillances qui peuvent affecter ses performances et sa sûreté de fonctionnement.

Ces différentes activités visent, le cas échéant, à déterminer et à engager les actions permettant de ramener, au mieux, le système dans un état normal, tant du point de vue du potentiel productif que du respect des contraintes de sécurité lors d'une défaillance. Ces actions peuvent être des émissions d'alarmes ou d'ordres d'arrêt d'urgence, des lancements de réparations ou d'opérations préventives ou encore des reconfigurations matérielles ou logicielles des éléments du système. Ces actions découlent directement de l'étude menée au niveau de représentation précédent ou peuvent être déterminées suite à la définition des modes de défaillance matérielle des composants au niveau représentation technique (paragraphe 4.2.2.).

Ainsi, d'un point de vue strictement Exploitation, nous pouvons écrire algébriquement une fonction de base de la façon suivante :

$$\mathbf{FBe = \{(Fo_{nk}, sp_k, Coe_k, Proced_k, Tr_{Co})\}}$$

FO_{nj}= ensemble des fonctions opératoires fo_{nk} de niveau n ; $fo_{nk} \in FO_i$ avec i = n ; $FO_{nj} \subset FO_i$

SP = ensemble des solutions de principes "sp_k"

FBe = ensemble des fonctions de base "fbe_k" de type Exploitation

COe = ensemble des composants exploitation "coe_k" associés à FBe

PROCED = ensemble des procédures "proced$_k$" associées à FBe. Proced$_k$ peut être considérée comme un opérateur de transformation Tr tel que :

$$\{Tr\} : X \longrightarrow Y$$

$$x \xmapsto{tr} tr(y)$$

avec : x : informations/données ou état d'entrée pour la réalisation de la fonction de base considérée ;

y : informations/données ou état de sortie après réalisation de la fonction de base considérée ;

Tr_{Co} = opérateur de transformation qui à fbe_k —> (coe_k, proced$_k$)

A chacune des fonctions de base Exploitation, nous pouvons associer une procédure. Celle-ci va permettre de définir comment la fonction de base à laquelle celle-ci est associée sera mise en oeuvre.

Une fonction de base Fb (mécanique ou automatique) permet d'assurer une fonction opératoire fo_{nk} en respectant un principe "p_k". D'un point de vue Exploitation, une fonction de base est introduite pour que la fonction opératoire soit assurée même en cas de défaillance ou de dégradation. Pour cela, la fonction de base Exploitation est caractérisée par un composant "coe" et une procédure "proced".

En ce qui concerne les fonctions de base dédiées Exploitation, celles-ci sont directement liées aux activités de la surveillance. Nous distinguons donc les fonctions de base suivantes :

— **Réaliser l'acquisition des données / informations de surveillance** : fonction de base en vue de la conception de l'exploitation qui, au travers d'un composant, permet de capter des informations sur l'état du système sous surveillance.

Cette activité d'*acquisition* des informations est constituée du relevé des signaux et de l'acquisition des données et paramètres définissant l'état actuel du processus ou de l'équipement sous surveillance. Cette opération est obtenue au moyen de capteurs de types différents suivant les grandeurs que l'on souhaite acquérir. On distingue ainsi /PRIEUR 95/ :

a) les *détecteurs* assurant les sécurités élémentaires de fonctionnement. Ils sont essentiellement destinés à donner, par un signal de type tout ou rien, l'état d'un composant (ouvert, fermé) et à éviter les manoeuvres inappropriées ;

b) les *capteurs dits classiques* destinés à la mesure de pression, température, niveau, débit, vitesse, vibrations, ... ;

c) les *analyseurs ou capteurs spéciaux* utilisés pour effectuer des relevés très spécifiques et pouvant demander une grande précision ;

— **Détecter la défaillance** : fonction de base en vue de la conception de l'exploitation qui, au travers des informations de surveillance associées à un composant, permet de déceler un fonctionnement anormal de la fonction opératoire ou du composant considéré(e).

L'activité qui précède celle de détection est celle de *réduction* de données. Celle-ci consiste à extraire, des données acquises, des paramètres ou des symptômes significatifs de l'état du système. Les méthodes réalisant cette fonction peuvent être schématiquement classées en deux catégories : à base de traitement du signal et à base de modélisation. Les méthodes à base de traitement du signal comprennent l'analyse temporelle du signal et des traitements statistiques (tels que les calculs de moyenne, variance, corrélations, tendance) et l'analyse fréquentielle qui utilise la transformée de Fourier et l'analyse de spectre. Les méthodes à base de modè-

les permettent quant à elles de lier à travers des relations de cause à effet les variables observées.

A partir des données significatives issues de la phase de réduction est réalisée l'activité de *détection*. Elle consiste à mettre en regard l'état actuel du système avec un état désiré prédéterminé. La détection d'un état anormal fournit des symptômes qui constituent les données d'entrée de l'opération suivante qui est le diagnostic. Cette phase de détection comporte un risque d'erreur qui se mesure en terme de probabilité de donner une mauvaise réponse : une probabilité de fausse détection c'est-à-dire que l'on détecte un défaut alors qu'il n'y en a pas (erreur préjudiciable conduisant à des reconfigurations ou des arrêts en pure perte) ; une probabilité de non-détection de panne caractérisée par l'omission d'un défaut qui, ultérieurement, peut entraîner une panne. Cette étape de détection peut être basée sur l'établissement des seuils et des tests relatifs aux paramètres issus de l'étape de réduction de données mais est néanmoins sous-tendue /BRUNET 90/ par une analyse statistique reposant sur une période d'apprentissage ;

— **Localiser la défaillance** : fonction de base qui permet de situer le composant à l'origine de la défaillance ou de la dégradation ;

— **Diagnostiquer la défaillance** : fonction de base qui permet de donner la cause première ayant entraîné la défaillance ou la dégradation du composant.

L'activité de *diagnostic* consiste à analyser des symptômes sur la base de stratégies systématiques de localisation du défaut (attribution de celui-ci à des modules de type capteurs, organes de commande, processus, unité de commande) et à déterminer le type, la cause et le degré de sévérité de celui-ci. Comme nous l'avons déjà dit, les modes de fonctionnement d'un système /DUBUISSON 90/ peuvent être normaux, anormaux (modes interdits, défaillants, dégradés ou critiques), exceptionnels ou encore évolutifs. Le *diagnostic* d'un système nécessite alors la reconnaissance de son mode de fonctionnement, l'identification et la localisation de sa cause, et le suivi décisionnel concernant les opérations à effectuer pour maintenir ou contrer ce mode. Ainsi, nous pouvons dire qu'un système est diagnosticable /DUBUISSON 90/ s'il est susceptible d'être soumis à un diagnostic c'est-à-dire s'il est muni d'organes d'observation (capteurs) et d'un système d'analyse pour étudier les informations fournies. Dans le cadre de modes de fonctionnement anormaux, domaine de la maintenance, le diagnostic /AFNOR 88/ est défini comme *l'identification de la cause probable de la (ou des) défaillance(s) à l'aide d'un raisonnement logique fondé sur un ensemble d'informations provenant d'une inspection, d'un contrôle ou d'un test.*

L'activité de diagnostic peut être parfois associée à une activité de *pronostic* qui vise, quant à elle, à analyser les dérives d'état des éléments du système, à établir leurs causes et à déterminer le temps de fonctionnement correct qui subsiste avant la défaillance des éléments défectueux, ceci en vue de la planification d'une intervention préventive ; le pronostic repose soit sur une connaissance *a priori* des lois d'évolution des phénomènes de vieillissement, soit sur une phase d'apprentissage ;

— **Réaliser la correction de la défaillance** : fonction de base en vue de la conception de l'exploitation qui, au travers d'un composant, permet de solutionner le problème généré par la défaillance (basculement sur un élément redondant, mode dégradé, maintenance ...).

Cette fonction de base, fortement liée au concept de mode de marche, a un double objectif : tout d'abord, permettre au concepteur de sélectionner le mode de correction qu'il souhaite mettre en place pour contrer l'apparition des défaillances ou des dégradations ; ensuite, spécifier les procédures qui seront à mettre en oeuvre pour effectivement corriger le problème présent (basculement automatique ou manuel sur l'élément redondant, description des gammes de maintenance, ...).

En définitive, cette activité de *prévision d'actions*, correctives et préventives, permet de choisir les modes d'actions permettant de redresser un état défectueux, d'éviter des défauts prévus ou de minimiser les conséquences de pannes inévitables. Ces actions peuvent être des émissions d'alarmes, d'avertissements ou d'ordre d'arrêt d'urgence ; des lancements de réparations ou d'actions de maintenance préventive ; des reconfigurations de matériel ou de logiciel du système ; des remaniements du programme de production ; des modifications des conditions du process ; la fourniture d'informations au niveau élevé de commande dans le but de modifier la conception de la machine ou du produit.

— **Informer l'opérateur** : fonction de base qui permet d'attirer l'attention de l'opérateur sur l'apparition d'un fonctionnement anormal d'un composant.

Cette activité est liée à la précédente et en particulier au mode de correction qui a été choisi. Elle a pour objectif de prévenir l'opérateur qu'une action de correction (basculement sur un élément redondant) a été entreprise automatiquement ou qu'il doit réaliser certaines tâches pour qu'elle puisse l'être de façon manuelle. Dans le cas où c'est une action de maintenance qui doit être entreprise, il est également nécessaire de prévenir l'opérateur des tâches qu'il doit réaliser (de façon autonome ou avec l'aide du personnel de maintenance).

Le modèle de représentation associé à ces différentes fonctions de base est un modèle symbolique (utilisation par exemple de rectangles et de liaisons entre eux). Cependant, en reliant chacune des fonctions de base entre elles, nous obtenons un schéma fonctionnel qui représente, graphiquement, le produit en cours de conception.

A partir de la définition de ces différentes fonctions de base, nous pouvons introduire le concept "Solution technologique".

3.2. Le concept "Solution technologique"

Ce concept vise à définir l'ensemble des fonctions de base retenues pour réaliser la fonction d'exploitation d'une partie ou de la totalité de la chaîne opératoire.

La définition algébrique de ce concept est la suivante :

$$sto = COa \cup COm \cup COe \quad \text{avec} \quad sto \in STo$$

STo = ensemble des solutions technologiques "sto"

COa = ensemble des composants Automatique "coa_i" caractérisant FBa

COm = ensemble des composants Mécanique "com_i" caractérisant FBm

COe = ensemble des composants Exploitation "coe_i" caractérisant FBe

COe = $\{(coe_i, te_i)\}$ $coe_i \in COe$; $te_i \in Te$

Te = ensemble des technologies "te_i" associées aux composants COe

FBe = ensemble des fonctions de base "fbe_k" de type Exploitation

La solution technologique de l'automaticien consiste à définir l'architecture de commande de la chaîne opératoire. Il peut décrire cette solution par l'intermédiaire du Modèle d'Exploitation des Systèmes Automatisés de Production (M.E.S.A.P.) /PARAYRE 92/ présenté figure 3.

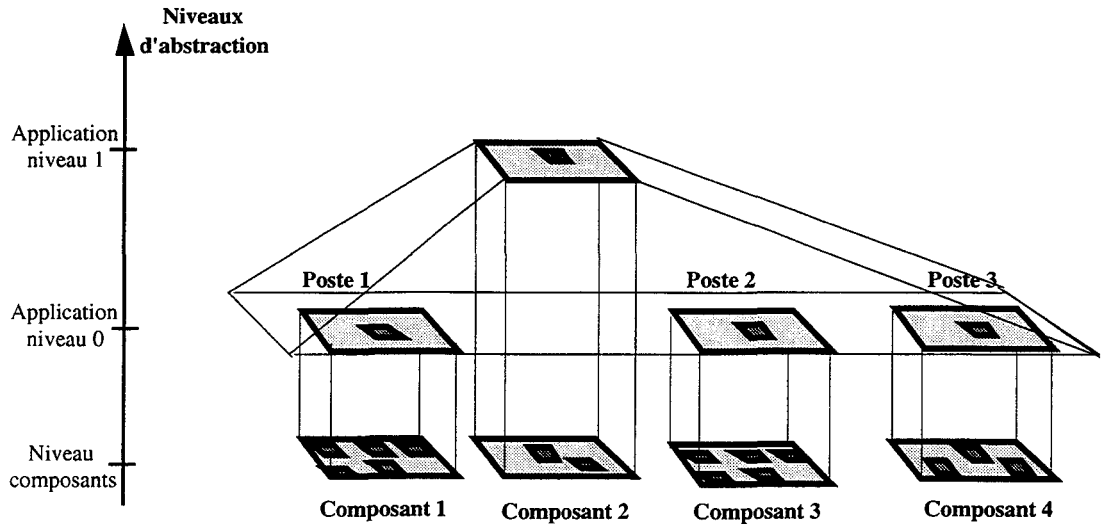

Figure 3 : Exemple d'architecture M.E.S.A.P.

Ce concept permet à l'automaticien de prendre en compte les différents modes d'exploitation que le maintenicien a pu définir précédemment pour chaque fonction opératoire élémentaire. Ces modes d'exploitation (secours, reprise, ...) peuvent conduire à mettre en redondance certains composants de commande. De même, les procédures de reconfiguration mises en évidence par les études précédentes (modes de défaillance possibles d'une part, fonctionnements alternatifs visant à contrer leur apparition d'autre part), imposent à l'automaticien la prise en compte de certaines contraintes.

Du point de vue du mécanicien, la solution technologique consiste à décrire, d'un point de vue cinématique, les différentes fonctions opératoires définies au niveau représentation des exigences fonctionnelles. Il peut décrire de cette même façon l'ensemble ou le sous-ensemble qu'il a réalisé pour structurer les fonctions opératoires (définies au niveau représentation des exigences fonctionnelles) ou les fonctions de base (définies à ce niveau).

Du point de vue du maintenicien, la solution technologique permet de décrire l'architecture d'instrumentation et de surveillance associée au produit (pour basculer sur une solution alternative en cas de défaillance c'est-à-dire une redondance ou une procédure d'arrêt pour maintenance). Il s'appuie pour cela sur l'architecture de commande définie par l'automaticien en y intégrant les aspects instrumentation, modes de marche, ...

Nous proposons donc, pour représenter ce concept "Solution technologique" d'un point de vue exploitation, d'utiliser, comme l'automaticien, le M.E.S.A.P. Ce concept peut être rapproché de celui d'Unité Fonctionnelle (UF) définie par /PARAYRE 92/. Ainsi, une unité fonctionnelle :

— décrit le comportement des modes de marche d'une partie d'un composant ou d'une application ;

— distingue différentes familles de modes de marche (arrêt, fonctionnement, défaillance) ;

— dispose d'un modèle de comportement.

Au niveau composant, quatre unités fonctionnelles, décrivant les différents types de modes de marche peuvent être distingués :

— l'U.F. de la Partie Commande (PC) qui prend en compte, pour un composant donné, ses modes opératoires (programmation, réglage, maintenance, ...) ;

— l'U.F. de la Partie Communication (PCo) qui indique le mode de marche du communicateur (déconnecté, connecté, défaillance) ;

— l'U.F. de la Partie Contrôle (PCt) qui prend en compte les aspects hors énergie, arrêt, fonctionnement, défaillance ;

— l'U.F. de la Partie Opérative (PO) qui est la constituante matérielle du composant. Elle fait apparaître les aspects hors puissance, à l'arrêt, en fonctionnement, en défaillance.

Ce niveau composant est générique et réutilisable pour tous types de composants constituant un produit ou un système quel qu'il soit.

Au niveau application, deux unités fonctionnelles décrivant les différents types de modes de marche sont distingués :

— l'U.F. de la Partie Exploitation (PE) qui correspond à la partie "logiciel utilisateur" du M.E.S.A.P. Sont introduits ici les termes du métier ou de l'application du composant. Nous pouvons associer cette unité fonctionnelle à l'exploitation de la partie commande des différents composants technologiques utilisés ;

— l'U.F. de la Partie Production (PP) qui reflète, par exemple, le bon déroulement des opérations par rapport à une gamme (ou une procédure) bien définie.

En définitive, le niveau technologique permet de définir l'architecture technologique du produit. Chaque acteur de la conception spécifie, de manière concourante, les composants technologiques associés à leurs fonctions de base respectives. Au niveau suivant, le niveau technique, chaque acteur affine ses choix en associant une technique à chaque solution technologique. Nous allons, dans le paragraphe suivant, présenter ce niveau de représentation en nous attachant à l'aspect exploitation uniquement.

4. Le niveau Représentation technique

Ce niveau a pour objectif de modéliser les entités techniques du système. Il s'agit, à partir des choix technologiques faits au niveau précédent, d'associer aux fonctions de base constituant la solution technologique, un ou plusieurs composants techniques. Pour cela, nous avons distingué les concepts suivants : le concept "Solution technique" qui correspond au composant ou au sous-ensemble de composants que l'on peut associer aux fonctions de base décrivant la solution technologique définie par le concepteur ; le concept "Mode de défaillance matérielle" qui consiste à identifier et modéliser *a priori* les défaillances pouvant apparaître au niveau des composants techniques choisis (il correspond à un affinement de l'analyse des défaillances menée au niveau fonctionnel). Nous allons dans les paragraphes suivants présenter plus en détail ces différents concepts.

4.1. Le concept " Solution technique "

Ce concept a pour objectif de préciser les choix technologiques en associant aux différentes fonctions de base un support matériel. Ainsi, du point de vue exploitation et suivant la fonction de base à assurer, les composants utilisés pourront être les suivants :

— le support de la fonction "**Acquérir des informations**" peut être un capteur ou une carte d'acquisition. Pour garantir la crédibilité des informations et s'assurer ainsi que le problème se trouve effectivement sur le système sous surveillance (et mettre ainsi hors de cause le capteur réalisant la mesure), des capteurs intelligents pourront être utilisés ;

— le support des fonctions de base "**Détecter la défaillance**", "**Localiser la défaillance**" et "**Diagnostiquer la défaillance**" peut être un ordinateur au sein duquel seraient regroupés différents logiciels permettant de remplir ces fonctions. Elles pourront être supportées par des composants différents suivant le type de commande utilisé (automate, calculateur, ...). Bien entendu, dans le cas où une action automatisée n'est pas nécessaire, c'est un simple schéma, une procédure, ... qui seront utilisés pour supporter ces fonctions ;

— le support de la fonction "**Informer l'utilisateur**" peut être un voyant, une alarme, un écran (d'ordinateur ou autre) sur lequel on vient présenter un message. Cette fonction peut être considérée comme l'interface entre le système de surveillance et le (ou les) opérateur(s) ;

— le support de la fonction "**Réaliser la correction de la défaillance**" peut être identique à celui de la fonction précédente. On peut indiquer à l'utilisateur une procédure à suivre ou lui indiquer l'action entreprise de façon automatique. Si la correction prévue est une intervention de maintenance, le support utilisé pourra être une procédure à suivre pour effectuer cette intervention dans les meilleures conditions possibles.

Nous pouvons ainsi définir une solution technique comme *un ensemble de composants techniques. Un composant technique est, du point de vue du maintenicien, une fonction de base à laquelle on associe une technique (spécifique à chaque métier) et un comportement (afin de connaître comment un système réagit face à différents stimuli).*

Ce concept de "Solution technique", d'une partie ou d'une ou de plusieurs chaînes opératoires, peut s'exprimer sous une forme algébrique de la façon suivante :

$$stte = COtea \cup COtem \cup COtee$$

$$\mathbf{COtee = \{(coe_i,\ tec_i,\ comp_i)\}}$$

$coe_i \in COe$; $tec_i \in TEC$; $comp_i \in COMP$

STte = ensemble des solutions techniques {stte}

COtea = ensemble des composants techniques Automatique "cotea$_i$" caractérisant FBa

COtem = ensemble des composants techniques Mécanique "cotem$_i$" caractérisant FBm

COtee = ensemble des composants techniques Exploitation "cotee$_i$" caractérisant FBe

TEC = ensemble des techniques "tec$_i$" associées à COe

COe = ensemble des composants technologiques "coe$_i$"

FBe = ensemble des fonctions de base "fbe$_k$" de type Exploitation

COMP = ensemble des comportements "comp$_i$" associés à COte

COte = {COtea, COtem, COtee} = ensemble des composants techniques

L'ensemble des solutions techniques définies par l'automaticien, le mécanicien et le maintenicien, définit la structure du produit. Chacune de ces entités peut être regroupée pour former un ensemble ou un sous-ensemble. Cette notion sera présentée plus en détail au paragraphe 6.

Différents modèles de représentation peuvent être associés à ce concept de solution technique. Ainsi, le dessin technique peut être utilisé pour donner une vue globale du produit et de ses différents constituants. A partir de là peuvent être établies des procédures de maintenance préventive à mettre en place ainsi que la liste des pièces de rechange associée.

Par contre, si l'on s'attache à l'aspect comportemental des éléments, des modèles du type fonction de transfert, graphe causal, ... peuvent être utilisés. Ici également, des modèles de comportement tels que le temporisateur défini par /BILAND 94/, des modèles de simulation de mouvements, ... (déjà abordés à la page 33) pourront être utilisés. Dans ce cas, nous pouvons associer un ou plusieurs modèles de représentation par fonction de base selon le composant technique choisi.

Les solutions techniques qui auront été définies à ce niveau vont comme les fonctions opératoires avoir un comportement nominal et des comportements anormaux (défaillant, dégradé, ...). Pour prendre en considération cette notion de comportement à ce niveau de représentation, nous ajoutons au modèle de produit un nouveau concept : celui de "mode de défaillance matérielle". Nous le décrivons dans le paragraphe suivant.

4.2. Le concept " Mode de défaillance matérielle "

Ce concept vise à modéliser pour chacun des composants techniques définis par chacun des acteurs de la conception, leurs modes de défaillance, leurs causes et leurs effets. Cette modélisation va permettre de décrire les différents comportements que chaque composant pourra avoir suite à l'apparition d'une défaillance ou d'une dégradation. Il s'agira ensuite, en fonction du type de comportement présent, de mettre en oeuvre des actions visant à le contrer (mise en redondance du composant, moyen de surveillance et de diagnostic, procédure de maintenance, ...).

Le modèle de représentation associé à ce concept est le tableau AMDE (tableau 3). A ce niveau de représentation, nous disposons maintenant d'informations sur les composants aptes à réaliser les fonctions recensées aux niveaux supérieurs. Nous définissons donc ici une AMDE matérielle.

Composant	Modes de défaillance	Causes	Effets
Moteur	Ne fournit pas de couple	Bobinage en court-circuit	Le tapis n'est pas mis en mouvement
		Arbre bloqué	
	Échauffement moteur	Défaillance bobinage	Détérioration du moteur
		Surcharge	

Tableau 2 : Exemple d'AMDE matérielle

Cette analyse qualitative des modes de défaillance peut être enrichie par une analyse quantitative. Celle-ci va consister à associer à chacun des modes de défaillance identifiés une fréquence d'apparition ainsi qu'une gravité à leurs conséquences. Ces deux informations seront obtenues sur la base des connaissances du concepteur ou à partir de données issues du retour d'expérience ou de banques de données. Ces deux grandeurs définissent donc la criticité du mode de défaillance considéré. Le modèle de représentation utilisé alors est le tableau AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité).

4.2.1. Expression algébrique du concept " Mode de défaillance matérielle "

De la même façon que nous avons mis sous forme algébrique les informations contenues dans le tableau d'analyse AMDE fonctionnelle (paragraphe 2.1.2. de ce chapitre) nous pouvons adopter la même démarche pour le tableau d'analyse AMDE matérielle.

On dispose là aussi :

— d'un ensemble Mo_m de Modes de défaillance matérielle ;

— d'un ensemble Ca_m de Causes associées ;

— d'un ensemble Ef_m d'Effets.

On peut également définir une relation de défaillance matérielle pour chacun des constituants associés à une fonction opératoire telle que :

$$Rd_m(Comp_i) \subseteq (\phi(Mo_m) \times \phi(Ca_m) \times \phi(Ef_m))$$

avec : Rd_m : relation de défaillance matérielle associée au composant ;

Ø : ensemble des partitions ;

x : produit cartésien.

Selon les conséquences (effets) que peut avoir l'apparition des défaillances, des actions vont alors devoir être mises en oeuvre. Nous présentons dans le paragraphe suivant le type d'actions qui peuvent être entreprises.

4.2.2. Types d'actions à mettre en place

Suivant les causes et les effets des défaillances ou des dégradations, des modifications constructives pourront alors être définies sur l'architecture et le dimensionnement des systèmes (accessibilité aux sous-ensembles et composants, modularité, facilité d'échange, ...) ainsi que des améliorations relatives à leur fiabilité et leur maintenabilité (réduction des conséquences des défaillances inévitables, proposition de recommandations de maintenance préventive, ...). Pour cela, différents types d'actions peuvent être mis en oeuvre. Ils comprennent :

— des actions de *prévention* des défaillances consistant à éviter ou limiter l'apparition de causes ou de modes de défaillance et supprimer les causes et les modes existants ;

— des actions de *réduction* des effets des défaillances où l'on va chercher à interrompre le plus tôt possible l'enchaînement des effets, à limiter les temps d'indisponibilité, à réduire les temps d'intervention et les coûts de maintenance corrective, ainsi que les impacts sur la sécurité et l'environnement ;

— des actions de *détection* de ces défaillances par la mise en oeuvre de moyens, dispositifs ou procédures pour détecter de façon précoce une anomalie. Ces moyens seront mis en oeuvre suivant la fréquence mais surtout suivant la gravité des effets de ces modes.

Selon leur type, ces actions peuvent être mises en oeuvre à ce niveau de représentation (technique) ou aux niveaux de représentation précédents. Ainsi des alternatives au fonctionnement normal d'une fonction opératoire pourront être introduites pour contrer certaines de ses défaillances ou dégradations (paragraphe 2.2., niveau représentation des exigences fonctionnelles) ; des fonctions de base Exploitation pourront être ajoûtées afin de détecter au plus tôt l'apparition de ces défaillances ou dégradations (paragraphe 3.1.3., niveau représentation technologique).

Cependant, l'ensemble de ces actions n'est pas toujours facile à mettre en place dans le cadre de la conception de nouveaux systèmes. Les composants utilisés peuvent être de technologies nouvelles et les défaillances pouvant les affecter ne sont donc pas nécessairement connues, voire maîtrisées (pas ou peu de retour d'expérience). Cependant, l'utilisation de composants connus, mais dans des conditions différentes, n'engendrera pas obligatoirement les mêmes défaillances et il ne sera donc pas toujours aisé de définir des actions sur des défaillances dont l'apparition n'est pas certaine.

Par contre, dans le cadre d'une reconception, ces actions vont pouvoir et/ou devoir être mises en oeuvre de façon plus aisée que dans le cadre d'une nouvelle conception. En effet, nous cherchons dans ce cadre à améliorer un système existant en remédiant à des problèmes apparus lors de son exploitation. L'objectif va donc être de proposer des actions possibles en fonction de ce qui est déjà apparu et que l'on ne veut plus voir sur le "nouveau" système.

Pourtant, il ne sera pas toujours possible de proposer les actions de type prévention ou réduction. Aussi, pour garantir la sûreté du système, seules les actions de détection pourront être émises. Dans ce cas, l'apparition de défaillances ou de dégradations peut être décelée en phase d'exploitation, au moyen de signes avant-coureurs (symptômes) tels que les grandeurs caractéristiques associées au comportement de chaque entité. Celles-ci caractérisent leurs comportements (normaux et anormaux) sur lesquels sera basée la détection.

La mise en redondance de certains composants ou la définition de gammes de maintenance préventive sont également des actions qui peuvent être proposées dans le cas où les actions citées précédemment étaient difficiles voire impossible à mettre en oeuvre.

Après avoir spécifié, d'un point de vue technique, les divers composants pouvant supporter chacune des fonctions de base qui ont été identifiées, nous passons au niveau suivant afin de définir plus précisément les caractéristiques de ces différents composants.

5. Niveau Représentation détaillée

Du point de vue de la spécification de la sûreté de fonctionnement, ce niveau de représentation n'apporte aucune information supplémentaire (du point de vue fonctionnel) par rapport aux niveaux précédents concernant la description du modèle de produit. Cependant, il peut permettre d'affiner certaines informations relatives aux calculs des MTBF, des probabilités d'occurrence de certains événements indésirés, ... Ainsi, à partir de ces informations plus complètes, ce niveau de représentation va également permettre une évaluation plus précise de la sûreté de fonctionnement du produit conçu.

En fait, ce niveau permet simplement de supporter la description détaillée du produit selon le point de vue des différents acteurs de la conception. Ils peuvent donner les différentes caractéristiques de chaque composant retenu pour la conception du produit. Les concepts que nous avons identifiés à ce niveau sont le concept "Caractéristiques matérielles" et le concept "Codage". Ce sont des concepts communs aux différents acteurs de la conception. Cependant, pour ce qui est du point de vue de l'exploitation, ces concepts vont permettre :

— d'attribuer aux composants techniques associés aux fonctions de base des caractéristiques précises ;

— de coder les différentes procédures retenues pour réaliser la surveillance et le diagnostic des défaillances.

Nous décrivons ces concepts dans les paragraphes suivants.

5.1. Le concept " Caractéristiques matérielles "

Ce concept vise à définir les caractéristiques des différents composants utilisés pour concevoir le produit. Ces caractéristiques découlent des concepts définis au niveau précédent et plus particulièrement des concepts "solution technologique" et "solution technique". Nous obtenons suite à cela un composant complètement spécifié. Du point de vue algébrique, nous pouvons définir ce concept de la façon suivante :

$$CM = CM_a \cup CM_m \cup CM_e$$

$$\mathbf{COsp = \{(COte,\ CM,\ Tr_{cm})\}}$$

COsp = ensemble des composants spécifiés

$$COsp = COsp_a \cup COsp_m \cup COsp_e$$

COte = ensemble des composants techniques "cote"

Tr_{CM} = opérateur de transformation qui à $cosp_i$ —> $\{cm_i\}$; $cm_i \in CM$; $cosp_i \in COsp$

Ces caractéristiques sont déterminées à partir des problèmes à résoudre, des contraintes définies dans le cahier des charges et celles imposées par les autres intervenants.

Le modèle de représentation associé à ce concept peut être par exemple un tableau dans lequel sont regroupées les différentes caractéristiques du composant : référence, dimensions, tension d'utilisation, vitesse de rotation, ...

En ce qui concerne l'aspect sûreté de fonctionnement, les caractéristiques qui seront ajoutées aux composants spécifiés par le mécanicien et l'automaticien vont être relatives à leur comportement. Elles concernent leur fiabilité, leur taux de défaillance, ..., obtenues auprès du constructeur (fournisseur) ou par retour d'expérience.

5.2. Le concept " Codage "

Ce concept modélise la façon dont seront représentées et codées les informations que l'on aura pu acquérir sur le système. En d'autres termes, il définit comment sera codée la connaissance nécessaire et disponible sur le système afin de réaliser sa surveillance et le diagnostic de ses défaillances.

Il permet également de traduire les différentes procédures qui ont été associées à chacune des fonctions de base Exploitation. Les procédures définissent les opérations à réaliser ainsi que leur enchaînement. Le codage les transforme en un langage particulier directement lié au concept "solution technologique" car suivant le support retenu pour assurer les fonctions de base le codage sera différent. Si c'est un automate, un programme en langage à contacts (ladder) sera réalisé ; si nous choisissons un ordinateur, il faudra décrire la procédure en un langage informatique particulier (C, lisp, Pascal, ...) ou utiliser des règles de production si nous choisissons un générateur de système expert. La définition algébrique de ce concept est la suivante :

$$\mathbf{COD = \{(Proced_k,\ Tr_{cod})\}}$$

COD = ensemble des codages "cod_k" associés à Proced

PROCED = ensemble des procédures "$proced_k$" associées à FBe

FBe = ensemble des fonctions de base "fbe_k" de type exploitation

TR_{cod} = opérateur de transformation qui à $proced_k$ —> (cod_k)

On voit là aussi que les choix entrepris sont directement liés à ceux faits par les autres intervenants de la conception, notamment les choix de l'automaticien. Si celui-ci a choisi un automate programmable pour coordonner les différentes fonctions de base qu'il a retenues, le maintenicien pourra utiliser ce même support pour mettre en oeuvre ses propres fonctions de base.

6. Remarque

Au cours de la conception, il peut s'avérer nécessaire de structurer en ensembles ou en sous-ensembles les solutions retenues par chacun des concepteurs.

Dans un premier temps, cette structuration peut correspondre à une solution que le concepteur propose *a priori* pour répondre aux besoins du client. Ainsi, une ou plusieurs fonctions opératoires élémentaires peuvent être regroupées au sein d'un même ensemble en accord avec la "Solution de principes" retenue au niveau représentation des exigences fonctionnelles. Ce regroupement est effectué en fonction de divers critères directement liés aux fonctions contraintes globales. Ainsi, les aspects coût et sûreté de fonctionnement peuvent avoir une incidence directe sur les regroupements possibles de fonctions opératoires au sein d'un même ensemble technique.

Dans un second temps, ce regroupement peut se faire sur les différentes fonctions de base définies au niveau représentation technologique par chacun des acteurs de la conception (automaticien, mécanicien, maintenicien, ...). On cherche alors à utiliser des sous-ensembles existants permettant ainsi de regrouper les différentes fonctions de base au sein d'une même entité. Pour l'aspect "conception pour l'exploitation", la structuration des fonctions de base dédiées à la surveillance et au diagnostic des défaillances conduit à la définition de l'architecture de surveillance à intégrer au produit.

7. Synthèse

Ce dernier paragraphe se veut être une synthèse des concepts, utilisés pour la représentation du produit et la prise en compte des aspects sûreté de fonctionnement, qui ont été présentés tout au long de ce chapitre.

Aussi, la figure 4 ci-dessous apporte un niveau de détail plus important par rapport à la figure 1 du chapitre 1. En effet, elle reprend l'ensemble des concepts dédiés sûreté de fonctionnement qui ont été introduits au niveau du modèle de produit. Elle permet également de donner une vision globale ainsi que le positionnement des différents concepts les uns par rapport aux autres (liaison entre les concepts). Les notations utilisées sur ce schéma pour représenter chaque concept sont les mêmes que celles qui ont été adoptées pour leur définition algébrique.

Le produit, décrit dans le cahier des charges par le client, regroupe plusieurs *fonctions de service* (FS_i). Chacune d'elles doit respecter une ou plusieurs *fonctions contraintes globales* (FCG_i) parmi lesquelles figure la sûreté de fonctionnement. Les fonctions de service (FS_i) sont ensuite décomposées en *fonctions opératoires* (FO_i) qui peuvent à leur tour être décomposées en *fonctions opératoires élémentaires* (FO_{ij}).

A ces fonctions opératoires élémentaires (FO_{ij}), nous associons deux concepts dédiés à la sûreté de fonctionnement. Le premier est le concept *Mode de défaillance fonctionnelle* (Mof_i) qui consiste à caractériser l'ensemble des défaillances et dégradations pouvant survenir sur ces

fonctions opératoires. Le second concept est le concept *Mode de marche* (MM_j) qui vise quant à lui à apporter des solutions pour contrer l'apparition de ces défaillances et dégradations. Cela consiste par exemple à prévoir des procédures de mise en sécurité, de basculer sur une fonction en redondance ou prévoir l'arrêt pour effectuer une intervention de maintenance.

Au niveau représentation technologique, nous associons aux fonctions opératoires élémentaires (FO_{ij}) des *fonctions de base* (FB_i). Il existe différents types de fonctions de base (automatique, mécanique, ...) mais celles que nous considérons sont dédiées à la surveillance et au diagnostic de défaillance du produit. Elles vont permettre de déceler au plus tôt l'apparition de défaillances ou de dégradations et enclencher l'action corrective appropriée pour les contrer. Le regroupement de ces différentes fonctions de base conduit à la définition de la *solution technologique* (Sto_i) pour le point de vue considéré (automatique, mécanique, maintenance, ...). Pour le maintenicien, la solution technologique (Sto_i) correspond à l'architecture de surveillance et d'instrumentation à intégrer au produit.

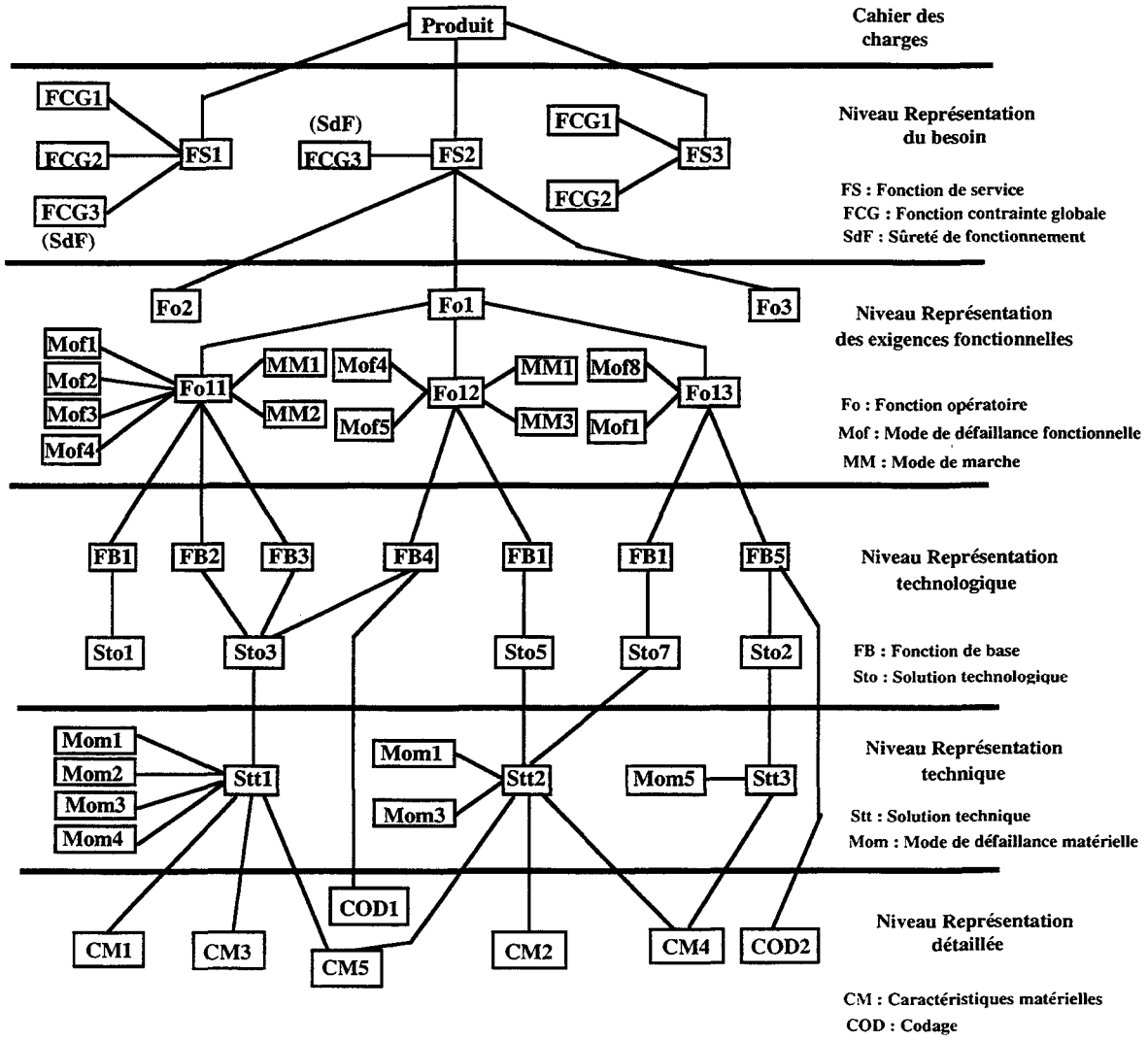

Figure 4 : Représentation produit et structuration des concepts dédiés sûreté de fonctionnement

Les solutions technologiques (Sto_i) sont affinées au niveau représentation technique par la définition de la *solution technique* (Stt_j) à leur associer. Cette solution technique correspond à un composant ou à un ensemble de composants que l'on va utiliser pour supporter les fonctions

de base. L'autre concept associé à ce niveau de représentation est le concept *Mode de défaillance matérielle* (Mom_j). Il vise à lister l'ensemble des défaillances pouvant apparaître sur les différents composants techniques retenus par chacun des concepteurs. Là aussi, selon les conséquences de ces défaillances, des actions correctives seront proposées afin de réduire leurs effets (redondance, maintenance, surveillance, ...).

Enfin, au niveau représentation détaillée, deux concepts ont été identifiés. Le concept *Caractéristiques matérielles* (CM_j) qui consiste à donner à la solution technique retenue (Stt_j) des caractéristiques précises (dimensions, tension d'alimentation, ...) mais également des informations plus complètes concernant sa fiabilité (MTBF) par exemple. Le concept *Codage* (COD_j) vise, quant à lui, à traduire les algorithmes qui ont été associés aux fonctions de base (FB_j) en des langages appropriés et adaptés à la solution technique retenue pour supporter les fonctions de base (ordinateur, calculateur, ...).

CONCLUSION

Nous avons présenté dans ce chapitre comment la caractéristique Sûreté de fonctionnement s'intègre au modèle de produit. Pour cela, nous avons introduit pour chacun des cinq niveaux de représentation les différents concepts que nous avons identifiés.

Les deux premiers niveaux regroupent des concepts généraux relatifs à la sûreté de fonctionnement. Tout d'abord, nous avons défini la sûreté comme une fonction contrainte globale que les concepteurs doivent respecter. Ensuite, nous avons cherché comment elle risquait de ne pas être obtenue. Dans cette optique, ont été exposés : le concept "Mode de défaillance fonctionnelle" qui vise à décrire les défaillances susceptibles de survenir dans les fonctions du produit, et le concept "Mode de marche" qui définit les alternatives capables d'être mises en oeuvre pour contourner ces défaillances.

Les trois autres proposent des concepts plus spécifiques puisqu'ils sont, pour la plupart, dédiés métier. Pour notre part, ces concepts sont dédiés Maintenance et concernent plus particulièrement la surveillance et le diagnostic de défaillance, activités qui contribuent grandement au maintien des caractéristiques de sûreté de fonctionnement d'un système dans le temps. Nous pouvons citer, parmi ces concepts, celui de "Fonction de base" qui correspond aux fonctionnalités qu'un système de surveillance doit avoir ; celui de "Solution technique" permettant d'associer aux fonctions de base un composant matériel ; ou encore celui de "Mode de défaillance matérielle" visant à mettre en évidence les composants sur lesquels une attention particulière doit être portée si l'on veut respecter les exigences de sûreté de fonctionnement.

Enfin, nous avons introduit la notion de "Comportement des entités", très importante au sein du modèle de produit. C'est un critère d'évaluation, dans le cadre des différents niveaux de représentation, des choix effectués par le concepteur. Cette notion contribue ainsi à la définition d'un produit respectant les exigences du client, notamment celles relatives à la sûreté de fonctionnement.

Dans le chapitre suivant, nous allons décrire le processus de conception c'est-à-dire les méthodes qui permettent de mettre en oeuvre les concepts dédiés à la sûreté de fonctionnement que nous avons identifiés aux cinq niveaux de représentation du modèle de produit et que nous venons de décrire. Cette présentation s'articulera autour de deux points essentiels. Le premier concerne les opérations nécessaires à la spécification des concepts décrits dans ce chapitre. Le second est relatif à l'évaluation des solutions proposées par chacun des concepteurs du point de vue de la sûreté de fonctionnement. Cette évaluation se fera à chacun des niveaux de représentation du modèle de produit.

CHAPITRE 3

LE PROCESSUS DE CONCEPTION

INTRODUCTION

L'activité de conception est, comme nous l'avons dit dans le chapitre précédent, caractérisée par deux aspects importants : le modèle de produit et le processus de conception. Dans le chapitre 2, nous avons introduit le modèle de produit et décrit les cinq niveaux de représentation qui le composent. Nous avons également présenté à chacun de ces niveaux, les différents concepts dédiés à la sûreté de fonctionnement que nous intégrons au modèle de produit.

Nous allons dans celui-ci présenter le processus de conception décrit suivant le *Méta-modèle d'élaboration des concepts* proposé par le laboratoire. Pour cela, nous présentons dans une première partie, ce méta-modèle qui regroupe plusieurs modèles (d'élaboration des concepts). Ceux-ci sont associés à chacun des niveaux de représentation du modèle de produit.

Dans une seconde partie, nous explicitons ce méta-modèle aux différents niveaux de représentation en décrivant comment sont instanciés les différents concepts (dédiés à la sûreté de fonctionnement) que nous avons identifiés et présentés au chapitre précédent. Cela passe donc par la description de chaque modèle d'élaboration des concepts à chaque niveau du modèle de produit. Ainsi, nous présentons les différentes opérations nécessaires à leur instanciation et décrivons les processus d'évaluation de la sûreté de fonctionnement mis en oeuvre à chacun des niveaux de représentation. Si les exigences du client ne sont pas respectées, des actions correctives sont alors proposées au concepteur pour qu'il puisse alors s'en approcher.

1. Le processus de conception

Le processus de conception est défini /KRAUSE 93/ comme *le travail nécessaire au développement du produit ou comme le processus de modélisation du produit faisant référence à un ensemble de fonctions (technique et de gestion) nécessaires à la transformation de l'idée initiale en produit final.* Il permet de supporter la dynamique de l'activité de conception. Il regroupe un ensemble d'opérations, d'outils et de modèles permettant l'instanciation des différents concepts associés au modèle de produit.

Il caractérise donc la démarche des concepteurs qui est souvent très variable d'une personne à l'autre, voire pour un même individu qui peut produire des résultats différents pour un même problème. C'est pourquoi il est généralement non monotone c'est-à-dire que l'enchaînement des opérations n'est ni ordonné, ni séquentiel.

Le processus de conception proposé par le laboratoire est composé d'un ensemble de fonctions génériques qui, aux cinq niveaux de représentation, s'instancie sous la forme de plusieurs *modèles d'élaboration de concepts*. Nous allons, dans le paragraphe suivant, décrire ce processus de conception dénommé *Méta-modèle d'élaboration des concepts.*

1.1. Description du méta-modèle d'élaboration des concepts

Le méta-modèle présenté figure 1 est présent à chacun des niveaux de représentation du modèle de produit. Il est constitué de six entités génériques qui sont :

— l'identification du "*Quoi faire ?* " : c'est une fonction générique visant à formaliser le problème à résoudre. Cette étape permet d'identifier les objectifs à atteindre à chacun des niveaux de représentation considéré et pour chaque intervenant de la conception ;

— l'identification du " *Comment faire ?* " : c'est une fonction générique ayant pour but d'identifier les solutions susceptibles de répondre au problème soulevé à l'étape précédente. Cette opération vise à identifier quelles sont les fonctions nécessaires à la satisfaction de l'objectif ;

— l'identification du " *Avec quoi ?* " : c'est une fonction générique dont le but est de préciser

les supports matériels et/ou logiciels que l'on peut associer à la (aux) solution(s) retenue(s) pour la satisfaction du " *comment faire ?* ". Cette opération permet, en définitive, de préciser les moyens à mettre en oeuvre pour atteindre l'objectif ;

— la quantification de " *Quelle valeur ?* " : c'est une fonction générique permettant de valuer les supports préconisés à l'étape précédente. Cette opération a pour but de donner une valeur aux différentes solutions données au problème posé. Elle permet donc de valuer les moyens mis en oeuvre ;

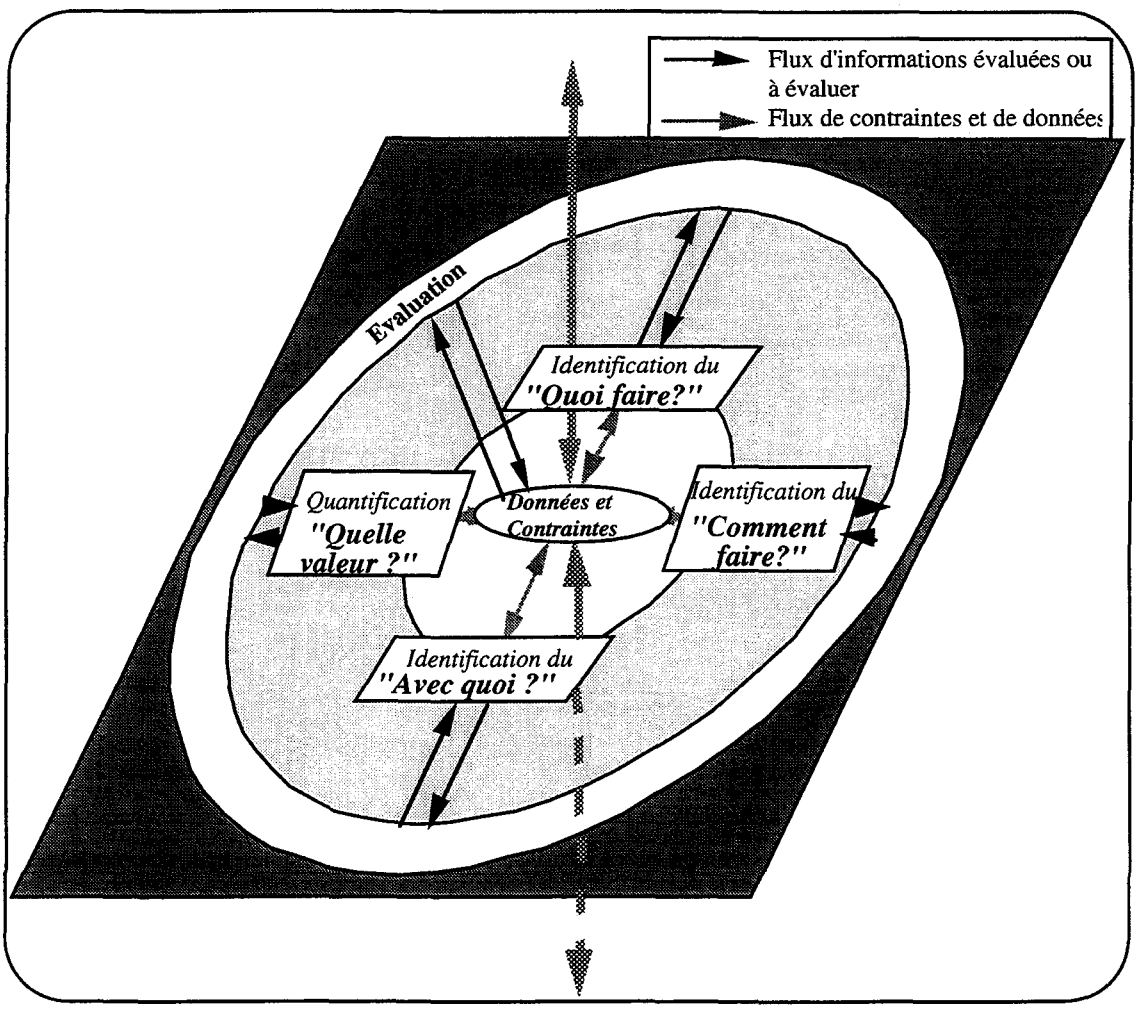

Figure 1 : Méta-modèle d'élaboration des concepts

— l' " *Évaluation* " : cette fonction générique a différents objectifs. Elle permet tout d'abord d'évaluer les résultats issus des différentes phases d'*identification* et de *valuation*. Elle permet ensuite de valider ou de remettre en cause certaines des propositions faites durant le processus de conception. Elle permettra notamment d'évaluer, à différents niveaux de granularité, la disponibilité du système, des fonctions, ... ;

— les *Données* et les *Contraintes* : elles représentent les limites définies dans le cahier des charges ainsi que l'ensemble des connaissances et des contraintes générées au cours de la conception. Les contraintes devront toutes être satisfaites afin d'obtenir un produit conforme aux exigences.

Le méta-modèle comprend donc les six entités que nous venons de décrire et s'instancie sous la forme de plusieurs modèles d'élaboration des concepts définis aux cinq niveaux de représentation associés au modèle de produit . Nous allons, dans le paragraphe suivant, décrire ces modèles.

1.2. Description des modèles d'élaboration des concepts

Le méta-modèle d'élaboration des concepts, présenté figure 1, permet d'instancier aux différents niveaux de représentation, les concepts définis au chapitre précédent par l'intermédiaire de plusieurs modèles d'élaboration de concepts. Chacun d'eux communique, échange des données et des informations à travers *Données et contraintes*. L'ensemble des fonctions génériques présentées au paragraphe précédent ne compose pas toujours les modèles d'élaboration des concepts à un niveau de représentation donné. Pour remédier à cela et afin qu'elles soient toutes sollicitées afin d'instancier l'ensemble des concepts du modèle de produit, nous associons à ces niveaux un domaine de conception (figure 2).

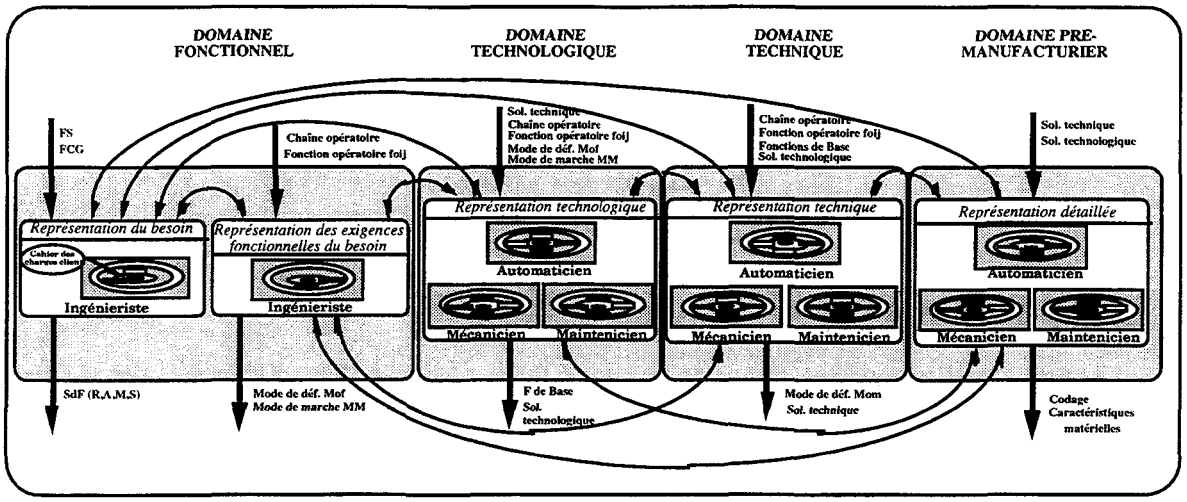

Figure 2 : Les domaines de conception

Ces domaines sont :

— le *Domaine fonctionnel* qui regroupe les niveaux **représentation du besoin** et **représentation des exigences fonctionnelles du besoin**.

C'est un domaine exclusivement fonctionnel puisque les besoins du client ne s'expriment qu'en termes de fonctions. On retrouve ici les concepts "Fonction de service", "Fonction contrainte globale", "Mode de défaillance fonctionnelle" et "Mode de marche" ;

— le *Domaine technologique* associé au niveau **représentation technologique.** Il fait la transition entre le domaine fonctionnel (fonctions) et le domaine technique (matériel). Il comprend les concepts "Fonction de base" et "Solution technologique" ;

— le *Domaine technique* qui fait référence au niveau **représentation technique.** On y retrouve les concepts "Solution technique" et "Mode de défaillance matérielle" ;

— le *Domaine Pré-manufacturier* associé au niveau **représentation détaillée**. Ce niveau permet d'aboutir aux composants spécifiés que l'on pourra alors fabriquer ou acquérir auprès d'un fournisseur. Il regroupe les concepts "Caractéristiques matérielles" et "Codage".

Les intervenants, au niveau du domaine fonctionnel, sont des ingénieristes chargés de traduire les exigences du client en fonctions à satisfaire grâce à leurs connaissances générales. Pour les trois autres domaines, seuls trois types de compétence ont été identifiés et représentés au niveau du modèle : l'automatique, la mécanique et la conception pour l'exploitation. Il faut, à l'avenir, envisager d'élargir le modèle de produit à d'autres métiers. En ce qui concerne nos travaux, ils se focalisent sur la conception en vue de l'exploitation. Nous allons, dans le paragraphe suivant, décrire le *méta-modèle d'élaboration des concepts* à chacun des niveaux de représentation du modèle de produit et selon le point de vue conception pour l'exploitation.

2. Opérations associées au niveau Représentation du besoin

Ce niveau de représentation permet de formaliser les besoins du client exprimés dans le cahier des charges et de vérifier que celui-ci contient toutes les informations nécessaires au concepteur. Ce niveau vise également à s'assurer que les informations contenues sont cohé-rentes. Cela se fait à travers l'instanciation des concepts "Fonction de service" et "Fonction contrainte globale" par l'intermédiaire du modèle d'élaboration (spécification) des concepts présenté figure 3.

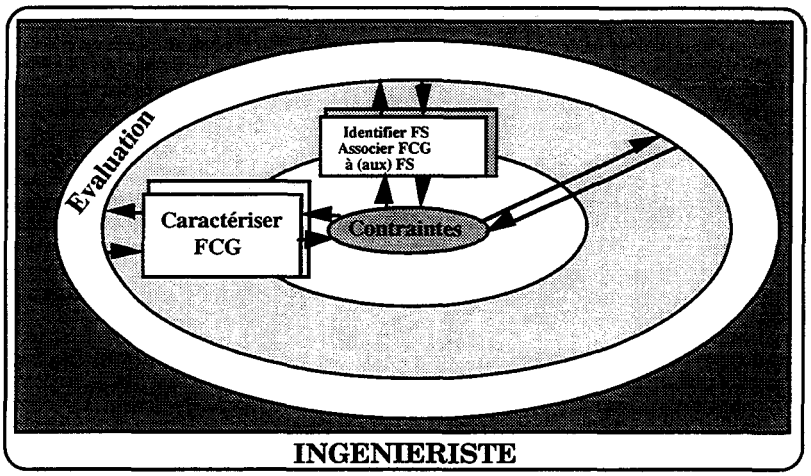

Figure 3 : Modèle d'élaboration des concepts pour le niveau Représentation du besoin

L'identification du "*Quoi faire?*" correspond d'une part, à la définition des fonctions de service. Cette opération consiste à déterminer si la fonction de service est principale (issue du cahier des charges) ou redondante (introduite suite à l'évaluation de la fonction principale d'un point de vue sûreté de fonctionnement). D'autre part, elle permet la définition de la fonction contrainte globale sûreté de fonctionnement que le produit doit respecter : le produit doit être sûr de fonctionnement c'est-à-dire qu'il devra être fiable, maintenable, disponible et ne pas mettre la sécurité des biens et des personnes en jeu.

La fonction générique "*Quelle valeur?*" va permettre de quantifier les différentes caractéristiques de la sûreté de fonctionnement. Cette valeur peut être donnée de façon explicite dans le cahier des charges ou simplement sous la forme d'un objectif global vers lequel le produit va devoir se rapprocher (voir figure 4).

Fonction de service	Fonction contrainte globale	Caractéristique	Valeur
FS1	Sûreté de fonctionnement	MTBF	V1 = 1500 heures
		Maintenabilité	Démontable
FS2	Qualité		Bonne qualité
FS3	Sûreté de fonctionnement	Disponibilité	V2 = 95 %

Figure 4 : Caractérisation des fonctions de service

La fonction "Évaluation" va intervenir de deux façons différentes au niveau du processus de conception :

— Dans le premier cas, nous cherchons à hiérarchiser les différentes fonctions de service du produit en fonction des contraintes de sûreté qu'elles doivent impérativement respecter. En effet, selon le service qu'elles rendent au niveau du produit, les fonctions de service n'auront pas les mêmes contraintes de sûreté à respecter. Pour certaines, c'est l'aspect sécurité qui sera privilégié ; pour d'autres, ce sera l'aspect fiabilité. Il convient donc de faire cette distinction d'une part et de hiérarchiser ensuite les fonctions de service pour une même contrainte de sûreté.

Pour effectuer cette évaluation, nous pouvons utiliser la méthode du tri croisé /RAK 92/ qui consiste à comparer des solutions deux à deux et à attribuer à celle qui est la plus adaptée un poids de 0 à 3 (voir figure 5). Du point de vue sûreté de fonctionnement, nous attribuons un poids aux caractéristiques (fiabilité, sécurité, ...) que la fonction de service doit respecter impérativement ou non. A partir de cette affectation de poids, nous pouvons alors classer les fonctions de service entre elles en fonction de la caractéristique de sûreté qu'elles doivent respecter et dans quelle mesure elle doit l'être.

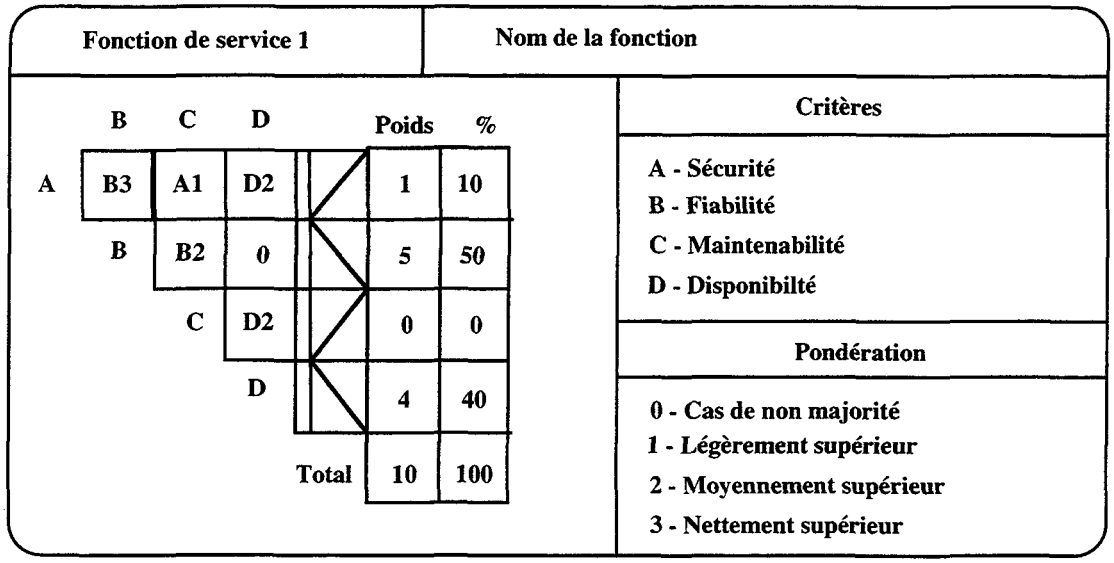

Figure 5 : Évaluation des fonctions de service

Dans ce cas, on peut constater que c'est le critère de fiabilité qui est à prendre en considération en priorité par rapport aux autres critères pour la fonction de service FS1 ;

— Dans le second cas, l'évaluation consiste à s'assurer que le produit respecte bien les exigences en matière de sûreté de fonctionnement. Cette évaluation intervient à chacun des niveaux de représentation du modèle de produit. Elle peut être faite, par exemple, par l'utilisation des relations mathématiques de définition de la fiabilité prévisionnelle des systèmes. Ces relations ont été présentées dans le chapitre 1 au paragraphe 3.3.2. Par exemple, on peut calculer la fiabilité d'une fonction de service à partir de celle de chacune des fonctions opératoires qui la composent. Les fonctions opératoires étant toutes en série (chaîne nominale), nous utilisons par conséquent la formule suivante :

$$R(FS) = \prod_{i=1}^{n} r_i(Fo_i)$$

et si elles ont respectivement pour valeurs de fiabilité $Fo_1 = 0,9$; $Fo_2 = 0,8$; $Fo_3 = 0,9$ nous obtenons alors pour FS_1 la valeur de 0,648 (0,9 x 0,8 x 0,9).

Nous détaillerons ces diverses évaluations à chacun des niveaux de représentation concernés (exigences fonctionnelles, technologique, technique et détaillée) en appliquant ces relations aux éléments concernés (fonctions opératoires, ensembles/sous-ensembles, composants, ...).

L'ensemble des opérations permettant de répondre aux fonctions génériques peut être représenté par le graphe de la figure 6 ci-dessous.

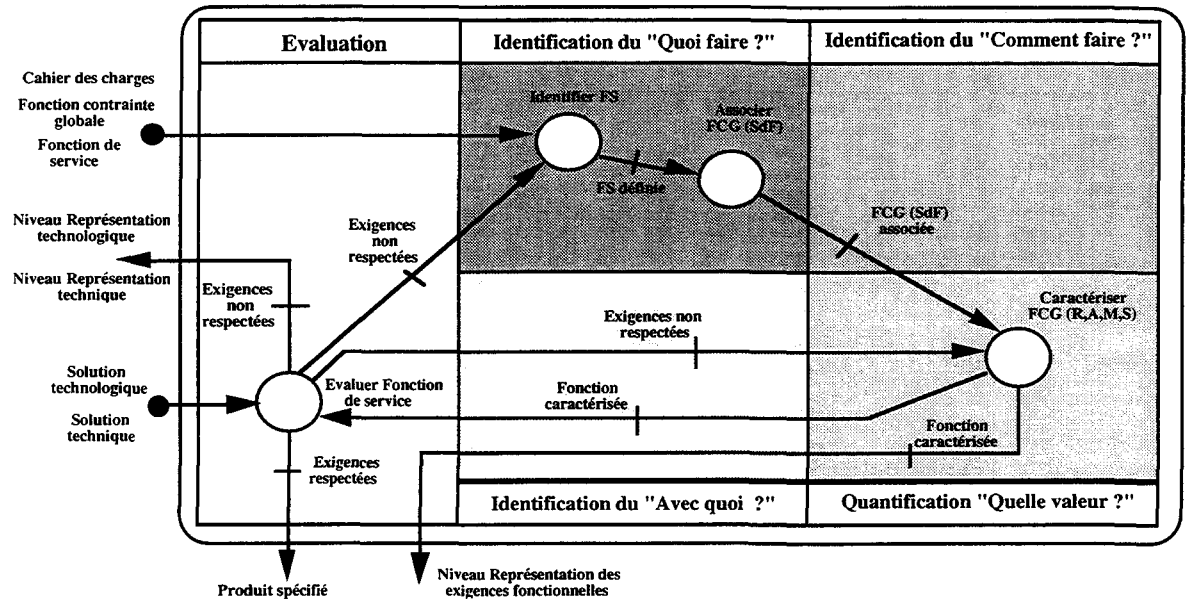

Figure 6 : Opérations et processus associés au niveau Représentation du besoin

Dans le cadre de la conception d'un produit nouveau (démarche descendante), les exigences à respecter vont être transmises au niveau de représentation suivant.

3. Opérations associées au niveau Représentation des exigences fonctionnelles du besoin

Ce niveau de représentation vise à déterminer comment seront satisfaits les besoins. D'un point de vue "Conception en vue de l'exploitation" (sûreté de fonctionnement), nous pouvons avoir à ce niveau une double approche :

— la première consiste à allouer aux différentes fonctions opératoires de la chaîne opératoire associée à une fonction de service des valeurs *a priori* dans l'objectif de respecter la contrainte globale définie au niveau de la fonction de service. Cette approche vise donc à répartir sur les fonctions opératoires les caractéristiques de sûreté demandées par le client pour la fonction de service. Ainsi, le taux de disponibilité, le MTBF, la probabilité de défaillance, ... vont être distribués sur chacune des fonctions opératoires de façon à obtenir la valeur désirée par le client. Cette approche est détaillée au paragraphe 3.1. ;

— la seconde vise quant à elle à rechercher comment les objectifs de sûreté définis par le client peuvent ne pas être atteints et quelles alternatives (procédures) peuvent être mises en oeuvre pour les respecter tout de même (ou s'en rapprocher). Cette approche est supportée par l'instanciation des concepts "Mode de défaillance fonctionnelle" et "Mode de marche" (paragraphes 2.1. et 2.2. du chapitre 2) à travers le modèle d'élaboration (spécification) des concepts présenté figure 7. Cette approche fait l'objet des paragraphes 3.2.1. et 3.2.2.

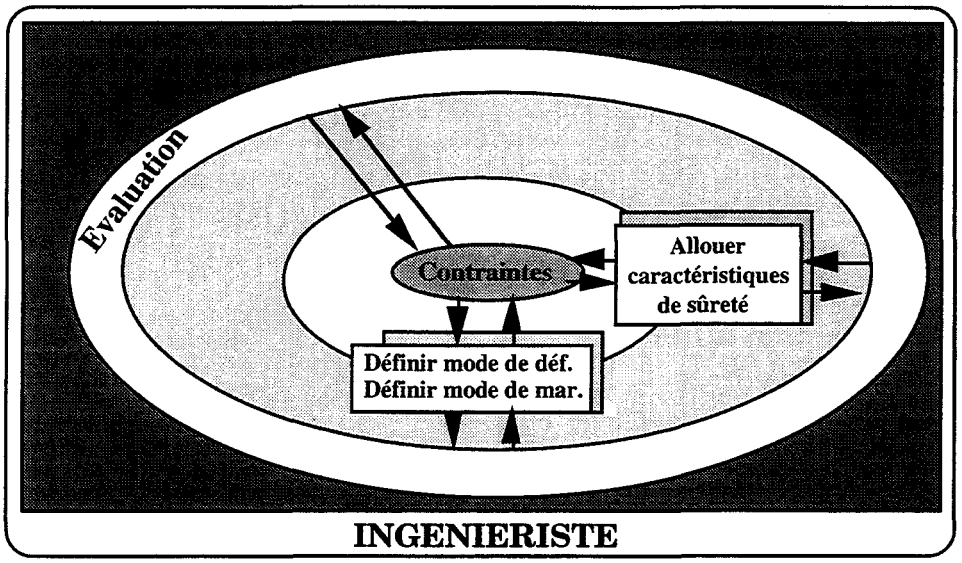

Figure 7: Modèle d'élaboration des concepts du niveau Représentation des exigences fonctionnelles

Les fonctions génériques du modèle d'élaboration des concepts font référence à un ensemble d'opérations permettant d'instancier les concepts associés à ce niveau de représentation. Les opérations et le processus assurant l'instanciation de ces concepts sont représentés figure 8.

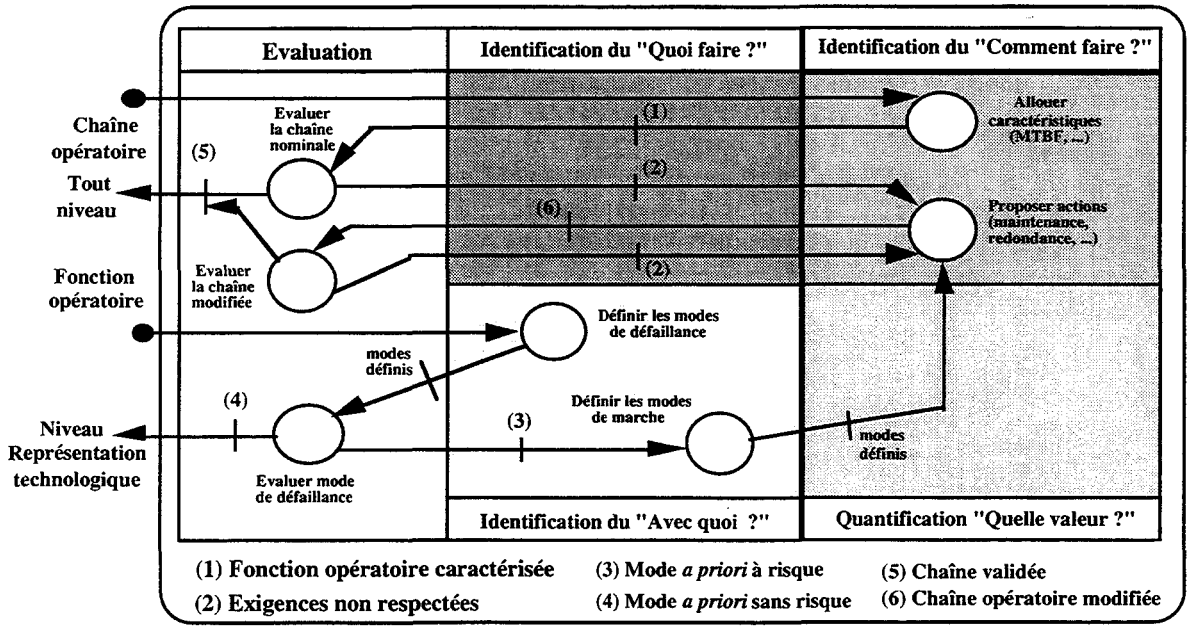

Figure 8 : Opérations et processus du niveau Représentation des exigences fonctionnelles

Les opérations composant ce graphe sont décrites dans les paragraphes qui suivent.

3.1. Allouer des caractéristiques de sûreté

Afin de respecter les exigences exprimées dans le cahier des charges, une première approche consiste à allouer des performances aux différentes fonctions opératoires constituant la chaîne opératoire. Le processus d'allocation consiste à traduire les exigences globales au niveau du système (fonction de service) en exigences pour chaque sous-système, ensemble, entité, ...

(fonctions opératoires, fonctions de base, ...). Il commence par la génération d'un bloc diagramme de fiabilité, extension de l'analyse fonctionnelle. Il utilise les relations série — parallèle existant entre les différents constituants. Le problème de l'allocation réside dans l'élaboration d'une procédure par laquelle des allocations raisonnables et cohérentes doivent être faites. Les phases ci-dessous peuvent être considérées comme appropriées pour mettre en place un processus d'allocation /BLANCHARD 95/ :

— identifier puis regrouper les fonctions opératoires au sein d'ensembles dont la conception est connue et le taux de défaillance disponible ou facile à évaluer. La différence entre les exigences du client et les caractéristiques déterminées sur les sous-ensembles constitue la part d'exigence restant à attribuer sur les ensembles de conception non connue ;

— identifier les fonctions sur lesquelles on ne dispose pas d'informations de conception (taux de défaillance, fiabilité, ...). On assigne à chaque fonction ou regroupement non caractérisé du point de vue sûreté de fonctionnement des facteurs pondérés donnés selon la complexité de chaque fonction ou regroupement. La portion des exigences de sûreté qui n'a pas été allouée lors de la première phase (objectif à atteindre auquel on retire les exigences attribuées aux ensembles de conception connue) est alors allouée aux fonctions et regroupements suivant les facteurs de pondération attribués.

Comme nous pouvons le constater, le processus d'allocation des exigences n'est pas une tâche aisée et peut s'avérer ardue dans le cas de systèmes complexes. Il nécessite la connaissance des regroupements de fonctions opératoires, tâche qui peut ne pas être aisée à mettre en oeuvre et demande d'être passée par d'autres niveaux de représentation. Dans le cas où des ensembles de conception connue ne sont pas intégrés au produit et afin de garantir en terme d'objectif, sa sûreté de fonctionnement, nous menons une analyse de ses dysfonctions afin d'y apporter des remèdes.

Nous présentons cette opération dans le paragraphe suivant.

3.2. Analyse des dysfonctions du produit

Afin de respecter les exigences en matière de sûreté de fonctionnement, nous menons à ce niveau une étude visant à rechercher tous les événements pouvant conduire au non-respect de ces exigences. Dans ce cadre, nous réalisons, d'une part, une analyse des modes de défaillance potentiels et de leurs effets sur les fonctions opératoires jugées à risque pour la réalisation de la mission ou du service. D'autre part, nous identifions les différents modes de fonctionnement possibles ou nécessaires de mettre en oeuvre suite à l'apparition d'une défaillance.

3.2.1. Définir les Modes de défaillance fonctionnelle

La définition des modes de défaillance se fait selon deux approches possibles.

Dans le premier cas, à partir de la chaîne opératoire constituée de plusieurs fonctions opératoires élémentaires, l'objectif de cette analyse est de rechercher les différents modes de défaillance susceptibles d'apparaître, d'en lister ensuite les causes possibles et de déterminer enfin leurs effets (notamment en termes de sûreté de fonctionnement). Le but essentiel de cette analyse est donc de recenser les modes de défaillance qui ont pour effets de mettre la sécurité et / ou la disponibilité du produit en jeu (et par conséquent de lister les fonctions sur lesquelles une attention toute particulière va devoir être portée). Le recensement de ces modes de défaillance s'accompagnera parfois de la définition de leur fréquence d'apparition ainsi que de la gravité de leurs effets.

Ces différents éléments seront obtenus en donnant des réponses à des questions du type /RIOUT 94/ :

— de quelle façon cette fonction peut-elle ne plus être assurée ?

Les réponses à cette question vont permettre de définir comment la fonction considérée passe de son état nominal à un état défaillant, dégradé, ... On obtient ainsi la liste des modes de défaillance de la fonction ;

— qu'est ce qui peut provoquer le mode de défaillance ?

L'objectif est ici de recenser toutes les causes (internes ou externes) entraînant l'apparition du mode de défaillance ;

— quels sont les effets du mode de défaillance sur le produit, l'environnement ?

En répondant à cette question, le concepteur va identifier les conséquences que le mode peut avoir sur le produit lorsqu'il apparaît (qualité, fonctionnement, sécurité, ...) comme le montre la figure 9. Selon la gravité de ses conséquences, des actions vont être entreprises (maintenance, redondance, autre solution, ...).

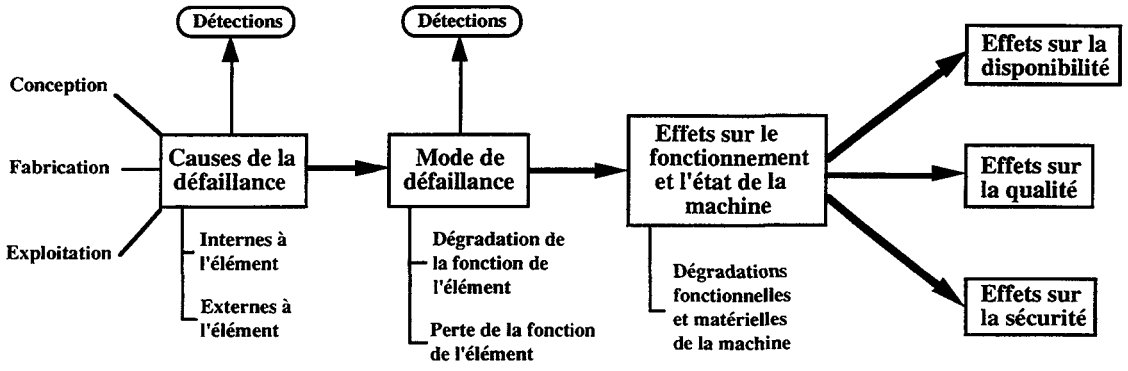

Figure 9 : Analyse des mécanismes de défaillance /RIOUT 94/

L'étude AMDE étant menée en groupe, les réponses à ces différentes questions peuvent être obtenues par l'utilisation d'outils d'analyse de la valeur. Nous pouvons notamment citer /PETITDEMANGE 95//BELLUT 90/ des méthodes telles que :

— le *brainstorming* : c'est une méthode intuitive et collective de recherche d'idées. Chaque membre du groupe livre sans retenue toutes les idées de solutions qu'un problème peut lui inspirer. Deux phases absolument distinctes se succèdent dans cette méthode : tout d'abord une phase de production d'idées puis une phase de classement et d'exploitation de ces idées. Cette méthode est généralement utilisée lorsque l'on est face à une situation nouvelle, face à un problème que l'on n'a jamais rencontré auparavant. On cherche alors à découvrir tout ce qui pourrait se passer dans le cas où une dégradation ou une défaillance survenait ;

— la méthode des *check-lists* : elle consiste à répondre à un ensemble de questions préétablies que l'on doit se poser à propos d'un problème.

Nous intégrons dans cette catégorie les listes-guides fournies par l'AFNOR /AFNOR 88/, proposant des modes de défaillance génériques et généraux pour faciliter la recherche des modes de défaillance d'un élément donné ;

— les *analogies et / ou transpositions techniques* : cette méthode consiste à imaginer les solutions au problème posé en recherchant des analogies avec des problèmes déjà rencontrés et résolus, dans des domaines qui peuvent parfois être très différents (le corps humain ou la nature en général). Transposé à notre problème, cette méthode peut être utilisée lorsqu'une même solution a été utilisée pour résoudre un problème similaire ou s'en approchant. On profite, dans ce cas, de l'expérience passée (acquise) sur cette solution pour résoudre le problème auquel on se trouve confronté.

Dans le second cas, le concepteur va intégrer et/ou améliorer des sous-ensembles existants sur lesquels des analyses AMDE auront déjà pu être menées. L'analyse vise ici à chercher si les modes de défaillance existants peuvent toujours apparaître dans le nouveau contexte d'utilisation, prendre en compte l'expérience acquise pour enrichir l'analyse, ajouter des nouveaux modes pouvant apparaître. Cette analyse permettra au concepteur de définir des actions à mettre en place (moyen de surveillance, redondance, ...).

Suite à cette analyse (simplement qualitative ou également quantitative) et en fonction de l'importance de la fonction opératoire sur le service à rendre et des exigences à respecter, des décisions vont être prises. La mise en place de différents modes de marche en est une.

3.2.2. Définir les modes de marche

La recherche des modes de défaillance vise à préciser les états dans lesquels un système se trouve ou peut se trouver suite à l'apparition d'une défaillance. On cherche alors à mettre en place des moyens visant à faire évoluer le système vers un état convenable c'est-à-dire respectant les exigences du client. Les modes de marche et d'arrêt ont cet objectif. Ils sont la mise en oeuvre des stratégies de maintien de la sûreté de fonctionnement.

La définition des modes de marche et d'arrêt peut se faire sur la base de l'"outil - méthode" G.E.M.M.A., Guide d'Études des Modes de Marche et d'Arrêt /ADEPA 81/. C'est un guide graphique que l'on remplit progressivement lors de la conception du système. Il regroupe sur un même document les trois grandes familles dans lesquelles on peut classer les modes de marche et d'arrêt :

— les procédures de fonctionnement (production normale, marche de préparation, marche de test, ...) ;

— les procédures d'arrêt (dans l'état initial, en fin de cycle, préparation pour remise en route après défaillance, ...) ;

— les procédures de défaillance (arrêt d'urgence, diagnostic et/ou traitement de défaillance, production tout de même).

Lors de l'étude d'un système, tous les modes possibles ne seront pas systématiquement recensés. Mais le G.E.M.M.A. permet, en phase de conception, de s'interroger sur la nécessité de prévoir ou non tel ou tel mode /BILAND 94/. L'étude des conditions d'évolution d'un mode à un autre permet au concepteur d'approfondir sa réflexion sur le comportement du système, de constater d'éventuelles erreurs de conception et d'y remédier en prévoyant, par exemple, d'autres commandes ou d'autres capteurs.

Cette définition passe, comme pour l'AMDE, par l'utilisation de méthodes telles que le brainstorming. Soit la conception est nouvelle et l'on cherche les modes à prendre en considération. Soit il s'agit de reconception et l'on peut s'appuyer sur une étude déjà menée sur laquelle on va apporter des modifications en fonction des exigences à respecter et de l'expérience acquise.

3.3. Évaluer les chaînes opératoires nominale et/ou modifiée

La définition des modes de défaillance a entraîné l'ajout d'états (défaillant, dégradé, ...)au niveau de la chaîne opératoire. Selon les effets que les modes de défaillance engendrent, des actions correctives peuvent être mises en oeuvre selon différents critères (coût, encombrement, ...). Ces actions peuvent être la mise en redondance de certaines fonctions (voire de toutes les fonctions opératoires), la mise en oeuvre de procédures de maintenance ou de changer complètement de solution.

L'évaluation de la chaîne opératoire nominale et/ou modifiée va se faire en comparant les contraintes exprimées par le client avec les caractéristiques des solutions proposées. Par exemple, on peut demander un MTBF de 1500 heures pour une fonction opératoire donnée. Si la solution proposée ne respecte pas cette contrainte, des mesures seront prises (actions décrites ci-dessus). Dans certains cas, il sera nécessaire d'avoir au préalable spécifié techniquement la fonction opératoire avant de pouvoir l'évaluer et s'assurer qu'elle vérifie les exigences de sûreté.

L'évaluation de la fiabilité de la chaîne opératoire nominale peut être faite par l'utilisation des relations mathématiques de définition de la fiabilité prévisionnelle des systèmes :

$$R_{cha\ neop.} = \prod_{i=1}^{n} r_i(fo_i)$$

puisque toutes les fonctions opératoires sont en série

avec :

$$r_i(fo_i) = \prod_{i=1}^{n} r_i(comp_i) \qquad \text{ou} \qquad r_i(fo_i) = 1 - \prod_{i=1}^{n} (1 - r_i(comp_i))$$

où $comp_i$ représente les composants associés à la fonction opératoire considérée

ou : $$r_i(fo_i) = \prod_{i=1}^{n} r_i(ens._i / ssens._i) \qquad \text{ou} \qquad r_i(fo_i) = 1 - \prod_{i=1}^{n} (1 - r_i(ens._i / ssens._i))$$

où ens_i / $ssens_i$ représente les ensembles ou sous-ensembles associés à la fonction opératoire considérée.

Pour l'évaluation de la chaîne opératoire modifiée, on utilisera également la formule suivante :

$$R_{ch.op.\,\mathrm{mod.}} = 1 - \prod_{i=1}^{n} (1 - r_i(fo_i))$$

puisque des fonctions opératoires vont être ajoutées en parallèle aux fonctions nominales (redondance active).

L'évaluation de la chaîne opératoire nominale peut aboutir à des caractéristiques de sûreté insuffisantes et ne respectant pas les exigences du client. Dans ce cas, des actions vont être mises en oeuvre pour remédier à cela (choix d'une autre fonction, redondance, ...) Suite à cela, une nouvelle évaluation sera faite pour s'assurer qu'une amélioration de ces caractéristiques a été apportée par les modifications réalisées.

En ce qui concerne la chaîne opératoire modifiée, une évaluation qualitative (AMDE) et/ou quantitative (définition des fréquences d'occurrence et des gravités des modes de défaillance) des fonctions redondantes qui la constituent sera (seront) également effectuée(s) pour s'assurer qu'elles permettent bien de respecter les exigences de sûreté du client. Ces opérations sont identiques à celles réalisées pour la chaîne opératoire nominale.

L'évaluation du comportement de la chaîne opératoire modifiée peut également être faite, par exemple, par l'utilisation d'un simulateur de réseau de Pétri. L'objectif de ces simulations sera de s'assurer qu'il n'y a pas de blocage dans la chaîne et que l'on bascule bien sur les alternatives prévues en cas de problèmes sur la chaîne opératoire nominale.

Ce niveau nous a permis de définir les défaillances fonctionnelles pouvant survenir sur les différentes fonctions opératoires constituant la chaîne opératoire. Nous avons, suite à cette étude, déterminé les différents modes de marche à considérer afin de contrer les défaillances les plus pénalisantes du point de vue sûreté de fonctionnement. Nous allons au niveau de représentation suivant décrire les moyens à mettre en place pour déceler un fonctionnement anormal et enclencher la procédure adaptée afin de le contrer.

4. Opérations associées au niveau Représentation technologique

Ce niveau de représentation a pour objectif de déterminer la structure technologique du système à concevoir c'est-à-dire de définir les différentes technologies à mettre en oeuvre afin de répondre au besoin du client. A ce niveau, chacun des acteurs de la conception intervient selon son point de vue. Nous considérons ici le point de vue du Maintenicien. Il apporte sa contribution par le modèle d'élaboration des concepts présenté figure 10, assurant l'instanciation des concepts "Fonction de base" (exploitation) et "Solution technologique" (paragraphes 3.1 et 3.2. du chapitre 2).

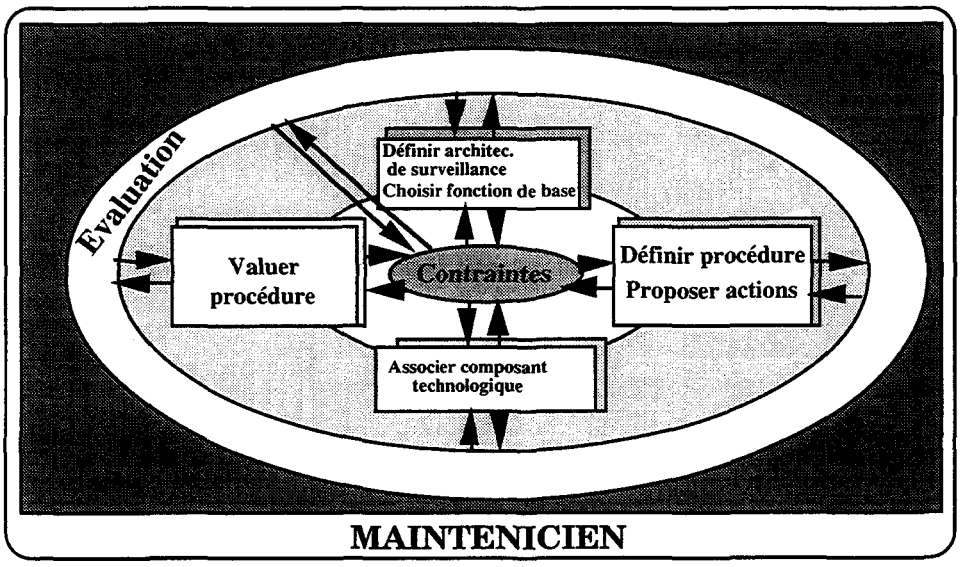

Figure 10 : Modèle d'élaboration des concepts pour le niveau Représentation technologique

Ce modèle d'élaboration des concepts regroupe toutes les fonctions génériques du méta-modèle d'élaboration des concepts. Ces fonctions font référence à un ensemble d'opérations permettant d'instancier les concepts cités précédemment. Ces opérations et le processus associé sont présentés figure 11.

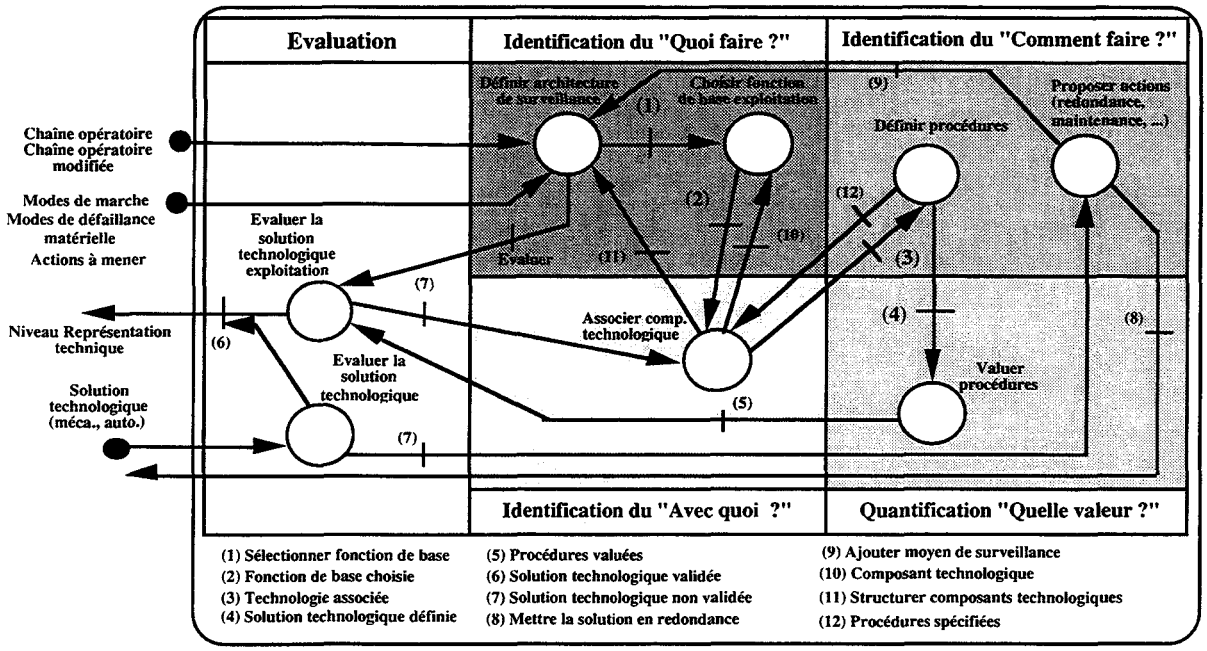

Figure 11 : Opérations et processus associés au niveau Représentation technologique

Nous allons dans les paragraphes suivants décrire ces différentes opérations.

4.1. Choisir les fonctions de base

Les fonctions de base constituent le point de départ de la conception simultanée du produit. Elles sont relatives à chaque domaine de conception qui ont été identifiés (automatique, mécanique, maintenance, ...).

Les fonctions de base relatives à la maintenance concernent la surveillance et le diagnostic des défaillances. Elles découlent directement des études précédentes (ou à venir) : analyse des modes de défaillance fonctionnelle (et matérielle) et définition des modes de fonctionnement. La première met en avant les fonctions opératoires susceptibles par leur défaillance, de mettre la sécurité des biens et/ou des personnes en jeu ou de compromettre la mission pour laquelle le produit est destiné. La seconde permet de définir les moyens à mettre en oeuvre pour éviter les effets des défaillances des fonctions opératoires. Cela peut se faire par la mise en place de mode de secours, de mise en sécurité, ...

Le passage d'un mode de fonctionnement à un autre va nécessiter la détection d'événements anormaux, lors de la future exploitation du produit. Cette détection précoce d'une défaillance ou d'une dégradation permettra de lancer un ordre de basculement vers un mode de fonctionnement apte à contrer ces événements (secours, arrêt, maintenance, ...). Ces opérations sont directement liées aux fonctions de base dédiées Exploitation. Le concepteur pour l'exploitation va donc ajouter, en fonction de son étude et des exigences à respecter, des fonctions de base à l'architecture technologique définie par l'automaticien et le mécanicien. La figure 12 ci-dessous reprend l'ensemble des fonctions de base qui ont été identifiées pour les différents points de vue considérés.

Fonctions de base Automaticien	Fonctions de base Mécanicien	Fonction de base Maintenicien
Communiquer entre composants matériels	Liaison ccomplète	Réaliser acquisition des données / infos de surveillance
Dialoguer avec l'opérateur	Guidage en translation	Détecter la défaillance
Coordonner	Guidage en rotation	Localiser la défaillance
Commander	Guidage en translation et en rotation	Diagnostiquer la défaillance
Contrôler	Guidage hélicoïdal	Réaliser la correction de la défaillance
		Informer l'opérateur

Figure 12 : Fonctions de base des différents acteurs de la conception

La nécessité d'introduire à l'architecture du produit des fonctions de base dédiées Exploitation peut également apparaître dans le cadre d'une reconception de produit. Dans ce cas, à partir d'une analyse des modes de défaillance matérielle pouvant apparaître sur les composants techniques utilisés (niveau représentation technique), des actions peuvent être proposées. Ces actions vont de la mise en redondance d'éléments mécaniques ou automatiques jusqu'à la mise en place de moyens de surveillance et de diagnostic (ce qui conduit à l'introduction de nouvelles fonctions de base dédiées Exploitation).

Il n'existe pas de méthode permettant de définir l'architecture de surveillance (ensemble des fonctions de base Exploitation). Celle-ci est obtenue de façon intuitive par le maintenicien qui la conçoit.

Chaque acteur va ensuite associer à chacune des fonctions de base qu'il aura choisie une technologie (composant technologique), l'ensemble de ces composants constituant alors la solution technologique du métier (point de vue) considéré. Nous présentons ce concept "Solution technologique" au paragraphe suivant.

4.2. Définir la Solution technologique

La solution technologique rassemble un ensemble de fonctions de base que chacun des acteurs de la conception a défini pour répondre à son problème.

Pour l'aspect Exploitation, l'outil utilisé pour instancier ce concept est l'*arbre de décision*. En effet, pour chacune des fonctions de base (acquérir, détecter, ...) un arbre de décision peut être défini. Celui-ci va permettre de déterminer la solution technologique la plus adaptée au problème à résoudre. Ces solutions vont venir enrichir la solution technologique de l'automa-

ticien qu'il représente par l'intermédiaire du M.E.S.A.P. /PARAYRE 92/. Il décrit grâce à lui l'architecture de commande du produit, regroupant les différentes fonctions de base Automatique qu'il aura choisies. La solution technologique du maintenicien suivra ce même schéma afin de décrire cette fois l'architecture de surveillance à intégrer au produit.

Les choix effectués à ce niveau par le maintenicien seront donc effectués en fonction des choix des autres acteurs et en particulier ceux de l'automaticien. En effet, les choix de commande qui auront été faits (automate, ordinateur) inciteront le maintenicien à adopter les mêmes choix pour la mise en place des systèmes de surveillance et de diagnostic des défaillances (pour des raisons d'encombrement ou de coût par exemple). En cas d'incompatibilité ou pour des problèmes liés à la sécurité, il sera dans l'obligation de choisir une solution différente.

4.3. Définir les procédures

Le choix des méthodes à utiliser pour concevoir les procédures de surveillance est fortement conditionné par la forme sous laquelle ces connaissances sont disponibles. Celles-ci nous permettent de distinguer les méthodes "sans modèle" des méthodes "avec modèle". Les premières sont dénommées ainsi car on ne dispose pas dans ce cas de modèle décrivant le comportement normal et le(s) comportement(s) défaillant(s) de l'équipement. Ceux-ci seront "appris" à partir des données expérimentales relevées lors de différents types de fonctionnement. Elles regroupent les méthodes issues de la *reconnaissance des formes* /DUBUISSON 90/. Les secondes sont basées sur la vérification de la cohérence des données disponibles (issues des capteurs équipant le processus et des interfaces opérateurs ou d'algorithmes de décision) avec le(s) modèle(s) disponible(s). La connaissance traduite par ces modèles se situe à différents niveaux et conduit à des algorithmes de surveillance très différents. Ces méthodes sont notamment :

— l'*estimation des paramètres* /ISERMANN 93/ : cette méthode est basée d'une part, sur la connaissance d'un modèle paramétrique décrivant le comportement du système et, d'autre part, sur la valeur de ses différents paramètres lors du fonctionnement normal. On compare ensuite les paramètres caractérisant le fonctionnement réel du système avec les paramètres théoriques. Tout écart entre ces valeurs est révélateur de la présence d'une défaillance.

— l'*estimation d'état* /FRANK 93/ : dans ce cas également, nous partons de la connaissance du modèle paramétrique décrivant le comportement du système ainsi que les valeurs des paramètres en fonctionnement normal. La comparaison se fait ici entre les sorties estimées du système et les sorties réelles. Tout écart traduit encore une fois la présence d'une défaillance. Les outils supportant cette méthode sont notamment les Observateurs et le filtre de Kalman.

— la *redondance analytique* /CASSAR 94/ /GERTLER 90/ : on connaît dans ce cas encore le modèle paramétrique décrivant le comportement du système et les valeurs de ses paramètres en fonctionnement normal. Les grandeurs relevées sur le système sont injectées dans le modèle. Si les résultats obtenus sont différents de ceux escomptés, on considère alors qu'une défaillance est présente.

La mise en oeuvre de ces méthodes nécessite la connaissance de certaines données fournies par les autres concepteurs : fonctions de transfert par l'automaticien, chaîne cinématique (torseur des forces) par le mécanicien,... On dispose ainsi des modèles du système ainsi que des paramètres à surveiller (avec éventuellement leurs valeurs nominales). A partir de là, et en fonction de ces informations, du type de produit à concevoir, des exigences à respecter, ..., une de ces méthodes de surveillance sera sélectionnée et mise en oeuvre par le concepteur. Cette sélection se fera sur la base de toutes ces informations ainsi que sur l'expérience du concepteur. En effet, ces différentes méthodes ne peuvent être mises en concurrence, elles donnent chacune des résultats intéressants mais elles ne s'appuient pas sur le même type d'informations pour y parvenir. Aussi, le choix d'une méthode plutôt qu'une autre ne pourra être fait que par le concepteur en fonction d'une part, du problème à résoudre et d'autre part, de ses connaissances personnelles (expérience).

4.4. Évaluer la solution technologique

L'évaluation de la solution technologique se fait à deux niveaux. Dans un premier temps, c'est une évaluation de la solution technologique propre au maintenicien. Celle-ci peut être obtenue par une pondération de critères retenus pour l'évaluation et à évaluer ensuite les solutions technologiques par rapport à ces différents critères. Cette évaluation peut se faire par l'utilisation de la méthode du tri croisé /RAK 92/ consistant à comparer deux à deux des solutions et d'attribuer à celle qui est la plus adaptée un poids allant de 0 à 3 ; la méthode O'Méara /DELAFOLIE 91/ qui, à partir des concepts de la méthode précédente, propose un classement des différentes solutions répondant au problème à résoudre ; de la méthode des plans d'expériences de Taguchi /SISSON 91/, méthode expérimentale basée sur l'évaluation d'une solution à partir du relevé temporel de l'évolution de ses paramètres de sortie.

Les autres acteurs de la conception vont également évaluer leurs solutions par l'utilisation de différents modèles de comportement.

Par exemple, l'automaticien peut simuler le comportement de sa solution en la représentant par des graphes d'états de commande /BILAND 94/. Il peut également utiliser l'outil Bond-graph (ou graphe de liaisons) qui est une représentation graphique des mécanismes d'interaction, de dissipation et de stockage d'énergie d'un système dynamique. Il se situe comme intermédiaire entre le système physique et les modèles mathématiques qui lui sont associés (matrice de transfert, équations d'état, système d'équations différentielles d'ordre 2). La méthodologie bond-graph /DAUPHIN-TANGUY 93/ demande l'analyse des phénomènes physiques qui seront pris en compte dans la modélisation (pesanteur, frottement, inertie, compressibilité, ...). Cependant, cette approche ne demande pas l'écriture de lois générales de conservation. Elle repose essentiellement sur la caractérisation des phénomènes d'échanges de puissance au sein du système. Le bond-graph obtenu peut facilement évoluer, par simple ajout d'éléments nouveaux, sans reprendre la démarche depuis le début. De plus, le choix particulier des variables d'état donne au modèle d'état une réalité physique non négligeable. Enfin, par son caractère graphique et sa structure causale, le modèle bond-graph apparaît comme un bon outil d'analyse.

Quel que soit le modèle utilisé, l'objectif de cette simulation est de vérifier l'adéquation entre ce qui est obtenu et ce que le concepteur souhaite obtenir.

De son côté, le mécanicien va simuler le comportement de sa chaîne cinématique. Par l'utilisation des équations de la cinématique, il réalise des calculs d'efforts pour s'assurer que sa solution répond bien aux exigences. Les résultats obtenus peuvent également être le point d'entrée du niveau représentation technique pour le dimensionnement des composants en vue de résister aux efforts auxquels ils seront soumis.

Dans un second temps, nous faisons une évaluation globale de la solution technologique. A partir de l'architecture M.E.S.A.P. définie par l'automaticien, les aspects sûreté de fonctionnement ont été spécifiés par la définition de l'architecture de surveillance à intégrer au produit (définition des fonctions de base à mettre en place, définition des composants à mettre en redondance suite à l'analyse AMDE menée au niveau représentation technique, ...). Différentes architectures peuvent alors être proposées. Nous évaluons donc chacune d'elles en fonction des exigences à respecter (évaluation par des modèles fiabilistes propres aux aspects commande (techniques d'injection de pannes, de défauts physiques, ...) ou mécaniques (lois statistiques, résultats d'essais, relevés en exploitation, ...)). La solution répondant le mieux aux exigences du client sera alors validée et retenue.

Si les résultats obtenus lors de cette évaluation ne sont pas satisfaisants, des actions correctives sont préconisées. Elles consistent à mettre en redondance certains des éléments critiques de la solution proposée ou à définir des procédures de maintenance préventive sur ces mêmes éléments.

L'ensemble des choix réalisés à ce niveau de représentation va contraindre ceux effectués au niveau inférieur, le niveau représentation technique. Nous allons décrire les opérations associées à ce niveau dans le paragraphe suivant.

5. Opérations associées au niveau Représentation technique

Ce niveau de représentation a pour objectif de définir la structure matérielle du produit. L'automaticien et le mécanicien vont préciser leurs solutions en associant aux fonctions de base, des composants matériels.

Le processus de conception associé à ce niveau de représentation revêt différentes formes selon les résultats obtenus suite à l'instanciation des concepts "Solution technique" et "Mode de défaillance" matérielle (paragraphes 4.1. et 4.2. du chapitre 2) à travers le modèle d'élaboration des concepts de la figure 13.

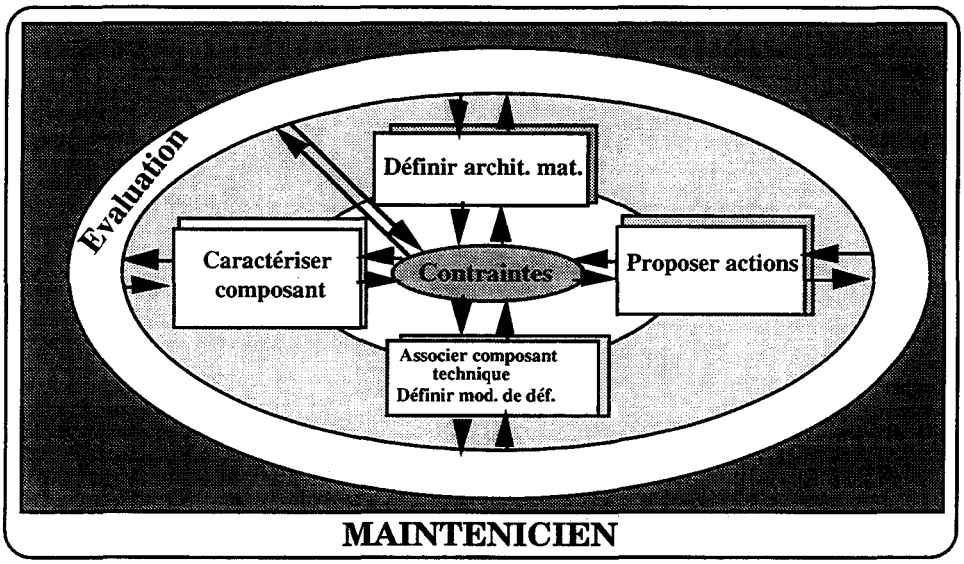

Figure 13 : Modèle d'élaboration des concepts pour le niveau Représentation technique

Du point de vue de la conception en vue de l'exploitation, le processus de conception associé à ce niveau de représentation vise à rechercher les composants dédiés à la surveillance et au diagnostic qu'il va falloir mettre en place pour supporter les fonctions de base Exploitation définies au niveau de représentation précédent. Ce type de processus sera mis en oeuvre si des moyens de surveillance et diagnostic sont nécessaires.

Si ce sont des actions de maintenance qui résultent de l'analyse AMDE menée à ce niveau, le processus de conception va consister à élaborer les différentes procédures de maintenance pour chacune des solutions choisies par les différents intervenants de la conception. C'est le concepteur en vue de l'exploitation (maintenicien) qui aura la charge de réaliser cette tâche.

Par contre, si les résultats obtenus lors de cette étude préconisent la mise en redondance d'un ou de plusieurs éléments, ces informations vont être envoyées aux intervenants concernés par cette mise en redondance (automaticien, mécanicien, ...). Ils auront alors la charge de prendre en compte cette contrainte afin que le produit à concevoir soit sûr de fonctionnement.

Une fois cette contrainte prise en compte, une nouvelle évaluation devra être faite afin de vérifier que la (ou les) caractéristiques qui n'était (ent) pas respectée(s) l'est (le sont) maintenant.

Le modèle d'élaboration des concepts considère toutes les fonctions génériques du méta-modèle d'élaboration des concepts. Les opérations associées à ce modèle sont présentées sur la figure 14 ci-dessous.

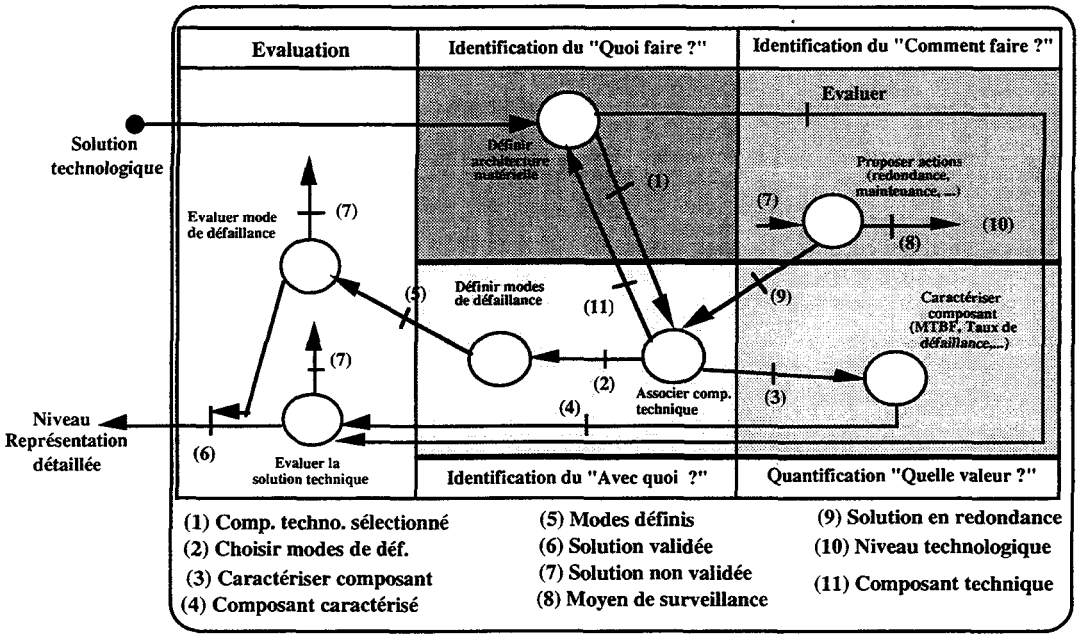

Figure 14 : Opérations et processus du niveau Représentation technique

Nous décrivons, dans les paragraphes qui suivent, ces différentes opérations.

5.1. Définir la solution technique

A partir de toutes les informations issues du niveau précédent et afin de supporter l'ensemble des fonctions de base définies pour le maintenicien, nous définissons pour chacune d'elles les composants matériels et/ou logiciels pouvant être utilisés.

La méthode permettant de mener cette tâche à bien est une nouvelle fois l'*arbre de décision*. Le concepteur va sélectionner dans cet arbre, les solutions les plus aptes à répondre au problème en fonction des choix effectués précédemment et en fonction des choix des autres intervenants.

5.2. Caractériser composant

La caractérisation des composants techniques passent par l'attribution à chacun d'eux d'informations concernant leur taux de défaillance, leur fiabilité, ... Du point de vue de leur comportement, des méthodes issues du domaine du diagnostic peuvent être utilisées pour réaliser cette caractérisation. Ces méthodes, utilisées seule ou en combinaison avec d'autres, sont les suivantes /BERGOT 95/ :

— le *raisonnement qualitatif* /LAURENT 92//TRAVÉ-MASSUYÈS 92/ a pour objectif de formaliser les raisonnements que l'on peut mener sur un système physique, à partir de données qualitatives plutôt que d'informations numériques précises. -

Trois approches apparaissent comme bases dans ce domaine : celle de /DE KLEER 84/, centrée sur la notion de composant ; celle de /FORBUS 84/ basée sur la notion de processus ; celle enfin de /KUIPERS 86/ composée d'un ensemble de contraintes sur les paramètres du sys-

tème physique. Mais quelque soit l'approche, le principe reste toujours le même. Il consiste à décrire des relations entre des grandeurs physiques par des équations (généralement différentielles) qualitatives ou par l'intermédiaire de différents opérateurs, puis à simuler le bon ou le mauvais fonctionnement en construisant le graphe des états possibles ;

Principales méthodes	Formalismes associés	Type d'application	Outils associés
Simulation qualitative (Kuipers)	Contraintes arithmétiques et fonctionnelles Graphes orientés	Détection, diagnostic et pronostic de dysfonctionnements à partir de la modélisation, la prédiction et l'explication du comportement de systèmes physiques pour lesquels la théorie est bien établie (systèmes thermo-hydrauliques.	Algorithme de simulation (outil QSIM)
—	—		—
Théorie des Processus Qualitatifs (Forbus)	Vues individuelles Processus Graphes orientés		Algorithme de simulation
—	—		—
Physique qualitative basée sur les confluences (De Kleer & Brown)	Confluences Règles de propagation Graphes orientés		Algorithme RAA (Reductio ad absurdum)
—	—		—
Automatique qualitative (Gentil et al.)	Graphes orientés (variables, fonctions de transfert qualitatives)		Algorithme de simulation causale
—	—		—
Ordres de grandeur (Travé-Massuyès, Raiman)	Algèbre des signes, algèbre des ordres de grandeur		Système formel FOG

Tableau 1 : Caractéristiques principales du raisonnement qualitatif

Cette méthode permet de décrire le comportement de systèmes physiques. On peut à partir de la modélisation du système simuler son comportement et faire des prédictions sur son évolution au cours du temps en fonction de l'apparition de perturbations.

La figure 15 ci-dessous donne un exemple d'utilisation de la physique qualitative. Elle propose un graphe causal représentant les liens entre les différentes variables du réservoir (pressions, débits, ...). Sur les arcs sont données les influences que les variables ont les unes sur les autres : le signe + traduit une augmentation (si Q_i augmente, Q augmente) ; le signe - traduit une diminution (si Q_0 augmente, Q diminue).

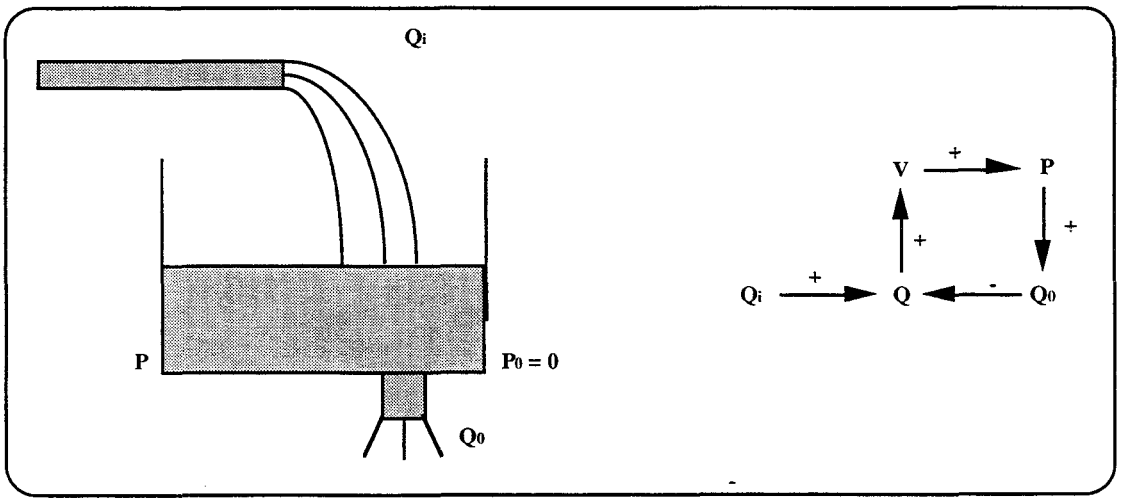

Figure 15 : Exemple de graphe causal qualitatif

Aucune valeur numérique n'est utilisée mais, par ce graphe de causalité, nous avons une représentation du comportement que le système doit avoir en fonction de l'évolution de ses paramètres caractéristiques.

— le *raisonnement approximatif* basé sur la théorie des ensembles flous /ZIMMERMANN 91/ ayant pour objet de prendre en compte l'*imprécision* dont sont parfois entachées certaines connaissances ; ou sur la théorie des possibilités /ANDRES 90/ qui considère quant à elle leur *incertitude*.

Dans le domaine du diagnostic, une première méthode /TERANO 92/ consiste à utiliser des relations floues pour décrire l'intensité des relations causales reliant les défaillances (causes) et les symptômes constatés (effets) ; une autre méthode /ULIERU 93/, inspirée du diagnostic médical, se base surtout sur les symptômes, les relations floues utilisées décrivant les liens symptômes-défaillances issus de l'expérience acquise par les experts humains.

Principales méthodes	**Formalismes associés**	**Type d'application**	**Outils associés**
Théorie des ensembles flous — Théorie des nombres flous — Théorie des possibilités	Ensembles Matrice des relations — Intervalles de Confiance Opérations algébriques — Logique possibliste	Prise en compte de connaissances entachées d'incertitude et d'imprécision dans le processus décisionnel en détection et diagnostic de pannes, ou au niveau du pronostic de déviations.	Algorithmes de résolution mathématique Expertise humaine

Tableau 2 : Caractéristiques principales du raisonnement approximatif

Le principe du diagnostic flou consiste, à partir d'un vecteur de symptômes B donné (informations subjectives et objectives perçues par l'opérateur humain), à trouver toutes les causes possibles pouvant l'avoir généré (vecteur de causes A). Pour cela, il faut inverser les relations floues liant le vecteur A au vecteur B : $B = R \circ A$, les relations R traduisant ici la connaissance du mauvais fonctionnement du processus. Lors du diagnostic, les effets (B) sont connus et la cause (A) est recherchée ;

— le *raisonnement causal* /LEYVAL 94//PENG 87/ est basé sur la connaissance *a priori* des relations de cause à effet des dysfonctionnements. Cette approche consiste à décrire un graphe de causalité de mauvais fonctionnement reliant des hypothèses de pannes (causes) à leurs effets. Trois niveaux de connaissances /FINK 87/ peuvent être distingués dans certain graphe : les *informations* (observations, tests...), les *hypothèses* de pannes et les *solutions* (réparations, pronostics...). Le diagnostic consiste à parcourir un réseau sémantique traduisant les relations de causalité entre les effets (informations) et les causes (hypothèses) et aboutissant à des propositions de solutions /MAN LEE 93/.

Principales méthodes	**Formalismes associés**	**Type d'application**	**Outils associés**
Méthodes numériques — Méthodes symboliques	Relations de causalité Graphes de causalité Règles de production Logique des prédicats	Diagnostic correctif (localisation de composants défaillants d'un système en panne) ou diagnostic prédictif (pronostic sur la tendance à la dérive de certaines grandeurs caractéristiques d'un système en état de fonctionnement).	Algorithmes de résolution de problèmes Générateurs de systèmes experts outils dédiés au diagnostic correctif ou prédictif

Tableau 3 : Caractéristiques principales du raisonnement causal

Dans les *systèmes experts à règles d'association* /CHATAIN 93//BARBER 92/, les relations de cause à effet sont encodées par des règles de production. Le raisonnement s'effectue à l'aide d'inférences avec association de coefficients de vraisemblance aux conclusions proposées /MARRAKCHI 86/, ou par inférences incertaines avec la présence de coefficients d'évocation et de rejet pour certains faits /DAVID 88/. Cette approche a fait l'objet de nombreuses applications en diagnostic de pannes /CHATAIN 93/ mais aussi en maintenance prédictive /MENEXIADIS 88//ENGELHARDT 87//SKATTEBOE 86/. Les informations contenues dans les tableaux AMDE peuvent être utiles pour la mise en oeuvre de cette technique de diagnostic.

Dans le domaine du diagnostic industriel, l'apparition de générateurs de systèmes experts, couplés avec des modules conviviaux de dialogue, permet aisément de capitaliser la connaissance pour le diagnostic de matériels simples (dépannage automobile, électroménager, ...). Par contre, pour des systèmes industriels complexes, le cycle de vie d'un système expert implique la mise en place d'une équipe qui doit être capable d'exploiter et de maintenir sa pérennité ;

— le *raisonnement basé sur le modèle* /DAVIS 93//PIECHOWIAK 92/ s'articule autour de trois composantes que sont le système réel, son modèle et les observations du comportement du système. Les approches associées reposent sur deux points fondamentaux : il faut d'abord disposer d'un modèle de bon fonctionnement du système à diagnostiquer et ensuite ne pas pouvoir remettre en cause la validité de ce modèle lorsque des contradictions (appelées symptômes) sont détectées entre les observations réelles et les prédictions calculées à partir du modèle.

Les entités de base nécessaires à l' élaboration d'une méthode de diagnostic selon les premiers principes sont la description de l'organisation structurelle interne du système à diagnostiquer, la description comportementale ou fonctionnelle de chacun des composants, sous-systèmes et du système global et enfin, les observations issues du système (mesures obtenues aux entrées/sorties des composants ou du système). Il est possible de simuler, à partir de ces entités, le fonctionnement normal du système, de détecter les incohérences entre le comportement réel (observations) et le comportement prédit dans le but de déterminer, parmi les composants, celui ou ceux dont la défaillance peut expliquer ces incohérences. La description du système peut être obtenue au travers de modèles basés sur les relations de causalité /LEYVAL 94//FINK 87//VAN DE VELDE 85/, de modèles causaux probabilistes /OLESEN 93//PEARL 86/ ou de modèles basés sur les connaissances fonctionnelles, structurelles et comportementales /DE KLEER 92, 87/ /SPUR 90/ /REITER 87/ /DAVIS 84/ /GENESERETH 84/.

Principales méthodes	**Formalismes associés**	**Type d'application**	**Outils associés**
Descriptions fonctionnelle, comportementale et structurelle (Davis, De Kleer, Genesereth, Reiter)	Réseaux de contraintes (Polybox) et règles d'inférences et de simulation (Davis, De Kleer) Logique des prédicats (Genesereth, Reiter)	Détection et diagnostic de pannes uniques (Davis, Genesereth) ou de pannes multiples (De Kleer, Reiter) de systèmes électroniques	Outil GDE (De Kleer) Outil DART (Genesereth)
—	—	—	—
Modélisation par relations de causalité (Fink, Van de Velde, Pearl)	Graphe bayésien (Pearl) Réseau abstrait de causalité (Van de Velde) Réseau de primitives fonctionnelles (Fink)	Détection et diagnostic de dysfonctionnements de systèmes électromécaniques)	Système expert IDM (Fink)

Tableau 4 : Caractéristiques principales du raisonnement basé sur le modèle

La figure 16 ci-dessous donne un exemple de réseau abstrait de causalité pour le circuit électrique associé. Les noeuds du graphe représentent les valeurs de bon fonctionnement d'une

caractéristique observable (alimentation = en marche, ...) qui sont soit normales, soit anormales. Quant aux arcs, ils représentent une relation de cause à effet entre deux noeuds. Ainsi, on peut écrire :

Si Relais = alimenté (cause)

Alors Contact 1 = fermé (effet)

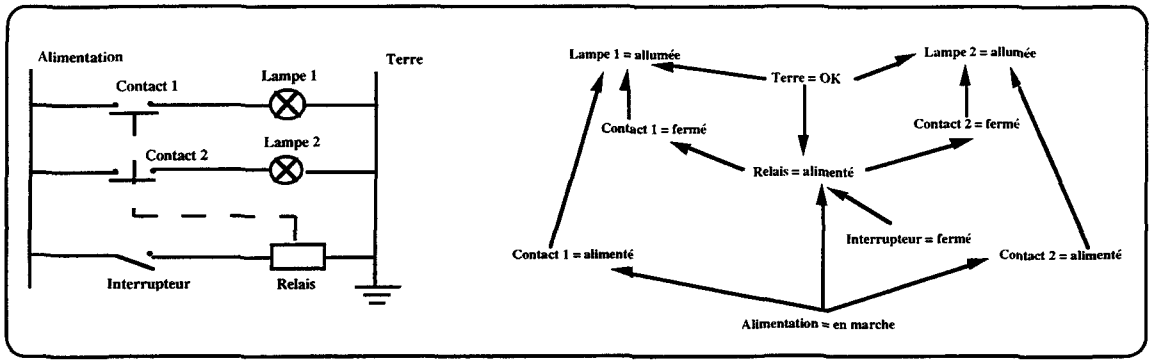

Figure 16 : Réseau causal relatif à un circuit électrique

Ce type de réseau, traduisant le fonctionnement normal souhaité du système étudié, peut être un bon outil d'aide au diagnostic des défaillances. Si l'événement attendu (désiré) ne se produit pas, on peut rechercher, à partir du graphe, les causes qui peuvent en être à l'origine.

Le choix de l'une (ou de plusieurs) de ces solutions est fonction des choix effectués aux niveaux de représentation précédents ainsi que de ceux des autres concepteurs, des informations disponibles (relations de causalité entre variables, relations de cause à effet tirées des analyses AMDE, ...). Les échanges et les communications entre concepteurs sont donc très importants.

5.3. Définir les modes de défaillance matérielle

Cette opération vise à analyser les modes de défaillances de chacune des solutions techniques choisies. Elle permet de s'assurer que les exigences en matière de sûreté de fonctionnement sont bien respectées à ce niveau de représentation.

Comme pour la définition des modes de défaillance fonctionnelle (paragraphe 3.2.1.), les méthodes telles que le *Brainstorming*, la méthode des *check-lists* ou la méthode des *analogies et/ou transpositions techniques* (toutes déjà présentées dans ce chapitre) peuvent être utilisées pour instancier ce concept.

Dans le cas où un risque persiste, des actions peuvent être prescrites puis mises en oeuvre. La définition de ces actions fait l'objet du paragraphe suivant.

5.4. Définir les actions à entreprendre

Sélectionner des sous-ensembles existants mais utilisés dans des conditions différentes, adapter une solution en fonction de contraintes spécifiques entraînent des modifications dans le comportement des entités utilisées. L'opération précédente a eu pour objet de détecter les éventuelles dégradations et défaillances pouvant apparaître. Cette opération vise à proposer des actions pour faire face à ces événements indésirables. La méthode utilisée pour réaliser cette opération peut être l'*arbre de décision* dans lequel on va sélectionner l'action la plus appropriée pour résoudre notre problème, en fonction de différents critères (coûts, encombrement, ...).

Ces actions peuvent être la mise en redondance du composant étudié, des procédures de maintenance préventive voire la remise en cause du choix effectué.

5.5. Évaluer solution technique

Comme pour la solution technologique, l'évaluation va se faire à deux niveaux. Tout d'abord, une évaluation locale de chaque solution technique par chacun des intervenants de la conception. Le mécanicien va, par exemple, utiliser des modèles de comportement des matériaux (élastique, viscoplastique, ...), des modèles de calcul (RDM, éléments finis, ...) pour évaluer la solution qu'il propose.

De son côté, l'automaticien peut évaluer sa solution par l'utilisation de modèles tels que les fonctions de transfert, les bond-graphs, ..., en y introduisant des informations plus précises concernant les composants utilisés.

L'autre type d'évaluation va être effectué par le concepteur pour l'exploitation. Celle-ci va consister à s'assurer que les choix effectués par les autres intervenants de la conception respectent bien les exigences de sûreté demandées par le client. Pour cela, les relations mathématiques d'évaluation prévisionnelle des systèmes peuvent par exemple être utilisées. Celles-ci sont appliquées aux ensembles ou sous-ensembles à partir de la connaissance des fiabilités des composants. Ces relations sont les suivantes :

$$R_{ens./ssens.} = \prod_{i=1}^{n} r_i(comp_i) \qquad R_{ens./ssens.} = 1 - \prod_{i=1}^{n} (1 - r_i(comp_i))$$

Si les résultats obtenus ne sont pas satisfaisants, des actions du même type que celles citées dans le paragraphe précédent devront être mises en oeuvre par chacun des concepteurs.

Une évaluation des différents modes de défaillance de chacun des composants techniques spécifiés peut également être effectuée. En fonction de la fréquence d'apparition des modes et de leur gravité, un niveau de criticité sera défini pour le mode considéré. Si celui-ci est jugé trop élevé, des actions correctives seront proposées. Celles-ci vont consister en la mise en redondance de certains des composants, en la définition de procédures de maintenance préventive ou en l'ajout de fonctions de surveillance (fonctions de base exploitation au niveau représentation technologique) afin de déceler au plus tôt l'apparition de défaillances ou de dégradations.

L'ensemble des choix techniques effectués à ce niveau de représentation va être affiné au niveau inférieur par la définition précise des caractéristiques des matériels et par le choix des modèles de représentation et de programmation des connaissances.

6. Opérations associées au niveau Représentation détaillée

Ce niveau de représentation a pour objectif de préciser les caractéristiques des différents composants constituant la structure technique du produit ainsi que la façon de coder les connaissances sur le produit lorsque l'on se trouve dans le cadre de la conception du système de surveillance et de diagnostic.

Pour cela, sont instanciés les concepts "Caractéristiques matérielles" (des composants techniques retenus) et "Codage" (paragraphes 5.1. et 5.2. du chapitre 2) par l'intermédiaire du modèle d'élaboration (spécification) des concepts de la figure 17.

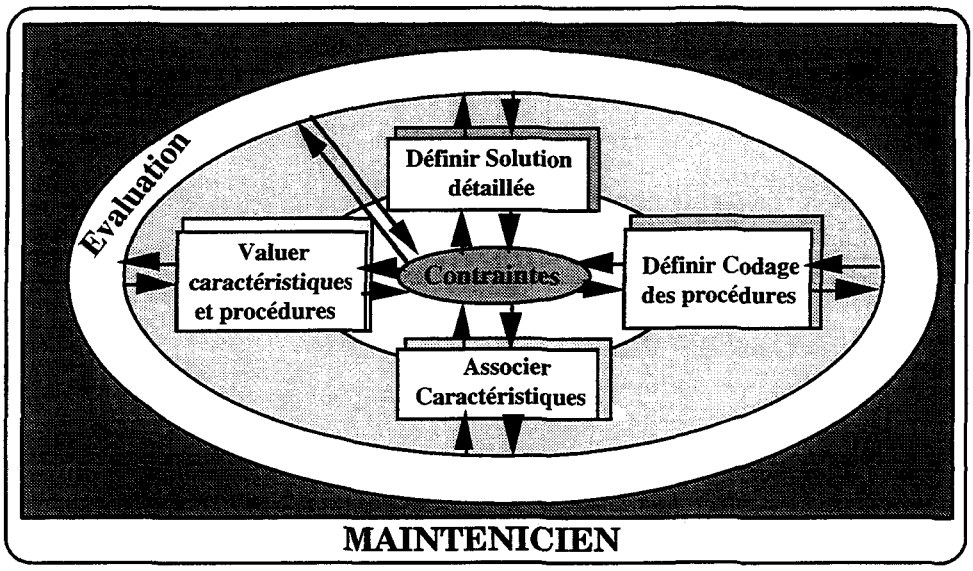

Figure 17 : Modèle d'élaboration des concepts pour le niveau Représentation détaillée

Le premier concept vise à donner aux composants techniques des caractéristiques précises permettant d'aboutir à un composant spécifié complètement. Il vise également à caractériser plus précisément les composants définis par les autres concepteurs en ajoutant des informations relatives à la fiabilité, la disponibilité, ... de ces composants.

Le second a pour objectif de traduire les procédures associées aux composants technologiques exploitation en langage informatique approprié.

Ce modèle d'élaboration des concepts intègre l'ensemble des fonctions génériques du méta-modèle d'élaboration des concepts. Les opérations associées à ces fonctions sont représentées sur la figure 18.

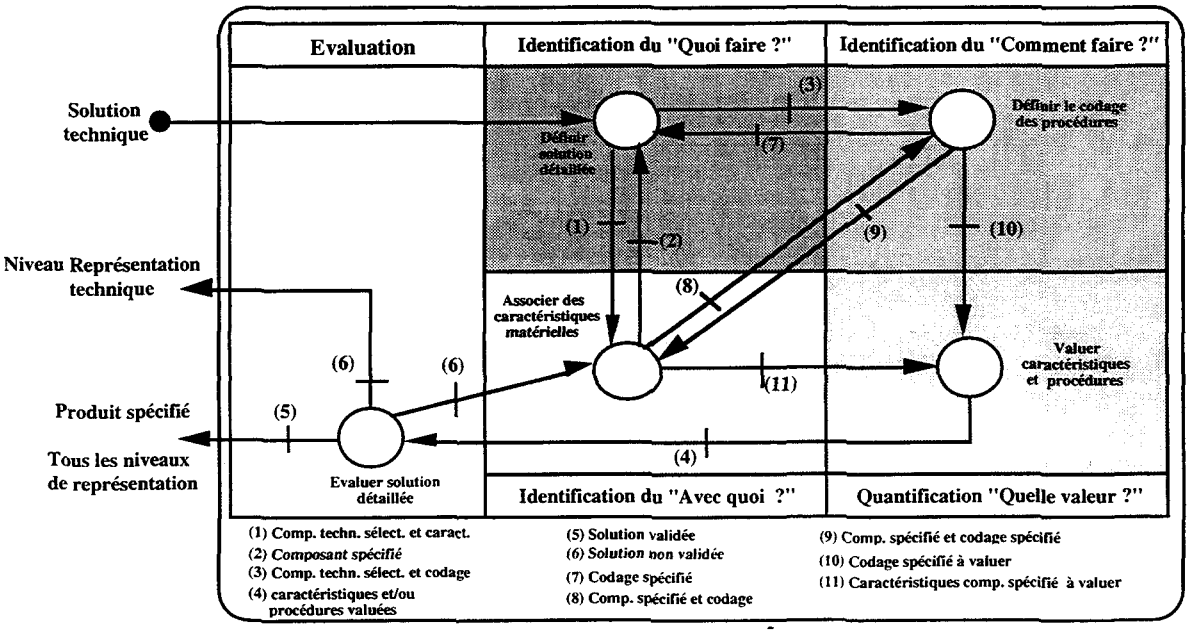

Figure 18 : Opérations et processus associés au niveau Représentation détaillée

Nous décrivons ces opérations dans les paragraphes suivants.

6.1. Définir les caractéristiques matérielles

Cette opération vise à donner les caractéristiques précises des composants spécifiés aux niveaux précédents pour assurer les fonctions de base. On détermine ainsi les références, tension d'alimentation, nombre d'entrées/sorties des cartes,... (tableau 5).

Désignation	Marque	Type	Caractéristiques princpales
Automate programmable	Télémécanique	TSX 17-20	22 entrées 24 Vcc isolées 12 sorties à relais Alimentation 110 à 240 Vca
Détecteur de proximité	Télémécanique	Inductif	Intensité nominale maxi : 80 à 500 mA Fréquence de commutation : 15 à 3000 Hz Fonctionnement de -25 °C à +70 °C
Moteur asynchrone	Leroy Sommer	Triphasé, rotor en court-circuit	2 sens de rotation Puissance : 1100 W Vitesse de rotation : 1500 tr/min
Roulement à billes	SNR	Roulement à contact radial	1 rangée de billes Diamètre intérieur : 10 Diamètre extérieur : 30 Largeur : 9

Tableau 5 : Exemples de composants Spécifiés

Les méthodes pouvant être utilisées pour réaliser ces opérations sont par exemple la méthode des check-lists ou la méthode des analogies ou transpositions techniques. Ces deux méthodes ont déjà été présentées au cours de ce chapitre.

6.2. Définir le codage

Ce concept vise à définir comment seront représentées les différentes connaissances manipulées dans le cadre de la surveillance et du diagnostic. En fonction des choix techniques, ces connaissances ne seront pas décrites de la même façon. On utilisera ainsi le langage ladder si c'est un automate qui a été choisi, des réseaux sémantiques, des règles de production, un langage informatique quelconque, selon la méthode de diagnostic qui aura été retenue et qu'il faudra implanter au sein d'un ordinateur (figure 19).

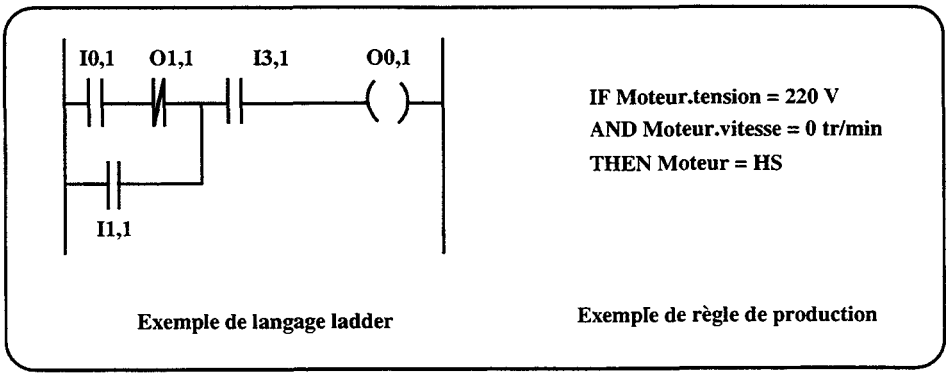

Figure 19 : Exemples de langages de programmation utilisés

La sélection entre ces différents types de représentation sera obtenue suite au parcours des différentes branches d'un *arbre de décision.*

6.3. Évaluer la solution détaillée

L'évaluation va se faire à deux niveaux. Une évaluation tout d'abord des choix faits, tant du point de vue des caractéristiques matérielles que du codage utilisé pour décrire les procédures. C'est une évaluation propre à l'aspect Exploitation qui consiste à s'assurer qu'en cas de défaillance, celle-ci est bien détectée, localisée, diagnostiquée et que l'action devant être entreprise est correctement réalisée. Un simulateur de réseau de Pétri peut par exemple être utilisé pour effectuer cette évaluation mais elle peut également être fortement liée aux méthodes de diagnostic qui ont été présentées au paragraphe 5.2.

L'autre évaluation va se faire sur la solution globale pour vérifier que le produit conçu répond bien aux exigences du client exprimées dans le cahier des charges. Les relations mathématiques d'évaluation de la fiabilité prévisionnelle des systèmes peuvent être utilisées dans le cas où des données complémentaires ou plus précises seraient disponibles à ce niveau alors qu'elles ne l'étaient pas au niveau précédent.

7. Synthèse

L'objectif de ce dernier paragraphe est de présenter, à travers deux exemples, une synthèse des opérations associées au processus de conception. Le premier exemple montre, sur une conception descendante et innovante, les opérations mises en oeuvre pour aboutir à la mise en redondance d'une fonction.

Le second exemple porte quant à lui, sur une reconception d'un élément existant et décrit les opérations conduisant à la mise en place de procédures de maintenance préventive en vue de respecter les exigences de sûreté demandées par le client.

7.1. Conception descendante et innovante

Les points d'entrée pour ce type de conception (figure 20) sont les fonctions de service que le produit doit remplir et les fonctions contraintes globales qu'il doit respecter. La première opération va consister, au niveau représentation du besoin, à associer aux fonctions de service les caractéristiques de sûreté qu'elles doivent respecter.

Au niveau représentation des exigences fonctionnelles, ces caractéristiques sont réparties, a priori, sur chacune des fonctions de la chaîne opératoire (Allouer caractéristiques sdf aux F. opératoires). Une évaluation de la chaîne permet de s'assurer que la répartition qui a été faite permet bien de respecter les caractéristiques demandées au niveau précédent.

L'autre type d'évaluation qui peut être mené sur la chaîne opératoire consiste à rechercher les modes de défaillance fonctionnelle susceptible d'apparaître sur chacune des fonctions opératoires. Cette recherche des différents modes s'accompagnera ensuite de la détermination de leur fréquence d'apparition et de leur gravité. Si la criticité ainsi obtenue est trop élevée ou si la répartition des caractéristiques de sûreté ne donne pas satisfaction (non respect des exigences du client), des actions correctives vont alors être proposées. Si l'on veut privilégier la sécurité ou la disponibilité du produit, c'est une mise en redondance de la fonction opératoire jugée à risque qui sera demandé et mise en oeuvre. Cette action va alors induire deux opérations.

La première va être d'informer les autres concepteurs (mécaniciens, automaticiens, ...) qui vont devoir prendre cette contrainte en considération (définition d'une chaîne opératoire modifiée).

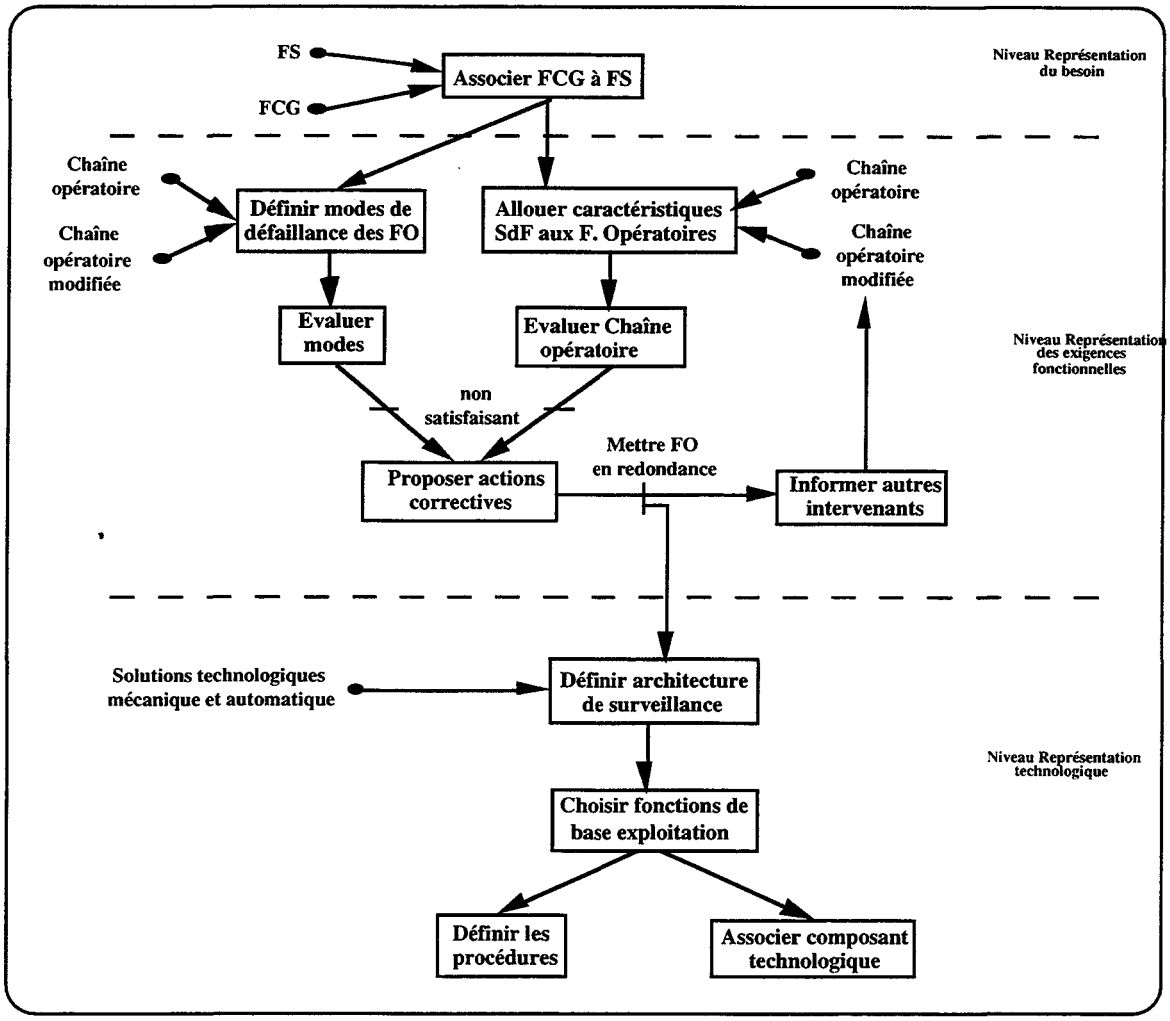

Figure 20 : Enchaînement des opérations pour une conception descendante

La seconde concerne le concepteur en vue de l'exploitation qui va mettre en oeuvre l'architecture de surveillance adaptée pour, d'une part, déceler au plus tôt l'apparition d'une défaillance sur la fonction nominale ; et d'autre part, activer la procédure adéquate pour mettre la fonction redondante en fonctionnement. Tout cela, il va l'obtenir en sélectionnant dans la liste des fonctions de base exploitation (acquérir, détecter, ...) celles qu'il souhaite mettre en oeuvre. Il leur associera ensuite un composant technologique et, pour celles pour lesquelles c'est nécessaire, une procédure (de détection, de diagnostic, ...).

7.2. Reconception d'une solution existante

Les premières opérations sont, dans ce cadre, identiques au cas précédent (figure 21). On associe aux fonctions de service les caractéristiques Sdf qu'elles doivent respecter, puis elles sont réparties sur les fonctions opératoires de la chaîne (niveaux représentation du besoin et représentation des exigences fonctionnelles). A partir de là, on suppose que le concepteur a une idée, a priori, de la solution permettant de supporter une ou l'ensemble des fonctions de la chaîne opératoire. Il va donc reprendre cette solution (architecture matérielle) et l'ensemble des composants techniques qui lui sont associés.

Outre les modifications que les autres concepteurs pourraient être amenés à apporter à cette solution technique, le concepteur en vue de l'exploitation va étudier cette solution du point de vue de sa sûreté de fonctionnement. Il peut tout d'abord évaluer sa fiabilité ou sa disponibilité à partir des informations relatives à chacun des composants utilisés (taux de défaillance,

MTBF, MTTR, ...). Ensuite, il peut rechercher les différents modes de défaillance pouvant apparaître sur chacun des composants. A partir de la fréquence d'apparition de ces modes et de leur gravité, un niveau de criticité leur est attribué. En fonction de ce niveau de criticité, des résultats de l'évaluation de l'architecture matérielle et des exigences que le client demande, des actions correctives seront proposées. Dans cet exemple, nous considérons que de simples procédures de maintenance préventive sont suffisantes (à partir de l'expérience du concepteur ou du retour d'expérience issu de la solution précédente).

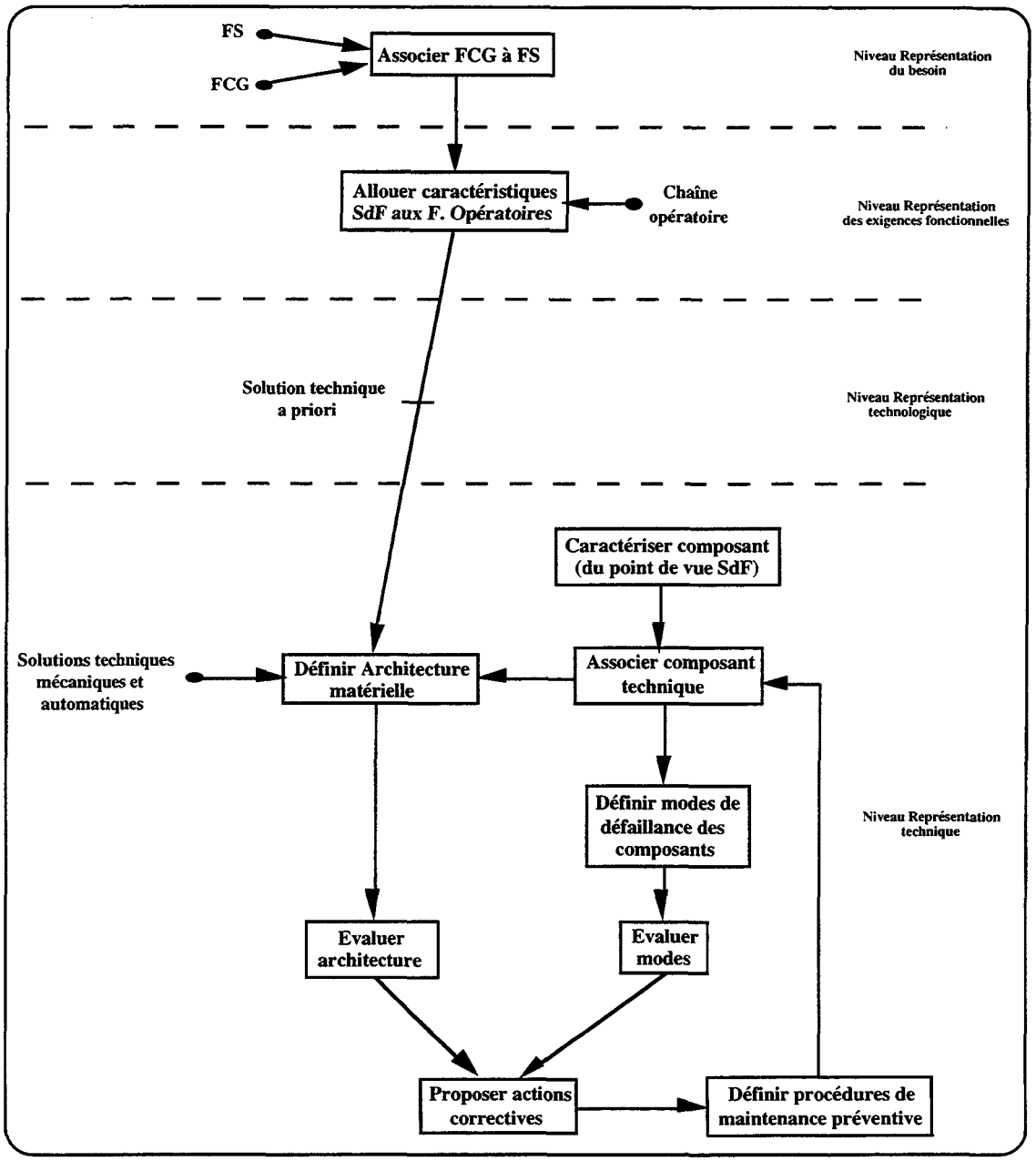

Figure 21 : Enchaînement des opérations dans le cadre d'une reconception

Si c'est une mise en redondance qui est préconisée, il faudra alors informer les autres concepteurs de cette action, modifier l'architecture matérielle initiale et mettre éventuellement des moyens de surveillance en place (sélection de fonctions de base exploitation au niveau représentation technologique). Cela permettra de déceler, au plus tôt, l'apparition d'une défaillance et activer ainsi la procédure de mise en fonctionnement du composant redondant.

CONCLUSION

Nous avons décrit, dans ce chapitre, le processus de conception qui est variable suivant le concepteur, son expérience, ... (processus non monotone). Nous avons dans une première partie, décrit le méta-modèle d'élaboration des concepts. Il est constitué de six entités génériques qui permettent d'instancier les concepts associés à chacun des cinq niveaux de représentation du modèle de produit (décrit au chapitre 2).

Puis, nous avons décrit les modèles d'élaboration des concepts associés à chaque niveau de représentation. Aux niveaux représentation du besoin et représentation des exigences fonctionnelles du besoin, ils permettent d'instancier les concepts :

- *Fonction contrainte globale* (sûreté de fonctionnement) qui définit une des contraintes que le produit doit respecter lors de sa future exploitation ;
- *Mode de défaillance fonctionnelle* qui permet de rechercher, de façon exhaustive, l'ensemble des défaillances et dégradations qui pourrait apparaître au niveau de la chaîne opératoire ;
- *Mode de marche* qui vise à introduire des fonctionnements alternatifs afin de contrer l'apparition de ces défaillances ou dégradations.

Au niveau représentation technologique, les concepts suivants sont instanciés :

- *Fonction de base* qui, du point de vue "Conception en vue de l'exploitation, correspond aux fonctionnalités qu'un système de surveillance doit posséder ;
- *Solution technologique* qui permet de structurer les différentes fonctions de base entre elles et définit ainsi l'architecture d'instrumentation et de surveillance.

Au niveau représentation technique, on retrouve les concepts :

- *Solution technique* qui précise la solution technologique en associant aux composants technologiques retenus une technique précise ;
- *Mode de défaillance matérielle* qui vise à rechercher les modes de défaillance de chaque composant technique et de proposer des actions (redondance, maintenance, ...) pour les plus critiques d'entre eux.

Enfin, au niveau représentation détaillée, les concepts instanciés sont :

- *Caractéristiques matérielles* qui permet de spécifier complètement les composants retenus par les différents concepteurs en leur ajoutant des caractéristiques de sûreté (MTBF, MTTR, ...) ;
- *Codage.* qui permet de traduire en des langages de programmation spécifiques les algorithmes de surveillance et de diagnostic qui ont été élaborés au niveau technologique.

Nous avons donné, pour chacun des niveaux de représentation, les opérations ainsi que le processus de conception associés. Ils décrivent comment sont instanciés les concepts introduits au sein du modèle de produit. Nous avons également proposé, à chacun de ces niveaux, des évaluations des solutions retenues par chacun des concepteurs et défini des actions correctives (redondance, maintenance, autre solution, ...) lorsque cela était nécessaire (exigences de sûreté non respectées).

Les modèles d'élaboration des concepts associés aux niveau représentation du besoin et représentation des exigences fonctionnelles sont complémentaires puisqu'ils permettent à eux deux de reprendre l'ensemble des entités génériques du méta-modèle d'élaboration des con-

cepts. Les modèles d'élaboration des concepts disposent aux trois derniers niveaux de représentation de toutes les fonctions génériques du méta-modèle. Cependant nous nous sommes focalisés à ces derniers niveaux sur les modèles d'élaboration des concepts propres au maintenicien, cadre de nos travaux.

Après avoir présenté l'ensemble des fonctions et opérations permettant d'instancier les concepts associés au modèle de produit, nous allons dans le chapitre suivant décrire le modèle informatique interne c'est-à-dire la structure des données manipulées lors du processus de conception.

CHAPITRE 4

SPECIFICATION DU SYSTÈME D'AIDE À LA CONCEPTION DE SYSTÈMES SÛRS

INTRODUCTION

Dans les chapitres précédents, nous avons décrit la démarche de conception élaborée au laboratoire. En particulier, le chapitre 2 était consacré au modèle de produit défini par cinq niveaux de représentation ; chacun d'eux comprend un certain nombre de concepts décrivant le produit à concevoir à partir de différents points de vue et relativement à divers métiers. Contrainte et/ou objectif qu'un produit se doit aujourd'hui de respecter, la sûreté de fonctionnement a été retenue comme cadre de nos travaux. Nous avons donc proposé différents concepts à prendre en compte pour concevoir un système ou produit au fonctionnement sûr.

Dans le chapitre 3 nous avons décrit le processus de conception en expliquant comment chaque concept du modèle de produit est mis en oeuvre pour aboutir au produit spécifié. Pour cela, nous avons présenté les différentes méthodes qui peuvent être utilisées pour mettre en oeuvre les concepts dédiés à la sûreté de fonctionnement. Nous avons également insisté sur l'aspect " évaluation " puisqu'à chacun des niveaux de représentation, il faut vérifier que les solutions proposées par chacun des concepteurs respectent bien les exigences du client. Si tel n'est pas le cas, des actions correctives sont alors proposées afin d'essayer d'y parvenir.

Dans le présent chapitre, nous allons décrire le modèle informatique interne de l'outil d'aide à la conception de systèmes prenant en compte la sûreté de fonctionnement. Ainsi, dans une première partie, nous exposons la technique de modélisation OMT (Object Modelling Technique) utilisée au laboratoire pour décrire les données à manipuler et à mettre en oeuvre. Cette technique se compose de trois modèles que nous présentons : le modèle objet, le modèle dynamique et le modèle fonctionnel. Elle a été retenue car elle permet de représenter l'aspect statique de la démarche (modèle de produit) par l'intermédiaire du modèle objet ainsi que l'aspect dynamique (processus de conception) grâce aux modèles dynamique et fonctionnel.

La seconde partie est consacrée à l'application de cette technique à la démarche de conception proposée : le modèle de produit et les concepts dédiés à la sûreté de fonctionnement (chapitre 2) ; le processus de conception et les opérations nécessaires à l'instanciation des concepts (chapitre 3). Nous donnons pour chacun des niveaux de représentation du modèle de produit les modèles objet, dynamique et fonctionnel associés.

1. La technique de modélisation par objet OMT

La technique de modélisation par objet OMT (Object Modelling Technique) /RUMBAUGH 95//RUMBAUGH 96/ regroupe un ensemble de concepts orientés objets ainsi qu'une notation graphique indépendante du langage de programmation. Elle peut être utilisée pour analyser les spécifications d'un problème, concevoir une solution pour celui-ci et enfin, mettre en oeuvre cette solution à l'aide d'un langage de programmation ou d'une base de données /DANIEL 97/.

La méthode OMT fait appel à trois modèles différents pour décrire un système :

— un modèle objet exposant les objets et leurs relations au sein du système ;

— un modèle dynamique représentant les interactions entre les objets dans le système ;

— un modèle fonctionnel qui rend compte de la transformation des données du système.

Nous allons détailler chacun de ces modèles dans les paragraphes suivants.

1.1. Le modèle objet

Le modèle objet saisit la structure statique d'un système en décrivant les objets qui le

composent, les relations entre ces objets ainsi que leurs attributs et leurs opérations. Il fournit le cadre essentiel dans lequel les modèles dynamique et fonctionnel peuvent être placés. Le modèle objet est par conséquent le modèle le plus important des trois.

Le modèle objet est représenté graphiquement par des diagrammes d'objets contenant des classes. Celles-ci sont également organisées en hiérarchies partageant une structure et un comportement communs et sont associées à d'autres classes. Elles définissent les valeurs des attributs portés par chaque objet et les opérations que chacun d'eux accomplit. La figure 1 ci-dessous donne les principaux concepts du modèle objet.

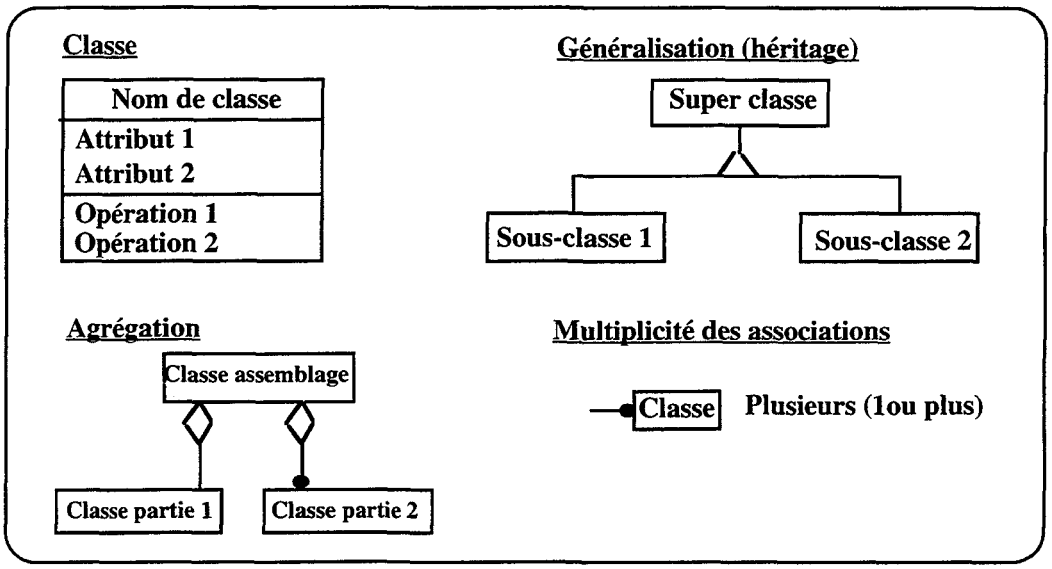

Figure 1 : Notations associées au modèle objet

2.2. Le modèle dynamique

Le modèle dynamique décrit les aspects du système qui se modifient avec le temps ainsi que la séquence des opérations possibles. Il modélise le contrôle c'est-à-dire qu'il décrit les successions d'opérations produites, sans attacher d'intérêt à ce que ces opérations produisent, à ce sur quoi elles portent ni à la façon dont elles sont mises en oeuvre.

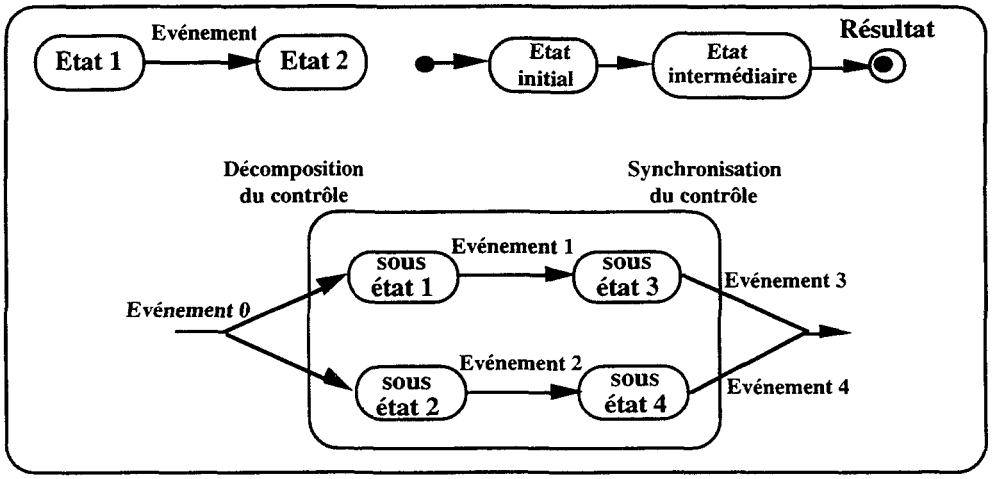

Figure 2 : Notations associées au modèle dynamique

Le contrôle est donc l'aspect du système qui décrit des séquences d'opérations activées par des stimuli externes, sans tenir compte de l'activité de ces opérations, de leur champ d'action et de leur mode de mise en oeuvre. Les concepts majeurs du modèle dynamique sont les événements qui représentent les stimuli externes et les états qui représentent les valeurs des objets.

La représentation graphique associée au modèle dynamique est le diagramme d'états. La figure 2 reprend les diverses notations associées au modèle dynamique.

Chacun des diagrammes d'états met en évidence les séquences d'états et d'événements autorisés pour une classe d'objets. Les diagrammes d'états sont bien sûr en relation avec les deux autres modèles. Les événements d'un diagramme d'états deviennent des opérations attachées aux objets dans le modèle objet. Les actions, au sein des diagrammes d'états, correspondent quant à elles, aux fonctions du modèle fonctionnel que nous allons présenter dans le paragraphe suivant.

2.3. Le modèle fonctionnel

Le modèle fonctionnel décrit les aspects relatifs aux transformations des valeurs : fonctions, correspondances, contraintes et dépendances fonctionnelles. Il modélise ce que fait un système, sans s'occuper de la façon ni du moment où il le fait. Le modèle fonctionnel décrit donc les calculs à l'intérieur d'un système. Il indique les résultats d'un calcul sans préciser quand et comment ils ont été obtenus. Il spécifie la signification des opérations dans le modèle objet et la signification des actions dans le modèle dynamique, aussi bien que n'importe quelle contrainte dans le modèle objet.

Le modèle fonctionnel est représenté par des diagrammes à flots de données. Ceux-ci montrent les dépendances entre les valeurs et le calcul des valeurs de sortie à partir des valeurs d'entrée et des fonctions, sans tenir compte du moment ni même de l'exécution des fonctions. Les fonctions sont invoquées en tant qu'actions dans le modèle dynamique et participent au modèle objet en tant qu'opérations attachées aux objets. Les notations associées à ce modèle sont présentées figure 3.

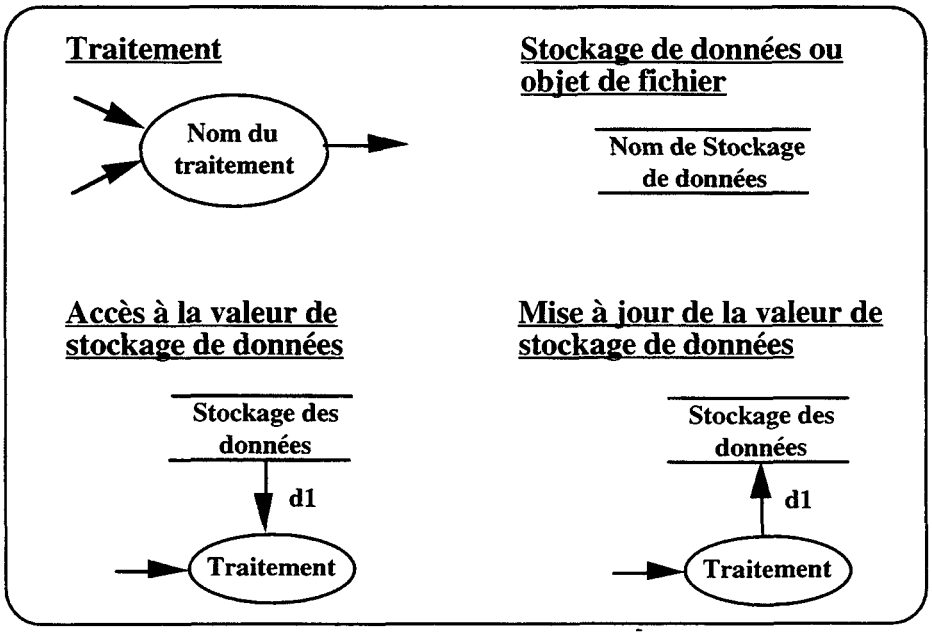

Figure 3 : Notations associées au modèle fonctionnel

2.4. Relations entre modèles

Chacun des modèles précédents décrit un aspect du système et contient des références aux autres modèles. Le modèle objet décrit les structures sur lesquelles les modèles dynamique et fonctionnel opèrent. Les opérations du modèle objet correspondent aux événements du modèle dynamique et aux fonctions du modèle fonctionnel.

Le modèle dynamique décrit la structure de contrôle des objets. Il met en évidence les décisions qui dépendent de la valeur des objets et invoquent des fonctions.

Le modèle fonctionnel décrit les fonctions invoquées par les opérations du modèle objet et les actions du modèle dynamique. Les fonctions opèrent sur les valeurs des données spécifiées par le modèle objet. Le modèle fonctionnel montre ainsi les contraintes qui pèsent sur les valeurs des objets. En résumé, nous pouvons dire que le modèle fonctionnel indique ce qui se passe, le modèle dynamique indique quand cela se passe et le modèle objet sur quoi cela se passe.

Après avoir présenté les trois modèles qui caractérisent OMT, nous allons maintenant appliquer cette technique à la modélisation de la démarche de conception décrite aux chapitres 2 (modèle de produit) et 3 (processus de conception) en s'appliquant à mettre en évidence les aspects spécifiques liés à la sûreté de fonctionnement.

2. Description du modèle de conception avec le formalisme OMT

Dans ce paragraphe, nous allons décrire comment est modélisée la démarche de conception par la technique OMT. Nous présentons les trois modèles (objet, dynamique, fonctionnel) associés à chacun des niveaux de représentation du modèle de produit. Nous allons porter notre attention uniquement sur l'aspect " Conception pour l'exploitation " qui enrichit le modèle défini par /JACQUET 98/ en lui intégrant la contrainte sûreté de fonctionnement. Chacun de ces modèles s'appuient sur les informations contenues dans les chapitres précédents.

2.1. Niveau Représentation du besoin

2.1.1. Le modèle objet

Le modèle objet associé à ce niveau comporte deux classes principales (figure 4) relatives aux concepts présentés au paragraphe 1. du chapitre 2 : il s'agit de la classe *Fonction de service FS* qui caractérise le besoin auquel le produit doit répondre et de la classe *Fonction contrainte globale FCG* qui représente les contraintes que le produit doit respecter. Nous retrouverons cette classe *Fonction contrainte globale* à chacun des niveaux de représentation puisque les contraintes sont propagées d'un niveau à un autre afin qu'elles soient respectées par le produit final (complètement spécifié). Seules les classes auxquelles elle sera associée seront différentes.

Cette classe *Fonction contrainte globale* nous intéresse plus particulièrement puisqu'elle comporte parmi ses éléments la sûreté de fonctionnement attendue. Celle-ci est une agrégation de quatre classes qui la caractérisent. Elle regroupe les sous-classes fiabilité, maintenabilité, disponibilité et sécurité. A chacune de ces caractéristiques va être attribuée une valeur qui correspond aux exigences que le client aura exprimées dans son cahier des charges. Ainsi, les attributs temps moyen de bon fonctionnement entre défaillances (MTBF), taux de défaillance, taux de disponibilité, ... vont être renseignés. Les valeurs attribuées constitueront les références pour l'évaluation des solutions proposées par les différents acteurs de la conception.

La sûreté de fonctionnement, avec ses différents attributs, va permettre de caractériser le comportement des fonctions de service du produit selon un point de vue particulier (fiabilité, disponibilité, ...). La classe *Comportement*, associée à la classe *Fonction de service*, a pour objectif de prendre en considération d'autres aspects comportementaux comme des temps d'exécution des fonctions, leurs enchaînements, ... C'est pour cette raison que nous l'avons

dissociée de l'aspect sûreté de fonctionnement.

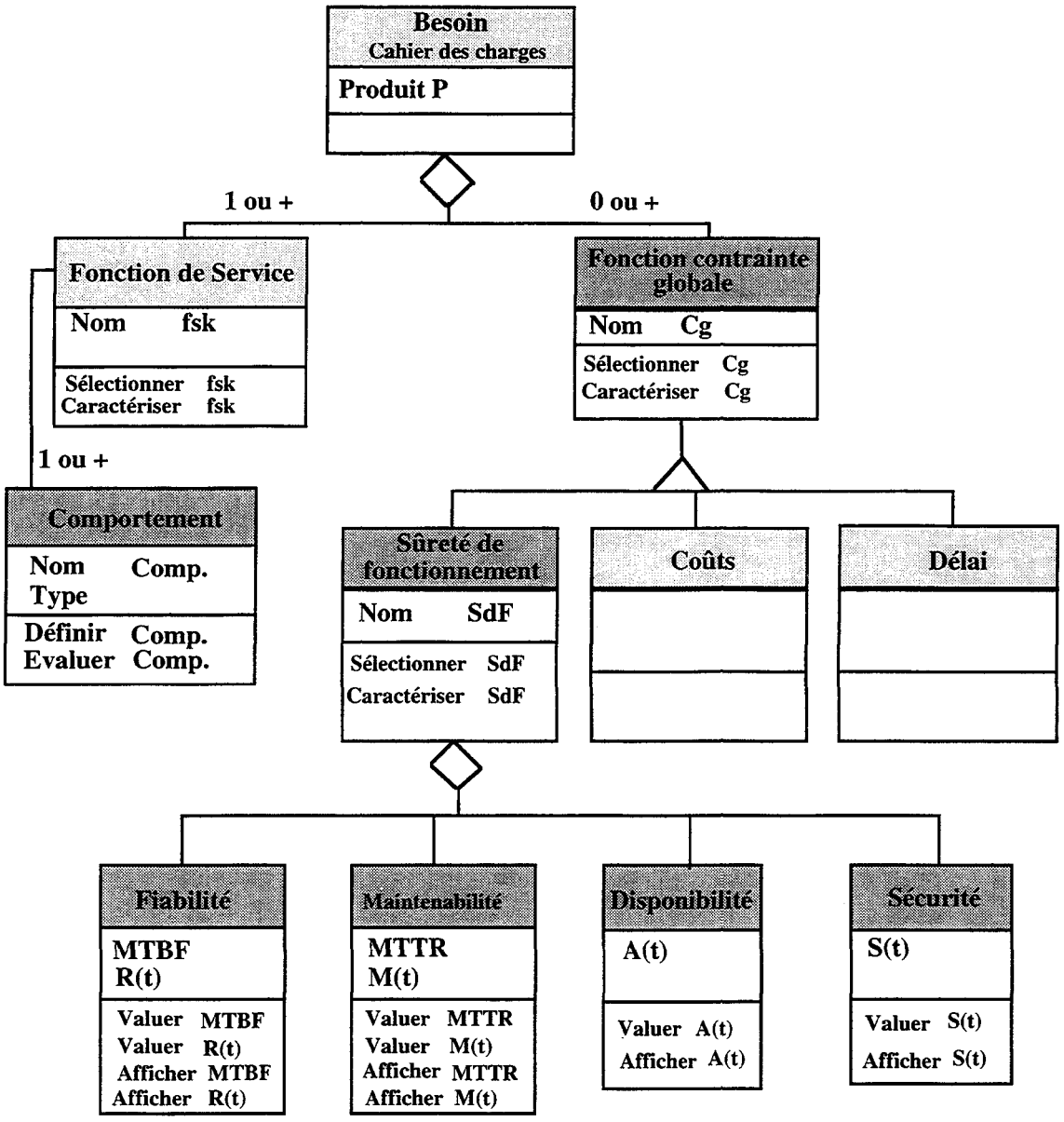

Figure 4 : Modèle objet du niveau Représentation du besoin

2.1.2. Le modèle dynamique

Nous associons à ce niveau de représentation un modèle dynamique aux classes *Fonction de service*, *Fonction contrainte globale* et aux sous-classes *Fiabilité*, *Maintenabilité*, *Disponibilité* et *Sécurité* (figure 5).

Pour la classe *Fonction de service*, ce modèle a pour premier objectif de caractériser les fonctions de service en leur associant une/des fonction(s) contrainte(s) qu'elles seront tenues de respecter. Le second objectif est d'évaluer du point de vue de leur comportement, les différentes fonctions de service afin de s'assurer qu'elles respectent bien les exigences du client. Les modèles de comportement utilisés pour cette évaluation sont les modèles définis à chacun des autres niveaux de représentation du modèle de produit. Les modèles utilisés seront dédiés à la sûreté de fonctionnement si ce sont des caractéristiques de ce type qui doivent être vérifiées. Cela pourra être un simulateur de réseau de Pétri si par contre on cherche à vérifier la cohérence (non blocage) des éléments mis en oeuvre.

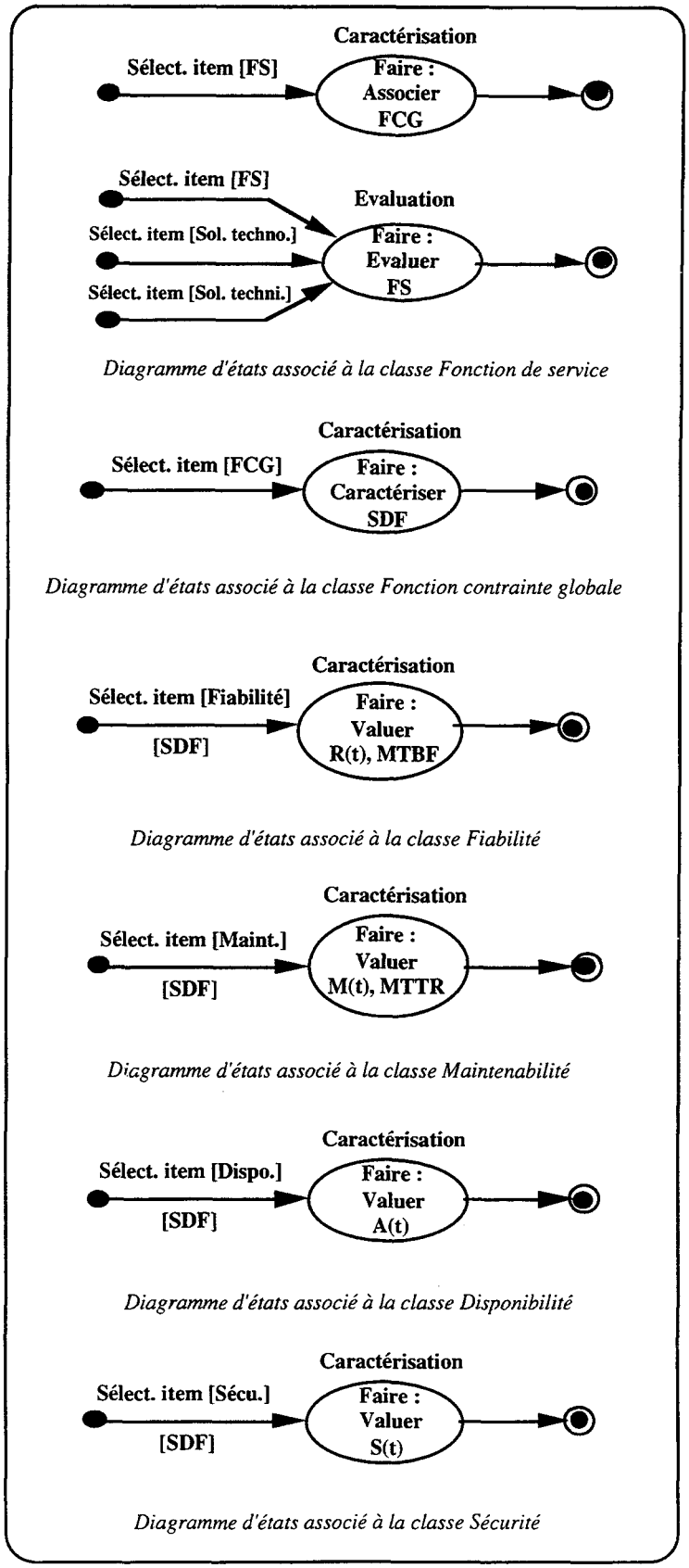

Figure 5 : Modèle dynamique du niveau représentation du besoin

Pour la classe *Fonction contrainte globale*, le modèle dynamique vise à la caractériser en

lui associant la sûreté de fonctionnement. Cette dernière sera précisée par la caractérisation des sous-classes qui la composent (fiabilité, maintenabilité, disponibilité, sécurité). Cette caractérisation passe par l'attribution de valeurs à ces différentes caractéristiques à partir des informations spécifiées par le client et contenues dans le cahier des charges.

2.1.3. Le modèle fonctionnel

Le modèle fonctionnel associé à ce niveau de représentation (figure 6) ne décrit pas les calculs effectués sur certaines entités du modèle de produit. Il permet simplement au concepteur d'associer les caractéristiques de sûreté issues du cahier des charges à la fonction contrainte globale *sûreté de fonctionnement* puis de les afficher éventuellement à l'écran (sinon, elles peuvent être stockées en mémoire pour une utilisation ultérieure).

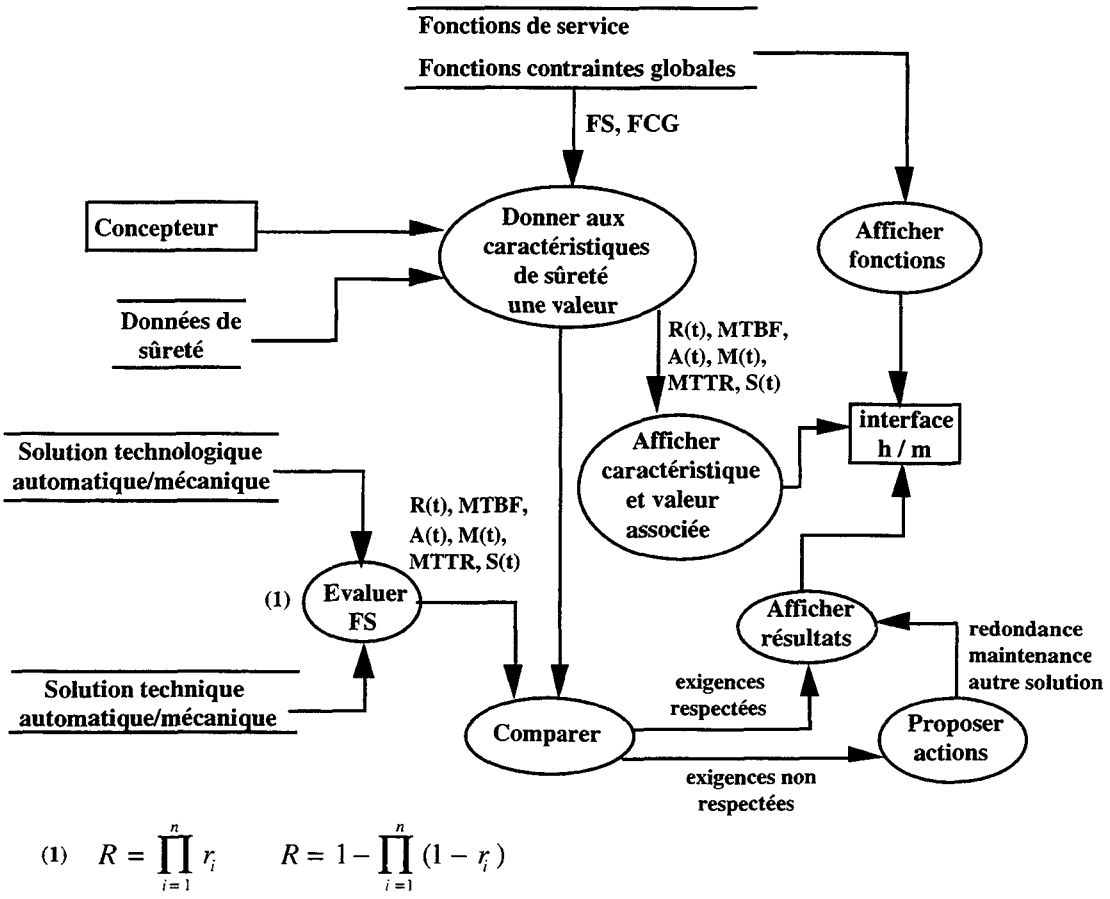

Figure 6 : Modèle fonctionnel associé au niveau Représentation du besoin

Ce sont ces valeurs qui seront ensuite propagées aux niveaux inférieurs et qui devront toujours être respectées. Comme nous l'avons dit précédemment, ce sont les valeurs données ici qui feront référence lors de l'évaluation de la sûreté de fonctionnement des diverses solutions proposées.

Les opérations et méthodes associées à ce modèle et au modèle dynamique ont été plus largement décrites au paragraphe 2. du chapitre 3.

2.2. Niveau Représentation des exigences fonctionnelles

2.2.1. Le modèle objet

Les éléments de base de ce modèle (figure 7) sont la chaîne opératoire et les fonctions

opératoires qui la constituent (ces éléments du modèle de produit ont été décrits au paragraphe 2. du chapitre 2) .

Nous associons à la classe *Fonction opératoire* la classe *Mode de marche MM* (concept décrit au paragraphe 2.2 du chapitre 2). Celle-ci regroupe l'ensemble des modes de fonctionnement qu'une fonction opératoire peut avoir. Nous lui associons également la classe *Mode de défaillance Mof* (concept présenté au paragraphe 2.1. de ce même chapitre) qui intègre les différentes façons qui font qu'une fonction opératoire peut ne pas avoir un fonctionnement nominal. L'évaluation de ces modes va conduire à la définition d'actions (correctives, préventives) qui mèneront à la mise en redondance de la fonction ou simplement à la prescription de procédures de maintenance préventive.

Nous associons aux classes *Chaîne opératoire* et *Fonction opératoire* la classe *Comportement*. Cette classe permet de caractériser les deux autres en leur associant des modèles, des valeurs, ... Ces modèles permettront d'une part, de vérifier la cohérence entre les fonctions opératoires de la chaîne initiale et celles qui pourraient être ajoutées à la suite de l'analyse AMDE. Un simulateur de réseau de Pétri permettrait par exemple de vérifier cette cohérence (recherche de blocages). D'autre part, l'utilisation des relations de définition de la fiabilité prévisionnelle vont permettre de s'assurer que les exigences de sûreté sont vérifiées par l'ensemble de la chaîne.

Par conséquent, cette classe *Comportement* joue un rôle essentiel dans l'évaluation qui peut être faite des fonctions opératoires et de la chaîne. En effet, c'est le résultat donné par la simulation du modèle de comportement que nous allons comparer à la valeur de référence définie au niveau de représentation précédent. Le résultat de cette comparaison conduit à la définition d'actions de type redondance, maintenance, autres solutions, ...

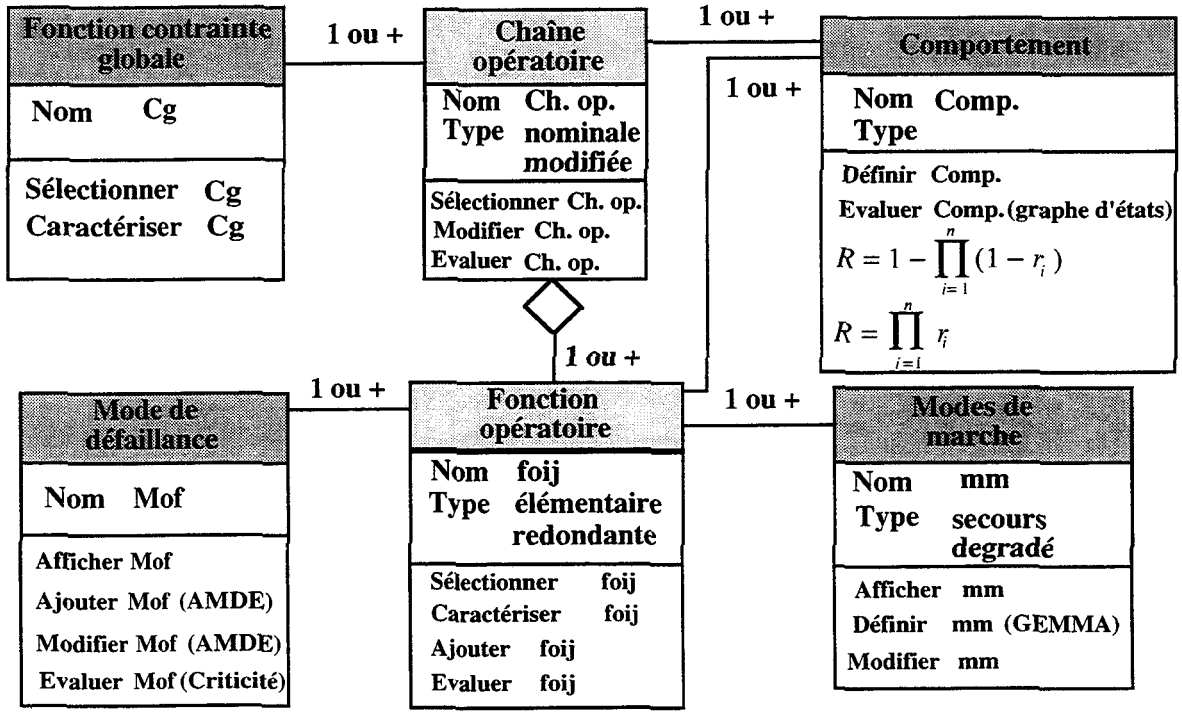

Figure 7 : Modèle objet du niveau Représentation des exigences fonctionnelles

Nous associons également aux fonctions opératoires une classe *Fonction contrainte globale* qui est la même que celle du niveau précédent. C'est la trame commune à tous les niveaux de représentation que l'on applique à des éléments différents suivant le niveau considéré. A ce niveau, c'est la chaîne opératoire (nominale ou modifiée), constituée de plusieurs fonctions opératoires, que nous évaluons. C'est donc elle qui va devoir respecter les exigences de sûreté

demandées par le client. Cette évaluation est faite à partir des caractéristiques de sûreté de chacune des fonctions opératoires qui la composent.

2.2.2. Le modèle dynamique

Les modèles dynamiques associés aux classes *Chaîne opératoire*, *Fonction opératoire*, *Mode de défaillance*, *Mode de marche* et *Comportement* sont présentés figure 8.

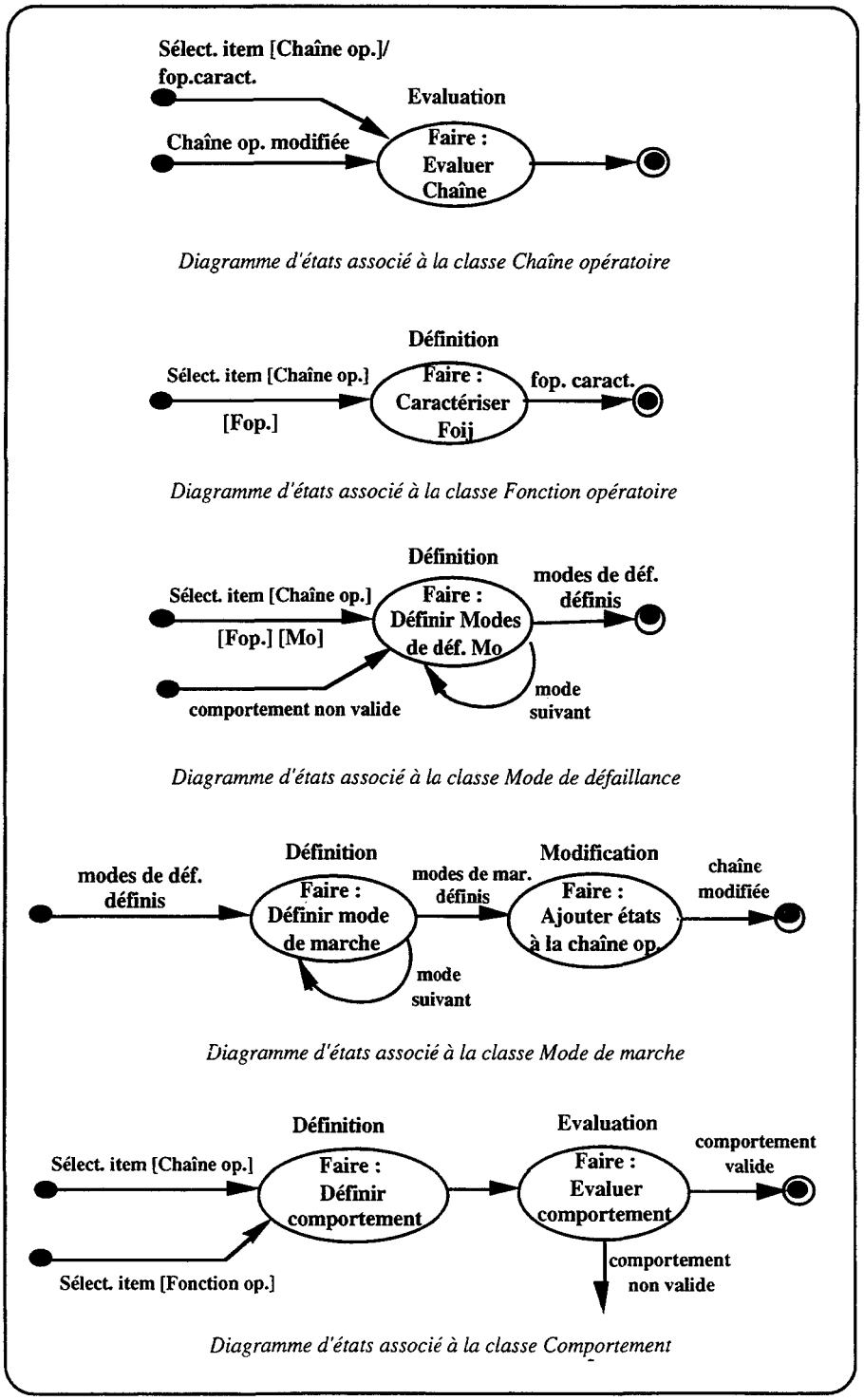

Diagramme d'états associé à la classe Chaîne opératoire

Diagramme d'états associé à la classe Fonction opératoire

Diagramme d'états associé à la classe Mode de défaillance

Diagramme d'états associé à la classe Mode de marche

Diagramme d'états associé à la classe Comportement

Figure 8 : Modèle dynamique associé au niveau Représentation des exigences fonctionnelles

Pour la classe *Fonction opératoire*, le modèle dynamique a pour objectif de caractériser chacune des fonctions opératoires de la chaîne. Pour cela, nous attribuons à chacune des fonctions une valeur en suivant par exemple la procédure qui a été décrite au paragraphe 3.1. du chapitre 3. A partir de là, une évaluation de la chaîne opératoire complète est possible (par l'utilisation de la relation de définition de la fiabilité prévisionnelle pour les systèmes ayant une structure série).

Pour la classe *Chaîne opératoire*, le modèle dynamique vise à faire une évaluation de la chaîne opératoire à partir de l'allocation de caractéristiques de sûreté de fonctionnement aux différentes fonctions opératoires qui la constituent (toujours par l'utilisation de cette même relation). On vérifie ainsi que les caractéristiques de sûreté de chacune des fonctions opératoires permettent de contribuer au respect des exigences demandées par le client.

Le modèle associé à la classe *Mode de défaillance* vise à définir, pour chaque fonction opératoire, les modes de défaillance susceptibles d'apparaître et de compromettre ainsi le respect des exigences de sûreté (le concepteur remplit le tableau AMDE qui lui est proposé à l'écran). Ainsi, les modes de défaillance vont conduire à ajouter des états supplémentaires à la chaîne opératoire initiale. Pour contrer l'apparition de ces défaillances et passer d'un état défaillant ou dégradé à un fonctionnement alternatif, nous ajoutons des modes de marche au produit qui pourront aboutir à l'ajout de fonctions opératoires (cas de la redondance). Cette chaîne opératoire modifiée sera évaluée afin de vérifier qu'elle respecte bien les exigences de sûreté du client.

Le modèle dynamique de la classe *Mode de marche* est activé lorsque des modes de défaillance jugés à risque ont été définis. Il vise alors à définir, en les sélectionnant dans une liste prédéfinie, les modes de marche qui permettront de contrer ces modes de défaillance et de respecter ainsi les exigences de sûreté. Des redondances, des modes de marche dégradée, des mises en position de sécurité, des procédures d'arrêt pourront alors être mises en oeuvre.

Enfin, nous avons un modèle dynamique associé à la classe *Comportement*. Le comportement concerne à ce niveau la chaîne opératoire. Il va consister à s'assurer que le comportement des différentes opérations de la chaîne se fait correctement et éventuellement dans un temps défini *a priori*. Quant à la caractéristique *comportement* associée aux fonctions opératoires, elle peut porter sur un temps d'exécution de la fonction mais également sur des taux de défaillance, des taux de fiabilité ou de disponibilité, ...

2.2.3. Le modèle fonctionnel

A ce niveau de représentation, la première opération consiste à répartir sur chacune des fonctions opératoires constituant la chaîne opératoire, les caractéristiques de sûreté définies au niveau de représentation précédent. Nous calculons, à partir des relations d'évaluation de la fiabilité prévisionelle d'un système, la fiabilité de l'ensemble afin de s'assurer que les exigences du client sont bien respectées. Si tel n'est pas le cas, le concepteur change la répartition et peut à nouveau faire une évaluation (figure 9).

En marge de cela, à partir de la chaîne opératoire issue de l'étude de projet, on peut apporter (par l'intermédiaire d'une fenêtre interactive) des renseignements au tableau d'analyse des modes de défaillance qui regroupe, pour chaque fonction opératoire, les différents types de défaillance susceptibles d'apparaître. Selon leur gravité (conséquence sur le respect des exigences de sûreté), des modes de marche seront proposés (secours par exemple). Ils engendreront la modification de la chaîne opératoire initiale par addition d'états nouveaux (sécurité, maintenance, ...) voire par ajout d'autres fonctions opératoires (redondance).

La chaîne opératoire modifiée pourra à son tour être évaluée suite à l'addition de nouvelles fonctions opératoires et par conséquent à la suite d'une nouvelle répartition des caractéristiques de sûreté sur la chaîne (notamment dans le cas de la mise en redondance active d'une fonction opératoire).

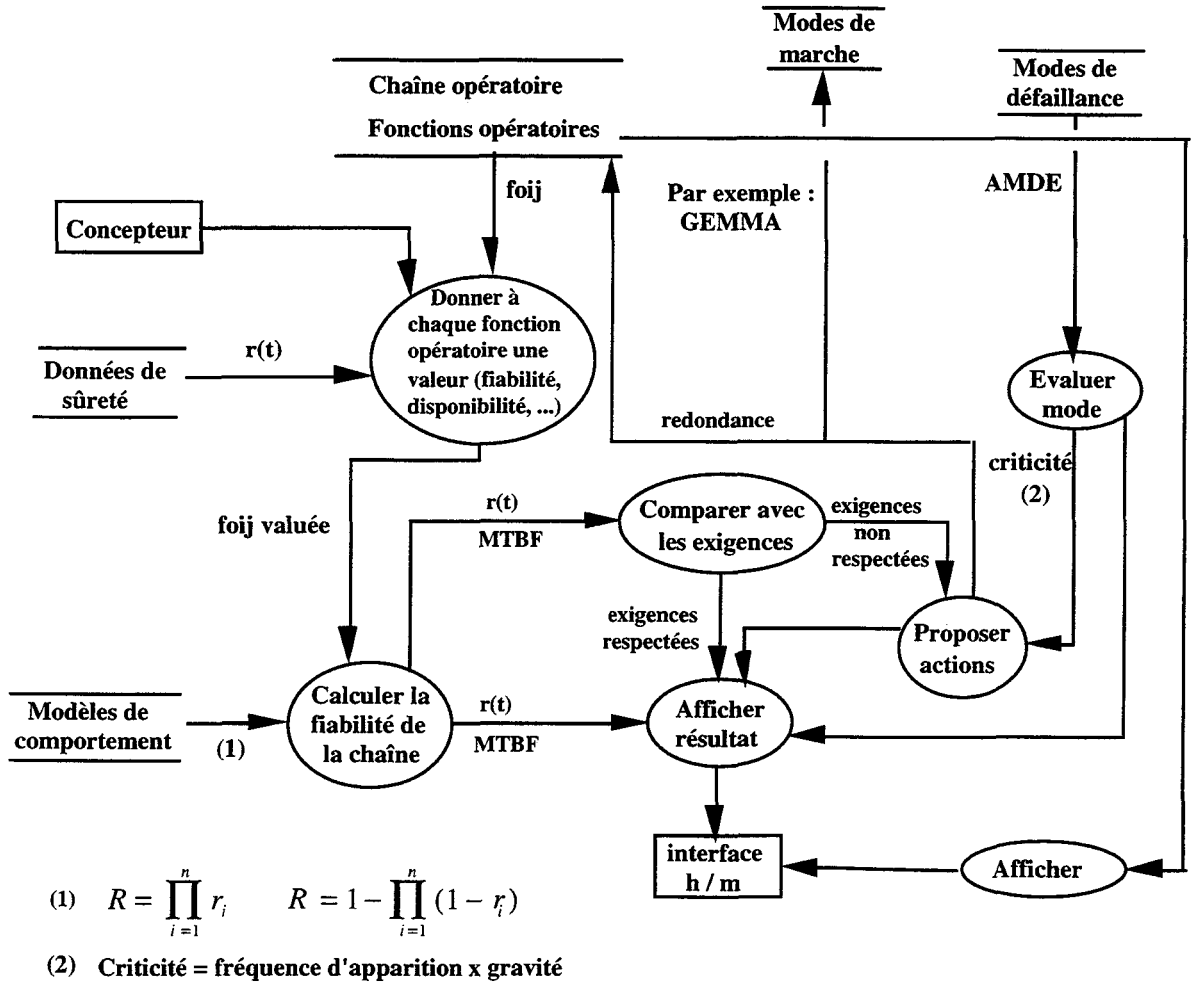

Figure 9 : Modèle fonctionnel associé aux niveau Représentation des exigences fonctionnelles

Les opérations et méthodes représentées par ce modèle et le modèle précédent ont été décrites des paragraphes 3.1. à 3.3. du chapitre 3.

2.3. Niveau Représentation technologique

2.3.1. Le modèle objet

A partir de la chaîne opératoire validée au niveau précédent, chacun des acteurs de la conception (automaticien, mécanicien) va associer aux fonctions opératoires de la chaîne une ou plusieurs fonctions de base FB (concept défini au paragraphe 3.1. du chapitre 2).

Si l'analyse des modes de défaillance a fait apparaître la nécessité de mettre en place des moyens de surveillance et de diagnostic, alors il faudra faire état des fonctions de base Maintenance (figure 10). Elles seront associées à des fonctions opératoires particulières (dans le cas par exemple d'une redondance partielle) ou à la chaîne opératoire complète (dans le cas d'une redondance totale).

La classe générique *Fonction de base* est relative à tous les métiers de la conception. Elle regroupe les fonctions de base de chaque concepteur. La classe *Composant technologique CO* lui est associée. Celle-ci regroupe l'ensemble des solutions qui peuvent supporter les fonctions de base retenues par les différents intervenants (automaticien, mécanicien, ...). L'agrégation de ces composants technologiques (donc des fonctions de base) constitue la solution technologique *Sto* (concept présenté au paragraphe 3.2. du chapitre 2) de chacun des intervenants.

Du point de vue de la conception en vue de l'exploitation, des procédures seront associées aux composants technologiques (stratégie de diagnostic par exemple) et cet ensemble (composant-procédure) constituera alors la Solution technologique du maintenicien (architecture d'instrumentation et de surveillance).

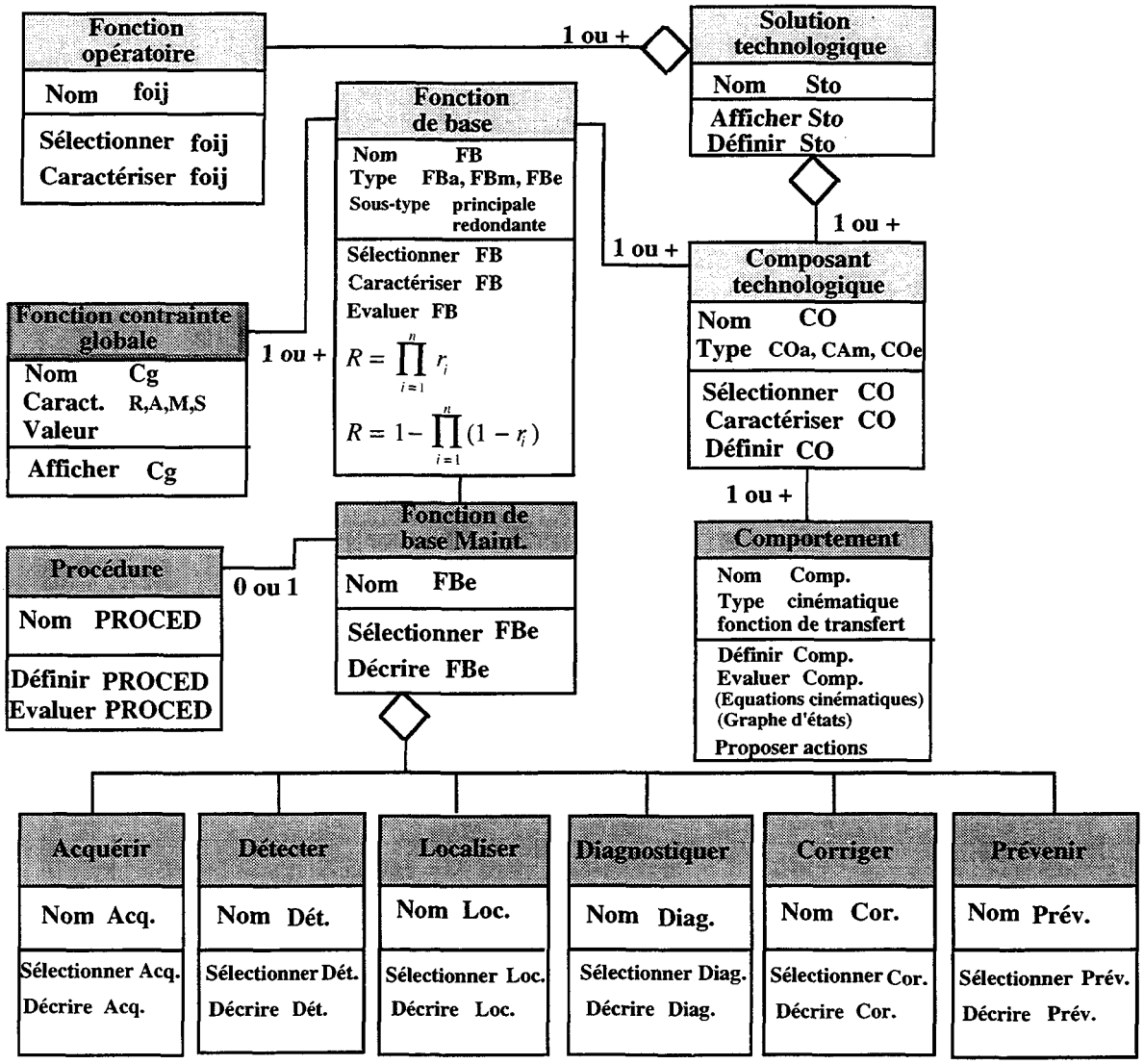

Figure 10 : Modèle objet du niveau Représentation technologique

Parmi ces fonctions de base, celles qui sont relatives au métier de la maintenance nous intéressent plus particulièrement. Elles sont une agrégation de fonctions relatives à la surveillance et au diagnostic des défaillances du produit que l'on a à concevoir.

Par l'intermédiaire de la classe *Comportement.*, l'ensemble des fonctions de base (solution technologique) va être évalué. Tout d'abord, d'un point de vue local c'est-à-dire que chaque acteur va évaluer sa solution technologique à partir de modèles de comportement propres à chacune des disciplines concernées (automatique, mécanique, ...). Du point de vue du respect des exigences de sûreté, les modèles de comportement issus de ce domaine seront utilisés et appliqués à l'ensemble des fonctions de base du produit. Si les résultats de cette évaluation sont conformes à ce qui est attendu par le client, la solution sera retenue. Si plusieurs solutions ont été proposées, celle qui donne les meilleurs résultats sera évidemment retenue. Si par contre aucune solution ne convient *a priori*, des actions seront proposées (redondance, maintenance, surveillance, autre solution, ...).

C'est donc par l'intermédiaire de cette classe *Comportement* que nous allons vérifier que ce qui est conçu respecte bien les contraintes demandées par le client dans le cahier des charges. C'est également elle qui permettra de s'assurer que chacun des concepteurs respecte les contraintes définies par les autres lors du processus de conception.

2.3.2. Le modèle dynamique

Les modèles dynamiques de ce niveau sont associés aux classes *Composant* (technologique), *Comportement* et *Solution technologique* (figure 11).

Le modèle associé à la classe *Composant* vise à définir le composant technologique que l'on souhaite adjoindre aux différentes fonctions de base retenues et à le caractériser en précisant la technologie qui lui sera attribuée.

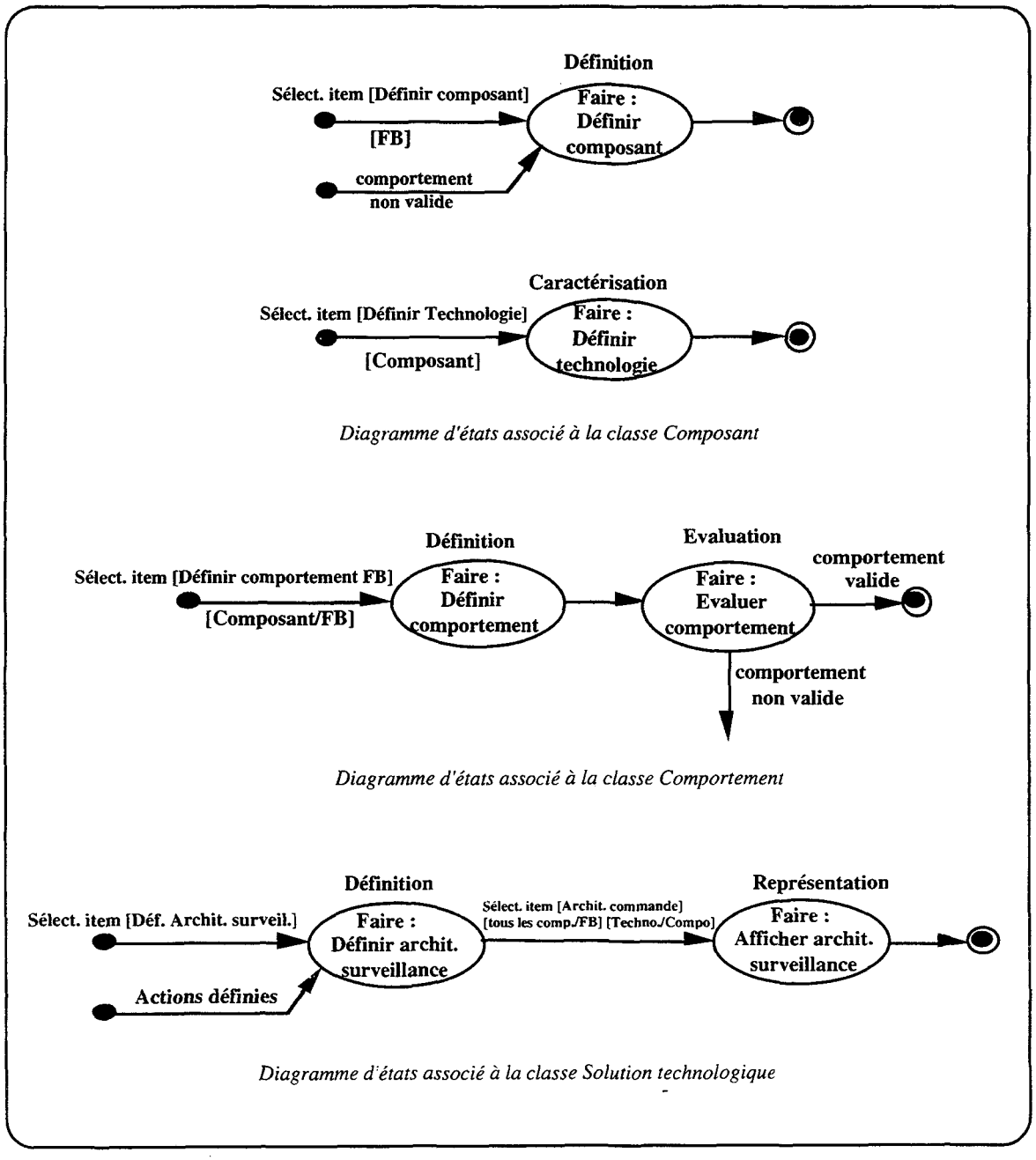

Diagramme d'états associé à la classe Composant

Diagramme d'états associé à la classe Comportement

Diagramme d'états associé à la classe Solution technologique

Figure 11 : Modèle dynamique associé au niveau Représentation technologique

L'ensemble des composants auxquels une technologie aura été associée va alors constituer la solution technologique du métier considéré. Pour le point de vue Conception pour l'exploitation, nous associons à la classe *Solution technologique* un modèle dynamique qui permettra de définir l'architecture de surveillance à intégrer au produit. L'autre opération va simplement consister à afficher cette architecture à l'écran .

Le dernier modèle dynamique est associé à la classe *Comportement*, cette classe est comme nous l'avons déjà dit associée aux classes *Fonction de base* et *Composant*. Chacun des acteurs de la conception, à l'aide de ses propres modèles, peut ainsi évaluer le comportement de sa solution technologique et vérifier qu'elle respecte bien les contraintes (du client ou d'un autre concepteur). Du point de vue sûreté de fonctionnement, l'évaluation se fera à l'aide de modèles spécifiques comme ceux qui ont été cités au paragraphe 4.3. du chapitre 3.

2.3.3. Le modèle fonctionnel

A ce niveau de représentation, les opérations et les calculs réalisés sont du même type que ceux effectués au niveau précédent. La différence réside dans la nature des éléments sur lesquels sont effectués ces opérations et ces calculs (figure 12). Au niveau précédent, ils étaient réalisés sur les fonctions opératoires, ici ils le sont sur les fonctions de base et plus précisément sur l'architecture technologique du produit (ensemble des fonctions de base de tous les acteurs de la conception).

Deux aspects peuvent être distingués :

Le premier concerne le concepteur qui, en vue de l'exploitation, va venir ajouter à l'architecture de commande de l'automaticien ses fonctions de base Maintenance. Celles-ci permettent d'intégrer, relativement aux résultats des niveaux supérieurs et/ou inférieurs, des aspects Surveillance et Diagnostic. Ce concepteur évaluera également sa solution et ne la retiendra que si elle est la plus appropriée (en termes de résultats). Il peut également l'évaluer localement d'un point de vue sûreté de fonctionnement.

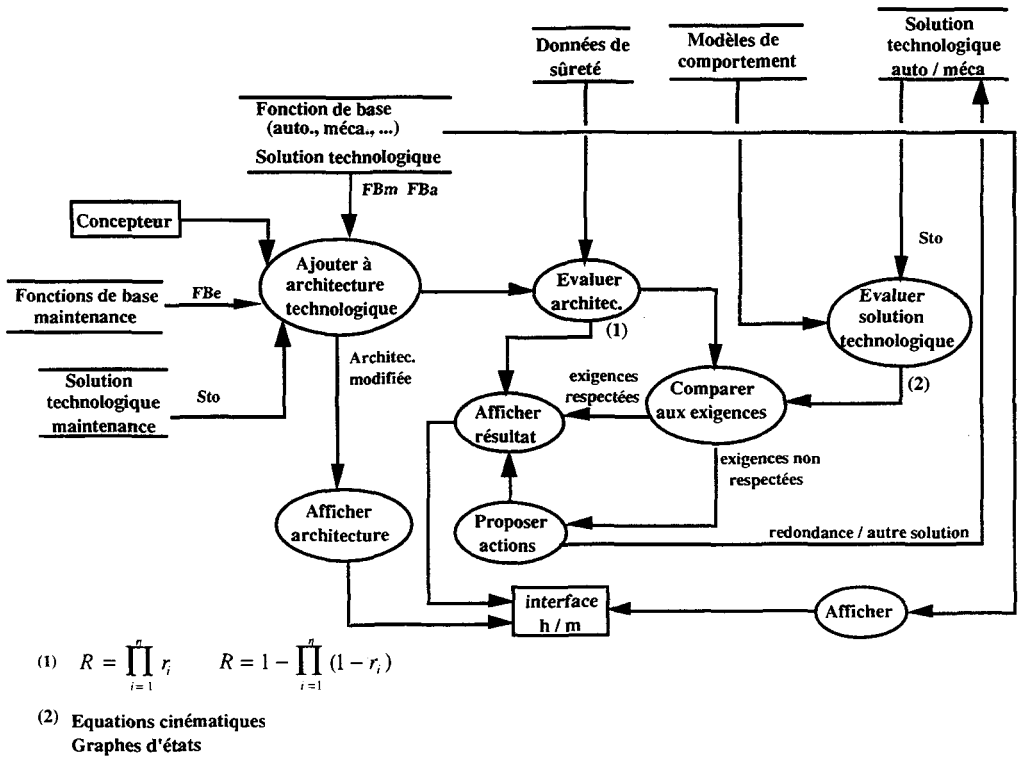

Figure 12 : Modèle fonctionnel associé au niveau Représentation technologique

Le second aspect concerne les autres concepteurs (mécanicien, automaticien, ...). Les solutions technologiques qu'ils proposent seront évaluées du point de vue de la sûreté de fonctionnement afin de s'assurer qu'elles respectent bien les exigences du client. Si tel n'est pas le cas, des actions seront alors avancées : mise en redondance de la solution, mise en oeuvre de politiques de maintenance, voire, remise en cause de la solution proposée.

Les opérations et méthodes utilisées dans ce modèle et dans le précédent ont été détaillées lors des paragraphes 4.1. à 4.4. du chapitre 3.

2.4. Niveau Représentation technique

2.4.1. Le modèle objet

Nous disposons à ce niveau de l'ensemble des fonctions de base que l'on peut regrouper au sein d'ensembles ou de sous-ensembles comme nous l'avons remarqué au paragraphe 6 du chapitre 2 (figure 13).

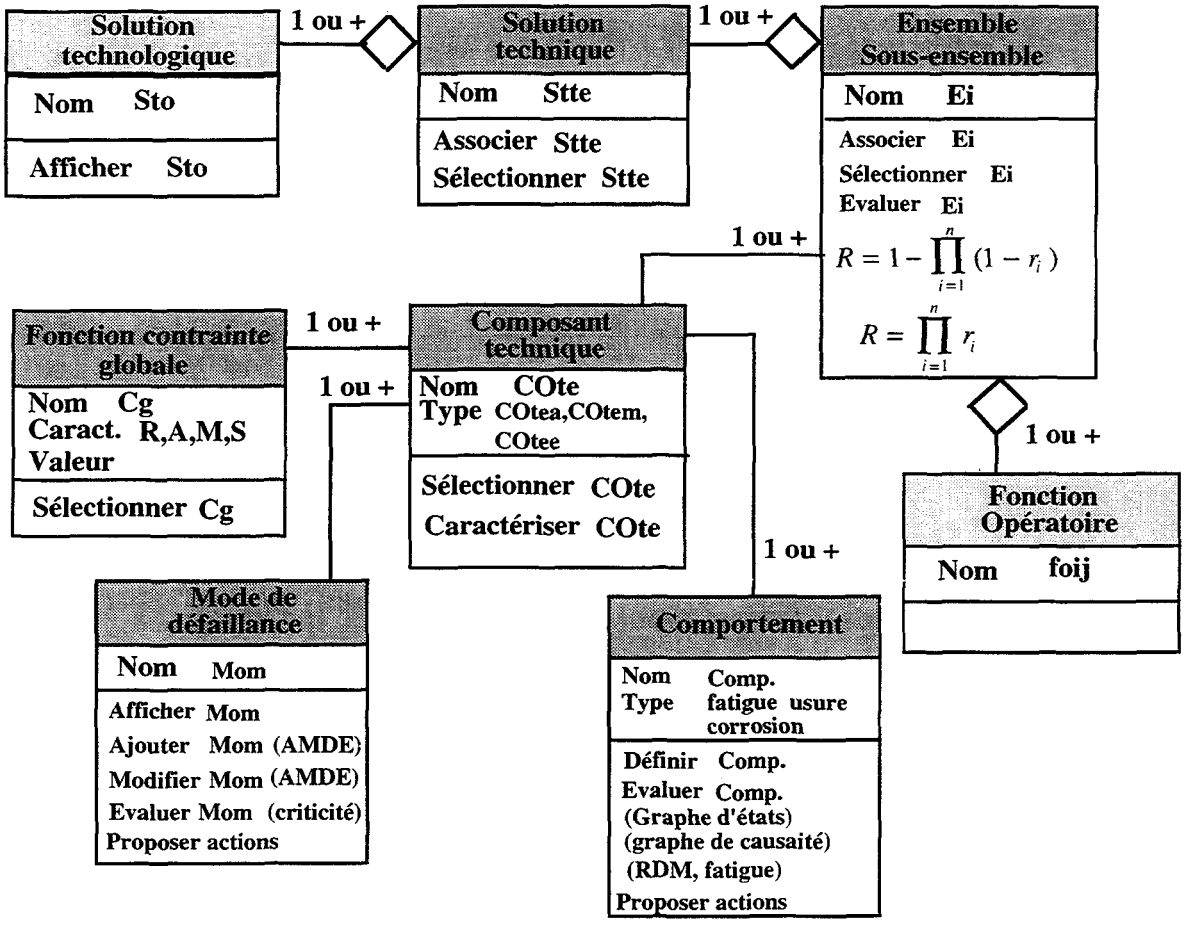

Figure 13 : Modèle objet du niveau Représentation technique

La structuration de tous les composants techniques d'un même concepteur constitue la solution technique Stte du métier considéré. Les solutions techniques (concept présenté au paragraphe 4.1. du chapitre 2) de chaque acteur de la conception sont regroupées au sein de la classe *Ensemble* qui est un élément structurant décrit au paragraphe 6. du chapitre 2. On peut également associer à cette classe, la classe *Fonction opératoire* déjà apparue au niveau représentation des exigences fonctionnelles. Ce lien existe dans le cas où, à partir de la chaîne opératoire, le concepteur a une idée *a priori* de la solution pouvant supporter les différentes fonctions opératoires de la chaîne opératoire. Il peut là aussi être amené à les regrouper entre elles.

Les contraintes globales s'appliquent à ce niveau sur la classe *Composant* c'est-à-dire sur l'entité technique que l'on associe aux fonctions de base définies au niveau de représentation précédent. C'est ensuite la solution technique (agrégation de composants techniques) qui est évaluée ici afin d'aboutir à un produit au fonctionnement sûr.

Ces composants techniques sont également caractérisés par un comportement (classe *Comportement*) et possèdent plusieurs modes de défaillance (classe *Mode de défaillance* caractérisant le concept décrit au paragraphe 4.2 du chapitre 2) obtenus par une analyse AMDE identique à celle menée au niveau représentation des exigences fonctionnelles mais elle porte cette fois sur des éléments matériels. Ces deux classes sont utiles pour la définition des composants sur lesquels une attention particulière sera à porter et qui engendreront alors la mise en redondance de certains composants, la définition de moyens de surveillance (ajout de fonctions de base), ..., en vue de respecter les exigences de sûreté de fonctionnement.

2.4.2. Le modèle dynamique

Les opérations associées à ce niveau sont du même type que celles que nous avons présentées au niveau représentation des exigences fonctionnelles mais elles s'appliquent cette fois à d'autres classes (figure 14).

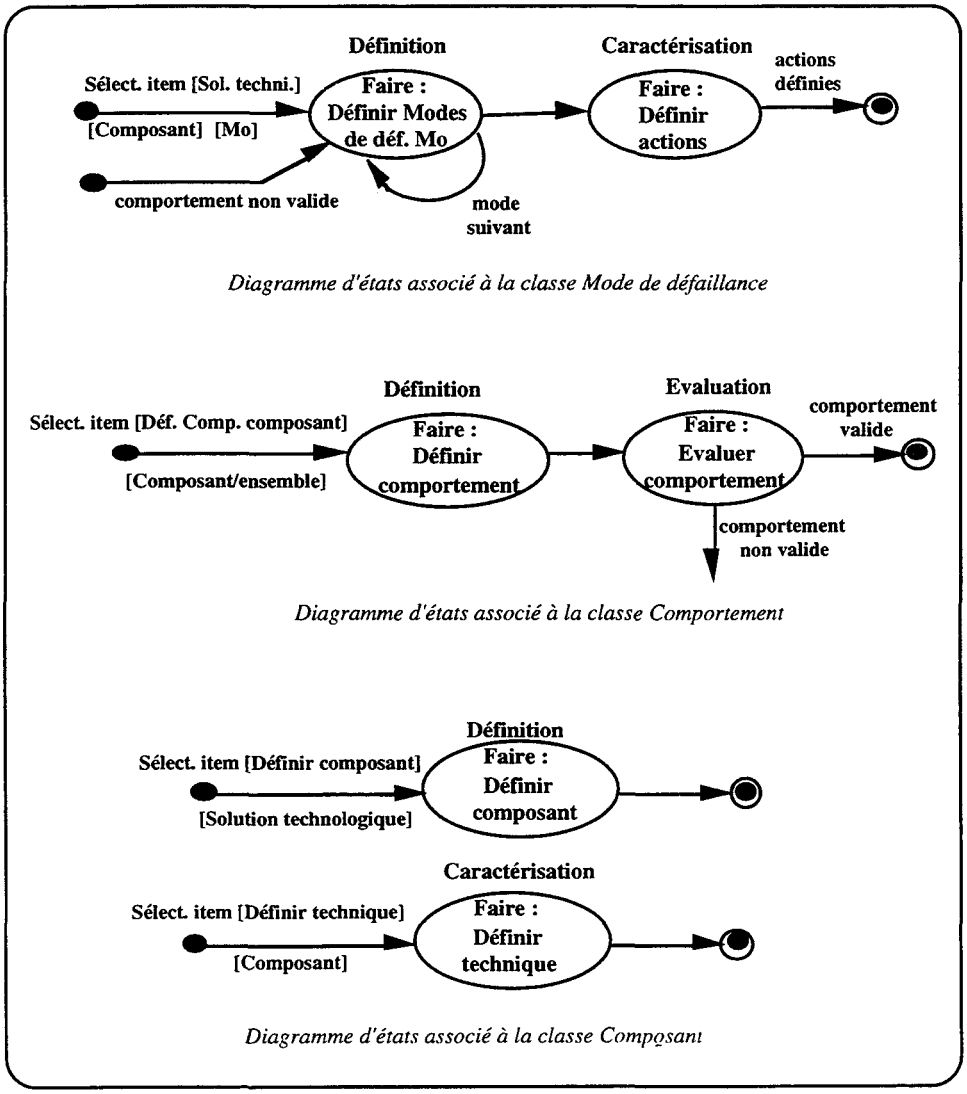

Diagramme d'états associé à la classe Mode de défaillance

Diagramme d'états associé à la classe Comportement

Diagramme d'états associé à la classe Composant

Figure 14 : Modèle dynamique associé au niveau Représentation technique

Nous associons tout d'abord un modèle dynamique à la classe *Mode de défaillance*. Il a pour objectif de définir les différents modes de défaillance pouvant apparaître sur les composants choisis par les autres concepteurs. Selon la gravité de ces modes, des actions vont alors être proposées. Elles vont de la mise en redondance de ce composant jusqu'à la mise en place de moyen de surveillance (ajout de fonctions de base au niveau représentation technologique) en passant par la mise en place de procédures de maintenance.

Le second modèle concerne la classe *Composant*. Il va permettre de définir les composants techniques qui supporteront les fonctions de base Maintenance définies au niveau précédent. Le concepteur pourra également par ce modèle caractériser la solution technologique (ensemble des fonctions de base)en lui associant une technique.

Enfin, le dernier modèle est associé à la classe *Comportement*. Il va chercher à définir, pour chaque composant, son comportement (toujours selon les différents points de vue métier), et à évaluer ensuite ce comportement afin de s'assurer que chaque composant respecte les contraintes (du client et / ou des autres acteurs de la conception).

2.4.3. Le modèle fonctionnel

Le principe de ce modèle est toujours le même mais s'applique cette fois sur les différents composants qui supportent les différentes fonctions de base (figure 15). Pour cela, le concepteur détermine tout d'abord les composants techniques qu'il utilise pour supporter les fonctions de base maintenance qu'il veut intégrer au produit. Dans le cadre de l'évaluation de la sûreté de fonctionnement, il va ensuite estimer les choix effectués par les autres concepteurs afin de s'assurer que les composants techniques choisis vérifient bien les exigences de sûreté du client.

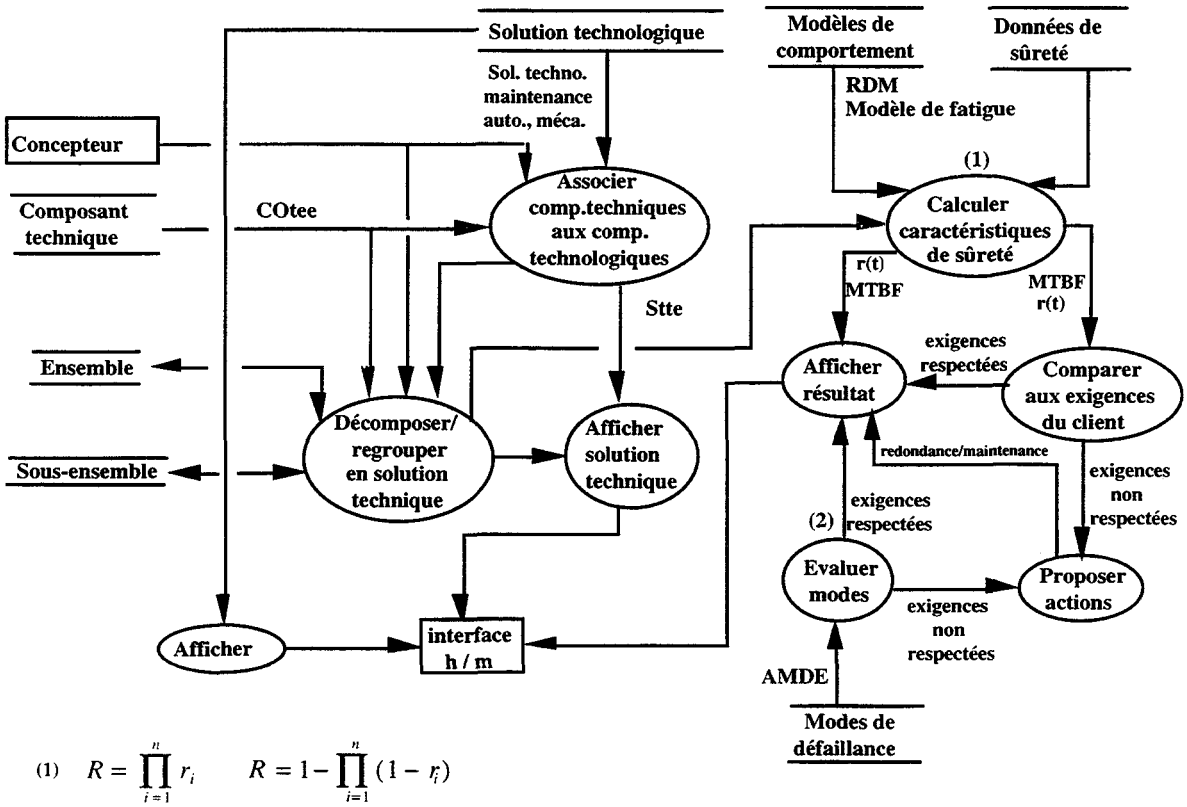

Figure 15 : Modèle fonctionnel associé au Niveau Représentation technique

Dans le cadre d'une nouvelle conception d'un élément existant (ensemble ou sous-ensem-

ble), le concepteur va modifier le tableau AMDE qui lui est associé en fonction du nouveau contexte dans lequel on se trouve. Des modes de défaillance vont apparaître, d'autres disparaître, changements qui aboutiront soit à la modification de l'architecture matérielle du produit (mise en redondance de certains éléments), soit à l'ajout de fonctions de base Maintenance au niveau représentation technologique.

Si des éléments sont mis en redondance (à partir de l'analyse AMDE menée sur les composants), l'évaluation de l'architecture matérielle sera réalisée à la suite de la mise en place de ces nouveaux composants. Les résultats de cette évaluation seront également comparés aux exigences du client afin de vérifier que celles-ci sont toujours respectées.

Les opérations et méthodes associées à ce modèle et au modèle précédent ont fait l'objet des paragraphes 5.1. à 5.5. du chapitre 3.

2.5. Niveau Représentation détaillée

2.5.1. Le modèle objet

Ce dernier modèle n'apporte pas d'informations complémentaires (figure 16) par rapport au modèle du niveau précédent.

Nous associons simplement aux solutions techniques (composants) des caractéristiques afin de les dimensionner précisément (classe *Caractéristiques matérielles* décrivant le concept présenté au paragraphe 5.1. du chapitre 2).

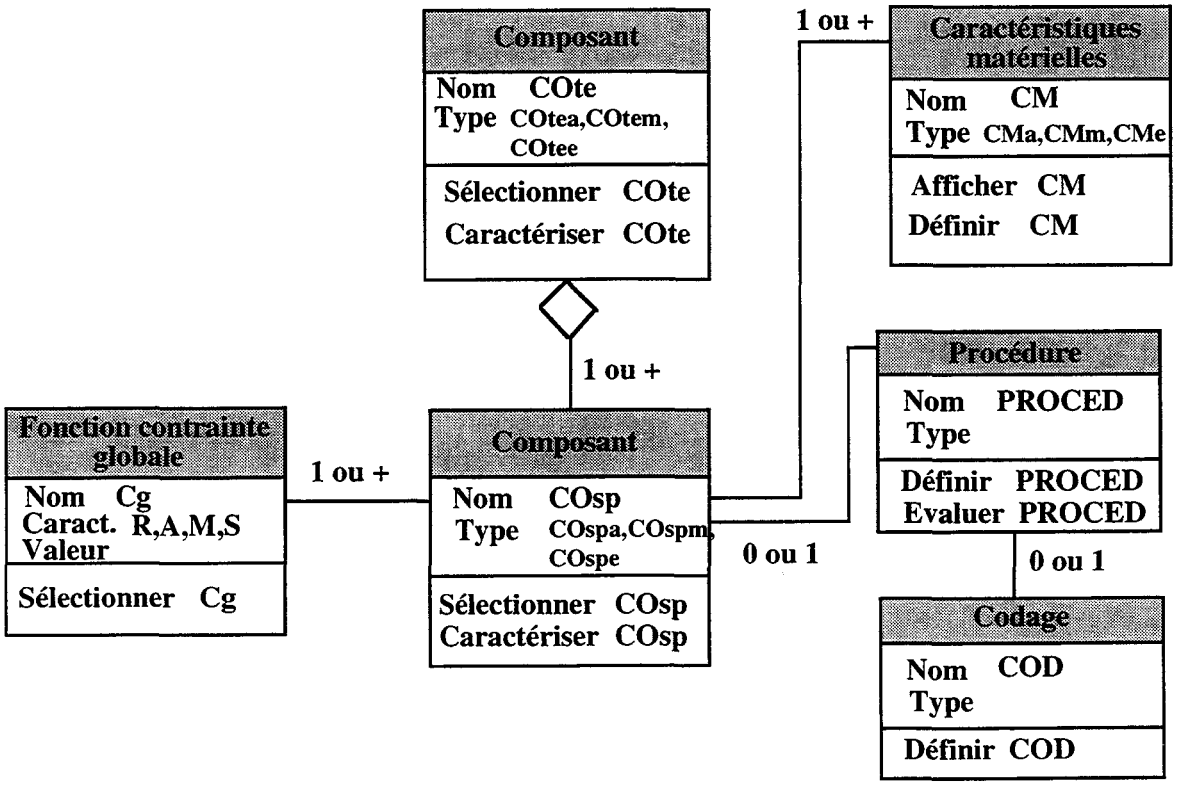

Figure 16 : Modèle objet associé au niveau Représentation détaillée

Nous associons également une classe *Codage* qui va consister à décrire, dans un langage approprié, les procédures associées aux fonctions de base du niveau représentation technologique. Le concept Codage a fait l'objet du paragraphe 5.2. du chapitre 2.

Une évaluation de la sûreté de fonctionnement du produit spécifié peut être effectuée. Par la connaissance du taux de défaillance, du taux de réparation, ..., des valeurs plus précises peuvent être obtenues pour les différentes caractéristiques de la sûreté de fonctionnement.

2.5.2. Le modèle dynamique

Deux modèles dynamiques sont distingués à ce niveau (figure 17).

Le premier est associé à la classe *Composant* afin de spécifier complètement le composant technique retenu au niveau de représentation précédent. Cette opération sera obtenue par la définition et l'attribution aux différents composants techniques de caractéristiques matérielles. Le second est associé à la classe *Codage* et va permettre de définir le codage à utiliser pour traduire les procédures décrites au niveau représentation technologique.

Les caractéristiques peuvent être modifiées dans le cas où le composant choisi s'avère moins fiable qu'un autre déjà connu et utilisé pour un autre produit par le concepteur.

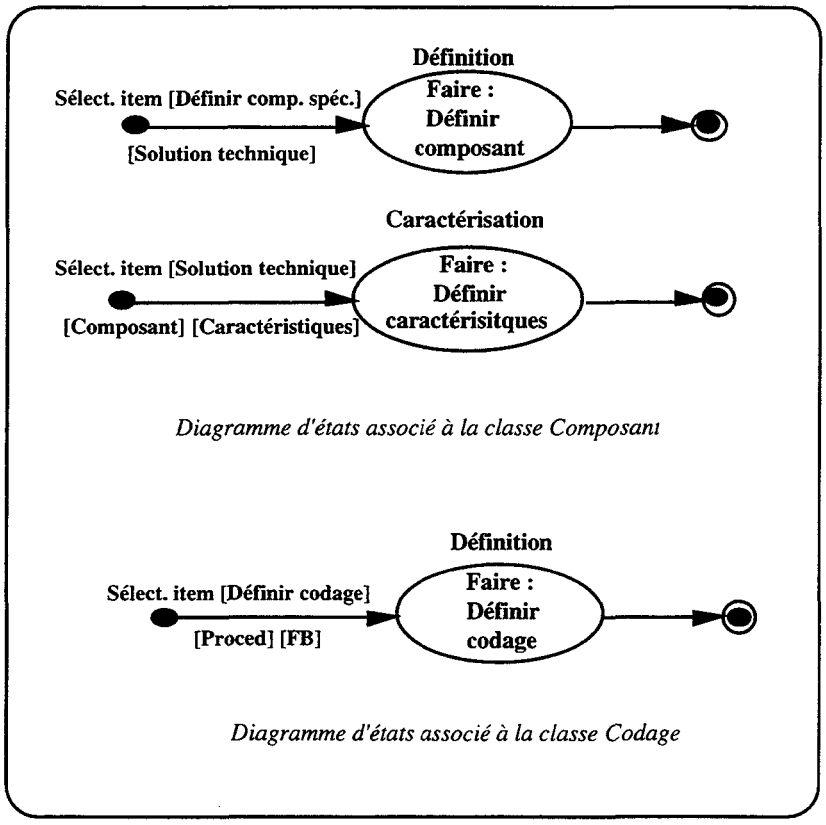

Figure 17 : Modèle dynamique associé au niveau Représentation détaillée

2.5.3. Le modèle fonctionnel

Ce dernier modèle permet de s'assurer que le produit spécifié respecte bien les exigences de sûreté exprimées par le client (figure 18).

Les calculs peuvent être simplement plus précis grâce à la connaissance exacte de certaines valeurs relatives à un type précis de composant (taux de défaillance, ...). Si les résultats obtenus ne sont pas satisfaisants, un autre composant sera choisi qui aura d'autres caractéristiques matérielles.

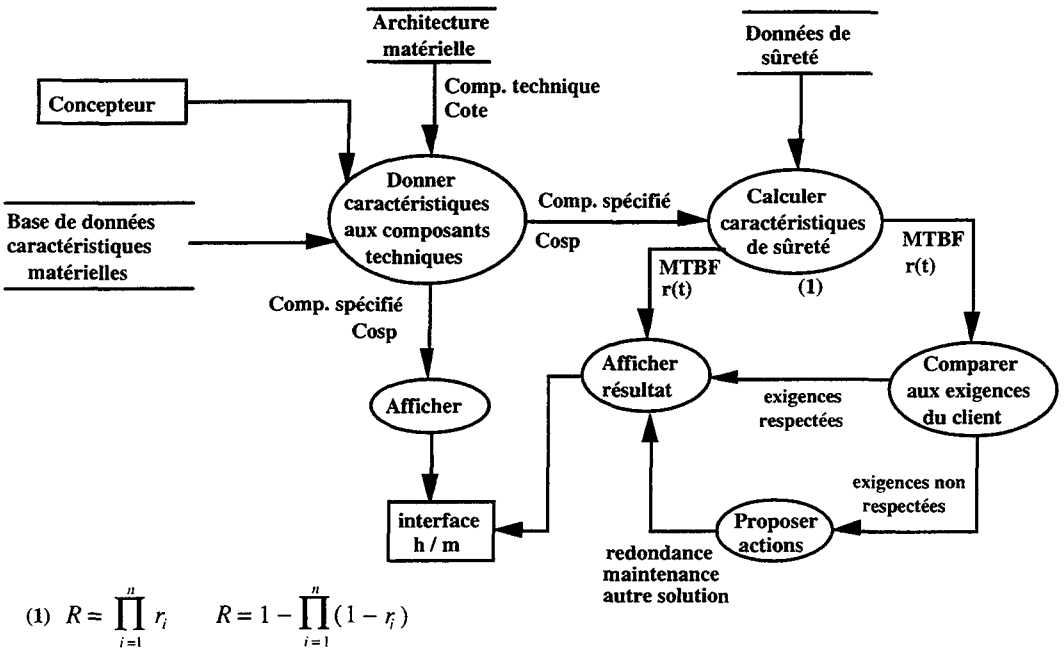

Figure 18 :Modèle fonctionnel associé au niveau Représentation détaillée

L'ensemble des opérations et méthodes composant les modèles dynamique et fonctionnel de ce niveau de représentation a fait l'objet des paragraphes 6.1. à 6.3. du chapitre 3.

CONCLUSION

Ce chapitre a présenté la structure de données de l'outil informatique, aide à la conception de systèmes au fonctionnement fiable.

Pour cela, nous avons décrit, dans une première partie, la technique de modélisation par objet OMT (Object Modelling Technique). Cette technique a pour objectif, par l'utilisation de trois modèles différents (modèle objet, modèle dynamique, modèle fonctionnel), d'analyser un problème, puis de concevoir sa solution et enfin de la mettre en oeuvre. Nous avons alors présenté chacun des trois modèles de la méthode afin de les expliquer et donner leur mode de représentation.

Dans la seconde partie du chapitre, nous avons proposé une représentation du modèle de produit et du processus de conception à l'aide des différents modèles OMT. Nous avons pour cela donné, à chacun des cinq niveaux de représentation (du besoin, des exigences fonctionnelles, technologique, technique, détaillée), les modèles objet, dynamique et fonctionnel associés. Nous nous sommes attachés à la description de l'intégration de la sûreté de fonctionnement au modèle proposé par /JACQUET 98/.

Nous avons ainsi traduit les concepts présentés au chapitre 2 par l'intermédiaire des modèles objet. Ces derniers présentent les éléments statiques qui seront manipulés lors du processus de conception. Les opérations associées à ce processus (chapitre 3) sont introduites au niveau des modèles dynamiques. Ils montrent comment les concepts sont mis en oeuvre (exemplifiés) lors de la conception. Enfin, le modèle fonctionnel décrit les données nécessaires, générées lors de l'exécution des opérations du modèle dynamique.

La technique OMT, par l'intermédiaire de ses trois modèles (objet, fonctionnel et surtout dynamique), permet donc de supporter l'ensemble des démarches de conception qu'un

concepteur est susceptible de mettre en oeuvre. C'est par conséquent un bon outil de modélisation qui permet, de plus, de supporter la non-monotonie de la démarche de conception proposée par le laboratoire.

Dans le chapitre suivant, nous allons présenter sur un exemple, différents scénario de conception afin d'illustrer, d'une part, la non monotonie de la démarche et, d'autre part, la prise en compte au sein de celle-ci, de la sûreté de fonctionnement.

CHAPITRE 5

VALIDATION DE LA DEMARCHE

INTRODUCTION

Dans les chapitres précédents, nous avons décrit la démarche de conception de systèmes au fonctionnement sûr. Pour cela, nous avons présenté dans le chapitre 2, les différents concepts relatifs à la sûreté de fonctionnement que nous intégrons au modèle de produit. Ces concepts visent, à chacun des niveaux de représentation, à ajouter des éléments qui finalement, garantiront que le produit conçu est sûr de fonctionnement et respecte bien les exigences du client.

Dans le chapitre 3, nous avons présenté le processus de conception c'est-à-dire les différentes méthodes qui peuvent être utilisées à chaque niveau pour mettre en œuvre les concepts associés au modèle de produit. Ce processus est non-monotone c'est-à-dire que les concepts ne sont pas obligatoirement instanciés de façon séquentielle et on peut donc passer d'un niveau de représentation à un autre non adjacent à celui-ci.

Dans le chapitre 4, nous avons décrit la structure de données associée à l'outil informatique d'aide à la conception de systèmes sûrs. Cette structure a été représentée par l'intermédiaire de la technique de modélisation objet OMT (Object Modelling Technique). Nous avons décrit cette structure grâce aux modèles objet, dynamique et fonctionnel que comporte cette technique.

Dans ce dernier chapitre, nous allons valider nos propositions à travers des scénarios de conception appliqués à un exemple, à différents niveaux. Pour cela, nous présentons dans une première partie le projet DSPT8, exemple sur lequel va être validée la démarche de conception proposée. Dans une seconde partie, nous présentons les différents scénarios de conception que le concepteur peut mettre en œuvre à chacun des niveaux de représentation du modèle de produit. Enfin, et dans une troisième partie, nous évaluons nos propositions à partir d'une maquette informatique que nous avons développée.

1. Description du projet DSPT8 /DSPT8 97/

Le projet «Scénario d'Ingénierie communicante pour les systèmes intégrés de production» visait à étudier le processus de conception d'un système de production dans un contexte d'ingénierie concourante.

Les objectifs majeurs de ce projet étaient de contribuer à l'élaboration de méthodes et d'outils en vue d'améliorer la coopération entre les différents acteurs de la conception ainsi que le processus de conception. Le scénario de conception a été appliqué à un système d'assemblage dont les spécifications sont issues d'une application industrielle d'assemblage de tronçons d'avions de chez Dassault Aviation à Argenteuil.

Nous allons, dans le paragraphe suivant, décrire plus précisément ce projet.

1.1. Le support du projet

Le projet sur lequel nous nous sommes appuyés est un banc d'assemblage de composants de fuselage d'avions, actuellement utilisé dans une version manuelle par la société Dassault. A partir des spécifications propres à l'assemblage de composants d'avions, l'objectif du projet était de concevoir un banc d'assemblage automatisé.

Le produit à réaliser est un sous-ensemble constituant un tronçon d'avion (fuselage). Il est obtenu par l'assemblage de six composants, chacun d'eux ayant leurs propres caractéristiques en termes de géométrie, de matériaux, d'éléments d'inertie. La figure 1 ci-dessous présente une vue éclatée du sous-ensemble, avant assemblage par rivetage, de chacun des composants.

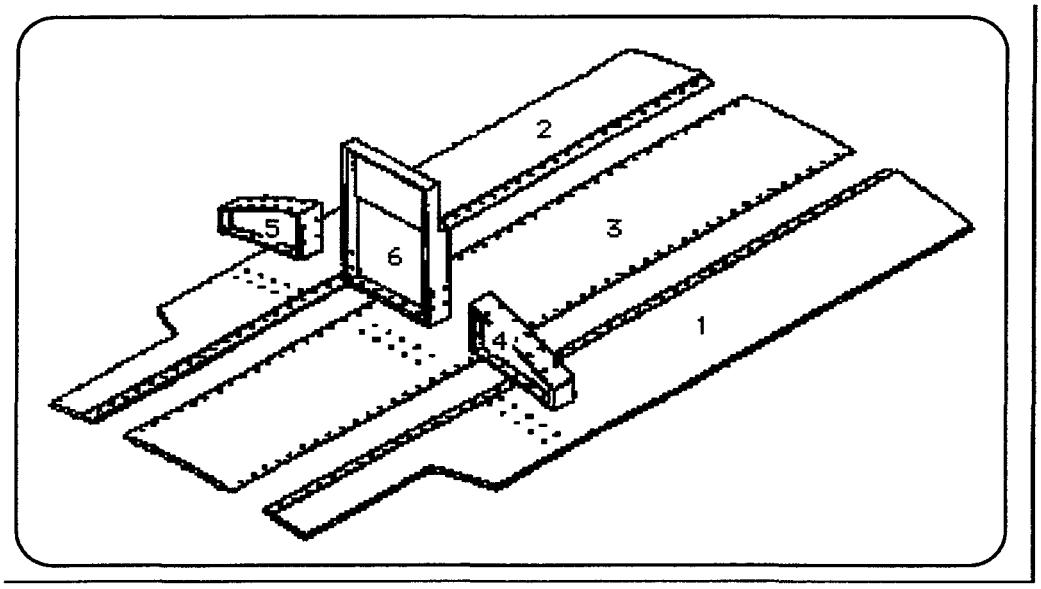

Figure 1 : Vue éclatée des composants à assembler

L'obtention du sous-ensemble du fuselage se fait par le rivetage de chacun des six composants qui le constituent par l'intermédiaire du banc d'assemblage. L'assemblage des six composants s'effectue en trois phases :

Phase 1 : assemblage des composants 1,2 et 3 ;

Phase 2 : assemblage du composant 6 sur l'ensemble {1,2,3} ;

Phase 3 : assemblage des composants 4 et 5 sur l'ensemble {1,2,3,6}.

Chacune de ces phases suit une gamme opératoire regroupant douze opérations distinctes :

Opération 1 : mise en position des composants à assembler

Opération 2 : maintien en position des composants à assembler

Opération 3 : épinglage des composants

Opération 4 : perçage et fraisage des composants

Opération 5 : démontage des composants

Opération 6 : nettoyage et ébavurage des composants

Opération 7 : étanchéité entre les composants

Opération 8 : remontage des composants

Opération 9 : épinglage des composants

Opération 10 : étanchéité des rivets

Opération 11 : rivetage des composants

Opération 12 : contrôle de l'assemblage

A partir de ces informations, le projet visait à automatiser l'opération d'assemblage des composants. La spécification de ce système d'assemblage s'est faite par la mise en œuvre de la démarche de conception proposée par /JACQUET 98/ à laquelle nous ajoutons la dimension sûreté de fonctionnement.

1.2. Le cahier des charges

Le cahier des charges initial ne contenait aucune information concernant les caractéristiques de sûreté que le système d'assemblage doit respecter. Dans le cadre de son automatisation et afin de valider nos propositions, nous introduisons des caractéristiques de sûreté que le système automatisé devra respecter. Ainsi, nous fixons :

- la fiabilité du système à 0.65 ou un temps moyen entre défaillances (MTBF) de 1800 heures ;
- la disponibilité à 0.85 ;
- la sécurité à 0 mort.

Le système doit être maintenable c'est-à-dire qu'il doit, entre autres, pouvoir être surveillé, testé, réparé, ..., en cas de défaillance ou de dégradation. Aussi, il est difficile de quantifier ces critères et c'est pour cela qu'en ce qui concerne la maintenabilité, nous ne lui fixons pas de valeur à respecter car les critères à prendre en compte sont trop nombreux (temps d'intervention, démontabilité, testabilité, ...).

Nous avons présenté dans cette première partie, le projet DSPT8 sur lequel nous allons valider nos propositions. Nous allons maintenant décrire, dans les paragraphes suivants, comment nous étendons le modèle proposé par /JACQUET 98/ par l'intégration de la sûreté de fonctionnement. Pour présenter comment nous vérifions que les caractéristiques de sûreté sont respectées, nous décrivons dans ce qui suit les scénarios de conception possibles qui permettent, à chacun des niveaux de représentation du modèle de produit :

- d'évaluer les solutions proposées par les différents acteurs de la conception et de vérifier que celles-ci respectent bien les exigences exprimées par le client ;
- de proposer des actions correctives lorsque les exigences ne sont pas respectées. Elles concernent notamment la définition de modes de marche (redondance, arrêt pour maintenance, ...), de procédures de maintenance ainsi que l'intégration de moyens de surveillance et de diagnostic au produit afin qu'il est un fonctionnement sûr.

2. Description des scénarios de conception

Les scénarios de conception représentent le processus de conception. Ils montrent quand et comment les concepts du modèle de produit (chapitre 2) sont mis en œuvre. La non-monotonie de la démarche fait que les concepts d'un niveau de représentation donné ne doivent pas nécessairement tous être instanciés pour passer à un autre niveau de

représentation. Le niveau auquel nous passons n'est pas obligatoirement le niveau suivant celui considéré comme nous l'avons décrit, de façon chronologique, dans les chapitres 2 et 3.

Nous allons présenter ci-dessous, sous forme de Grafcet, les scénarios de conception de systèmes sûrs que nous avons retenus pour chacun des niveaux de représentation du modèle de produit. En effet, par l'intermédiaire des transitions (qui représentent les choix que le concepteur peut faire) et des actions (qui donnent les réactions du simulateur face à ces événements), ce formalisme est bien adapté pour la description du processus de conception décrit au chapitre 3. Les étapes des grafcets correspondent donc aux opérations associées au processus de conception. Les transitions peuvent quant à elles, être mises en correspondance avec les événements qui régissent le passage d'un état à un autre au niveau du modèle dynamique d'OMT.

2.1. Niveau Représentation du besoin

2.1.1. Scénario d'évaluation au niveau Représentation du besoin

Ce niveau de représentation vise à traduire les besoins et les exigences du client sous la forme de fonctions de service et de fonctions contraintes globales en intégrant l'aspect sûreté de fonctionnement. Pour notre part, nous nous intéressons simplement aux fonctions contraintes globales exprimant les exigences du client en matière de sûreté de fonctionnement du produit.

Le scénario associé à ce niveau de représentation peut être décrit par le grafcet de la figure 2 .

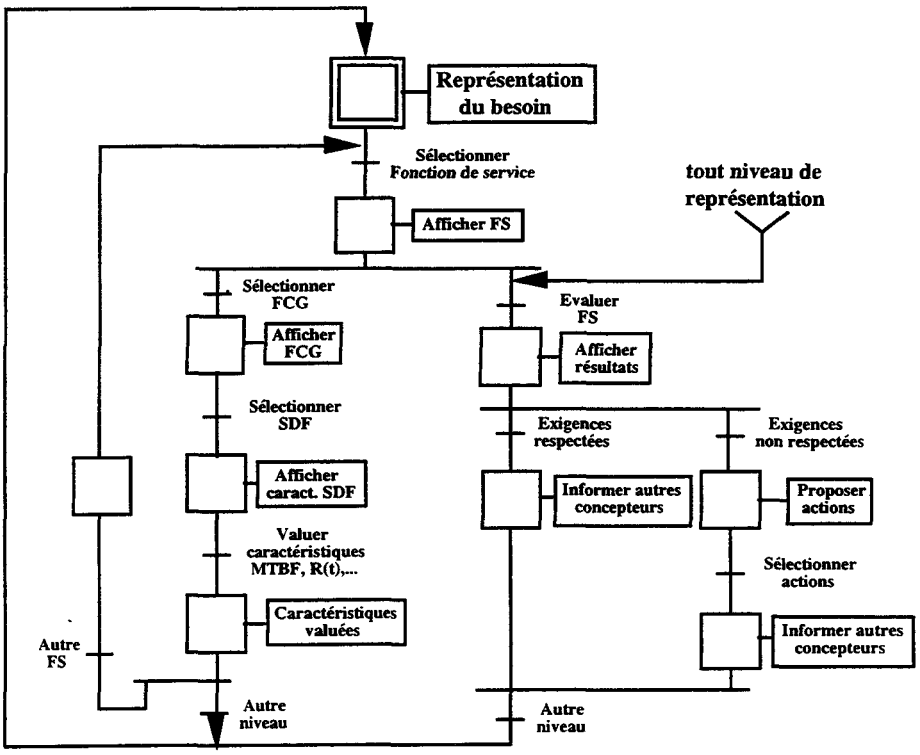

Figure 2 : Scénario d'évaluation associé au niveau Représentation du besoin

A partir d'une liste regroupant l'ensemble des fonctions de service (défini par l'ingénieriste) que le produit doit satisfaire (figure 3), le concepteur en charge de la sûreté de fonctionnement sélectionne celle(s) qu'il veut (ou qu'il doit) caractériser d'un point de vue sûreté de fonctionnement.

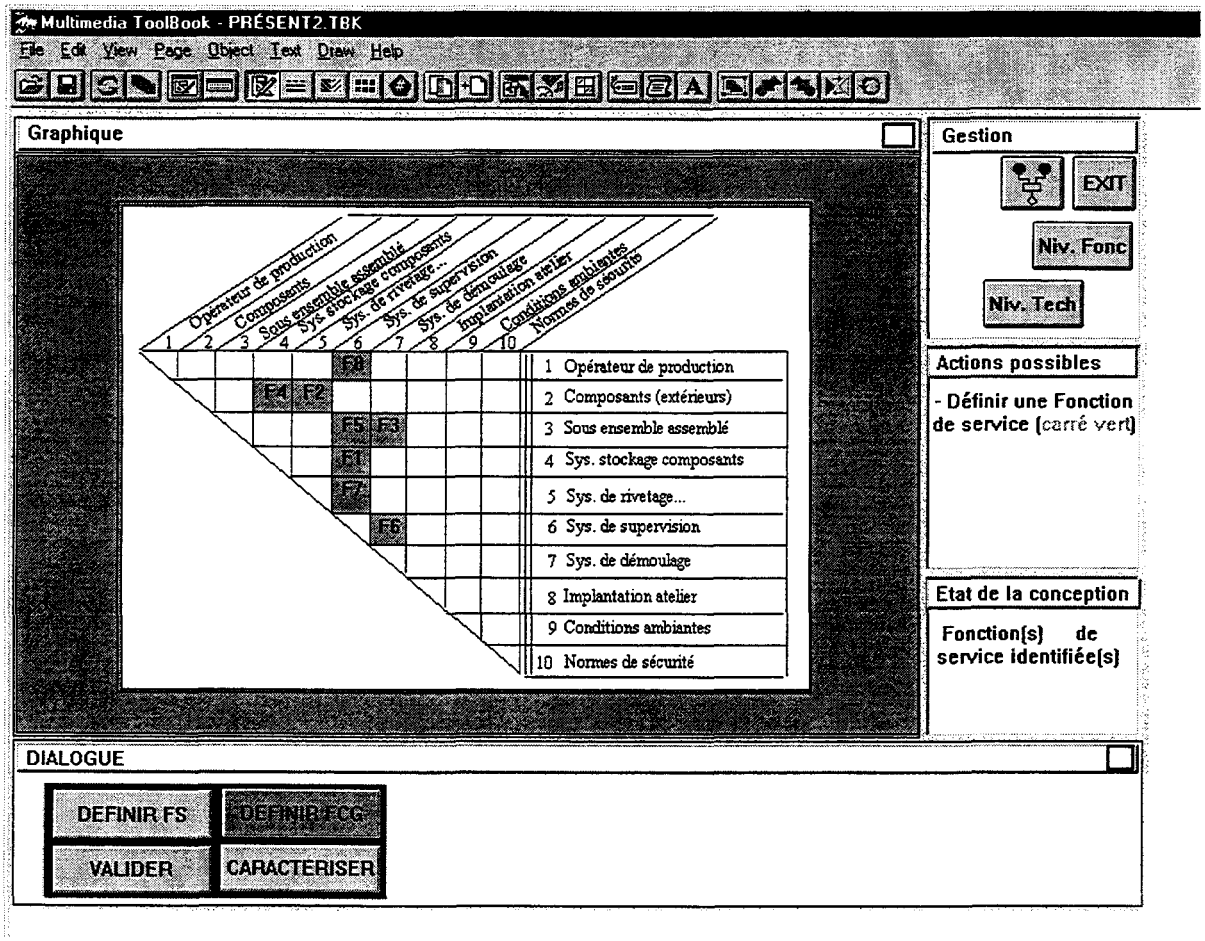

Figure 3 : Fonctions de service à satisfaire

Le concepteur peut, à partir de là, effectuer deux types d'actions à ce niveau de représentation :

Le premier consiste à indiquer, pour chaque ou seulement certaines fonctions de service, les caractéristiques de sûreté que celle(s)-ci doit(vent) respecter. Cela consiste donc à saisir ou renseigner les champs relatifs à la fiabilité, à la maintenabilité, à la disponibilité et à la sécurité. Toutes ces caractéristiques ont pu être données par le client dans le cahier des charges. Le concepteur renseigne alors les différents champs qui lui sont proposés (figure 4). Ainsi, les caractéristiques de fiabilité R(t), de disponibilité A(t), les temps moyens de bon fonctionnement entre défaillances MTBF ou les temps moyens de réparation MTTR attendus pourront être entrés au clavier au sein du système informatique. Les valeurs entrées constitueront les contraintes à respecter et par conséquent les références sur lesquelles s'appuieront les évaluations faites aux autres niveaux de représentation du modèle de produit.

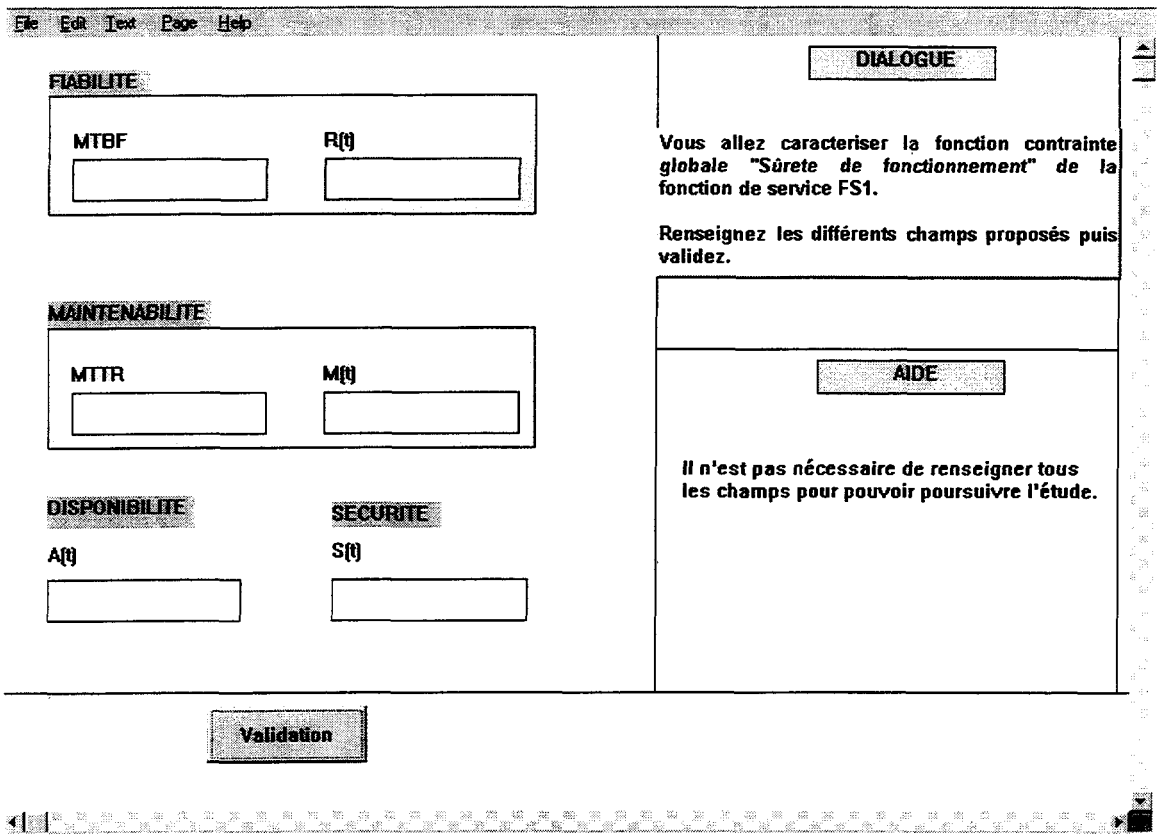

Figure 4 : Caractéristiques de sûreté de fonctionnement à renseigner

Le second vise à évaluer la fonction de service du point de vue de la sûreté de fonctionnement. Cette évaluation ne peut se faire qu'après la définition complète du produit c'est-à-dire dès que les niveaux technique et détaillé ont été spécifiés. Cette évaluation se fera à l'aide de modèles utilisés aux autres niveaux de représentation (les relations mathématiques de définition de la fiabilité prévisionnelle d'un système par exemple).

Seul ce type d'évaluation peut être effectué à ce niveau de représentation. Il constitue la valeur ajoutée de l'ingénieur sûreté de fonctionnement à ce qui a été spécifié par l'ingénieriste. Nous présentons, dans le paragraphe suivant, les propositions que ce dernier a fait pour ce niveau.

2.1.2. Propositions de l'ingénieriste

Les propositions faites par l'ingénieriste ont pour objectif de spécifier et de valider le besoin du client ainsi que de le décrire en termes de fonctions à remplir et de contraintes à respecter indépendamment des aspects sûreté de fonctionnement. L'étude de ce banc /DSPT8 97/ a abouti, à partir de la matrice présentée sur la figure 3, à la définition des fonctions de service et des fonctions contraintes globales suivantes :

FS1 : réaliser le dialogue entre l'opérateur de production et le système de gestion

FS2 : renseigner le système de supervision sur l'état du système de stockage des composants

FS3 : assembler des composants avec le système de rivetage

FS4 : permettre au système de démoulage d'extraire le sous-ensemble assemblé

FS5 : pré-positionner pour l'assemblage un composant stocké dans le stock composant

FS6 : renseigner le système de gestion de production sur le nombre de sous-ensembles assemblés réalisés

FS7 : renseigner le système de supervision de l'état du système de démoulage

FS8 : donner au système de gestion l'état du stock composant

FS9 : renseigner le système de supervision sur l'état du système de rivetage

FS10 : réaliser le dialogue entre l'opérateur de production et le système de supervision

En ce qui concerne les fonctions contraintes globales, celles qui ont été retenues sont :

FCG1 : le système doit respecter les normes de sécurité humaine

FCG2 : le système doit respecter les normes de sécurité matérielle

Ces deux fonctions contraintes globales sont les seules qui ont été identifiées à l'issue du projet. Elles sont relatives à la sécurité puisque l'opérateur est conservé pour la réalisation de certaines des opérations. Dans le cadre de nos travaux, nous avons ajouté des contraintes sur la fiabilité du système automatisé ainsi que sur sa disponibilité afin de pouvoir valider nos propositions (voir paragraphe 1.2.).

Dans le cadre du DSPT8, seule la fonction de service FS3 a été étudiée par la suite. Nous donnons les éléments de sa décomposition (les différentes fonctions opératoires) dans le paragraphe suivant.

2.2. Niveau Représentation des exigences fonctionnelles

2.2.2. Scénario d'évaluation au niveau Représentation des exigences fonctionnelles

La chaîne opératoire définie à l'issue de l'analyse fonctionnelle effectuée par l'ingénieriste est le point d'entrée de l'étude menée par l'ingénieur sûreté de fonctionnement au niveau représentation des exigences fonctionnelles (figure 5). Il va analyser le produit à concevoir en recherchant les éléments susceptibles d'apparaître lors de sa future exploitation et qui peuvent nuire à son bon fonctionnement (fonctionnement nominal).

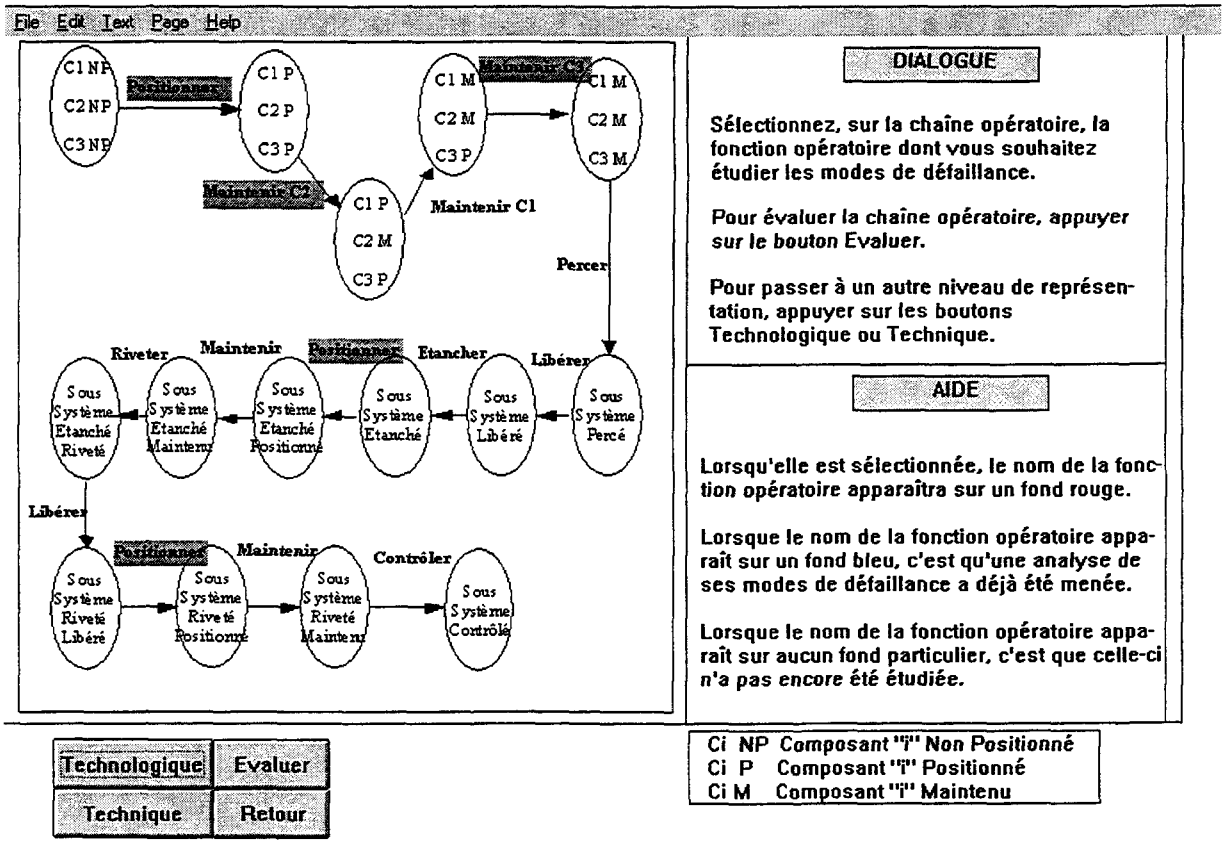

Figure 5 : Chaîne opératoire initiale (avant évaluation)

Le grafcet présenté figure 6 décrit le scénario associé à ce niveau de représentation. Il distingue deux points importants dans le cadre de l'évaluation de la sûreté de fonctionnement du produit.

Le premier point concerne l'évaluation de la chaîne opératoire définie par l'analyse fonctionnelle. Cette évaluation globale consiste à vérifier que l'ensemble de la chaîne opératoire respecte les exigences demandées par le client. Cela se fait à partir des données de fiabilité relatives à chacune des fonctions opératoires qui la composent. Pour cela, les relations mathématiques présentées au paragraphe 3.3.2. du chapitre 1 relatives à la détermination de la fiabilité prévisionnelle d'un système sont activées. Les résultats de cette évaluation donnent les fonctions opératoires sur lesquelles un risque potentiel existe.

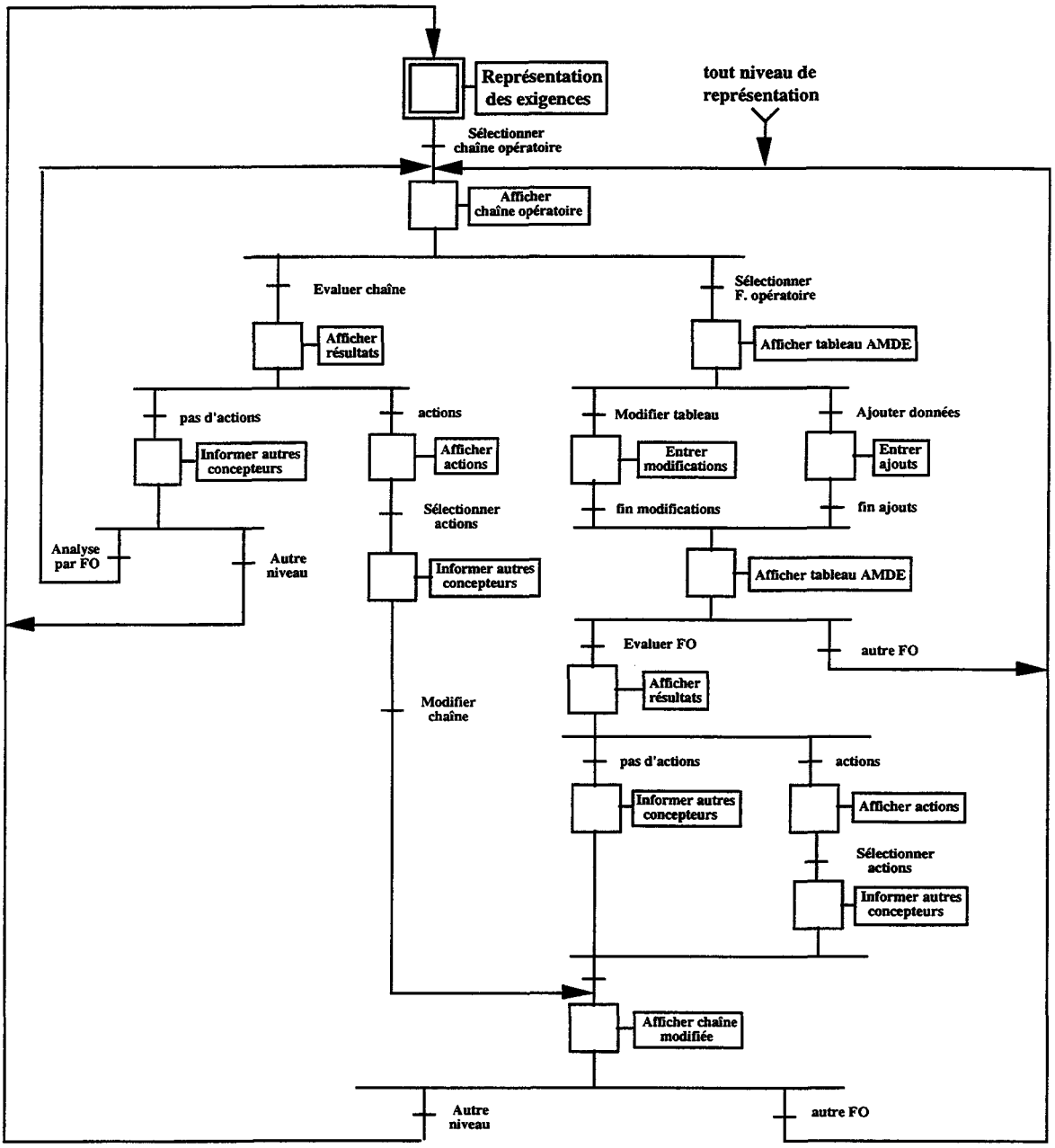

Figure 6 : Scénario d'évaluation associé au niveau Représentation des exigences fonctionnelles

Ainsi, à partir de la chaîne opératoire présentée figure 5 (décrite par un graphe d'états), le concepteur peut, par exemple, vouloir évaluer la fiabilité de la première partie de la chaîne (fonctions opératoires Positionner, Maintenir C1, Maintenir C2, Maintenir C3).

Pour effectuer ce calcul, il a besoin d'informations sur chacune de ces fonctions. Pour cela, deux alternatives s'offrent à lui : soit il doit passer par le niveau technique afin de définir les composants à associer aux fonctions opératoires (nous disposons ainsi d'informations sur la fiabilité, les taux de défaillance, ..., des éléments pour effectuer ces calculs à un niveau fonctionnel) ; soit il attribue à chacune des fonctions opératoires une valeur *a priori* pour effectuer cette évaluation, valeur qui sera ensuite propagée aux niveaux de représentation inférieurs (si cette valeur est jugée acceptable).

Par exemple, il peut attribuer les valeurs suivantes à chacune des fonctions :

Fiabilité de Positionner = 0.98
Fiabilité de Maintenir C1 = 0.97
Fiabilité de Maintenir C2 = 0.98
Fiabilité de Maintenir C3 = 0.95

Les fonctions étant toutes en série, on utilise donc la première l'équation adéquate et on aboutit au résultat suivant :

Fiabilité de la chaîne = 0.98 x 0.97 x 0.98 x 0.95 = 0.88

Si l'on se reporte aux exigences exprimées par le client (0.65), on constate que la fiabilité de chacune des fonctions opératoires permet de respecter la fiabilité désirée. Si tel n'avait pas été le cas, des actions correctives auraient du être proposées. Elles auraient consisté en la mise en redondance de la fonction la moins fiable ou en la préconisation d'opérations de maintenance préventive sur ses éléments les plus critiques.

Les valeurs associées aux fonctions opératoires peuvent donc constituer des références pour la spécification des éléments aux niveaux inférieurs.

Le second point du scénario porte sur la spécification des éventuelles défaillances de chaque fonction opératoire, de leurs causes et de leurs effets. Elle est sous cet angle uniquement qualitative et vise à rechercher les différents modes de défaillance fonctionnelle susceptibles d'apparaître lors de la future exploitation du produit (figure 7).

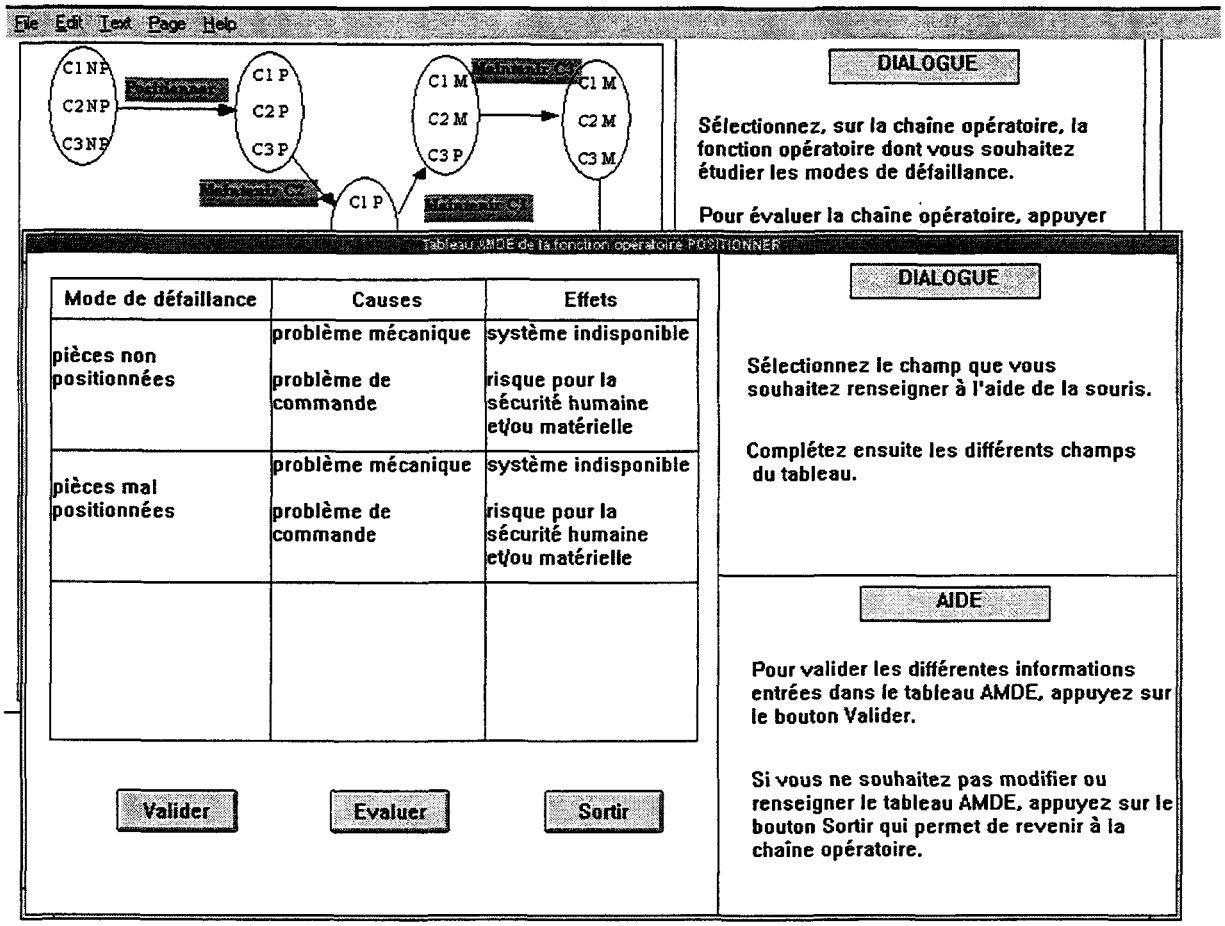

Figure 7 : Exemple de tableau AMDE pour la fonction opératoire Positionner

Le concepteur peut modifier ce tableau s'il contient déjà des informations, sinon le renseigner en fonction de l'analyse *a priori* qu'il aura pu mener. Il se posera pour cela les questions qui ont été présentées au paragraphe 3.2.1. du chapitre 3 (de quelle façon cette fonction peut-elle ne plus être assurée, quels sont les effets de cette défaillance, ...).

Suite à la définition de ces différents modes de défaillance, une évaluation quantitative de chacun d'eux peut être entreprise. Par la recherche de leur fréquence d'apparition ainsi que de leur gravité (estimées par exemple à partir d'une base de données d'historiques disponible sur des fonctions analogues), la criticité de ces modes peut être établie et par conséquent, une hiérarchie de ces modes peut être réalisée, mettant en avant celle(s) susceptible(s) de présenter un risque pour le matériel, pour les utilisateurs ou pour l'environnement. La figure 8 montre les résultats d'une évaluation individuelle de la fonction opératoire *Positionner*.

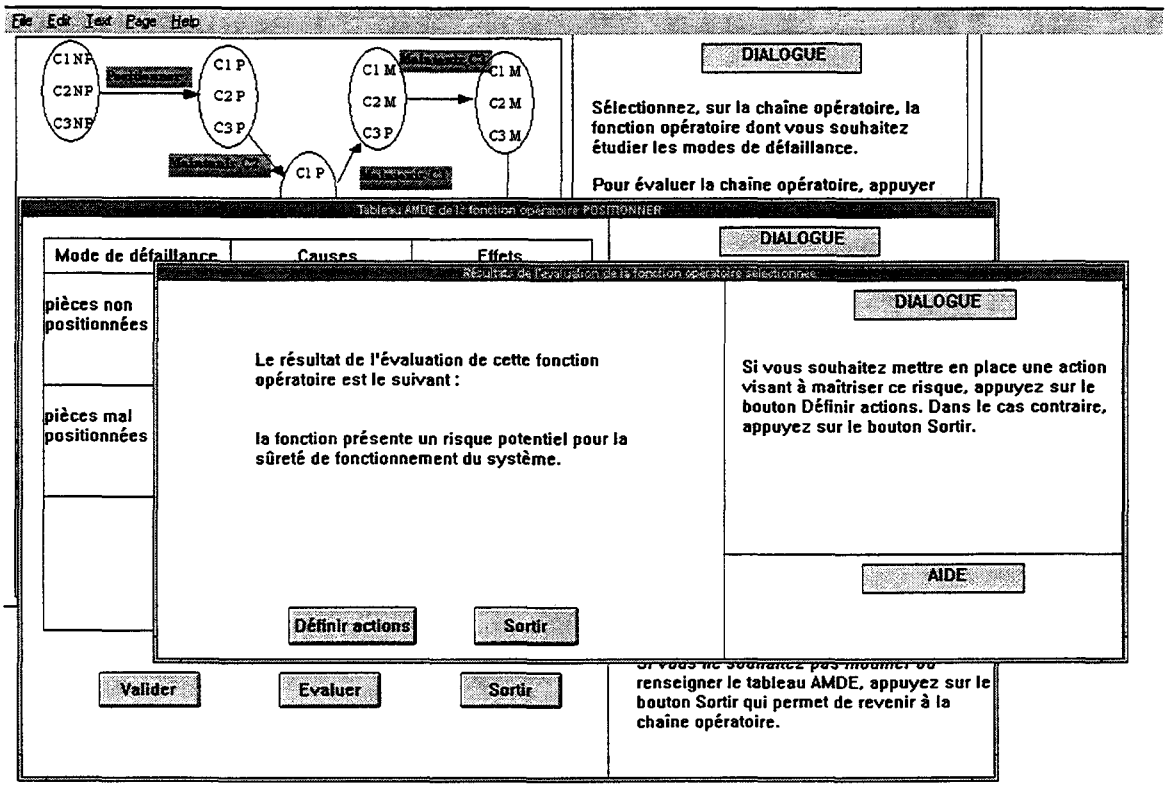

Figure 8 : Résultats d'évaluation de la fonction opératoire Positionner

Des actions correctives peuvent alors être proposées au concepteur afin de faire disparaître ou, tout au moins, réduire ce risque (figure 9).

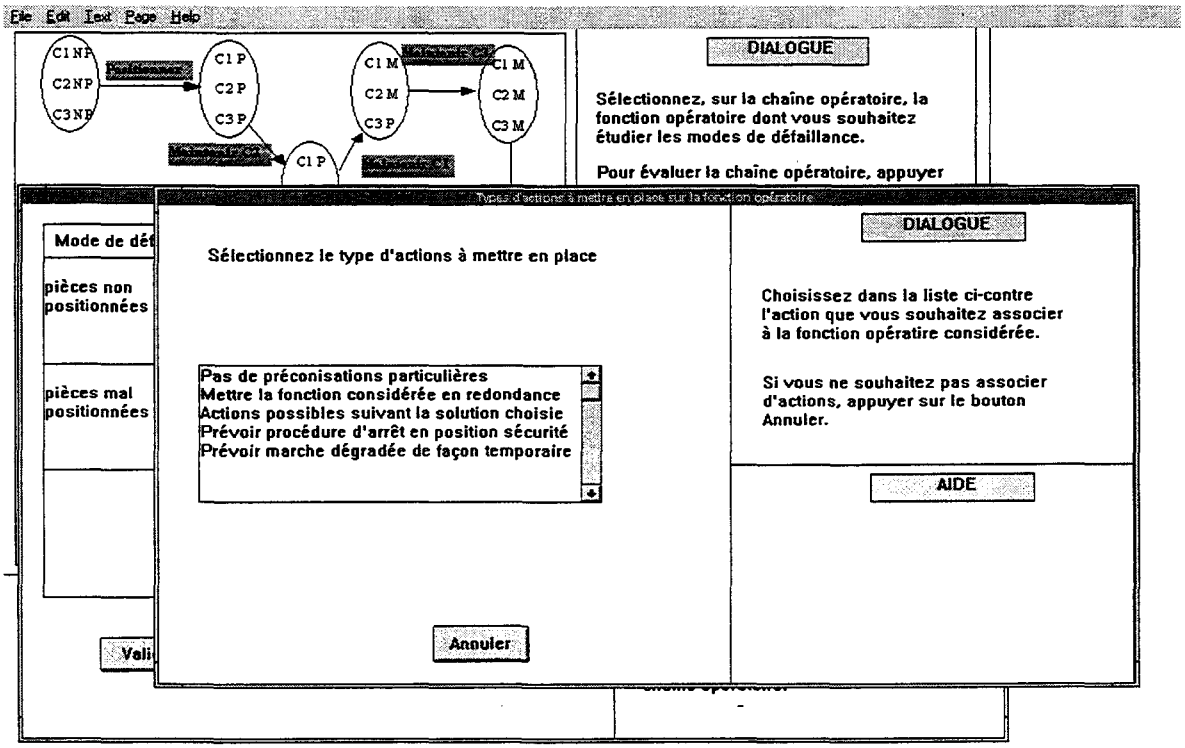

Figure 9 : Types d'actions correctives

Cela peut être un changement de composant (technologique ou technique), la mise en redondance de la fonction opératoire voire de la fonction de service, la mise en œuvre de moyens de surveillance, la préconisation de procédures de maintenance préventive, ... Le choix d'une action vis-à-vis d'une autre sera fonction du coût, des moyens utilisés, de l'encombrement, des contraintes imposées par le client ou par les autres concepteurs (mécaniciens, automaticiens, ...). En fonction des exigences à respecter (sécurité humaine, matérielle mais également fiabilité et disponibilité) et des résultats de l'analyse AMDE précédente (notamment le niveau de gravité des modes), l'ingénieur sûreté de fonctionnement va alors entreprendre de mettre en œuvre des actions visant à contrer l'apparition de ces modes de défaillance. A ce niveau de représentation, ces actions consistent essentiellement à des mises en garde pour les autres concepteurs et à des mises en redondance des fonctions opératoires jugées à risque.

La figure 10 montre, à partir de la chaîne opératoire modifiée, les modifications qui ont été apportées à la chaîne opératoire nominale suite à son évaluation et à l'intégration des actions correctives que le concepteur a choisi de mettre en place. Ainsi, on peut voir que la fonction *Positionner* devra être mise en redondance (ajout d'une flèche plus épaisse sur la chaîne) si l'on veut respecter les exigences du client en matière de sécurité. D'autres actions pourront être proposées aux niveaux inférieurs en fonction des choix technologiques et techniques qui seront faits.

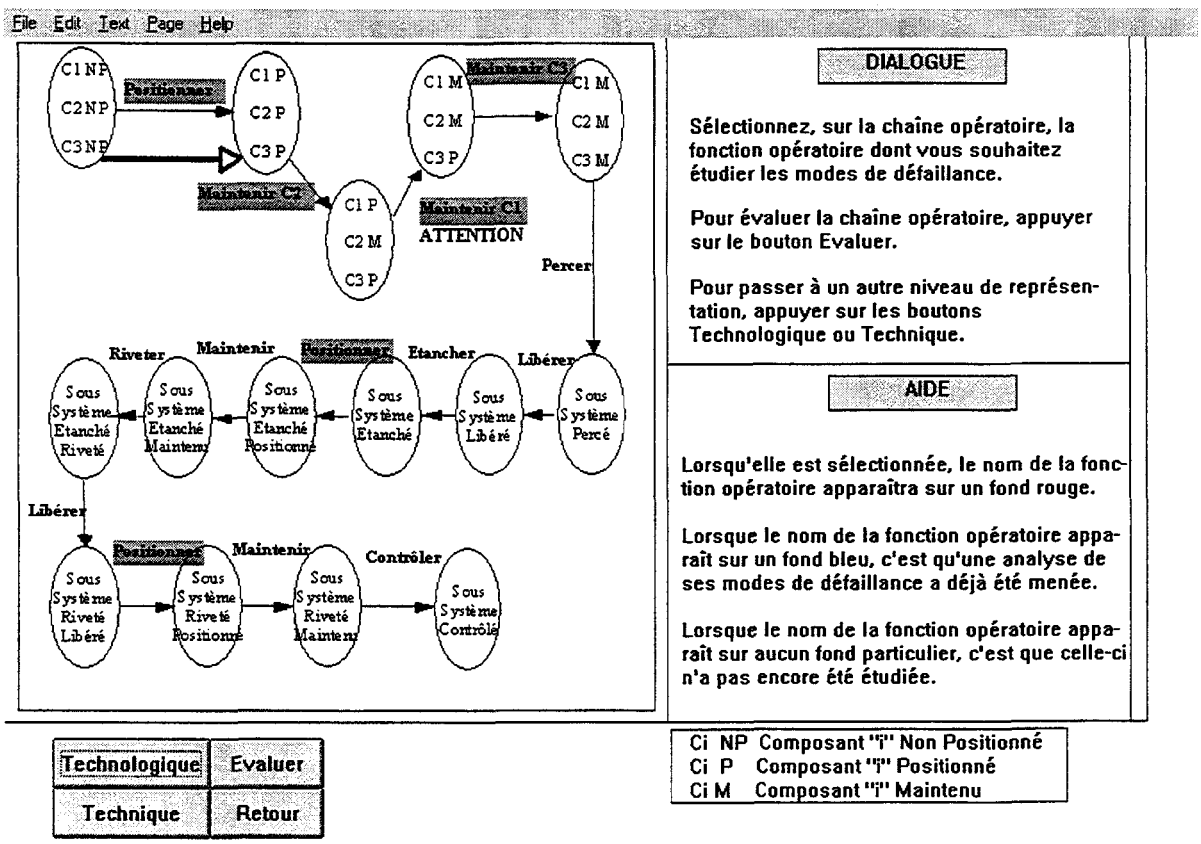

Figure 10 : Chaîne opératoire modifiée (après évaluation)

La décision de mettre en redondance certaines fonctions opératoires va entraîner alors la définition, au niveau technologique, de fonctions de base exploitation visant à détecter l'apparition d'un état anormal et de lancer alors la procédure la plus adaptée à la situation

(secours, arrêt pour maintenance, ...). Les évaluations menées par l'ingénieur sûreté de fonctionnement ont pour but de rechercher, parmi les fonctions opératoires constituant la chaîne opératoire, celles susceptibles de présenter un risque lors de l'exploitation future du produit. Nous allons, dans le paragraphe suivant, décrire succinctement comment sont obtenues les fonctions opératoires à partir des fonctions de service.

2.2.2. Propositions fonctionnelles

Après plusieurs itérations /JACQUET 98/, les chaînes de fonctions opératoires associées aux différentes fonctions de service sont obtenues. L'étude de la fonction de service FS3 dans le cadre de ce projet, a abouti pour ce niveau de représentation, à la définition de la chaîne opératoire présentée sur la figure 11 ci-après. Elle correspond à la décomposition de la fonction *Assembler* les composants 1,2 et 3 de la phase 1 de la gamme d'assemblage.

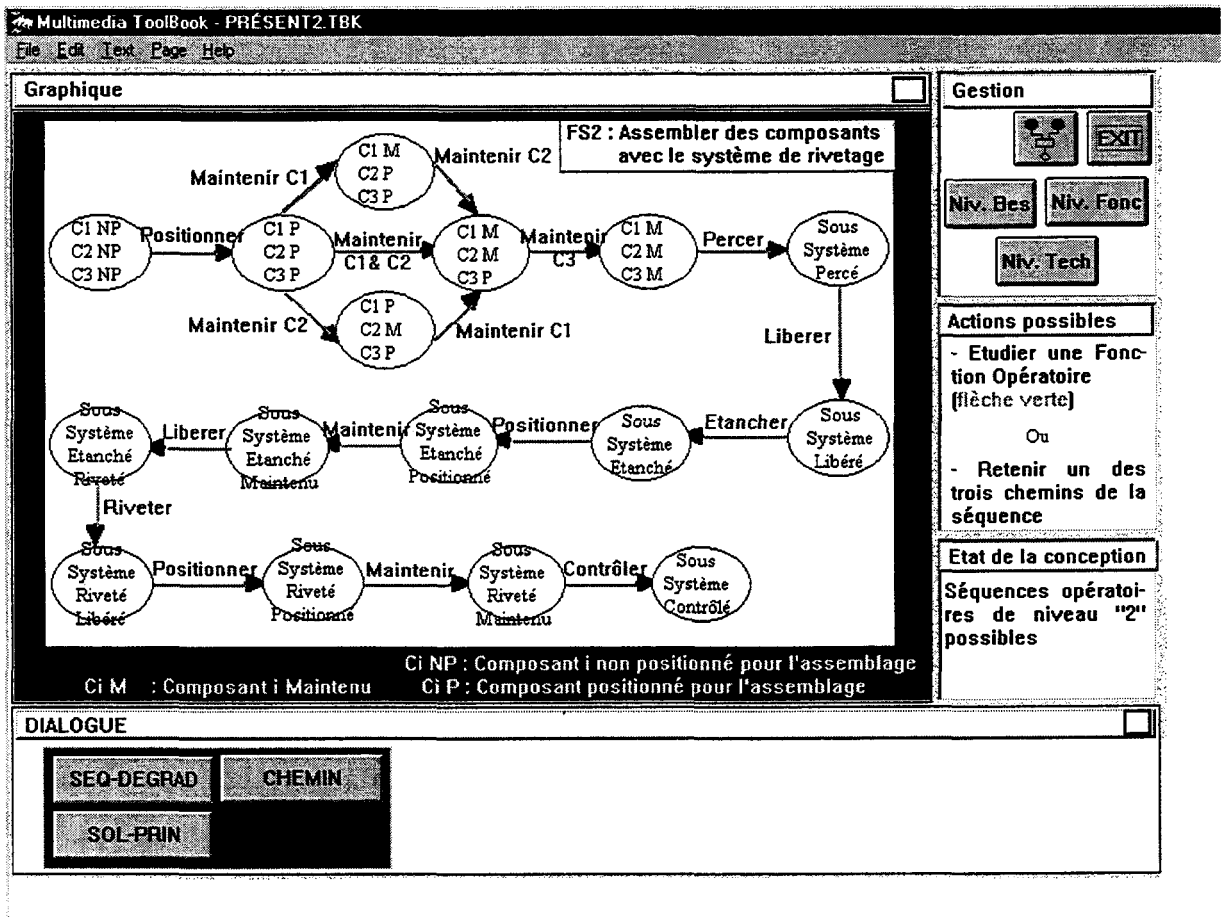

Figure 11 : Chaîne opératoire issue de la décomposition de la fonction Assembler

La définition de cette chaîne opératoire, associée à la détermination des différents principes opératoires susceptibles de supporter chacune des fonctions opératoires qui la composent, permet aux concepteurs de déterminer la solution technologique apte à répondre au problème posé par le client.

2.3. Niveau Représentation technologique

2.3.1. Scénario d'évaluation au niveau Représentation technologique

Dans le cadre du projet DSPT8, l'objectif de ce niveau technologique va être d'ajouter des fonctions de base exploitation à l'architecture de commande pour les différentes fonctions de base à risque. Ainsi, plusieurs fonctions de base *Acquérir les informations* vont par exemple être nécessaires pour capter les informations sur différentes fonctions opératoires de la chaîne (Maintenir C1, Maintenir C2 et Maintenir C3). Par contre, les fonctions de base *Détecter*, *Localiser*, *Diagnostiquer*, ..., pourront n'apparaître qu'une seule fois et être toutes regroupées à un niveau supervision. Ces fonctions de base seront alors supportées par un seul et même composant pouvant être un ordinateur ou un automate, selon la solution que l'automaticien aura adoptée pour répondre à son problème (à la condition que celle-ci convienne au concepteur en charge de la sûreté de fonctionnement).

Le point d'entrée de l'étude menée par l'ingénieur sûreté de fonctionnement au niveau représentation technologique est la solution technologique de l'automaticien proposée à partir de la solution du mécanicien. La solution de l'automaticien décrit l'architecture de commande du produit (figure 12) définie à partir de la chaîne cinématique élaborée par le mécanicien. La chaîne cinématique a été élaborée à partir de la chaîne opératoire décrite au niveau représentation des exigences fonctionnelles du besoin.

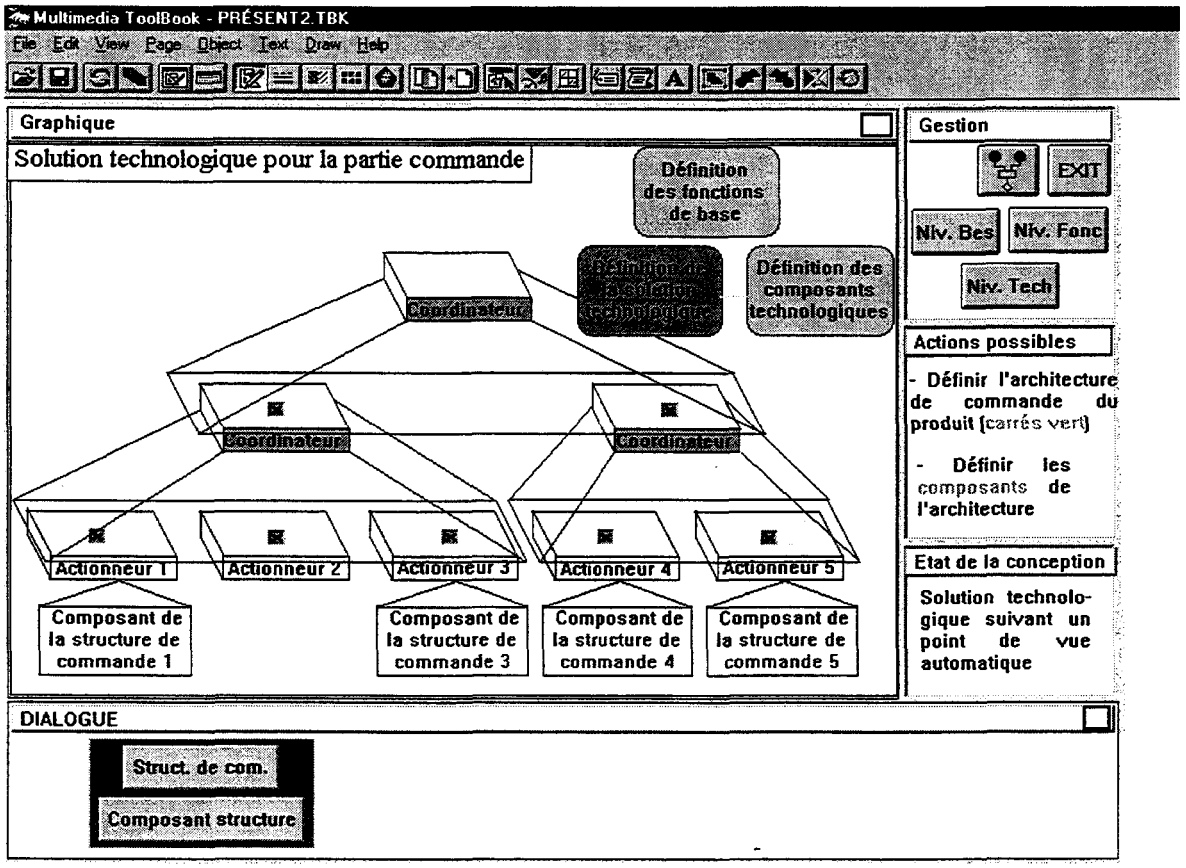

Figure 12 : Solution technologique de l'automaticien

Les informations nécessaires au concepteur en charge de l'évaluation de la sûreté de fonctionnement à ce niveau de représentation sont les solutions technologiques des autres intervenants et les informations issues du niveau précédent (les actions correctives à mettre en place, les redondances notamment). Cependant, comme le montre le scénario de conception associé à ce niveau de représentation qui est décrit par le grafcet de la figure 13, deux alternatives s'offrent au concepteur en charge de l'évaluation de la sûreté de fonctionnement du produit.

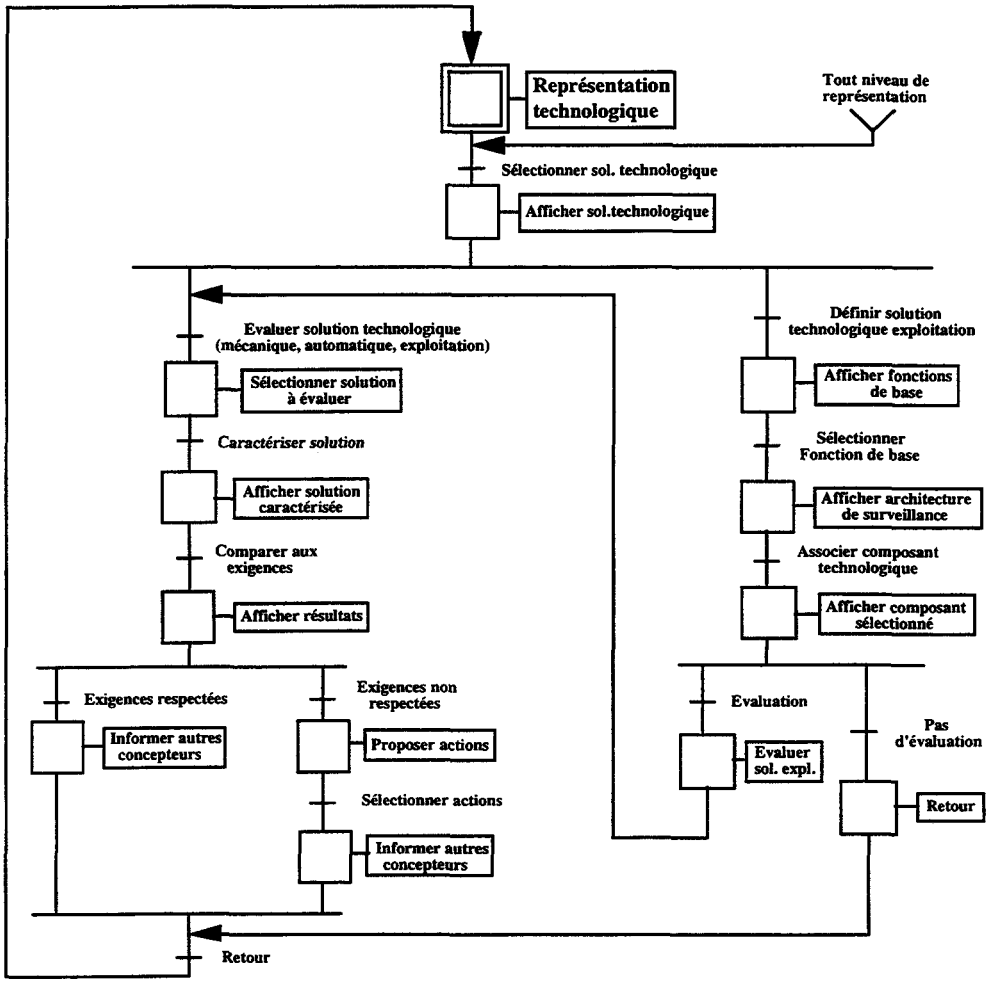

Figure 13 : Scénario d'évaluation associé au niveau Représentation technologique

La première alternative consiste à évaluer les différentes solutions technologiques (figure 14) proposées par les autres concepteurs (mécaniciens, automaticiens, ...). Cette évaluation consistera à comparer les grandeurs calculées (fiabilité, MTBF,...) aux valeurs de référence entrées au niveau représentation du besoin. Les modèles utilisés pour cette évaluation peuvent être les relations mathématiques utilisées pour déterminer la fiabilité prévisionnelle d'un système. Il est nécessaire pour cela de passer auparavant par les niveaux de représentation technique ou détaillée afin de disposer d'informations précises sur les fiabilités, taux de défaillance, ... des différents composants. Ces informations auront été déterminées à partir d'une banque de données de fiabilité ou d'un retour d'expérience.

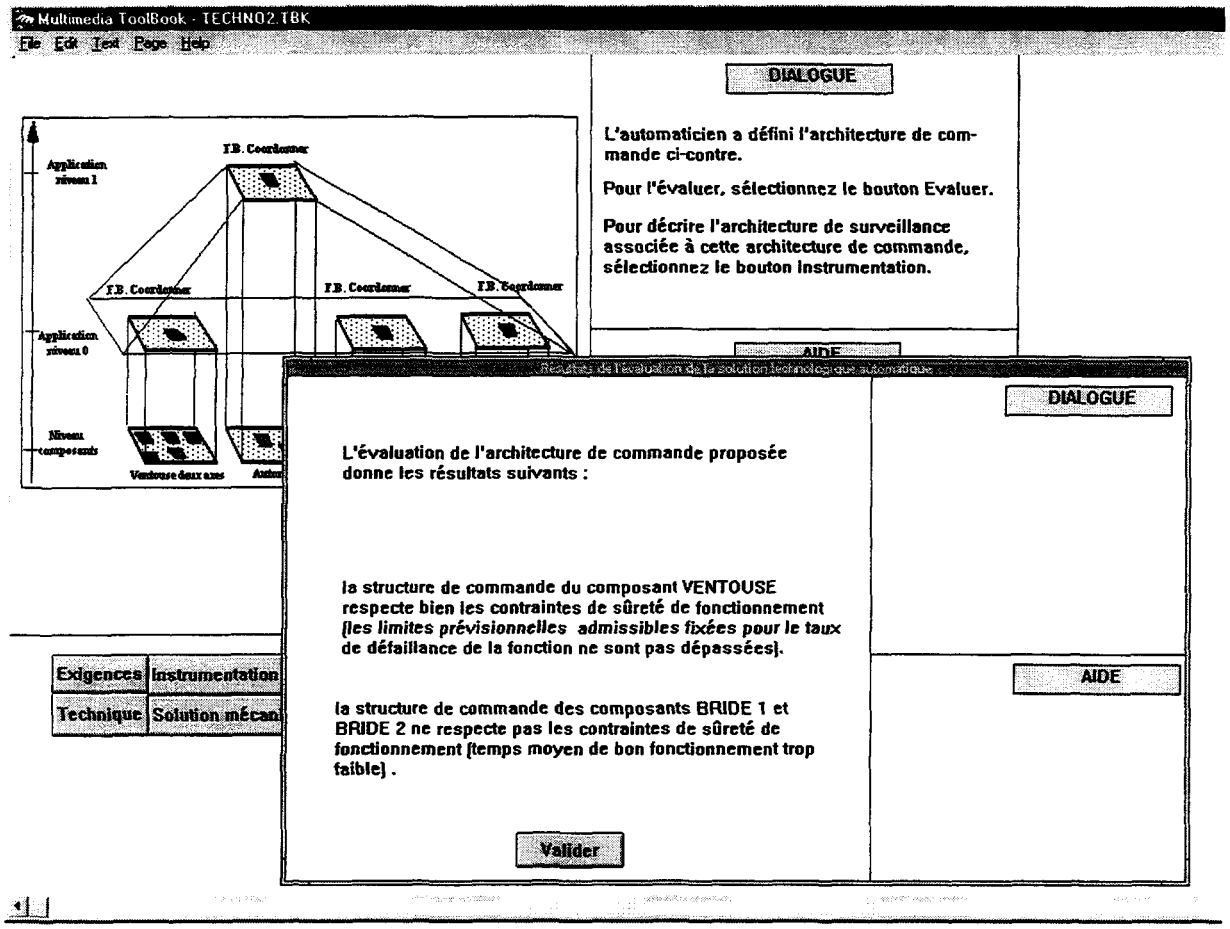

Figure 14 : Résultats d'évaluation de la solution technologique automatique

Cependant, le concepteur peut, s'il le souhaite, faire des estimations sur la fiabilité des composants pour effectuer ces calculs, estimations qu'il affinera aux niveaux de représentation inférieurs (comme pour l'évaluation de la chaîne opératoire). Si les exigences de sûreté ne sont pas respectées, des actions pourront alors être proposées (redondance, maintenance, autres solutions technologiques, ...).

Les modèles d'évaluation peuvent également être spécifiques à un métier considéré. Ce sont par exemple le modèle de comportement cinématique, le modèle de comportement des éléments standards, le modèle de comportement statique pour le mécanicien (figure 15), les graphes d'états, ... pour l'automaticien.

La seconde alternative vise à spécifier les moyens de surveillance et de diagnostic à intégrer au produit par l'ajout de fonctions de base Exploitation (maintenance) à l'architecture de commande définie par l'automaticien et à la structure mécanique élaborée par le mécanicien. Suite à l'étude menée au niveau précédent (recherche des modes de défaillance et définition des modes de marche), nous associons à la (aux) fonction(s) opératoire(s) à risque des fonctions de base exploitation. Reprenant les fonctionnalités que doit avoir tout système de surveillance, ces fonctions de base visent à détecter un fonctionnement anormal de la fonction opératoire, à en déceler sa cause et à prendre l'action corrective la plus appropriée.

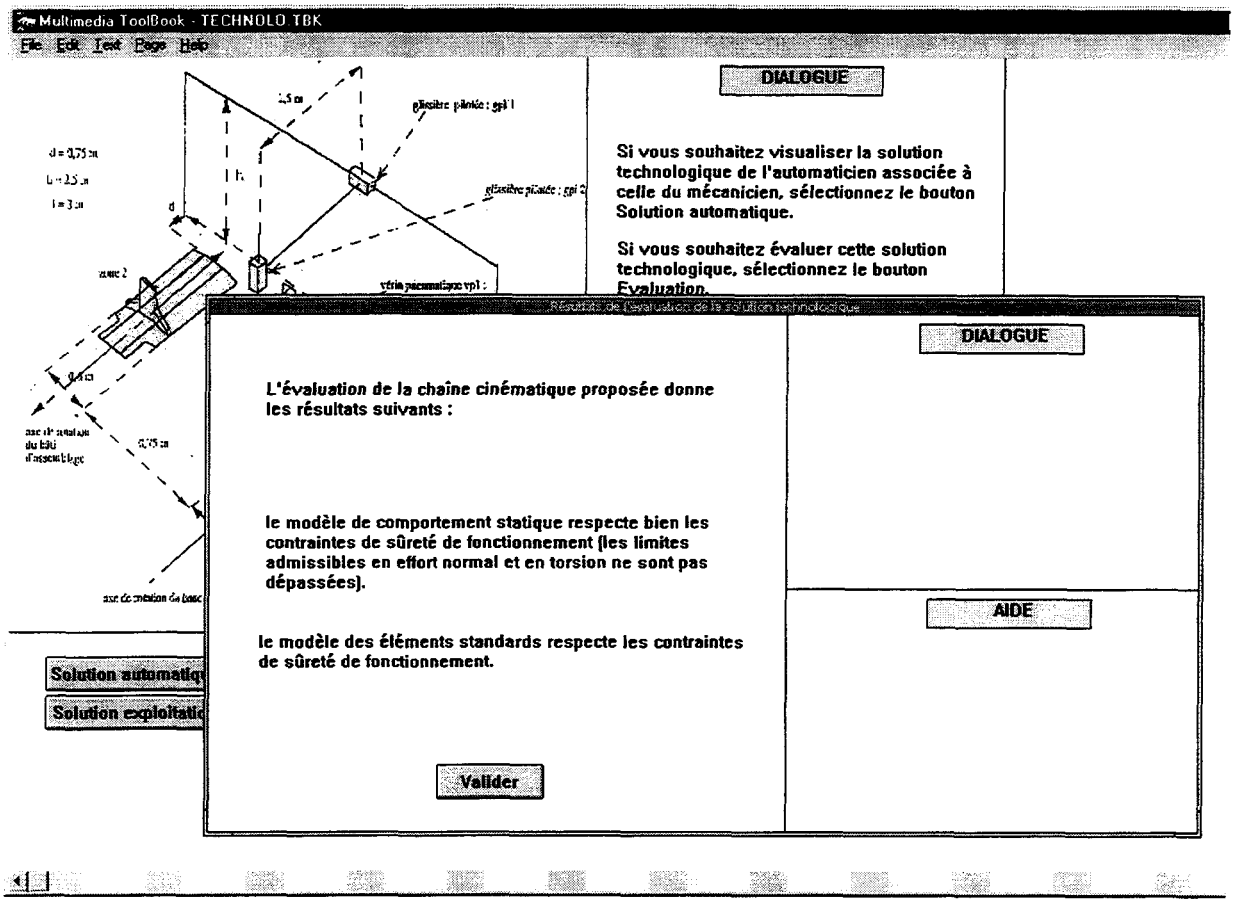

Figure 15 : Résultats de l'évaluation de la solution technologique mécanique

A partir des résultats des niveaux précédents (chaîne et fonctions opératoires, analyse AMDE, actions correctives), le concepteur pour l'exploitation va venir ajouter sa solution technologique à celle de l'automaticien. Elle correspond, lorsque l'action corrective proposée est une mise en redondance de la fonction opératoire étudiée, à l'architecture de surveillance à intégrer au produit afin de le rendre sûr de fonctionnement lors de sa future exploitation. En effet, pour déceler un fonctionnement anormal de la chaîne ou de l'une de ses fonctions opératoires, il va être nécessaire d'intégrer au produit des moyens permettant de déceler au plus tôt un comportement non nominal. La procédure adéquate pour contrer ce mode anormal pourra ensuite être enclenchée afin d'assurer la sûreté de fonctionnement du système.

Pour décrire cette architecture de surveillance, le concepteur va sélectionner les fonctions de base exploitation qu'il souhaite intégrer au produit et à quel niveau de l'architecture de commande (figure 16) il souhaite les placer.

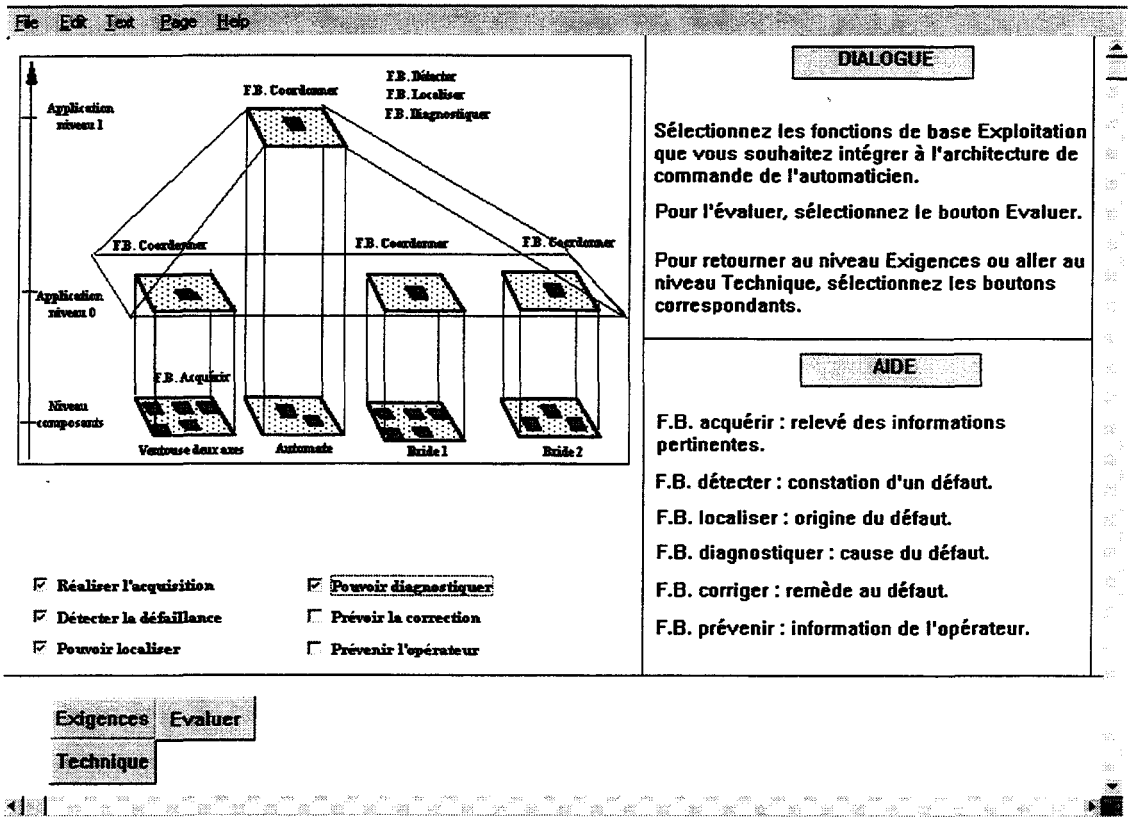

Figure 16 : Fonctions de base Exploitation associées à l'architecture de commande

Le regroupement de ces différentes fonctions de base constitue la solution technologique pour le point de vue Exploitation (figure 17). Ce regroupement est obtenu en associant à chacune des fonctions de base que le concepteur a sélectionnées un composant technologique : des capteurs pour la fonction Acquérir, un automate pour les fonctions Détecter, Localiser, Diagnostiquer, ... Cette association de composants constituent la chaîne d'instrumentation et de surveillance à intégrer au produit.

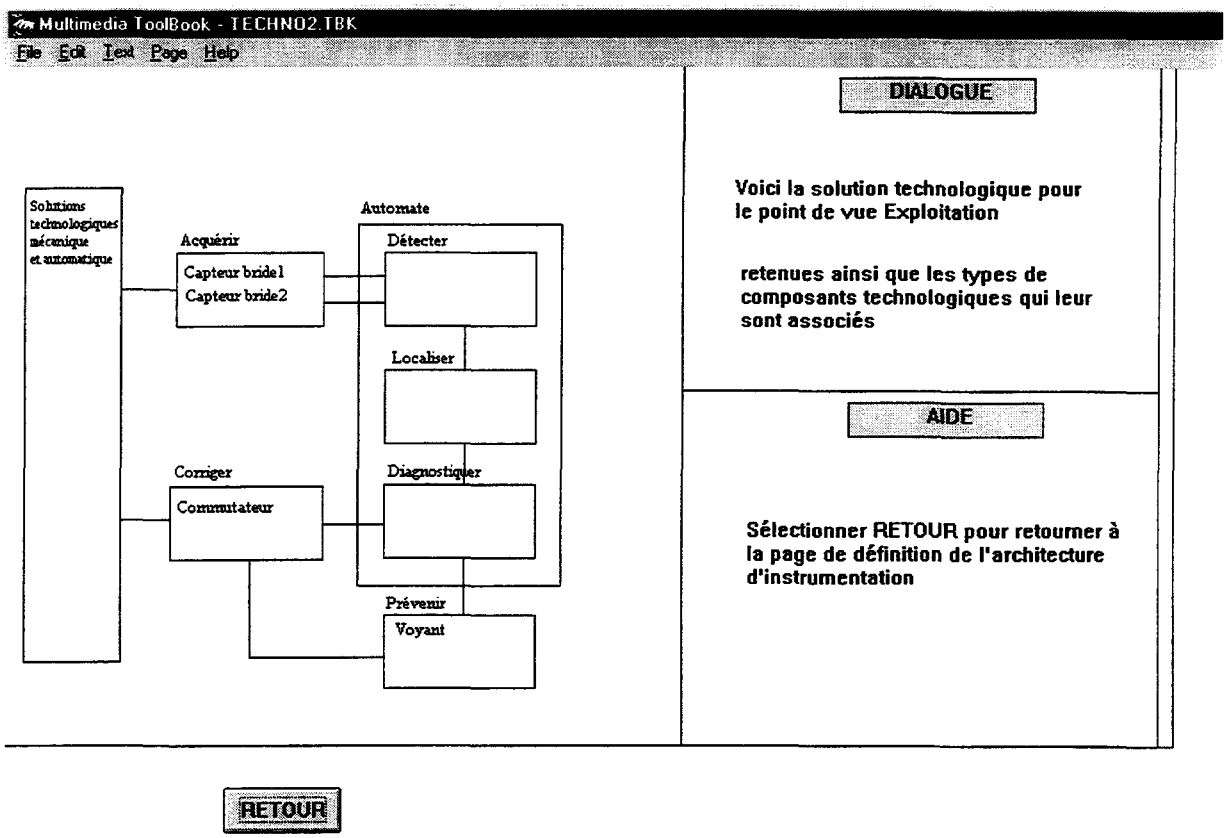

Figure 17 : Solution technologique du point de vue Exploitation

Si les actions correctives correspondent à la mise en place de maintenance préventive sur la (les) fonction(s) opératoire(s) étudiée(s), les procédures établies pourront être affinées à partir de ce niveau puisque les composants technologiques seront connus.

L'exemple du système d'assemblage, support du DSPT8, a été traité jusqu'au niveau technologique. C'est donc jusqu'à ce stade que nous avons pu intégrer des aspects sûreté de fonctionnement, n'ayant malheureusement pas d'informations concernant les niveaux de représentation inférieurs. Cependant, nous proposons tout de même les scénarios d'évaluation de la sûreté de fonctionnement pour les niveaux technique et détaillé. Ils font l'objet des paragraphes 2.4 et 2.5. Auparavant, nous présentons la solution technologique qui a été proposée à l'issue du projet DSPT8.

2.3.2. Propositions du technologue

A partir de l'étude menée au niveau de représentation précédent (définition de la chaîne opératoire), une structure générale du système d'assemblage a été proposée. A partir d'une zone 1 de stockage des six composants, ceux-ci sont transportés vers une zone 2 afin d'y être assemblés. La figure 18 ci-après présente donc la chaîne cinématique de la solution qui a été envisagée pour transporter les composants de la zone 1 à la zone 2. Seule cette solution technologique mécanique a été proposée à l'issue du projet.

Les tâches de perçage, de rivetage, d'étanchéité et de contrôle sont toujours réalisées de façon manuelle par l'opérateur. Le maintien en position des composants 1, 2 et 3 est obtenu par l'intermédiaire de ventouses ou de systèmes de brides pneumatiques.

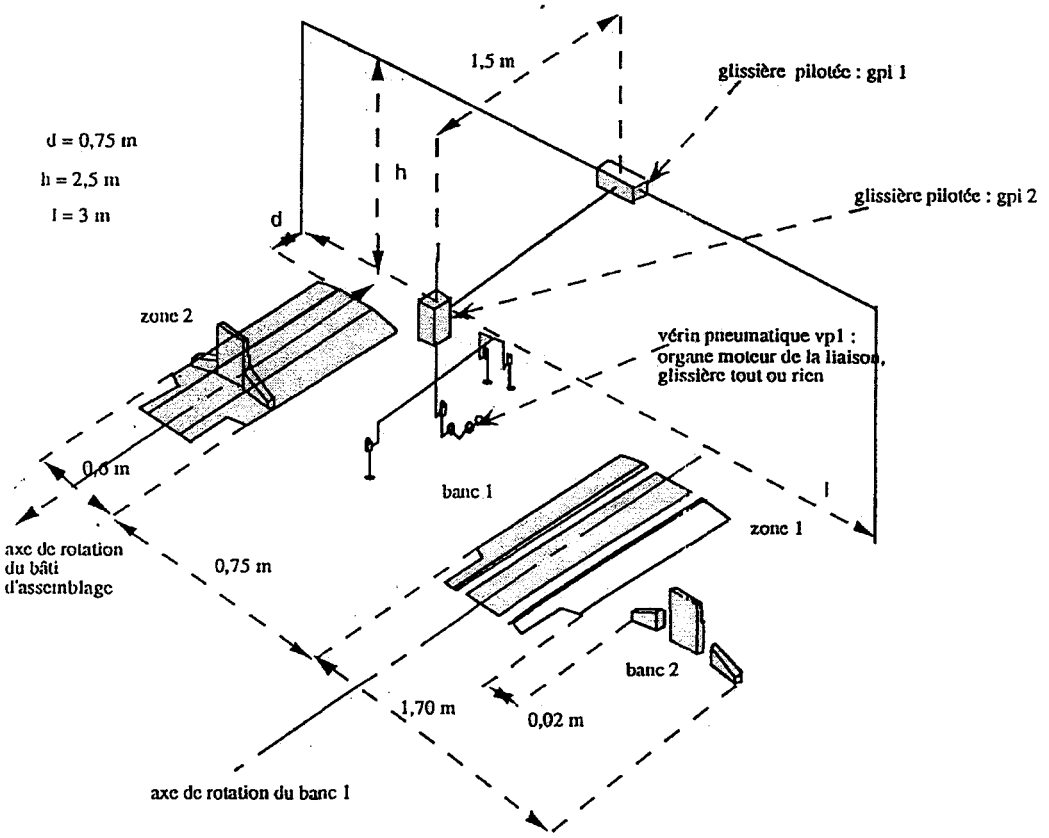

Figure 18 : Système portique de transfert des composants

Les informations concernant les paramètres à mesurer, les types de procédures à élaborer, le type d'actions à mettre en œuvre, ..., vont être obtenues au niveau représentation technique où sont spécifiés précisément les composants qui seront utilisés pour réaliser (fabriquer) le produit.

2.4. Scénario du niveau Représentation technique

A ce niveau, les différents concepteurs regroupent les fonctions de base qu'ils ont choisies pour résoudre leur problème au sein d'un ou de plusieurs ensemble(s) (ou sous-ensemble(s)), chacun spécifiant ainsi sa solution technique. Les composants techniques sélectionnés vont permettre d'affiner les choix effectués au niveau de représentation technologique (si l'on se place dans le cadre d'une conception innovante).

Le grafcet de la figure 19 décrit le scénario de conception associé à ce niveau.

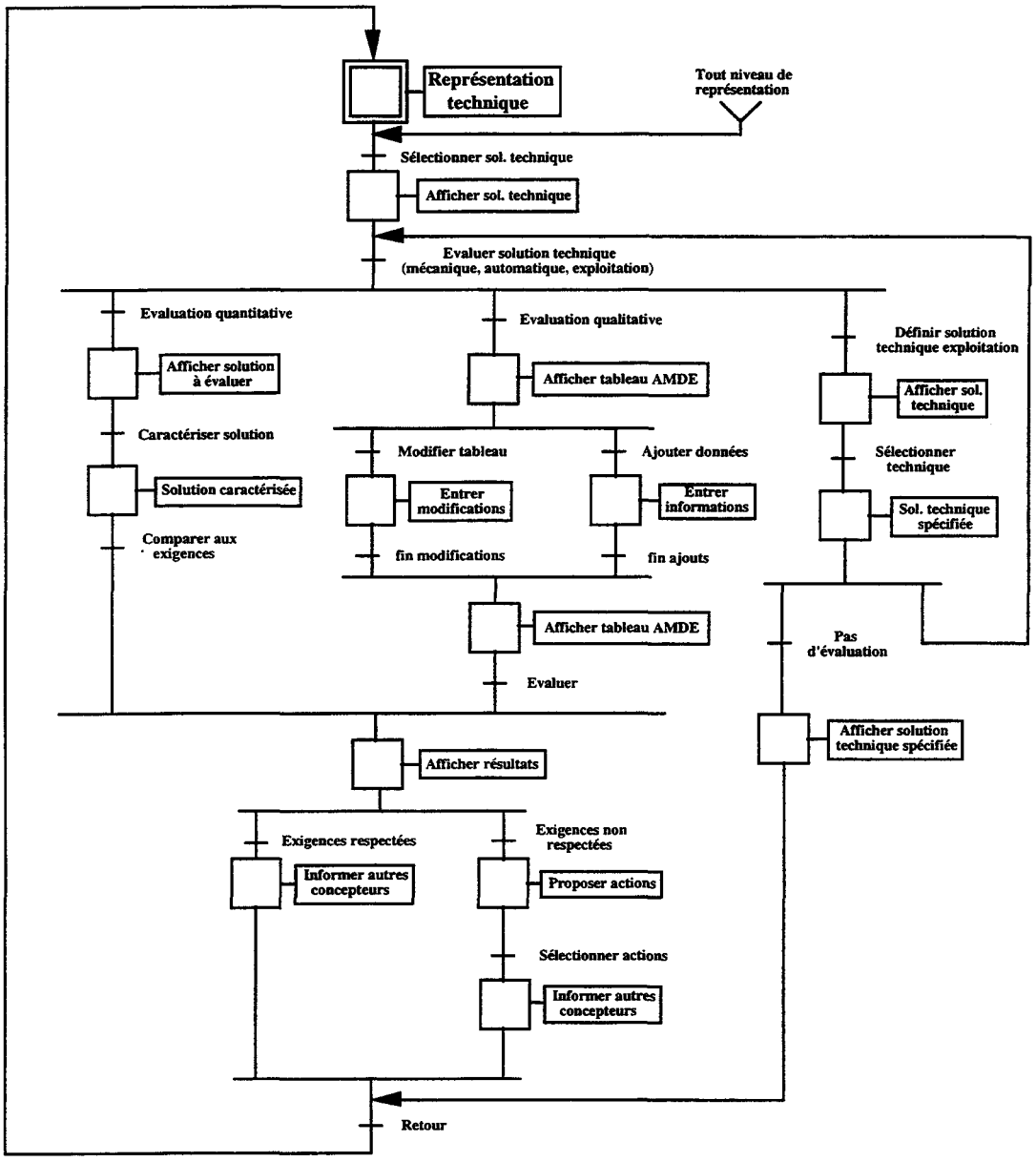

Figure 19 : Scénario d'évaluation associé au niveau représentation technique

Par exemple, pour un ensemble regroupant quatre composants techniques (quatre fonctions de base), l'évaluation de sa fiabilité va être obtenue par la connaissance de la fiabilité de chacun de ces composants et par l'utilisation des relations de détermination de la fiabilité prévisionnelle d'un système. On peut, par consultation d'une banque de données par exemple, obtenir les valeurs suivantes :

Fiabilité Composant 1 = 0.65
Fiabilité Composant 2 et Composant 3 en parallèle = 0.5
Fiabilité Composant 4 = 0.6

permettant d'obtenir le résultat suivant :

Fiabilité de l'ensemble = 0.65 x 0.5 x 0.6 = 0.195 (pour une durée de fonctionnement de l'ordre de 10000 heures par exemple).

A partir de ce résultat, une décision est à prendre : la fiabilité est-elle suffisante ou faut-il changer un des composants ? Le mettre en redondance ? Proposer des actions de maintenance préventive ? La réponse à ces questions est fortement liée au coût de chacune de ces solutions.

Dans le cadre de la reconception d'une solution existante (ou si le concepteur a une idée *a priori* de la solution pouvant répondre à son problème), la valeur calculée pour l'ensemble (ou le sous-ensemble) pourra être associée à des valeurs calculées pour d'autres ensembles (ou sous-ensembles), puis sera remontée au niveau de la fonction opératoire supportée par ces ensembles. La valeur ainsi obtenue constituera alors la caractéristique de fiabilité de la fonction opératoire.

Une évaluation qualitative de la sûreté de chacun des composants d'un ensemble (ou sous-ensemble) pourra également être réalisée. Elle consistera tout d'abord à effectuer une analyse des modes de défaillance de chacun de ces composants. Les résultats de cette analyse vont ainsi permettre de spécifier les moyens de surveillance et de diagnostic qui peuvent être intégrer au produit : soit l'analyse va permettre de préciser les composants sur lesquels les fonctions de base (choisies au niveau précédent) devront être mises en place ; soit d'autres fonctions de base vont devoir être définies et mises en place afin d'acquérir d'autres paramètres pour améliorer encore la sûreté de fonctionnement du produit. En fonction des conséquences de ces modes (liées à leur fréquence d'apparition et de leur gravité), des actions correctives seront proposées au concepteur : le choix d'un autre composant, sa mise en redondance, la mise en place de procédures de maintenance préventive, l'ajout de moyens de surveillance et de diagnostic, ...

Ce scénario distingue également une partie définition des composants techniques exploitation à associer aux différentes fonctions de base retenues au niveau représentation technologique (du point de vue exploitation uniquement). Le concepteur va ainsi spécifier plus finement les composants technologiques qu'il a retenu au niveau précédent. Il peut également sélectionner ce composant directement à partir du niveau représentation des exigences fonctionnelles si il a une idée de solution dès ce stade pour supporter une ou plusieurs fonctions opératoires.

Quand les composants techniques sont définis, nous pouvons passer au niveau représentation détaillée.

2.5. Scénario associé au niveau de Représentation détaillée

Ce dernier niveau de représentation vise à fixer définitivement les composants qui seront retenus pour supporter les différentes fonctions du produit et répondre ainsi aux besoins du client tout en respectant les contraintes qu'il aura pu imposer.

Pour cela, nous associons à ce niveau de représentation le grafcet présenté sur la figure 20 ci-après. Celui-ci décrit un scénario de conception possible.

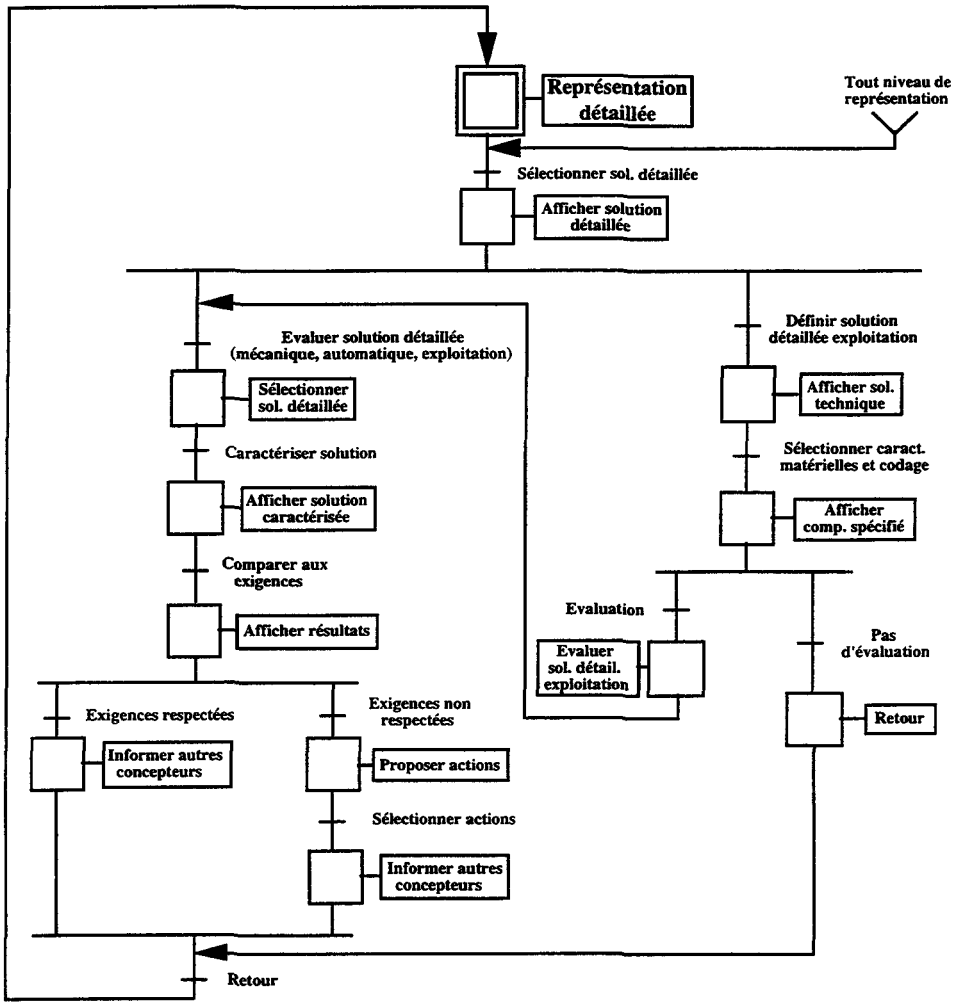

Figure 20 : Scénario d'évaluation associé au niveau Représentation détaillée

Comme pour les niveaux de représentation précédents, le scénario de conception distingue deux aspects.

Un aspect évaluation qui permet de valider les solutions complètement spécifiées de chacun des acteurs (ces derniers ayant à ce niveau attribué des caractéristiques précises aux composants techniques qu'ils ont retenus). Cela consiste finalement à évaluer la fonction de service étudiée ou le produit complet à partir de données fournies par le(s) constructeur(s) (taux de défaillance, fiabilité, ...).

Le second aspect concerne le concepteur pour l'exploitation qui va spécifier sa solution en précisant les caractéristiques des composants techniques qu'il a choisis et en codant les algorithmes des fonctions de base qui le nécessitent. On aura alors des composants spécifiés que l'on pourra acheter directement dans le commerce ou envoyer en fabrication si ceux-ci sont trop spécifiques.

Nous avons présenté dans cette seconde partie de chapitre, les différents scénarios de conception possibles à chacun des niveaux de représentation. Ceux-ci décrivent comment évaluer la sûreté de fonctionnement du produit au fur et à mesure que celui-ci est spécifié.

Nous allons dans la troisième partie évaluer et valider les propositions que nous avons faites dans le cadre de nos travaux de recherche.

3. Analyse des résultats

3.1. Objectifs

Les protocoles d'évaluation présentés au paragraphe précédent, visaient à valider les principaux éléments de la méthodologie proposée : les modèles conceptuels d'une part et l'environnement informatique d'autre part. Pour effectuer cette validation, nous avons retenus les critères suivants :

En ce qui concerne la validation des modèles, celle-ci porte sur quatre points :

- la capacité à prendre en compte la sûreté de fonctionnement à tout instant de la conception ;
- la pertinence des résultats et l'apport du concept de sûreté de fonctionnement pour l'aide à la décision ;
- l'adéquation des modèles utilisés pour l'estimation de la sûreté de fonctionnement à chacun des niveaux de représentation du modèle de produit ;
- l'aptitude des modèles à être pris en compte dans un processus de conception non-monotone.

Pour la validation de l'environnement informatique, l'objectif est de vérifier la faisabilité de la structure logicielle et ses capacités à répondre aux besoins des utilisateurs.

3.2. Validation des modèles

3.2.1. Capacité à prendre en compte la sûreté de fonctionnement

La sûreté de fonctionnement est aujourd'hui un enjeu majeur qu'il faut prendre en compte et intégrer dès la phase de conception d'un produit. L'extension du modèle de produit proposé par [JACQUET 98] par l'ajout de concepts dédiés à la sûreté de fonctionnement, montre qu'il est possible de la prendre en compte dès ce stade.

Les évaluations faites aux différents niveaux de représentation permettent de vérifier que les exigences du client sont respectées, de déceler les points faibles de la conception et, à partir de là, mettre en œuvre les actions correctives adéquates pour parvenir à atteindre les objectifs fixés.

Nos propositions visent donc à agir au plus tôt et à propager les modifications dans la conception du produit afin de réduire les coûts induits par les remises en cause ultérieures (en exploitation par exemple) de solutions ayant pu être proposées et ne s'avérant finalement pas satisfaisantes.

3.2.2. Pertinence des résultats

Les premiers résultats tirés de notre expérimentation sont encore trop peu nombreux et incomplets pour pouvoir valider l'approche dans sa globalité. En effet, nous n'avons implémenté que les trois premiers niveaux de représentation du modèle de produit. L'aspect concourance n'apparaît qu'au niveau technologique et nous ne disposons pas de plusieurs solutions (tant automatiques que mécaniques) à évaluer afin de proposer celle qui offre le fonctionnement le plus sûr.

De plus, ces résultats portent essentiellement sur une évaluation qualitative de la sûreté de fonctionnement, l'aspect quantitatif ayant été peu pris en compte pour l'instant. Cependant, sur un exemple simple et sur une solution technologique unique, les résultats obtenus sont encourageants et nous incitent à poursuivre dans cette voie.

Enfin, sans comparaison de résultats d'évaluation de diverses solutions, il est difficile de fournir aux concepteurs des éléments d'aide à la décision sur lesquels ils pourraient s'appuyer pour choisir telle solution (plus fiable) plutôt qu'une autre. C'est sans nul doute un critère important dans le cadre de l'élaboration d'une démarche de conception de systèmes au fonctionnement sûr.

3.2.3. Adéquation des modèles

Comme nous l'avons précisé au paragraphe précédent, l'évaluation de la sûreté de fonctionnement s'est essentiellement faite à partir de modèles qualitatifs, le tableau d'Analyse des Modes de Défaillance et de leurs Effets (AMDE). Les avantages de cette méthode ainsi que son intérêt pour la recherche des défaillances d'un système ainsi que pour l'aide à sa maintenance, sont reconnus à la fois dans le milieu industriel et dans la communauté scientifique.

Une extension aux propositions faites est l'utilisation cette fois de modèles quantitatifs de la sûreté de fonctionnement. En effet, les relations mathématiques permettant de déterminer la fiabilité prévisionnelle d'un système sont relativement difficiles à mettre en œuvre car elles nécessitent de nombreuses données et de nombreux calculs. L'extension de nos propositions à d'autres modèles, relatifs au comportement (mécanique ou autre) des entités et des systèmes (voir paragraphe 2.3.) nous semble inévitable.

L'étape suivante consistera donc à intégrer ces modèles à la maquette.

3.2.4. Non-monotonie du processus de conception

La non-monotonie est une des caractéristiques principales du processus de conception. Les résultats que nous avons obtenus montrent que les modèles et les concepts proposés peuvent et se doivent d'être utilisés dans un tel cadre. Des évaluations à la fois locales et globales permettent d'identifier des problèmes de sûreté sur un élément particulier ou sur un tout.

Nous avons essentiellement illustré la non-monotonie sur les concepts propres à la sûreté de fonctionnement en fonction d'hypothèses que nous avons dû faire à chacun des niveaux de représentation du modèle de produit. En effet, seuls les trois premiers niveaux de représentation ayant été considérés dans le cadre du projet DSPT8, il s'est avérer nécessaire de faire un certain nombre d'hypothèses concernant les composants techniques choisis et sur leurs caractéristiques (de fiabilité notamment pour les diverses évaluations). Une poursuite

des travaux serait de travailler sur des données plus vraisemblables pour valider nos propositions.

Il faudra également vérifier, dans le cas où plusieurs solutions sont possibles ou que des branches sont traitées de façon simultanée, que les propositions que nous avons faites sont toujours valides et qu'elles permettent bien de proposer au concepteur la solution qui offre, *a priori*, le fonctionnement le plus sûr.

3.3. Validation de l'outil

L'implémentation de la maquette a pour objectif principal de montrer, par démonstration et formation d'utilisateurs, la faisabilité ainsi que d'illustrer les propositions qui ont été faites, dans l'objectif de concevoir des systèmes sûrs de fonctionnement.

La maquette informatique a été développée à l'aide du logiciel Multimedia Toolbook (de Assymetric) qui vise à développer des applications multimédia quelles qu'elles soient.

Multimedia Toolbook est un système orienté objet permettant, à partir d'un langage de programmation simple appelé Open Script®, de programmer des applications multimédia. Ces applications peuvent être diverses et variées, allant de l'éducation au démonstrateur de produit. Pour notre part, nous utilisons cet outil en tant que support informatique pour développer le démonstrateur de validation de nos propositions.

Dans l'objectif de montrer la validité de nos propositions, nous avons réalisé un démonstrateur de laboratoire /FEAST 96/. Son but est de démontrer par l'exemple la faisabilité des propositions faites lors des chapitres précédents. Comme support applicatif de ce démonstrateur, nous avons choisi de représenter l'exemple du DSPT8 que nous venons de décrire afin d'illustrer d'une part, la démarche de conception de systèmes sûrs et d'autre part, sa non-monotonie.

Dans sa forme actuelle, la maquette ne permet pas de valider complètement la démarche. Le démonstrateur ne présente, pour l'instant, que les éléments relatifs aux trois premiers niveaux de représentation du modèle de produit. L'aide à la décision que ce critère peut apporter aux autres concepteurs (automaticiens, mécaniciens, ...) s'en trouve donc limitée. Cependant, l'objectif qui était de montrer que la sûreté de fonctionnement pouvait être mieux intégrée au cours du processus de conception et que des concepts qui lui sont dédiés pouvaient être introduits au modèle de produit, est atteint.

Une évolution de l'outil dans ce sens est donc nécessaire si l'on veut proposer aux concepteurs une démarche de conception de systèmes sûrs la plus complète qui soit. Cette évolution passera sans doute par l'utilisation d'un autre support informatique, CAS.CADE par exemple pour permettre le dialogue avec d'autres maquettes informatiques (les autres intervenants de la conception).

CONCLUSION

Nous avons décrit dans ce cinquième chapitre, la maquette de validation de nos propositions en matière de conception de systèmes au fonctionnement sûr. A l'issue du projet, les aspects sûreté de fonctionnement n'étaient pas pris en compte au niveau de l'étude. Seule

une solution technologique mécanique avait été proposée. C'est donc sur cette base ainsi que sur les travaux de /JACQUET 98/ que nous nous sommes appuyés pour illustrer nos propositions et enrichir ce qui avait été proposé. Aussi, dans une première partie, nous avons présenté les résultats obtenus à l'issue du projet DSPT8 qui est l'exemple sur lequel nous avons validé la démarche de conception de systèmes sûrs.

Dans la seconde partie, nous avons décrit les différents scénarios de conception que le concepteur peut mettre en œuvre à chacun des niveaux de représentation du modèle de produit (représentations du besoin, des exigences fonctionnelles, technologique, technique et détaillée). Ces scénarios sont décrits par l'intermédiaire de grafcets représentant les opérations à effectuer pour mettre en œuvre les concepts du modèle de produit (chapitre 2). Ils sont donc une instance particulière du processus de conception (chapitre 3) qui décrit quant à lui l'ensemble des scénarios possibles pour le concepteur.

Dans la troisième et dernière partie, nous avons validé nos propositions à partir des protocoles d'évaluation qui ont été définis et présentés dans la seconde partie. Ces protocoles ont abouti à la définition de critères nous permettant de montrer l'intérêt de l'approche. Ces critères concernent la capacité des modèles à prendre en compte la sûreté de fonctionnement ; la pertinence des résultats en ce qui concerne l'évaluation de la sûreté de fonctionnement ; l'adéquation des modèles proposés aux chapitres 2 et 3 à la problématique de la conception de systèmes au fonctionnement sûr ; et enfin la non-monotonie du processus de conception qui permet d'une part, de disposer des informations pertinentes plus rapidement et, d'autre part, de proposer, au plus tôt, les actions correctives à mettre en place afin de garantir la sûreté de fonctionnement du produit.

Cependant, il reste encore un certain nombre de points en cours de mise en œuvre (définition plus précise du niveau représentation technique, interactions avec les autres concepteurs). Ceux-ci devraient nous permettre de valider la démarche dans sa globalité.

CONCLUSION GENERALE

La création et le développement rapide de nouveaux produits de plus en plus complexes, combinant de nouvelles et de multiples technologies, ont fait apparaître de nouveaux objectifs ambitieux. Ils consistent à maîtriser simultanément la qualité par le Zéro défaut et la fiabilité par le Zéro panne. Dans ce contexte, la sûreté de fonctionnement est devenue aujourd'hui incontournable que ce soit lors de la conception et /ou de l'exploitation des systèmes modernes.

D'un domaine industriel à l'autre, les activités liées à la sûreté de fonctionnement peuvent s'avérer différentes car les systèmes de production, les contraintes, les besoins et attentes, ... sont différents. Cependant, la problématique reste la même. En effet, pour mener une étude de sûreté de fonctionnement, il est nécessaire :

— de comprendre le système (son fonctionnement, ses dysfonctionnements) ;

— de calculer les conséquences que peut engendrer l'apparition d'incidents ou d'accidents ainsi que les probabilités d'apparition de ces événements indésirés ;

— d'identifier et de hiérarchiser les actions visant à réduire les risques ainsi que celles limitant les conséquences des incidents ;

— de fournir enfin des éléments d'aide à la décision.

Les travaux présentés dans ce mémoire s'intègrent dans cette problématique. Ils avaient pour objectif de contribuer à intégrer la contrainte sûreté de fonctionnement au sein d'une démarche de spécification et de conception multimétiers.

Le premier chapitre a montré tout d'abord l'insuffisance des méthodes de conception actuelles qui n'intègrent pas cette notion importante qu'est la sûreté de fonctionnement ainsi que les concepts de l'ingénierie simultanée. Pour pallier à ces manques, une démarche de conception a été élaborée au sein du laboratoire. Elle distingue le Modèle de produit, rassemblant différents concepts relatifs au produit à concevoir, et le processus de conception qui spécifie comment sont instanciés ces concepts. Nous avons présenté le domaine de la sûreté de fonctionnement ainsi que les différentes méthodes qui permettent son évaluation. Nous avons montré que la méthode d'Analyse des Modes de Défaillance et de leurs Effets (AMDE) était la plus adaptée dans le cadre de nos travaux.

Le second chapitre a été consacré à la présentation du modèle de produit. Nous avons vu qu'il était décrit par l'intermédiaire de cinq niveaux de représentation. Chacun d'eux regroupe un certain nombre de concepts, à la fois génériques et dédiés métier suivant le niveau de représentation considéré. Nous nous sommes attachés à présenter les concepts dédiés à la sûreté de fonctionnement que nous avons recensés et intégrés au modèle de produit. Il s'agit des concepts *Fonction contrainte globale* qui correspond dans le cadre de nos travaux à la sûreté de fonctionnement ; *Mode de défaillance fonctionnelle* et *Mode de marche* pour recenser d'une part et limiter d'autre part, les effets des défaillances jugées critiques pour les fonctions opératoires de la chaîne ; *Fonction de base* et *Solution technologique* afin d'intégrer

au produit des fonctions de surveillance et de diagnostic ; *Mode de défaillance matérielle* et *Solution technique* pour affiner les évaluations aux niveaux de représentation précédents ; *Codage et Caractéristiques matérielles* qui ont pour objectif de spécifier complètement le produit. Ces différents concepts ont également été présentés de façon formelle et exprimés sous la forme d'expressions algébriques.

Nous avons également vu que les concepts étaient plutôt généraux aux deux premiers niveaux de représentation du modèle de produit et qu'ils s'orientaient vers les aspects surveillance et diagnostic aux niveaux suivants. Ce sont en effet ces activités que nous avons choisies parmi d'autres, de mettre en œuvre afin de garantir la sûreté de fonctionnement du produit lors de son exploitation future.

Dans le troisième chapitre, nous nous sommes intéressés à l'autre aspect important de la démarche de conception : le processus de conception. C'est par son intermédiaire que sont instanciés chacun des concepts relatifs au modèle de produit. Nous avons pour cela présenté le méta-modèle d'élaboration des concepts puis décrit comment celui-ci était utilisé à chacun des niveaux de représentation du modèle de produit.

Nous avons également vu que ce processus pouvait être non monotone c'est-à-dire que les concepts ne sont pas obligatoirement instanciés dans l'ordre chronologique dans lequel ils ont été présentés au cours du second chapitre. Le concepteur peut ainsi aller d'un niveau de représentation à un autre lui étant non adjacent. De même, il n'est pas nécessaire d'instancier tous les concepts d'un niveau de représentation donné pour pouvoir passer à un autre niveau de représentation.

Dans le chapitre quatre, après avoir présenté la technique de modélisation par objet OMT (Object Modelling Technique), nous avons proposé une représentation des propositions faites dans les chapitres précédents à l'aide des différents modèles que regroupe la technique. Ainsi, pour chacun des niveaux de représentation, nous avons décrit les concepts (modèle de produit) et les opérations permettant de les instancier (processus de conception) sous la forme de modèles objet, dynamique et fonctionnel.

Nous avons finalement proposé la structure de données associée à l'outil informatique d'aide à la conception de systèmes sûrs.

Le cinquième et dernier chapitre de ce mémoire a permis d'évaluer et de valider les principaux éléments de notre proposition. Après avoir présenté l'exemple de validation, nous avons présenté les scénarios de conception qui pouvaient être mis en œuvre à chacun des niveaux de représentation du modèle de produit. Ils sont les éléments sur lesquels s'appuient l'évaluation et la validation puisque d'une part, ils décrivent les opérations à réaliser pour intégrer la sûreté de fonctionnement dans le modèle de produit ; et d'autre part, ils décrivent le processus de conception mis en œuvre pour y parvenir.

Nous avons enfin terminé par une présentation de résultats nous permettant de valider, en partie seulement, la démarche de conception de systèmes sûrs de fonctionnement. Les protocoles d'évaluation mis en œuvre nous ont permis de définir différents critères afin de valider l'approche proposée. Ces critères concernent la capacité des modèles utilisés à prendre en compte la sûreté de fonctionnement ainsi que leur adéquation à la problématique de la conception de systèmes sûrs dans une organisation *ingénierie concourante* ; la pertinence des résultats obtenus lors des diverses évaluations de la sûreté de fonctionnement aux différents niveaux de représentation du modèle de produit ; la non-monotonie du processus de conception qui permet de remettre en cause, au plus tôt, les choix effectués par chacun des concepteurs aux différents stades de la spécification du produit.

Les perspectives de notre travail portent sur différents points.

Le premier concerne l'aspect "Comportement des entités", composante importante du modèle de produit. Il joue un rôle essentiel dans l'aide à la décision au concepteur concernant le choix d'un composant plutôt qu'un autre en fonction de ses réactions à diverses sollicitations. Les modèles relatifs à la résistance des matériaux seront notamment à intégrer au modèle.

Un autre point qui est lié au précédent est la notion de coût qui est également très importante dans l'aide au choix des composants. Intégrer des composants ou proposer des actions correctives ayant le meilleur rapport coût / efficacité sont des objectifs (voire des contraintes) que le client cherche de plus en plus à atteindre (à imposer). La solution retenue par le concepteur doit également être celle qui satisfait le mieux au compromis sûreté de fonctionnement / coût.

Un autre axe de recherche pourrait être lancé sur l'intégration de la maintenance au modèle et notamment ce qui concerne l'établissement de gammes de maintenance préventive pour certains composants jugés à risque d'un point de vue sûreté de fonctionnement et sur lesquels d'autres types d'actions (redondance) ne peuvent être mis en œuvre.

Nous proposons également le développement approfondi de la maquette. Celui-ci porterait sur deux points particuliers.

Le premier concerne l'implémentation de nos propositions sur plusieures applications industrielles permettant de prétendre ainsi à une véritable évaluation de notre approche.

L'autre aspect concerne le dialogue et les échanges entre acteurs de la conception. En effet, les choix de chacun d'eux, les remises en cause faites par les uns ou les autres doivent être bien sûr justifiés et surtout être transmis rapidement, notamment lorsque l'on se trouve dans un contexte d'ingénierie simultanée. Des travaux de recherche sur ce thème sont actuellement en cours au sein du laboratoire.

BIBLIOGRAPHIE

/ADEPA 81/ *Le GEMMA, guide d'étude des modes de marches et d'arrêts*, ADEPA, Collection Génie Productique, 1981.

/AFNOR 88/ AFNOR, *Fiabilité, maintenabilité, disponibilité*, recueil de normes françaises, Afnor-UTE, 1988.

/AFNOR 94/ Fascicule de documentation X 60-010, Vocabulaire de maintenance et de gestion des biens durables, Décembre 1994.

/ANDRES 90/ ANDRES V., DUBOIS D., LANG J., PRADE H., «Logique possibliste et logique floue - Applications au raisonnement automatisé et aux systèmes d'informations», dans ITURRIOZ L., DUSSAUCHOY A., *Modèles logiques et systèmes d'intelligence artificielle*, Col. Traité des Nouvelles Tecnologies, Série Intelligence Artificielle, Hermès 1990, pp. 163-179.

/ARINC 95/ ARINC Reseach Corporation, *Product reliability, maintainability and supportability handbook*, Edited by M. PECHT, CRC Press, 1995.

/BANDEKAR 89/ BANDEKAR V.R., « Causal models for diagnostic reasoning », *Artificial Intelligence in Engineering*, Vol.4, n°2, 1989.

/BARBER 92/ BARBER R., *BONES, an expert system for diagnosis with fault models*, Ellis Horwood Limited, London, 1992

/BARBIER 93/ BARBIER C., DAPERE R.,HUBER C., *Le zéro-panne par la topomaintenance. La TPM à la française*, Maxima, 1993.

/BELLUT 90/ BELLUT S., *La compétitivité par la maîtrise des coûts - Conception à coût objectif et analyse de la valeur*, Afnor gestion, 1990.

/BENCHIMOL 91/ BENCHIMOL G., VERLINDE Ch., ROSTAN G., *Méthode d'automatisation industrielle*, Hermès, 1991.

/BERGOT 95/BERGOT M., GRUDZIEN L., « Sûreté et diagnostic des systèmes industriels - Principaux concepts, méthodes, techniques et outils » , *Revue européenne Diagnostic et sûreté de fonctionnement*, Vol.5, n°3, pp 317-344, 1995.

/BILAND 94/ BILAND P., Modélisation des modes de marche d'un système automatisé de production, thèse de doctorat, Université de Nantes,1994.

/BLANCHARD 95/ BLANCHARD B.S., VERMA D., PETERSON E.L., *Maintainability, a key to effective serviceability and maintenance management*, John WILEY & SONS, 1995.

/BON 95/ BON J-L., *Fiabilité des systèmes — Méthodes mathématiques*, Collection Techniques stochastiques, Masson, 1995.

/BONNEVAL 93/ DE BONNEVAL A., Mécanismes de reprises dans les systèmes de commande à évènements discrets, thèse de doctorat, université Paul Sabatier de Toulouse, 1993.

/BORNE 93/ BORNE P., DAUPHIN-TANGUY G., RICHARD J.P., ROTELLA F., ZAMBETTAKIS I., *Analyse et régulation des processus industriels -Tome 1 : Régulation continue*, Éditions TECHNIP, 1993.

/BOUGEARD 93/ BOUGEARD J., BRACQUEMOND A., LEGEARD B., PETITIMBERT P., «Failure diagnosis of industrial processes based on logic programming», *TOOLDIAG 93 International Conference on Fault Diagnosis*, Toulouse, 5-7 Avril 1993, pp. 213-221.

/BOULENGER 88/ BOULENGER A., *Vers le zéro panne avec la maintenance conditionnelle*, Col. Guides de l'utilisateur, Afnor, 1988.

/BRUNET 90/ BRUNET J., JAUME D., LABARRERE M., RAULT A., VERGE M., *Détection et diagnostic de pannes. Approche par modélisation*, Col. Traité des Nouvelles Technologies, Série Diagnostic et maintenance, Hermès, 1990.

/BRUNET 92/ BRUNET J., «Reconfiguration et diagnostic prédictif de machines outils», *4ème Congrès international sur les techniques de surveillance, de diagnostic et de maintenance*, Senlis, 15-17 Juillet 1992, pp. 163-169.

/BTE 92/ *Maîtrise et gestion de la maintenance*, Tomes 1 et 2, Edition BTE, 1992.

/CASSAR 94/ CASSAR J-P., « Génération des relations de redondance analytique pour la surveillance », *Journées Sûreté, Surveillance, Supervision*, Paris, 17-18 Novembre 1994.

/CHATAIN 93/ CHATAIN J-N., *Diagnostic par système expert,* Col. Traité des Nouvelles Technologies, Série Diagnostic et Maintenance, Hermès, 1993.

/COCQUEBERT 90/ COCQUEBERT E., «Modélisation des métiers de l'entreprise», Projet MRT n° 89 P 0470, LGIL, Université de Valenciennes, 1990.

/CORRAZA 75/ CORRAZA M., *Techniques mathématiques de la fiabilité prévisionnelle*, Cépaduès Editions, 1975.

/CUENCA 92/ CUENCA A., « Méthode d'attribution des objectifs de sûreté de fonctionnement aux systèmes composant la future base de lancement Ariane et Hermes de Kourou », *Safety and reliability '92, Proceedings of the European Safety and reliability conference*, pp. 213-224. Elsevier, 1992.

/DANIEL 97/ DANIEL M. et al., «ERBUS - Towards a knowledge Management System for Designers», Knowledge based systems for knowledge management in enterprises conference, 9-12 September, Freiburg, Baden-Württemburg, Germany, 1997.

/DAVID 88/ DAVID J-M., KRIVINE J-P., «Utilisation de prototypes dans un système expert de diagnostic : le projet DIVA», *8èmes journées internationales Les systèmes experts et leurs applications*, Avignon, 1988, pp.889-907.

/DAVIS 84/ DAVIS R., «Diagnostic reasoning based on structure and behavior», *Artificial Intelligence*, n°24, 1984, pp. 347-410.

/DAVIS 93/ DAVIS R., «Retrospective on diagnostic reasoning based on structure and behavior», *Artificial Intelligence*, n°59, 1993, pp.149-157.

/DAUPHIN-TANGUY 93/ DAUPHIN-TANGUY G., SCAVARDA S., «Modélisation des systèmes physiques par bond-graphs» dans *Systèmes non linéaires - Tome 1 : modélisation-estimation*, Coordonné par FOSSARD A.J. et NORMAND-CYROT D., MASSON, 1993.

/DE KLEER 84/ DE KLEER J., BROWN J.S., « A qualitative physics based on confluences», *Artificial Intelligence*, n°24, 1984, pp. 7-83.

/DE KLEER 87/ DE KLEER J., WILLIAMS B.C., «Diagnosing multiple faults», *Artificial Intelligence*, n°32, 1987, pp 97-130.

/DE KLEER 92/ DE KLEER J., MACKWORTH A.K., REITER R., «Characterizing diagnosis and systems», *Artificial Intelligence*, n°56, 1992, pp.197-222.

/DELAFOLLIE 91/ DELAFOLLIE G., *Analyse de la valeur*, Hachette Technique, 1991.

/DESROCHES 95/ DESROCHES A., *Concepts & méthodes probabilistes de base de la sécurité*, Lavoisier TEC & DOC, 1995.

/DSPT8 97/ DSPT8, «Scénario d'ingénierie communicante pour les systèmes intégrés de production», Rapport final du projet DSPT8 en productique, 1997.

/DUBUISSON 90/ DUBUISSON B., *Diagnostic et reconnaissance des formes*, Col. Traité des nouvelles technologies, Série Diagnostic et maintenance, Hermès, 1990.

/ENGELHARDT 87/ ENGELHARDT R., «ARME: système d'aide au diagnostic appliqué à l'analyse vibratoire des machines tournantes», *Doc. Laborde and Ruffer-Repelec*, Groupe Alsthom, 1987.

/FADIER 90/ FADIER E., «Fiabilité humaine : méthodes d'analyse et domaines d'application», dans LEPLAT J., TERSSAC G., *Les facteurs humains de la fiabilité dans les systèmes complexes*, Octarès Entreprises, 1990, pp. 47-80.

/FAKRI 94/ FAKRI A., ROCARIES F., «Transfert bond-graphs-blocs diagramme. Application aux calculs de paramètres de systèmes dynamiques sous $MATIX_X$ / XMath-SYSTEM BUILD, Conférences Automatique Assistée par Ordinateur, 17-18 novembre 1994, Paris.

/FEAST 96/ FEAST, FEature based ASsembly, Projet européen Brite-Euram n°BRE2-CT94-1015, 1996.

/FERRAY BEAUMONT 91/FERRAY BEAUMONT S., GENTIL S., «Modèle qualitatif de comportement pour un système d'aide à la supervision», *R.A.I.R.O. APII*, Vol. 25, n°4, 1991, pp. 325-348.

/FERREIRO 93/ FERREIRO GARCIA R., RODRIGUEZ GOMEZ B., «Process control failure diagnostic fuzzy expert system», *TOOLDIAG 93 International Conference on Fault Diagnosis*, Toulouse, 5-7 Avril 1993, pp. 197-206.

/FINK 87/ FINK P.K., LUSTH J.C., «Expert systems and diagnostic expertise in the mechanical and electrical domains», *IEEE Transactions on Systems, Man and Cybernetics*, vol. 17, n°3, 1987, pp. 340-349.

/FORBUS 84/ FORBUS K.D., «Qualitative process theory», *Artificial Intelligence*, n°24, 1984, pp. 85-168.

/FRANCOIS 93/ FRANCOIS D., PINEAU A., ZAOUI A.,*Comportement mécanique des matériaux - viscoplasticité, endommagement, mécanique de la rupture, mécanique du contact*, Editions Hermès, 1993.

/FRANK 93/ FRANK P.M., « Advances in observer-based fault diagnosis», *TOOLDIAG 93 International Conference on Fault Diagnosis*, Toulouse, 5-7 Avril 1993, pp. 817-836.

/GABRIEL 85/ GABRIEL M., PIMOR Y., *Maintenance assistée par ordinateur*, Masson, Col. Informatique et gestion de l'entreprise, 1985.

/GABRIEL 93/ GABRIEL M., RICHET D., O'REILLY K., «Approche maintenance basée sur la fiabilité, application au secteur de la fonderie en Europe», *4ème Congrès international de Génie industriel*, Marseille, 15-17 décembre 1993, pp. 105-110.

/GAUTIER 93/ GAUTIER P.O., GRUBER T.R., « Generating explanations of device behavior using compositional modeling and causal ordering », *Proceedings of the eleventh National conference on Artificial Intelligence*, Washington, 1993.

/GENESERETH 84/ GENESERETH M.R., «The use of design descriptions in automated diagnosis», *Artificial Intelligence*, n°24, 1984, pp. 411-436.

/GERTLER 90/ GERTLER J., SINGER D., «A new structural framework for parity equation-based failure detection and isolation», Automatica, Vol. 26, n°2, 1990, pp. 381-388.

/GRUDZIEN 97/ GRUDZIEN L., JACQUET L., SOENEN R., «A design approach that integrates the safety and dependability concept», 4th IFAC Workshop on Intelligent Manufacturing Systems (IMS'97), 21-23 Juillet 1997, Séoul, Corée, pp. 115-120.

/IRI 79/ IRI M.K., AOKI K., O'SHIMA E., MATSUYAMA H., « An algorithm for diagnosis of system failure in chemical process », *Computers and Chemical Engineering*, Vol.3, pp. 489-493, 1979.

/ISERMANN 93/ ISERMANN R., «Fault diagnosis of machines via parameter estimation and knowledge processing», *Automatica*, Vol. 29, n°4, 1993, pp. 815-835.

/IWASAKI 86/ IWASAKI Y., SIMON H.A., « Causality in device behavior », *Artificial Intelligence*, Vol. 29, 1986, pp. 3-32.

/JACQUET 98/ JACQUET L., Contribution à l'élaboration d'une démarche de spécification fonctionnelle, thèse de doctorat, Université de Valenciennes, Février 1998.

/KARA-ZAITRI 93/ KARA-ZAITRI C., «Advanced F.M.E.A. modelling», *4ème Congrès international de Génie Industriel*, Marseille, 15-17 Décembre 1993, pp. 265-274.

/KERMAD 96/ KERMAD L., 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 1996.

/KRAUSE 93/ KRAUSE F.L., KIMURA F., KJELLBERG T., LU S.C.Y., « Product modelling », CIRP annals manufacturing technology, Vol. 42/2, 1993.

/KUIPERS 86/ KUIPERS B., « Qualitative simulation », *Artificial Intelligence*, n°29, 1986, pp. 289-338.

/LANNOY 94/ LANNOY A., PROCACCIA H., *Méthodes avancées d'analyse des bases de données du retour d'expérience industriel*, Collection de la Direction des Etudes et Recherches d'EDF, Eyrolles, 1994.

/LANNOY 95/ LANNOY A., *Analyse quantitative et utilité du retour d'expérience pour la maintenance des matériels et la sécurité*, Col. de la direction des Etudes et Recherches d'EDF, Editions Eyrolles, 1995.

/LAURENT 92/ LAURENT J.-P., VESCOVI M.-R., *La représentation des connaissances et le raisonnement sur les systèmes physiques - physique qualitative*, Cépaduès Éditions, 1992.

/LAVINA 92/ LAVINA Y., *Audit de la maintenance*, Les Editions d'Organisation, 1992.

/LEROY 92/ LEROY A., SIGNORET J-P, *Le risque technologique*, Col. Que Sais-Je ?, PUF, 1992.

/LEYVAL 94/Leyval L., « Causal reasoning », Ecole d'été d'Automatique de Grenoble, session Intelligence Artificielle et Automatique, Grenoble, 12-16 septembre 1994.

/LIMNIOS 91/ LIMNIOS N., *Arbres de défaillances*, Col. Traité des Nouvelles Technologies, Série Diagnostic et maintenance, Hermès, 1991.

/LUCAS 93/ LUCAS B., EVRARD J.-M., « An improved diagnosis method using a mixed model », *Tooldiag93*, International conference on fault diagnosis, Toulouse, 1993.

/MAN LEE 93/ MAN LEE J., KIM J.H., «An integration of heuristic and model-based reasoning in fault diagnosis», *Engineering applications of artificial intelligence*,Vol. 6, n°4, 1993, pp. 345-356

/MARRAKCHI 86/ MARRAKCHI M., Représentation des connaissances pour l'aide au diagnostic industriel : application au système expert SEDIAG, thèse de doctorat, université de Valenciennes, 1986.

/MENEXIADIS 88/ MENEXIADIS D., Conception d'un système expert d'aide au diagnostic pour les machines tournantes, thèse de doctorat, Université de Valenciennes, 1988.

/MOBLEY 92/ MOBLEY R. Keith, *La maintenance prédictive*, Edition Masson, 1992.

/MONTMAIN 93/ MONTMAIN J., GENTIL S, « Interprétation qualitative pour le diagnostic en ligne », *Revue européenne Diagnostic et sûreté de fonctionnement*, Vol. 3, n°1, 1993, pp.23-45.

/MONTMAIN 94/ MONTMAIN J., « Raisonnement approximatif et graphes causaux pour la détection et la localisation de défaillance », *Journées d'Etudes S3 Sûreté, Surveillance, Supervision*, Paris, Novembre 1994.

/MOREAU 95/ MOREAU J-C., «Automatismes et maîtrise de la complexité», dans *Les nouvelles stratégies techniques — La puce à l'usine*, Collection F. R. BULL, Masson, 1995.

/MOUBRAY 91/ MOUBRAY J., *Reliability-centred maintenance*, Butterworth Heinemann, Oxford, UK, 1991.

/OLESEN 93/ OLESEN K.G., «Causal probabilistic networks with both discrete and continuous variables», *IEEE Transactions on Pattern Analysis and Machine intelligence*, Vol..15, n°3, 1993, pp. 275-279.

/PAHL 84/ PAHL G., BEITZ W., *Engineering design*, Edited by Ken Wallace, published by The design council, London, 1984.

/PARAYRE 92/ PARAYRE Th., Le MESAP : vers une méthodologie d'exploitation des systèmes automatisés de production, thèse de doctorat, Université de Valenciennes, 1992.

/PEARL 86/ PEARL J., « Fusion, propagation, and structuring in belief networks », *Artificial Intelligence*, n°29, 1986, pp. 241-288.

/PENALVA 93/ PENALVA J.M., COUDOUNEAU L., LEYVAL L., MONTMAIN J., «A supervision support system for industrial processes », *IEEE Expert, Intelligent Systems and Their Applications*, vol. 8, n°5, 1993, pp. 57-65.

/PENG 87/ PENG Y., REGGIA J.A., « A probabilistic causal model for diagnostic problem solving », *IEEE Transactions on Systems, Man and Cybernetics*, vol. 17, n°2, 1987, pp. 146-162 (Part I) et vol. 17, n°3, 1987, pp. 395-406 (Part II).

/PETITDEMANGE 95/ PETITDEMANGE C., *Analyse de la valeur et ingénierie simultanée*, AFNOR, 1995.

/PIECHOWIAK 92/ PIECHOWIAK S., Système de diagnostic à base de connaissance fondé sur les premiers principes : application au diagnostic des équipements électroniques de conduite et de sécurité des transports guidés, thèse de doctorat, université de Valenciennes, 1992.

/PIMOR 91/ PIMOR Y., *TPM. La maintenance productive pour produire juste à temps*, Masson, 1991.

/PRIEUR 95/ PRIEUR G., NADI M., *La mesure et l'instrumentation : Etat de l'art et perspectives*, sous la direction de NGYEN L-N. et TSALKOVITCH G., Masson, 1995.

/PROCACCIA 92/ PROCACCIA H., PIEPSZOWNIK L., *Fiabilité des équipements et Théorie de la décision statistique fréquentielle et bayésienne*, Collection de la Direction des Etudes et Recherches d'EDF, Eyrolles, 1992.

/RAIMAN 91/ RAIMAN O., « Order of magnitude reasoning », *Artificial Intelligence*, n°51, 1991, pp. 11-38.

/RAK 92/ RAK I., *La démarche de projet industriel : technologie et pédagogie*, Editions Foucher, Paris, 1992.

/REITER 87/ REITER R., « A theory of diagnosis from first principles », *Artificial Intelligence*, n°32, 1987, pp. 57-95.

/RIOUT 94/ RIOUT J., *Le guide de l'AMDEC machine*, CETIM, 1994.

/RUMBAUGH 95/ RUMBAUGH J., BLAHA M., EDDY F., LORENSEN W., PREMERLANI W., *OMT - Modélisation et conception orientées objet*, Édition française, Prentice Hall, Masson 1995.

/RUMBAUGH 96/ RUMBAUGH J., BLAHA M., EDDY F., LORENSEN W., PREMERLANI W., *Solution des exercices*, Édition française, Prentice Hall, Masson 1996.

/SISSON 91/ SISSON J.C., «La méthodologie Taguchi», Revue Qualité et espace, n°17, pp. 20-22, 1991.

/SKATTEBOE 86/ SKATTEBOE R., LIHOVD E., AAS HYSTAD R., «DIAMON : a knowledge based system for fault diagnosis and maintenance planning for rotating machinery», *6èmes journées internationales Les systèmes experts et leurs applications*, Avignon, 1986, pp. 633-647.

/SOURIS 90/ SOURIS J-P., *La maintenance source de profits*, Les Editions d'Organisation, 1990.

/SPUR 90/ SPUR G., WEISS S., «Application of model-based diagnosis to machine tools », *International workshop on Expert systems in engineering - Principles and applications*, Vienna, September 1990, pp. 233-240.

/SRINIVASAN 93/ SRINIVASAN V.S., JAFARI M.A., « Fault detection/monitoring using time Petri nets », *IEEE Transactions on systems, man, and cybernetics*, vol. 23, n°4, 1993, pp. 1155-1162.

/SUH 90/ SUH Nam P., The principles of design, Oxford series on advanced manufacturing, Oxford university press, 1990.

/SUHNER 92/ SUHNER M.Ch., GABRIEL M. , «L'AMDEC pour générer la base de connaissances de systèmes d'aide au diagnostic», *L'AMDEC, un atout pour les PMI*, Recueil de conférence CETIM, pp.69-76, 1992.

/TERANO 92/ TERANO T., ASAI K., SUGENO M., *Fuzzy systems theory and its applications*, Academic Press Limited, London, 1992.

/TOMASENA 94/ TOMASENA M., BELMEGUENAÏ Y., «Diagnostic à base de modèles des procédés dynamiques : Approche et résultats», *9ème congrès Reconnaissance des formes et intelligence artificielle*, Paris, 11-14 janvier 1994, pp. 685-690.

/TOP 91/ TOP J., AKKERMANS H., « Computational and physical causality », *12th International Joint Conference on Artificial Intelligence*, Sydney, Australia, 1991.

/TRAVE MASSUYES 92/ TRAVE - MASSUYES L., « Qualitative reasoning over time : history and current prospects », *The Knowledge Engineering Review*, vol. 7, n° 1, 1992, pp. 1-18.

/ULIERU 93/ ULIERU M., ISERMANN R., « Design of a fuzzy-logic based diagnostic model for technical processes », *Fuzzy Sets and Systems*, n°58, 1993, pp. 249-271.

/VALETTE 94/ VALETTE R., KÜNZLE L.A., « Réseaux de Pétri pour la détection et le diagnostic », *Journées d'Etude S3 Sûreté, Surveillance, Supervision, Journées Détection et localisation de défaillances*, Paris, 17-18 novembre 1994.

/VAN DE VELDE 85/ VAN DE VELDE W., «Naive causal reasoning for diagnosis», *Journées Internationales d'Intelligence Artificielle*, Avignon, mai 1985, pp. 455-473.

/VILLEMEUR 88/ VILLEMEUR A., *Sûreté de fonctionnement des systèmes industriels*, Col. Direction des Etudes et Recherches d'EDF, Eyrolles, 1988.

/YOSHIKAWA 89/ YOSHIKAWA H., « Design philosophy : the state of the art », CIRP annals manufacturing technology, Vol. 38/2, pp. 579-586.

/ZIMMERMANN 91/ ZIMMERMANN H.-J., *Fuzzy set theory and its applications*, Kluwer Academic Publishers, London, 1991.

/ZWINGELSTEIN 92/ ZWINGELSTEIN G., «Optimisation de la maintenance par la fiabilité», *Maintenance & Entreprise*, n°454, pp. 27-31, 1992.

/ZWINGELSTEIN 96/ ZWINGELSTEIN G., *La maintenance basée sur la fiabilité - Guide pratique d'application de la RCM*, Editions HERMES, 1996.

ANNEXES

CONTRIBUTION A L'INTEGRATION DE LA SURETE DE FONCTIONNMENT AU SEIN D'UNE DEMARCHE DE CONCEPTION MULTIMETIERS

ANNEXE 1 : LA MAINTENANCE DES SYSTEMES

A1. La maintenance

La **maintenance** regroupe /AFNOR 94/ *toutes les activités destinées à maintenir ou à rétablir un bien dans un état ou dans des conditions données de sûreté de fonctionnement, pour accomplir une fonction requise. Ces activités sont une combinaison d'activités techniques, administratives et de management.* Maintenir c'est donc effectuer, au coût global optimum, des opérations qui permettent de conserver le potentiel du matériel pour assurer la continuité et la qualité de la production. Une politique de maintenance est essentiellement basée sur quatre types de stratégies : la maintenance corrective, la maintenance préventive systématique, la maintenance préventive conditionnelle et la maintenance améliorative (figure A1).

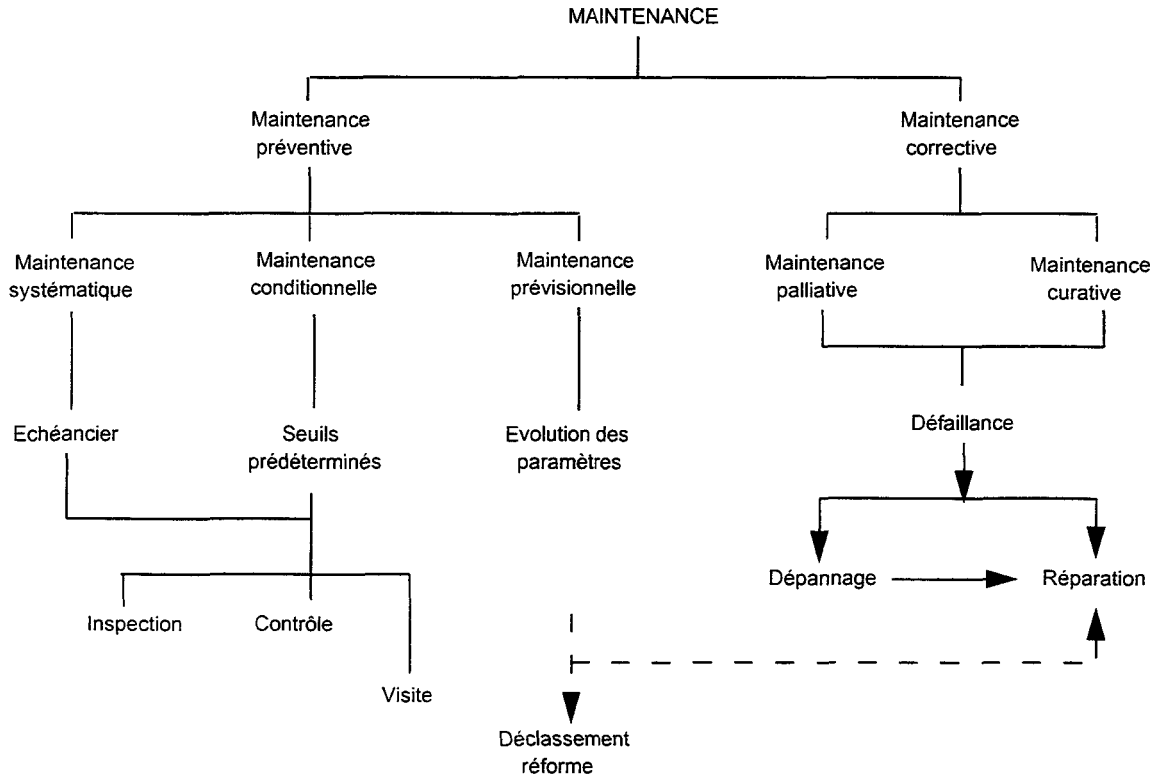

Figure A1 : Types de maintenance

La norme X 60-010 distingue cinq degrés de maintenance, classés de manière croissante selon la nature et la complexité des interventions à effectuer, la qualification des intervenants et des moyens mis en œuvre.

A1.1. 1er niveau

Ce niveau regroupe tous les réglages simples prévus par le constructeur au moyen d'éléments accessibles sans aucun démontage ou ouverture de l'équipement ou échanges d'éléments consommables accessibles en toute sécurité, tels que voyants ou certains fusibles, ...

Ce type d'intervention peut être effectué par l'exploitant du bien, sur place, sans outillage et à l'aide des instructions d'utilisation. Le stock de pièces consommables nécessaires est très faible.

A1.2. 2ème niveau

Il comprend tous les dépannages par échange standard des éléments prévus à cet effet et opérations mineures de maintenance préventive telles que graissage ou contrôle de bon fonctionnement.

Ce type d'intervention peut être effectué par un technicien habilité de qualité moyenne, sur place, avec l'outillage portable défini par les instructions de maintenance et à l'aide de ces mêmes instructions. On peut se procurer les pièces de rechange transportables nécessaires sans délai et à proximité immédiate du lieu d'exploitation.

A1.3. 3ème niveau

Il correspond à l'identification et au diagnostic des pannes, réparations par échanges de composants ou d'éléments fonctionnels, réparations mécaniques mineures, et toutes les opérations courantes de maintenance préventive telles que le réglage général ou le réalignement des appareils de mesure.

Ce type d'intervention peut être effectué par un technicien spécialisé, sur place ou dans le local de maintenance, à l'aide de l'outillage prévu dans les instructions de maintenance ainsi que des appareils de mesure et de réglage (éventuellement des bancs d'essais et de contrôle des équipements). Il utilise également l'ensemble de la documentation nécessaire à la maintenance du bien ainsi que les pièces approvisionnées par le magasin.

A1.4. 4ème niveau

Ce niveau regroupe tous les travaux importants de maintenance corrective ou préventive à l'exception de la rénovation et de la reconstruction. Il comprend aussi le réglage des appareils de mesure utilisés pour la maintenance, et éventuellement la vérification des étalons de travail par les organismes spécialisés.

Ce type d'intervention peut être effectué par une équipe comprenant un encadrement technique très spécialisé, dans un atelier approprié doté d'un outillage général (moyens mécaniques, de câblage, de nettoyage, ...) et éventuellement des bancs de mesure (et des étalons de travail nécessaires), à l'aide de toutes documentations générales ou particulières.

A1.5. 5ème niveau

Ce niveau comprend les travaux de rénovation, reconstruction ou exécution des réparations importantes confiées à un atelier central ou à une unité extérieure.

Par définition, ce type de travaux est donc effectué par le constructeur ou par le reconstructeur, avec des moyens définis par le constructeur et donc proches de la fabrication.

Aussi, pour faire face aux nouvelles démarches d'organisation des systèmes de production et à l'influence de facteurs technologiques, économiques et humains, la fonction

maintenance a subi une importante mutation. De cette évolution sont nées cinq politiques de maintenance que nous allons maintenant présenter.

A2. Les nouvelles politiques de maintenance

A2.1. La Maintenance Productive Totale

La *Maintenance Productive Totale* (Total Productive Maintenance) ou *Topomaintenance*, est un ensemble organisé de principes et de méthodes visant à obtenir au moindre coût, le rendement maximum du système de production sur toute sa durée de vie /BARBIER 93/. Ce rendement est traduit par le taux de rendement synthétique (TRS) obtenu par le produit des taux de disponibilité, de performance et de qualité des équipements. La topomaintenance /PIMOR 91/ implique la participation de tous les acteurs du système de production, des dirigeants aux opérateurs, et vise à éliminer les sept grandes causes de pertes de production que sont les défaillances, les réglages, les changements de série, les micro-arrêts, les cadences réduites, les aléas de procédés et les rebuts.

A2.2. La Maintenance Basée sur la Fiabilité

La Maintenance Basée sur la Fiabilité (Reliability Centered Maintenance), a pour objectifs l'amélioration de la sûreté de fonctionnement, la maîtrise des coûts et l'optimisation de la maintenance des équipements de production. Elle repose sur quatre phases principales /MOUBRAY 91//ZWINGELSTEIN 92/ : la recherche des équipements critiques, l'analyse systématique de leurs modes de défaillance et l'évaluation de leur criticité, la sélection des tâches de maintenance préventive grâce à une logique de décision /GABRIEL 93/ spécifique à la criti-cité des défaillances, et l'utilisation du retour d'expérience pour le réajustement des programmes de maintenance.

A2.3. L'Assurance Capacité de l'Outil de Production (ACOP)

Cette approche est centrée sur les méthodes et démarches qui permettent de maîtriser la capacité de production. Elle vise à garantir une disponibilité maximale et à atteindre un rendement optimum pour les équipements de production en agissant dans trois directions complémentaires /LAVINA 92/ : la réduction des temps de changement de fabrication, l'élimination des arrêts pour aléas de procédés et la fiabilisation du fonctionnement des équipements (diminution du taux de défaillance et des marches dégradées).

A2.4. La Maintenance Base Zéro (MBZ)

C'est une approche économique qui vise à rationaliser et réduire les coûts de maintenance. Elle s'appuie /LAVINA 92/ sur le recentrage des méthodes de maintenance (formalisation des moyens de suivi technique des équipements, préparation et planification fine des interventions), le transfert d'effectifs vers la sous-traitance (mise en place de partenariats), l'immersion d'équipes polyvalentes en production et la constitution d'une ingénierie de maintenance.

A2.5. Les Contrats Internes de Maintenance (CIM)

Ils consistent /LAVINA 92/ à formaliser les relations client/fournisseur entre la production et la maintenance, en définissant notamment les objectifs et critères de mesure des performances de la fonction maintenance et les modalités d'intervention et de suivi technique des équipements.

L'efficacité de ces différentes stratégies passe par la mise en place de moyens (humains, matériels, logistiques et économiques) adaptés aux objectifs fixés par la politique de maintenance. La mise en œuvre de ces moyens implique une organisation rationnelle de la fonction maintenance et surtout son informatisation : la maintenance doit en effet gérer un

grand volume d'informations pour décider en horizon immédiat (plusieurs fois par jour) ou à moyen terme avec calculs et simulations. La fonction maintenance doit ainsi se doter d'outils informatiques dédiés à la gestion (GMAO, Gestion de la Maintenance Assistée par Ordinateur) ou aux techniques de maintenance (TMAO, Techniques de Maintenance Assistées par Ordinateur), comme les systè-mes d'aide au diagnostic, les systèmes d'acquisition automatique des données, les systèmes de gestion électronique de documents, ...

A3. La gestion de la maintenance assistée par ordinateur (GMAO)

Un système informatique de gestion de la maintenance ou système informatique de GMAO est un progiciel organisé autour d'une base de données permettant de programmer, sous les trois aspects technique, budgétaire et organisationnel, toutes les activités d'un service de maintenance et les objets de cette activité /GABRIEL 85/.

Les systèmes informatiques de GMAO sont donc des logiciels/progiciels de gestion dont les objectifs sont :

— l'établissement d'une base de données centralisée accessible par tout le personnel autorisé ;

— l'amélioration de la gestion des disponibilités des ressources humaines et matérielles pour une maintenance plus efficace et moins coûteuse ;

— la planification des travaux de maintenance afin d'optimiser le rapport correctif/préventif ;

— la réduction de la fréquence et de la durée des pannes des équipements dont l'indisponibilité entraîne des interruptions ou des diminutions coûteuses de production.

Un système de GMAO est organisé sous une forme modulaire. Une telle structure facilite les interfaçages soit entre modules soit avec les systèmes extérieurs. Une GMAO type comprend sept modules de base.

A3.1. Le module Gestion des codes et paramètres

Ce module est dédié à l'initialisation des codes et paramètres utilisés dans le système et a pour objectif d'adapter le logiciel aux structures de l'entreprise. Ces codes et paramètres sont des données permanentes. La description de l'environnement industriel s'articule essentiellement autour de trois notions (objets, personnes, métiers) et des relations que le système permet d'établir entre-elles.

A3.2. Le module Gestion des intervenants

Il traite l'ensemble des informations relatives aux agents et équipes de maintenance. Il doit permettre la création, la modification, la consultation et la suppression de fiches intervenants.

A3.3. Le module Gestion des équipements

C'est essentiellement un module de documentation. Il est organisé autour d'un fichier principal de nomenclature du matériel auquel sont associés des fichiers auxiliaires permettant de regrouper les informations techniques suivant leur utilisation (documentation technique, historiques ou analyses). La nomenclature du matériel représente le répertoire classé et codifié des équipements de l'entreprise à maintenir.

A3.4. Le module Gestion des stocks

Ce module gère l'ensemble du stock de pièces de rechange, d'outillage et de fournitures de maintenance. Il se distingue d'un module classique de gestion de stock dans le sens où il

prend en compte les problèmes de maintenance à travers les réservations de pièces pour travaux, les possibilités de réintégration d'organes réparés, la multiplicité des modes de gestion (pièces neuves, réparées, immobilisées) ou la consommation de type aléatoire.

A3.5. Le module Gestion des achats

Ce module est complémentaire au module Gestion des stocks. Il permet de gérer les demandes d'achat et de réapprovisionnement de pièces de rechange, les demandes de devis et les appels d'offre, de suivre les ordres d'achat, de gérer les relances de commande, les réceptions et les reliquats de commande, ou encore de gérer les achats directs de biens et de services.

A3.6. Le module Gestion des travaux

Il permet de gérer toute opération de maintenance effectuée sur un équipement en apportant une aide à toutes les étapes de la vie d'un travail : demande de travail, ouverture d'un ordre de travail, phases d'un ordre de travail, contenu et suivi des travaux, saisie des informations propres à chaque travail, clôture technique et financière, enrichissement des historiques.

A3.7. Le module Gestion des budgets et coûts

Ce module est dédié aux prévisions et engagements des dépenses. Il traite plus particulièrement les dépenses de la fonction maintenance dont les informations sont fournies par la comptabilité analytique ; la valorisation des travaux qui regroupe l'ensemble des dépenses imputables à chaque travail ; les coûts indirects qui correspondent à une estimation des pertes de production pour raisons de maintenance ; les analyses statistiques de ces coûts et de leur évolution réalisées soit par des études ponctuelles, soit par édition périodique d'un tableau de bord. Ce module apporte aussi une aide à l'élaboration des budgets prévisionnels grâce aux possibilités de simulation qu'il offre.

Après avoir abordé la composante gestion de la maintenance, nous allons maintenant présenté sa composante technique.

A4. Les Techniques de Maintenance Assistées par Ordinateur (TMAO) /SOURIS 90/

Les techniques modernes de maintenance assistées par ordinateur regroupent toutes les utilisations, non strictement de gestion, dont peuvent avoir besoin les hommes de maintenance pour les aider dans leur diagnostic de pannes (système d'aide au diagnostic), pour relever des mesures avec un appareil portatif relié à un ordinateur, pour traiter ces données, pour élaborer des AMDEC.

A4.1. Aide aux relevés de disponibilité

Les systèmes d'aide aux relevés doivent avoir deux fonctions différentes :

- une fonction d'acquisition qui nécessite un système miniaturisé portable ou un système convivial connecté aux automates de process ;
- un logiciel de traitement des informations recueillies.

A4.2. Aide au diagnostic

Les progiciels d'aide à la recherche des causes initiales de défaillance se présentent sous plusieurs configurations :

— les systèmes intégrés dans les automates programmables, pilotes de l'équipement, ou dans les commandes numériques. Ils nécessitent une programmation particulière à l'aide des programmes calculs adaptés ;

— les cartes de diagnostic ou systèmes d'acquisition de données comparant en temps réel les cycles machines à un état de bon fonctionnement initial ou théorique. Elles fonction-nent par apprentissage ;

— les cartes de diagnostic programmables réalisant un pré diagnostic et un suivi de production ;

— les générateurs de systèmes experts permettant de rechercher la cause initiale de la défaillance si elle a été correctement documentée.

A4.3. Les systèmes experts

Les systèmes experts en maintenance sont une aide au diagnostic sophistiquée et efficace ; ils ont l'avantage d'être, en plus, la mémoire de l'entreprise dans le cas où l'expérience des anciens ne peut être transmise aux nouveaux. Comme la maintenance intervient depuis la conception jusqu'à l'exploitation d'un bien d'équipement, le système expert apporte la continuité de sa mémoire, permettant ainsi d'aider au diagnostic. Comme l'expert, le système réalisé doit savoir résoudre les problèmes dans un domaine limité, pouvoir expliquer son raisonnement, détecter les contradictions, tenir compte de certains renseignements inexacts et des moyens dont il dispose, tant humains que matériels.

A4.4. Les systèmes d'aide à la gestion de la documentation

La documentation est une matière essentielle de l'activité de maintenance. Malheureusement, celle-ci est bien souvent dispersée, incomplète voire inexistante.

Le développement des moyens de communication, l'apparition des mémoires optiques permettent aujourd'hui d'augmenter la densité des informations stockées et de centraliser ainsi tous ces documents. Le couplage des techniques systèmes experts, hypertexte et hypermédia à ces supports permet aujourd'hui une utilisation simple de la documentation.

Les principales missions de la maintenance sont donc de maintenir voire d'augmenter la productivité de l'outil de production, de participer à la réduction des coûts de production et d'obtenir des produits de qualité. Le respect de ces objectifs implique que celle-ci maîtrise les paramètres de fonctionnement du système de production. Elle doit en conséquence, autour d'une organisation rationnelle, disposer de méthodes et de moyens qui soient intégrés au système de production. Ils doivent également apporter une aide quant à la définition de la politique générale de maintenance du système ainsi que dans le choix et l'optimisation des stratégies de maintenance à appliquer aux différents équipements qui le composent.

ANNEXE 2 : LE COMPORTEMENT DES ENTITES

A2.1. Les graphes de fluence /BORNE 93/

La méthode du graphe de fluence permet de décrire le fonctionnement d'un système à partir de ces variables et de leurs interrelations. Ce mode de représentation est très proche de la représentation par schémas fonctionnels.

Une variable est représentée par un nœud (nœud source associé à une variable d'entrée externe au système, nœud puits isolant une variable choisie comme sortie) et une liaison entre variables par un arc, c'est-à-dire une branche orientée (figure A2.1).

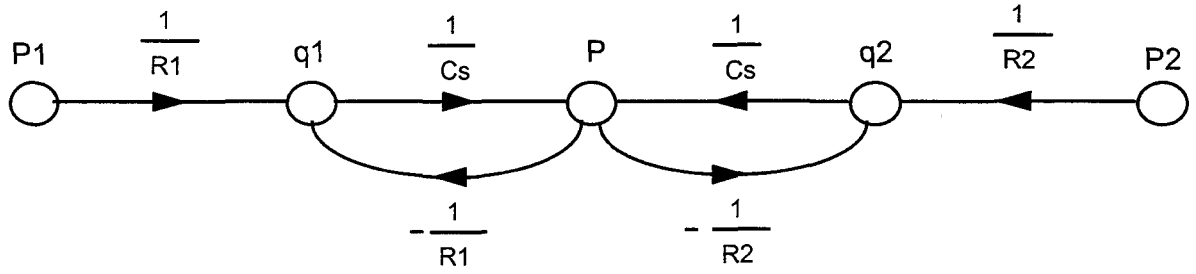

Figure A2.1: Exemple de graphe de fluence

La valeur de la variable représentée par un nœud est égale à la somme pondérée des variables qui y sont reliées par une flèche (branche) dirigée vers le nœud. Le coefficient de pondération ou poids est une valeur inscrite sur la branche et correspond à un nombre ou une transmittance.

A2.1.1. Principe /FADIER 90/

Le principe de modélisation par graphe de fluence consiste à représenter graphiquement les variables d'un système et leurs interactions. Partant d'une variable, on cherche à identifier ses interactions pour remonter jusqu'au niveau le plus haut du système et établir ainsi son schéma fonctionnel.

Le graphe de fluence est un diagramme qui distingue les "variables simples" (cercle avec une entrée et une sortie) et les "variables complexes" (cercle avec plusieurs entrées et plusieurs sorties). Les liaisons causales reliant les variables sont représentées par des flèches.

La construction d'un graphe comprend deux étapes importantes : la première consiste à établir un tableau déterminant les relations fonctionnelles entre les variables ; la seconde consiste à tracer, à partir du tableau précédent, le diagramme causal entre variables.

A2.1.2. Contexte d'utilisation /FADIER 90/

Le graphe de fluence est une technique d'analyse fonctionnelle adaptée de la technique d' "analyse des schémas électriques" utilisée pour aménager les dispositifs de signalisation et de commande. Cette méthode a été utilisée pour décrire des mécanismes biologiques, pour analyser des situations de contrôle de processus, pour décrire des systèmes homme-machine,....

Compte tenu de ses caractéristiques, cette méthode peut être appliquée aussi bien en phase de conception des systèmes qu'en phase d'utilisation.

Au stade de la conception, elle peut fournir rapidement des indications sur la répartition des fonctions entre les opérateurs, les machines et les automatismes. Par contre, pour un système en fonctionnement, le graphe permet de mettre en évidence les variables (et leurs interactions) pertinentes pour l'opérateur. Il donne ainsi une représentation que l'opérateur a du système.

A2.2. Les bond-graphs

A2.2.1. Principe

L'outil Bond-graph (ou graphe de liaisons) est une représentation graphique des mécanismes d'interaction, de dissipation et de stockage d'énergie d'un système dynamique. Il se situe comme intermédiaire entre le système physique et les modèles mathématiques qui lui sont associés (matrice de transfert, équations d'état, système d'équations différentielles d'ordre 2).

La méthodologie bond-graph /DAUPHIN-TANGUY 93/ demande l'analyse des phénomènes physiques qui seront pris en compte dans la modélisation (pesanteur, frottement, inertie, compressibilité, ...). Cependant, cette approche ne demande pas l'écriture de lois générales de conservation. Elle repose essentiellement sur la caractérisation des phénomènes d'échanges de puissance au sein du système. Le bond-graph obtenu peut facilement évoluer, par simple ajout d'éléments nouveaux, sans reprendre la démarche depuis le début. De plus, le choix particulier des variables d'état donne au modèle d'état une réalité physique non négligeable. Enfin, par son caractère graphique et sa structure causale, le modèle bond-graph apparaît comme un bon outil d'analyse.

A2.2.2. Éléments constitutifs d'un schéma bond-graph

Un modèle bond-graph /FAKRI 94/ est un ensemble de jonctions exprimant l'équilibre entre les puissances transmises et reçues (figure A2.2). Ces jonctions sont formées et liées entre elles par des liens. Chaque jonction est caractérisée par une variable de puissance commune à tous les liens qui la composent. On parlera de flux (f) ou d'effort commun (e). Les règles d'affectation des causalités sont telles qu'un seul lien fixe la variable de puissance de la jonction (effort ou flux).

Les éléments bond-graphs utilisés pour représenter tout système des différents domaines de la physique (hydraulique, mécanique, électrique, ...) sont :

— les éléments passifs (R, C, I) car ils dissipent de la puissance ;

— les éléments actifs car ils fournissent de la puissance au système (les sources d'effort Se (force de gravité, générateur de tension, ...) et les sources de flux Sf (vitesse appliquée, générateur de courant, ...)) ;

— les éléments de jonctions (0, 1, TF, GY) qui servent à coupler les éléments passifs et composent la structure de jonction du modèle correspondant à l'architecture du système étudié. Ils sont conservatifs de puissance.

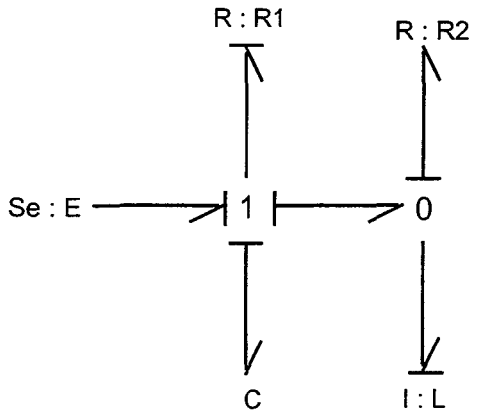

Figure A2.2 : Exemple de représentation Bond-graph

A partir de cette description, nous pouvons construire le schéma-bloc associé au bond-graph, rechercher l'équation d'état associée à ce modèle bond-graph ou déduire les propriétés structurelles d'un système.

A2.3. La physique qualitative

La physique qualitative /LAURENT 92//TRAVÉ-MASSUYÈS 92/ a pour objectif de formaliser les raisonnements que l'on peut mener sur un système physique, à partir de données qualitatives plutôt que d'informations numériques précises.

Trois approches apparaissent comme bases dans ce domaine : celle de /DE KLEER 84/, centrée sur la notion de composant ; celle de /FORBUS 84/ basée sur la notion de processus ; celle enfin de /KUIPERS 86/ composée d'un ensemble de contraintes sur les paramètres du système physique. Mais quelque soit l'approche, le principe reste toujours le même. Il consiste à décrire des relations entre des grandeurs physiques par des équations (généralement différentielles) qualitatives ou par l'intermédiaire de différents opérateurs, puis à simuler le bon ou le mauvais fonctionnement en construisant le graphe des états possibles.

A2.3.1. La représentation des connaissances

La plupart des connaissances sur les systèmes physiques sont mises sous la forme d'équations. Mais cet ensemble d'équations n'est pas un modèle causal et la notion de causalité est fondamentale pour la compréhension des phénomènes. Elle doit permettre d'expliquer comment un système arrive à son comportement global à partir des interactions de cause à effet entre les variables. Lors d'un changement du comportement d'une variable, celui-ci cause des changements dans le comportement d'autres variables et ainsi de suite.

A2.3.2. Notion de causalité

La causalité peut être définie selon deux points de vue /LAURENT 92/ :

— d'abord, elle désigne la recherche de la raison d'être des choses, c'est-à-dire la recherche des phénomènes primaires essentiels ;

— ensuite, elle est un mode d'explication des faits d'expérience. En physique qualitative, la causalité est généralement définie comme une relation unidirectionnelle entre variables (par exemple, A ——> B) signifiant que le comportement de la variable B à un instant t dépend du comportement de la variable A à des instants inférieurs ou égaux à t.

A2.3.3. Le graphe causal

Le comportement de tout système peut être décrit, au moins partiellement, par un graphe causal composé de relations unidirectionnelles entre des variables : un système peut souvent être décrit par ses équations structurelles qui sont généralement des interprétations algébriques des lois physiques régissant le système /MONTMAIN 94/. Une structure causale est une description des influences que les variables peuvent avoir les unes sur les autres (relations de cause à effet). L'ordonnancement causal fournit un guide pour identifier les asymétries entre les variables dépendantes et indépendantes. /BANDEKAR 89/ a montré qu'une représentation explicite de telles relations est directement utile pour le diagnostic : dans un raisonnement basé sur le modèle, cela signifie que la connaissance de dépendances causales peut être utilisée dans la recherche de la déviation première dans le graphe.

/IWASAKI 86/ a proposé une méthode basée sur la théorie de l'ordonnancement causal pour générer la causalité à partir d'une structure mixte composée par un ensemble d'équations dynamiques et statiques.

L'ordonnancement causal est une relation asymétrique entre les variables d'une structure équilibrée et dynamique " self-contained ". Une structure équilibrée " self-contained " est un système de n équations d'équilibre à n variables ayant les propriétés suivantes :

- dans chaque sous-ensemble possible de k équations, au moins k variables différentes apparaissent avec un coefficient non nul dans une ou plusieurs équations du sous-ensemble ;

- pour chaque sous-ensemble de k équations dans lequel r (r > k) variables apparaissent avec un coefficient non nul, alors, en choisissant arbitrairement les valeurs de (r - k) variables, on obtient une solution unique pour les k autres variables.

La figure A2.3 ci-après propose un exemple de graphe de causalité.

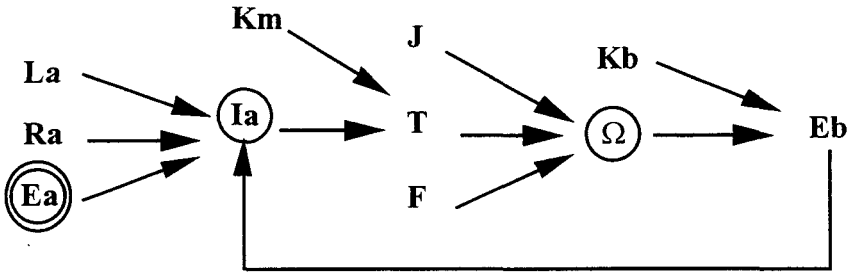

Figure A2.3 : Graphe de causalité d'un moteur à courant continu

Mais, ce simple graphe de causalité n'est pas suffisant car il ne donne que les relations entre les variables ; par contre les types d'influence entre-elles ne figurent pas. Aussi, l'approche graphe orienté semble être bien adaptée pour représenter la propagation des phénomènes physiques à travers des processus. Le graphe signé orienté est le graphe causal le plus simple : les nœuds correspondent aux variables et les arcs représentent les influences causales entre les nœuds. Ces influences sont représentées par des signes (+, -) sur les arcs

indiquant que les variables cause et effet tendent à évoluer dans le même sens ou dans des sens opposés. Cet aspect est très intéressant en simulation lorsque l'on cherche à savoir le type d'influence reliant deux variables. Le graphe signé orienté (SDG) pour un système physique peut être construit /IRI 79/ d'après :

— les données de l'installation ou l'expérience des opérateurs ;

— un modèle mathématique.

Des approches plus récentes consistent à porter sur les arcs du graphe des fonctions de propagation /TOMASENA 94/ ou des fonctions de transfert qualitatives /FERRAY-BEAUMONT 91//MONTMAIN 93//PENALVA 93/ propageant de variables en variables les perturbations ou changements significatifs.

A2.4. Synthèse

Connaître le comportement d'un système, en situation normale ou en présence de perturbations, est une activité très importante de la modélisation des systèmes. Elle est aujourd'hui primordiale dans le cadre de la surveillance et du diagnostic de défaillances de ces systèmes.

Nous avons présenté dans cette annexe trois approches susceptibles de représenter le comportement d'un système. Le *graphe de fluence* indique les relations entre variables mais ne donne malheureusement pas d'informations sur le type d'évolution qu'engendre la perturbation d'une variable sur les autres. Les *bond-graphs*, outre leur représentation graphique plutôt complexe, donnent essentiellement les relations entre composants d'un même système. Ils ne donnent pas les relations entre variables d'un même composant, ce qui s'avère utile lorsque l'on recherche la cause d'une défaillance ou d'une dégradation.

Nous retenons, dans le cadre de la surveillance et du diagnostic, l'approche par graphe de causalité. Elle permet en effet de représenter les relations de cause à effet entre variables et de fournir, dans le cadre d'un diagnostic, des explications sur l'origine des évolutions. L'*ordonnancement causal* et les bond-graphs produiront un ordre causal identique si les modèles mathématiques sous-jacents sont égaux. La différence fondamentale entre ces deux méthodes /TOP 91/ /LUCAS 93/ est que l'ordonnancement causal est basé sur des relations mathématiques abstraites et la méthode bond-graph sur les principes physiques formels. Ces méthodes diffèrent également au niveau des informations qu'elles nécessitent et les classes de modèles qu'elles acceptent /GAUTIER 93/.

ANNEXE 3 : SYNTHÈSE DU MODÈLE DE PRODUIT PROPOSÉ PAR /JACQUET 98/

Le modèle de produit se compose de cinq sous-ensembles de modèles. Il est défini à travers l'instanciation de concepts associés à chacun de ces sous-ensembles. Seuls les trois premiers sous-ensembles de modèles ont été étudiés. Le modèle de représentation des besoins et le modèle de représentation des exigences fonctionnelles du besoin permettent de spécifier d'un point de vue fonctionnel le produit à concevoir. Le modèle de représentation technologique permet de spécifier la partie automatique du produit. Nous allons dans les paragraphes suivants décrire les concepts associés à ces trois modèle de représentation.

A1. Le modèle de représentation des besoins

Ce modèle transcrit les besoins du client en un ensemble d'exigences "FS" spécifiant les services que doit satisfaire le produit "P" et l'ensemble des contraintes "FCg" qu'il doit respecter. De manière formelle, un produit est défini comme :

$$P = < FS , FCg >$$

avec :

P : Produit
FS : Ensemble des fonctions de service "fs_k"
FCg : Ensemble des Fonctions Contraintes globales "fcg_k" s'appliquant à l'ensemble des "fsk"

Afin de répondre à ces objectifs, deux concepts sont associés à ce modèle de représentation : le concept Fonction de service et le concept Fonction contrainte globale.

A1.1. Le concept "Fonction de service"

La fonction de service est un concept énoncé par l'Analyse de la valeur. Il est défini comme "l'action attendue du produit sur un élément du milieu extérieur au bénéfice d'un autre élément de ce milieu, dans une des phases d'utilisation". Ce concept modélise les services que le produit doit remplir.

Les fonctions de service diffèrent selon leur type. Ainsi, elles sont dites principales lorsqu'elles traduisent le besoin pour lequel le produit est effectivement réalisé et complémentaires quand elles découlent de l'utilisation que l'on veut faire du produit par rapport à son futur milieu d'implantation.

Par rapport à cette définition, la position de L. Jacquet est qu'il n'effectue pas de distinction entre les différents types de fonctions (principales, complémentaires, ...). Quel que soit son type, il considère qu'un fonction de service doit toujours être satisfaite. De plus, il considère que lorsqu'un élément du milieu extérieur "x" induit des contraintes sur la réalisation de la fonction, alors celles-ci seront transcrites sous la forme d'une contrainte d'action "ca" associée à l'action "a" caractérisant la fonction de service "fs_k". Ainsi, lorsque deux milieux extérieurs sont retenus pour spécifier une fonction de service, ils ne peuvent plus être considérés pour la définition d'une fonction contrainte globale.

Une fonction de service est donc définie comme *une fonction qui décrit un des objectifs que le produit doit satisfaire afin de répondre au besoin. Elle traduit une relation orientée (de "x" vers "y") entre deux éléments du milieu environnant du produit. Elle explicite, par un verbe d'action "a", quel est l'objectif à atteindre. Elle est contrainte par les Fonctions Contraintes Globales. Une fonction de service est indécomposable.*

A1.2. Le concept "Fonction contrainte globale"

Le concept de "Fonction contrainte" ou de "Contrainte" est propre à l'analyse de la valeur. Il est défini comme "une limitation de la liberté du concepteur (règlements, normes, ...)". L'analyse de la valeur considère que cette limitation peut être induite par n'importe quel élément extérieur.

La position de L. Jacquet par rapport à cette définition est assez similaire puisqu'il considère également que ce concept formalise des contraintes de conception. Cependant, il considère que ces contraintes s'appliquent sur l'ensemble du produit et ne portent jamais sur un seul service. Les contraintes devant être satisfaites par l'ensemble des fonctions de service, il donc appelé ce concept "Fonction contrainte globale".

Une Fonction contrainte globale est définie comme une fonction qui modélise les limites ou contraintes devant être satisfaites par l'ensemble des Fonctions de service du produit.

A2. Le modèle de représentation des exigences fonctionnelles du besoin

Ce modèle décrit "comment" répondre à chacun des services "fs_k" identifiés et représentés par le modèle précédent tout en respectant l'ensemble des contraintes "fcg" spécifiées par le client. Il ne présume ni du lieu ni des moyens qui permettent de satisfaire le service à remplir. Il précise le comportement (ensemble des opérations) que doit adopter le produit pour remplir chacun des services. Il détermine également les principes de réalisation nécessaire à la mise en œuvre de chaque opération. Afin de répondre à ces objectifs, trois concepts sont associés à ce modèle de représentation : les concepts "Fonction opératoire", "Principe opératoire" et "Solution de principe".

A2.1. Le concept "Fonction opératoire"

Chaque fonction de service "fs_k" précise un objectif à atteindre pour satisfaire le besoin du client. Ceci est réalisé par une ou plusieurs fonctions opératoires "fo_{ij}". Une fonction opératoire est donc une fonction précisant l'opération ou les opérations nécessaires à la réalisation de l'objectif fixé par la fonction de service. Une fonction opératoire est décomposable en fonctions opératoires de niveau inférieur. On distingue ainsi les fonctions opératoires de niveau $i = 0$ et celles de niveau $i \neq 0$.

A 2.1.1. Fonction opératoire de niveau i = 0

Une fonction opératoire de niveau i = 0 est une fonction qui assure la transcription d'un objectif fixé par une fonction de service "fsk" en une opération globale "o" précisant "Comment" atteindre cet objectif. Cette fonction précise l'état initial "ϕefs_k" ainsi que l'état final "ϕsfs_k" qui sera obtenu suite à la réalisation de la fonction opératoire.

A2.1.2. Fonction opératoire de niveau i ≠ 0

Une fonction opératoire de niveau i ≠ 0 explicite partiellement comment assurer une fonction opératoire de niveau i – 1 "$fo_{(i-1)j}$". La décomposition d'une fonction opératoire en sous-fonctions opératoires est contrainte par le choix d'un des "Principes opératoires" "po" susceptibles de supporter la fonction de niveau i-1. Les fonctions opératoires de niveau i ≠ 0 sont ordonnées afin de satisfaire les contraintes d'antécédence et/ou de parallélisme des opérations mises à jour.

Une fonction opératoire est ainsi définie comme une fonction assurant une transformation (informationnelle, physique, énergétique, ...) afin de passer d'un état opératoire à un autre. Elle est l'une des fonctions dont la séquence satisfait (ou la fonction satisfait) une fonction de service au moyen d'un principe opératoire "po_k". La notion de fonction opératoire est récursive . Elle précise "Comment" atteindre l'objectif fixé par la fonction de service indépendamment du lieu et des moyens nécessaires à sa réalisation.

A2.2. Le concept "Principe opératoire"

Le concept de principe a été énoncé par /PAHL 84/ qui l'a défini comme "l'effet physique et les caractéristiques de forme nécessaires à l'accomplissement de la fonction". Par rapport à cette définition, L. Jacquet considère qu'un principe opératoire "po_k" se borne à préciser un des effets physiques capables de supporter l'opération "o" caractérisant la fonction opératoire "fo_{ij}" considérée. Un principe opératoire ne présume pas de la technologie du ou des moyens nécessaires à la réalisation de l'opération. Il contraint la décomposition d'une fonction opératoire en sous-fonctions opératoires.

Le concept "Principe opératoire" "po_k" est donc défini comme un concept capable de supporter une fonction opératoire "fo_{ij}". Il fait référence à une classe de solutions (physique, chimique, cognitive, ...) mais ne fait pas référence à un moyen matériel spécifique. Il contraint la décomposition d'une fonction opératoire en sous-fonctions opératoires. Plusieurs principes opératoires peuvent être candidats pour supporter une fonction opératoire.

A2.3. Le concept "Solution de principe"

/PAHL 84/ a définit ce concept comme "une combinaison de principe ayant comme objectif de remplir une fonction globale". Le but de cette combinaison est d'établir la structure fonctionnelle du produit qui est représentée par l'association physique et/ou logique possible des sous-fonctions.

La position de L. Jacquet est assez similaire à celle-là. Il considère que toute solution de principe "sp_i", élément de l'ensemble des solutions de principe "SP" d'un produit, est définie comme la combinaison d'éléments "$spfs_{kl}$". Une solution de principe "$spfs_{kl}$" est un élément de l'ensemble des solutions de principe "$SPfs_k$" relatif à une fonction de service "fs_k" du produit. Enfin, une solution de principe "$spfs_{kl}$" est définie comme la combinaison des principes opératoires "po_k" candidats à supporter chaque fonction opératoire "fo_{ij}" de la

séquence opératoire de niveau "i". Une ou plusieurs solutions de principe "$spfs_{kl}$" sont donc déterminées pour chaque séquence opératoire de niveau "i".

Une solution de principe "$spfs_{kl}$" est définie comme *une combinaison des principes opératoires "po_k" associés aux fonctions opératoires "fo_{ij}" d'une séquence opératoire de niveau "i". Il peut exister plusieurs solutions de principe. L'ensemble des solutions de principe du produit "SP" est défini par le produit cartésien des ensembles des solutions de principe "$SPfs_k$" ("$SPfs_k$" est l'ensemble des solutions de principe "$spfs_{kl}$" relatives à une fonction de service "fs_k" du produit).*

A3.Le modèle de représentation technologique

Ce modèle représente les fonctions opératoires "fo_{ij}" qui caractérisent les séquences opératoires de plus bas niveau sous la forme d'un ensemble de fonctions de base "FB". Les fonctions de base sont spécifiques à un métier et assure de manière autonome une fonction particulière du produit. Ce modèle représente la structure technologique du produit suivant les point de vue de chaque métier (mécanique, automatique, maintenance, ...). Deux concepts sont associés à ce modèle de représentation : le concept "Fonction de base" et le concept "Solution technologique".

A3.1. Le concept "Fonction de base"

La description de ce concept a été faite dans le cadre de ce mémoire au chapitre 2. Nous ne reviendrons donc pas sur sa description ici. Nous ajouterons simplement que ce concept est défini ainsi : *une fonction de base assure de manière autonome et spécifique à un métier, une fonction particulière du produit. Plusieurs familles de fonctions de base peuvent être distinguées, notamment les fonctions de base de la mécanique (FB_m), les fonctions de base de l'automatique (Fb_a), les fonctions de base de l'exploitation (Fb_e), ...*

A3.2. Le concept "Solution technologique automatique"

Du point de vue automatique, la définition du concept solution technologique a pour objectif de déterminer l'architecture de commande (différents niveaux de commande) du produit. A cet effet, l'automaticien prend en compte les modes d'exploitation que le maintenicien a définis pour chaque actionneur. Ces modes d'exploitation (secours, ...) peuvent conduire à la mise en redondance des composants de commande du produit. De même, les procédures de reconfiguration préconisées par le maintenicien en cas de défaillance ont une répercution directe sur l'architecture de commande.

Le concept "Solution technologique automatique" est défini ainsi : *c'est un ensemble de composants technologiques. Elle représente les composants spécifiés, de manière concourante par les différents acteurs (automaticien, mécanicien, maintenicien, ...) afin que chacun d'eux ait une vue globale du produit. Elle définit, d'un point de vue automatique, les différents niveaux de commande du produit.*

GLOSSAIRE

Fiabilité [AFNOR 88] : Aptitude d'une entité à accomplir une fonction requise, dans des conditions données et pendant un intervalle de temps donné ;

Maintenabilité [AFNOR 88] : Dans des conditions données d'utilisation, aptitude d'une entité à être maintenue ou rétablie, sur un intervalle de temps donné, 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 ;

Disponibilité [AFNOR 88] : 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, en supposant que la fourniture des moyens extérieurs nécessaires soit assurée ;

Sécurité [VILLEMEUR 88] : Aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques ;

Maintenance [AFNOR 94] : Toutes les activités destinées à maintenir ou à rétablir un bien dans un état ou dans des conditions données de sûreté de fonctionnement, pour accomplir une fonction requise. Ces activités sont une combinaison d'activités techniques, administratives et de management ;

Maintenance préventive [AFNOR 88] : Maintenance effectuée selon des critères prédéterminés, dans l'intention de réduire la probabilité de défaillance d'un bien ou la dégradation d'un service rendu ;

Maintenance préventive systématique [AFNOR 88] : Maintenance préventive effectuée selon un échéancier établi selon le temps ou le nombre d'unités d'usage ;

Maintenance préventive conditionnelle [AFNOR 88] : Maintenance préventive subordonnée à un type d'événement prédéterminé (autodiagnostic, information d'un capteur, mesure d'une usure, ...) révélateur de l'état de dégradation du bien ;

Maintenance corrective [AFNOR 88] : Ensemble des activités réalisées après la défaillance d'un bien ou la dégradation de sa fonction pour lui permettre d'accomplir une fonction requise au moins provisoirement ;

Maintenance curative [AFNOR 88] : Activités de maintenance corrective ayant pour objet de rétablir un bien dans un état spécifié ou de lui permettre d'accomplir une fonction requise. Le résultat ded activités doit présenter un caractère permanent ;

Maintenance palliative [AFNOR 88] : Activités de maintenance corrective destinées à permettre à un bien d'accomplir provisoirement tout ou partie d'une fonction requise. Appelée couramment dépannage, cette maintenance palliative est principalement constituée d'actions à caractère provisoire qui devront être suivies d'actions curatives.

Titre : Contribution à l'intégration de la sûreté de fonctionnement au sein d'une démarche de conception multimétiers

Mots clés : Conception, Modèle de produit, Processus de conception, Sûreté de fonctionnement, Surveillance, Diagnostic, Maintenance.

Résumé :

Dans le contexte actuel d'amélioration de la productivité et d'automatisation, la sûreté de fonctionnement est devenue aujourd'hui un véritable enjeu car elle joue un rôle important dans la maîtrise des risques économiques, humains ou environnementaux. Les caractéristiques de sûreté de fonctionnement qu'un système devra avoir en phase d'exploitation sont définis dès sa conception.

Notre contribution porte sur trois points principaux. Tout d'abord, nous proposons un ensemble de concepts dédiés à la sûreté de fonctionnement intégrés au sein d'un modèle de produit. Ces concepts visent à concevoir des systèmes au fonctionnement sûr par la recherche de leurs points faibles d'une part, et la préconisation d'actions correctives (maintenance, redondance, ...) pour les éliminer ou les réduire d'autre part. Ensuite, pour mettre en œuvre ces concepts, nous exposons les opérations qui seront associées au processus de conception et qui permettront de les exemplifier. Ce processus est non-monotone c'est-à-dire que les concepts du modèle de produit ne sont pas instanciés de façon séquentielle. Enfin, nous présentons la conception et la mise en œuvre du système informatique, aide à la conception de systèmes fiables, qui nous permet d'évaluer et de valider, sur la base de plusieurs critères, nos propositions.

Les perspectives de ces travaux concernent la mise en place d'un retour d'expérience afin d'enrichir les modèles proposés. D'autres modèles tels que la théorie de la décision bayésienne ou l'analyse markovienne pourront être ajoutés. Ces perspectives s'orientent également vers l'évaluation des performances des systèmes en s'intéressant plus particulièrement à des critères relatifs à la fiabilité, à la disponibilité et aux coûts.

Title : Contribution towards the integration of safety and dependability into a multicraft design process

Key-words : Design, Product model, Design process, Dependability and safety, Supervision, Diagnosis, Maintenance.

Abstract :

In the presentday context of productivity improvement and automation, dependability and safety have indeed been put at stake because of the foremost part they play in the mastery of human, economical or environmental risks. The typical features of dependability a system must have on its working stage will be defined as early as its design is on process.

Our contribution is grounded on three main points. To begin with, we shall propose a body of concepts devoted to dependability within a product model. These concepts are intended to form reliable systems owing to search for weak points on the one hand, and on the other hand, for the proposal of corrective actions (maintenance, redundancy, ...) to eliminate or reduce these weak points. Then, to bring these concepts into play, we shall set out the operations which will be associated to the design process and will allow to exemplify them. This process is non-monotonous, that is to say, the concepts of the product model won't be instanciated in a sequential way. In the end, we'll present the conception and the implementation of the computer system designing which, by means of different criteria, allows us to assess and to validate our proposals.

The propects of these works take in the setting up of an experience return that the above proposed models may get the richer. It will be possible to add some other models such as Bayes's theory of decision or Markov's analysis. These perspectives which are also turned towards the appraisal of sustem results, will take into account criteria related to reliability, availability and costs.