Méthodes et modèles pour l'évaluation de la sûreté de fonctionnement de systèmes automatisés complexes : Application à l'exploitation de lignes de production - Application à la conception de systèmes intelligents distribués

Laurent Cauffriez

LAMIH
LABORATOIRE D'AUTOMATIQUE DE MECANIQUE ET D'INFORMATIQUE INDUSTRIELLES ET HUMAINES
UMR CNRS 8530

N° d' ordre 05-03

Mémoire

présenté à

L' UNIVERSITÉ DE VALENCIENNES
ET DU HAINAUT-CAMBRÉSIS

pour l'obtention de

L'Habilitation à Diriger des Recherches

spécialité

AUTOMATIQUE INDUSTRIELLE ET HUMAINE

par

Laurent CAUFFRIEZ
Maître de Conférences

Méthodes et Modèles pour l'Évaluation de la Sûreté de Fonctionnement de Systèmes Automatisés Complexes

—

Application à l'Exploitation de Lignes de Production
Application à la Conception de Systèmes Intelligents Distribués

Soutenue le 21.09.2005 devant la commission d'examen :

M.	**Laurent FOULLOY**	Professeur à l'ESIA d'Annecy	Rapporteur
M.	**Francis LEPAGE**	Professeur à l'Université Henri Poincaré de Nancy	Rapporteur
M.	**Daniel NOYES**	Professeur à l'ENIT de Tarbes	Rapporteur
Mme	**Mireille BAYART**	Professeur à Polytech'Lille	Examinateur
M.	**Jörg SCHÜTTE**	Professeur à l'Université Technique de Dresde	Examinateur
M.	**Christian TAHON**	Professeur à l'Université de Valenciennes	Examinateur
M.	**Christophe DELEBARRE**	Professeur à l'Université de Valenciennes	Examinateur
M.	**Patrick MILLOT**	Professeur à l'Université de Valenciennes	Directeur

A mon père André CAUFFRIEZ
11 juin 1927-12 octobre 2005

A ma famille

Avant-Propos

Les travaux d'habilitation présentés dans ce mémoire ont été réalisés au Laboratoire d'Automatique, de Mécanique et d'Informatique Industrielles et Humaines UMR CNRS 8530 de l'Université de Valenciennes et du Hainaut Cambrésis, au sein de l'équipe Systèmes Homme-Machine (SHM) dirigée, jusque décembre 2004, par le Professeur Patrick Millot. Je tiens à lui exprimer ici toute ma reconnaissance de m'avoir accueilli au sein de son équipe et de la confiance qu'il m'a accordée depuis.

Je remercie vivement Monsieur Laurent Foulloy, Professeur à l'ESIA d'Annecy, Monsieur Francis Lepage, Professeur à l'Université Henri Poincaré de Nancy, et Monsieur Daniel Noyes, Professeur à l'ENIT de Tarbes de me faire l'honneur d'être rapporteurs de ce mémoire.

Je témoigne toute ma gratitude à Madame Mireille Bayart, Professeur à Polytech'Lille, Monsieur Jörg Schütte, Professeur à l'Université Technique de Dresde, Messieurs Christian Tahon et Christophe Delebarre, Professeurs à l'Université de Valenciennes, pour l'honneur qu'ils me font en siègeant à la commission d'examen.

Mes remerciements s'adressent également à Messieurs Jean Defrenne (retraité), Noël Malvache et Didier Willaeys, Professeurs à l'Université de Valenciennes pour m'avoir initié à cette thématique de recherche.

J'adresse une pensée des plus sincères à Monsieur Bernard Houriez, Professeur à l'Université de Valenciennes trop tôt disparu, et le remercie pour ses précieux conseils pendant les quatre années où je l'ai côtoyé en tant que moniteur de l'enseignement supérieur au sein de son département.

Mes plus vifs remerciements vont également à Monsieur Alain Lecocq, Professeur certifié en allemand.

Je remercie également toutes les personnes avec lesquelles j'ai travaillé (membres du GT Ciame, enseignants-chercheurs, ingénieurs, techniciens, doctorants, DEA, industriels...) et tout particulièrement Madame Mireille Bayart, animatrice du Ciame ainsi que Vincent Benard, Julie Beugin, René Mandiau, Bernard Philippe, Sylvain Piechowiak, Philippe Polet, Dominique Renaux, et Frédéric Vanderhaegen.

Résumé

La nécessité de prendre en considération les aspects sûreté de fonctionnement des systèmes automatisés, dès la phase de conception, pour tendre vers le concept de « systèmes automatisés sûrs de fonctionnement » représente aujourd'hui un enjeu majeur.

Nous présentons dans cette Habilitation à Diriger les Recherches le concept de systèmes automatisés sûrs de fonctionnement et procédons à une analyse de la problématique globale de la conception de tels systèmes. Nous identifions clairement les frontières des différents systèmes constituant les systèmes automatisés sûrs de fonctionnement : processus physique, systèmes d'automatisation, systèmes de sécurité, systèmes de contrôlabilité du risque (barrières). Pour ce faire, nous nous appuyons sur la notion de service rendu.

Nous introduisons ensuite les différents concepts de sûreté de fonctionnement des systèmes en dégageant deux grands niveaux : la sûreté de fonctionnement prédictive et la gestion de la sûreté de fonctionnement avec prise en compte des risques pour l'Homme et l'environnement. Cette étude aborde les aspects normatifs incontournables pour les systèmes industriels et décline notre point de vue sur la notion de complexité. L'identification de ces grands axes de recherche en conception des systèmes automatisés sûrs de fonctionnement nous permet de situer dans la communauté scientifique nos activités de recherche, dont les contributions et résultats sont présentés dans le mémoire selon deux axes :

- L'axe I porte sur la sûreté de fonctionnement de processus physiques avec une application à l'évaluation des paramètres FMD (Fiabilité-Maintenabilité-Disponibilité) des lignes de production dans le but d'en améliorer la performance,
- L'axe II porte sur la sûreté de fonctionnement des systèmes d'automatisation à intelligence distribuée avec la proposition d'une démarche de conception de tels systèmes et d'un formalisme pour la spécification des besoins et contraintes d'architecture, l'originalité de cette méthode repose sur la volonté d'obtenir une architecture validée par des paramètres de sûreté quantifiés.

De ces travaux découlent nos activités de recherche actuelles et futures relatives à l'analyse systémique de la sûreté de fonctionnement des systèmes complexes et à l'exploration de voies de recherche pour la proposition d'une méthodologie générique, indépendante du domaine d'application, pour la conception de systèmes complexes sûrs de fonctionnement.

Mots-Clés :

Modélisation de systèmes complexes, méthodes de conception, étude de sûreté, systèmes stochastiques, processus physique, systèmes d'automatisation, systèmes intelligents, systèmes distribués

Table des matières

Introduction Générale

L'objet de ce mémoire est de synthétiser mes activités de recherche, d'enseignement, et d'administration accomplies à l'Université de Valenciennes et du Hainaut Cambrésis (UVHC) depuis ma thèse de doctorat soutenue le 22 Novembre 1994.

Mes activités de recherche ont été initialement menées dans l'équipe Fiabilité Technique sous la direction du Professeur Jean Defrenne de 1991 à 1999, année de son départ en retraite ; puis sous la direction du Professeur Millot dans le Groupe de Recherche « Fiabilité Technique et Humaine » de l'équipe des Systèmes Homme-Machine, dont la direction a été cédée en décembre 2004 au Professeur Frédéric Vanderhaegen récemment nommé.

Mes travaux de doctorat ont porté sur l'évaluation de la sûreté de lignes de production – paramètres Fiabilité, Maintenabilité, Disponibilité – à partir d'informations asynchrones, datées, issues de sites répartis de contrôle/commande communicant au niveau terrain dans le but de détecter les causes de non-performance. Si de nombreux travaux de recherche sont menés pour aider l'opérateur humain dans sa tâche de supervision (synthèse et représentation des données, définition d'interfaces de communication Homme-Machine...), il est juste de remarquer que la qualité de son intervention dépend fortement des temps de réponse du système de remontée d'informations et de la pertinence des informations collectées. Or, la distribution sans cesse croissante des systèmes de contrôle/commande et la répartition géographique des moyens de production rendent difficile la collecte et le traitement en temps-réel des nombreuses informations.

La poursuite de ces travaux a mis en évidence la nécessité de prendre en considération les aspects sûreté de fonctionnement dès la phase de conception des systèmes automatisés pour tendre vers le concept de « *systèmes automatisés sûrs de fonctionnement* ». Une étude plus détaillée du contexte a montré la nécessité d'identifier les frontières des différents systèmes constituant les systèmes automatisés sûrs de fonctionnement – processus physiques, systèmes d'automatisation, systèmes de sécurité, systèmes de contrôlabilité du risque (notion de barrières) – en s'appuyant sur la notion de services rendus.

Deux grands niveaux se dégagent du concept de sûreté de fonctionnement des systèmes complexes : d'une part *la sûreté de fonctionnement prédictive* et d'autre part *la gestion des objectifs de sûreté* avec la prise en compte des risques pour l'Homme et l'environnement. Le premier niveau consiste en l'évaluation a priori des objectifs de sûreté ; le second niveau repose plutôt sur un jugement de valeur face à une prise de décision touchant une population de taille variable.

Les limites des méthodes classiques de la sûreté de fonctionnement, qui sont discutées dans ce mémoire, m'ont incité à prendre pour thème principal de recherche *l'élaboration de méthodes et modèles pour l'évaluation de la sûreté de fonctionnement de systèmes automatisés complexes*.

Dans un premier temps, mes activités de recherche se sont focalisées sur la *sûreté de processus physique* et plus particulièrement sur la modélisation de lignes de production. Ces travaux ont mis en évidence les problèmes liés à la complexité d'intégration des moyens et les difficultés rencontrées

pour atteindre les objectifs Fiabilité, Maintenabilité, Disponibilité du processus physique global caractérisant de fait la performance globale du système. Dans ce cas, la complexité repose sur le nombre important de moyens, de stocks intermédiaires et la multitude de paramètres à prendre en compte : vitesse, capacité de stocks, taux de défaillances et réparations des moyens.

Dans un deuxième temps, mes travaux se sont concentrés sur la *sûreté des systèmes d'automatisation.* Compte tenu de l'offre technologique actuelle qui induit de nouvelles possibilités pour les systèmes d'automatisation avec l'apparition d'instruments intelligents et de réseaux de communication, la recherche et les sciences de l'ingénierie doivent elles aussi conduire à de nouveaux apports permettant de construire et mieux cerner les problèmes, de faciliter la compréhension et la prise de décision à partir de modèles et de simulations.

Dans ce contexte, les travaux que j'ai menés ont conduit à la *proposition d'une démarche de conception* de systèmes d'automatisation pour atteindre les objectifs de sûreté de fonctionnement fixés par le cahier des charges. L'originalité de l'approche réside dans la complémentarité de trois classes d'architectures à distinguer lors de la conception : une architecture opérationnelle résultant de la projection d'une architecture fonctionnelle sur une architecture matérielle issue de choix matériels.

La volonté de mettre en œuvre cette démarche de conception m'a conduit à encadrer des travaux de DEA et de thèses qui ont abouti à la *proposition d'une méthode fonctionnelle dynamique* pour la spécification des besoins et contraintes d'architecture opérationnelle : contraintes dépendantes des spécifications fonctionnelles, contraintes dépendantes des spécifications matérielles, contraintes de sûreté qui dépendent à la fois de l'ingénierie « générale » du système, des spécifications matérielles et logicielles (topologie, choix des constituants, choix et type des systèmes de communication, temps de propagation, élaboration d'informations pertinentes, stratégiques et de sécurité...). L'aspect novateur repose sur la volonté de ne pas se limiter à une simple analyse fonctionnelle ; l'idée de base consiste à atteindre une phase de conception avancée avec l'obtention d'une architecture opérationnelle validée par des paramètres de sûreté quantifiés.

De ces travaux découlent mes activités de recherche actuelles et futures relatives à *l'analyse systémique de la sûreté de fonctionnement des systèmes complexes* et à l'exploration de voies de recherche pour la proposition d'une méthodologie générique, indépendante du domaine d'application, pour la conception de systèmes complexes sûrs de fonctionnement.

Ce mémoire est composé de deux grandes parties. La première partie présente un Curriculum Vitae détaillé décrivant mes activités à caractère scientifique, pédagogique et administratif.

La deuxième partie de ce mémoire positionne mon activité scientifique dans le contexte régional, national et international ; elle se décompose en trois chapitres :

- le premier chapitre procède à une analyse de la problématique globale de la conception de systèmes automatisés sûrs de fonctionnement,

- le deuxième chapitre présente mes activités de recherche, contributions et résultats sur la sûreté de fonctionnement des systèmes complexes automatisés avec, d'une part, l'étude de la sûreté de processus physiques avec une application aux lignes de production et, d'autre part, la sûreté de fonctionnement des systèmes d'automatisation à intelligence distribuée,

- le troisième chapitre aborde les principales perspectives de ces travaux en introduisant mon projet personnel de recherche et de pédagogie pour les années à venir.

Partie 1

Curriculum Vitae Étendu

Curriculum Vitae Étendu[1]

Présentation des activités de recherche, d'enseignement, et d'administration

1. Curriculum Vitae

Laurent CAUFFRIEZ

Nationalité française
Libéré des obligations militaires

Adresse Professionnelle :

Université de Valenciennes et du Hainaut-Cambrésis (UVHC)
LAMIH - UMR CNRS 8530
Le Mont Houy, 59313 VALENCIENNES Cedex 9 – France
Tél : 03.27.51.14.86 (Direct)
Tél : 03.27.51.13.50 (Secrétariat - Mme Oliveira)
Fax : 03.27.51.13.16
Email : Laurent.Cauffriez@univ-valenciennes.fr

[1] **Dans cette version PDF, le CV étendu est partiellement tronqué.**

2. Activités de recherche et encadrement scientifique

2.1 Thème de recherche

La démarche de conception d'un *système complexe automatisé sûr de fonctionnement* engendre de nombreuses réflexions scientifiques dans le domaine de l'automatique industrielle et humaine. La complexité revêt différents aspects si on la considère sous l'angle fonctionnel, structurel, comportemental et technologique. Les contraintes sont par ailleurs multiples : contraintes de sûreté, de performance, contraintes temporelles, logicielles, matérielles et technologiques ... Mes recherches dans ce domaine se focalisent sur la *caractérisation, l'évaluation et la quantification des paramètres fiabilité, disponibilité, maintenabilité et sécurité des systèmes* complexes automatisés.

Depuis 1991, mes activités de recherche ont consisté à « fiabiliser » les systèmes complexes automatisés. Mes travaux de recherche se sont principalement focalisés sur des modèles analytiques et événementiels pour évaluer les paramètres fiabilité, maintenabilité, disponibilité de processus physique. Une classe d'application particulièrement demandée par les industriels concerne les systèmes automatisés de production et plus particulièrement les lignes de production. La complexité du processus physique porte dans ce cas sur le nombre de moyens, de stocks intermédiaires et la multitude de paramètres à prendre en compte : vitesse, capacité des stocks avec leurs effets « mémoire », taux de défaillances et réparations des moyens.

La littérature du domaine montre que les modèles analytiques sont limités. Sur ce point, certains auteurs introduisent le terme « d'indécomposabilité » qui qualifie « *l'impossibilité de décomposer l'étude d'un système complexe en sous-systèmes dont les solutions exactes sont connues* » et prônent des méthodes approximatives à base d'heuristiques avec deux grandes tendances : *approche par agrégation (modélisation des parties du système pour tendre vers le système dans sa globalité)* et *approche par décomposition (modélisation qui part du système dans sa globalité pour tendre vers les parties)*. Dans ce contexte, mes recherches ont consisté à vérifier l'applicabilité des précédents modèles au diagnostic de non-performance. Cette non-performance se traduit par une mauvaise valeur des paramètres fiabilité, maintenabilité, disponibilité du système ; l'objectif est alors d'identifier les actions les plus pertinentes à mener et à quantifier les espoirs de gain selon le principe coût/bénéfice.

A partir de ces contributions sur la « fiabilisation » des processus physiques, mes recherches se sont orientées vers l'impact du « service rendu » par le système d'automatisation sur le comportement du processus physique : en effet, une faible disponibilité du système d'automatisation peut conduire à une faible disponibilité du processus physique selon le principe bien connu mode de défaillances/effets sur le système. Or l'apport de nouvelles technologies avec l'apparition de capteurs, actionneurs intelligents, de réseaux de terrain offre de nouvelles possibilités de par leurs facultés à percevoir, décider, agir, communiquer mais introduit également de nouvelles contraintes en terme de sûreté. Le problème de conception d'un système automatisé à intelligence distribuée peut se résumer par la question suivante : comment se traduit *l'agrégation des différentes fonctions du système en terme de disponibilité, fiabilité, maintenabilité et sécurité pour le système global* ? Mes recherches depuis 1994 partent du constat de l'absence de langages et d'outils pour la modélisation d'architectures abstraites obtenues par composition d'entités logicielles et matérielles. Elles contribuent ainsi à la spécification d'une démarche de conception de tels systèmes. Cette démarche repose sur la coexistence d'une démarche descendante (du tout vers les parties) et d'une démarche ascendante (des parties vers le tout) pour les activités de spécification et conception de la partie commande des systèmes automatisés.

L'originalité des travaux menés réside dans la complémentarité de trois classes d'architectures à distinguer lors de la conception : une architecture opérationnelle résultant de la projection de l'architecture fonctionnelle sur l'architecture matérielle issue de choix matériels. Le modèle obtenu par cette démarche doit permettre :

- *d'une part, la caractérisation, l'identification et la représentation des dépendances au sein de l'architecture opérationnelle (défaillances de mode commun).* Il s'agit d'une approche

qualitative visant à modéliser les sous-ensembles fonctionnels en intégrant dès la conception différentes contraintes telles que sûreté de fonctionnement, performances, contraintes temporelles, logicielles, matérielles et technologiques.

- *d'autre part, la quantification des paramètres de sûreté à des fins de validation de l'architecture opérationnelle en prenant en compte les aspects dynamiques*, c'est à dire représenter l'évolution des paramètres fiabilité, maintenabilité, disponibilité du système durant son cycle de vie, et ce dès la phase de conception. Il est en effet à déplorer que les études de la sûreté de fonctionnement soient encore trop souvent limitées au comportement stationnaire du système.

Compte tenu de la complexité stochastique des systèmes de grande taille, mes recherches se sont orientées vers les outils permettant d'appréhender cette complexité : la théorie du renouvellement et les simulations de Monte-Carlo ont fait l'objet d'une étude approfondie. La théorie du renouvellement a pour origine l'étude des « ensembles renouvelés » ; le renouvellement caractérise le remplacement d'un composant défaillant par un autre. Par extension, le renouvellement peut modéliser l'alternance état de fonctionnement/état défaillant d'un composant : après l'occurrence d'une défaillance le composant est renouvelé (par extension réparé) et se trouve alors en état d'assurer sa mission. L'intérêt d'une telle démarche réside dans la possibilité de modéliser les paramètres équivalents pour le système global à partir des densités de défaillance et de réparation des différentes entités qui le constituent et connaître leur évolution quelle que soit le type de loi de distribution utilisé : distribution normale, lognormale, de Weibull,... Les études réalisées ont cependant montré les limites de ce modèle analytique, dues aux nombreuses dépendances fonctionnelles, pour l'étude de la sûreté de fonctionnement des systèmes complexes.

Mes recherches se sont alors orientées vers une approche systémique en se focalisant sur les simulations de Monte Carlo. La simulation de Monte Carlo est à l'heure actuelle l'outil le plus prometteur pour mener à bien une analyse de la fiabilité et de la disponibilité de systèmes complexes. Cet outil est fort usité dans le domaine du nucléaire et repose sur une modélisation mathématique du comportement du système grâce à une équation générale d'état ; le principe de base repose sur une simulation dans l'espace temporel doublée d'une simulation dans l'espace d'états.

Le modèle de l'architecture opérationnelle couplé à cet outil doit permettre d'améliorer toute architecture opérationnelle par une analyse de « sensibilité » de l'architecture sur deux points : *analyse de sensibilité au niveau des taux de défaillances/réparations* des entités logicielles et matérielles, *analyse de sensibilité au niveau de la structure du système* par ajout ou suppression d'entités qui peut se traduire par une augmentation ou une diminution des paramètres fiabilité et disponibilité du système. Le concepteur d'une architecture opérationnelle doit ainsi se voir offrir les moyens d'identifier le gain/coût et juger de la nécessité d'investir dans des entités redondantes ou de sécurité (automate de sécurité par exemple) pour atteindre les objectifs de sûreté fixés. Il doit en outre également avoir la possibilité de valider l'architecture opérationnelle par rapport aux dépendances fonctionnelles et matérielles, dont la prise en compte est absolument nécessaire pour l'obtention de résultats pertinents.

Mots clés :
Modélisation de systèmes complexes, méthodes de conception, étude de sûreté, systèmes stochastiques, processus physique, systèmes d'automatisation, systèmes intelligents, systèmes distribués

6. Liste des publications

6.1 Revues d'audience Nationale et Internationale (7 dont 3 parues, 2 acceptées et 2 en évaluation)

[1] Cauffriez, L., Defrenne, J. (1995). Viabilité de l'information et réseau à diffusion : deux atouts pour la prise de décision dans un système réparti de contrôle/commande tolérant les fautes. Revue Européenne de Sûreté de Fonctionnement et de Diagnostic, Vol 5/2, (pp. 219-247), Hermès. ISSN 1166-3049. Référencée en bibliographie [Cauffriez & al., 1995]

[2] Cauffriez, L., Willaeys, D., Defrenne, J. (1997). Mesure des indicateurs de performances de lignes de production : présentation d'une méthode et retour d'expérience. Journal Européen des systèmes Automatisés Vol. 31/8, (pp.1297-1310), Hermès. ISSN 0296-1598. Référencée en bibliographie [Cauffriez & al., 1997]

[3] Cauffriez, L., Ciccotelli, J., Conrard, B., Bayart, M. (2004). Design of intelligent distributed control systems: A Dependability point of view. Journal of Reliability Engineering and System Safety. (pp.19-32).Vol 84/1, April. Elsevier. ISSN 0951-8320. Référencée en bibliographie [Cauffriez & al., 2004]

[4] Cauffriez, L., Willaeys, D. (Acceptée le 26 janvier 2005) A predictive model for performance diagnosis of line production. The international Journal of Advanced Manufacturing Technology. Springer. Référencée en bibliographie [Cauffriez & al., 2005]

[5] Cauffriez, L., Benard, V., Renaux, D. (Acceptée le 24 août 2005) A new formalism for designing and specifying RAMS parameters for safe complex distributed control systems : the Safe-SADT formalism, IEEE Transactions on Reliability. Référencée en bibliographie [Cauffriez & al., 2005b]

[6] Cauffriez, L., Willaeys, D. (Soumise en octobre 2003, révisée en septembre 2005 suite au reviewing). Towards a Predictive Model for Production Line Performance Diagnosis. Control Engineering Practice. Référencée en bibliographie [Cauffriez & al., 2003]

[7] Benard, V., Cauffriez, L., Renaux, D. (Soumise le 11 mai 2005) The Safe-SADT method for aiding designers to choose and improve dependable architectures for complex automated systems, Journal of Reliability Engineering and System Safety, Elsevier. Référencée en bibliographie [Benard & al., 2005]

6.2 Revue de vulgarisation (1 parue)

[1] Bayart M., Robert, M., Benoit, G., Cauffriez, L., & al. (1998). Dans la jungle des réseaux de Terrain. : Vers un guide de choix dédié « Automatisation d'applications. (pp. 44-48). Revue de l'Electricité et de l'Electronique, n°3. ISSN 1265-6534. Référencée en bibliographie [Bayart & al., 1998]

6.3 Livre et chapitres d'ouvrages (1 livre paru, 2 chapitres à paraître)

[1] Cauffriez, L. (1999). Sous la direction de L. Cauffriez, Ciame, Tome 1 : Réseaux de terrain - Description et critères de choix. CIAME, 204 pages, Paris, Hermès. ISBN 286601-7242. Référencé en bibliographie [Cauffriez & al., 1999c]

[2] Cauffriez, L., Conrard, B. (à paraître en 2005). Chapitre 2 : « Généralité sur la sûreté de fonctionnement ». Dans Tome 2 : Réseaux de terrain - Problématique et Sûreté de Fonctionnement, CIAME, Sous la direction de M. Bayart, Paris, Hermès. Référencé en bibliographie [Cauffriez & al., 2005c]

[3] Cauffriez, L., Ciccotelli, J. (à paraître en 2005). Chapitre 4 : « Approche réseau ». Dans Tome 2 : Réseaux de Terrain - Problématique et Sûreté de Fonctionnement, CIAME, Sous la direction de M. Bayart., Paris, Hermès. Référencé en bibliographie [Cauffriez & al., 2005d]

6.4 Congrès internationaux avec actes et comité de lecture (19 publiés)

[1] Cauffriez, L., Willaeys, D., Defrenne, J. (1993). A new method to compute programmed logic functions in real-time applications : The Event-Triggered Method, IEEE/SMC'93, International Conference on "Systems, Man and Cybernetics", Proceedings Vol. 3, (pp. 210-215), October 17-20, Le Touquet, France, 1993. Référencé en bibliographie [Cauffriez & al., 1993]

[2] Cauffriez, L., Defrenne, J., Willaeys, D. (1995). A tool to measure in real-time the production performances of automated manufacturing shop systems, International Conference on Industrial Automation, Proceedings Vol. 2, (pp. 433-438), June 7-9, Nancy, France. Référencé en bibliographie [Cauffriez & al., 1995b]

[3] Cauffriez, L., Willaeys, D., Defrenne, J. (1996). A method and a Diagnosis System to value the Production Performances of Manufacturing Flow-Line Systems, International Conference on "Systems, Man and Cybernetics", IEEE/SMC CESA'96 IMACS Multiconference, Proceedings Vol. 2 , (pp. 814-819), July 9-12, Lille, France. 1996. Référencé en bibliographie [Cauffriez & al., 1996]

[4] Cauffriez, L., Defrenne, J. (1997). An Experimental Platform for the Reliability-Availability Evaluation of Intelligent distributed Systems, IFAC SICICA'97, 3rd International Conference Symposium on Intelligent Components and Instruments for Control Applications, (pp. 591-596), June 9-11, Annecy, France. Référencé en bibliographie [Cauffriez & al., 1997b]

[5] Philippe, B. Cauffriez, L. (1999) Une architecture objet basée sur un réseau CAN : Application à la description d'un robot mobile, INNOCAP 99, European Symposium sensor networks and communications, (pp. 87-92). 28-29 Avril 1999, Grenoble, France. Référencé en bibliographie [Philippe & al., 1999]

[6] Cauffriez, L., Defrenne, J. (1999). Influence upon the Temporal Coherence of Informations of Medium Access Control Method and Adressage Mode by fieldbusses, International Conference on Industrial Automation, June 7-9. (pp 20.1-20.4). Montréal, Canada. ISBN 2-9802946-2-4. Référencé en bibliographie [Cauffriez & al., 1999b]

[7] Renaux, D., Cauffriez, L. (1999) Equivalent Failure Rate Assessment in case of Periodically Tested Systems, ESREL'99 Tenth European Conference on Safety and Reliability, (pp 1573-1578), September 13-17, Münich-Garching, Germany. ISBN 9058091090. Référencé en bibliographie [Renaux & al., 1999]

[8] Cauffriez, L., Philippe, B. (1999). Classification of Medium Access Control Method, Adressage Mode and Type of Trafic by fieldbusses., International Conference on Industrial Automation. (pp. 19.13-19.16). Montréal – Canada. ISBN 2-9802946-2-4. Référencé en bibliographie [Cauffriez & al., 1999]

[9] Berger, T., Cauffriez, L., Deneux, D., Popieul, J-C., Sallez, Y. (2000). Retour d'une expérience de pédagogie par projet : mise en œuvre intégrale d'une cellule flexible en école d'ingénieur.

CIFA'2000, Conférence Internationale Francophone d'Automatique. (pp. 600-605). Lille, France. ISBN 2-9512309-1-5. Référencé en bibliographie [Berger & al. 2000]

[10] Renaux, D., Cauffriez, L., Aramini, S. (2001). Quantification du coût des défaillances, Méthode de l'arbre de causes-coûts. In (Ed.), Qualita 2001 4ème congrés international pluridisciplinaire. (pp. 328-333). Mars, Annecy, France. ISBN 2-9516453-0-9. Référencé en bibliographie [Renaux & al. 2001]

[11] Benard, V., Cauffriez, L., Renaux, D. (2001). Point of view of availability assessment for complex system: A method based onto transfer function, International Conference IFAC-INCOM'01, Vienna, Austria, 20-22 Sept 2001, CDRom. Référencé en bibliographie [Benard & al., 2001]

[12] Renaux, D., Cauffriez, L., Aramini, S. (2001). Application of the Cause-cost tree methodology for the evaluation of a failure cost. In (Ed.), International Conference European Safety and Reliability ESREL 2001. (pp. 293-300). September, Turin, Italie, ISBN 88-8202-099-1, Eds Zio Demichela Piccinini. Référencé en bibliographie [Renaux & al., 2001b]

[13] Benard, V., Cauffriez, L., Renaux, D. (2002). Modélisation des paramètres de la sûreté de fonctionnement par des fonctions de transfert : Application à la disponibilité. In (Ed.), CIFA 2002, CDRom. Juillet, Nantes, France. Référencé en bibliographie [Benard & al., 2002]

[14] Renaux, D., Cauffriez, L., Benard, V., (2002). Towards an optimal production cost. In (Ed.), European Conference on System Dependability and Safety, ESREL 2002. (pp. 218-223). March, Lyon, France. Référencé en bibliographie [Renaux & al. 2002]

[15] Renaux, D., Beugin, J., Cauffriez, L. (2003). Proposal for a neural network approach and ordering heuristic for the fault tree evaluation, European Safety and Reliability Conference ESREL 2003. (pp.1301-1306). June, Maastricht, Nederland, ISBN 9058095517, Eds Bedford & van Gelder. Référencé en bibliographie [Renaux & al., 2003]

[16] Cauffriez, L., Conrard, B., Thiriet, J-M., Bayart, M. (2003). Fieldbuses and their influence on Dependability, 20th IEEE Instrumentation and Measurement Technology conference, IEEE/IMTC2003, (pp.83-88). Vail (Colorado, United Sates), 20-22nd May 2003. ISBN 0-7803-7705-2 SSN 1091-5281. Référencé en bibliographie [Cauffriez & al., 2003b]

[17] Benard, V., Cauffriez, L., Renaux, D., (2004). Dependability evaluation of complex systems based on a functional dynamic model : the Safe-SADT Method, Conférence Internationale EuroSim'04, Paris, Septembre 2004, CDRom. Référencé en bibliographie [Benard & al. 2004]

[18] Beugin, J., Renaux, D., Cauffriez, L., (2005). A SIL quantification approach in complex systems of guided transport, European Safety and Reliability Conference ESREL 2005. 27-30 June, Tri City, Poland, acceptée. Référencé en bibliographie [Beugin & al., 2005b]

[19] Beugin, J., Renaux, D., Cauffriez, L., (2005). A safety assessment method for guided transport systems : a dynamic approach using Monte Carlo and discrete event simulations, 17th IMACS World Congress, Paris, 11-15 July, 2005. Référencé en bibliographie [Beugin & al., 2005]

6.5 Colloques francophones avec actes et comité de lecture

[1] Beugin, J., Renaux, D., Cauffriez, L., (2003). Modélisation d'arbres de fautes par réseaux neuronaux pour l'évaluation de la sûreté de systèmes complexes, Colloque Francophone PENTOM 2003. (pp 315-327). Valenciennes, 26-28 Mars 2003, Eds PUV Valensciences n°2, ISBN 2-905725-51-6. Référencé en bibliographie [Beugin & al., 2003]

[2] Benard, V., Cauffriez, L., Renaux, D. (2003). Proposition d'un modèle probabiliste pour l'évaluation de systèmes non markoviens sûrs de fonctionnement, Colloque Francophone PENTOM 2003. (pp 347-361). Valenciennes, 26-28 Mars 2003, Eds PUV Valensciences n°2, ISBN 2-905725-51-6. Référencé en bibliographie [Benard & al., 2003]

[3] Renaux, D., Beugin, J., Cauffriez, L. (2005). Allocation et évaluation globale de la sécurité d'un système : Application aux systèmes guidés. Pentom 2005. (pp. 289-303). Marrakech (Maroc), 18-21 Avril 2005. Référencé en bibliographie [Renaux & al., 2005]

6.6 Communication invitée

[1] Cauffriez, L., Beugin, J., Renaux, D., Millot, P. (2003). Design of Urban Guided Trasnport Management System : A dependability point of view, Deliverable D6, Safety conceptual approach & guidelines, 5th Framework Programme, Contract GRD2-2000-30090, pp70-75. Référencée en bibliographie [Cauffriez & al., 2003c]

6.7 Rapports de contrats

[1] Cauffriez, L., Defrenne, J. (1994). In Rapport final du projet MESR 2033, « Impact de l'émergence des réseaux de terrain et de l'instrumentation intelligente dans la conception des systèmes d'automatisation de processus », Ministère de l'Enseignement Supérieur et de la Recherche, pp 39-44 et pp 87-90, Paris. Référencé en bibliographie [Cauffriez & al., 1994]

[2] Aramini, S., Renaux, D., Cauffriez, L., Defrenne J., Willaeys, D., (1996) Rapport de contrat, Renault-LAMIH, Juin 1996. Référencé en bibliographie [Aramini & al., 1996]

[3] Patchong, A., Cauffriez, L., Willaeys D., Defrenne, J. (1996). Diagnostic pour l'amélioration d'un atelier de production : le cas de l'atelier ferrage de Sevelnord, Rapport de contrat LAMIH-Sevelnord, Juin 1996, Valenciennes. Référencé en bibliographie [Patchong & al., 1996]

[4] Benard, V., Cauffriez, L., (2001). Méthode et modèle pour l'évaluation de la sûreté de fonctionnement des systèmes complexes en phase de conception - Application à la conception des Systèmes de Transport, Rapport CNRS d'avancement n°1, Université de Valenciennes, 2001, Référencé en bibliographie [Benard & al., 2001b]

[5] Benard, V., Cauffriez, L., (2002). Méthode et modèle pour l'évaluation de la sûreté de fonctionnement des systèmes complexes en phase de conception - Application à la conception des Systèmes de Transport, Rapport CNRS d'avancement n°2, Université de Valenciennes, 2002, Référencé en bibliographie [Benard & al., 2002b]

[6] Cauffriez, L., Renaux, D., Vanderhaegen, F. (2003). Deliverable D6, Safety conceptual approach & guidelines, 5th Framework Programme, Contract GRD2-2000-30090, Urban Guided Transport Management System, pp 2-76, Paris. Référencé en bibliographie [Cauffriez & al., 2003e]

[7] Cauffriez, L., Renaux, D., Vanderhaegen, F. (2003). Deliverable D4 Report on Users Group and Network of Universities Activities, 5th Framework Programme, Contract GRD2-2000-30090, Urban Guided Transport Management System, pp 2-17, Paris. Référencé en bibliographie [Cauffriez & al., 2003d]

Chapitre 1

Sûreté de fonctionnement des systèmes automatisés :

Analyse de la problématique globale

Introduction

Nous abordons ici la deuxième partie de ce mémoire dont l'objectif est de présenter mes travaux de recherche sur la sûreté de fonctionnement des systèmes complexes automatisés. Dans ce chapitre, je présente le concept de « systèmes automatisés sûrs de fonctionnement » et procède à une analyse de la problématique globale de la conception de tels systèmes.

Dans un premier temps, j'identifie clairement les frontières des différents systèmes constituant les systèmes automatisés sûrs de fonctionnement : processus physique, systèmes d'automatisation, systèmes de sécurité, systèmes de contrôlabilité du risque. Pour ce faire, je m'appuie sur la notion de service rendu. Cette phase préliminaire est indispensable pour mener à bien une étude de sûreté de fonctionnement.

J'introduis ensuite les différents concepts de sûreté de fonctionnement des systèmes en dégageant deux grands niveaux : la sûreté de fonctionnement prédictive et la gestion de la sûreté de fonctionnement avec prise en compte des risques pour l'Homme et l'environnement.

Enfin, je mets l'accent sur les grands axes de recherche en conception de systèmes automatisés sûrs de fonctionnement : conception de processus physiques sûrs, conception de systèmes d'automatisation sûrs, conception de systèmes de sécurité sûrs et conception de systèmes de contrôlabilité du risque (barrières) sûrs de fonctionnement. Cette étude prend en compte les aspects normatifs incontournables pour les systèmes industriels et décline mon point de vue sur la notion de complexité.

L'identification de ces grands axes de recherche en conception des systèmes automatisés sûrs de fonctionnement me permet de situer dans la communauté scientifique mes activités de recherche, dont les contributions et résultats sont présentés au chapitre 2 de cette deuxième partie de mémoire selon deux axes :

- L'axe I porte sur la sûreté de fonctionnement de processus physiques avec une application à l'évaluation des paramètres FMD (Fiabilité-Maintenabilité-Disponibilité) des lignes de production dans le but d'en améliorer la performance,
- L'axe II porte sur la sûreté de fonctionnement des systèmes d'automatisation à intelligence distribuée avec la proposition d'une démarche de conception de tels systèmes et d'un formalisme pour la spécification des besoins et contraintes d'architecture, l'originalité de cette méthode repose sur la volonté d'obtenir une architecture validée par des paramètres de sûreté quantifiés.

Dans le chapitre 3, j'introduis les principales perspectives de mes travaux en présentant mon projet personnel de recherche et de pédagogie pour les années à venir.

1.1 Notions de systèmes automatisés

Il existe de nombreuses approches pour définir et caractériser le concept de systèmes. L'approche de [Lemoigne, 1994] vise à caractériser un système général par sa nature (quel système est- ce ?) et par l'action qui lui est appliquée (quelle est son utilisation ?).

La perception d'un système est par ailleurs différente en fonction du référentiel retenu pour le caractériser, vue interne/externe, logique/physique [Trentesaux, 2002] :

- la vue externe définit la mission du système et caractérise son interaction avec l'environnement,
- la vue interne décrit l'activité (fonctions), la structure (agencement d'organes internes) et l'évolution du système (évolutivité, adaptativité, auto-apprentissage, auto-organisation, auto-configuration, auto-finalisation [Lemoigne, 1994]),
- la vue logique s'attache au traitement de l'information et fait partie intégrante de la vue interne,
- la vue physique considère le traitement de matière et d'énergie.

Je propose à la figure 1.1 un modèle de systèmes automatisés reprenant ces différentes notions de vues physiques, internes, externes. Ce modèle met en évidence l'interaction que le système a avec son environnement et illustre l'aboutissement à une situation critique lourde de conséquences telles que dégradation ou perte du système, dommages subis par les personnes, dommages subis par les biens, impact sur l'environnement.

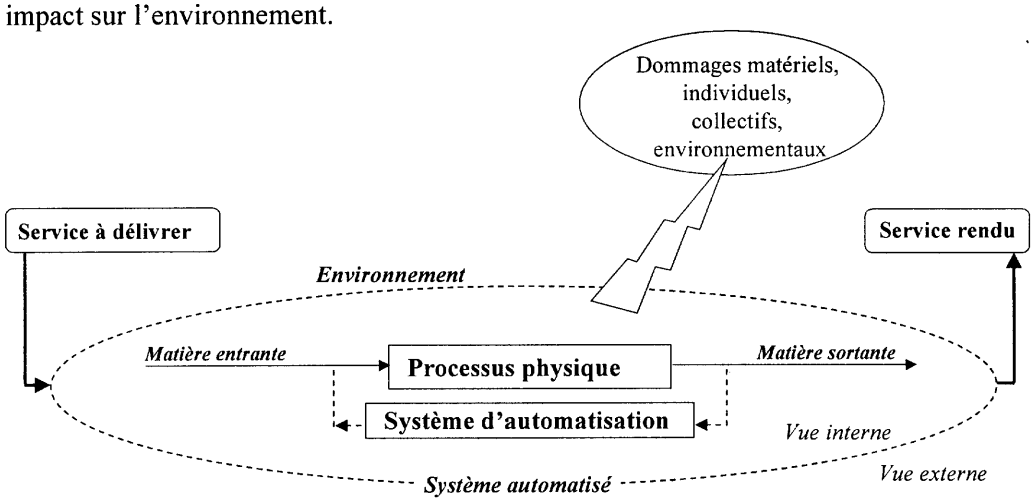

Figure 1.1 Vues internes et externes de systèmes automatisés

Le processus physique modélise l'entité où les flux de produits subissent des transformations. Il comprend des équipements, des machines, des postes de charge qui réalisent les différentes phases des gammes de fabrication et apportent une valeur ajoutée aux produits fabriqués.

Le système d'automatisation a pour but de contrôler les transformations réalisées par le processus physique [Staroswiecki & al., 1994]. Ce contrôle est réalisé au niveau du terrain par des capteurs et actionneurs qui modulent certaines variables du processus : pression, débit, position d'une pièce, vitesse rotation d'une machine, etc...

Le service rendu par le système d'automatisation est de fournir :

- des services de pilotage au processus physique,
- des aides à l'exploitation pour les opérateurs humains via un interface Homme/Machine.

Il est possible de structurer les fonctions d'un système automatisé, différents modèles ont été proposés en ce sens.

Le modèle introduit par [Bayart, 1994] spécifie les frontières du système d'automatisation (cf. figure 1.2). Dans ce modèle, les opérateurs n'appartiennent pas au système d'automatisation ; le système d'automatisation est dans cette approche considéré comme un interface entre le processus physique et les opérateurs.

Le modèle élaboré par [Verlinde, 1989] pour les systèmes d'automatisation structure les fonctions du système d'automatisation selon 4 grandes pyramides rappelant une certaine hiérarchie ainsi qu'une abstraction des informations synthétisées (cf. figure 1.3) :

- la fonction Conduire est destinée à contrôler le processus pour atteindre les objectifs tant du point de vue de la qualité que du point de vue de la productivité,
- la fonction Maintenir correspond à la mise en œuvre de moyens permettant d'assurer le respect du paramètre maintenabilité en appliquant les procédures et moyens prescrits, elle contribue à assurer une disponibilité maximale du système automatisé,
- la fonction Suivre est destinée à archiver et synthétiser les informations relatives à l'état du processus physique et des produits,
- la fonction Sécuriser est destinée à assurer la non-occurrence de défaillances mineures ou catastrophiques ; ces dernières pouvant mettre en danger les hommes, l'environnement, le processus physique ou les produits.

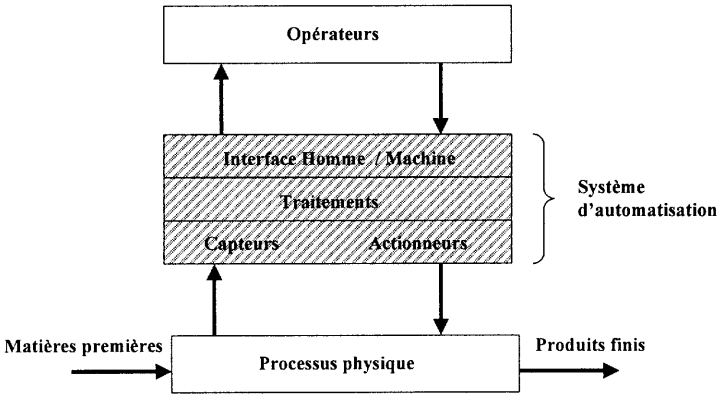

Figure 1.2 Frontières du système d'automatisation d'après [Bayart, 1994]

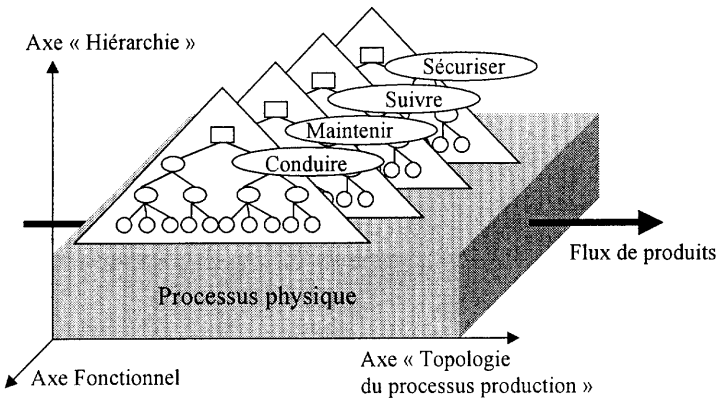

Figure 1.3 Modèle de Système Automatisé d'après [Verlinde, 1989]

Lorsqu'on intègre les aspects sûreté de fonctionnement, il convient de structurer les fonctions du système automatisé en précisant les services offerts et en délimitant les frontières, ce qui permet de clarifier les différents niveaux de protection.

Je propose ainsi le modèle de la figure 1.4 qui met en évidence les différents niveaux de sûreté d'installations automatisées et s'interprète comme suit :

- si le système d'automatisation fait l'objet de dysfonctionnements, des incidents (événements de peu d'importance) surviennent,
- si le système de sécurité ne peut gérer ces incidents, des accidents (événements dommageables) surviennent au niveau de l'installation,
- si les procédures de sécurité sur site n'arrivent pas à contrôler l'accident et que les barrières défaillent, l'accident s'étend à l'environnement,
- si les procédures de sécurité hors site n'arrivent pas à gérer la situation, cela implique des conséquences pour la collectivité et l'environnement.

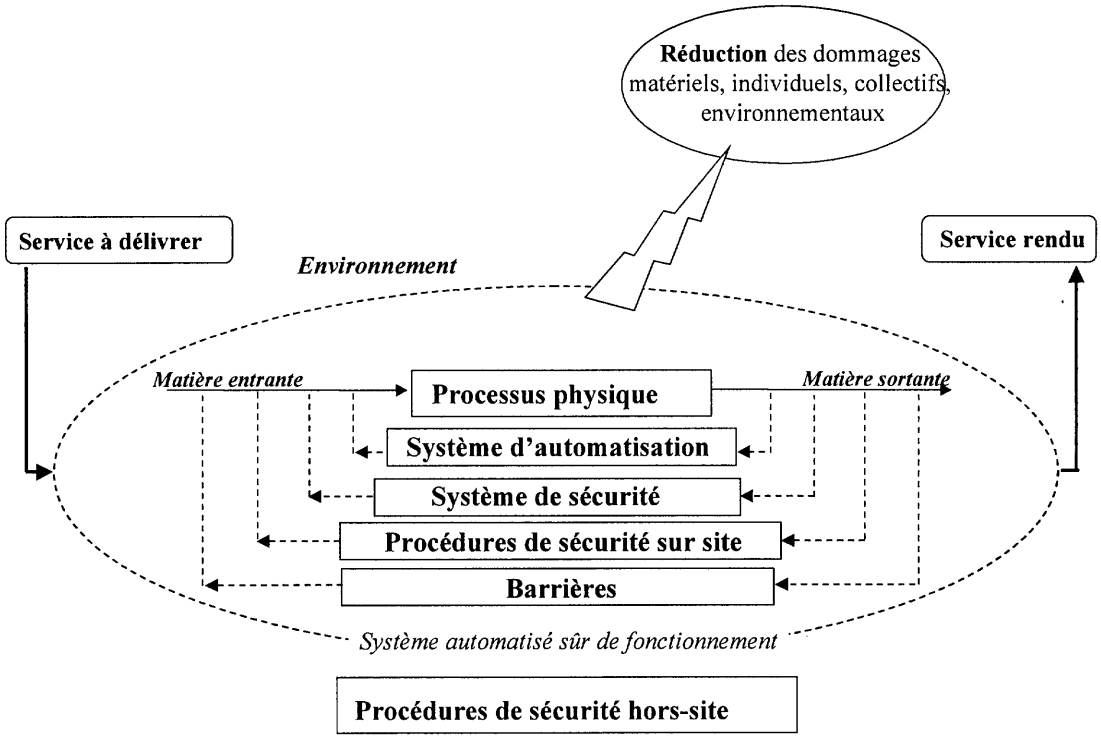

Figure 1.4 Niveaux de protection d'un système automatisé sûr de fonctionnement

1.2 Notions de sûreté de fonctionnement

La sûreté de fonctionnement correspond à une démarche qualité. Lorsque les objectifs sont identifiés, le problème de sûreté de fonctionnement est plus facile à appréhender. Deux niveaux sont à distinguer dans la démarche retenue pour atteindre ces objectifs :

- le premier niveau s'attache à la *sûreté de fonctionnement prédictive* et consiste en l'évaluation a priori des objectifs de sûreté. Ce niveau correspond plutôt à une démarche scientifique, technique, formelle, quantitative et objective. Il a pour but d'énumérer les différentes situations possibles et d'en quantifier la probabilité d'occurrence. Ainsi, face à une situation donnée, sont identifiés les différents profils de sûreté : énumération des séquences d'événements qui peuvent conduire à un événement redouté, identification des

modes de confinement des défaillances, calcul des probabilités d'occurrence et des durées, identification des procédures de sécurité, identification des conséquences pour le matériel, l'Homme et l'environnement en cas de défaillance des mécanismes de confinement.

- le second niveau consiste en *la gestion des objectifs de sûreté*. Ce niveau repose plutôt sur un jugement de valeur, sur des heuristiques et est plutôt d'ordre subjectif, qualitatif, social et politique face à une prise de décision touchant une population de taille variable : une seule personne, un petit groupe d'individus, plusieurs millions de personnes (manière dont les industriels et politiques ont géré la crise de la légionellose dans le Nord-Pas-de-Calais, ou de la vache folle en France). A ce niveau, les prises de décision se font souvent par rapport à une fonction de coût (financière ou autre) telle que gain/perte, risque/coût, risque/coût/bénéfice.

Les objectifs de sûreté peuvent être spécifiés en terme de grandeurs variées telles que fiabilité, maintenabilité, disponibilité, sécurité et risque [Laprie & al., 1995]. Le paragraphe suivant rappelle brièvement ces différentes notions.

1.2.1 Fiabilité, Maintenabilité, Disponibilité, Sécurité et Risque

1.2.1.1 La Fiabilité (Reliability)

La fiabilité est l'aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné [X60500, 1988].

La fiabilité est donnée par la probabilité qu'une entité E accomplisse une fonction requise, dans des conditions données et pendant une durée donnée :

$$R(t)=P\{\text{ E fonctionne sur } [0,t[\ \}$$

L'expression mathématique de R(t) repose généralement sur l'hypothèse que l'entité est en fonctionnement au temps t=0 ou, plus généralement, que l'entité est supposée en état d'accomplir la fonction requise au début de l'intervalle de temps donné.

1.2.1.2 La Maintenabilité (Maintainability)

La maintenabilité est dans des conditions données d'utilisation, l'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 [X60500, 1988].

La maintenabilité est la probabilité qu'une entité E soit réparée après une durée donnée, l'entité étant en panne à l'instant t=0 :

$$M(t)=P\{\text{ E est réparée sur } [0,t[\ \}$$

Cette notion concerne les systèmes réparables. Une entité est donc maintenable si elle est réparable et s'il existe des procédures et des moyens de maintenance.

1.2.1.3 La Disponibilité (Availability)

La disponibilité est l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné, en supposant que la fourniture des moyens extérieurs nécessaires soit assurée [X60500, 1988].

La disponibilité correspond ainsi à la probabilité d'une entité E a être en état d'accomplir une fonction requise, dans des conditions données et à un instant donné :

$$A(t) = P\{ \text{E non défaillante à l'instant t} \}$$

Cette aptitude est fonction d'une combinaison de la fiabilité, de la maintenabilité et de la politique de maintenance de l'entité. La carence des moyens extérieurs nécessaires autres que les moyens de maintenance n'est pas à prendre en compte dans le concept de disponibilité [X60500, 1988]. Quand t tend vers l'infini, on parle alors de disponibilité asymptotique $A(t\rightarrow\infty)$, correspondant à la disponibilité en régime permanent. Pour une entité non-réparable, on a que $A(t)=R(t)$.

1.2.1.4 La sécurité (safety)

La sécurité est l'aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques [Villemeur, 1988]. Il y a lieu de distinguer plusieurs définitions du terme sécurité [Laprie & al., 1995].

a) Sécurité - Confidentialité/Intégrité (Security/Integrity)

La sécurité-confidentialité est l'aptitude à prévenir l'occurrence de divulgations non-autorisées de l'information.

La sécurité-intégrité est l'aptitude à prévenir l'occurrence d'altérations inappropriées des produits, des processus et de l'information.

b) Sécurité – Innocuité (Safety)

La sécurité-innocuité est l'aptitude à prévenir l'occurrence de conséquences catastrophiques pour l'environnement.

Dans le domaine de la sécurité relative aux machines, c'est l'aptitude d'une machine à accomplir sa fonction, à être transportée, installée, mise au point, entretenue, démontée et mise au rebut dans les conditions d'utilisation normale spécifiées dans la notice d'instructions sans causer de lésion ou d'atteinte à la santé [EN292, 1997]. Le tableau 1.1 présente les conséquences classées par niveaux de gravité [Sourisse & al.,1996].

Niveau de gravité	Dégradation ou perte du système	Dommages subis par les personnes	Dommages subis par les biens	Impact sur l'environnement
I	Gêne au bon fonctionnement	Aucun dommage	Aucun dommage	Aucun impact
II	Fonctionnement perturbé	Dommages légers (arrêt de travail)	Pas de dommage notable	Léger impact
III	Perte possible de la fonction	Dommages graves (risque d'incapacité permanente)	Dommages significatifs	Impact significatif
IV	Perte certaine de la fonction	Dommages très graves (risque de mort)	Dommages importants	Impact important voire très important

Tableau 1.1 : Classement des aboutissements en quatre catégories

Pour [Kumamoto & al., 1996], la sécurité est à regarder comme inversement proportionnel au risque, ces deux termes sont ainsi interchangeables. Selon lui, la sécurité s'applique à des personnes soumises à des pertes potentielles :

- une alternative avec moins de risque est ainsi considérée plus sécuritaire,
- un équipement avec une plus grande fiabilité est supposé augmenter la sécurité.

Le risque dépend de l'évaluation gain/perte au niveau des personnes impliquées [Maccrimmon & al., 1986]. A noter qu'une entreprise investissant trop dans la sécurité peut faire face à un autre risque : la faillite. Un recensement des méthodes et techniques exploitables en gestion des risques est présenté dans [Noyes & al., 2001] ; cette classification présente l'avantage de mettre en évidence les fonctions dominantes réalisées par ces outils et a conduit à une proposition de fiches descriptives pour le chaînage d'outils pour l'analyse de risques.

1.2.1.5 Notion de risques [Kumamoto & al. , 1996]

Lors de la conception d'un système d'automatisation, l'évaluation des objectifs de sûreté de fonctionnement nécessite une analyse de profil de risques afin d'identifier les différentes alternatives de solution.

Le profil de risque se définit par un quintuplé :

Profil de risque de l'alternative $_i$ = (Vraisemblance$_i$, Conséquence$_i$, Significativité$_i$, Scenario Causal$_i$, Population$_i$)

- la vraisemblance **V** caractérise une mesure d'apparition du risque pour l'alternative étudiée « i ». Il peut s'agir d'une probabilité par action, d'une densité par unité de temps, d'une fréquence sur la durée de vie, d'un ratio pendant un intervalle de temps, d'une probabilité qualitative (fréquent, plausible, possible, rare), d'un pourcentage par demande, par opération ou par distance,
- la conséquence **C** désigne la situation vers laquelle on tend avec le profil de risque considéré « i ». Il peut s'agir de décès, d'incapacité permanente, d'arrêt de travail ou de bénignité,
- la significativité **S** s'applique à la conséquence de l'alternative « i » et constitue une mesure unifiée pour comparer les alternatives entre-elles et retenir une solution satisfaisante à défaut d'optimale,
- le scénario causal **SC** est une aide à la quantification de la vraisemblance et de la significativité de l'alternative « i ». Cette quantification se fait en effet plus aisément lorsque l'étude peut s'appuyer sur un scénario causal identifiant les différents chemins qui mènent à la conséquence « i ». Les méthodes bien connues d'arbres de conséquences ou d'arbres des causes s'y prêtent aisément [Villemeur, 1988],
- la population **P** désigne les personnes exposées pour l'alternative « i ». Il peut s'agir d'un risque individuel (lorsqu'une seule personne est exposée), d'un risque collectif (atelier d'une usine, voisinage aux alentours d'une entreprise chimique ou nucléaire), national ou mondial.

Remarques :

- d'un point de vue plus général, le risque R est caractérisé par un ensemble de « n » quintuplés (indice i variant de 1 à n) correspondant à la déclinaison des alternatives de risque dont une particularité est que la somme des vraisemblances est égale à l'unité quelle que soit la métrique retenue (probabilité, pourcentage, ...).
  $R = \{ (V_1, C_1, S_1, SC_1, P_1),.....(V_i, C_i, S_i, SC_i, P_i),....., (V_n, C_n, S_n, SC_n, P_n) \}$

- risque individuel et risque collectif sont à examiner de près en fonction de la taille de la population exposée qui a un effet important sur le risque collectif encouru : soit un risque individuel de 10^{-6} décès par an ; si 1000 personnes sont exposées à ce risque, le risque collectif est de 10^{-3} décès par an alors que ce même risque individuel appliqué à la population française de 61 millions conduit à un risque collectif de 61 décès par an.

- une même conséquence peut conduire à une prise de décision différente lors de la gestion des objectifs de sûreté de fonctionnement :
  1. soit un risque individuel sur une période donnée de 10^{-6} décès, appliqué aux 61 millions de Français[1], cela conduit à une conséquence de 61 décès qui est acceptable en comparaison des 550000 décès[1] par an.
  2. soit la totalité des 61 employés d'une entreprise décimée par cancer sur une période donnée à cause de produits cancérigènes confinés dans l'entreprise, le risque individuel est alors de 1 et cette conséquence de 61 décès est inacceptable bien que le nombre de décès total soit identique au cas précédent.

- il est bien connu que l'opinion publique a une attitude ambivalente devant des situations dramatiques : les journaux ignorent 10 décès accidentels isolés mais pas un accident avec 10 décès.

- certains auteurs réduisent la notion de risques à deux dimensions : ils se ramènent dans ce cas à la vraisemblance et la conséquence [Polet, 2002].

1.2.2 Relation entre les attributs de la Sûreté de Fonctionnement

L'analyse des dépendances entre les différentes grandeurs de sûreté de fonctionnement conduit aux relations suivantes [Cauffriez & al., 2004] :

- une mauvaise fiabilité d'un système peut conduire à une mauvaise disponibilité en cas de nombreuses défaillances, mais peut également agir sur la sécurité puisque l'occurrence d'un accident est souvent associée à une défaillance,
- une maintenabilité insuffisante (dans le cas de systèmes réparables) peut compromettre la disponibilité d'un système (augmentation du nombre de défaillances) mais aussi sa sécurité (augmentation de l'exposition au risque d'accidents en opération de maintenance),
- un système peut être fiable et maintenable sans nécessairement être de sécurité,
- la sécurité (à l'inverse de la disponibilité) ne dépend pas entièrement de la maintenabilité et de la fiabilité,
- les contraintes liées à la sécurité influent souvent négativement sur la disponibilité.

La figure 1.5 illustre les relations entre les différentes grandeurs de la sûreté de fonctionnement.

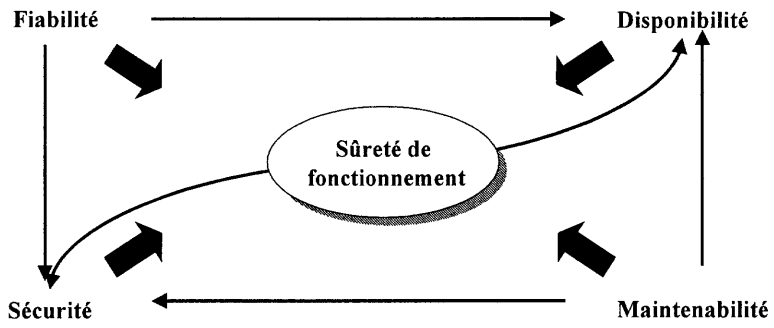

Figure 1.5 : Relation entre les attributs de Sûreté de Fonctionnement

[1] Données INSEE au 1er janvier 2004, bilan démographique 2003

1.2.3 Discussion

L'évaluation des objectifs de sûreté de fonctionnement a pour but d'identifier un ensemble de situations indues mais il est très difficile d'être exhaustif (aucune étude de sûreté n'aurait pu identifier la séquence d'événements menant au crash du Concorde) et les oublis sont faciles notamment lorsque de nouvelles technologies sont employées ou lorsque l'évaluation a trait à des systèmes entièrement nouveaux (absence de retour d'expérience).

Les méthodes d'arbres de conséquences ou de fautes permettent certes d'énumérer des séquences d'événements conduisant à un événement redouté mais elles ne suffisent pas : la génération de ces arbres nécessite d'une part un certain savoir-faire, ces évaluations conduisent d'autre part à des séquences d'événements souvent différentes et donc à des résultats différents. Certains modèles ou simulations sont nécessaires pour mieux maîtriser les scénarios d'événements, identifier les événements initiateurs et mettre en place des méthodes de confinement.

Par ailleurs, toute étude de sûreté de fonctionnement nécessite de préciser clairement les frontières du système étudié : dans un premier temps, on se limite à une installation ou un ensemble d'équipements puis on repousse les frontières du système : qu'en est-il au niveau de l'usine, de l'environnement direct et de la population touchée (exemple de l'explosion de l'usine AZF de Toulouse) ?

Autre exemple qu'est celui du ferroviaire où il ne suffit pas de limiter l'étude de sûreté à une rame pleine de nouvelles technologies mais où il convient d'étendre les frontières du système en étudiant le comportement de cette rame dans son infrastructure, certains auteurs parlent alors de sécurité opérationnelle, concept récent qui assure un fonctionnement sûr sous risques contrôlés [Niel, 1998].

Enfin s'il est aisé d'obtenir la probabilité d'occurrence d'événements élémentaires pour des composants hardware (composants électroniques, pompes, vannes,..), la tâche est plus difficile lorsque de nouvelles technologies entrent en jeu ou lorsque des erreurs humaines dues à des tâches cognitives complexes sont à prendre en compte, dans ce cas les probabilités doivent être estimées à partir d'opinions d'experts.

1.3 Les grands axes de recherche en sûreté de fonctionnement des systèmes automatisés

Dans la suite de ce chapitre, j'aborde les grands axes de recherche sur *la conception de systèmes complexes automatisés sûrs de fonctionnement* en m'appuyant sur les différents niveaux de protection décrits à la figure 1.4, à savoir :

- étude de la sûreté lors de la conception du processus physique,
- étude de la sûreté lors de la conception du système d'automatisation,
- étude de la sûreté lors de la conception du système de sécurité,
- étude de la sûreté lors de la conception des barrières pour la contrôlabilité du risque,
- étude des facteurs humains lors de la conception de systèmes automatisés sûrs de fonctionnement.

Ces cinq grands axes de recherche sont développés dans les paragraphes 1.3.1 à 1.3.5.

1.3.1 Conception du processus physique

Le processus physique est différent selon la nature du domaine étudié :

- *dans le domaine de la production manufacturière* (cf. figure 1.6), le processus physique est constitué de « moyens » interconnectés éventuellement séparés par des stocks intermédiaires. Les « moyens » sont définis comme l'ensemble des ressources fixes nécessaires à la réalisation d'une opération [Cnomo, 1987],
- d'autres auteurs parlent non pas de « moyens » mais de « machines » [EN 292, 1997] : une machine est ainsi définie comme un ensemble de pièces ou d'organes liés entre eux, dont au moins un est mobile et, le cas échéant, d'actionneurs, de circuits de commande et de puissance, etc.., réunis de façon solidaire en vue d'une application définie, notamment pour la transformation, le traitement, le déplacement et le conditionnement de matériaux [Charpentier, 2002].

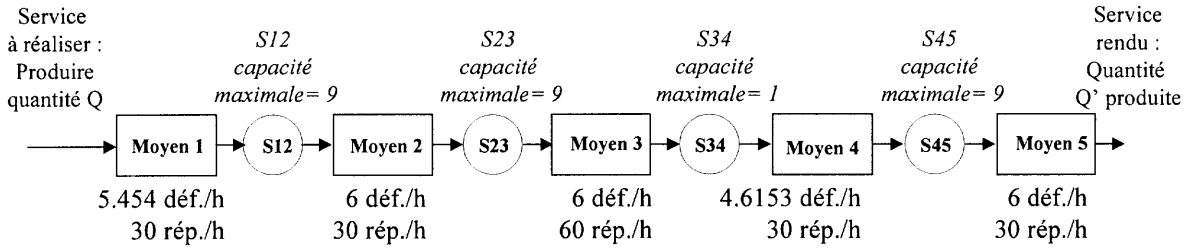

Figure 1.6 : Exemple de processus de production (déf : défaillances, rép : réparation, h : heure)

- *dans le domaine de la production continue* (cf. figure 1.7), le processus physique est constitué de canalisations, de vannes, de pompes, de compresseurs…

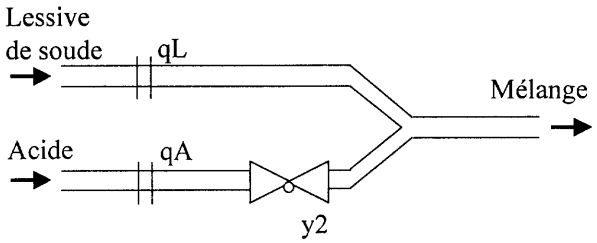

Figure 1.7 : Exemple de processus physique continu

- *dans le domaine ferroviaire* (cf. figure 1.8), le processus physique est par exemple constitué « d'équipements » dédiés à la circulation des trains tels que matériels roulants, voies, postes de manœuvre, caténaires etc…[EST 2002].

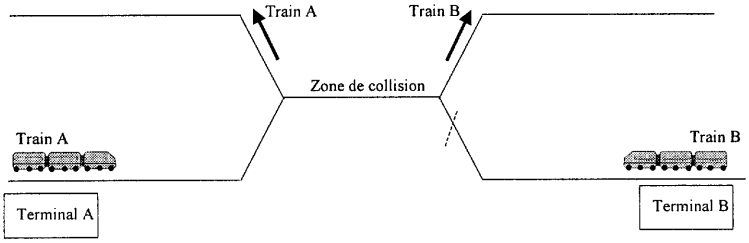

Figure 1.8 : Exemple de processus physique dans le domaine du ferroviaire

D'une manière générale, le service rendu par le processus physique peut être caractérisé par son efficacité ou sa qualité. Trois grandes classes de causes peuvent affecter cette efficacité [Sourisse & al., 1996] :

- les *dysfonctionnements* qui peuvent conduire à des anomalies d'exploitation, des pannes (énergie, ralentissements,....),
- les *performances insuffisantes* dues à la conception intrinsèque du processus physique ou à son opérabilité (procédures d'exploitation et de maintenance, pertes rendement, pertes qualité...)
- les *gaspillages* (tâches inutiles ou excessives de contrôle, réglage, gestion, investissements improductifs, dommages et pénalités...).

Lors de la conception du processus physique, il convient donc de choisir judicieusement les différents moyens et équipements le constituant afin de ne pas introduire d'entités pouvant mener à une perte de disponibilité ou de sécurité selon le schéma de sûreté présenté à la figure 1.5.

1.3.2 Conception du système d'automatisation

1.3.2.1 Instrumentation du processus physique

Afin d'obtenir les actions souhaitées sur le processus physique, les automaticiens ont recours à des actionneurs. Le service rendu par un actionneur est de moduler, en fonction de la commande appliquée, la puissance primaire pour obtenir les actions désirées sur le processus physique en dépit de perturbations (force résistante, force de frottement,...) [Staroswiecki & al., 1994]. Les variables usuellement modulées sont la position, la vitesse, le débit, la température, la pression, le volume, la quantité de matières, le PH, la viscosité....

Moduler les variables du processus physique ne suffit pas. Il faut que ce dernier soit instrumenté de capteurs pour que le mécanisme de commande dispose d'une image du résultat obtenu afin de la comparer à la consigne souhaitée et réagir par rapport à l'écart observé : les automaticiens parlent de commande en boucle fermée. Le service rendu par un capteur est donc de délivrer une image fidèle d'une variable réelle.

La figure 1.9 donne le schéma Mesure-Décision-Action d'une commande en boucle fermée : dans cet exemple, l'actionneur est un moteur soumis à perturbations, le mécanisme de commande est un régulateur PID, le capteur a pour but de délivrer l'image y(t) de la variable réelle x(t) soit en principe y(t)=x(t) si l'image est fidèle.

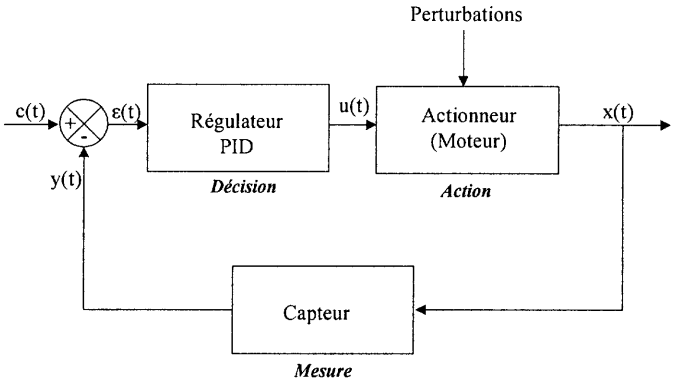

Figure 1.9 : Commande en boucle fermée

La figure 1.10 décrit le processus d'instrumentation pour l'exemple du mélange acide-soude de la figure 1.7 et illustre sur un cas concret la boucle Mesure-Décision-Action.

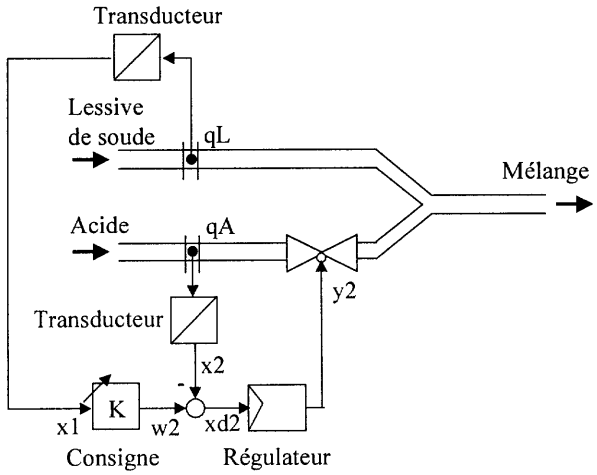

Figure 1.10 : Système d'automatisation pour l'exemple de mélange Acide-Soude

1.3.2.2 Grandeurs d'influence pour l'instrumentation du système d'automatisation

Un capteur peut être caractérisé par sa relation entrée/sortie, il en est de même pour l'actionneur. Cette caractérisation permet de rendre compte du service délivré tel que perçu par le ou les utilisateurs du capteur ou de l'actionneur.

Ce service peut cependant être altéré si l'environnement du système automatisé (ou le processus physique lui-même) soumet ces deux entités à des contraintes opérationnelles mécaniques, vibratoires, thermiques, climatiques, électriques ou électromagnétiques... Le fonctionnement des capteurs et actionneurs peut ainsi être perturbé et occasionner des variations de certaines grandeurs. Ces variations peuvent également survenir suite à des phénomènes d'usure et de vieillissement.

Il est donc impératif de caractériser lors de la phase de conception les domaines de variation des paramètres (ou la combinaison de ces paramètres) à l'intérieur desquels [Ciame-Afcet, 1987] [Staroswiecki & al., 1994]:

- les performances entrée/sortie sont garanties : le domaine nominal d'utilisation qui est l'intersection entre l'ensemble des états physiques atteignables et l'ensemble des contraintes opérationnelles,
- les performances ne sont plus garanties mais sont retrouvées lors du retour au domaine nominal : domaine de non-détérioration (dégradation temporaire),
- les performances sont définitivement altérées et le retour vers le domaine nominal ne permet pas de retrouver les performances initiales (apparitions de fonctionnements défaillants).

La figure 1.11 inspirée de [Niel, 1998] précise le domaine nominal d'utilisation, détérioration et non-détérioration à partir des ensembles physiques atteignables et des contraintes opérationnelles.

Afin d'améliorer les performances des actionneurs de nombreux travaux de recherche sont menés avec le développement d'instruments intelligents pour la commande non linéaire, adaptative, multivariable, optimale et floue. Dans le chapitre 2 de ce mémoire, je fais un état de l'art et positionne ma recherche par rapport à ces thématiques (cf. Axe II, paragraphe 2.3).

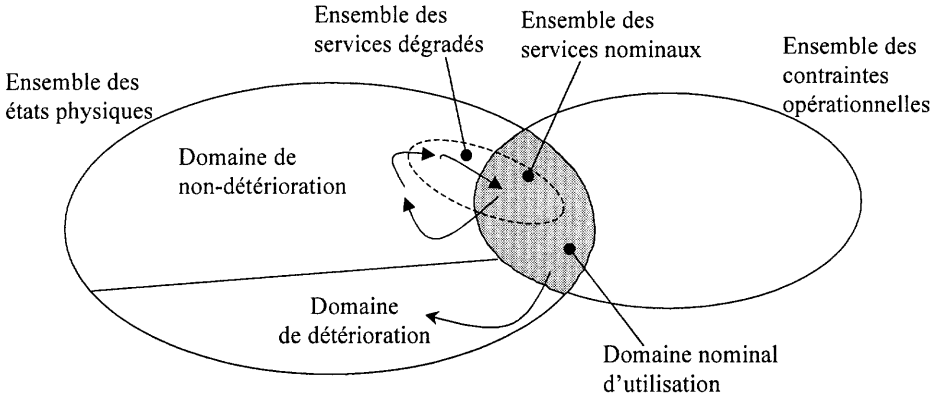

Figure 1.11 : Illustration des domaines de performances de capteurs ou d'actionneurs

1.3.2.3 Complexité du système d'automatisation

Dans la réalité, le système d'automatisation comporte de nombreuses boucles Mesure-Décision-Action telle que celle présentée figure 1.9 et, est de loin très complexe. La différence entre la notion de système compliqué et de système complexe est introduite par [Ciccotelli, 1999] [Ciccotelli & al., 2002] : les systèmes compliqués se caractérisent par des relations d'arborescence (hiérarchiques) entre des entités élémentaires qui peuvent être en grand nombre alors que dans un système complexe, les entités peuvent être en moindre nombre mais leurs inter-relations sont de type « *rétromettante* » avec l'existence de fonctions réentrantes et de rebouclages.

[Le Moigne, 1994] souligne que le contraire de « simple » n'est pas « complexe » mais « implexe » du latin implexus (compliqué). A la différence des systèmes compliqués, qui sont décomposables, les systèmes complexes sont indécomposables sans risque de mutilation. Selon [Morin, 1990], il existe des systèmes de basse complexité, quasi-décomposables en niveaux implexes et hiérarchisables ; les systèmes d'automatisation pourraient trouver leur place dans cette catégorie.

Tout concepteur de système d'automatisation peut baser sa réflexion sur les préceptes fondateurs introduits par Le Moigne reposant sur une démarche scientifique cartésienne [Ciccotelli, 1999]:

- le précepte d'*évidence*, qui sans un certain bon sens, masque parfois le fait qu'une évidence est souvent dépendante de son contexte (l'équation i=i+1 est évidente sur le plan informatique mais ne l'est pas sur le plan mathématique),
- le précepte de *réductionnisme* qui sous prétexte de simplification mène l'analyste à s'interroger sur « de quoi c'est fait » plutôt que de s'intéresser à « qu'est ce que ça fait »,
- le précepte de *déterminisme* qui veut que l'on exprime les choses au travers de lois bien identifiées, même si elles font défaut dans certains cas,
- le précepte d'*exhaustivité* qui suppose que l'on n'omet rien, volontairement ou non. Force est de constater que dans la pratique il est difficile de ne pas déroger à ce dernier précepte.

Le génie automatique avec l'analyse des systèmes et la théorie de la modélisation systémique a ouvert de nouvelles voies en élargissant les préceptes cartésiens ci-dessus évoqués. Sont venus ainsi s'ajouter les quatre préceptes du nouveau discours de la méthode [Le Moigne, 1994] :

- *pertinence* qui sous-entend que la perception d'un système est dépendante de ce que recherche le modélisateur, de ce fait la pertinence est tributaire autant du système que du modélisateur,
- *globalisme* qui consiste à percevoir les relations fonctionnelles du système dans sa globalité par rapport à son environnement et contribue à délaisser dans un premier temps sa structure interne,

- *téléologisme* qui vise à interpréter le système par son comportement par rapport aux « intentions » que l'on attribue au système sans pour autant chercher à expliquer ce comportement par une loi impliquée dans une éventuelle structure,
- *agrégativité* qui suggère au modélisateur de s'attacher aux agrégats jugés les plus pertinents et exclure l'illusoire objectivité d'un recensement exhaustif des éléments à considérer.

La théorie du système général conduit Le Moigne à caractériser tout système par son déplacement dans le référentiel « Temps, Espace, Forme » et à présenter une articulation des systèmes en neuf niveaux (cf. Tableau 1.2).

L'emploi de nouvelles technologies telles que les instruments intelligents, les réseaux de communication va permettre pour les systèmes d'automatisation supervisés par l'Homme de s'approcher des niveaux 7 et 8 car ces équipements intelligents sont capables de s'autosurveiller, d'optimiser leur comportement, de gérer leurs données, d'assister leur propre exploitation et maintenance [Ciccotelli, 1999].

Niveau	L'objet, qu'il soit système ou sous-système
1	Est passif et sans nécessité, il est alors reconnaissable
2	Est actif. Il fait, il intervient et est connu par son activité
3	Est actif et régulé. Son activité présente une certaine régularité, relation de bouclage
4	S'informe grâce à des informations repérables par des relations informationnelles spécifiques dans les objets représentés
5	Décide de son activité
6	A une mémoire
7	Se coordonne
8	Imagine et donc s'auto-organise
9	S'auto-finalise. Emergence de la conscience

Tableau 1.2 Articulation des systèmes en neuf niveaux

En résumé, la complexité d'un système d'automatisation peut être représentée par les différentes vues qui contribuent à le définir [Ciccotelli, 1999]:

- la *vue fonctionnelle* représentative du « qu'est ce que ça fait ». Plus les fonctionnalités du système d'automatisation sont nombreuses, plus le système montrera une complexité fonctionnelle importante,
- la *vue comportementale* représentative du « qu'est ce ça devient » ; on peut en effet se demander ce qui résulte pour le système global de l'agrégation d'entités (complexité d'agrégation) présentant chacune un certain nombre d'états (complexité d'états) et des lois probabilistes de transition inter-états (complexité stochastique),
- la *vue structurelle* représentative du « qui fait quoi et avec qui », fait référence à une structure composite compliquée (composants, logiciels, sous-systèmes, systèmes, individus, équipes, départements, usines, environnements) où les interactions horizontales et verticales sont nombreuses,
- la *vue technologique* représentative du « de quoi c'est fait ». Dans la majorité des cas, les composants matériels ne sont pas développés spécifiquement pour le système d'automatisation à concevoir. Certains auteurs parlent de « composants sur l'étagère » (on-shelf component) [Quintian, 2003], ces derniers présentent un inconvénient majeur car ils reposent sur une documentation succincte voire inexistante avec des modes de défaillances inconnus et non maîtrisés.

1.3.2.4 Entraves à la sûreté de fonctionnement du système d'automatisation

La sûreté de fonctionnement du système d'automatisation peut faire l'objet d'entraves tout au long de son cycle de vie :

- lors de la conception où les contraintes budgétaires peuvent rendre quasi inexistante la conception de prototypes ou de sites pilotes permettant de mieux appréhender les différents aspects de la conception, de la recherche et du développement de systèmes automatisés. Les concepteurs doivent durant cette phase faire face à la complexité des composants, aux complexités technologiques, d'intégration et s'appuyer sur des données « propriétaires » sans en connaître la véritable origine ni la validité. Une méconnaissance de ces composants, la mauvaise utilisation ou la modification des spécifications d'origine peuvent ainsi conduire à des erreurs de conception lourdes de conséquences,
- lors de la phase de réalisation avec l'introduction durant la mise en œuvre de défauts ou d'imperfections dus à des écarts par rapport aux spécifications issues de la phase de conception,
- lors de la validation avec la rémanence d'erreurs introduites aux étapes de conception et réalisation en dépit d'une activité de validation sérieuse ayant prouvé que le système automatisé était apte à rendre le service pour lequel il a été conçu,
- lors de l'exploitation, durant les différentes phases de fonctionnement du système d'automatisation (démarrage, régime permanent, maintenance, mise en/hors-service...). Deux cas de figures peuvent se présenter : soit les défaillances sont identifiées et prises en compte par le système d'automatisation (grâce à une conception appropriée) et sont dans ce cas confinées à ce niveau ; soit elles n'ont pas été prises en compte et c'est au système de sécurité à les gérer pour éviter de conduire à des dysfonctionnements anormaux ou à des séquences d'événements menant à un accident.

1.3.2.5 Les types de défaillance pour un système d'automatisation

Différents types de défaillance peuvent être caractérisés selon leur rapidité de manifestation, leurs causes, leurs conséquences ou par la combinaison de ces différents concepts. La figure 1.12 donne une classification de ces défaillances d'après le BTE [BTE, 1992].

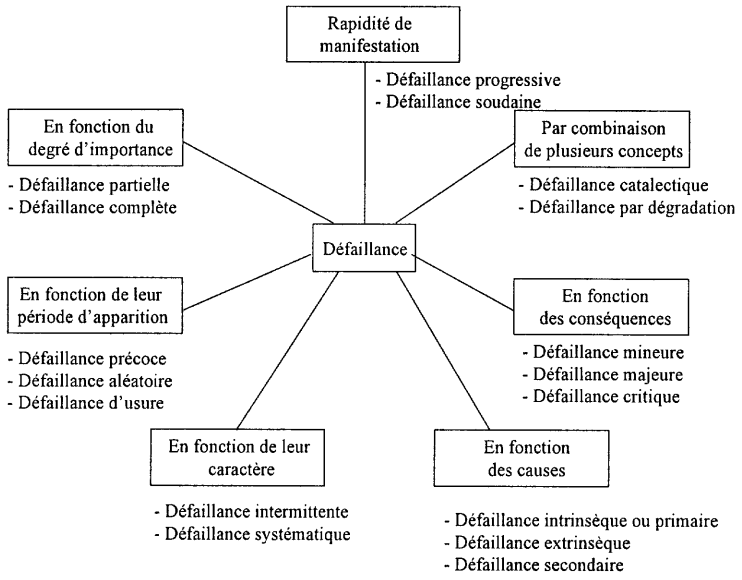

Figure 1.12 : Classification des défaillances d'après [BTE, 1992]

1.3.2.6 Aspects normatifs

La norme de référence pour les études de sûreté de fonctionnement est la norme internationale [CEI60300-3-1, 2003] qui traite de la gestion de la sûreté. Elle constitue en fait un guide méthodologique d'application des méthodes de sûreté de fonctionnement. Selon cette norme, une analyse de sûreté est constituée de cinq phases : définition du système à analyser et des modes opératoires, définition des objectifs et exigences de sûreté accompagnée des profils de mission et de la durée de la mission, allocation des exigences de sûreté aux différents sous-systèmes, analyse de sûreté qualitative et quantitative, validation pour vérifier que les objectifs sont atteints avec étude des alternatives de conception conduisant à une augmentation de la sûreté.

Lorsque le système utilise des systèmes informatiques appelés plus communément Systèmes Electroniques Programmables à base de technologie dite E/E/PE (Electrical / Electronic / Programmable Electronic), la norme de référence devient la norme [CEI61508a-g, 2002]. En effet, on utilise depuis des années des systèmes électroniques programmables dans tout secteur d'application (nucléaire, aéronautique, spatial, transport) pour exécuter des fonctions qui ne sont pas de sécurité mais aussi de plus en plus souvent liées à la sécurité. Cette norme aborde ainsi les problèmes induits par l'utilisation de systèmes programmés et s'attache à la sécurité fonctionnelle de tels systèmes, on y retrouve : des prescriptions générales, des prescriptions pour les systèmes électriques/électroniques/électroniques programmables, des prescriptions relatives aux logiciels, des exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité, un guide d'application, une bibliographie relative aux techniques et mesures. La figure 1.13 décrit la démarche globale préconisée par la norme CEI61508 pour satisfaire les objectifs de sûreté lors de la conception de systèmes à base de technologie E/E/PE [Bell & al., 2000].

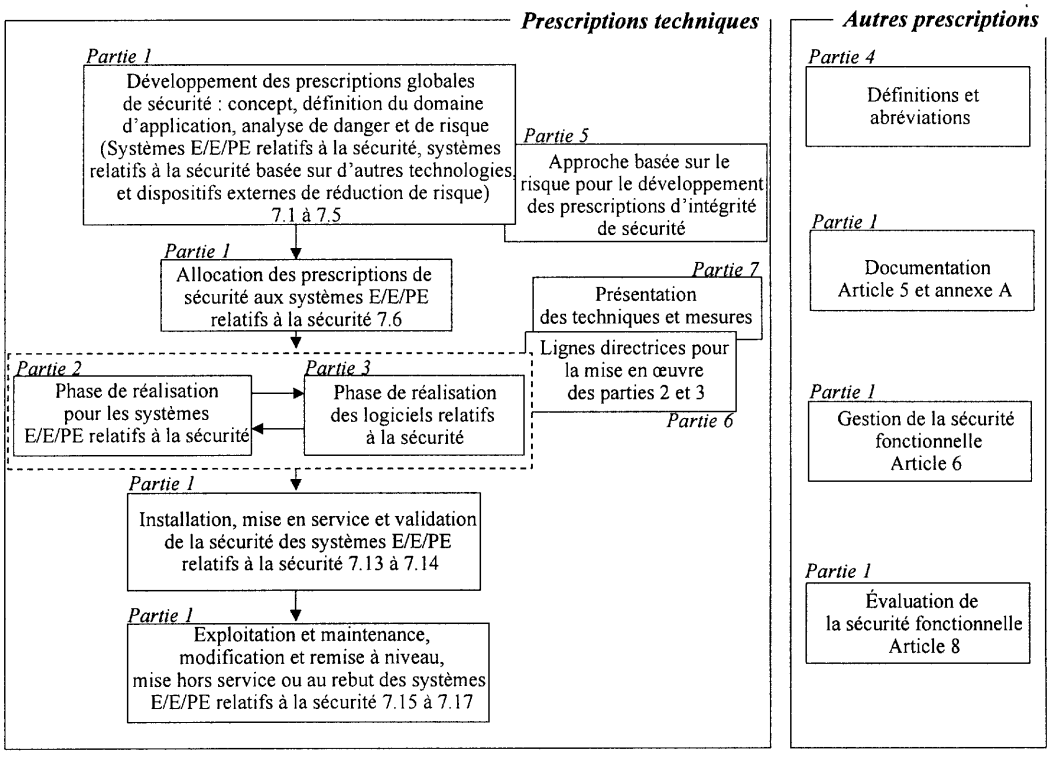

Figure 1.13 : Démarche générale d'une étude de sécurité

1.3.3 Conception du système de sécurité

1.3.3.1 Instrumentation du système de sécurité

Le système de sécurité gère les défaillances qui ne peuvent être confinées au niveau du système d'automatisation lors de l'exploitation du système automatisé. Celles-ci ne peuvent être confinées par le système d'automatisation soit parce qu'elles n'ont pas été prises en compte lors de la conception soit parce que leur confinement a été volontairement reporté au niveau du système de sécurité. Pour ce faire, des protections supplémentaires sont incorporées. Il peut s'agir d'instruments de sécurité passifs (détecteurs de présence, tapis sensitif, ...) ou actifs (fusibles, arrêts d'urgence, arrosages incendie....).

La distinction entre instruments de sécurité actifs ou passifs repose sur la notion de réponse à la sollicitation : un fusible, un arrêt d'urgence ou l'arrosage incendie ne doivent fonctionner qu'en cas de besoin alors qu'un détecteur de présence ou un tapis sensitif délivrent un service continu.

1.3.3.2 Grandeurs d'influence pour l'instrumentation du système de sécurité

Le service délivré par le système de sécurité peut être altéré si les contraintes opérationnelles mécaniques, vibratoires, thermiques, climatiques, électriques ou électromagnétiques imposées par l'environnement ou le processus physique lui-même sont fortes. En effet, le fonctionnement du système de sécurité peut en être fortement perturbé et il est impératif de s'affranchir des contraintes de l'environnement pour que le système de sécurité soit disponible à la sollicitation.

Pour ce faire, on a recours à des composants dits «de sécurité » qui présentent de meilleures caractéristiques en environnement perturbé et dont le domaine d'utilisation est plus étendu que des composants classiques : on ne peut imaginer le dysfonctionnement d'un système de lutte contre l'incendie suite à l'utilisation de détecteurs ne supportant pas les hautes températures. De ce point de vue, la conception d'un système de sécurité requiert l'utilisation et le développement de composants de sécurité à performances améliorées.

La figure 1.14 montre que le domaine d'utilisation nominal d'un composant de sécurité couvre un spectre plus large que le domaine d'utilisation d'un composant classique. Le domaine nominal de fonctionnement est ainsi borné par des limites extrêmes, inférieures aux valeurs fixées par les seuils d'arrêt d'urgence, dont le dépassement déclenche une action automatique de protection du système automatisé telle que mise hors tension ou hors service. En cas de dépassement des seuils d'arrêt d'urgence, on atteint les limites de sécurité qui sont des valeurs extrêmes conduisant à des dommages indésirables ou inacceptables pour le système. Les systèmes de sécurité peuvent a contrario avoir des effets pervers et la conception de système de sécurité nécessite des études approfondies pour ne pas introduire trop de seuils d'arrêt d'urgence pouvant compromettre la sécurité en changeant soudainement l'état du système et en affaiblissant sa disponibilité par des usages excessifs.

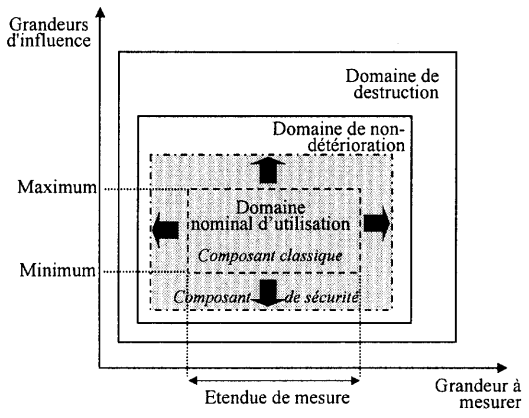

Figure 1.14 : Comparaison du domaine nominal d'utilisation des composants classique et de sécurité

1.3.3.3 Complexité du système de sécurité

La conception d'un système de sécurité est délicate car les systèmes de sécurité sont devenus à l'heure actuelle des systèmes automatisés à part entière : la complexité du système de sécurité est donc sur de nombreux points similaires à celle du système d'automatisation mais des spécificités existent qui nécessitent des choix et des exigences particulières.

La conception d'un système de sécurité se ramène ainsi à la conception d'un système d'automatisation à haut degré de sûreté dont le fonctionnement se fait sur sollicitation lors de la gestion d'incidents [Charpentier, 2002].

A ce stade, les pires cas doivent être envisagés et tout doit être mis en œuvre pour pallier la célèbre loi de Murphy. En outre, il est important d'étudier de manière approfondie les dysfonctionnements du système de sécurité car tout dysfonctionnement du système de sécurité introduit une modification dans la gestion de la sécurité ou annule purement et simplement la sécurité du système d'automatisation et *a fortiori* du processus physique.

1.3.3.4 Les types de défaillances pour un système de sécurité

Un système de sécurité peut être affecté par deux types de défaillances [Laprie & al., 1995] :

- défaillance de type Fail-Safe : le système de sécurité est activé alors qu'il ne devrait pas l'être : une fausse alarme de détection de fumée est une défaillance de type Fail-safe,
- défaillance de type Fail-Dangerous : un système de sécurité n'est pas activé alors qu'il devrait l'être : exemple de la non-détection de fumée par un détecteur lors d'un incendie.

Différentes causes peuvent conduire à ces types de défaillance :

- mauvaise localisation du capteur,
- mauvaise prise de l'information (prise de l'information au niveau du signal de commande d'un actionneur plutôt que surveillance de son état par un capteur supplémentaire),
- défaillance capteur,
- surcharge d'un calculateur décisionnel,
- dérive de capteur (nécessité d'utiliser des capteurs de sécurité spécifiques aux limites extrêmes du domaine nominal d'utilisation),
- trop ou trop peu d'informations,
- trop d'alarmes (effet d'arbres de Noël),
- désactivation intentionnelle du système de sécurité (exemple de la centrale de Tchernobyl),
- validation du système de sécurité non exhaustive et limitée à des scénarios d'accident.

1.3.3.5 Aspects normatifs

Même si les grandes lignes pour traiter les problèmes de sécurité sont semblables d'un domaine à l'autre (nucléaire, aéronautique, spatial, transport, industrie), il n'en demeure pas moins des spécificités au niveau de la conception des systèmes de sécurité. On voit donc apparaître des normes spécifiques au domaine d'utilisation.

Seules les normes relatives à nos activités de recherche sont mentionnées ci-après.

1.3.3.5.1 Sécurité dans le domaine des machines

La norme [CEI62061, 2002] traite de la sécurité fonctionnelle de commande de machines à

technologie E/E/PE (Electrical / Electronic / Programmable Electronic) et est appliquée pour l'amélioration de la sécurité des opérateurs travaillant sur des machines ou côtoyant des lignes de production. Elle vise à concevoir et valider les systèmes de commande intégrant des composants ou des sous-systèmes dont les spécifications sont conformes à la norme [CEI 61508a-g, 2002].

Outre les normes internationales, il existe un grand nombre de normes européennes. Le diagramme élaboré par le CEN (Comité Européen de Normalisation) repris dans [Lacore, 1998] donne une vue globale des normes européennes (cf. Figure 1.15). Sont principalement à retenir :

- la norme [EN1050, 1991] qui donne les principes pour l'estimation des risques,
- la norme [EN292, 1997] qui définit la terminologie et les méthodes générales de conception,
- la norme [EN954-1, 1996] qui donne les principes généraux de conception de commande relatifs à la sécurité machine (celle-ci incluant la norme EN 61496 pour les barrières immatérielles).

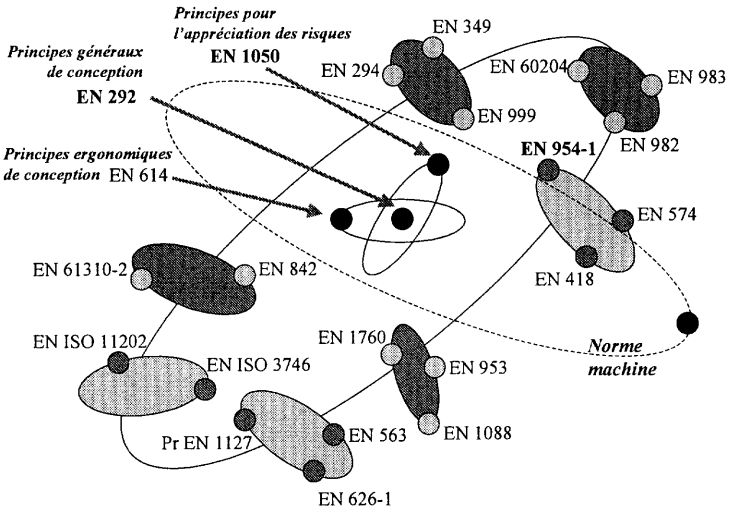

Figure 1.15 : Vue globale des normes européennes en sécurité machine

1.3.3.5.2 Sécurité dans le domaine ferroviaire

Les systèmes de sécurité ferroviaire sont ceux qui interviennent directement dans la prévention des accidents liés à la circulation des trains. A titre d'exemple, il s'agit aussi bien du matériel roulant, de la signalisation, de la voie, des postes de manœuvre, les caténaires, les automatismes de conduite [EST 2002]. Lorsqu'ils sont réalisés par des systèmes électroniques ou comportent une partie logicielle, ces systèmes rentrent dans le champ d'application des normes européennes [EN50126, 2000], [EN50128, 1995], [EN50129, 2002]. Les normes de références internationales sont :

- la norme internationale [CEI62279, 2002] qui traite des systèmes de signalisation, de télécommunication et de traitement ainsi que des logiciels pour systèmes de commande et protection ferroviaire,
- la norme internationale [CEI62236a-f, 2003], qui aborde la compatibilité électro-magnétique,
- les normes internationales [CEI62280a-b, 2002] qui s'appliquent (respectivement) à une communication sécuritaire dans un système de transmission fermé (ouvert),
- les normes issues du projet ERTMS (European Railway Transport Management System) non encore référencées à ce jour.

1.3.4 Contrôlabilité du risque : conception de barrières

Lorsque le système de sécurité (accompagné des procédures de sécurité mises en œuvre sur site) n'arrive pas à gérer les incidents, il convient de mettre en place un moyen supplémentaire de contrôlabilité du risque afin de maîtriser la situation et éviter la dégénération de l'incident (événement sans conséquences) en accident (événement dommageable).

Ce moyen ultime de contrôlabilité du risque est appelé « barrière ». Le concept de barrières correspond à un principe de défense en série tel qu'introduit par [Reason, 1993] (cf. Figure 1.16).

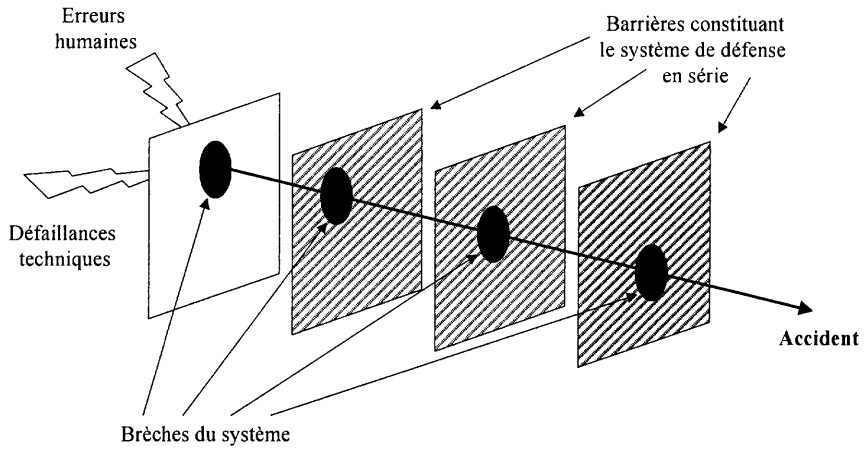

Figure 1.16 : Principe de défense en série

La barrière est définie par [Hollnagel, 1999] comme un obstacle, une obstruction ou une gêne qui peut soit prévenir l'exécution d'une action ou l'apparition d'un événement, soit prévenir ou diminuer l'impact des conséquences. Une classification des barrières en quatre catégories est proposée par [Polet, 2002] :

- les barrières matérielles qui empêchent physiquement la réalisation de certaines actions ou la propagation de leurs conséquences. La principale caractéristique de ces barrières est qu'elles réalisent leur fonction sans que l'agent actif n'ait à les percevoir ou les interpréter. Elles visent à réduire l'occurrence d'un événement redouté,
- les barrières fonctionnelles dites actives créent un lien logique ou temporel entre les événements de sorte que leur exécution est implicitement orchestrée. Elles constituent un moyen de sécurité par rapport à un événement dangereux,
- les barrières symboliques requièrent d'être interprétées pour être effectives. Elles préconisent le comportement à adopter pour se protéger,
- les barrières immatérielles demandent que leur existence soit connue pour être actives et ne sont pas physiquement présentes ou représentées. Elles spécifient les règlements, les procédures et la législation à suivre.

Le tableau 1.3 tiré de [Polet & al., 2002] résume les différents types de barrières que l'on peut rencontrer et spécifie les différents acteurs qui les mettent en place dans le cycle de vie du système.

	Barrières matérielles	**Barrières fonctionnelles**	**Barrières symboliques**	**Barrières immatérielles**
Le constructeur	Armoires électriques, grille de protection, carter, isolation,...	Capteurs de présence, Interverrouillage, commande à distance,...	Affichage, étiquetage, signalisation visuelle et sonore, supervision,...	Formation des futurs utilisateurs, manuels d'utilisation
L'employeur	Aménagement des postes de travail et des ateliers, issues de secours, moyens individuels de protection,...	Porte coupe-feu, limitation d'accès à certaines personnes, mots de passe,...	Affichage des consignes de sécurité, marquage au sol,...	Formation interne, règlement intérieur, procédures internes
Le collectif de travail (opérateurs)	Condamnation de certaines zones, consignation d'équipements	Verrouillage	Communication orale, gestuelle, sonore, affichage	Consigne lors du changement de poste, rapport

Tableau 1.3 : Les différents types de barrière de sécurité

Les limites des différentes barrières sont discutées dans [Polet, 2002] :

- le masquage d'erreur ou de défaillance [Reason, 1993] : de par son rôle de défense en série et de limitation de propagation des conséquences, les fautes techniques ou humaines conduisant aux défaillances sont masquées. Ce masquage conduit à un manque de retour d'information qui ne permet pas de mieux connaître le comportement du système technique ou de l'opérateur humain et de le corriger,
- l'homéostasie du risque [Hollnagel, 1993] : l'usage des barrières est détourné et la confiance dans le service rendu par celles-ci est telle que les utilisateurs repoussent les limites de leur utilisation en augmentant le risque individuel et *a fortiori* le risque collectif,
- la possible inhibition des barrières [Rasmussen, 1997] : certaines barrières peuvent être désactivées, par exemple pour accroître la productivité.

La désactivation de barrière pour permettre un franchissement est intrinsèquement liée à la notion de violation. Ce thème de recherche constitue un axe fort de recherche au LAMIH avec l'identification et la modélisation des conditions limites tolérées par l'usage [Vanderhaegen, 2003].

1.3.5 Facteurs humains lors de la conception de systèmes automatisés sûrs de fonctionnement

L'Homme intervient en de nombreux points tout au long de la vie du système lors de la spécification, la conception, la réalisation, l'installation, la mise en service, la validation, l'exploitation, la maintenance.

Les performances des systèmes automatisés dépendent ainsi fortement du comportement de l'Homme. Il apparaît donc nécessaire lors de la conception de systèmes automatisés sûrs de fonctionnement de prendre en compte les facteurs humains qui influencent les exigences de sûreté, notamment [Carey, 2000]:

- les moyens par lesquels l'intervention de l'Homme peut affecter la sûreté du système (erreur de l'opérateur, erreur de maintenance, violation de procédures, ...),
- les moyens par lesquels l'intervention de l'Homme peut prévenir ou minimiser une perte de sûreté (procédure de contrôles, actions de recouvrement, ..),

- la prise en compte, lors de la conception du système, des aspects qui peuvent améliorer ou entraver les performances humaines (interfaces d'opérateurs, de maintenanciers, support de documentation et de formation),
- la prise en compte des aspects opérationnels dans l'environnement de travail lors de la conception et l'implémentation du système (aspect psychologique, culture de sûreté, aptitudes des utilisateurs, ...).

La norme [CEI61508a-g, 2002] souligne la nécessité de prendre en compte lors de la conception et l'implémentation de systèmes automatisés les facteurs qui peuvent affecter les performances humaines :

- caractéristiques intrinsèques de l'Homme (aptitudes et niveau de compétences, acquis par expérience et formation, pour la réalisation d'une tâche),
- caractéristiques de la tâche (novatrice, contraintes temporelles, complexité),
- conception d'équipement (interfaces utilisateurs, temps de réponse, caractéristiques de sûreté),
- environnement de travail (bruit, éblouissement, implantation),
- attributs d'organisation (culture de sûreté, supervision, nombre de ressources humaines disponibles, travail en équipes, postes en 3×8h).

Le tableau 1.4 donne les prescriptions relatives aux facteurs humains, dans la phase du cycle de vie de sécurité, spécifiés dans la norme CEI61508a :

Facteurs humains dans la phase du cycle de vie de sécurité	**Prescriptions**
2 Définition globale du domaine d'application	- Identification des événements initiateurs d'accident, erreur humaine incluse
3 Analyse de danger et risque	- Inclure tout problème pertinent lié au facteur humain - Couvrir les situations de mauvais usage raisonnablement - Porter une attention particulière aux modes d'exploitations anormaux, peu fréquents - Prendre en compte les contraintes d'exploitation ou d'intervention humaine qui doivent être détaillées et documentées
4 Prescriptions globales de sécurité (prescriptions implicites)	- Inclure à cette étape les fonctions réalisées par les opérateurs ou supposées être assignées aux opérateurs - Inclure également les fonctions réalisées par d'autres technologies (opérateurs humains, opérateurs en interaction avec des systèmes non E/E/PE)
5 Allocation des prescriptions de sécurité (prescriptions implicites)	- Allocation des fonctions de sécurité à des systèmes E/E/PE spécifiques ou à des systèmes de sécurité à base d'autres technologies ou à des dispositifs de réduction de risques ; ceci inclut les fonctions réalisées partiellement ou totalement par les opérateurs - Cette allocation doit prendre en compte les conséquences des performances humaines sur l'allocation choisie des fonctions de sécurité, les fonctions de sécurité réalisées par l'Homme en dehors du domaine du système E/E/PE doivent recevoir des informations issues du système ou doivent être interrompues s'il y a eu mauvaise conception (alarmes inappropriées ou intempestives)
6 Planification globale de l'exploitation et de la maintenance	- Spécification des actions systématiques qui doivent être réalisées et domaine des activités de maintenance - Spécification des procédures opératoires pour des états dégradés et anormaux du système
7 Planification globale de la validation de la sécurité (prescriptions implicites)	- Le programme de validation de la sécurité doit inclure la validation appropriée des facteurs humains - Nécessité d'identifier une planification en adéquation aux exigences de la phase 9 qui démontre que le personnel utilisé a les compétences requises pour valider les facteurs technico-humains
9 Système de sécurité E/E/PE : réalisation	- La conception du système E/E/PE doit être tolérante aux erreurs imputables à l'opérateur du matériel commandé - La conception du système de sécurité E/E/PE relatif à la sécurité doit tenir

	compte des aptitudes et limites humaines et doit convenir aux actions attribuées aux opérateurs et au personnel chargé de la maintenance - La conception de toutes les interfaces doit être fondée sur de bonnes pratiques en termes de facteur humain et doit s'accommoder du niveau probable de formation et de connaissances des opérateurs
14 Exploitation, maintenance et réparation globales	- Implémentation des procédures

Tableau 1.4 : Les prescriptions en facteurs humains spécifiés dans la norme [CEI61508a-g, 2002]

Conclusion

Ce chapitre présentait une analyse de la problématique globale de la sûreté de fonctionnement des systèmes automatisés en s'appuyant sur la notion de service rendu par les différents constituants du système global. Les frontières du processus physique, du système d'automatisation, du système de sécurité et du système de contrôlabilité du risque — notion de barrières — ont été clairement définies.

Cette étude fait apparaître deux grands niveaux dans la sûreté de fonctionnement des systèmes complexes : la *sûreté de fonctionnement prédictive* et *la gestion des objectifs de sûreté.* La sûreté de fonctionnement prédictive a pour but d'énumérer les différentes situations possibles et d'en quantifier la probabilité d'occurrence. La gestion de la sûreté repose plutôt sur un jugement de valeur et sur une prise de décision relative aux risques encourus par l'Homme et l'environnement.

Nous avons identifié les grands axes de recherche dans le domaine de la sûreté de fonctionnement des systèmes automatisés avec l'étude des exigences de sûreté pour le processus physique, le système d'automatisation, le système de sécurité et le système de contrôlabilité du risque.

Ont été également pris en compte les aspects normatifs incontournables lorsqu'il s'agit de systèmes industriels complexes, cette complexité a été déclinée en regard de la théorie du système général.

Dans le chapitre suivant, sont présentés mes contributions et résultats de recherche dans le domaine de la sûreté de fonctionnement. Mes travaux de recherche se décomposent en deux axes principaux : le premier axe porte sur la sûreté de fonctionnement de processus physiques avec une application directe aux lignes de production ; le deuxième axe se focalise sur la problématique de conception de systèmes d'automatisation sûrs de fonctionnement.

Pour chacun de ces axes de recherche, le positionnement dans la communauté scientifique est fourni et l'apport de mes travaux de recherche par rapport à l'existant est montré.

Chapitre 2

Sûreté de fonctionnement des systèmes complexes :

Contributions et résultats de recherche

Introduction

Mes travaux de recherche se décomposent en deux axes principaux : l'axe I porte sur la sûreté de fonctionnement de processus physiques avec une application directe aux lignes de production ; l'axe II se focalise sur la problématique de conception de systèmes d'automatisation sûrs de fonctionnement avec une application directe aux systèmes automatisés à intelligence distribuée, encore appelés Network Controled System.

Le *but de l'axe I* est d'améliorer la performance de lignes de production. La première action, que j'ai menée sur ce thème, vise à évaluer les paramètres FMD (Fiabilité-Maintenabilité-Disponibilité) des lignes de production et à en diagnostiquer les causes de non-performance en préconisant les actions à effectuer pour améliorer ces paramètres. La deuxième action aborde la problématique de la maîtrise des flux avec la détection, la localisation et l'identification des défaillances de rendez-vous entre plusieurs flux de production. Les aspects coûts, primordiaux dans le contexte industriel, sont abordés avec l'introduction de la notion de coûts propres aux défaillances et de coûts induits par certaines défaillances.

L'*objectif de l'axe II* de ma recherche porte sur la conception de systèmes d'automatisation sûrs de fonctionnement. Ces travaux partent du constat de l'absence de langages, d'outils pour la modélisation d'architectures abstraites obtenues par composition d'entités logicielles et matérielles. L'analyse faite met en évidence la nécessité de valider la sûreté de fonctionnement du système d'automatisation à chaque étape de la conception par rapport aux spécifications de services appropriés et inappropriés. La réflexion que j'ai menée montre la nécessité de formaliser, d'exprimer les besoins et les contraintes de l'architecture opérationnelle ; cette analyse fait apparaître l'existence de fonctions principales, secondaires et de fonctions techniques qui coopèrent et interagissent pour assurer la mission principale du système.

Une discussion s'ensuit sur les limites des méthodes classiques de sûreté de fonctionnement et finalement une méthodologie de Codesign pour la conception de systèmes d'automatisation sûr de fonctionnement est présentée. L'originalité de l'approche réside dans la complémentarité de trois classes d'architectures à distinguer lors de la conception : une architecture opérationnelle résultant de la projection de l'architecture fonctionnelle sur l'architecture matérielle issue de choix matériels.

Dans ce contexte, je propose sur cette thématique comme premier élément de réponse le formalisme SAFE-SADT développé lors d'une thèse encadrée. Ce formalisme permet la modélisation, caractérisation, identification des dépendances au sein de l'architecture opérationnelle et la génération d'une fonction de structure matérielo-fonctionnelle, qui, couplée à une simulation de Monte Carlo, permet d'étudier l'évolution des paramètres de sûreté tout au long du cycle de vie du système et conduit ainsi à la proposition d'une méthode fonctionnelle dynamique pour l'évaluation de la sûreté de systèmes complexes.

Axe I : Sûreté de fonctionnement de processus physiques : Application à des lignes de production

2.1 Positionnement dans la communauté scientifique

Tout réalisateur d'une étude de sûreté de fonctionnement doit « imaginer » ce que sont les états de fonctionnement et de dysfonctionnement du processus étudié. Mais lorsque le système est complexe, il devient difficile d'appréhender ces états car la défaillance d'un constituant ne conduit pas forcément à la défaillance globale du système. L'analyse du comportement global du système peut alors être effectuée en s'appuyant sur différents modèles tels que modèles analytiques (outils : matlab, mathematica,...), modèles événementiels (outils : markov, Petri, grafcet, Siman/Arena, Qnap2, ...), modèles qualitatifs (outils : arbres de fautes, blocs-diagrammes), modèles de simulation (Monte Carlo...).

Lorsque le processus physique étudié est une ligne de production, la complexité porte alors sur le nombre de moyens, de stocks intermédiaires constituant la ligne de production et la multitude de paramètres à prendre en compte : vitesse, capacité de stocks, taux de défaillances et réparations des moyens. D'une manière générale, une ligne de production peut être caractérisée par quatre vecteurs : le vecteur taux de défaillances $\vec{\lambda}=(\lambda_1, \ldots, \lambda_k)$, le vecteur taux de réparations $\vec{\mu}=(\mu_1, \ldots, \mu_k)$, le vecteur vitesse $\vec{V}=(V_1,\ldots, V_k)$ et le vecteur capacité des stocks $\vec{C}=(C_{12},\ldots,C_{k-1k})$.Lors du fonctionnement de la ligne, les niveaux courants de stocks peuvent être caractérisés par le vecteur $\vec{H}=(h_{12},\ldots,h_{k-1k})$ (cf. figure 2.1).

On parle de *ligne homogène* lorsque tous les moyens ont la même vitesse et de *ligne non-homogène* dans le cas contraire ; les vitesses ne sont pas forcément égales entre-elles et peuvent être soumises à variation (accélération, ralentissement ou suivre une loi de distribution) .

Les moyens peuvent être soit *synchrones*, dans ce cas tous les moyens en état de fonctionnement commencent à travailler au même instant, soit *asynchrones* dans le cas contraire. Si les moyens ont les mêmes taux de défaillances/réparations et une capacité de stocks identique, la ligne est dite *symétrique* sinon elle est *asymétrique*.

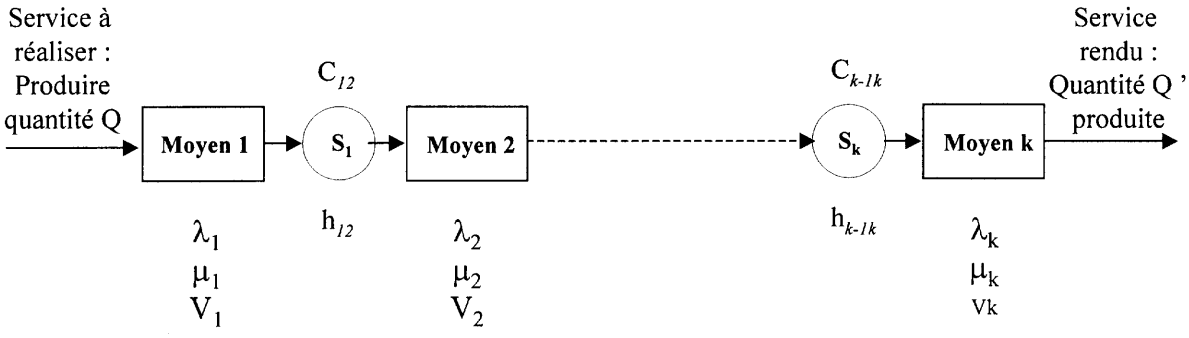

Figure 2.1 : Ligne composée de « n » moyens séparés par un stock intermédiaire

L'étude de tels processus physiques, complexes de par le nombre de moyens et des nombreux paramètres à prendre en compte, porte sur l'analyse comportementale de la ligne. Cette analyse comportementale peut se décomposer en deux étapes :

- *En l'absence de défaillances*, dans ce cas on étudie l'influence des vitesses différentes (sources de ralentissement) et de la capacité des stocks sur le comportement global de la

ligne. Cette étape est nécessaire lors de la conception de la ligne avec le dimensionnement des stocks pour éviter des ruptures d'approvisionnement au niveau des moyens.

- *En présence de défaillances*, il faut alors étudier l'influence des défaillances et réparations des différents moyens sur le comportement global de la ligne. Pour une gestion à flux poussés, il faut dimensionner les stocks de telle manière qu'ils « masquent » les défaillances des moyens sans pour autant atteindre une taille excessive. Pour une gestion à flux tirés, les stocks sont dimensionnés au plus juste afin que le flux « casse » lors de défaillances, ce qui facilite la détection et le déclenchement d'action corrective [Marty, 1996].

La « fiabilisation » des lignes de production passent par la maîtrise des flux physiques (coûts des stocks, implantation des équipements, délais de production, temps de séjour, taille des lots, temps de changement d'outils,...), l'application de méthodes de maintenance visant à maintenir les potentialités des équipements telles que la TPM (Total Productive Maintenance) ou la RCM (Reliability Centered Maintenance) [Pham, 2003] [Anderson & al., 1990], la recherche d'un pilotage adéquat pour le système de production allant vers une performance globale [Burlat & al., 2003] [Besombes & al., 2003] [Frein & al. 1996] [Trentesaux, 2002] [Senechal, 2004].

Ces travaux abordent différents aspects de recherche dans la communauté de la productique, du génie logiciel et du contrôle de gestion :

- les approches par simulation et par réseaux de Petri [Di Mascolo, 1996] [Chabot, 2001] [Châtelet & al., 2002],
- les indicateurs de performance et tableaux de bord [Bellon, 1997], [Bitton, 1990], [Cauffriez, 1994] [Lorino, 1997],
- les outils de décision multi-critères [Roy, 1993][Kosturiak & al., 1995],
- les approches analytiques : théorie des files d'attente [Baynat, 2000], les chaînes de markov [Noyes, 2002] , modèles analytiques de lignes [Burman, 1995] [Gershwin, 1987a-b], [Gershwin, 1994] [Dallery& al., 1988] [Dallery & al. , 1989] [Dallery & &l., 1992].

Ces différentes thématiques de recherche sont abordées :

- au sein du GRP (Groupement de Recherche en Productique) créé en 1996 par le biais de 5 groupes thématiques : Organisation et gestion de la production, Modélisation d'entreprises, Evaluation de performances, Conception Produit/Process, Automatisation des systèmes sûrs de fonctionnement. Ce dernier groupe a été fusionné en 2003 avec le groupe de travail Commande Opérationnelle des Systèmes à Evénements Discrets pour devenir Ingénierie de la Commande et de la supervision des systèmes à événements discrets du GDR MACS (Modélisation, Analyse et Conduite des Systèmes Dynamiques) du CNRS dans les pôles « Automatique » et « Sciences et Techniques de la production »,
- par le programme de recherche PROSPER de 1998 à 2002 soutenu par le CNRS et le Ministère de l'éducation Nationale, ce programme a contribué à développer les connaissances relatives aux systèmes de production en privilégiant le caractère interdisciplinaire,
- par le groupe S3 (Surveillance, Supervision, Sûreté) soutenu par le GDR Automatique du CNRS,
- par le Groupement de Recherche en Automatisation Intégrée et Systèmes Homme-Machine GRAISYHM de la région Nord-Pas-de-Calais.

2.2 Contributions majeures sur l'amélioration de lignes de production

Mes travaux de recherche se sont principalement focalisés sur l'amélioration de la performance de lignes de production selon deux actions :

- la première action vise à évaluer les paramètres FMD (Fiabilité-Maintenabilité-Disponibilité) des lignes de production et à identifier les actions à effectuer pour améliorer ces paramètres afin d'accroître la performance de la ligne,
- la seconde action porte sur la maîtrise des flux avec la détection, la localisation et l'identification des défaillances de rendez-vous entre plusieurs flux de production ; cette action prend en compte les aspects coûts avec la notion de coûts propres et de coûts induits par certaines défaillances.

Dans la suite de ce paragraphe, sont désignés par « travaux d'équipe » les travaux de recherche auxquels j'ai participé conjointement avec J. Defrenne et D. Willaeys dans le cadre des travaux de thèse de A. Patchong et S. Aramini, qui prenaient la suite de ma thèse de doctorat.

2.2.1. Action I.1 : Diagnostic de non-performance de lignes de production

L'amélioration des lignes de production passe par une phase de modélisation des lignes étudiées. Cette modélisation peut être réalisée à l'aide d'outils logiciels très sophistiqués (Arena, Cadence, Dosimis, Factor, Mosys, Quest, Siman, Simple++, Slamsystem, etc...), l'aspect sophistication est lié à la prise en compte de la configuration de la ligne, aux types de machines, aux gammes opératoires, aux temps de déplacement, etc... Une étude comparative approfondie de ces outils logiciels est réalisée dans [Kosturiak, 1995] ; le principal inconvénient souligné est le temps nécessaire à l'élaboration et à la validation des modèles avant de pouvoir effectuer un diagnostic de non-performance.

Fort de ce constat, nous nous sommes intéressés aux modèles analytiques qui permettent une modélisation, certes, moins fine mais suffisante pour effectuer un diagnostic de non-performance. Les principaux modèles rencontrés dans la littérature, sur lesquels se sont appuyés les travaux de l'équipe, sont présentés ici. Ces travaux illustrent, sur le cas particulier des lignes de production, les deux approches permettant de cerner la complexité : soit *l'agrégation* d'entités pour aller vers le système complexe, soit la *décomposition* du système complexe pour aller vers les entités.

2.2.1.1 Modèle continu pour une ligne homogène composée de 2 moyens séparés par un stock intermédiaire

Le modèle continu de lignes homogènes est un cas particulier car il ne s'applique qu'aux lignes constituées de moyens ayant tous la même vitesse $V_i(t) = V_i = V$. Dans ce cas, il n'y a pas de ralentissement dû à des différences de vitesse entre moyens. Les travaux menés par [Dallery & al., 1989] [Dubois & al., 1982] permettent de calculer les paramètres du modèle continu pour une ligne composée de deux moyens séparés par un stock intermédiaire.

Dans ce cas, la complexité est liée aux états pris par le système global { Moyen 1 + Stock + Moyen 2 }, ces états dépendent alors de la vitesse des moyens ($V_1=V_2=V$ pour une ligne homogène) et de la valeur courante des stocks h_1, h_2.

Le processus stochastique qui représente l'évolution du système est hybride : il est continu pour les états internes qui dépendent du niveau de remplissage h compris entre $]0,C[$ et discret pour les valeurs du niveau de remplissage égales à 0 et C. Le graphe d'état pour une ligne homogène constituée de deux moyens séparés par un stock intermédiaire est donné figure 2.2 ; ce graphe met en évidence la complexité au niveau des états de la ligne et des transitions inter-états.

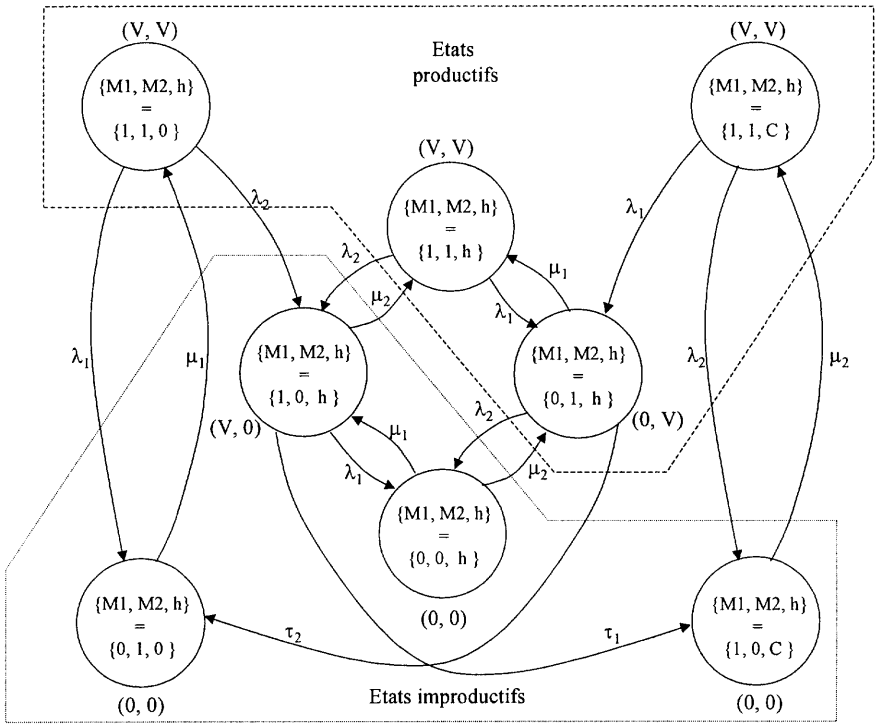

Figure 2.2 : Graphe d'états d'une ligne homogène constituée de deux moyens d'après [Vargas, 1992]

2.2.1.2 Modèle continu pour une ligne homogène composée de N moyens séparés par des stocks intermédiaires

Lorsque la ligne de production est composée de N moyens séparés par des stocks intermédiaires, se pose le problème de trouver un modèle équivalent à la ligne globale. La première démarche scientifique qui vient à l'esprit est de s'appuyer sur le modèle analytique continu proposé par [Dubois & al., 1982] pour une ligne constituée de 2 moyens et de l'étendre à une ligne composée de N moyens.

Malheureusement, cette démarche n'est pas viable car on ne peut étendre les résultats obtenus pour une ligne à deux moyens à une ligne plus longue. [Gerschwin, 1994] introduit le terme « d'indécomposabilité » qui *qualifie l'impossibilité de décomposer l'étude d'un système complexe en sous-systèmes dont les solutions sont connues.* Des méthodes approximatives s'avèrent ainsi nécessaires avec deux courants scientifiques : l'approche par aggrégation [Burman, 1995] ou par décomposition [Gershwin, 1987a].

Les *méthodes par agrégation* consistent à remplacer par un seul moyen équivalent les groupes de deux moyens séparés par un stock intermédiaire. Dans cette démarche, il faut déterminer les paramètres du moyen équivalent : vitesse de travail équivalente, taux de défaillances équivalent, taux de réparations équivalent. Selon que l'agrégation commence par l'amont ou l'aval de la ligne, on peut obtenir des modèles équivalents différents (cf. figures 2.3 et 2.4) [Ancelin & al. 1987] [Terracol & al., 1987]. Le principal reproche fait à cette méthode est de ne prendre en compte qu'une propagation mono-directionnelle des événements : la figure 2.3 montre qu'il est impossible de répercuter les effets

bloquants de l'aval sur les paramètres équivalents du moyen agrégé équivalent « équ.12 » précédemment calculé. Ce constat a incité les chercheurs à délaisser cette méthode au profit des méthodes par décomposition [Burman, 1995].

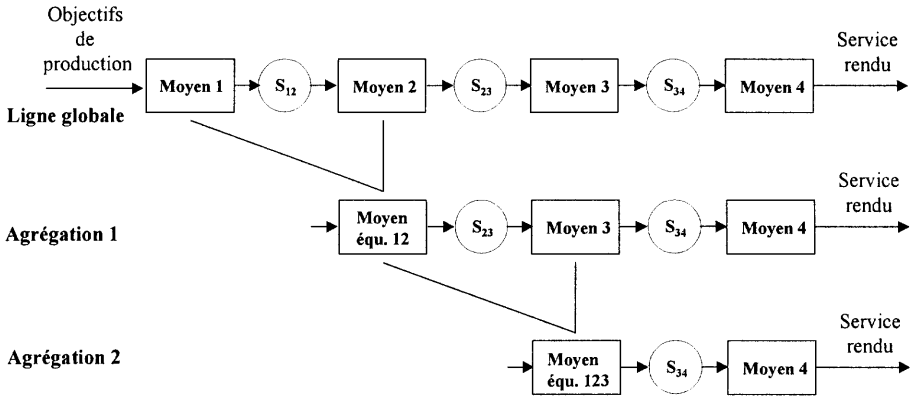

Figure 2.3 : Agrégation amont d'une ligne de production composée de quatre moyens

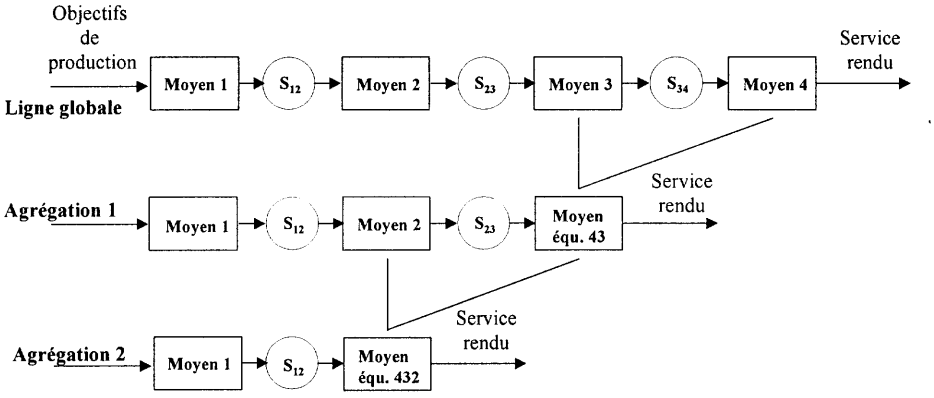

Figure 2.4 : Agrégation aval d'une ligne de production composée de quatre moyens

La *méthode par décomposition* la plus usitée est celle proposée par [Gershwin, 1987a]. Les premiers travaux relatifs à cette méthode ont permis d'élaborer un algorithme itératif pour des lignes de production homogènes qui a ensuite été étendu aux lignes de production non-homogènes [Gershwin, 1987b]. Le principe de la méthode par décomposition consiste à décomposer une ligne L constituée de N moyens en N-1 sous-ligne L(i), i allant de 1 à N-1. Chaque sous-ligne est modélisée par un moyen amont $M_a(i)$ et un moyen aval $M_v(i)$ séparés par un stock S(i). Le moyen amont $M_a(i)$ modélise la partie de la ligne L en amont du stock S_i et le moyen aval modélise la partie de la ligne L en aval de ce même stock. La méthode cherche à identifier les quatre paramètres inconnus, taux de défaillances $\lambda_a(i)$, $\lambda_v(i)$ et réparations $\mu_a(i)$, $\mu_v(i)$, des moyens amont et aval de chaque sous-ligne L(i).

Le calcul de ces paramètres est réalisé de sorte que le flux de pièces qui rentre et sort du stock S(i) de la sous-ligne se rapproche au maximum du stock S_i de la ligne réelle. Pour maintenir le même comportement, on affecte à S(i) une capacité identique à celle de S_i de la ligne réelle. Cette technique de décomposition est illustrée figure 2.5.

La décomposition en sous-lignes aboutit à des équations permettant d'identifier les paramètres $\lambda_a(i)$, $\lambda_v(i)$ et $\mu_a(i)$, $\mu_v(i)$ des sous lignes avec $i \in [1..N]$. Ces paramètres sont identifiés grâce à un algorithme appelé DDX (acronyme des initiales des auteurs) dont le critère de convergence est une équation de conservation de flux [Dallery & al.,1988] [Dallery & al., 1989].

Des améliorations à l'algorithme DDX ont été proposées et ont abouti à l'algorithme ADDX (Accelerate DDX algorithme) plus robuste et dix fois plus rapide avec une fiabilité de convergence proche de 100% [Burman, 1995]. La méthode analytique élaborée par [Gerschwin, 1987a] a été depuis étendue à deux moyens séparés par un stock à capacité finie, les deux moyens pouvant atteindre différents états de pannes contrairement aux travaux antérieurs qui ne se limitaient qu'à un seul état de pannes [Tolio & al., 2002].

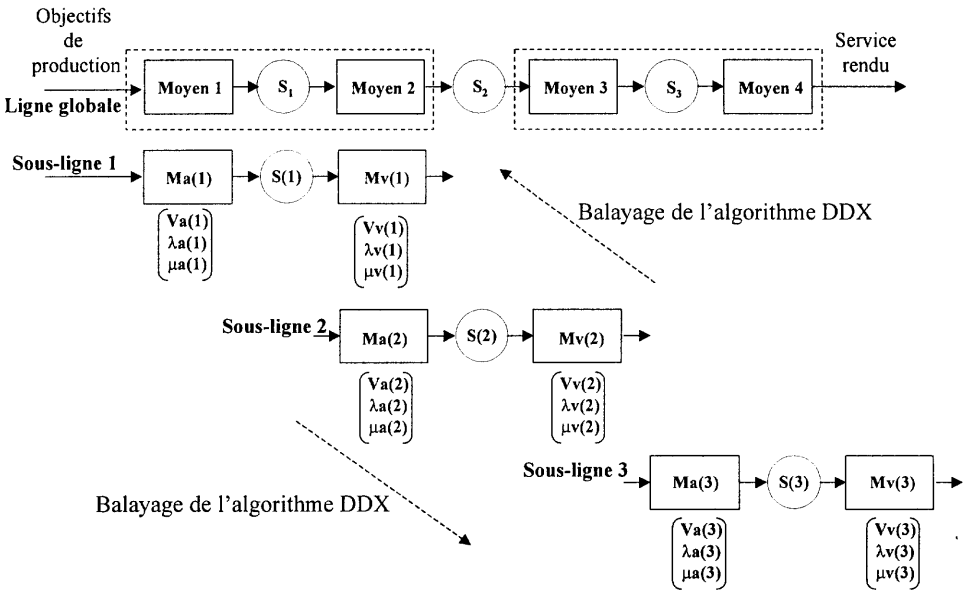

Figure 2.5 : Décomposition d'une ligne de N moyens

2.2.1.3 Modèles analytiques pour les lignes non-homogènes

Dans le cas des lignes non-homogènes, il faut non seulement identifier les quatre paramètres inconnus, taux de défaillances $\lambda_a(i)$, $\lambda_v(i)$ et réparations $\mu_a(i)$, $\mu_v(i)$, des moyens amont et aval de chaque sous-ligne L(i) mais aussi les paramètres vitesses $V_a(i)$ et $V_v(i)$ de ces moyens. Pour ce faire, la ligne non-homogène originelle subit une transformation — soit une *désagrégation* soit une *homogénéisation* — qui a pour but de rendre homogène une ligne non-homogène [Gershwin, 1987b] [Dallery & al. 1989].

L'approche par désagrégation proposée par [Gershwin, 1987b] vise à transformer une ligne non-homogène en une ligne homogène ayant un comportement équivalent afin de pouvoir appliquer ensuite l'algorithme de décomposition qu'il a développé. Pour ce faire, le principe consiste à remplacer tout moyen de la ligne originelle sauf le plus rapide par deux moyens équivalents ayant le même temps de cycle en supprimant le stock intermédiaire.

[Dallery & al., 1989] émettent cependant une certaine réserve par rapport à cette méthode qui conduit à des erreurs très significatives si les paramètres des différents moyens ne sont pas du même ordre de grandeur, cela est particulièrement vrai pour les taux de réparations.

L'approche par homogénéisation proposée par [Dallery & al. 1989] consiste à aligner la vitesse des moyens équivalents sur la vitesse du moyen le plus rapide de la ligne originelle et à appliquer l'algorithme DDX sur la ligne équivalente ainsi obtenue. Lorsque la ligne non-homogène s'approche des caractéristiques d'une ligne homogène, c'est à dire lorsque la vitesse des différents moyens est presque identique, la méthode par homogénéisation donne de bons résultats. D'autres algorithmes de décomposition ont été ultérieurement développés tels que ceux proposés par [Vargas, 1992] et [Le Bihan, 1998].

Les travaux menés au LAMIH se sont basés sur l'algorithme ADDX proposé par [Burman, 1995] pour la modélisation des lignes de production afin d'en évaluer la non-performance. Dans ce contexte, j'ai mené un certain nombre d'actions sur la métrologie des données, l'application et validation de la méthode, l'identification d'espoir de gain. Ces actions sont présentées dans le paragraphe suivant.

2.2.1.4 Proposition d'une méthode de diagnostic de non-performance de ligne de production

Cette méthode de diagnostic a été développée au sein de l'équipe Systèmes Homme-Machine sous la direction du Professeur Willaeys et sous l'égide de la société Prosyst, filiale de Schneider Electric, elle se décompose en trois étapes.

a) Métrologie des données

Une phase importante de la modélisation est la métrologie des données nécessaires à la réalisation du modèle pour l'évaluation des indicateurs de performance de la ligne étudiée. Ces indicateurs traduisent différentes notions telles que des notions de rendement (rendement synthétique RS), de disponibilité (propre DP, opérationnelle DO), de fiabilité (TFM), de maintenabilité (TAPM) et renseignent sur la qualité de la production (TQ). Vu le nombre important de données à appréhender et la nécessité de collecter des données fiables en provenance de la ligne de production, la collecte sur site représente une tâche délicate et complexe.

En premier lieu, j'ai mené des travaux de recherche portant sur l'identification des principales informations à mesurer et des indicateurs à calculer pour la modélisation de lignes réelles [Cauffriez & al., 1995b] [Cauffriez & al., 1996].

J'ai ainsi synthétisé dans [Cauffriez & al., 1997] l'ensemble E={tr, tf, tap, tai, tcn, tcr, pb, pt, nap} des indicateurs à calculer en fonction des informations d'entrée mesurées telles que : le temps requis (tr), le temps de fonctionnement (tf), le temps d'arrêt propre (tap), le temps d'arrêt induit (tai), le temps de cycle nominal (tcn), le temps de cycle réel (tcr), les pièces bonnes (pb), les pièces totales (pt), le nombre d'arrêts propres (nap).

J'ai prouvé dans [Cauffriez & al., 1997] que sept informations d'entrées sont au minimum nécessaires pour la détermination des indicateurs de performance avec une contrainte sur les équations (2.1) et (2.2) :

$$tf = pt \cdot tcr \tag{2.1}$$

$$tr = tf + tai + tap \tag{2.2}$$

Soient D1={tf, pt, tcr} et D2={tf, tr, tai, tap} les domaines respectifs des équations (2.1) et (2.2) et D=D1$\cup$ D2. Le cardinal de D est égal à 6 et le nombre maximal d'informations inconnues que l'on peut accepter dans ce cas est de 2 car on se ramène alors à un système de 2 équations à 2 inconnues. Ces 2 inconnues ne peuvent toutefois être choisies arbitrairement puisque les équations (2.1) et (2.2) sont liées ($D1 \cap D2 \neq \varnothing$), deux cas se présentent :

1) les 2 équations ont une variable inconnue en commun et le sous-ensemble des variables inconnues E' vaut alors E'={ x1, x2 : x1 $\in$ D1$\cap$D2, x2 $\in$ C(D1$\cap$D2) } avec C(D1$\cap$D2)={x : x $\notin$ D1$\cap$D2}.

2) les 2 équations n'ont aucune variable inconnue en commun. Il faut alors ajouter une condition restrictive pour s'assurer que les 2 variables inconnues n'appartiennent pas à la même équation. Le

sous-ensemble des variables inconnues E' vaut alors E'={ x1, x2 : x1 ∈ C_{D1} D2, x2 ∈ C_{D2} D1 } avec C_{D1} D2={x : x ∈ D1, x ∉ D2} et C_{D2} D1={x : x ∈ D2, x ∉ D1}.

Le retour d'expérience montre que E'={tf, tap} et E={tr, tai, pt, tcr, pb, tcn, nap} dans la plupart des cas.

Une fois cette phase de métrologie réalisée, il est alors possible d'appliquer la méthode de diagnostic élaborée qui calcule le moyen équivalent à la ligne en utilisant la démarche de décomposition reposant sur l'algorithme ADDX de [Burman, 1995]. Cette méthode repose sur les hypothèses des modèles analytiques présentés précédemment. Dans la pratique, il faut en effet vérifier que les données de production recueillies satisfassent ces hypothèses pour que la modélisation puisse être réalisée sur le système étudié. Les principales hypothèses sont les suivantes :

- le nombre de rebuts n'est pas suffisamment significatif pour affecter la production globale de la ligne,
- le temps de transfert entre deux moyens consécutifs est supposé nul,
- les distributions des temps de fonctionnement et de réparation sont exponentielles,
- un moyen ne peut tomber en défaillance que s'il travaille,
- la ligne de production est supposée saturée c'est-à-dire qu'il n'y a jamais de manque de matière première en début de ligne et qu'il y a toujours de la place pour décharger les pièces finies.

b) Diagnostic de premier niveau

La méthode proposée pour le diagnostic de premier niveau comporte 4 étapes :

1) Métrologie: Mesures pertinentes des informations nécessaires à l'évaluation de la performance (cf. métrologie des données)
2) Diagnostic de ligne : Faire un classement ordonné des moyens en calculant le RS de la ligne en suivant les points ci-après :
   - chaque moyen est "nominalisé", un par un, en saisissant dans le système de diagnostic développé à partir de ADDX, les valeurs définies pour une production nominale du moyen : Temps de cycle nominal tcn, Temps de fonctionnement moyen (MTTF ≈ TFM), temps d'arrêt propre moyen (MTTR ≈ TAPM),
   - un classement de ces moyens est effectué selon un critère de RS décroissant. Ce classement permet d'identifier les moyens contribuant au mauvais taux de production de la ligne.
3) Diagnostic moyen : Pour les moyens identifiés au point 2, le gain potentiel est calculé en agissant sur : la qualité, le taux de production, la fiabilité du moyen, la maintenabilité du moyen
4) Diagnostic Fiabilité-Maintenabilité : La méthode consiste à réaliser un classement des mauvais indicateurs de fiabilité et/ou maintenabilité. Le diagnostic de premier niveau est ensuite approfondi par un diagnostic de second niveau accompagné d'un calcul d'espoir de gain.

c) Diagnostic de second niveau : Espoir de gain

Le second niveau de diagnostic a pour but d'identifier l'espoir de gain réalisé en menant des actions sur le TFM, le TAPM et les temps d'arrêt induits par saturation et désamorçage (tai_{SAT} et tai_{DES}). La comparaison des espoirs de gain obtenus conduit à identifier les actions à mener pour l'amélioration de la performance de production de la ligne. Le tableau 2.1 présente une synthèse des formules démontrées dans [Cauffriez & al., 2003] pour l'identification d'espoir de gain de ligne de production constituant un modèle prédictif pour le diagnostic de performance.

Action sur :	Hypothèse	Espoir de gain
TFM $\rightarrow$ TFM_N	tai et TAPM ne changent pas	$\Delta pb_{TFM} = pb' - pb = pb\,(\frac{DP'}{DP} - 1)$
TAPM $\rightarrow$ $TAPM_N$	tai et TFM ne changent pas	$\Delta pb_{TAPM} = pb' - pb = pb\,(\frac{DP'}{DP} - 1)$
$tai_{DES} \rightarrow tai_{DESN}$	La diminution des tai_{DES} pour tendre vers la valeur nominale tai_{DESN} s'accompagne d'une augmentation de tf, tap et éventuellement des temps d'arrêt induits pour saturation tai_{SAT}	$\Delta pb_{DES} = pb' - pb = pb\,\frac{tai_{DES} - tai_{DESN}}{tf + tap + tai_{SAT}}$
$tai_{SAT} \rightarrow tai_{SATN}$	La diminution des tai_{SAT} pour tendre vers la valeur nominale appelée tai_{SATN} s'accompagne d'une augmentation de tf, tap et éventuellement des temps d'arrêt induits pour désamorçage tai_{DES}	Formule pessimiste : $\Delta pb_{SAT} = pb' - pb = pb\,\frac{tai_{SAT} - tai_{SATN}}{tf + tap + tai_{DES}}$ Formule optimiste : $\Delta pb_{SAT} = pb' - pb = pb\,\frac{tai_{SAT} - tai_{SATN}}{tf + tap}$
Action sur tap et nap	Diminution β des tap	$\Delta pb_{TAP} = pb' - pb = \frac{TQ}{tcr}\frac{\beta R}{R+1}$

Tableau 2.1 : Récapitulatif des espoirs de gain en fonction des actions menées

Bilan de l'action I.1 : 1 DEA soutenu [Guéguan, 1995], 1 thèse soutenue dans le cadre d'un contrat industriel avec la société Sevelnord (38 Keuros) [Patchong, 1997], 1 DRT soutenu [Boumaza, 2003] dans le cadre d'un contrat avec le centre de recherche Bosch Schwieberdingen (16 Keuros, Allemagne). En ce qui concerne ce DRT, j'ai été contacté par le centre de recherche Bosch Schwieberdingen pour participer aux travaux sur le projet COOPE (Cooperative Engineering) ; le projet COOPE s'inscrit dans une politique d'ingénierie simultanée appliquée aux lignes de production. Ce projet lancé depuis une dizaine d'années au sein du groupe Bosch vise à réduire la durée de conception des lignes de production tout en assurant une meilleure qualité du produit fini ; ma contribution a consisté à mettre en place des modèles de lignes non-homogènes pour estimer a priori les paramètres FMD des lignes conçues.

Au niveau publication, cette action a conduit à 3 congrès internationaux (AIAI, IEEE/SMC, EDA) [Cauffriez & al., 1995b] [Cauffriez & al., 1996] [Patchong & al., 1997], à une revue européenne JESA [Cauffriez & al., 1997], et à deux revues internationales International Journal of Advanced Manufacturing Technology (acceptée) [Cauffriez & al., 2005] et Control Engineering Practice (a passé un premier stade de reviewing) [Cauffriez & al., 2003].

2.2.2 Action I.2 : Maîtrise des flux par la quantification du coût de défaillances de synchronisation

Cette deuxième action de recherche porte sur la maîtrise des flux avec la détection, la localisation et l'identification des défaillances de rendez-vous entre plusieurs flux de production. Les aspects coûts ont été pris en compte avec l'introduction de la notion de coûts propres et de coûts induits par les défaillances. Ces travaux visent à définir une méthodologie pour la quantification du coût des défaillances de « désynchronisation de flux » ; l'événement redouté dans le cas présent est la perturbation du flux matérialisé par un rendez-vous manqué. L'objectif est ainsi de quantifier le coût de l'événement redouté « désynchronisation de flux » selon la fréquence, la nature des causes, les coûts propres et induits associés, selon le principe présenté figure 2.6, pour identifier les modes ayant des effets économiques significatifs.

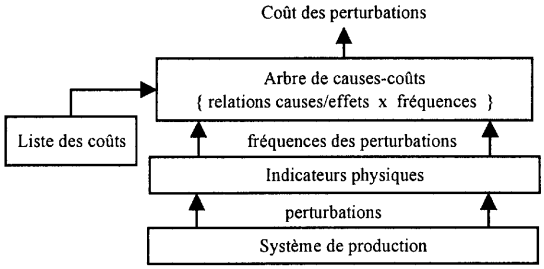

Figure 2.6 : Principe d'évaluation de l'événement redouté « Perturbation de flux »

Dans ce contexte, deux méthodes ont été proposées : la méthode AMD2E pour « Analyse des Modes de Défaillances et de leurs Effets Economiques » et la méthode MAEC pour « Méthode de l'Arbre Economique des Causes ».

Ces deux méthodes ont été appliquées et validées chez Renault-Douai dans le cadre de la thèse de S. Aramini. Les perturbations, causes de la désynchronisation des flux, ont pu être classées en trois catégories pour le cas d'étude de Renault-Douai :

- les *sorties de flux*, qui concernent les contrôles de fabrication, les retouches sur véhicules, l'extraction et le tri local de certains véhicules,
- les *règles de gestion du flux* des véhicules, qui concernent les choix d'orientation des véhicules en fonction des contraintes techniques dans les différents ateliers,
- les *causes externes*, qui sont les défaillances des installations ou fournisseurs au niveau des approvisionnements.

Deux types d'effets sont à distinguer : les effets propres et les effets induits ; les effets propres sont directement liés au mode de défaillance et les effets induits résultent de la propagation de l'effet propre dans le système. A un effet propre est associé un coût propre et à un effet induit est associé un coût induit. L'élaboration de l'AMD2E passe par quatre étapes : la définition des frontières du système de production, la spécification des modes de défaillances et de leurs causes, les effets de ces modes, le chiffrage du coût élémentaire de ces effets dans les différents points du flux.

La figure 2.7 représente les relations liées au mode de défaillance. Les principaux modes de défaillances retenus sont liés au système de production. Seuls les effets mesurables, pertinents et financièrement quantifiables sont pris en compte dans la constitution du coût des perturbations.

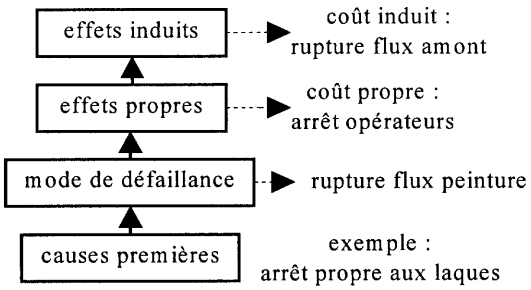

Figure 2.7 : Relations liées au mode de défaillance

L'élaboration de l'AMD2E consiste en une première phase d'analyse. La deuxième phase a pour objet de définir un Arbre Economique des Causes (Méthode de l'Arbre Économique des Causes MAEC). Cette phase conduit à une représentation graphique des combinaisons d'événements les plus probables menant à la réalisation d'un événement redouté unique. Les règles de base de la construction sont identiques aux règles employées pour la méthode de l'arbre des fautes [Villemeur,

1988] [Kumamoto & al., 1996]. Chaque événement se voit attribuer deux variables supplémentaires qui sont la fréquence d'apparition de la perturbation et son coût moyen évalués sur une période d'observation donnée, l'opérateur employé pour relier les événements dans l'arbre est le OU logique. Les causes de défaillances 1 et 2 de niveau i alimentent l'entrée de l'opérateur OU (cf. figure 2.8), chaque cause de niveau j se voit attribuer une fréquence d'apparition f_{ji} et un coût moyen Cm_{ji}. Le coût total de l'effet résultant est déduit du coût moyen de chaque cause et du coût propre Cp_{ji} à l'effet isolé à partir de l'équation (2.3).

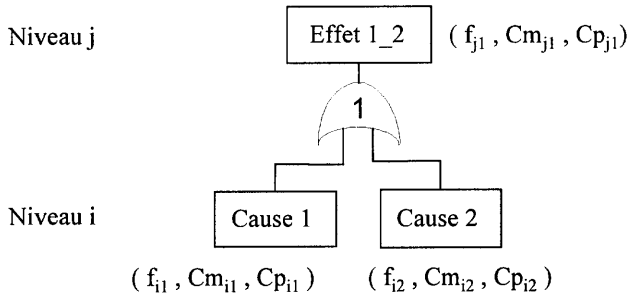

Figure 2.8 : Opérateur OU isolé et variables associées

$$Cm_{j1}=\frac{f_{i1}\times Cm_{i1}+f_{i2}\times Cm_{i2}+f_{j1}\times Cp_{j1}}{f_{j1}} \text{ avec } f_{j1}=f_{i1}+f_{i2}\neq 0 \qquad (2.3)$$

L'emploi de l'arbre économique des causes nécessite la vérification de plusieurs hypothèses :

- les causes élémentaires 1 et 2 doivent être uniques, indépendantes et ne peuvent se produire simultanément,
- la distribution des causes est supposée exponentielle, ce qui simplifie les calculs des probabilités en sortie des opérateurs logiques,
- la propagation des causes dans l'arborescence est à sens unique (absence de cycle),
- l'additivé des coûts permet leur propagation dans la branche de l'arbre.

Pour l'exemple de la figure 2.9, l'occurrence de l'événement redouté « Défaillances de rendez-vous » conduit à un coût journalier moyen égal au produit $f61\times Cm61$. Ceci permet d'identifier l'impact de la fréquence des perturbations du flux en prenant en compte le coût moyen : faible fréquence fort coût ou faible coût forte fréquence. Une analyse de sensibilité peut facilement être réalisée à partir de la méthode MAEC en inhibant la propagation de chaque cause de défaillance élémentaire dans l'arbre.

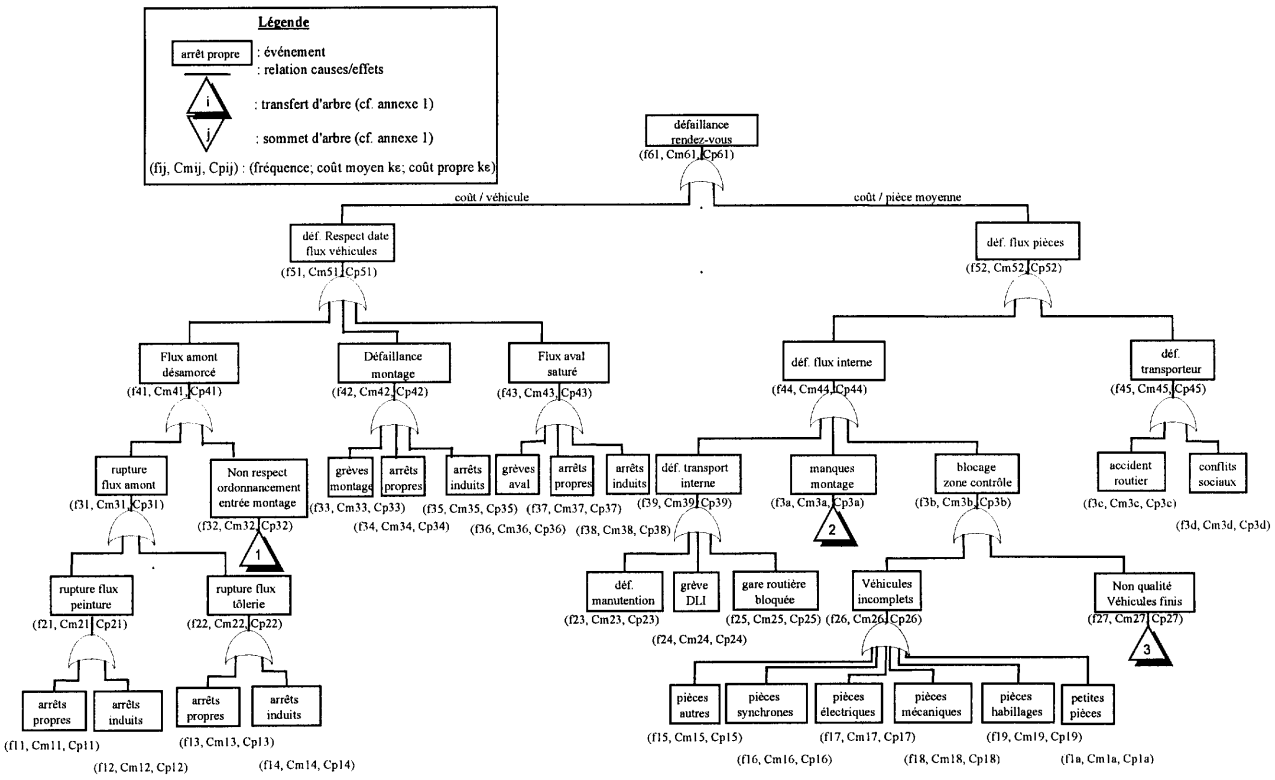

Figure 2.9 : Méthode de l'Arbre Economique des Causes

Les avantages de la méthode MAEC sont les suivants :

- la méthode MAEC permet de structurer de façon hiérarchique les relations de causes à effets économiques dans le système de production,
- une analyse de sensibilité des causes premières et un classement des perturbations les plus onéreuses permettent de définir les chemins critiques de l'arbre,
- la méthode MAEC constitue un outil d'aide à la décision dans la mesure où les coûts sont proches de la réalité et les variables de décision sont présentes dans l'arbre,
- cette description permet d'évaluer les pertes financières en identifiant les perturbations liées aux défaillances et les actions à mener pour les inhiber.

Les inconvénients portent sur les points énumérés ci-après :

- l'arbre construit par la méthode MAEC est spécifique à un système donné, il nécessite une analyse régulière des défaillances, un suivi de leur évolution et une correction des équations de l'arbre en fonction des dysfonctionnements identifiés,
- la mise à jour régulière des fréquences des perturbations, des coûts des causes premières et du coût des effets propres s'impose,
- un nombre important de modes de défaillances implique de nombreux niveaux dans l'arbre rendant la description à base de ce formalisme plus complexe.

Bilan de l'action I.2 : Les méthodes AMD2E et MAEC ont été appliquées et validées lors de la thèse de [Aramini, 1999] réalisée dans le cadre d'un contrat industriel avec la société Renault Douai (69 Keuros) et soutenue à huis clos. Les publications relatives à ces travaux ont fait l'objet de 4 congrès internationaux (IMACS98, Esrel01, Qualita01, Esrel02) [Aramini & al., 1998] [Renaux & al., 2001] [Renaux & al., 2001b] [Renaux & al., 2002].

2.3 Conclusion sur l'axe I

Les travaux de recherche de l'axe I portaient sur l'amélioration de la performance de lignes de production. J'ai montré qu'une phase importante de la modélisation de lignes industrielles réelles consiste en la métrologie des données nécessaires à la réalisation du modèle. Les principales informations à mesurer sur sites parmi les myriades d'informations délivrées par les lignes de production ont fait l'objet d'une étude approfondie.

Une méthode de diagnostic a été proposée pour améliorer les paramètres FMD (Fiabilité-Maintenabilité-Disponibilité) des lignes de production et en diagnostiquer les causes de non-performance. Cette méthode calcule le moyen équivalent à la ligne de production en utilisant une démarche de décomposition selon l'algorithme ADDX.

Ces travaux ont permis de cerner sur le cas particulier des lignes de production les deux approches permettant de caractériser et modéliser la complexité : soit *l'agrégation* d'entités pour aller vers le système complexe, soit la *décomposition* du système complexe pour aller vers les entités.

La maîtrise des flux est le deuxième aspect qui a été étudié pour l'amélioration de la performance de lignes de production. Cette maîtrise des flux consiste en la détection, la localisation et l'identification des défaillances de rendez-vous entre plusieurs flux de production. Les aspects coûts, primordiaux dans le contexte industriel ont été abordés avec l'introduction de la notion de coûts propres aux défaillances et de coûts induits par les défaillances. Cette maîtrise des flux montre également, sur le cas particulier des lignes de production, les problèmes d'interaction et de dépendance au sein de systèmes complexes.

Je poursuis sur l'axe I une activité de veille dans la mesure où j'en assure l'enseignement au sein de l'ENSIAME. A partir de ces travaux sur l'évaluation des paramètres FMD de processus physiques, il m'a semblé opportun d'étudier l'impact du service rendu par le système d'automatisation sur le comportement du processus physique. En effet, une faible disponibilité du système d'automatisation peut conduire à une faible disponibilité du processus physique. La présentation de mes contributions et résultats sur cette thématique de recherche fait l'objet de l'axe II.

Axe II : Sûreté de fonctionnement des Systèmes d'Automatisation à Intelligence Distribuée

2.4 Positionnement dans la communauté scientifique

Mes travaux s'attachent essentiellement à l'étude de la sûreté de fonctionnement prédictive des systèmes d'automatisation. Le modèle élaboré par [Rafoux, 1995] organise une telle étude autour de 2 axes : l'axe 1 se focalise sur les études relatives aux équipements, matériels, aux systèmes d'automatisation et de sécurité alors que l'axe 2 privilégie les opérateurs et l'environnement (cf. figure 2.10).

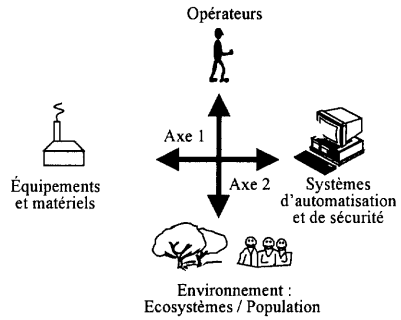

Figure 2.10 : Les deux axes de la sûreté de fonctionnement prédictive

Depuis 1994, je travaille essentiellement sur les aspects relatifs à l'axe 1 avec l'étude de la sûreté de fonctionnement des Systèmes Automatisés à Intelligence Distribuée (SAID) pour la conception de systèmes complexes sûrs de fonctionnement.

Depuis 2000, j'ai étendu mes activités de recherche à l'évaluation de la sûreté de systèmes de transports guidés dont la problématique couvre les axes 1 et 2. Cette thématique s'inscrit dans la politique de recherche de la région Nord-Pas-de-Calais avec le pôle de compétitivité i-trans et dans la politique de l'union européenne avec le projet UGTMS Urban Guided Transport Management System ($5^{ème}$ PCRD).

2.4.1 Positionnement par rapport à la communauté « Instrumentation intelligente et réseaux de terrain »

En 1981, un rapport du Professeur Soutif de l'Université de Grenoble souligne que le développement de la microélectronique doit aboutir au développement de nouveaux capteurs et actionneurs, appelés SMART Instruments et des systèmes de communication associés. Le livre blanc édité en 1987 sous l'égide du CIAME et de l'AFCET a contribué à analyser les besoins en matière de mesure intelligente et à dégager les spécificités des composants intelligents [Ciame-Afcet, 1987]. Un instrument intelligent a ainsi été défini par son aptitude à communiquer, décider et agir.

Côté systèmes de communication, un groupe de travail a été créé en France en 1982 regroupant des universitaires et industriels, cette recherche a abouti au réseau de terrain FIP devenu depuis Worldfip [Thomesse, 1997]. Au niveau européen, des normes nationales ont été votées P-Net au Danemark [DS 21906, 1990], Profibus en Allemagne [DIN 19245a-c, 1990], FIP en France [NF C46602-604, 1990].

Parallèlement, un certain nombre de réseaux de terrain ont vu le jour dont les plus connus sont : Arcnet, ASI, Batibus, Bitbus, CAN, Devicenet, EIB, FAIS, Flexray, Hart, Interbus-S, LON, Modbus/Jbus, Profibus-FMS/PA, Profibus-DP, SDI-12, Sercos,VAN. Des réseaux de terrain spécifiques à la sécurité machine ont également été développés : réseaux Safety-Bus p, SiBus...

Les principales exigences en matière de réseaux de terrain vont dans le sens d'une plus grande modularité, évolutivité, interopérabilité, interchangeabilité, une meilleure fiabilité-maintenabilité-disponibilité-sécurité (détection et recouvrement d'erreurs de transmission, respect des contraintes temporelles, compatibilité électromagnétique...), une meilleure performance, et une minimisation des coûts.

Le réseau en lui-même n'a que peu d'intérêt ; ce qui importe c'est le système d'automatisation pris dans sa globalité. Il convient toutefois de constater que le choix du réseau va faciliter ou non la distribution de l'application. De même, le choix de distribution de l'application conduit à choisir tel réseau plutôt que tel autre. Cette analyse s'applique à tout type de système d'automatisation que ce soit en production, en domotique ou en embarqué (trains, métros, voitures,...) ; la différence porte sur

la satisfaction des contraintes de temps de réponse du système d'automatisation (notion de temps-réel, de temps critique) et des contraintes de sûreté pour l'application développée.

Côté normalisation, l'effort mené pour obtenir une norme internationale en matière de réseaux de terrain a été un échec pour différentes raisons :

- la diversité des applications : systèmes continus, systèmes discrets, systèmes embarqués, etc..
- les méthodes de conception et d'implémentation des systèmes automatisés reposant sur ces nouvelles technologies,
- la qualité de service rendu par le système de communication,
- la concurrence entre les différents offreurs.

Côté recherche, la communauté scientifique se répartit en deux grandes tendances :

- la *définition de services et de nouveaux protocoles* pour garantir une qualité de service adéquate aux différents types d'application et aux différentes stratégies de répartition du système d'automatisation [Decotignie, 1993] [Decotignie, 1999] [Decotignie, 2002] [Hong, 1995] [Juanole, 2002] [Kopetz, 1997] [Kopetz, 2002] [Thomesse, 1999a] [Tindell & al., 1995a-c] [Le Lann, 1993] [Le Lann & al., 1994] [Salvatore & al., 2002],

- la *définition de capteurs actionneurs intelligents, leur modélisation et l'apparition de profils de communication* garantissant les exigences d'interopérabilité et d'interchangeabilité [Bayart, 1993], [Benoit, 1993] [Benoit & al., 2000] [Benoit & al., 2001][Bouras, 1995] [Dapoigny, 04] [Dias, 1993] [Masten, 1997] [Mauris & al., 2002] [Neumann & al., 2002] [Robert & al., 1993] [Staroswiecki & al., 1994] [Staroswiecki & al., 1996] [Thomesse, 1997] [Thomesse, 1999b].

2.4.2 Positionnement par rapport à la communauté « Conception d'application distribuée »

La démarche globale de conception des systèmes automatisés repose sur un ensemble d'activités élémentaires qui vont de l'expression des besoins à l'exploitation-maintenance. La modélisation de ces activités a donné naissance à un certain nombre de modèles dans le domaine du génie logiciel qui ont été étendus aux systèmes automatisés. On peut citer à titre d'exemple le modèle en cascade [Royce, 1970], en V proposé par le mouvement français pour la qualité, ou en spirale [Boehm, 1988] [Lepreux, 2003].

La particularité de ces systèmes automatisés repose sur leur complexité dont les différents aspects ont été mentionnés au chapitre 1 : complexité fonctionnelle, structurelle, comportementale ou technologique ; la mission de ces systèmes automatisés repose sur un ensemble de systèmes interconnectés ou en interaction qui assure une ou plusieurs fonctions spécifiques et concourt à un certain niveau de complexité.

Cette complexité justifie les travaux sur la modélisation hiérarchique et l'approche systémique développée par [Lemoigne, 1994] qui ont donné naissance à d'autres méthodes d'analyse et de modélisation [Millot, 2003]. Ces méthodes reposent sur le modèle MFM (Multilevel Flow Modelling, Danemark) de [Lind, 1990] qui prône une décomposition du système global selon deux axes : l'axe buts/moyens et l'axe tout/partie (cf. figure 2.11).

L'axe buts/moyens se décline en trois niveaux de modèles : niveau des objectifs, niveau des fonctions, niveau des composants. Il existe donc une hiérarchie avec passage d'un niveau plus global à un niveau plus granulaire ; le modèle élaboré à un niveau donné est un but pour ce même niveau qui devient un moyen pour le niveau immédiatement supérieur. Quant à l'axe tout/partie, il est une conséquence de la décomposition selon l'axe buts/moyens : plus on est près du but, plus le système est

pris dans sa globalité ; plus on est près des moyens, plus la modélisation concerne les parties.

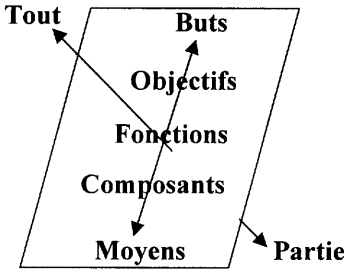

Figure 2.11 : Décomposition multiniveau d'un grand système [Lind, 1990]

La phase de conception oblige ainsi à prendre en compte non seulement les *parties* (moyens logiciels et matériels) mais aussi à étudier le *tout* avec la répartition du logiciel sur le matériel (répartition des traitements, des contrôles des traitements, des données, du contrôle d'accès aux données, de l'horloge globale...) ; cette problématique rend nécessaire l'établissement de méthodes pour valider le résultat obtenu.
Une démarche classique de conception s'appuie sur trois phases :

- la modélisation de l'architecture fonctionnelle, abstraction faite de la partie matérielle. Cette phase de modélisation vise à décrire les fonctions réalisées par l'application. La spécification fonctionnelle peut être réalisée à partir de différents outils et langages tels que Java, méthode B, orientée objet, réseaux de Petri, blocs diagrammes, langages de description d'architecture tels que UML. Un objectif est privilégié : obtenir un langage d'implémentation, définir des blocs fonctionnels modulaires, standardisés et réutilisables, spécifier des méthodes de preuve formelle pour la vérification des propriétés de l'application (vérification du code, respect des contraintes temporelles, détection d'état puits, faculté à s'auto-initialiser,....).
- la modélisation de l'architecture matérielle qui résulte du choix des équipements (réseaux, équipements, systèmes d'exploitation,...) supportant l'application. Cette description concerne les capteurs et actionneurs intelligents, les réseaux de terrain, les contrôleurs, les machines hôtes accueillant les interfaces Homme-Machine pour le contrôle-commande, la supervision, la maintenance et le suivi. Cette modélisation nécessite de prendre en compte les caractéristiques techniques des équipements : taille mémoire, caractéristiques de la CPU, temps d'exécution, débit du réseau, ordonnancement des tâches et des messages...
- la modélisation de l'architecture opérationnelle qui décrit la projection et l'affectation des fonctions apparaissant dans la modélisation de l'architecture fonctionnelle. Cette description est partiellement faite si l'architecture contient des équipements dotés de fonctions intégrées. Ces équipements sont hétérogènes et ne peuvent en aucun cas être complètement propriétaires. Ils accueillent une partie de l'application et doivent être configurés, téléchargés et « orchestrés » comme un tout ; leurs fonctions intégrées doivent être compatibles et interopérables. Les contraintes et les caractéristiques des applications organisées autour de réseaux de terrain montrent un certain nombre de spécificités qui font que ces applications se différencient des applications classiques.

Les actions de recherche menées par la communauté scientifique portent sur :

- la *modélisation et la description de l'architecture opérationnelle* à des fins de validation [Simonot-Lion, 1999]. Cette validation porte sur les aspects fonctionnels, temporels, d'interopérabilité entre le réseau de terrain et les équipements (capteurs, actionneurs intelligents, calculateurs, automates programmables,...), de dimensionnement, de performance. Certains langages de description appliqués à l'embarqué émergent [Elloy & al., 2002] [Migge & al., 2000].

- la *définition d'outils logiciels* pour la programmation de l'application, son implémentation, sa configuration et sa phase de test. Il apparaît nécessaire de disposer d'outils de CAD couvrant l'ensemble des phases de conception allant de la spécification à l'implémentation. Ces outils doivent être dotés de modèles réalistes des protocoles de réseaux de terrain, des profils des instruments intelligents et des modèles d'applications distribuées [Son & al., 2003].
- *L'évaluation du niveau de sûreté* des applications organisées autour de réseau de terrain qui doivent être sûres de fonctionnement, sécuritaires, et tolérantes aux fautes. Les principaux travaux dans ce domaine sont les suivants : [Barger & al.,, 2002] [Barger & al.,, 2004] [Campelo & al., 1997] [Conrard & al., 2000] [Conrard & al., 2004] [Juanole & al., 1995] [Juanole & al., 1998] [Meunier & al. , 2000] [Moncelet, 1998] [Barger & al., 2004] [Thiriet, 2004].

2.4.3 Positionnement par rapport à la communauté sûreté de fonctionnement

La sûreté de fonctionnement est par nature interdisciplinaire. J'ai montré au chapitre 1 qu'elle pouvait affecter différents aspects de la société : santé, politique, transport, industries. La sûreté de fonctionnement, qui se définit comme la science des défaillances, prend en compte les différents aspects de l'aléatoire et a recours aux méthodes et techniques des sciences pour l'ingénieur (SPI : automatique, sciences de l'information, ingénierie des systèmes), des sciences humaines et sociales (SHS : sciences de gestion, sociologie, économie), et des sciences de la vie (SDV : ergonomie, santé, psychologie).

Mes travaux se sont essentiellement focalisés durant la dernière décennie sur la modélisation et l'élaboration de méthodes pour évaluer la sûreté de systèmes complexes soumis à défaillances (domaine relevant du SPI). Ce travail a demandé d'acquérir une vue globale des méthodes, modèles, hypothèses et techniques qui sont propres à cette problématique.

A noter que depuis 2000, mes travaux prennent en compte les aspects SDV et SHS, avec mon implication dans la sûreté et sécurité des systèmes de transports guidés, Projet UGTMS du 5ème PCRD et réseaux d'excellence EURNEX. Les systèmes de transport guidés sont à proprement parler des systèmes dynamiques hybrides [Zaytoon, 2002] dont on doit évaluer la sécurité opérationnelle dès la phase de conception. Les aspects fiabilité humaine sont indissociables des aspects fiabilité technique lorsqu'il s'agit d'étudier la maîtrise des risques.

Il existe de nombreux ouvrages traitant de la sûreté de fonctionnement [Pagès & al., 1980] [Villemeur, 1988] [Laprie & al., 1995] [Kumamoto & al., 1996] [Zwingelstein, 1996] [Niel & al., 2002] [Pham, 2003]...

Les principaux laboratoires, instituts et réseaux qui travaillent au niveau national sur une thématique proche de la mienne sont :

- le CRAN de Nancy (M. Robert, J-M Thiriet) qui propose une méthode d'aide à la conception de systèmes automatisés à intelligence distribuée selon trois approches complémentaires : statique, dynamique et informationnelle,
- le LAAS de Toulouse (R. Valette, G. Juanole) qui modélise par réseaux de Petri les protocoles de communication et les systèmes à événements discrets,
- le LAB de Besançon (N. Zerhouni) qui applique les réseaux de Petri flous à la surveillance,
- le LAG de Grenoble CAPA/S3D (S. Gentil, J-M. Flaus) qui développe une méthodologie d'analyse et d'évaluation des indicateurs caractéristiques de sûreté reposant sur la modélisation, l'évaluation, la décision pour une étude de sensibilité afin de valider l'architecture de systèmes de conduite,

- le LAGIS de Lille (M. Bayart, B. Conrard) qui travaillent sur des modèles de capteurs/actionneurs intelligents et l'optimisation d'architecture connectée en réseaux à base d'instruments intelligents,
- l'INSA de Lyon (I. Blum) qui modélise le fonctionnement de réseaux de communication,
- le LAI/3SP de Lyon (E. Niel) qui a travaillé sur la sécurité opérationnelle pour l'analyse des dysfonctionnements, la conception et la réalisation de moyens de détection assurant un niveau de sécurité pour les plateformes robotiques et pour les opérateurs,
- le LAP/ADS de Bordeaux (Y. Dutuit) qui développe une approche de fiabilité dynamique par réseaux de Petri,
- le LASQUO d'Angers (B. Dumon) qui s'intéresse à la sûreté de fonctionnement lors du cycle de vie des produits, de la conception à la production, en passant par le développement et en prenant en compte le système (matériel et logiciel) et les contraintes financières du projet,
- le LCIS de Valence (D. Genon-Catalot) qui implante des applications autour de réseaux terrain,
- le LGP de Tarbes (D. Noyes) qui développe des modèles conceptuels de données pour l'analyse des risques,
- le LISTIC d'Annecy (E. Benoit, G. Mauris) qui modélise et conçoit des capteurs intelligents à base de la théorie d'ensembles flous probabilistes-possibilistes,
- le LM2S de Troyes (E. Châtelet, C. Berenguer) qui travaille sur les aspects fiabilistes et maintenance,
- LURPA/ISA de Cachan qui propose des apports formels et méthodologiques pour améliorer la sûreté de fonctionnement et les performances des systèmes de commande discrets,
- les RTP 20 (Fiabilité, diagnostic et tolérance aux fautes des systèmes complexes), 21 (Sûreté de fonctionnement des systèmes complexes ouverts), 55 (Systèmes commandés en réseaux),
- côté instituts, on peut citer l'IMdR/SDF, l'INRS, l'INERIS et l'INRETS,
- côté indutriels, le CEA et EDF/DER qui s'intéressent de près à cette thématique de recherche.

2.5 Contributions majeures sur la conception de systèmes d'automatisation sûrs de fonctionnement

La complexité des systèmes d'automatisation rend nécessaire leur décomposition en sous-systèmes ; ces sous-systèmes doivent accomplir une mission principale qui repose sur un ensemble de sous-fonctions.

J'ai proposé dans [Cauffriez & al., 2003c] le modèle de la figure 2.12 (inspiré du modèle 3 axes et adapté aux études de sûreté) qui présente l'avantage de faire clairement apparaître cette décomposition pour un système d'automatisation donné :

- *l'axe fonctionnel* représente les différentes fonctions du système d'automatisation pour le système étudié,

- *l'axe hiérarchique* représente la décomposition d'une fonction selon un certain nombre de niveaux hiérarchisés,

- *l'axe topologique* représente la topologie du processus physique pour le système étudié ; il peut s'agir de matériels, d'équipements, de capteurs, d'actionneurs.....

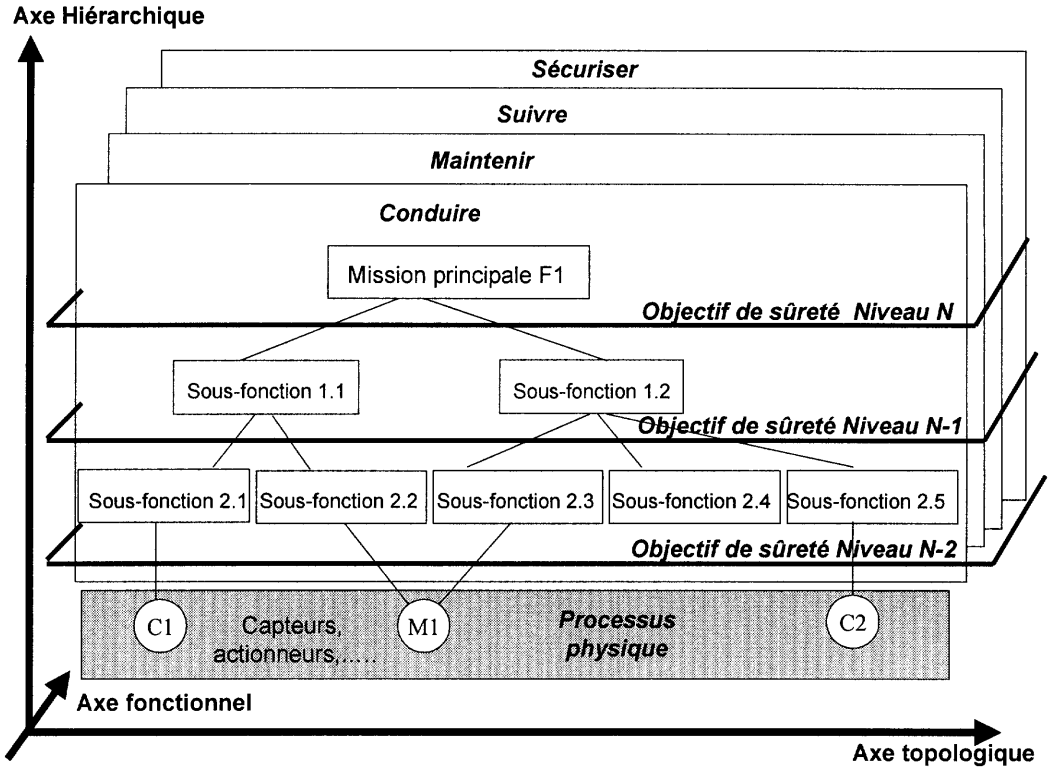

Figure 2.12 : Modèle de décomposition hiérarchique, topologique et fonctionnelle d'un système sûr de fonctionnement

La décomposition en niveaux selon l'axe hiérarchique fait apparaître les objectifs de sûreté propres à chaque niveau : à titre d'exemple, la « Mission principale F1 » doit requérir une disponibilité de 99% et un niveau de sécurité SIL 4. Cette modélisation sous forme de niveau de sûreté vise à rappeler que l'objectif global de sûreté ne peut être atteint que si les objectifs de sûreté de chaque niveau sont satisfaits. Mais s'il est aisé d'assigner à une fonction donnée une exigence de disponibilité ou de sécurité, il appartient aux concepteurs de prouver que la fonction réellement réalisée suite à la projection et l'allocation des sous-fonctions sur le matériel satisfait aux objectifs de sûreté (cf. figure 2.13). A ce stade, doivent également être détectées les incohérences pour que des fonctions indépendantes ne conduisent pas à des modes opératoires contraires : à titre d'exemple pour la figure 2.12, une faute de conception peut conduire la sous-fonction 2.2 à donner un ordre d'accélération au moteur M1 et la sous-fonction 2.3 à donner un ordre contraire au même instant. De même, un système ne peut être en mode de conduite automatique et en mode manuel.

Il appartient donc au concepteur de valider les fonctions opérationnelles obtenues et éventuellement de les optimiser parmi les solutions admissibles selon un ou plusieurs objectifs qui respectent les contraintes énoncées dans le cahier des charges ; on peut en effet envisager que l'implémentation de la « Mission principale F1 » se fasse différemment selon les compromis envisagés : sécurité élevée et faible disponibilité ou bien forte disponibilité et faible sécurité sous contraintes de faible consommation et de faible encombrement [Conrard, 1999].

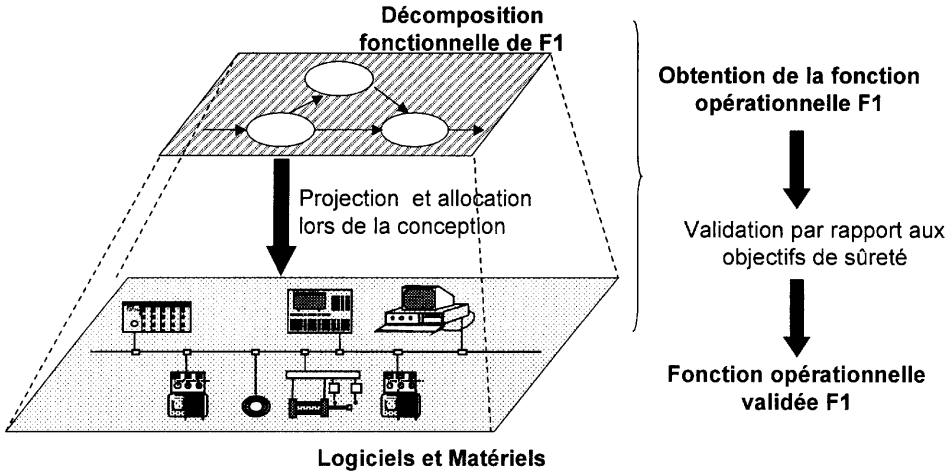

Figure 2.13 : Obtention d'une fonction opérationnelle validée

Il va de soi que cette démarche de projection et d'allocation doit être étendue à l'ensemble des fonctions du système d'automatisation en recherchant le meilleur compromis sur l'ensemble des fonctions et en évitant des optima locaux. La phase de conception d'un système d'automatisation doit ainsi s'appuyer sur des méthodes et outils pour prédire, combattre, éliminer ou tolérer les fautes identifiées. Ces méthodes doivent permettre de prouver, pour le système conçu, un certain nombre de propriétés relatives aux aspects :

- *Temporels* : il s'agit de prendre en compte les contraintes temporelles (voire temps critiques) et de définir une métrique pour le système étudié,
- *Performances* : cela concerne les performances matérielles (capacité de traitement, mémorisation, faibles coûts, fiabilité accrue, miniaturisation, nombre d'entrées-sorties) mais aussi les performances logicielles (exécutif mono-tâche ou multi-tâche, algorithmes séquentiels ou concurrents, ordonnancement de tâches, approche asynchrone ou synchrone),
- *Interopérabilité* : c'est-à-dire être capable de coopérer avec d'autres composants d'automatismes dans et pour une application particulière, cette aptitude nécessite a minima la possibilité de communiquer et de s'échanger des informations,
- *Interfonctionnement* : les composants d'automatisme dialoguant doivent parler le même langage, dans le cas d'une pression il ne faudra pas mélanger les bars et les PSI,
- *Interchangeabilité* : le composant d'un fabricant doit pouvoir être remplacé par celui d'un autre fabricant sans altération des comportements prévus,
- *Sûreté de fonctionnement* : le système conçu doit répondre aux exigences de fiabilité, maintenabilité, disponibilité et sécurité pour l'application mise en œuvre,
- *Assurance qualité* : respect des normes qualité (ISO 9000 par exemple) pour la maîtrise et l'évaluation de l'activité de conception : documentation, définition des activités, contrôles, tests,...
- *Conformité* : le système doit être conforme aux exigences requises qui sont souvent définies sous forme de normes : normes machines, normes ferroviaires pour obtenir la certification nécessaire à l'exploitation du système (certification selon les domaines par l'INRS, l'INERIS, ou CERTIFER...).

Je souligne dans [Cauffriez & al., 1994] la nécessité d'évaluer la sûreté de fonctionnement à chaque étape de la conception par rapport aux spécifications du système qui doivent comporter :

- la spécification du service approprié en terme de fonctionnalités du système incluant les conditions dans et sous lesquelles ces fonctions doivent être remplies : performances, durée, observabilité, promptitude, disponibilité, ...

- la spécification du service inapproprié, c'est-à-dire la durée acceptable d'un service inapproprié, mode de défaillance contrôlé, ...

Ces descriptions doivent être exprimées sous la forme d'objectifs quantifiés de performances et notamment de mesures de sûreté. Certains modèles peuvent servir de référence lors de séances de brainstorming tels que le modèle de [Embrey, 1992] (cf. figure 2.14). Ce modèle présente l'avantage de mettre en évidence les mécanismes qui peuvent conduire à un accident en identifiant des causes directes et sous-jacentes.

C'est dans ce contexte que j'ai mené trois grandes actions de recherche qui sont présentées dans les paragraphes suivants.

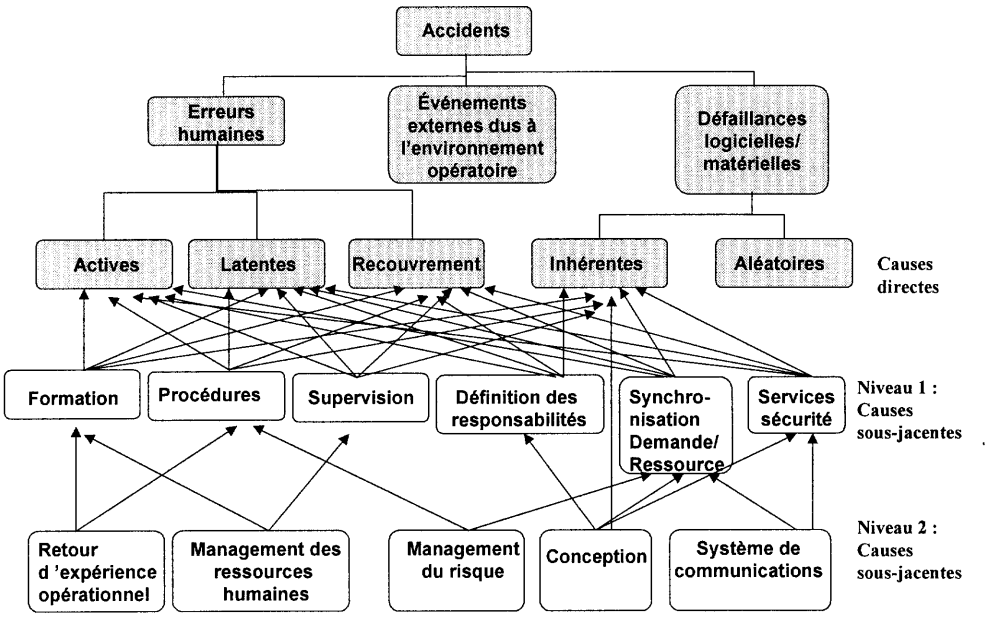

Figure 2.14 : Modèle de Embrey présentant les mécanismes conduisant à un accident

2.5.1 Action II.1 : Intégrité des informations et cohérence temporelle dans les systèmes d'automatisation à intelligence distribuée

La conception d'un système sûr de fonctionnement doit se fonder sur les moyens de la sûreté de fonctionnement. Outre l'aspect matériel lié aux défaillances premières ou aux défaillances externes induites par l'environnement, *l'intégrité des informations transmises* représente un fondement pour rendre la transmission sécuritaire vis à vis de certaines fautes.

Cette intégrité des informations transmises dépend de la nature des informations véhiculées ; ceci m'amène à distinguer deux types d'information au sein d'un système d'automatisation :

- les *informations dites de sécurité* telles que : informations d'état et de défaut, informations relatives à des commandes de mise en sécurité (ordres de mise en repli),
- les *informations générales de fonctionnement.*

De ce point de vue, il me semble qu'un système de communication sécuritaire devrait pouvoir s'appuyer sur deux protocoles distincts dédiés respectivement aux informations de sécurité et aux informations générales de fonctionnement [Cauffriez & al., 2005b-c]. Le système de communication, en dépit d'une complexité accrue, serait à la fois sûr (pour les informations de sécurité) et efficace (pour les informations générales de fonctionnement). De même, il est envisageable d'étendre ce point

de vue aux *informations de sécurité* issues des fonctions de sécurité directe dont le dysfonctionnement serait immédiatement préjudiciable et aux *informations issues des fonctions de sécurité indirecte* dont la défaillance n'engendre pas immédiatement de risque, mais abaisse le niveau de sécurité.

Les défaillances qui peuvent entraver l'intégrité des informations sont soit des défaillances en valeur, soit des défaillances temporelles. C'est précisément cet aspect temporel que j'ai étudié dans [Cauffriez, & al., 1995] en introduisant le concept de *viabilité de l'information.* La *viabilité* qui est un dérivé de l'adjectif viable s'applique aux *choses qui sont aptes à vivre, qui présentent les conditions anatomiques et physiologiques indispensables à une certaine durée de vie.* La notion de durée de vie implique qu'une information viable est exploitable durant un certain temps. Au-delà de ce laps de temps, l'information jugée trop vieille, n'est plus exploitable : on dit qu'elle est non-viable.

Ceci m'a amené à faire la distinction entre la *cohérence temporelle de l'information* et la *cohérence temporelle d'un ensemble d'informations* :

- *Appliqué à une information donnée*, ce concept vise à garantir que toutes les fonctions consommatrices de cette information (ou les sites consommateurs) ont une image datant du même instant. Dans ce cas, je parle de cohérence temporelle de l'information.
- *Appliqué à un ensemble d'informations*, ce concept vise à garantir que la cohérence temporelle de chaque élément de l'ensemble est respectée et que toutes les informations appartenant à cet ensemble ont été produites à l'intérieur d'une même fenêtre temporelle et sont toutes valides dans cette fenêtre. En outre, j'ai mis en évidence dans [Cauffriez & al., 1999-1999b] que le respect de la cohérence temporelle est intrinsèquement lié aux méthodes d'accès au médium de communication (accès aléatoire reposant sur la méthode CSMA, ou bien accès contrôlé reposant sur une gestion centralisée, décentralisée, hybride), aux modes d'adressage (adressages par les variables ou adressages par les équipements), aux types de trafic (périodique ou apériodique).

J'ai introduit de prime abord le concept de viabilité de l'information pour éviter toute prise de décision aberrante due au non-respect de la cohérence temporelle d'un ensemble d'informations et autoriser des prises de décision dégradée. Ce non-respect de la cohérence temporelle peut être occasionné par des défaillances (du réseau ou des processus applications) entraînant le non-rafraîchissement d'informations par un ou plusieurs producteurs et/ou la non-arrivée d'informations chez un ou plusieurs sites consommateurs.

Ces défaillances peuvent survenir aussi bien dans une prise de décision élaborée à partir d'un ensemble d'informations produites par des processus synchrones (processus dont l'exécution est associée à des indications du réseau) que dans une prise de décision élaborée à partir d'un ensemble d'informations produites par des processus asynchrones (processus dont l'exécution est indépendante du réseau). Se pose alors la question : que faire en cas de défaillances ? On peut envisager de:

1. Surseoir à la décision et tirer profit de la redondance temporelle naturelle offerte par un type de trafic périodique,
2. Surseoir à la décision et enclencher une procédure de reprise, cela revient à recourir à une redondance temporelle effective (par opposition à la redondance temporelle naturelle),
3. Appliquer la décision après avoir évalué les risques encourus,
4. Prendre une décision dégradée telle que procédure de sauvegarde, maintien des sorties en l'état afin de réduire la criticité de la situation.

En outre, il ressort de cette contribution scientifique que l'utilisation de lois de viabilité associées aux informations permettent d'accorder un taux de confiance à une prise de décision élaborée à partir d'un ensemble d'informations et ainsi de crédibiliser cette prise de décision. Ce taux de confiance peut alors engendrer:

- soit une prise de décision dégradée: on sait que des variables non-viables ont contribué à la prise de décision, mais comme il est impossible de consulter ces informations avant la prise de décision (soit par manque de temps, soit parce que l'application ne le permet pas), il faut impérativement prendre une décision dégradée,
- soit une prise de décision avec un taux de confiance maximum, si on a la possibilité de consulter les informations jugées non-viables avant la prise de décision.

Lors de la conception d'un système réparti, il est nécessaire de définir les types de trafic requis par l'application. L'approche, qui consiste à faire circuler les informations selon un mode périodique, oblige à rechercher l'ensemble des variables cycliques ayant la même périodicité dans le but de vérifier l'aptitude du réseau à accepter la charge. Pour mener à bien cette tâche, il est nécessaire d'avoir une vue globale des échanges d'informations au sein du système réparti; ceci va à l'encontre des démarches de conception qui prônent généralement une décomposition du problème en sous-ensembles indépendants.

Par contre, une approche apériodique correspond à une approche plus naturelle pour la mise en œuvre d'applications indépendantes, et ce, grâce à la gestion dynamique des échanges mais pose le problème de la garantie des temps de réponse intrinsèquement liée à la charge du réseau. Le concepteur doit choisir le type de trafic pour son application en fonction de la nature de l'information transmise *informations de sécurité* ou *informations générales de fonctionnement* et de la granularité de l'application.

Bilan de l'action II.1 :

Les travaux relatifs à cette action de recherche ont été menés dans le cadre des DEA de Frédéric Dessi [Dessi, 1996] et de Rémy Renard [Renard, 1998] dont j'ai effectué l'encadrement à 100%. Ces travaux de DEA ont consisté à mettre en place la plate-forme FIP au sein du laboratoire et à implémenter le concept de viabilité de l'information proposé sur une régulation de température distribuée autour de ce réseau de terrain.

Ces travaux ont fait l'objet d'une revue européenne [Cauffriez & al., 1995] et 2 congrès internationaux [Cauffriez & al., 1999-1999b].

L'étude comparative sur les réseaux de terrain (comparaison de 22 réseaux de terrain) s'appuie sur les travaux de veille technologique réalisés dans le cadre du GT CIAME (Comité Interprofessionnel pour l'Automatisation et la MEsure), qui ont abouti à un ouvrage collectif de 203 pages publié chez Hermès et rédigé sous ma direction [Cauffriez & al., 1999c] ; les perspectives de ces travaux sont présentées dans le chapitre 3 de ce mémoire.

2.5.2 Action II.2 : Analyse des Modes de défaillances et des Effets pour la fonction « Communication » au sein d'un système d'automatisation

La description de l'architecture fonctionnelle, qui fait abstraction de la partie matérielle, renforce la nécessité d'étudier l'interaction entre les fonctions élémentaires et de modéliser les échanges d'informations dont les caractéristiques sont nombreuses telles que : taille des messages, périodicité des messages, contraintes de temps, délai de prise en compte d'une requête, délai de réception d'un acquittement, sécurité-confidentialité (divulgation de l'information), sécurité-intégrité (altération de l'information), sécurité-innocuité (milieu sensible tel que atmosphère explosive).

Si l'on reprend la boucle Mesure/Décision/Action présentée au chapitre 1 paragraphe 1.3.2.1, l'architecture fonctionnelle se décompose alors en trois fonctions élémentaires : fonction « Mesure », fonction « Décision », fonction « Action ». Mais ces trois fonctions ne peuvent interopérer que si elles

communiquent et s'échangent des informations ; la boucle Mesure/Décision/Action se transforme ainsi en Mesure/Communication/Décision/Communication/Action telle que représentée sur la figure 2.15.

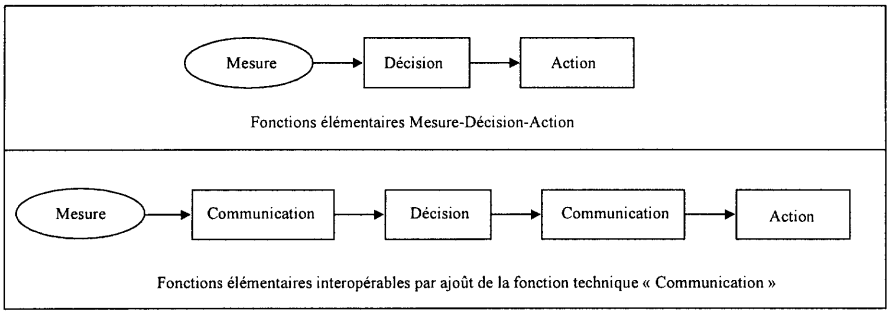

Figure 2.15 : Fonction « Communication » au sein d'une architecture distribuée

Si la fonction « Communication » n'appartient pas à la mission principale du système, elle en fait partie intégrante et toute défaillance de cette fonction peut affecter le bon fonctionnement du système ; une analyse des modes de défaillances de cette fonction et l'étude des conséquences pour le système s'impose donc.

De ce point de vue, j'ai orienté ma recherche sur le thème de la sûreté de fonctionnement des systèmes d'automatisation en me focalisant selon une approche réseau. Afin d'identifier les modes de défaillances de la fonction « Communication », les causes et les effets sur le système d'automatisation, j'ai envisagé une démarche inductive reposant sur une analyse AMDE. L'analyse AMDE réalisée s'appuie sur le modèle OSI [Lepage & al. 1989]. Dans le cas de réseaux de terrain, ce modèle OSI est réduit aux couches Physique, Liaison de Données, Application et Management de réseau (cf. figure 2.16) [Mammeri & al., 1993].

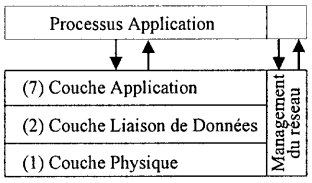

Figure 2.16 : Modèle ISO/OSI réduit pour un système de communication temps critique

Cette analyse AMDE des modes de défaillances et des causes possibles (causes internes ou externes) a pour but de conduire à une meilleure compréhension de la fonction « Communication » et de prendre en compte, dès la phase de conception, les effets de ces modes de défaillances sur le fonctionnement du système d'automatisation.

La première version que j'ai proposée de cette AMDE a fait l'objet d'une publication au congrès SICICA'97 [Cauffriez & al., 1997]. Cette première version a ensuite servi de document de base pour les séances de brainstorming du GT CIAME (devenu entre-temps Club 18.4 de la SEE et rebaptisé Composant Intelligent pour l'Automatisation et la Mesure) et a été enrichie par une réflexion collective avec des laboratoires de recherche et industriels suivants : CRAN (Nancy), LAGIS (Lille), LCIS(Valence), LISTIC(Annecy), INERIS (Verneuil en Halatte), INRS (Nancy), INRETS (Villeneuve d'Ascq), CEA (Saclay), Crouzet (Valence).

Je présente ci-après une synthèse des points de vue évoqués lors des réunions parfois très animées suite à des divergences d'opinion mais qui ont de manière constructive permis d'élaborer l'AMDE donnée par les tableaux 2.2 à 2.4.

L'objectif visé est de mettre en relation un mode de défaillances considéré avec la couche du modèle OSI, les moyens de détection pouvant être localisés dans une autre couche du modèle OSI (il convient de rappeler qu'un mode de défaillances d'un composant est défini comme l'effet permettant

d'observer la défaillance de ce composant) :
1) Modes de défaillances identifiés au niveau de la couche physique :

- la non-réception de signaux par un ou plusieurs sites consommateurs conduit à une perte de l'information pour le système d'automatisation car le médium est un point dur du système d'automatisation,
- l'émission continue sur le réseau provoque une surcharge du système de communication. Il est alors possible que le service approprié ne soit pas rendu dans le temps imparti pour le système d'automatisation. Il y a donc défaillance du système de communication qui peut conduire à une faute pour le système d'automatisation. Il est nécessaire de rendre le système sécuritaire vis-à-vis de cette faute pour éviter qu'elle ne soit préjudiciable à la sûreté. La disponibilité est également réduite, mais la nature temporaire du phénomène fait que le système retrouve rapidement toutes ses aptitudes à fournir un service approprié.

2) Modes de défaillances identifiés au niveau de la couche liaison de données :

- l'arrivée d'une trame erronée à la couche Liaison de Données conduit à une information non valide pour le système d'automatisation (à noter que cette trame est forcément complète, c'est à dire non tronquée, puisque selon le principe OSI, la couche physique ne l'aurait pas transmise à la couche liaison de données). La couche Liaison de Données est parfois dotée de mécanisme de recouvrement pour les erreurs de transmission (compensation, reprise, ou poursuite) suite à détection par un code détecteur d'erreurs. Il est à noter que ce recouvrement ne doit être mis en œuvre que si le système le permet temporellement, et si l'intégrité de l'information n'est pas altérée pas ce recouvrement.
- l'arrivée d'une information temporellement erronée conduit à une information temporellement non valide. Parmi les causes possibles, on recense le non-respect des délais de production et/ou le non-respect des délais de transmission.

3) Modes de défaillances identifiés au niveau de la couche application :

- comme le système de communication a en charge la maîtrise du temps affecté à sa communication, il convient de ne pas négliger l'aspect transmission des informations. Le non-respect des délais de transmission conduit à l'arrivée d'une information temporellement erronée au niveau de la couche application et a fortiori à une information temporellement non valide. Le non-respect des délais de production est également une cause possible d'information temporellement non valide.
- outre l'aspect matériel lié aux défaillances premières ou aux défaillances externes de l'environnement, l'intégrité des informations transmises et la cohérence temporelle des informations (cf. paragraphe 2.5.1) sont les fondements pour rendre la transmission sécuritaire vis-à-vis de certaines fautes. Je rappelle que l'intégrité des informations transmises dépend de la nature des informations véhiculées : informations de sécurité ou informations générales de fonctionnement.

4) Modes de défaillances identifiés au niveau de la couche gestion du système de communication :

- la gestion du système de communication soulève la problématique de la « non-détection de la disparition d'une station » ou « la non-détection de l'apparition d'une station » qui peut être catastrophique si la station concernée gère l'accès au réseau. Dans ce cas, l'effet pour le système d'automatisation est une interruption de l'accès au médium. Il faut toutefois souligner que la couche gestion de réseau dépend fortement du réseau étudié : station privilégiée qui possède la liste des stations actives et la réactualise (maître), fonction Node Guarding qui permet de détecter la disparition d'une station.
- la défaillance au niveau de la couche gestion de système de communication peut provenir d'une faute de conception ou d'une faute opérationnelle : cas de deux stations s'étant vues affecter la même adresse lors de la phase de conception ou à l'issue d'une opération de maintenance.

	Modes de défaillance	Causes possibles	Effets sur le système d'automatisation	Moyens de détection	Actions correctives		Evitement
					Recouvrement par poursuite	Recouvrement par compensation	
Couche Physique	Non-Réception de signaux par un ou plusieurs sites consommateurs	Perturbation de la transmission sur le médium (trame totalement illisible ou en partie) problème lié au début de trame, fin de trame, décodage de bit	Perte de l'information	1) Utilisation d'un compte-rendu de requête au niveau de la couche 2 (négatif dans ce cas) 2) Surveillance des paramètres électriques de la ligne (fuites à la masse, amplitude signal trop faible ou trop élevée)	1) Redondance temporelle effective 2) Redondance temporelle naturelle Adéquation avec les contraintes temps-réel de l'application		Adéquation du médium au besoin (Paire torsadée blindée, coaxial, fibre optique, ...) Précautions de câblage, surveillance des alimentations)
		Agression externe (pincements, coupure, déformation, chocs, conditions climatiques, vieillissement, désadaptation d'impédance : perte de la terminaison de ligne	Perte de l'information	1) Utilisation d'un compte-rendu de requête au niveau de la couche 2 (négatif dans ce cas) 2) Utilisation de mécanisme de cohérence temporelle implanté couche 7 3) Surveillance des paramètres électriques de la ligne (fuites à la masse, amplitude signal trop faible ou trop élevé)		Redondance active du médium et de la couche physique Le temps de basculement du Gestionnaire d'Accès au réseau doit être négligeable (Exemple de WorldFip : problème de la reprise du vecteur d'état de l'Arbitre de bus)	Précautions de câblage, qualité du câblage de l'installation, qualité physique (soudures)
		Abonné non-connecté sur le réseau		Sous-détection de courant (déconnecté)	Répétition des tentatives d'émission jusque succès	Redondance de l'abonné si la station concernée gère l'accès au réseau : maître/esclave ou arbitre de bus	
		Abonné connecté au réseau mais en court-circuit		Sur-détection de courant (court-circuit)	Fonctionnement en mode dégradé en cas d'échec		Isolation galvanique Transformateur d'isolement Parafoudre
	Emission continue sur le réseau (bavardage intempestif)	Répétition infinie des tentatives d'émission	Surcharge réseau	1) Chien de garde intégré au microprocesseur de communication 2) Comptage des erreurs d'acquittement (exemple de CAN)	Auto déconnexion de l'émetteur Déconnexion physique de l'émetteur par un tiers		Limitation personnalisée du nombre de tentatives d'émission
		Défaillance première d'un composant		Redondance matérielle		Redondance matérielle	Evitement des modes communs par diversification matérielle

Tableau 2.2 : AMDE de la Couche Physique

	Modes de défaillance	Causes possibles	Effets sur le système d'automatisation	Moyens de détection	Actions correctives		Evitement
					Recouvrement par poursuite	Recouvrement par compensation	
Couche Liaison de Données	Arrivée d'une trame erronée	Perturbation due à l'environnement (électromagnétique, ...)	Information fournie non valide	Code détecteur d'erreur : Envoi de deux trames complémentées	1) Redondance temporelle effective (apériodique) 2) Redondance temporelle naturelle (périodique) Adéquation avec les contraintes temps-réel de l'application	Utilisation d'un code de correction d'erreur	Qualité de blindage suffisante : - paire torsadée blindée - câble coaxial - fibre optique en silice (+) ou plastique (-)
		Défaillance première d'un composant de couche liaison de données		Redondance matérielle		Redondance matérielle	Evitement des modes communs par diversification matérielle
	Arrivée d'une information temporellement erronée	Non-respect des délais de production	Information temporellement non-valide	Mécanisme de détection du respect des délais de production chien de garde, timers	1) Redondance temporelle effective 2) Redondance temporelle naturelle	Estimation de la valeur	Redondance du producteur
		Non-respect des délais de transmission	Information temporellement non-valide	Mécanisme de détection du respect des délais de transmission chien de garde, timers	1) Redondance temporelle effective 2) Redondance temporelle naturelle	Estimation de la valeur	

Tableau 2.3 : AMDE de la Couche Liaison de Données

	Modes de défaillance	Causes possibles	Effets sur le système d'automatisation	Moyens de détection	Actions correctives		Evitement
					Recouvrement par poursuite	Recouvrement par compensation	
Couche Gestion de Réseau	Non-détection de la disparition d'une station Non-détection de l'apparition d'une station Arrêt gestionnaire	Erreur de configuration Erreur de configuration Défaillance première	Perte des informations produites Perte des informations produites Interruption de l'accès au médium	Mécanisme de détection du respect des délais de production chien de garde, timers Mécanisme de détection du respect des délais de production chien de garde, timers		Redondance du gestionnaire d'accès au réseau	Mécanisme de détection dynamique apparition/disparition Mécanisme de détection dynamique apparition/disparition Diversification matérielle et logicielle du gestionnaire d'accès au réseau

Tableau 2.4 : AMDE de la Couche Application

Bilan de l'action II.2 :

Cette action de recherche a permis d'élaborer une AMDE de la fonction « Communication » dans un système d'automatisation distribuée et a permis d'identifier pour les couches du modèle OSI réduit les modes de défaillances, leurs causes possibles, les effets sur le système d'automatisation, les moyens de détection et de recouvrement par poursuite ou compensation ainsi que les procédures d'évitement lors de la conception du système d'automatisation.

Les travaux relatifs à cette action de recherche ont fait l'objet d'un congrès international [Cauffriez & al., 1997b], d'une revue internationale Reliability Engineering and System Safety [Cauffriez & al., 2004] et de 2 chapitres dans un ouvrage collectif à paraître en 2005 [Cauffriez & al., 2005b-c]. Les perspectives de ces travaux sont présentées dans le chapitre 3 de ce mémoire.

2.5.3 Action II.3 : Proposition d'une méthodologie de Codesign pour la conception de systèmes d'automatisation sûrs de fonctionnement

La démarche de conception d'un système d'automatisation nécessite d'aborder un certain nombre de points délicats lors de la construction d'une architecture opérationnelle sûre de fonctionnement. Je livre dans les paragraphes qui suivent une réflexion personnelle sur cette problématique en mettant en exergue les différents types de contraintes que tout concepteur peut rencontrer. Cette réflexion m'amène à proposer une méthodologie de Codesign pour la conception de systèmes d'automatisation sûrs de fonctionnement.

2.5.3.1 Difficultés rencontrées lors de la conception de systèmes d'automatisation sûrs de fonctionnement

La première difficulté repose sur la répartition, l'allocation, la projection, l'agrégation de l'architecture fonctionnelle sur l'architecture matérielle. Il s'agit d'envisager les différentes solutions pour lesquelles les contraintes sont respectées (contraintes de sûreté de fonctionnement mais aussi des contraintes autres, telles que le coût...), d'évaluer pour chaque solution les critères et retenir finalement la solution la meilleure par rapport aux critères privilégiés. De ce point de vue, la première étape consiste à lister l'ensemble des contraintes pour le système d'automatisation, de les exprimer clairement, d'étudier leurs interactions et leurs éventuelles incompatibilités.

La deuxième difficulté vise à identifier les solutions partielles qui satisfont les contraintes identifiées. La complexité des systèmes fait que le nombre de solutions envisageables est important et il est alors nécessaire de recourir à de l'algorithmique. Les méthodes actuellement les plus utilisées pour les problèmes d'allocation sont : *le gradient descendant, le recuit simulé, la recherche Tabou, les algorithmes génétiques* [Akaichi, 1996] [Conrard, 1999] et *les réseaux de contraintes* dont les algorithmes de backtracking et de filtrage permettent respectivement d'énumérer les solutions et de restreindre l'espace des solutions [Piechowiak, 2001].

La troisième difficulté réside dans le choix d'une solution parmi toutes celles qui satisfassent les contraintes. Pour ce faire, il faut comparer les différentes solutions selon un ou plusieurs critères. A défaut de solutions optimales, il faudra se contenter d'une solution satisfaisant au mieux les objectifs fixés et reposant sur d'éventuels compromis.

2.5.3.2 Expression des contraintes d'une architecture opérationnelle

Les contraintes d'une architecture opérationnelle peuvent se décliner en trois grandes classes :

- contraintes dépendantes des spécifications fonctionnelles,
- contraintes dépendantes des spécifications matérielles,

- contraintes de sûreté qui dépendent à la fois de l'ingénierie « générale » du système, des spécifications matérielles et logicielles[Laprie & al., 1995].

2.5.3.2.1 Contraintes dépendantes des spécifications fonctionnelles

Parmi les contraintes dépendantes des spécifications fonctionnelles, sont à distinguer :

- les *contraintes implicites aux caractéristiques des fonctions élémentaires* qui imposent la solution d'allocation/projection : certaines caractéristiques de ces fonctions rendent en effet obligatoire l'affectation de ces fonctions sur du matériel qui est le seul à satisfaire les besoins,
- les *contraintes de regroupement* qui imposent, une fois une fonction élémentaire affectée à un matériel donné, de regrouper sur ce même matériel d'autres fonctions élémentaires,
- les *contraintes d'exclusion* qui obligent, une fois une fonction élémentaire affectée à un matériel donné, de dissocier d'autres fonctions élémentaires dont les caractéristiques sont incompatibles.

2.5.3.2.2 Contraintes dépendantes des spécifications matérielles

Les principales contraintes dépendantes des spécifications matérielles sont les suivantes :

- les *contraintes de capacité mémoire* qui conduisent à exclure des fonctions élémentaires trop gourmandes en mémoire,
- les *contraintes de gestion des fonctions* qui imposent de limiter le nombre de fonctions élémentaires implémentables sur un même matériel,
- les *contraintes d'échanges de données* qui doivent être telles que la capacité de la fonction « Communication » étudiée dans l'action II.2 de ma recherche ne soit pas rapidement dépassée,
- les *contraintes d'entrées/sorties* qui conduisent à exclure des fonctions élémentaires trop gourmandes en entrées/sorties.

2.5.3.2.3 Contraintes de sûreté

Les contraintes de sûreté imposent de recourir à des techniques de diversification fonctionnelle et matérielle.

a) Diversification fonctionnelle pour des contraintes de fiabilité

La fiabilité mesure la continuité d'un service. Lorsque le service repose sur un ensemble de sous-fonctions, la fiabilité de la mission globale du système dépend de la fiabilité/disponibilité de chacune des sous-fonctions et de l'état physique des composants du système. Il s'agit alors d'étudier la robustesse du service global suite à l'apparition d'un événement indésirable affectant une sous-fonction donnée et d'identifier les conséquences de cet événement sur la continuité du service global. Compte tenu de la probabilité d'apparition de cet événement indésirable, il faut alors chercher à caractériser la fréquence et la durée de la perte du service global.

La réalisation de la mission globale du système dépend fortement des modes de défaillances de la partie opérative : une régulation de débit reposant sur une structure de deux vannes mises en série peut se faire pour une des deux vannes bloquée en position ouverte mais est impossible pour un blocage en position fermée.

b) Diversification fonctionnelle pour des contraintes de disponibilité

En fonction de la fréquence et de la durée de la perte du service global, il peut paraître nécessaire de s'affranchir de ces situations en procédant à une diversification fonctionnelle par le biais de redondance pour des contraintes de disponibilité.

L'état d'indisponibilité d'une fonction globale dépend alors directement de l'état de disponibilité des sous-fonctions en redondance. La forme de la redondance peut être soit passive soit active. Dans le cas d'une redondance passive, il faut s'affranchir d'une défaillance de l'entité assurant la commutation entre les sous-fonctions redondantes. Pour une redondance active, il faut s'appuyer sur un vote majoritaire de type m/n pour éviter que des fonctions indépendantes ne conduisent à des modes opératoires contraires.

c) Diversification fonctionnelle pour des contraintes de sécurité

Les contraintes de sécurité imposent l'identification des états sécuritaires du système global parmi tous les états que ce dernier peut prendre. Lorsque les contraintes de sécurité sont fortes, il faut recourir à un système de sécurité indépendant du système d'automatisation dont la mission est de mettre en repli, dans tous les cas, l'installation en présence de modes de défaillances préjudiciables pour la sécurité [EN50126, 2000].

Le service global rendu par le système de sécurité peut également se décomposer en fonctions et sous-fonctions jusqu'à obtenir des fonctions élémentaires. La problématique de conception du système de sécurité se ramène ainsi à celle d'un système d'automatisation à hautes exigences en matière de fiabilité et disponibilité. Il appartient au concepteur de vérifier que la décomposition en fonctions n'introduit pas de brèches dans le système de sécurité selon le principe de défense en série préconisé par [Reason, 1993]. En liaison avec la gravité des événements redoutés et de leur fréquence d'occurrence, les normes définissent un niveau d'intégrité de la sécurité SIL (Safety Integrated Level, cf. tableau 2.5) que l'on peut définir comme étant le niveau de confiance que l'on peut accorder au respect des exigences de sécurité allouées à une fonction de sécurité [CEI61508a]. Sur ce point, une problématique de recherche intéressante est l'identification du niveau de SIL global pour un système de défense en série composé d'un ensemble de fonctions de sécurité. Ce thème de recherche fait l'objet de la thèse de Melle Julie BEUGIN que j'encadre à hauteur de 50%.

Niveau d'intégrité de sécurité	**Mode de fonctionnement à faible sollicitation**[1] (Probabilité moyenne de défaillance à exécuter, lors d'une sollicitation, la fonction pour laquelle il a été conçu)	**Mode de fonctionnement continu ou à forte sollicitation** (Probabilité d'une défaillance dangereuse par heure)
4	≥ 10-5 à < 10-4	≥ 10-9 à < 10-8
3	≥ 10-4 à < 10-3	≥10-8 à <10-7
2	≥ 10-3 à < 10-2	≥ 10-7à < 10-6
1	≥10-2 à <10-1	≥ 10-6 à < 10-5

Tableau 2.5 : Niveaux d'intégrité de sécurité d'après [CEI61508a]

[1] Un mode de fonctionnement à faible sollicitation est caractérisée par une fréquence des demandes plus grande que une par an et au plus égale à deux fois la fréquence des tests périodiques alors qu'un mode de fonctionnement à forte sollicitation est plus grande que une par an ou supérieure à la fréquence des tests périodiques. Cette définition tirée de la norme [CEI61508a] montre l'absence de définition explicite pour une fréquence des demandes inférieure à une par an ; ce dernier cas pourrait en effet caractériser un mode de fonctionnement à très faible sollicitation.

2.5.3.2.4 Diversification matérielle

Le concepteur est tôt ou tard confronté à la projection, allocation, agrégation de l'architecture fonctionnelle sur le matériel pour la réalisation des fonctions spécifiées.

Cette activité n'est pas sans conséquence pour l'obtention des objectifs de sûreté de fonctionnement du système. En outre, le regroupement de fonctions sur un même matériel peut engendrer un mode commun de défaillances pour l'ensemble de ces fonctions en cas de défaillance du matériel support d'exécution. Il appartient donc au concepteur de faire en sorte que des fonctions définies de manière redondante pour des objectifs de fiabilité, de disponibilité, ou de sécurité au niveau de l'architecture fonctionnelle ne soient pas regroupées sur un même matériel pour ne pas annihiler les objectifs de sûreté souhaités. Ceci introduit donc une contrainte supplémentaire en obligeant le concepteur à recourir à des diversifications matérielles qui visent à fournir des services identiques via des conceptions et réalisations séparées [Laprie & al., 1995]. Cette démarche s'applique également à des *fonctions techniques* telles que la fonction « communication » ou « gestion des modes d'utilisation » du système automatisé.

2.5.3.3 Modélisation de l'architecture fonctionnelle

a) Architecture fonctionnelle de la mission principale du système

Je propose d'étudier les systèmes par rapport à leur mission principale, identifiée par des modes de fonctionnement donnés (nominaux ou dégradés) reposant sur la disponibilité de macro-fonctions. L'accomplissement de ces macro-fonctions est quant à lui exprimé sous forme de services rendus par un ensemble de services élémentaires nécessitant l'exécution d'entité(s) logicielle(s) sur une entité matérielle. La figure 2.17 décline ce point de vue. C'est donc sur la fiabilité, disponibilité, maintenabilité des entités logicielles et matérielles que reposent la fiabilité, disponibilité, et maintenabilité des services élémentaires. L'exploration de cette approche du problème, sur les plans qualitatifs et quantitatifs en terme de sûreté, a fait l'objet de la thèse de V. Benard. Le tableau 2.6 illustre l'ensemble des services possibles pour un mode d'utilisation donné.

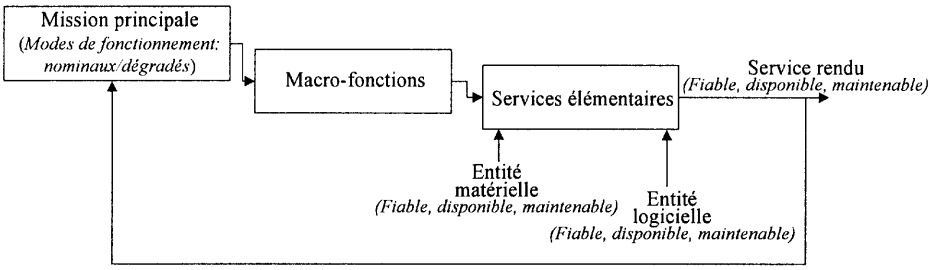

Figure 2.17 : Déclinaison de la mission principale d'un système

Modes de fonctionnement de la mission principale / Services élémentaires	Nominal 1	Nominal 2	■ ■ ■	Dégradé 1	Dégradé 2	■ ■ ■	Dégradé n
1							✓
2	✓			✓			
3	✓	✓					
4		✓			✓		
■ ■							
n-1							
n							

Tableau 2.6 : Identification des modes de fonctionnement nominaux ou dégradés pour la mission principale du système en fonction de la disponibilité des services élémentaires

L'ensemble de ces fonctions constitue l'architecture fonctionnelle qui peut alors être facilement modélisée à partir des méthodes et outils usuels : SADT, SART, Merise, Graphes fonctionnels, Objet, UML, Petri, langages synchrones (Lustre, Esterel, Signal)…

L'avantage des méthodes orientées « fonctions » est de décrire l'architecture fonctionnelle sous forme d'un ensemble d'éléments structurés par des activités, des liens de données et des liens de contrôles en permettant la spécification des contraintes. Lors de la modélisation de l'architecture fonctionnelle, la principale difficulté réside dans la manière de décomposer les fonctions principales en sous-fonctions jusqu'à obtenir des *fonctions élémentaires indivisibles* encore appelées *fonctions atomiques*. Ces fonctions peuvent être représentées par un quintuplé :

<Données consommées, Données produites, Données de contrôle, Traitement, Contraintes>

La décomposition en fonctions implique cependant la notion d'interaction et de relations inter-fonctions qui peuvent relever de l'*indépendance* ou de la *coopération* [Banâtre, 1991] ; la coopération se manifeste sous deux formes : la coopération par partage d'informations et la coopération par échange d'informations.

Discussion : Ces notions d'interaction et de relation inter-fonctions corroborent l'existence de fonctions secondaires purement techniques mais nécessaires à la réalisation de la mission principale du système qui malheureusement font rarement l'objet de spécifications approfondies telles que : durée d'exécution maximale d'une activité, délai de prise en compte d'une requête ou délai de réception d'un acquittement (liens de contrôle), viabilité d'une donnée (liens de données). L'architecture fonctionnelle réduite aux seuls modes de fonctionnement de la mission principale est alors selon moi incomplète car la dynamique fonctionnelle du système est peu, voire pas étudiée. L'étude de sûreté ne fait alors que révéler des banalités et ne soulève pas les problèmes réels au sens de [Ligeron, 2003].

b) Architecture fonctionnelle des fonctions secondaires du système

Comme vu précédemment, l'architecture fonctionnelle se limite dans la plupart des cas, à la modélisation de la mission principale du système. Or, pour que les services décrits dans la mission principale du système soient effectivement rendus, ces services doivent s'appuyer sur des fonctions secondaires qui sont certes purement techniques mais dont dépend la bonne réalisation de la mission principale du système. La fonction « Communication » au sein du système d'automatisation est un bon exemple de fonction technique au même titre que les fonctions gérant le passage entre les différents modes d'utilisation du système.

J'introduis ici une nuance entre les *modes de fonctionnement* (nominaux, dégradés) de la mission principale du système et les *modes d'utilisation* (automatique ou manuel). A titre d'exemple, la fonction « Conduire » peut être réalisée en modes de fonctionnement nominal ou dégradé qui peuvent eux-mêmes se décliner en modes d'utilisation automatique ou manuel ; le passage en « utilisation manuelle » peut être imposé lorsque la macro-fonction « utilisation automatique » se trouve dans un mode dégradé. De même, si la macro-fonction « utilisation manuelle » se trouve dans un mode dégradé, le système peut être amené à basculer en position de repli ; ce basculement peut être géré soit par une fonction technique du système soit par une intervention humaine.

Discussion : La modélisation fonctionnelle doit être approfondie en intégrant la dynamique fonctionnelle et en s'intéressant de près aux transitions entre les différents modes d'utilisations : l'étude de sûreté ne se restreint plus au régime permanent (mission principale) mais prend également en compte le régime transitoire (changement de mode d'utilisation ou de fonctionnement) et s'attache essentiellement aux conséquences de la non-fiabilité et/ou non-disponibilité d'une fonction secondaire pour la mission principale du système. Il convient ainsi de définir précisément ces fonctions en termes d'objectifs quantifiés de performances et de sûreté lors de la conception.

2.5.3.4 Modélisation de l'architecture matérielle

L'architecture matérielle, support d'exécution, se définit comme l'ensemble des ressources matérielles et des exécutifs permettant la réalisation d'une application [Bouras, 1997]. Une telle architecture est spécifiée par [Conrard, 1999] comme étant :

- la liste des équipements interconnectés via un système de communication, l'agencement des équipements les uns par rapport aux autres définit ainsi l'organisation de cette architecture,
- les caractéristiques de chaque équipement qui définissent l'ensemble des comportements et des possibilités d'actions de ces équipements.

L'architecture matérielle passe par une activité de choix et de dimensionnement des différents constituants, de placement, de structuration des *fonctions élémentaires ou atomiques* de l'architecture fonctionnelle. Chacune de ces activités doit fournir un embryon de solution partiellement validée par rapport à certaines propriétés. Une validation globale est ensuite nécessaire pour vérifier que l'architecture matérielle envisagée peut supporter l'architecture fonctionnelle préalablement définie. Ces vérifications nécessitent alors la connaissance des performances et, plus largement, des caractéristiques du matériel support d'exécution. Le tableau 2.7 donne à titre d'exemple les principales caractéristiques pour certains constituants d'un système d'automatisation d'après [MESR, 1994]. La notion de profils est intéressante pour favoriser l'intégration et atteindre les objectifs d'interopérabilité, d'interfonctionnement, d'interchangeabilité et de conformité. Un profil est un ensemble bien identifié de services au niveau du système de communication en terme de besoins et contraintes mais aussi au niveau des besoins fonctionnels pour le processus d'application considéré. On voit ainsi apparaître des profils de communication dédiés métiers : dans le manufacturier, le continu, le domaine machine, etc... En outre, des modèles d'équipements intelligents tels que capteurs/actionneurs intelligents dont la principale particularité est de présenter une capacité à communiquer, à décider et à agir (grâce principalement à une unité de traitement interne et un interface de communication) ont été proposés par [Gehin, 1994] [Staroswiecki & al., 1994], [Robert & al., 1993]. Ces modèles d'équipements accompagnés de la notion de profils facilitent ainsi la modélisation de l'architecture matérielle.

Caractéristiques	Description
Générales	Aspect Conditions d'utilisation Consommation Constructeur Coût d'achat Coût de formation sur le produit Encombrement Fonctions de sûreté intégrées Interfaces Homme-Machine pour la programmation, la configuration, l'exploitation, la maintenance Poids Type d'énergie
De communication	Classes de conformité Nombre de connexions disponibles / maximales Gestion de l'accès au support Coût connexion supplémentaire Charge maximale du système de communication Indications temporelles : temps de réponse à une sollicitation, temps moyen d'exécution du protocole Profils de communication
De l'unité de traitement	Nombre de processeurs Nombre de coprocesseurs Taille mémoire programme par défaut / maximale Taille mémoire données par défaut / maximale Temps de cycle Charge maximale de l'unité de traitement

	Coût mémoire supplémentaire Granularité de l'horloge interne – externe Interruptions disponibles Nombre d'entrées-sorties disponibles / maximal
Des exécutifs	Gestion des programmes : chargement, téléchargement, nombre maximum Gestion des tâches : dynamiques, statiques, priorités, échéances, nombre maximal Gestion de la mémoire Gestion des fichiers Gestion des entrées-sorties Gestion de la synchronisation – communication Gestion du temps Ordonnancement Gestion des exceptions Initialisation Configuration Temps moyen de commutation Temps de prise en compte des interruptions Granularité de l'horloge Coût de l'exécutif
D'intégration	Interopérabilité Interfonctionnement Interchangeabilité Conformité Profils

Tableau 2.7 : Exemple de caractéristiques des constituants d'un système d'automatisation

2.5.3.5 Proposition d'une méthodologie de Codesign pour la conception de systèmes d'automatisation sûrs de fonctionnement

J'ai présenté dans les paragraphes 2.5.3.1 à 2.5.3.4 les difficultés rencontrées lors de la conception de systèmes d'automatisation sûrs de fonctionnement ainsi que la problématique d'expression des contraintes d'une architecture opérationnelle, de modélisation des architectures fonctionnelles et matérielles. Fort de cette réflexion, la méthodologie de Codesign proposée structure l'activité de conception d'un système d'automatisation sûr de fonctionnement autour de six étapes décrites par la figure 2.18 :

- Activité A1 : Modélisation fonctionnelle conduisant à une architecture fonctionnelle,
- Activité A2 : Partitionnement en fonctions élémentaires,
- Activité A3 : Choix du matériel conduisant à une architecture matérielle,
- Activité A4 :Projection, allocation et agrégation conduisant à une proposition d'architecture opérationnelle avec éventuelle remise en cause des choix pris à l'activité A2,
- Activité A5 : Validation et/ou remise en cause de l'architecture matérielle compte tenu des résultats obtenus à l'issue de l'activité A3,
- Activité A6 : Validation globale conduisant à une architecture opérationnelle validée avec parfois une boucle de rétroaction si les objectifs de sûreté ne sont pas satisfaits.

Le concept de Codesign, appliqué à une architecture opérationnelle, se justifie dans la mesure où il faut, d'une part, décomposer l'architecture fonctionnelle en fonctions élémentaires et, d'autre part, choisir le matériel, en affinant progressivement les choix adoptés pour atteindre les objectifs de sûreté de fonctionnement et satisfaire les contraintes du système d'automatisation étudié.

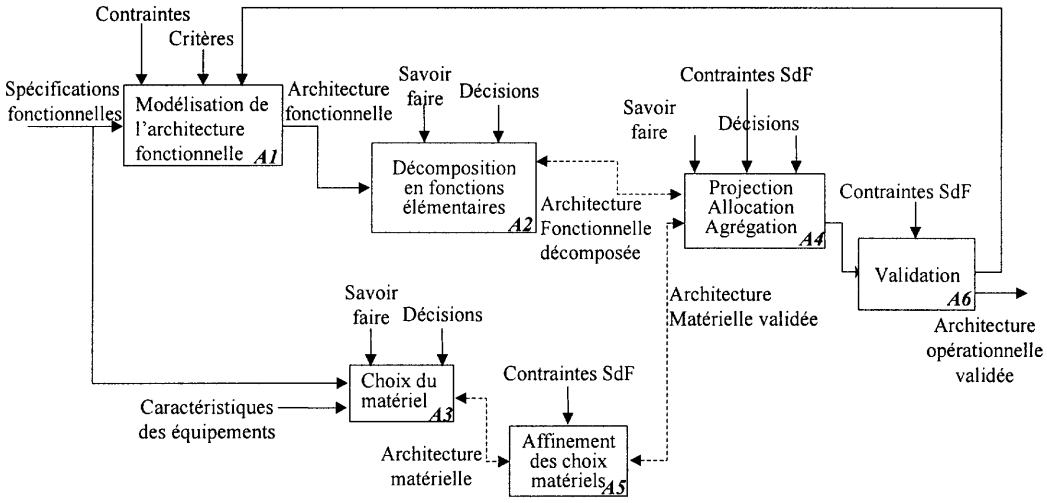

Figure 2.18 : Proposition d'une méthodologie de Codesign pour la conception de systèmes d'automatisation sûrs de fonctionnement

Cette démarche résumant les activités de conception d'un système d'automatisation sûr de fonctionnement a été discutée, finalisée et validée dans le cadre de mes activités de recherche au sein de l'Action Spécifique du CNRS « Méthodes et modèles pour l'analyse de la sûreté de fonctionnement des systèmes distribués » rattachée au RTP55 SyCoRéso en collaboration avec des laboratoires de recherche et industriels CRAN (Nancy), LAGIS (Lille), LCIS(Valence), LISTIC(Annecy), INERIS(Verneuil en Halatte) , INRS (Nancy), INRETS (Villeneuve d'Ascq), CEA (Saclay), Crouzet (Valence) ainsi qu'au sein du cercle thématique CIAME du groupe automatique 18.3 de la SEE. A noter qu'une demande de rattachement au GDR MACS a été faite en juin 2005.

Bilan de l'action II.3 : Ces travaux ont fait l'objet d'un DEA [Beugin, 2002], de 2 congrès francophones (Pentom03, Pentom05) [Beugin & al., 2003] [Renaux & al., 2005] , de 3 congrès internationaux (IEEE/IMTC, Esrel03, Esrel05) [Cauffriez & al., 2003b] [Renaux & al., 2003] [Beugin & al., 2005] et d'une revue internationale Reliability Engineering and System Safety [Cauffriez & al., 2004] ; les perspectives de ces travaux sont présentées dans le chapitre 3 de ce mémoire.

2.5.4 Action II.4 : Proposition d'une méthode fonctionnelle dynamique pour la description et l'évaluation de la sûreté de fonctionnement de systèmes complexes automatisés

2.5.4.1 Limites des méthodes classiques de sûreté de fonctionnement

Les limites des méthodes classiques de la sûreté de fonctionnement ont été discutées lors de la séance plénière du Congrès Pentom'2003 et j'avoue rejoindre totalement le point de vue évoqué par [Ligeron, 2003] que je résume ci-après. Ce dernier souligne en effet que, dans la plupart des cas, les accidents qui surviennent en exploitation n'ont pas été envisagés lors des études de sûreté menées en phase de conception. La combinaison des événements qui a mené au crash du Concorde était difficilement prévisible. Ces accidents correspondent en fait à une zone de probabilité difficilement atteignable surtout lorsque les études sont faites à partir des méthodes classiques telles que : Arbre de fautes, Graphe de Markov, ou AMDEC, etc…

Les études sont généralement faites pour la mission principale du système c'est-à-dire pour un

fonctionnement en régime permanent. Les missions secondaires et les fonctions techniques, telles que je les ai appelées, font rarement l'objet d'une étude approfondie car le cahier des charges fonctionnelles se restreint bien souvent aux fonctions contribuant à la mission principale.

L'approche systémique qui vise à décomposer le système en sous-systèmes est rarement utilisée bien qu'elle met davantage en exergue les échanges de flux Matière, d'Energie, d'Information, et Psychologiques (cf. chapitre 1, §1.3.2.3). Les méthodes et outils classiques tels que APTE, Petri, SADT, Merise communiquent peu entre-eux et appartiennent à des champs disciplinaires différents : mécanique, automatique, informatique.

La dynamique fonctionnelle du système est rarement étudiée. Les taux de défaillances sont dans la plupart des cas supposés constants alors qu'il n'en est rien dans la réalité : une rapide démonstration met en évidence que le taux de défaillances pour un système constitué de deux composants en parallèle n'est pas constant [Cocozza-Thivent, 1997] ; de même le vieillissement des composants font que le taux de défaillances a tendance à croître et n'est plus constant. Ceci laisse imaginer l'erreur commise par des méthodes telles que graphes de Markov sur un système complexe constitué d'une multitude de fonctions et composants associés selon diverses structures : série, parallèle, en ponts... Fort de ce constat, il apparaît que « *les études de sûreté de fonctionnement sont pauvres et ne soulèvent pas les problèmes réels* » [Ligeron, 2003].

L'émergence de la notion de *sûreté de fonctionnement dynamique* [Becker & al., 2001] [Labeau, 2001] [Woltereck, 2001] reposant sur des méthodes telles que simulation de Monte Carlo, Réseaux Bayésiens, tente de pallier ce vide et ouvre de nouvelles perspectives de recherche. Par ailleurs, il est un fait que le concepteur manque de méthodes et d'outils permettant de spécifier les objectifs de sûreté de fonctionnement et de comparer des alternatives de conception face à une complexité accrue.

Dans ce contexte, les travaux de thèse de V. Benard ont porté sur l'évaluation en phase de conception de la sûreté de fonctionnement de systèmes complexes automatisés en prenant en compte à la fois les aspects qualitatifs (modélisation, caractérisation, identification et représentation des dépendances au sein de l'architecture opérationnelle), quantitatifs (quantification des paramètres de sûreté à des fins de validation de l'architecture opérationnelle) et dynamiques. L'originalité repose sur la volonté de prendre en compte dès la phase de conception les aspects sûreté de fonctionnement. Cette thèse a été soutenue en décembre 2004 et a abouti à la proposition d'une méthode fonctionnelle dynamique baptisée SAFE-SADT présentée dans les paragraphes suivants.

2.5.4.2 Formalisme de la méthode SAFE-SADT

La méthode SAFE-SADT qui utilise le formalisme SADT [IGL, 1989] tente de répondre à la problématique suivante : que résulte t-il de la projection/allocation d'une architecture logicielle sur une architecture matérielle en terme de sûreté ?

Un premier élément de réponse consiste à considérer qu'une fonction réalisée par du logiciel implanté sur du matériel se ramène à une structure série : si le matériel ou le logiciel est défaillant, la fonction est alors défaillante.

Le formalisme retenu pour la méthode SAFE-SADT est celui de la figure 2.19, on trouve :

- en entrée du SAFE-bloc Ai, les fonctions à réaliser « Nom, Code logiciel, Var produites, Var consommées » avec les objectifs de sûreté à atteindre : vecteur paramètres FMDS ; ce vecteur FMDS peut être selon les cas d'étude restreint à certains paramètres (FMD par exemple si le paramètre sécurité ne fait l'objet d'aucune étude). La fonction exécutée est disponible si les variables d'entrées sont disponibles et viables (notion de rafraîchissement relative à la fonction technique « Communication »),
- à la base du SAFE-bloc Ai, le(s) support(s) d'exécution matériel avec leurs caractéristiques de sûreté (vecteur FMDS) obtenues par retour d'expérience, tests en laboratoire ou à partir de données fournisseurs. Le formalisme utilisé permet de modéliser la redondance du support d'exécution afin d'étudier l'impact de cette redondance sur les paramètres FMDS

de la fonction étudiée en prenant en compte certaines contraintes telles que financières par exemple,

- au sommet du SAFE-bloc Ai, les données de contrôle telles que les événements contrôlables, les événements incontrôlables ainsi que l'expression de contraintes et critères (objectifs de coûts, objectifs de temps de réponse, ...). La notion d'événement incontrôlable fait référence aux travaux de [Niel, 1998] où pour un événement incontrôlable ayant affecté le système, il existe un événement contrôlable le ramenant dans un état fiable, disponible ou sécuritaire (action de maintenance corrective par exemple),
- à la sortie du SAFE-bloc Ai, le résultat obtenu pour la projection/allocation envisagée. On retrouve naturellement en premier lieu le vecteur FMDS mais aussi d'autres paramètres permettant de caractériser les versions des macro-fonctions réalisées : fonction nominale, fonction dégradée, le temps de réponse obtenu pour les versions nominales et dégradées ainsi que les coûts (ces deux derniers paramètres dépendant des choix technologiques effectués). Ce formalisme permet aussi d'identifier les événements qui demeurent incontrôlés après la projection/allocation et dont la propagation pourrait être à l'origine d'une entrave à la sûreté de fonctionnement pour d'autres fonctions utilisatrices ; il conviendra naturellement de confiner les événements incontrôlés d'un niveau au niveau immédiatement supérieur du modèle SAFE-SADT,
- l'opérateur « projection » représenté par le symbole « $\perp$ » qui permet de spécifier de manière explicite la projection d'éléments logiciels sur du matériel pour l'accomplissement d'une fonction. Les différents chemins de succès matérielo-fonctionnels pour les macro-fonctions du système sont clairement mis en exergue par ce formalisme avec le chemin de succès conduisant à la version nominale $(F_1 \perp M_1) \bullet ... (F_2 \perp M_2) ... \bullet (F_n \perp M_n)$ ou aux versions dégradées $(F_1 \perp M_1) + ... (F_2 \perp M_2) ... + (F_n \perp M_n)$.

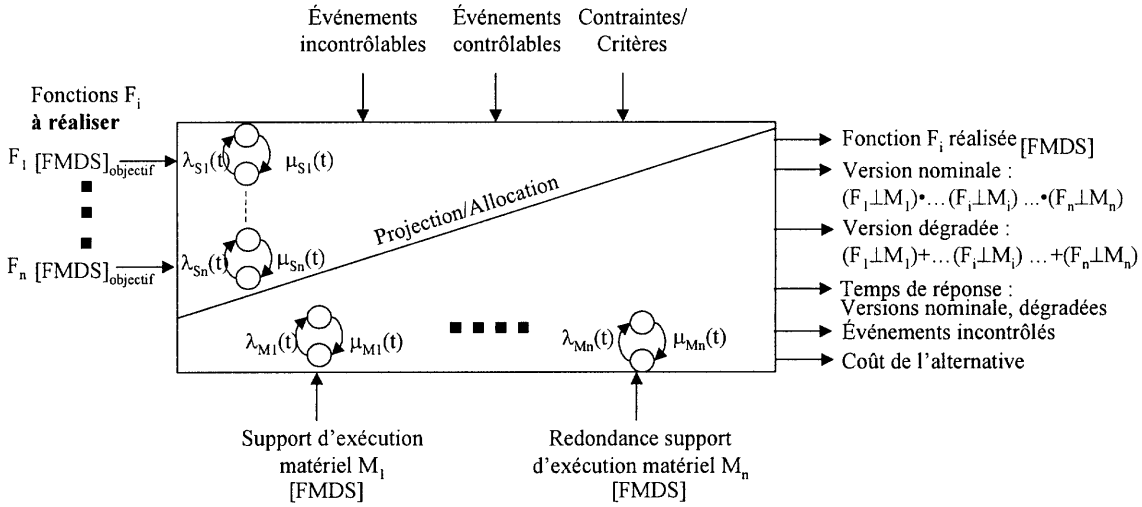

Figure 2.19 : Formalisme pour la méthode SAFE-SADT

Le SAFE-SADT se décompose selon une approche TOP-DOWN en bloc SAFE-SADT allant de la mission principale du système (niveau global A_0) jusqu'à atteindre les fonctions élémentaires de niveau A_n (cf. figure 2.20). Cette décomposition en niveaux permet de modéliser de manière explicite les caractéristiques de l'architecture opérationnelle et d'identifier les dépendances qui y règnent pour mieux appréhender les aspects sûreté de fonctionnement de l'architecture globale. L'approche BOTTOM-UP correspond à l'agrégation des « Fonctions élémentaires » obtenues, il appartient alors au concepteur de vérifier que les contraintes de spécifications logicielles, matérielles et de sûreté présentées sont satisfaites. Lors de cette démarche d'agrégation, il est possible de quantifier les temps de réponse ou, à défaut, de les borner (cf. figure 2.20) et d'estimer le coût d'une fonction agrégée si la réalisation de certaines fonctions élémentaires nécessite l'utilisation de composants de sécurité.

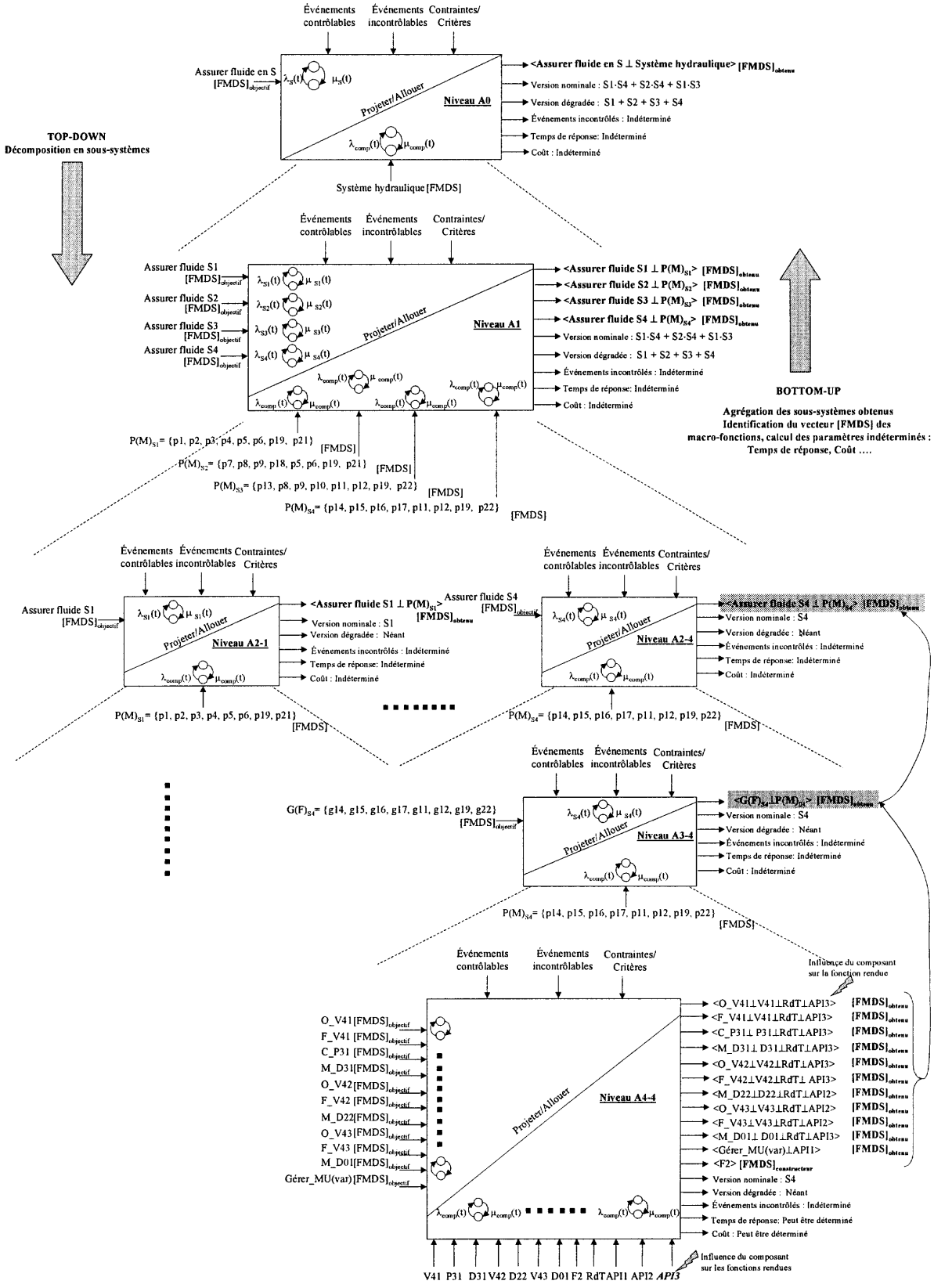

Figure 2.20 : Exemple de SAFE-SADT pour un système hydraulique

La décomposition en niveaux doit permettre d'étudier l'impact en terme de sûreté de l'affectation d'une ou plusieurs fonctions ou sous-fonctions à du matériel donné :

- identification de toutes les fonctions faisant l'objet d'une défaillance de mode commun en cas de dysfonctionnement du matériel support d'exécution,
- nécessité de redonder le matériel support d'exécution,
- devenir d'une fonction réalisée à partir d'un logiciel très fiable implémenté sur du matériel peu fiable,
- devenir d'une fonction implémentée sur du matériel très fiable mais dont le code logiciel est entaché d'erreurs.

La figure 2.21a décrit le SAFE-SADT d'une architecture fonctionnelle comprenant deux fonctions F1 et F1' en redondance active pour des raisons de haute disponibilité. La figure 2.21a met en évidence une défaillance de mode commun si F1 et F1' sont implémentées sur un même matériel M1. Le concepteur s'affranchit de ce mode commun de défaillances avec la solution préconisée par le SAFE-SADT de la figure 2.21b et augmente ainsi la disponibilité du service rendu par ces 2 fonctions ; toutefois on peut supposer pour cette deuxième solution que le coût C2 est supérieur au coût C1 par l'adjonction d'un matériel supplémentaire M2. La méthode SAFE-SADT permet ainsi d'étudier des alternatives de solution lors de la conception d'architecture opérationnelle de systèmes automatisés complexes en exprimant clairement les choix techniques, les choix de répartition/allocation des fonctions, et met en exergue les coûts induits par chaque alternative de solution.

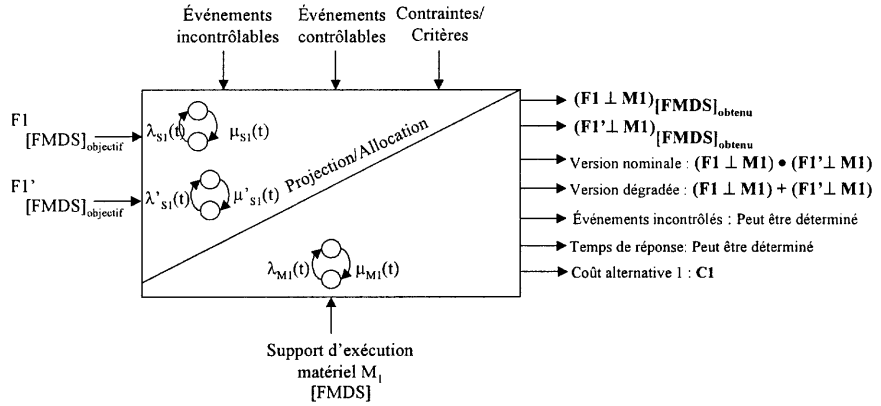

Figure 2.21a : Étude d'alternative de solution – Défaillance de mode commun avec 1 support d'exécution matériel M1

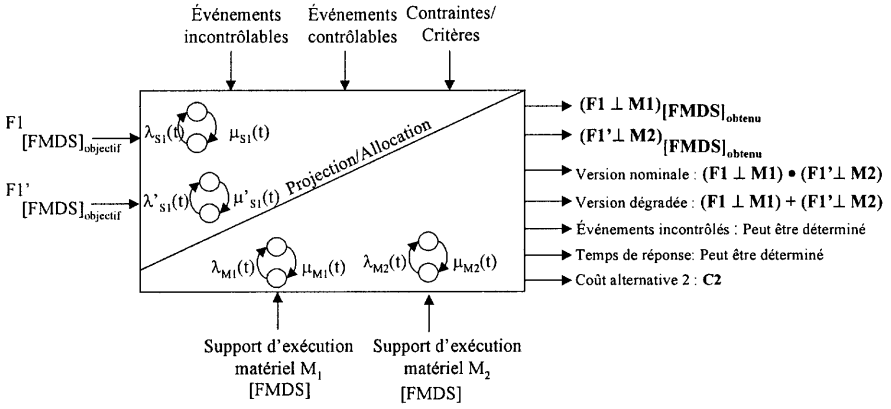

Figure 2.21b : Étude d'alternative de solution – Suppression de la défaillance de mode commun mais coût matériel C2>C1

2.5.4.3 Etude des propriétés de la méthode SAFE-SADT

a) Bijectivité

Soient F l'ensemble des fonctions élémentaires $F=\{f_1, f_2,...f_n\}$, M l'ensemble des matériels nécessaires à la réalisation de l'architecture opérationnelle $M=\{M_1, M_2,...M_j\}$ et $G(F) = \{g_1, g_2, ...g_l\}$ l'ensemble des parties de F projeté sur l'ensemble P(M) des parties de M avec $P(M) = \{p_1, p_2,...p_k\}$. *Si une approche fonctionnellement redondante n'entraîne pas l'implémentation d'une même fonction élémentaire (même nom, même code) sur du matériel distinct, on a alors :*

- $g_i \in G(F)$ et $g_i \neq 0$ pour $i \in [1..l]$ caractérise l'existence d'au moins une partition de F,
- $\forall\ i \neq j$, $g_i \cap g_j = \varnothing$, cette condition exprime l'absence d'implémentation d'une même fonction élémentaire (même nom, même code) sur du matériel distinct,
- $\bigcup_{i=1}^{l} g_i = F$ définit l'ensemble de l'architecture fonctionnelle,
- $p_i \in P(M)$ et $p_i \neq 0$ pour $i \in [1..k]$ caractérise au moins une partition de M,
- $\forall\ i \neq j$, $p_i \cap p_j \neq \varnothing$ met en évidence une dépendance liée au matériel alors que $p_i \cap p_j = \varnothing$ démontre une indépendance matérielle,
- $\bigcup_{i=1}^{k} p_i = M$ définit l'ensemble de l'architecture matérielle,
- $\forall\ g_i \in G(F)$ et $p_j \in P(M)$, $(g_i \perp p_j)$ a une et une seule image,
- $\forall\ p_j \in P(M)$ et $g_i \in G(F)$, $(p_j \perp^{-1} g_i)$ a un et un seul antécédent.

Les deux dernières conditions mettent en évidence une propriété de bijectivité de l'opérateur projection « $\perp$ » si et seulement si $\forall\ i \neq j$, $g_i \cap g_j = \varnothing$.

b) Charge de communication inter-matériel post projection

Soient g_i et $g_j \in G(F)$. On désigne par $VP(g_i)$ et $VP(g_j)$ les ensembles de données produites par g_i et g_j et par $VC(g_i)$ et $VC(g_j)$ les ensembles de données consommées par g_i et g_j. On a alors que $\phi\ (g_i, g_j) = VP(g_i) \cap VC(g_j)$ représente les données produites par les fonctions élémentaires de gi et consommées par les fonctions élémentaires de g_j.

La totalité des données échangées entre g_i et g_j est $T(g_i, g_j) = \phi(g_i, g_j) \cup \phi(g_j, g_i)$. La charge de communication entre les fonctions élémentaires est égale à $K(g_i, g_j) = \rho(T(g_i,g_j))$ avec ρ dépendant du type de données échangées, de la fréquence des échanges, du délai de transport et de synchronisation des données par la fonction technique « Communication ».

La charge globale de communication pour l'architecture opérationnelle obtenue est ainsi égale à $\sum_{i\neq j}^{l}\sum_{j=1}^{l} K(g_i,g_j)$ [Akaïchi, 1996], cette charge globale ne doit pas dépasser la capacité maximale de la fonction technique « Communication » (Cf. Action II.2).

c) Charge intra-matériel

La charge d'un matériel M_j est fonction du nombre de fonctions élémentaires projetées sur celui-ci ($g_i \perp M_j$), de la quantité de données manipulées par ces fonctions, de la somme des codes logiciels $\sigma(fi)$ de chaque fonction élémentaire.

$$\text{Charge obtenue} = \text{Car}(g_i)+\text{Car}\left\{VP(M_i)\cup VC(M_i)\right\}+\sum\sigma(f_i)$$

où Car désigne le cardinal des ensembles. Il va de soi que la charge obtenue ne doit pas dépasser la capacité maximale du matériel considéré.

d) Aspects quantitatifs de la méthode SAFE-SADT

J'ai orienté les travaux de thèse de Vincent Benard sur le concept de SAFE-SADT pour offrir au concepteur la possibilité de modéliser, caractériser, identifier et représenter les dépendances au sein de l'architecture opérationnelle d'un système d'automatisation. J'aborde ici les aspects de la quantification des paramètres de sûreté à des fins de validation de l'architecture opérationnelle en prenant en compte les aspects dynamiques grâce à une approche basée sur les simulations de Monte-carlo.

Pour ce faire, une hypothèse forte a été introduite dans la thèse à savoir que toute entité logicielle ou matérielle ne peut prendre au plus que deux états : soit un état de fonctionnement soit un état de défaillance ; ce qui explique le graphe à 2 états représentés sur le formalisme SAFE-SADT dont les arcs portent le taux de défaillances $\lambda(t)$ et réparations $\mu(t)$.

Dans ce contexte, Vincent Benard a exploré dans un premier temps la théorie du renouvellement. La théorie du renouvellement a pour origine l'étude des « ensembles renouvelés » ; le renouvellement caractérise le remplacement d'un composant défaillant par un autre [Cox, 1966] [Bon, 1995] [Lyonnet, 2000]. Par extension, le renouvellement peut modéliser l'alternance état de fonctionnement/état défaillant d'une entité : après occurrence d'une défaillance, l'entité est renouvelée (par extension réparée) et se trouve alors en état d'assurer sa mission. La littérature fait apparaître quatre principaux processus de renouvellement qui peuvent être modélisés par des fonctions de transfert : processus de renouvellement simple, modifié, alterné simple, alterné modifié [Cox, 1966]. L'extension de cette démarche à un système, grâce aux propriétés des transformées de Laplace présentées dans [Hanus & al., 1996], a conduit aux fonctions de transfert caractérisant l'évolution des paramètres fiabilité et disponibilité pour des systèmes série et parallèle constitués d'entités non réparables.

Cette première piste a montré ses limites lorsqu'on a souhaité étendre la démarche à un système composé d'entités réparables, notamment pour des structures parallèles : une entité défaillante peut en effet être réparée avant qu'une entité en redondance active ne défaille à son tour. Dans ce cas, le système formé par ces deux entités remplit sa mission et apparaît comme fiable et disponible en dépit de la défaillance séquentielle de ses entités. Cette limite est corroborée par les travaux de [Coccoza-Thivent, 1997] qui montrent que la superposition de deux processus de renouvellement ne donne pas forcément un processus de renouvellement.

Fort de ce constat, nous avons abandonné cette première approche et nous nous sommes orientés vers une approche par simulations de Monte Carlo, outil fortement utilisé dans le domaine du nucléaire et très prometteur pour mener à bien une analyse de la fiabilité et de la disponibilité de systèmes complexes. Cet outil repose sur une modélisation mathématique du comportement du système grâce à une équation générale d'état. Le principe de base repose sur [Dubi, 2000] [Labeau, 2000] :

- une **simulation dans l'espace temporel** avec un noyau T de « vol libre » (Free Flight Kernel) qui définit la densité de probabilité qu'un système entré dans un état B' à un instant t' fera l'objet d'un prochain événement de changement d'état à l'instant t. Ce noyau définit en réalité le transfert du système dans l'espace temporel jusqu'au changement d'état soit l'instant t. Dans le domaine du nucléaire, le noyau neutronique définit le transfert de la particule dans le repère de coordonnées spatiales avec un angle et une énergie inchangés.
- une **simulation dans l'espace d'état** avec un noyau C de collision (Collision Kernel) qui se définit comme la probabilité de transfert dans un nouvel état B à partir de l'état précédent B' dans lequel le système était rentré à l'instant t'.

Le noyau de transport K du système dans les espaces temporels et spatiaux se définit alors par le produit des noyaux T et C (équation 2.3)

$$K(B',t'\rightarrow B,t)=T(B',t'\rightarrow t)\cdot C(t,B'\rightarrow B) \qquad (2.3)$$

Une forme simplifiée de l'équation générale de transport du système est donnée par [Dubi, 2000] et traduit la séquence d'événements suivants : le système entre dans l'état j à l'instant t' et y reste jusque l'instant t où il bascule dans l'état i (équation 2.4) ; cette équation correspond ainsi à la densité d'entrée dans un état i à l'instant t.

$$\Psi_i(t)=P_{i0}\delta(t)+\sum_{j=1 et j\neq i}^{n}\int_0^t \Psi_j(t')\cdot T(j,t'\rightarrow t)\cdot C(t,j\rightarrow i)\cdot dt' \qquad (2.4)$$

avec

- P_{i0} est la probabilité que le système soit dans l'état i au temps t=0,
- $T(B',t'\rightarrow t)=T(j;t'\rightarrow t)=f_j(t',t)=R_j(t',t)\cdot z_j(t',t)$ avec $R_j(t',t)$ la probabilité que le système entré dans l'état j à t' reste dans cet état jusque t et $z_j(t',t)$ la fonction de hasard pour cet état,
- $C(t,B'\rightarrow B)=C(t,j\rightarrow i)=\frac{z_{j,i}(t',t)}{z_j(t',t)}$ avec $z_{j,i}(t',t)$ la fonction de hasard partielle du transfert de l'état j dans l'état i.

Cette équation générale est extrêmement compliquée et donne une solution analytique exacte pour quelques cas simples. Une approche par simulation a été de ce fait privilégiée. Dans le cadre de la thèse de Vincent Benard, la simulation de Monte Carlo a été mise en œuvre pour des lois de distribution exponentielle. L'échantillonnage du noyau T donne le prochain instant de changement d'état du système et l'échantillonnage du noyau de collision C permet d'identifier le composant qui fait l'objet du changement d'état.

Une « *histoire* » correspond ainsi à un transport du système dans les espaces temporels et d'état sur un horizon de mission Tm préalablement défini. Dans [Pasquet, 1999], sont données les relations caractérisant les paramètres de fiabilité, maintenabilité, disponibilité en fonction des compteurs qui sont associées à ces paramètres pour un nombre d'histoires simulées. La qualité d'une simulation de Monte Carlo est caractérisée par un certain nombre d'indicateurs tels que le PRSD (Percentage Relative Standard Deviation).

Cette approche par simulation de Monte Carlo a mis en évidence l'existence de 3 grandeurs permettant de faire une analyse de sensibilité et d'améliorer par conséquent toute architecture opérationnelle lors de sa conception :

- Sensibilité au niveau des taux de défaillances/réparations des entités : la simulation de Monte Carlo permet d'obtenir le nombre moyen de défaillances de chaque entité matérielle et logicielle présente dans le système. Il est évident que le choix des entités logicielles et matérielles du système revêt une importance considérable. Le fait de substituer à ces entités d'autres entités plus fiables conduit inévitablement à améliorer le comportement du système. Si cette approche ne peut être envisagée, il faut s'orienter vers l'identification de stratégie de maintenance préventive afin d'éviter une stratégie de maintenance curative pour garantir les objectifs de sûreté du système global (notion d'événements contrôlables).
- Sensibilité au niveau de la topologie du système : une étude du facteur d'importance topologique lors de simulation de Monte Carlo permet d'identifier les faiblesses structurelles du système lors de la conception. En effet, cette analyse de sensibilité permet de localiser les éléments dans la structure du système dont la défaillance a un impact non négligeable sur l'évaluation des paramètres de sûreté estimés. Le facteur d'importance topologique est obtenu indépendamment des lois de défaillance de chaque entité et de toute notion de temps. Une nouvelle simulation de Monte Carlo après modification de la structure du système par ajout ou suppression de chemins de succès

conduit à identifier l'impact de cette modification sur le système qui peut se traduire par une augmentation ou une diminution des paramètres fiabilité et disponibilité du système. Le concepteur d'une architecture opérationnelle peut par une telle démarche identifier le gain/coût et juger de la nécessité d'investir dans des entités redondantes ou de sécurité (automate de sécurité par exemple) pour atteindre les objectifs [FMDS] fixés.

- Sensibilité au niveau du compromis « défaillances/réparations des entités » en fonction « de leur place dans la topologie du système » : Une analyse de sensibilité à ce niveau permet d'identifier la responsabilité de chaque entité et d'étudier la criticité des défaillances vis à vis du fonctionnement global du système : il se peut en effet que certaines entités fassent l'objet de nombreuses défaillances sans impact sur les performances globales du système mais que d'autres présentent un nombre réduit de défaillances lourdes de conséquences pour le système. En modifiant les grandeurs caractérisant les taux de défaillances d'une entité, il est ainsi possible de mieux cerner les répercussions engendrées sur le fonctionnement global du système et percevoir les points faibles de l'architecture opérationnelle lors de sa phase de validation.

Un certain nombre de points reste à approfondir sur cette approche par simulation de Monte Carlo pour l'évaluation de la sûreté de systèmes complexes automatisés. Une mise en œuvre complète de la méthode SAFE-SADT sur un système hydraulique complexe, à la fois sur les aspects qualitatifs et quantitatifs, a été présentée dans le mémoire de thèse de Vincent Benard.

Bilan de l'action II.4 :

Les travaux relatifs à cette action de recherche ont été menés dans le cadre de la thèse de Vincent Benard dont j'ai effectué l'encadrement à 90%. Ces travaux ont abouti à la proposition de la méthode fonctionnelle dynamique SAFE-SADT pour la description et l'évaluation de la sûreté de fonctionnement de systèmes complexes automatisés

Ces travaux ont fait l'objet d'un DEA [Benard, 2000], d'une thèse soutenue [Benard, 2004], de 3 congrès internationaux (IFAC/INCOM, CIFA, EUROSIM) [Benard & al. 2001] [Benard & al. 2002] [Benard & al., 2004], d'un congrès francophone (Pentom'03) [Benard & al., 2003] et 2 rapports CNRS [Benard & al., 2001b] [Benard & al., 2002b]. Une revue internationale est acceptée [Cauffriez & al., 2005b] et une autre est actuellement en cours de reviewing [Benard & al., 2005]. Les perspectives de ces travaux sont présentées dans le chapitre 3 de ce mémoire.

2.6 Bilan quantitatif des publications

Le tableau 2.8 présente un récapitulatif des publications pour l'ensemble des actions menées et donne le nombre de publications par catégorie en précisant mon rang d'auteur.

Catégorie de publications	**1er auteur**	2ème auteur	3ème auteur et +
Revues	**6**	1	
Ouvrages collectifs	**1**		
Chapitre d'ouvrages	**2**		
Congrès internationaux	**7**	9	3
Colloques francophones		1	2
Communication invitée	**1**		
Rapports de contrat	**3**	3	1
Total	***20***	*14*	*6*

Tableau 2.8 : Bilan quantitatif des publications par catégorie

Conclusion

J'ai détaillé, dans ce chapitre, l'axe I de mes travaux de recherche qui portent sur l'amélioration de la performance de lignes de productions. Une méthode de diagnostic a été proposée pour améliorer les paramètres FMD (Fiabilité-Maintenabilité-Disponibilité) des lignes de production et en diagnostiquer les causes de non-performance. Cette méthode calcule le moyen équivalent à la ligne de production en utilisant une démarche de décomposition selon l'algorithme ADDX.

La maîtrise des flux a été le deuxième aspect étudié pour l'amélioration de la performance de lignes de production. Cette maîtrise des flux consiste en la détection, la localisation et l'identification des défaillances de rendez-vous entre plusieurs flux de production. Les aspects coûts, primordiaux dans le contexte industriel ont été abordés avec l'introduction de la notion de coûts propres et de coûts induits par les défaillances. L'axe I a mis en évidence la difficulté à caractériser et modéliser le comportement de système complexe. Les deux grandes approches d'étude des systèmes complexes, soit par agrégation d'entités pour converger vers le système global soit par décomposition du système global en éléments simples, ont été étudiées sur le cas particulier des lignes de production.

A partir de ces contributions sur l'évaluation des paramètres FMD de processus physiques, j'ai orienté ma recherche sur la sûreté du système d'automatisation en étudiant l'impact qu'il peut avoir sur le comportement du processus physique. En effet, une faible disponibilité du système d'automatisation peut conduire à une faible disponibilité du processus physique. Or, l'apport de nouvelles technologies avec l'apparition de capteurs, actionneurs intelligents, de réseaux de terrain offre de nouvelles possibilités pour la conception de système d'automatisation mais introduit également de nouvelles contraintes en terme de sûreté de fonctionnement. Cette autre thématique de recherche fait l'objet de l'axe II de ma recherche sur la conception de systèmes d'automatisation à intelligence distribuée encore appelée Network Controled System.

Ces travaux partent du constat de l'absence de langages, d'outils pour la modélisation d'architectures abstraites obtenues par composition d'entités logicielles et matérielles. La mission de ces systèmes automatisés repose sur un ensemble de systèmes interconnectés ou en interaction qui assurent une ou plusieurs fonctions spécifiques. La particularité de ces systèmes est de présenter une certaine complexité qui est différente selon qu'on s'attache aux aspects fonctionnels, structurels, comportementaux ou technologiques. Cette complexité rend nécessaire la décomposition de ces systèmes en sous-systèmes qui vont eux-mêmes se décomposer en sous-fonctions. La plupart des études de sûreté de fonctionnement actuellement menées sur des systèmes complexes s'attachent généralement à la mission principale du système définie dans le cahier des charges fonctionnel, les missions secondaires et les fonctions techniques font malheureusement rarement l'objet d'étude approfondie. Ma participation au projet européen UGTMS Urban Guided Transport Management System ($5^{ème}$ PCRD) me conforte dans cette opinion où seules les fonctions principales ont été spécifiées dans les Deliverable D1 « First Report for a preliminary definition of UGTMS » et D5 « Functional Requirement specification of ATP Core Functions » [UGTMS, 2002] [UGTMS, 2003]. La dynamique fonctionnelle du système est rarement évoquée lors de l'analyse fonctionnelle : l'interaction des fonctions ainsi que la nature de leurs relations (indépendance, coopération par partage d'informations ou par échange d'informations) sont peu ou pas analysées. L'hypothèse forte de taux constants de défaillances et réparations n'est jamais remise en cause alors que l'agencement en parallèle des composants et leur vieillissement mettent en défaut cette hypothèse. Cette faiblesse au niveau des études de sûreté de fonctionnement est due à un manque de méthodes et d'outils permettant de spécifier les objectifs de sûreté de fonctionnement et de comparer des alternatives de conception face à une complexité accrue.

Ma première contribution sur ce thème se focalise sur la proposition d'une méthodologie de Codesign pour la conception de systèmes d'automatisation sûrs de fonctionnement. L'aspect novateur repose sur la volonté ne pas se limiter à une simple analyse fonctionnelle ; l'idée de base consiste à atteindre une phase de conception avancée avec l'obtention d'une architecture opérationnelle validée.

Ma deuxième contribution sur cette problématique de conception de système d'automatisation sûr de fonctionnement réside en la proposition d'une méthodologie de Codesign pour la spécification des besoins et des contraintes d'architecture opérationnelle : contraintes dépendantes des spécifications fonctionnelles, contraintes dépendantes des spécifications matérielles, contraintes de sûreté qui dépendent à la fois de l'ingénierie « générale » du système, des spécifications matérielles et logicielles.

Le formalisme SAFE-SADT a été proposé comme support à l'implémentation de cette méthodologie de Codesign. Il vise à mettre en évidence les dépendances fonctionnelles et matérielles pour l'identification « des points durs » du système d'automatisation. Il repose sur une analyse systémique selon une approche TOP-DOWN pour la décomposition des fonctions principales du système en fonctions élémentaires et selon une approche BOTTOM-UP lors de l'agrégation de ces fonctions dans le but de réaliser la mission principale du système. Ce formalisme permet la modélisation, caractérisation, identification et représentation des dépendances au sein de l'architecture opérationnelle. La volonté d'identifier l'évolution des paramètres de sûreté du système d'automatisation tout au long de son cycle de vie nous a amené à proposer une méthode fonctionnelle dynamique reposant sur le formalisme SAFE-SADT, l'approche retenue pour la quantification des paramètres de sûreté est basée sur les simulations de Monte Carlo.

Les simulations de Monte Carlo font actuellement l'objet de recherches sur le thème de la « fiabilité dynamique » avec pour objectif de prendre en compte les variations des paramètres du système automatisé induites par la présence de défaillances (la défaillance d'un composant peut modifier la loi de défaillances d'autres composants, un autre exemple est la modification de débits au sein du système en présence de défaillances,...). Ces travaux sur la « fiabilité dynamique » vont pleinement dans le sens de nos préoccupations et font l'objet de perspectives de recherche présentées au chapitre 3 de ce mémoire.

Chapitre 3

Projets de recherche et de pédagogie

Introduction

Les projets de recherche et de pédagogie que je présente dans ce chapitre s'inscrivent dans la politique du laboratoire, de la Région Nord-Pas-de-Calais et de l'Europe.

Dans un premier temps, j'aborde mon projet recherche qui porte sur l'analyse systémique de la sûreté de fonctionnement des systèmes complexes. Pour ce faire, différentes approches de modélisation sont envisagées telles que : approches par simulation de Monte Carlo, par Réseaux Bayésiens, par méthode UML, par méthode B, approche basée sur la modélisation des connaissances normatives et d'experts.

Ces différentes perspectives alimentent mon projet de recherche pour les années à venir qui a pour ambition de proposer une méthodologie pour l'analyse systémique de la sûreté et se concrétiser par la spécification d'un outil d'aide à la conception et à l'étude d'alternatives de solutions. Cette méthodologie doit, selon moi, être suffisamment générique pour être appliquée dans différents domaines. En effet, le caractère générique de l'approche doit permettre de modéliser et d'analyser les problèmes et contraintes propres à chaque domaine.

Cette thématique de recherche correspond à un réel besoin de la société avec l'apparition de technologies innovantes aussi bien dans les systèmes de production (instrumentation intelligente, réseaux de terrain), dans l'automobile (In-Vehicle networks, Drive-by-wire system) ou dans les systèmes ferroviaires (mobilité intelligente).

Dans un deuxième temps, je présente les résultats attendus de mes recherches et les situe dans le contexte local, régional et européen.

J'aborde ensuite mon projet pédagogie et souligne l'aspect international avec la création de formations et filières internationales sur le principe LMD dans la thématique prioritaire de l'université, c'est à dire la sécurité des systèmes de Transports.

3.1 Projet de recherche : Analyse systémique de la sûreté de fonctionnement des systèmes complexes

Les systèmes complexes sont composés d'éléments actifs et/ou inactifs au sens de [Le Moigne, 1994] formant un ensemble fonctionnellement cohérent et assurant une fonction définie.

La conception de systèmes sûrs et leur exploitation posent le problème de leur modélisation pour laquelle les méthodes analytiques ne sont pas toujours applicables. En effet, la causalité est l'hypothèse fondamentale sous-jacente à l'analyse de sûreté et au diagnostic. Pour une analyse de sûreté, on propage les conséquences prévisibles d'une défaillance. Pour un diagnostic, on part de symptômes détectés par exemple par des procédures de surveillance et on remonte aux causes selon un point de vue soit structurel (localisation) soit fonctionnel.

Les modèles utilisés sont souvent des graphes causaux qui ne donnent qu'une vision uniquement déterministe et logique du système. Ils intègrent donc difficilement les éléments qui visent à limiter les effets d'une défaillance et assurent la robustesse du système. Ils ne tiennent pas compte de la performance du système de surveillance qui peut se mesurer en terme de fausses alarmes ou de non-détection. Ces modèles reposent sur une vision statique du diagnostic alors que des actions des opérateurs sont souvent indispensables et doivent être pris en compte.

Les objectifs de recherche que je me fixe pour les années à venir s'inscrivent dans la continuité des travaux présentés au chapitre 2 et visent à enrichir et conforter la proposition de méthodes pour la description, la modélisation systémique et l'évaluation de la sûreté de fonctionnement de systèmes complexes. Cette complexité rend nécessaire la modélisation des grands systèmes pour les concevoir, les réaliser et les exploiter tant en modes de fonctionnement normaux, qu'en présence de défaillances ou de perturbations, dans le respect des critères de la sûreté de fonctionnement humaine, technique et environnementale.

J'ai montré au chapitre précédent que ces systèmes complexes se définissent, par un ensemble en interaction de sous-systèmes techniques, opérationnels, humains..., et qu'il existe une multitude de points de vue suivant lesquels un système complexe peut être analysé.

En effet, la décomposition en sous-systèmes peut procéder par analyse des objectifs, peut s'appuyer sur une approche topologique, fonctionnelle ou comportementale. Un certain nombre de méthodes existent ; bien que très générales, elles comportent beaucoup de subjectivité dans leur mise en œuvre et ne font appel à aucune formalisation standard. Le principal verrou porte ainsi sur les modèles de systèmes complexes : la finalité de mon programme de recherche pour les années à venir vise donc à développer des modèles systémiques plus rigoureux permettant d'intégrer les points de vue sûreté de fonctionnement et normatifs (domaine machines ou ferroviaire,...)

Cette approche doit conduire à la mise en œuvre d'une démarche de conception intégrée de systèmes dynamiques hybrides qui prend en compte dès la phase de conception les contraintes opérationnelles, de sécurité et de sûreté de fonctionnement, de maintenance et de fiabilité avec un objectif de coût global. Il va de soi que cette approche systémique de la sûreté doit s'appuyer sur les outils d'analyse tels que le suivi d'exigences, le retour d'expérience et la simulation intégrant les facteurs humains et les bases de données accidents/incidents des systèmes étudiés.

En complément de cette approche « statique », qui vise à intégrer la sûreté de fonctionnement dès la conception du système en assurant sa robustesse, sa fiabilité et sa maintenabilité, il est nécessaire que les modèles développés puissent être utilisés en exploitation, c'est à dire pour une approche en ligne fondée sur la supervision : la surveillance, la détection de défaillances, le diagnostic (identification des missions que le système est encore capable d'assurer compte tenu des défaillances ou du blocage de ses composants) et le pronostic (prédiction de l'état futur du système compte tenu de ses états précédents, de son état actuel et du résultat de diagnostic) sont alors destinés à élaborer des

commandes tolérantes aux fautes sécuritaires par accommodation ou reconfiguration de la commande, voire la redéfinition des objectifs [Cocquempot, 2004].

L'analyse de la reconfigurabilité du système permet de qualifier la robustesse de ce dernier en analysant sa tolérance aux fautes et de définir un ensemble de règles de conception qui, si elles sont respectées, doivent aboutir à des systèmes plus sûrs, plus fiables, plus facilement maintenables et conduiront globalement à une optimisation des coûts.

Les principaux verrous portent sur l'utilisation de ces *modèles multipoints de vue* des systèmes complexes, je propose donc d'étudier l'exploitation combinée de modèles pour :

- générer des données de sûreté quantitatives visant à déterminer la fiabilité/maintenabilité/disponibilité/sécurité du système global à partir de celles de ses constituants ; il s'agit donc de mettre au point des techniques et algorithmes d'évaluation de la sûreté de fonctionnement de systèmes complexes pour étayer et valider les alternatives de solution lors de la conception,
- identifier en quoi de tels modèles peuvent favoriser le diagnostic d'un système dynamique complexe, c'est-à-dire contribuer à la localisation de l'origine de la défaillance et à la caractérisation (instant d'apparition, amplitude, cause, conséquence) de cette défaillance,
- caractériser en quoi de tels modèles peuvent aider à prédire l'état futur, alarmant ou non, d'un système dynamique complexe,
- aider à mettre en œuvre le pronostic pour la prise de décision (aide à la conduite des opérateurs, élaboration de commandes sécuritaires tolérantes aux fautes par accommodation ou reconfiguration, redéfinition des objectifs...).

Dans les paragraphes qui suivent, je donne quelques pistes de recherche allant dans le sens des quatre points évoqués précédemment et qui font l'objet de mes perspectives de recherche.

3.1.1 Perspectives pour une approche par Monte Carlo

Le problème de conception d'un système dynamique hybride nécessite d'identifier ce qui résulte de l'agrégation de nombreuses entités en terme de fiabilité, maintenabilité, disponibilité pour le système global.

Ce dernier point prend toute son importance avec les derniers développements de la législation (en particulier, la norme CEI 61508 sur la « sécurité fonctionnelle des systèmes électriques, électroniques, électroniques programmables relatifs à la sécurité » [CEI61508a-g, 2002]) et la détermination de niveaux de SIL (Safety Integrity Level) qui définit un degré de confiance accordé à la déclinaison système/sous-système/fonction de sécurité pour remplir de manière satisfaisante les conditions de sécurité. Cette étude doit prendre en compte l'architecture du système (topologie, choix des constituants, choix et type de système de communication...) mais également sa dynamique (temps de propagation et d'élaboration des informations pertinentes, stratégiques, de sécurité...).

La méthode SAFE-SADT, sur laquelle j'ai orienté mon doctorant Vincent Benard, a mis l'accent sur les aspects modélisation, caractérisation, identification et représentation des dépendances au sein de l'architecture opérationnelle. Les aspects dynamiques de cette méthode de conception ont été également abordés pour la quantification des paramètres FMDS à des fins de validation de l'architecture opérationnelle du système automatisé conçu ; mais la quantification des paramètres de sûreté d'une architecture opérationnelle constitue en soi une étape difficile lors de la phase de validation d'une architecture opérationnelle. Sur ce point, on est confronté aux limites qui alimentent les recherches actuelles relatives aux *simulations de Monte Carlo dynamique*. Ces recherches étudient en effet les variations des paramètres du système qui ne fonctionne plus de la même manière en

situation dégradée et, où les lois de distribution sont à fortiori quelconques (et ne suivent plus des lois de distribution exponentielles) puisque le changement d'état d'un composant est susceptible de changer les lois des autres.

Pour les systèmes complexes, *l'hypothèse d'indépendance* entre les entités constituant les systèmes est *rarement vérifiée* (cas d'un système à deux composants en redondance active, la défaillance de l'un des deux est susceptible de provoquer une charge supplémentaire pour le second dont la propension à défaillir tend alors à augmenter ; cas d'un système à deux composants en redondance passive dont la mise en service du deuxième composant est assujettie à la défaillance du premier ; cas des systèmes d'automatisation qui font également apparaître des défaillances de mode commun pour toutes les entités logicielles implémentées sur une même entité matérielle).

Ces types de dépendances conduisent ainsi à une modification des lois de probabilité dont la prise en compte est absolument nécessaire pour l'obtention de résultats pertinents [Labeau, 2000] ; les travaux de recherche actuels en simulation de Monte Carlo dynamique portent sur cette thématique que je souhaite étudier pour l'analyse systémique de la sûreté de fonctionnement des systèmes complexes.

En dépit de ces inconvénients, la simulation de Monte Carlo présente un certain avantage lorsque le système étudié fait l'objet d'*événements rares* grâce aux techniques de biasage qui consistent à forcer l'occurrence de l'événement avant la fin de mission du système en introduisant une notion de poids statistique et permet ainsi d'étudier le comportement du système face à de tels événements.

Une analyse de sûreté par simulation de Monte Carlo est en soi simple, la plus grande difficulté réside dans l'établissement de la *fonction de structure, des noyaux Free Flight Kernel et Collision Kernel* sur lesquels s'appuie la simulation de Monte Carlo pour quantifier les paramètres de sûreté du système complexe étudié[Dubi, 2000] [Pasquet, 1999].

Sur cette thématique de recherche, j'ai établi une coopération avec P.E Labeau du FNRS de Bruxelles, qui travaille essentiellement sur les simulations de Monte Carlo [Labeau, 2000] [Labeau 2001], [Labeau, 2002], et nous envisageons de monter des cotutelles de thèses essentiellement appliquées au transport.

3.1.2 Perspectives pour une approche par Réseaux Bayésiens

Pour répondre à la problématique de la dépendance au sein des systèmes complexes, il me semble qu'une approche par réseaux Bayésiens est envisageable. Les réseaux Bayésiens sont des graphes causaux acycliques portant des informations probabilistes [Becker & al., 1999]. Ils permettent de représenter graphiquement la structure d'un système : les nœuds du graphe matérialisent un « concept » et les liens orientés modélisent des « relations de causalité ».

Chaque nœud du graphe se voit associer des informations probabilistes par l'intermédiaire de variable aléatoire. Les probabilités des valeurs des variables dépendent des valeurs des variables des nœuds « pères » directs et constituent ainsi des probabilités conditionnelles. Lorsqu'un nœud n'a pas de père, la distribution de ses valeurs est *supposée a priori* connue. La figure 3.1 illustre le concept de réseaux Bayésiens [Lin, 1997] [Piechowiak, 2001]. Chaque nœud porte une variable caractéristique pour le problème posé. Une distribution de probabilité des valeurs possibles est associée aux nœuds sans parents, des probabilités conditionnelles sont données aux nœuds intermédiaires en fonction des nœuds parents directs. Les liens entre les nœuds modélisent une causalité.

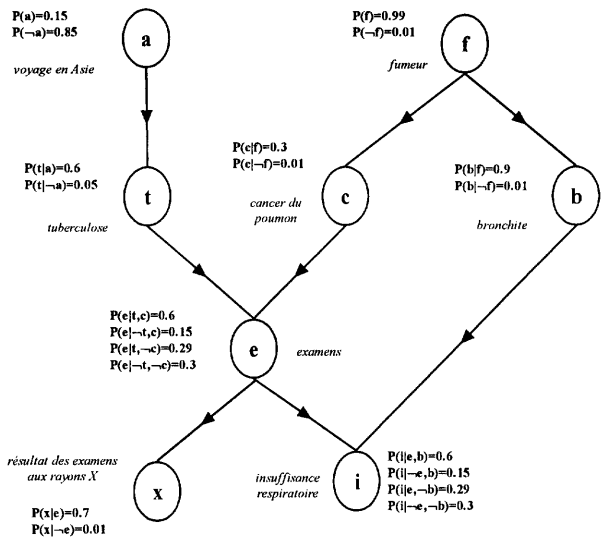

Figure 3.1 : Exemple de réseaux Bayésiens

La principale caractéristique des réseaux Bayésiens est de pouvoir calculer les probabilités conditionnelles d'événements reliés les uns aux autres par des relations de cause à effet. La modification d'une variable est propagée dans le réseau et conduit à une mise à jour des autres variables par application de la règle de Bayes : soit un ensemble d'événements B_1, B_2,....,B_n et A un événement tel que P(A)>0 alors pour tout k, la probabilité conditionnelle de B_k sachant que l'événement A s'est produit est donné par $P(B_k/A)=\frac{P(A/B_k)\cdot P(B_k)}{\sum_{j=1}^{n} P(A/B_j)\cdot P(B_j)}$. Les deux principaux inconvénients pour les réseaux Bayésiens sont la nécessité de connaître le graphe de causalité et l'obligation d'identifier toutes les probabilités conditionnelles des variables.

Des propositions de techniques d'apprentissage, de détermination de structure de réseau ou de recherche des probabilités des réseaux ont été émises [Cooper & al., 1992] [Buntime, 1996] [Cheng & al. 1997] [Krause, 1998] ainsi que des techniques de construction et traitement de réseaux hiérarchiques pour le diagnostic [Delcroix & al., 2001].

Pour ma part, l'intérêt de cet outil réside dans la modélisation des scénarios caractérisant les profils de risque d'un système complexe — profil de risque d'une alternative i={ Probabilité i, Conséquence i, Scénario causal i, Population i } — et l'étude de l'enchaînement causal des « échecs des fonctions de sécurité » menant à un événement redouté tel que celui représenté sur le diagramme cause-conséquence de la figure 3.2. J'ai orienté les travaux de thèse de Julie Beugin sur cette perspective de recherche pour l'étude de sécurité de système ferroviaire.

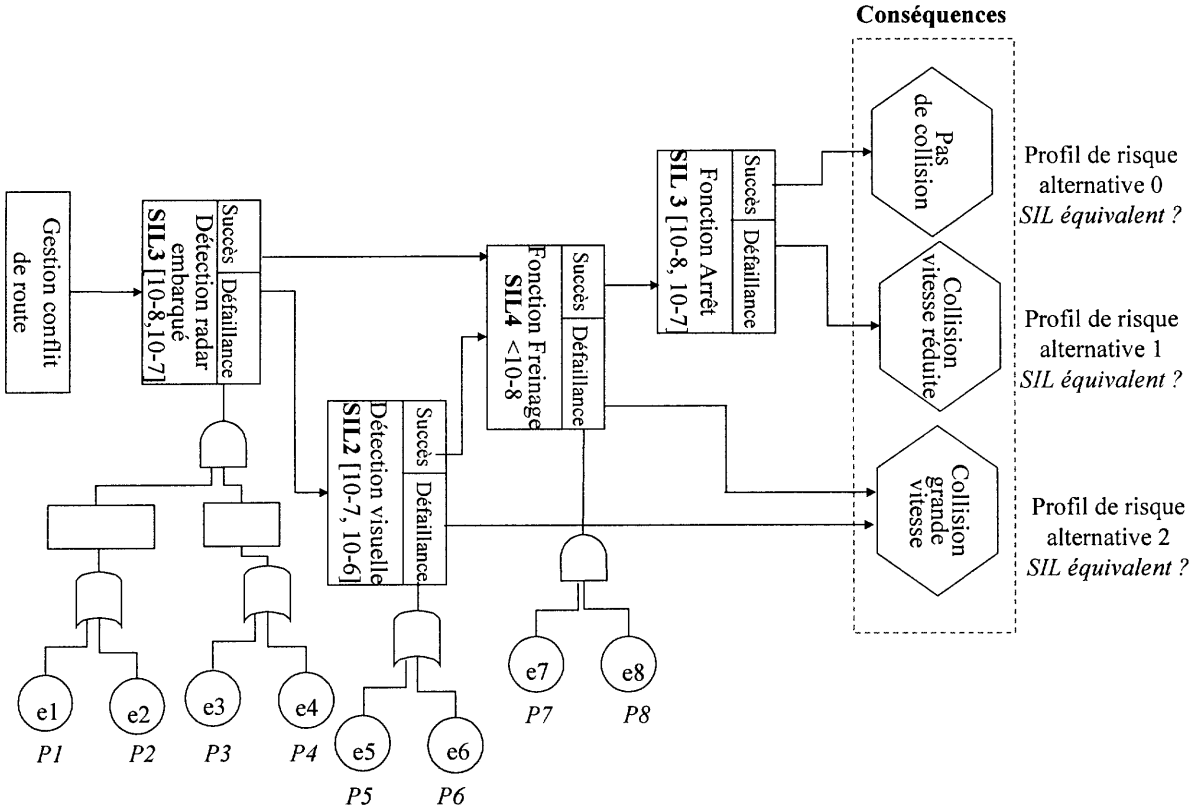

Figure 3.2 : Application des réseaux Bayésiens à un diagramme cause-conséquence pour l'étude de sécurité des systèmes ferroviaires

3.1.3 Perspectives pour une approche par UML

La volonté d'intégrer les aspects sûreté le plus tôt possible dans la conception oblige à donner aux concepteurs les moyens d'identifier et de caractériser les situations potentielles d'exploitation du système étudié. La nécessité de présence humaine autour de ces systèmes est croissante et la conception représente ainsi un enjeu socio-technico-économique.

Sur ce point, un de mes objectifs de recherche est de prendre en compte le point de vue « comportement du système » pour prévenir les défaillances et, a fortiori, les risques liés à son utilisation. Il faut donc procéder à une analyse du système étudié, déterminer les modes nominaux et dégradés du système, identifier les modes nécessitant une intervention humaine, préciser les niveaux d'intervention et identifier le partage de tâches Homme-Machine.

De ce point de vue, il faut que le concepteur dispose d'une approche systémique formelle afin d'intégrer la sûreté dès le début de conception. En ce sens, une approche UML me paraît intéressante à explorer [Booch & al., 2000]. Une modélisation UML dans le domaine machine a été réalisée par [Hasan & al., 2002] qui introduit le concept de « situation de travail », cette étude montre qu'une modélisation UML permet d'atteindre quatre objectifs :

- visualiser le système dans sa situation de travail telle qu'elle est ou telle qu'elle devrait être,
- préciser la structure et/ou le comportement du système et des opérateurs y travaillant,
- fournir un canevas guidant la construction du système en prenant en compte les contextes d'utilisation,
- documenter les décisions prises dans le déroulement du processus de conception et la capitalisation des connaissances acquises au cours du temps.

Pour être riche, une modélisation UML ne doit pas se limiter à lister les entités du système mais doit montrer les interactions entre ces différentes entités, c'est à dire mettre en exergue la dynamique du système. En ce sens, il me semble très intéressant d'adapter et généraliser le modèle UML établi pour l'intégration de la sécurité dans le processus de conception de machines à d'autres domaines (systèmes mécatroniques embarqués, systèmes ferroviaires...) [Hasan & al., 2002]. Une modélisation des systèmes complexes par systèmes multi-agents peut être également intéressante pour l'étude de la communication inter-agents [Mandiau & al., 2002].

Deux cas sont à distinguer :

- le système complexe est fixe dans son environnement de travail, la situation de travail est alors unique et les contraintes environnementales sont a fortiori imposées par cette dernière (domaine machine),
- le système complexe se déplace dans son environnement de travail, *l'exploitation du système complexe se ramène alors à une succession de « situations de travail »* dont les objectifs, les techniques mises en œuvre et les contraintes environnementales sont évolutifs (domaine ferroviaire).

Une modélisation UML telle que celle représentée à la figure 3.3 me semble prometteuse pour favoriser la prise en compte de la variabilité des objectifs poursuivis par les systèmes dynamiques hybrides et de la forte dynamique de leur environnement.

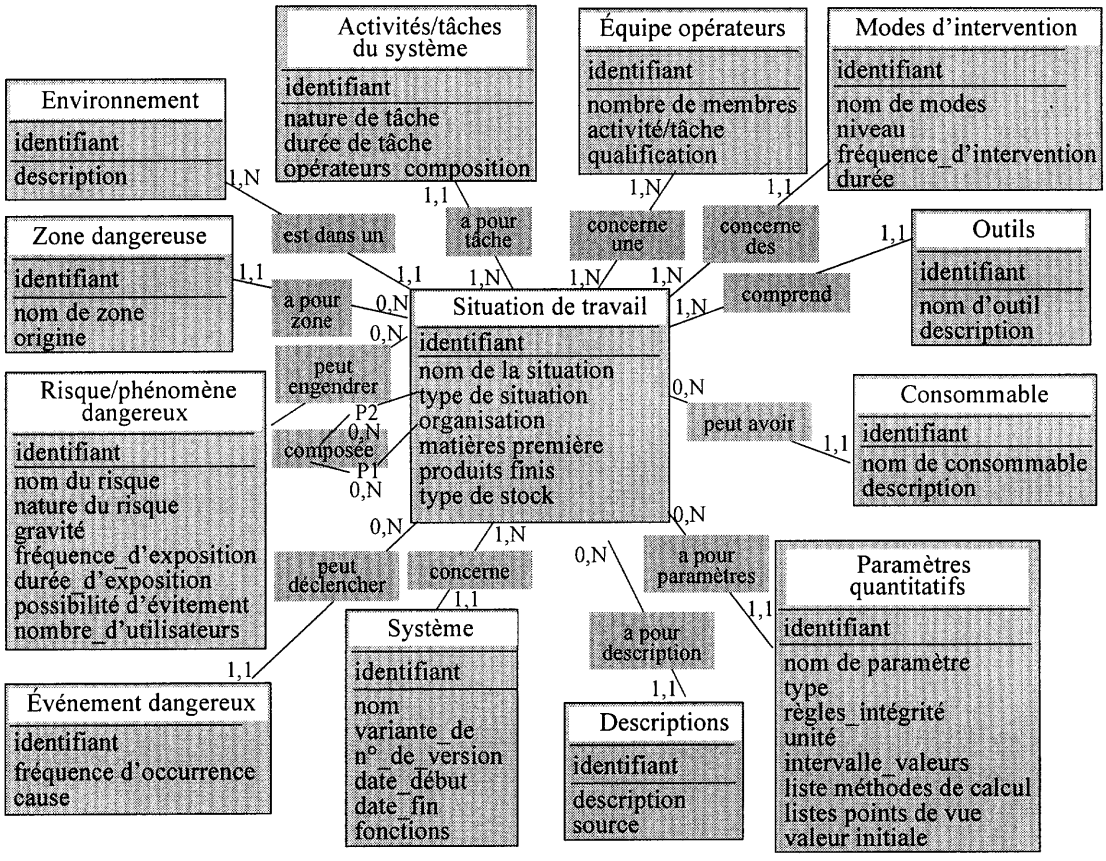

Figure 3.3 : Modélisation UML des relations entre les entités constituant une situation de travail

3.1.4 Perspectives pour une approche par Méthode B

La communauté scientifique est unanime quant à la nécessité de mettre au point des méthodes et outils pour l'évaluation de la sûreté de fonctionnement de systèmes complexes. Cette complexité rend

nécessaire la décomposition de ces systèmes en sous-systèmes qui vont eux-mêmes se décomposer en sous-fonctions. L'interaction des fonctions ainsi que la nature de leurs relations (indépendance, coopération par partage d'informations ou par échange d'informations) sont peu ou pas analysées, la dynamique fonctionnelle du système est souvent délaissée.

Les travaux de recherche que je mène actuellement et souhaite poursuivre partent du constat de l'absence de méthodes, d'outils, de langages pour la modélisation d'architectures abstraites obtenues par composition d'entités logicielles et matérielles. Mes travaux de recherche s'orienteront sur l'élaboration d'environnements logiciels, permettant de spécifier les objectifs de sûreté de fonctionnement, de comparer des alternatives de conception face à une complexité accrue et d'automatiser ces traitements.

De ce point de vue, la recherche que j'ai encadrée dans la thèse de Vincent Benard a conduit à un premier élément de réponse avec la proposition de la méthode SAFE-SADT qui a permis d'introduire « un début de langage de spécification d'architecture automatisée » avec la définition de l'ensemble F des fonctions élémentaires F={f1, f2,...fn}, la définition de l'ensemble M={M1, M2,...Mj} des matériels nécessaires à la réalisation de l'architecture opérationnelle, la définition de l'ensemble G(F) = {g1, g2, ...gl} des parties de F projeté sur l'ensemble des parties de M, et l'introduction de l'opérateur projection $\perp$.

Ce « début de langage de spécification » fait apparaître des ensembles, des prédicats sur les ensembles, des relations ainsi que des fonctions partielles, totales, injectives ou bijectives que l'on retrouve dans les méthodes formelles telles que la méthode B pour la conception de logiciels. La principale caractéristique des logiciels conçus avec la méthode B est que leur fonctionnement est conforme à leurs spécifications avec des propriétés attestées par l'existence de preuves formelles [Abrial, 1996], [Morgan, 1990]. Dans le cycle de vie des logiciels, l'objectif de la méthode B est de formaliser la spécification, expliciter la conception et simplifier la programmation.

La terminologie de la méthode B définit une entité logicielle comme une machine abstraite dont on doit pouvoir comprendre son comportement, cerner sa cohérence et sa conformité au cahier des charges ; elle contient des données (cachées) et propose à ses utilisateurs des opérations ou services (visibles). L'analogie avec la notion de service rendu et de service dégradé en sûreté de fonctionnement trouve ici tout son sens.

La méthode B a été appliquée par [Abrial, 2002] à une analyse formelle de défaillances d'un échangeur calorifique. Son objectif est d'analyser sur un système réel existant l'éventualité de certaines défaillances et d'arriver à une complétude sans pour autant vouloir corriger ou construire un nouveau système. Il a ainsi formalisé les défaillances de l'échangeur calorifique à l'aide de conditions spécifiques afin de prouver que ces conditions sont toujours fausses en mode normal et parfois vraies en mode dégradé. L'approche proposée par [Abrial, 2002] est certes limitée à un système existant mais son extension à la conception de systèmes automatisés mérite d'être explorée pour l'étude de diverses alternatives de solution.

3.1.5 Perspectives pour une approche basée sur la formalisation des connaissances normatives et d'experts

Les contraintes normatives étant de plus en plus fortes selon les domaines (domaine machine, domaine ferroviaire, domaine automobile), il apparaît de plus en plus nécessaire de disposer d'une méthode formelle de modélisation des connaissances normatives [Lacore, 1998]. Il convient ainsi de structurer les connaissances normatives en une structure générique pour que les ingénieurs, concepteurs et utilisateurs puissent utiliser de manière efficace les normes et les exploiter ainsi plus facilement que sous la forme de texte.

Le retour d'expérience est à la base de l'activité de conception de nouveaux systèmes par capitalisation des connaissances normatives et des connaissances acquises par les experts (même si elles sont incomplètes). Le concepteur souhaite intégrer le plus tôt possible dans l'activité de conception les contraintes et problèmes détectés en exploitation. Ceci met en exergue deux types de relation informelle entre les prescriptions et le retour d'expérience lors des activités de conception et d'exploitation.

Une harmonisation des normes européennes est basée à ce jour sur le concept de « New approach standardisation in the European internal Market[1] » qui donne principalement des exigences générales et précise rarement des solutions techniques. Les concepteurs doivent intégrer ces directives dans leurs activités de conception mais sans être pour autant guidés dans des prémices de solutions permettant d'atteindre les objectifs globaux. L'harmonisation des normes européennes ne suffit donc pas à elle seule pour intégrer les aspects législatifs car la conception de systèmes sûrs sous-entend de trouver des solutions techniques permettant d'atteindre les objectifs spécifiés dans les normes.

Une telle approche a été initiée par [Blaise & al., 2000] qui a recours aux modèles NIAM (Nijssen Information Analysis Method) [Habbrias, 1988] [Wintraecken, 1990] et ORM (Object Role Modelling) [Halpin, 1998] pour transcrire ces modèles en langage naturel binaire (Binary Natural Language). Une description NIAM/ORM des relations entre les législateurs, les normes, les concepteurs et utilisateurs est donnée par la figure 3.4 [Blaise & al., 2000].

Ma participation aux projets européens UGTMS (Urban Guided Transport Management Systems) et Eurnex (European Railway Network of Excellence) me conforte dans la nécessité d'exploiter une telle approche qui me semble judicieuse pour faire face aux difficultés rencontrées pour prendre en compte les lois et normes dans la conception, réalisation et exploitation de systèmes complexes (mécatroniques, embarqués, ferroviaires,....).

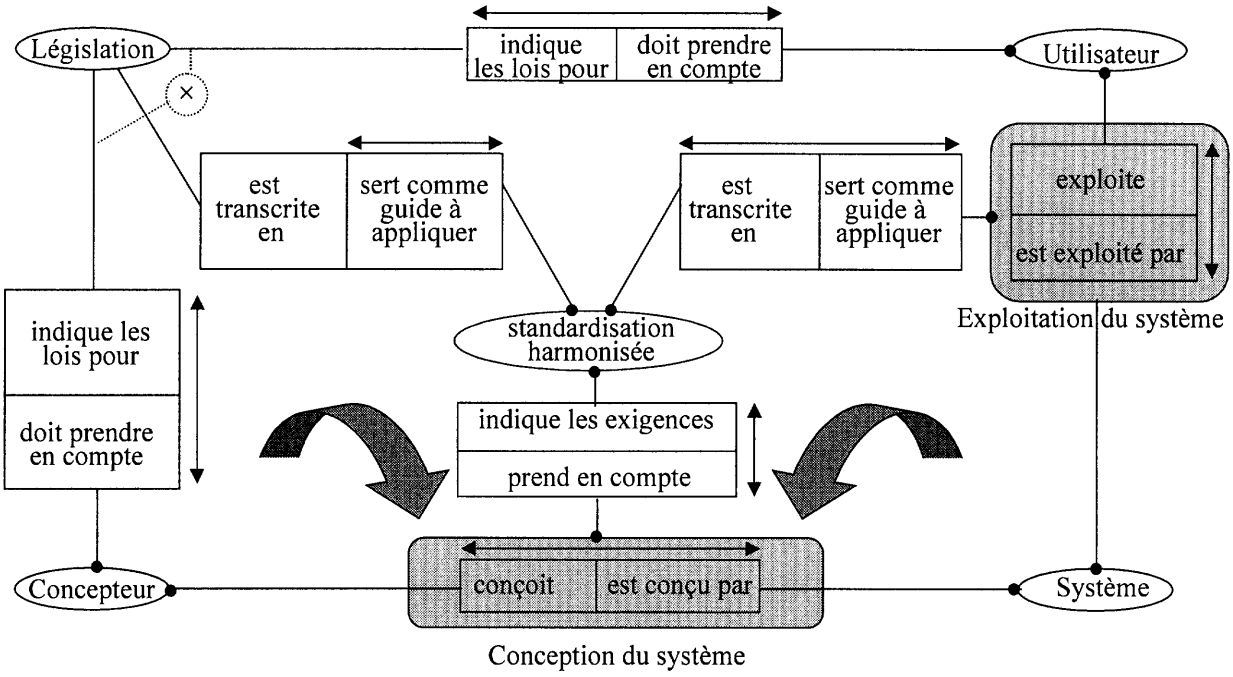

Figure 3.4 : Description des relations entre les législateurs, les normes, les concepteurs et les utilisateurs

[1] http://www.newapproach.org

3.1.6 Vers une méthodologie et un outil d'aide à la conception de systèmes complexes sûrs de fonctionnement

Mon projet de recherche pour les années à venir se situe à l'intersection des différentes perspectives de recherche que j'ai précédemment présentées.

Les réalisations en cours et à venir de mes travaux de recherche devraient converger vers une méthodologie pour l'analyse systémique de la sûreté de systèmes complexes et se concrétiser par la spécification d'un outil d'aide à la conception et à l'étude d'alternatives de solutions. Cette méthodologie doit en outre permettre de valider le système par simulation et vérifier sa conformité sous contraintes techniques, économiques, législatives et normatives [Kaufman, & al., 2001]. La figure 3.5 montre la synergie des différentes approches envisagées au niveau des perspectives pour la définition d'une méthodologie d'analyse systémique de la sûreté de fonctionnement des systèmes complexes.

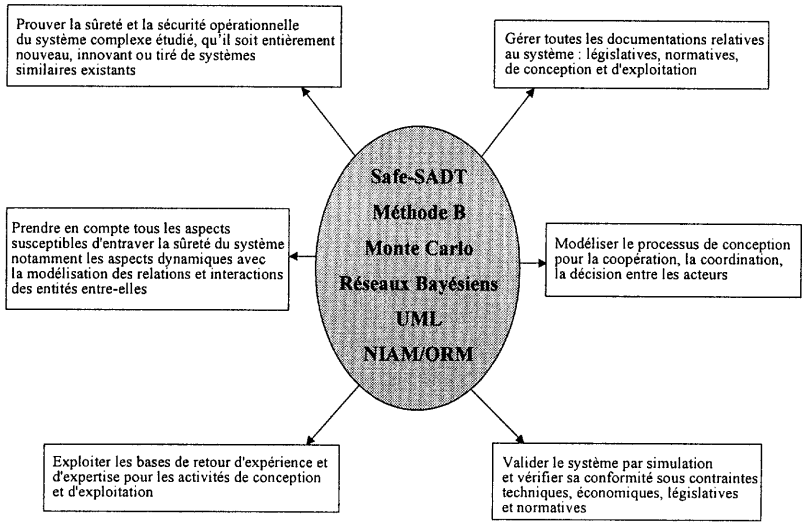

Figure 3.5 : Synergie des différentes approches pour une analyse systémique de la sûreté de fonctionnement

L'analyse systémique de la sûreté de fonctionnement des systèmes complexes doit, selon moi, aboutir à une méthodologie indépendante du domaine étudié : le caractère générique de la méthodologie à élaborer et de l'outil à concevoir doit faire en sorte que les contraintes relatives à chaque domaine (machine, embarqué, ferroviaire) soient modélisables.

En effet, cette thématique de recherche correspond à un besoin de la société dans bien des domaines avec l'apparition de technologies innovantes, je peux citer l'exemple des systèmes mécatroniques embarqués en automobile (In-Vehicle networks, Fault tolerant Drive-by-wire system) [Leen & al., 2002] [Isermann & al., 2002] ainsi que les systèmes de transport ferroviaires [Renpenning & al., 2002] [Cailliez & al., 2002].

Dans sa thèse, Julie Beugin explore actuellement certaines de ces voies pour l'évaluation du niveau de SIL global (Safety Integrated Level) d'un système ferroviaire [Beugin & al., 2003] [Cauffriez & al., 2003c] [Renaux & al., 2003] [Beugin & al., 2005] [Renaux & al. 2005].

Je souhaite ainsi faire de cette thématique de recherche un moteur pour ma recherche personnelle, l'encadrement de thèses et le rayonnement scientifique du laboratoire.

3.1.7 Résultats attendus de mes recherches

Les résultats attendus de mes travaux au niveau du laboratoire et de la région Nord-Pas-de-Calais, qui veut acquérir une véritable identité et une reconnaissance européenne dans le domaine de

la sécurité des transports, sont les suivants :

- une amélioration des connaissances des méthodes actuelles pour l'évaluation quantitative de la sûreté de fonctionnement des systèmes complexes, l'élaboration d'une méthodologie et d'un outil d'analyse systémique de la sûreté reprenant les perspectives de recherche envisagées,
- des liens étroits avec des spécialistes du domaine avec l'organisation de séminaires à Valenciennes et Bruxelles : le CEA (M. Mohamed Eid, ingénieur recherche spécialiste de simulation de Monte Carlo) et le FNRS (Fond National de la Recherche Scientifique, M. PE Labeau, chercheur et spécialiste des simulations de Monte Carlo),
- une coopération avec des laboratoires régionaux et plus particulièrement le LAGIS de l'Université des Sciences et Techniques de Lille dans le cadre du pôle d'excellence Sciences et Technologies pour la Sécurité dans les Transports ST2 de la région Nord-Pas-de-Calais (2001-2006),
- une coopération avec des industriels tels que la RATP qui attendent de mes travaux un état de l'art des méthodes innovantes pour l'évaluation de la sûreté des systèmes guidés. Cet état de l'art est accompagné d'une étude de faisabilité sur des cas réels. Ces travaux initialement amorcés dans la thèse de Vincent Benard se sont poursuivis avec la thèse de Julie Beugin en partenariat avec la RATP dans le cadre du projet européen UGTMS (Urban Guided Transport Management System, 5ème PCRD) et de sa suite ModUrban. Melle Beugin a dans ce contexte bénéficié d'une formation interne à la RATP sur la problématique de sûreté inhérente aux systèmes guidés et tente actuellement d'y répondre,
- une coopération internationale se traduisant à terme par des thèses en cotutelle avec le FNRS (M. PE Labeau), le centre de recherche en transport de Dresde (Fraunhofer IVI , Pr. J. Schütte) et le GDR européen HAMASYT (Human-Machine Systems in Transportation, LAMIH, TU de Delft, UTC, Pr. Vanderhaegen). Ces partenariats sont valorisés dans le projet européen EURNEX, réseau d'excellence dans le domaine du ferroviaire (6ème PCRD),
- un rayonnement régional avec une situation propice à la stimulation des activités de recherche et développement technologiques liées aux systèmes de transport due à la politique scientifique des Contrats de Plan État – Région (Projet TACT Technologies avancées dans le domaine de la Communication et des Transports Terrestres sur 2000-2003, Projet TAT Technologies avancées pour les Transports sur 2004-2006), le Groupement Régional pour la Recherche dans les Transports GRRT et le Réseau Interrégional de Recherche Technologique pour les Transports Terrestres RT3,
- un rayonnement du laboratoire dans le domaine du transport renforcé par la coopération régionale avec l'INRETS, le centre d'essais ferroviaires de Alstom Petite-Forêt, et l'arrivée de l'agence européenne de sécurité ferroviaire implantée à Villeneuve d'Ascq et Valenciennes,
- la nécessité de recherches pluridisciplinaires dans les domaines techniques, des sciences humaines et de la vie. L'objectif de ces coopérations vise à enrichir les connaissances scientifiques pour analyser et quantifier les risques, pour les prévenir, les gérer et en minimiser les conséquences, définir des parades techniques et les intégrer dans le système de transport dès sa conception pour en assurer la sécurité (notion de sécurité passive : mécanique, science des matériaux, énergétique et de sécurité active : automatique, électronique, génie informatique). Il faut ainsi créer une complémentarité effective entre les composantes humaines et techniques pour renforcer la sécurité globale du système Homme-Machine.

Ce dernier point rejoint les prérogatives du livre blanc de la commission européenne publié en 2001 qui veut que la sécurité soit une priorité pour les transports aériens, maritimes, et ferroviaires. Le plus haut niveau possible de sécurité doit être garanti aux citoyens par une législation appropriée et la

stricte application des contrôles et sanctions.[2] Le Comité ERRAC (European Rail Research Advisory Committee), a repris les éléments applicables au système européen de Chemin de Fer, et les a extrapolés à l'horizon 2020 dans son document « Strategic Rail Research Agenda 2020 ». Cette démarche fait apparaître les thèmes de recherche nécessaires pour atteindre les objectifs fixés dans ce livre blanc : *interopérabilité, mobilité intelligente, sûreté et sécurité, environnement, matériaux et méthodes de production innovants.*

Le réseau EURNEX, dont je fais partie, est un réseau d'excellence pour la recherche ferroviaire accepté par la commission européenne dans le cadre du 6ème PCRD. Il vise l'intégration durable des capacités de recherche présentes dans les différentes régions européennes et la création à terme d'un centre d'excellence virtuel. Il s'inscrit dans une stratégie globale de développement d'un système ferroviaire européen unique. Les principaux objectifs d'EURNEX sont : l'intégration durable des capacités de recherche et de développement technologique européennes dans le domaine ferroviaire, le développement d'un programme commun de recherches pour la création d'un véritable système ferroviaire aux dimensions du continent et la garantie d'une exploitation rentable, compétitive et sûre, la mise en place de pôles d'excellences thématiques et l'identification de nouveaux projets de recherche.

Le pôle ST2, dédié aux Sciences et Technologies pour la Sécurité dans les Transports, auquel je participe au projet 7 ambitionne d'être, à l'horizon 2006, un des pôles de référence en Europe pour les recherches interdisciplinaires sur la sécurité dans les transports terrestres, rail et route. La recherche de ST2 se focalise sur la levée de deux verrous scientifiques relatifs à la sécurité des transports : d'une part la coopération entre le pilote, le véhicule et l'environnement, d'autre part l'approche système, qui implique la prise en compte de l'interaction de multiples sous-ensembles.

Compte tenu de ce contexte, mes travaux de recherche actuels et futurs convergent vers les objectifs régionaux, nationaux et européens sur la sûreté et sécurité des systèmes complexes appliqués aux domaines de l'automobile et du ferroviaire.

3.2 Projet pédagogique

3.2.1 Formations internationales

Au cours de ces dix années en tant que Maître de Conférences, j'ai démontré mon aptitude à m'investir en pédagogie en concevant des enseignements nouveaux de productique (gestion de production, simulation de flux, modélisation et commande des robots, pédagogie par projets sur les systèmes automatisés de production) et d'informatique industrielle (sûreté de fonctionnement, instrumentation intelligente, réseaux locaux industriels) au sein de la filière Informatique-Automatique de l'Ensiame.

Je souhaite poursuivre cette action au sein de l'Ensiame et de l'Université, non seulement par la création d'enseignements nouveaux en sûreté dans les filières mécanique-énergétique et mécatronique de l'Ensiame, mais aussi par la création de formations internationales telles que doubles diplômes, diplômes tripartites, voire réseaux de formations internationales,...

J'ai en ce moment un double diplôme opérationnel avec la TU de Dresde (filière mécanique, option productique) et deux projets de doubles diplômes en cours : l'un avec la filière Transport de la TU de Dresde (conventions et conditions générales rédigées par Valenciennes et à l'étude chez le partenaire allemand qui met en place la réforme LMD), l'autre avec la filière Mécatronique de l'Université de Sarrebruck (conventions et conditions générales en cours de négociations).

Ces deux projets me semblent en très bonne voie car les partenaires ont bien identifié la nécessité et les enjeux de l'harmonisation européenne en enseignement et recherche. A ce titre, j'ai été

[2] http://europa.eu.int/comm/energy_transport/fr/lb_fr.html

sollicité par ces deux universités pour dispenser des enseignements en sûreté de fonctionnement ; ces enseignements ont été intégrés aux programmes pédagogiques des doubles diplômes sous forme de séminaires.

Le projet de double diplôme en Transport est né de ma participation au projet européen UGTMS et de mes contacts en recherche avec le Fraunhofer de Dresde. Ce projet de double diplôme en Transport a été perçu, on ne peut mieux, par la commission européenne de Bruxelles lors du « UGTMS Second Users Group Meeting » qui s'est tenu à Noisiel en décembre 2003 (M. Theodore Schlickmann). La commission européenne a trouvé là un signe précurseur de l'harmonisation européenne en matière de transports ferroviaires et ce double diplôme est devenu un point fort des résultats du projet européen UGTMS sous forme de livrable.

Le projet de double diplôme en Transport avec la TU de Dresde a pu voir le jour grâce à la création d'un master professionnel en Transports à Valenciennes. Sur ce point, j'ai participé à la rédaction du dossier d'habilitation sur les aspects internationaux à la demande de mes collègues Christian Tahon (Professeur) et Olivier Sénéchal (MdC) en charge du dossier. Ce master professionnel propose deux parcours : un parcours « sécurité des systèmes de transport non guidés » dédié au domaine de l'automobile et abordant la sécurité technologique (ergonomie des postes de conduite, biomécanique du choc, systèmes d'assistance à la conduite...) et un parcours « sécurité des systèmes intégrés de transports guidés » abordant la sécurité au niveau global du système (véhicule + passagers + infrastructure + tunnels + éléments externes).

J'ai personnellement contribué, avec mes collègues porteurs de ce projet, à l'élaboration du contenu pédagogique sur les aspects sûreté de fonctionnement avec des modules scientifiques permettant d'appréhender la sécurité des systèmes de transport (preuves formelles, sûreté de fonctionnement, analyse systémique, modélisation, simulation, plans d'expérience, déformation des structures mécaniques,...) et des modules spécifiques à la conception des systèmes de transport (sécurité des transports, politique d'exploitation, dossier de sécurité, aspects normatifs, logistique, expertise des systèmes guidés, méthodologie de conception...).

Pour les aspects sûreté de fonctionnement, j'ai particulièrement insisté sur les définitions et concepts de base (défaillances, missions et fonctions d'un système et de ses composants, description générale du système, fonctionnelle et matérielle, rappels probabilistes, FMDS), les analyses prévisionnelles de la sûreté des systèmes (méthodes d'analyse fonctionnelle FAST, APTE, SADT), les méthodes qualitatives (AMDEC, APD, APR, Hazop), les méthodes quantitatives et mixtes (diagramme de succès, arbre des causes, arbre de causes-conséquences, graphes de Markov, Monte Carlo), la conception et l'exploitation sous l'angle de la sécurité, le management de la sûreté, l'assurance qualité et la notion d'audits.

Ce master a été habilité par le ministère mais la commission d'admission, dont je suis membre, n'a pu procéder à un recrutement de qualité pour l'année universitaire 2004-2005 (20 dossiers de candidature dont 10 licences professionnelles) et a préféré après discussion avec le directeur de l'Institut des Sciences et Techniques de Valenciennes différer l'ouverture de ce master en septembre 2005 pour mieux correspondre aux objectifs fixés et aux critères des instances évaluatrices.

3.2.2 Résultats attendus pour le projet pédagogique

J'ai mis au profit de l'université de Valenciennes mes compétences acquises dans le domaine de l'international puisque j'ai moi-même intégré en 1989 l'une des premières formations européennes bi-diplomantes pour ingénieurs dans le domaine de l'EEA.

Je suis un adepte convaincu de la nécessité d'initier nos ingénieurs, nos étudiants et nos jeunes chercheurs à la culture internationale qui représente à l'heure actuelle un rayonnement des universités.

J'ai pour objectifs de poursuivre le travail en cours et de le renforcer avec la création de *doubles diplômes de proximité* (distance de 400 km) favorisant la mobilité estudiantine et enseignante avec les universités d'Aix-La-Chapelle et de Sarrebruck dans les domaines de la Mécatronique, du Transport et de la Productique.

Pour ce faire, je pense que le GDR européen HAMASYT (Human-Machine Systems in Transportation) va, par l'intermédiaire de la TU de Delft, favoriser les prises de contacts avec des TU d'autres pays telles que la TU d'Aix-La-Chapelle. Ceci démontre une fois de plus les liens étroits entre enseignements et recherche qui facilitent l'aboutissement de grands projets internationaux.

Les retombées de formations internationales en sûreté et sécurité des systèmes sont nombreuses et vont dans le sens des priorités de recherche du LAMIH, de la région Nord-Pas-de-Calais et de la commission européenne dans le domaine des transports automobiles et ferrovaires (cf. Résultats attendus en recherche, paragraphe 3.1.7).

Je pense que cette synergie avec la recherche peut conduire rapidement à la création d'une filière Transport au sein de l'Université de Valenciennes selon l'approche modulaire du LMD (modules dispensés aussi bien en université qu'en école d'ingénieurs), au même titre que la filière Maintenance récemment créée, dans lesquelles je suis prêt à m'investir au niveau local, régional, national et international, dans la continuité de mes actions et projets déjà menés à ce jour.

Conclusion générale

Ce mémoire d'habilitation à diriger les recherches est organisé en deux grandes parties. La première partie consiste en un Curriculum Vitae étendu dans lequel j'ai résumé mes activités d'enseignement, de recherche et d'administration. J'y ai succinctement présenté mon thème de recherche, mes activités d'encadrement et d'animation de la recherche sur la *sûreté de fonctionnement des systèmes automatisés complexes*.

La seconde partie de ce mémoire fait l'objet d'une présentation détaillée de mes activités de recherche, actuelles et futures, et se compose de trois chapitres.

Dans le premier chapitre, j'ai analysé la problématique globale de la sûreté de fonctionnement des systèmes automatisés en m'appuyant sur la notion de service rendu par les différents constituants du système global. J'y ai clairement défini les frontières du processus physique, du système d'automatisation, du système de sécurité et du système de contrôlabilité du risque (notion de barrières). J'ai ainsi identifié les grands axes de recherche dans le domaine de la sûreté de fonctionnement des systèmes automatisés et mis en exergue les exigences de sûreté qui s'y rattachent. Les aspects normatifs incontournables lorsqu'il s'agit de systèmes industriels complexes ont été précisés : complexité vue sous l'angle fonctionnel, structurel, comportemental et technologique.

Dans le deuxième chapitre, j'ai présenté mes contributions et résultats sur cette thématique de recherche que j'ai décomposé en deux axes.

L'axe I se focalise sur la *sûreté de processus physique*. Mon objectif était d'améliorer la performance de lignes de production en agissant sur les paramètres FMD (Fiabilité-Maintenabilité-Disponibilité) du système. J'ai mis ici en évidence les problèmes liés à la complexité d'intégration des moyens et les difficultés rencontrées pour atteindre les objectifs Fiabilité, Maintenabilité, Disponibilité du processus physique global caractérisant la performance globale du système. Ce travail a abouti à la proposition d'une méthode pour diagnostiquer les causes de non-performance et préconiser les actions les plus pertinentes à envisager. Un autre aspect de la complexité a été également abordé dans cet axe avec le problème de la maîtrise des flux et du coût engendré par des défaillances matérialisées par un rendez-vous manqué entre véhicules et composants. Ce travail a conduit à la proposition des méthodes AMD2E (Analyse des Modes de Défaillances et de leurs Effets Economiques) et MAEC (Méthode de l'Arbre Economique des Causes) qui ont été validées dans le cadre d'une thèse industrielle.

L'axe II porte sur *la conception de systèmes d'automatisation sûrs de fonctionnement*. Ces travaux partaient du constat de l'absence de langages, d'outils pour la modélisation d'architectures abstraites obtenues par composition d'entités logicielles et matérielles. L'analyse faite a mis en évidence la nécessité de valider la sûreté de fonctionnement du système d'automatisation à chaque étape de la conception par rapport aux spécifications de service approprié et inapproprié. La réflexion que j'ai menée montre la nécessité de formaliser, d'exprimer les besoins et les contraintes de l'architecture opérationnelle et fait apparaître l'existence de fonctions principales, secondaires et de fonctions techniques qui coopèrent et interagissent pour assurer la mission principale du système.

Bibliographie[1]

[Abrial, 1996] Abrial, J.R., The B-Book, Assigning programs to meanings, CUP

[Abrial, 2002] Abrial, J.M., Analyse formelle de défaillance, Exposé, Mai 2002, présenté au Club 18.3 de la SEE

[Afnor, 1989] Norme NF C46601 à C46607. Bus Fip pour échange d'information entre transmetteurs, actionneurs, automate programmable

[Akaichi, 1996] Akaïchi, J., Systèmes automatisés de production à intelligence distribuée, Thèse de doctorat, LAIL, Université des Sciences et Technologies de Lille, 1996

[Ancelin & al. 1987] Ancelin, B., Semery, A., Calcul de la productivité d'une ligne intégrée de fabrication : CALIF, une méthode analytique industrielle, RAIRO APII, 21(3), pp209-238, 1987

[Anderson & al., 1990] Anderson, RT., Neri, L., Reliability centered maintenance. Management and engineering methods, London, Elsevier Applied Science, 1990

[Aramini & al., 1996] Aramini, S., Renaux, D., Cauffriez, L., Defrenne J., Willaeys, D., Rapport de contrat, Renault-LAMIH, Juin 1996

[Aramini & al., 1998] Aramini, S., Renaux, D., Defrenne, J., Willaeys, D. A Production System Performance Assessing Approach Methodology to Analyse the Economic Cost of Disturbances. 2nd IMACS Multiconference on Computational Engineering in Systems Applications, April 1-4, 1998, Nabeul-Hammamet, Tunisia.

[Aramini, 1999] Aramini, S., Diagnostic pour l'amélioration de l'efficacité d'une usine de carrosserie montage, Thèse de doctorat, Université de Valenciennes et du Hainaut-Cambrésis, Mars, 1999 (Thèse à huis clos confidentielle jusque 30/10/2002)

[Banâtre, 1991] Banâtre, J-P., La programmation parallèle: outils, méthodes et éléments de mise en œuvre, Edition Eyrolles, 1991

[Barger & al., 2002] Parger, P., Thiriet, J-M., Robert, M., Performance and dependability evaluation of distributed dynamical systems, European Conference on System Dependability and Safety, ESRA2002/Lambda-Mu13, Lyon, France, March 2002, pp. 16-22.

[Barger & al. 2004] Barger, P., Thiriet, J-M., Robert, M., Aubry, J-F., Dependability study in distributed control systems integrating smart devices, 7th IFAC Symposium on Cost Oriented Automation (COA'2004), 7-9 juin 2004, Gatineau/Ottawa, Canada, pp. 79-84

[Bayart, 1993] Bayart, M., Staroswiecki, M., Hierarchical data and processing structures for the integration of production processes, Proceedings of the IFAC workshop on production control in process industry, PCPI'93, pp 209-216, Düsseldorf, Allemagne, 29-31 mars, 1993

[Bayart, 1994] Bayart, M., Instrumentation intelligente – Systèmes automatisés de Production à Intelligence distribuée, Habilitation à diriger les recherches, Université des sciences et technologies de Lille, Décembre, 1994

[1] Les publications où je suis auteur ou co-auteur sont bordurées sur la droite

[Bayart & al., 1998] Bayart M., Robert, M., Benoit, G., Cauffriez, L., & al. Dans la jungle des réseaux de Terrain. : Vers un guide de choix dédié « Automatisation d'applications. (pp. 44-48). Revue de l'Electricité et de l'Electronique, n°3. ISSN 1265-6534, 1998.

[Baynat, 2000] Baynat, B., Théorie des files d'attente – des chaînes de Markov aux réseaux à forme produit, Editions Hermès, 2000

[Becker & al., 1999] Becker, A., Naïm, P, Les réseaux bayésiens : modèles graphiques de connaissance, Eyrolles, 1999

[Becker & al., 2001] Becker, G., Nagel, J., Camarinopoulos, L., Kabranis, D., Dynamic reliability expressed in terms of transition frequency densities, Esrel 2001, pp1383-1386

[Bell & al., 2000] Bell, R., Bennett, P.A., Functional safety of electrical/ electronic/ programmable electronic safety-related systems, Computing & control engineering journal, february, 2000, pp3-5

[Bellon, 1997] Bellon, B., Innover ou disparaître, Ed Economica, 1994

[Benard, 2000] Benard V., Etude de la théorie du renouvellement pour l'évaluation de la sûreté de fonctionnement des systèmes complexes réparables : application au paramètre disponibilité, Mémoire de DEA, LAMIH, Université de Valenciennes, 2000

[Benard & al., 2001] Benard, V., Cauffriez, L., Renaux, D. (2001). Point of view of availability assessment for complex system: A method based onto transfer function, International Conference IFAC-INCOM'01. (cdrom). Vienna, Austria, 20-22 Sept 2001.

[Benard & al., 2001b] Benard, V., Cauffriez, L., Méthode et modèle pour l'évaluation de la sûreté de fonctionnement des systèmes complexes en phase de conception - Application à la conception des Systèmes de Transport, Rapport CNRS d'avancement n°1, Université de Valenciennes, 2001

[Benard & al., 2002] Benard V., Cauffriez L., Renaux D, Modélisation des paramètres de la sûreté de fonctionnement par des fonctions de transfert : Application à la disponibilité. In (Ed.), CIFA 2002. (cdrom). Juillet, Nantes, France, Juillet 2002.

[Benard & al., 2002b] Benard, V., Cauffriez, L., Méthode et modèle pour l'évaluation de la sûreté de fonctionnement des systèmes complexes en phase de conception - Application à la conception des Systèmes de Transport, Rapport CNRS d'avancement n°2, Université de Valenciennes, 2002

[Benard & al., 2003] Benard, V., Cauffriez, L., Renaux, D., Proposition d'un modèle probabiliste pour l'évaluation de systèmes non Markoviens sûrs de fonctionnement, PENTOM'03, 26-28 Mars 2003, pp 347-361, PUV 2003, ISBN-2-905725-51-6

[Benard & al., 2004] Benard, V., Cauffriez, L., Renaux, D., Dependability evaluation of complex systems based on a functional dynamic model : the Safe-SADT Method, Conférence Internationale EuroSim'04. (cdrom). Paris, Septembre 2004.

[Benard, 2004] Benard, V., Evaluation de la sûreté de fonctionnement des systèmes complexes basée sur un modèle fonctionnel dynamique : la méthode SAFE-SADT, Thèse de l'Université de Valenciennes, LAMIH, Décembre 2004.

[Benard & al., 2005] Benard, V., Cauffriez, L., Renaux, D. The Safe-SADT method for aiding designers to choose and improve dependable architectures for complex automated systems. Journal of Reliability Engineering and System Safety, Elsevier. Soumise le 11 mai 2005

[Benoît, 1993] Benoît, E., Capteurs symboliques et capteurs flous : un nouveau pas vers l'intelligence, Thèse de doctorat de l'Université Joseph Fourier, Grenoble I, 1993.

[Benoit & al., 2000] Benoit E., Tailland J., Foulloy L., Mauris G., A software tool for designing intelligent sensors, 16th IEEE Instrumentation and Measurement Technology Conference (IMTC 2000), Baltimore, USA, May 2000, pp. 322-326.

[Benoit & al., 2001] Benoit E., Chovin A., Foulloy L., Chatenay A., Mauris G., Safe design of CANopen distributed Instruments, 18th IEEE Instrumentation and Measurement Technology Conference (IMTC 2001), Vol. 3, Budapest, Hungary, May 2001, pp. 1768-1772.

[Berger & al., 2000] Berger, T., Cauffriez, L., Deneux, D., Popieul, J-C., Sallez, Y. Retour d'une expérience de pédagogie par projet : mise en œuvre intégrale d'une cellule flexible en école d'ingénieur. CIFA'2000, Conférence Internationale Francophone d'Automatique. (pp. 600-605). Lille, France. ISBN 2-9512309-1-5, 2000

[Besombes, 2003] Besombes, B., Senechal, O., Burlat, P., Evaluation de performance et proximité, in Evaluation des performances des systèmes de production, Chapitre 5, Sous la direction de C. Tahon, Ouvrage collectif GRP, Traité IC2 Hermès Paris, Mars 2003, pp 107-120

[Beugin, 2002] Beugin, J., Modélisation d'arbres de fautes par réseaux neuronaux pour l'évaluation de la sûreté de systèmes complexes, Rapport de DEA en coopération avec le Fraunhofer de Dresde (Allemagne), LAMIH-Université de Valenciennes, Septembre 2002

[Beugin & al., 2003] Beugin, J., Renaux, D., Cauffriez, L., Modélisation d'arbres de fautes par réseaux neuronaux pour l'évaluation de la sûreté de systèmes complexes, Colloque francophone PENTOM 2003. (pp 315-327). Valenciennes, 26-28 Mars 2003, Eds PUV Valensciences n°2, ISBN 2-905725-51-6 , 2003

[Beugin & al., 2005] Beugin, J., Renaux, D., Cauffriez, L., (2005). A safety assessment method for guided transport systems : a dynamic approach using Monte Carlo and discrete event simulations, 17th IMACS World Congress, Paris, 11-15 July, 2005, acceptée

[Beugin & al., 2005b] Beugin, J., Renaux, D., Cauffriez, L., A SIL quantification approach in complex systems of guided transport, European Safety and Reliability Conference ESREL 2005. 27-30 June, Tri City, Poland, acceptée.

[Bitton, 1990] Bitton M., Ecograi : Méthodes de conception et d'implantation de systèmes de mesure de performances pour organisations industrielles, Thèse de doctorat de l'université de Bordeaux I, Septembre 1990

[Blaise & al., 2000] Blaise, JC., Lhoste, P., Ciccotelli, J., Formalisation of normative knowledge for safe design, Safety Science – Special Issue « Safety in design », Vol. 41, n°2-3, pp 241-262, ISSN 0925-7535, March 2003

[Boehm, 1988] Boehm, B.W., A spiral Model of software development and enhancement, IEEE Computer, Vol.21, pp61-72

[Bon, 1995] Bon, J-L., Fiabilité des systèmes : méthodes mathématiques, Techniques stochastiques, 1995

[Booch & al., 2000] Booch, G., Rumbaug, J., Jacobson, I., Le guide de l'utilisateur UML, traduit de l'anglais par la société Alinter, ISBN 2-212-09103-6, Editions Eyrolles, 2000

[Boumaza, 2003] Boumaza F., Ingénierie simultanée appliquée à la conception de systèmes automatisés de production : projet COPE, Diplôme de Recherche Technologique, Université de Valenciennes et du Hainaut-Cambrésis, Octobre, 2003

[Bouras, 1995] Bouras, A., Bayart, M., Staroswiecki, M., Specification of Smart Instruments for Intelligent Control, IEEE SMC, Vancouver, Canada, 22-25 October, 1995

[Bouras, 1997] Bouras, A., Contribution à la conception d'architectures réparties : modèles génériques et interopérabilité d'instruments intelligents, Thèse de doctorat, Université des Sciences et Technologies de Lille, 1997

[BTE, 1992] BTE, Maîtrise et gestion de la maintenance, Tomes 1 et 2, Edition BTE, 1992

[Buntime, 1996] Buntime, W., A guide to the literature on learning probabilistic networks from data, IEEE Transactions On Knowledge And Data Engineering, n°8, pp195-210, 1996

[Burlat & al., 2003] Burlat, P, Marcon, E. Senechal, O., Dupas, R., Berrah, L., Démarches d'évaluation et de pilotage de la performance, in Evaluation des performances des systèmes de production, Chapitre 3, Sous la direction de C. Tahon, Ouvrage collectif GRP, Traité IC2 Hermès Paris, Mars 2003, pp 49-77

[Burman, 1995] Burman, M. H., New Results in Flow Line Analysis, Laboratory for Manufacturing and Productivity, Thèse de doctorat, Massachusetts Institute of Technology, Cambridge, MA 02139, June, 1995

[Cailliez & al., 2002] Cailliez P., Desforges, P., Sécurité ferroviaire et disponibilité de systèmes de surveillance, Lambda-Mu Esrel 2002 European Conference, pp 236-243, Lyon, 18-21th, March 2002

[Carey, 2000] Carey, M.S., Human factors in the design of safety-related systems, Computing & control engineering journal, february, 2000, pp28-32

[Campelo & al., 1997] Campelo, JC., Rodriguez, F., Gil, P-J., Serrano, J-J, Dependability evaluation of fault tolerant architectures in distributed industrial control systems, WFCS'97, 2nd IEEE International Workshop on Factory Communication Systems, Barcelona, Spain, 1997

[Cauffriez & al., 1993] Cauffriez, L., Willaeys, D., Defrenne, J. A new method to compute programmed logic functions in real-time applications : The Event-Triggered Method, IEEE/SMC'93, International Conference on "Systems, Man and Cybernetics", Proceedings Vol. 3, (pp. 210-215), October 17-20, Le Touquet, France, 1993.

[Cauffriez, 1994] Cauffriez, L., Contribution à la mesure en temps-réel des performances de production d'ateliers manufacturiers dans les applications de supervision distribuées, Novembre, 1994

[Cauffriez & al., 1994] Cauffriez, L., Defrenne, J., Impact de l'émergence des réseaux de terrain et de l'instrumentation intelligente dans la conception des systèmes d'automatisation de processus, Ministère de l'Enseignement Supérieur et de la Recherche, Rapport final du projet MESR 2033, chapitres sûreté de fonctionnement, pp 39-44 et pp 87-90, Paris, Juin 1994

[Cauffriez, & al., 1995] Cauffriez, L., Defrenne, J. Viabilité de l'information et réseau à diffusion : deux atouts pour la prise de décision dans un système réparti de contrôle/commande tolérant les fautes. Revue Européenne de Sûreté de Fonctionnement et de Diagnostic, Vol 5/2, (pp. 219-247), Hermès. ISSN 1166-3049, 1995

[Cauffriez & al., 1995b] Cauffriez, L., Defrenne, J., Willaeys, D., A tool to measure in real-time the production performances of automated manufacturing shop systems, AIAI, International Conference on Industrial Automation, Proceedings Vol. 2 pp. 433-438, June 7-9, Nancy, France, 1995

[Cauffriez & al., 1996] Cauffriez, L., Willaeys, D., Defrenne, J., A method and a Diagnosis System to value the Production Performances of Manufacturing Flow-Line Systems, IEEE/SMC CESA'96 IMACS Multiconference, International Conference on "Systems, Man and Cybernetics", Proceedings Vol. 2 pp. 814-819, July 9-12, Lille, France, 1996

[Cauffriez & al., 1997] Cauffriez, L., Willaeys, D., Defrenne, J., Mesure des indicateurs de performances de lignes de production : présentation d'une méthode et retour d'expérience. Journal Européen des systèmes Automatisés Vol. 31/8, (pp.1297-1310), Hermès. ISSN 0296-1598, Novembre, 1997

[Cauffriez & al., 1997b] Cauffriez, L. Defrenne, J. An Experimental Platform for the Reliability-Availability Evaluation of Intelligent distributed Systems, IFAC SICICA'97, 3rd International Conference Symposium on Intelligent Components and Instruments for Control Applications, (pp. 591-596), June 9-11, Annecy, France. 1997

[Cauffriez & al., 1999] Cauffriez, L., Philippe, B. Classification of Medium Access Control Method, Adressage Mode and Type of Trafic by fieldbusses., Intertional Conference on Industrial Automation. (pp. 19.13-19.16). Montréal – Canada. ISBN 2-9802946-2-4.

[Cauffriez & al., 1999b] Cauffriez, L., Defrenne, J. Influence upon the Temporal Coherence of Informations of Medium Access Control Method and Adressage Mode by fieldbusses, International Conference on Industrial Automation, June 7-9. (pp 20.1-20.4). Montréal, Canada. ISBN 2-9802946-2-4, 1999

[Cauffriez & al., 1999c] Cauffriez, L. Sous la direction de L. Cauffriez, Réseaux de terrain - Description et critères de choix. CIAME, 204 pages, Paris, Hermès. ISBN 286601-7242, 1999

[Cauffriez & al., 2003] Cauffriez, L., Willaeys, D. Towards a Predictive Model for Production Line Performance Diagnosis. Control Engineering Practice. Soumise en octobre 2003, révisée en septembre 2005 suite au reviewing

[Cauffriez & al., 2003b] Cauffriez, L., Conrard, B., Thiriet, J-M., Bayart, M., Fieldbuses and their influence on Dependability, 20th IEEE Instrumentation and Measurement Technology conference, IEEE/IMTC2003, (pp.83-88). Vail (Colorado, United Sates), 20-22nd May 2003. ISBN 0-7803-7705-2 SSN 1091-5281.

[Cauffriez & al., 2003c] Cauffriez, L., Beugin, J., Renaux, D., Millot, P., Design of Urban Guided Transport Management System : A dependability point of view, Deliverable D6, Safety conceptual approach & guidelines, 5th Framework Programme, Contract GRD2-2000-30090, pp 70-75

[Cauffriez & al., 2003d] Cauffriez, L., Renaux, D., Vanderhaegen, F., Deliverable D4 Report on Users Group and Network of Universities Activities, 5th Framework Programme, Contract GRD2-2000-30090, Urban Guided Transport Management System, pp 2-17, Paris, 2003

[Cauffriez & al., 2003e] Cauffriez, L., Renaux, D., Vanderhaegen, F., Deliverable D6, Safety conceptual approach & guidelines, 5th Framework Programme, Contract GRD2-2000-30090, Urban Guided Transport Management System, pp 2-76, Paris, 2003

[Cauffriez & al., 2004] Cauffriez, L., Cicottelli, J., Conrard, B., Bayart, M., Design of intelligent distributed control systems: A Dependability point of view. Journal of Reliability Engineering and System Safety. pp.19-32.Vol 84/1, April, Elsevier. ISSN 0951-8320, 2004

[Cauffriez & al., 2005] Cauffriez, L., Willaeys, D. A predictive model for performance diagnosis of line production. The international Journal of Advanced Manufacturing Technology. Springer. Acceptée le 26 janvier 2005

[Cauffriez & al., 2005b] Cauffriez, L., Benard, V., Renaux, D. A new formalism for designing and specifying RAMS parameters for safe complex distributed control systems : the Safe-SADT formalism, IEEE Transactions on Reliability. Acceptée le 24 août 2005

[Cauffriez & al., 2005c] Cauffriez, L., Conrard, B., Chapitre 2 : « Généralité sur la sûreté de fonctionnement ». Réseaux de terrain - Problématique et Sûreté de Fonctionnement, CIAME, Sous la direction de M. Bayart, à paraître en 2005. Paris: Hermès

[Cauffriez & al., 2005d] Cauffriez, L., Ciccotelli, J., Chapitre 4 : « Approche réseau ». Dans Tome 2 : Réseaux de terrain - Problématique et Sûreté de Fonctionnement, CIAME, Sous la direction de M. Bayart, à paraître en 2005. Paris: Hermès

[CEI60300-3-1, 2003] Dependability management – Part 3-1 : Application guide – Analysis techniques for dependability – Guide on methodology, IEC

[CEI61508a, 2002] Sécurité fonctionnelle des systèmes électriques/ électroniques/ électroniques programmables relatifs à la sûreté – Partie 1 : Prescriptions générales, avril 2000, UTE C 46-061

[CEI61508b, 2002] Sécurité fonctionnelle des systèmes électriques/ électroniques/ électroniques programmables relatifs à la sûreté – Partie 2 : Exigences pour les systèmes électriques/électroniques/ électroniques programmables, avril 2000, UTE C 46-062

[CEI61508c, 2002] Sécurité fonctionnelle des systèmes électriques/ électroniques/ électroniques programmables relatifs à la sûreté – Partie 3 : Prescriptions concernant les logiciels, avril 2000, UTE C 46-063

[CEI61508d, 2002] Sécurité fonctionnelle des systèmes électriques/ électroniques/ électroniques programmables relatifs à la sûreté – Partie 4 : Définitions et abréviations, avril 2000, UTE C46-064

[CEI61508e, 2002] Sécurité fonctionnelle des systèmes électriques/ électroniques/ électroniques programmables relatifs à la sûreté – Partie 5 : Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité, avril 2000, UTE C46-065

[CEI61508f, 2002] Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sûreté – Partie 6 : Guide pour l'application des parties 2 et 3, avril 2000, UTE C46-066

[CEI61508g, 2002] Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sûreté – Partie 7 : Bibliographie des techniques et des mesures, avril 2000, UTE C46-067

[CEI62061, 2002] CEI 62061 « Sécurité des machines – sécurité fonctionnelle des systèmes Electriques/Electroniques/Electroniques programmables, Version n°44/380/CD, Mai 2002

[CEI62236a, 2003] Railway applications – Electromagnetic compatibility – Part 1 : General maintenance result, April 2003

[CEI62236b, 2003] Railway applications – Emission of the whole railway system to the outside world, April 2003

[CEI62236c, 2003] Railway applications – Electromagnetic compatibility – Part 3-1 : Rolling stock – Train and complete vehicle, April 2003

[CEI62236d, 2003] Railway applications – Electromagnetic compatibility – Part 3-2 : Rolling stock – Apparatus, April 2003

[CEI62236e, 2003] Railway applications – Electromagnetic compatibility – Part 4 : Emission and imunity of the signalling and telecomunications apparatus, April 2003

[CEI62236f, 2003] Railway applications – Electromagnetic compatibility – Part 5 : Emission and imunity of fixed power supply installations and apparatus, April 2003

[CEI62279, 2002] Norme CEI62279, Railway applications - Communications, signalling and processing systems – Software for railway control and protection systems, September 2002

[CEI62280a, 2002] Railway applications Communication, signalling and processing systems – Part 1 : Safety related communication in closed transmission systems

[CEI62280b, 2002] Railway applications Communication, signalling and processing systems – Part 2 : Safety related communication in open transmission systems

[Chabot, 2001] Chabot, J.L., Dutuit, Y., Rauzy, A., A Petri net approach to dynamic reliability, Esrel 2001, Vol. 2, pp 1387-1394

[Charpentier, 2002] Charpentier, P., Architecture d'automatisme en sécurité des machines : études des conditions de conception liées aux défaillances de mode commun, Thèse de doctorat de l'Institut Polytechnique de Lorraine INPL, Université de Nancy I, Juillet 2002

[Châtelet & al., 2002] Châtelet E., Berenguerand C., Jellouli, O., Performance assessment of complexe maintenance policies using stochastic Petri nets, Lambda Mu13, Esrel 2002, Lyon, pp 532-537

[Cheng et al. 1997] Cheng, J., Bell, D., Liu, W., Learning Bayesian networks from data : an efficient approach based on information theory, Proceedings of the 6th ACM International Conference on Information and Knowledge Management, ICIKM97, 1997

[Ciame-Afcet, 1987] Ciame, Afcet, Livre blanc « Les capteurs intelligents – réflexion des utilisateurs », 169 pages, Paris, 1987

[Ciccotelli, 1999] Ciccotelli, J., Des systèmes compliqués aux systèmes complexes, INRS, Cahiers de notes documentaires – Hygiène et sécurité du travail, n° 1777, pp 125-133, 4ème trimestre, 1999, ISBN 2-7389-0843-8

[Ciccotelli & al., 2002] Ciccotelli, J., Bernard, A. Aide à la maîtrise de la complexité du processus de conception de systèmes complexes de production. Colloque transdisciplinaire « La complexité : ses formes, ses traitements, ses effets », 19-20 septembre, Université de Caen Basse-normandie, 2002

[CNOMO, 1987] Norme Cnomo E.41.50 .520.N, Moyens de production agrément fiabilité-maintenabilité, disponibilité, définition des temps d'état d'un moyen, Comité de normalisation des outillages et machines outils, Novembre 1987

[Coccoza-Thivent, 1997] Cocozza-Thivent, C., Processus stochastique et fiabilité des systèmes, Springer, 1997

[Cocquempot, 2004] Cocquempot, V., Contribution à la surveillance des systèmes industriels complexes, Habilitation à Diriger les Recherches, LAGIS, Université de Lille I, 10 novembre 2004

[Conrard, 1999] Conrard, B., Contribution à l'évaluation quantitative de la sûreté de fonctionnement des systèmes d'automatisation en phase de conception, Thèse de doctorat, Université Henry Poincaré Nancy 1, 1999

[Conrard & al., 2000] Conrard, B., Thiriet, J-M., Bicking, F., Dependability as a criterion for distributed systems design. 4th IFAC International Symposium on Intelligent Components and Instruments for Control Applications, Buenos Aires, Argentina, 13-15 september, 2000, pp 45-50

[Conrard & al., 2004] Conrard, B., Thiriet, J-M., Robert, M., Distributed system design based on dependability evaluation : a case study on a pilot thermal process, Reliability and Engineering System Safety, Elsevier, Article in Press, 2004

[Cooper et al., 1992] Cooper, G., Hersovits, E., A Bayesian method for the induction of probabilistic networks from data , Machine learning, n°9, pp309-405, 1990

[Cox, 1966] Cox, DR., Théorie du renouvellement, Dunod, Paris, 1966

[Dallery & al.,1988] Dallery, Y., David, R., Xie, X-L., An efficient algorithm for analysis of transfer lines with unreliable machine and finite buffers, IIE Transactions, vol. 20, pp280-283, 1988

[Dallery & al., 1989] Dallery, Y., David, R., Xie, X-L, "Approximate analysis of transfer lines with unreliable machines and finite buffers", IEEE Transactions on Automatic Control, Vol. 34, n°9, pp943-953, 1989

[Dallery & al., 1992] Dallery, Y., Gershwin, S. B., "Manufacturing flow line systems: a review of models and analytical results", Queueing Systems : Theory and Applications, vol.12, pp 3-94, 1992

[Dapoigny & al., 2004] Dapoigny, R., Barlatier, P., Benoit, E., Foulloy, L., A functional and behavorial knowledge-based implementation for intelligent sensors/actuators, 17th Int. Flairs Conf. (Flairs'04) (AAAI Press), Miami, US, May 2004, pp 122-127

[Decotignie, 1993] Decotignie, J-D., Pleinevaux, A., A survey on industrial communication networks, Ann. Telecommunications 1993, 48 (9-10), 435-48

[Decotignie, 1999] Decotignie, J.D., Some future directions in fieldbus research and development. In Fieldbus Technology, Systems Integration, Networking and Engineering, Proceedings of the Fieldbus Conference FeT'99, Spreinger, pp 308-312

[Decotignie, 2002] Decotignie, J.D., Wireless Fieldbuses, Proceedings IFAC 2002, 15th Triennal World Congress, Barcelona, Spain

[Delcroix & al., 2001] Delcroix, V., Piechowiak, S., Rodriguez, J., Diagnostic à base de réseaux bayésiens hiérarchiques, Journées Nationales sur les Modèles de Raisonnement JNMR2001, Mai 2001

[Dessi, 1996] Dessi, F., Conception de systèmes automatisés sûrs de fonctionnement – Application à une régulation de température autour du réseau de terrain Fip, Rapport de DEA, LAMIH-Université de

Valenciennes, Juillet 1996

[Dias, 1993] Projet Esprit n°2172, Distributed intelligent actuators and sensors, 1993

[Di Mascolo, 1996] Di Mascolo, Sur l'évaluation de performances et le pilotage des systèmes de production, HDR de l'Institut Polytechnique de Grenoble, 1996

[DS21906, 1990] Norme Dannoise, DS21906, P-Net, Multi-master, multi-net fieldbus for sensor, actuator and controller communications, 1990

[DIN19245a-c, 1990] Norme allemande, Profibus, Process Fieldbus, 1990

[Dubi, 2000] Dubi, A., Monte Carlo Applications in Systems Engineering, John Wiley & Sons, Ltd, ISBN 0471981729, 2000

[Dubois & al., 1982] Dubois, D., Forestier, J-P., "Productivité et en-cours moyen d'un ensemble de deux machines séparées par une zone de stockage", Revue RAIRO, vol. 16, pp105-132, 1982

[Elloy & al., 2002] Elloy, J-P., Simonot-Lion, F., An architecture description language supporting development process of in-vehicule embedded systems, Proceedings IFAC 2002, 15th Triennal World Congress, Barcelona, Spain

[Embrey, 1992] Embrey, D.E., Incorporating management and organizational factors into probabilistic safety assessment, Relianility Engineering and System Safety, vol. 38, pp 199-208, Elsevier, 1992

[EN292, 1997] Norme EN 292, Sécurité des machines - Notions fondamentales. Principes généraux de conception. Partie 1 : Terminologie de base, méthodologie, AFNOR, Janvier 1997

[EN954-1,1996] Norme EN954-1, Sécurité des machines – Parties des systèmes de commande relatives à la sécurité - Partie 1 : Principes généraux de conception, Décembre 1996

[EN1050, 1991] Norme EN 1050, Sécurité des machines – Principes pour l'appréciation du risque, Décembre 1991

[EN50126, 2000] Norme EN50126, Applications ferroviaires : spécification et démonstration de la fiabilité, disponibilité, maintenabilité et sécurité (FDMS), Janvier 2000

[EN50128, 1995] Norme EN50128, Draft, Railway applications : software for railway control and protection systems, November, 1995

[EN50129, 2002] Norme EN50129, Railway applications : comunication, signalling and processing systems – safety related electronic systems for signalling, 2002

[EST 2002] Maîtrise des risques en conception des systèmes ferroviaires, EST Equipement et Systèmes du Transport, RATP, EST/CTA/MRS/ID 172V1

[Foata & al., 2002] Foata, D., Fuchs, A., Processus stochastiques, Dunod, 2002

[Frein & al., 1996] Frein Y., Commault C., Dallery, Y. (1996) Modeling and analysis of closed-loop production lines with unreliable machine and finite buffers, IIE Transactions, Vol. 28, pp 545-554

[Gehin, 1994] Gehin, A.L., Analyse fonctionnelle et modèle générique des capteurs intelligents – application à la surveillance de l'anesthésie, Thèse de doctorat de l'Université de Lille 1, Janvier 1994

[Gershwin, 1987a] Gershwin, S.B., An efficient decomposition algorithm for the approximate evaluation of tandem queues with finite storage space and blocking, Operations Research, March-April, pp 291-305, 1987

[Gershwin, 1987b] Gershwin S.B., Representation and analysis of transfer lines with machines that have different processing rates, Annals of Operations Research, Vol. 9, pp 511-530, 1987

[Gershwin, 1994] Gershwin, S.B., Manufacturing Systems Engineering, Prentice Hall, New Jersey, 1994

[Guéguan, 1995] Guégan, M-J., Degré d'automatisation de système automatisé de production, Rapport de DEA, LAMIH, Université de Valenciennes et du Hainaut-Cambrésis, Juillet 1995

[Habbrias, 1988] Habbrias, H., Le modèle relationnel binaire, Méthode I.A. (NIAM), Editions Eyrolles

[Halpin, 1998] Halpin, T.A., Object-Role Modeling (ORM/NIAM), Handbook on Architectures of Information Systems, Springer, ISBN 3-540-64453-9

[Hanus & al., 1996] Hanus, R., Bogaerts, P., Introduction à l'automatisme – Système continu, Vol.1, De Boeck Université, 1996

[Hasan & al., 2002] Hasan, R., Bernard, A., Ciccotelli, J., Martin, P., Integrating safety into design process : elements and concepts relative to the working station, Safety Science – Special Issue « Safety in design », Vol. 41, n°2-3, pp 155-180, ISSN 0925-7535, March 2003

[Hollnagel, 1993] Hollnagel, E., Reliability of cognition : Foundations of Human Reliability Analysis, Academic Press, London, 1996

[Hollnagel, 1999] Hollnagel, E. Accident and barriers, 7th European Conference on Cognitive Science Approaches to Process Control, 21-24 Septembre, Villeneuve d'Ascq, France, 1999, pp175-180

[Hong, 1995] Hong S.H. Scheduling Algorithm of data sampling times in the integrated communication and control systems, IEEE Transactions on Control Systems Technology, 3(2), pp. 225-230, 1995

[IGL, 1989] IGL Technology, SADT un langage pour communiquer, Eyrolles, Paris, 1989

[Isermann & al., 2002] Isermann, R., Schwarz, R., Stölzl S., Fault tolerant Drive-by-wire Systems, IEEE Control Systems, October 2002

[Juanole & al., 1995] Juanole, G., Gallon, L., Critical Time Distributed Systems : Qualitative and quantitative analysis based on stochastic timed Petri Nets, FORTE95, 8th IFIP Conference on Formal Description Techniques for Distributed Systems and Communication Protocols, Montreal, Canada, 1995

[Juanole & al., 1998] Juanole, G., Blum, I., Evaluating the Quality of Service of a real-time distributed system and its impcat on the performance on an industrial application, Rapport LAAS 98202, Mai, 1998

[Juanole, 2002] Juanole, G., Quality of service of local area networks and distributed automation : models and performances, Proceedings IFAC 2002, 15th Triennal World Congress, Barcelona, Spain

[Kaufman & al., 2001] Kaufman, L.M., Giras, T.C., Simulation of rare events in transportation systems, Proceedings of the 2001 Winter Simulation Conference, Eds Peters, Smith, Medeiros, Rohrer, pp 1380-1385, 2001

[Kopetz, 1997] Kopetz H. Real-time systems design principles for distributed embedded applications, Kluwer Academics Publishers, 1997

[Kopetz, 2002] Kopetz, H., Time-triggered real-time computing, , Proceedings IFAC 2002, 15th Triennal World Congress, Barcelona, Spain

[Kosturiak & al., 1995] Kosturiak, J., Gregor, M., Simulation von Produktionssystemen, Springer-Verlag Wien New York, ISBN 3-211-82701-3

[Krause, 1998] Krause, P., Learning probabilistic networks, Technical Report, Philips Research Lab, 1998

[Kumamoto & al., 1996] Kumamoto, H., Henley, E.J., Risk assessment and Management for Engineers and scientists, IEEE Press, ISBN 0780310047, 1996

[Labeau,2000] Labeau, P.E., Partially unbiaised estimators for reliability and availability calculations, Progress in Nuclear Energy, Vol. 36, n°2, pp131-187, 2000

[Labeau, 2001] Labeau, P.E., Monte Carlo simulation for dynamic reliability problems with distributed safety borders, Esrel 2001, pp1395-1400

[Labeau, 2002] Labeau, P.E., Zio, E., Procedures of Monte Carlo transport simulation for applications in system engineering, Journal of Reliability Engineering and System Safety, vol. 77, pp217-228, 2002

[Lacore, 1998] Lacore, J-P., Rôle joué par la normalisation : Bilan et perspectives, Actes de la journée INRS SRS 98, Systèmes relatifs à la sécurité, Paris, Mars 1998, 69p

[Laprie & al., 1995] Laprie, J.-C., Blanquart, J-P., & al., *Guide de la sûreté de fonctionnement*, éditions Cépaduès, 1995

[Le Bihan, 1998] Le Bihan, Hervé, "De nouvelles méthodes analytiques pour l'évaluation des performances de lignes de production", Thèse de doctorat, Paris 6, 1998

[Leen & al., 2002] Leen, G., Hefferman, D., Expanding Automotive Electronic Systems, IEEE Computer, 0018-9162/02, pp 88-93, January 2002

[Le Lann, 1993]Le Lann G. Deterministic multiple access protocols for real time local area networks, research report 246, INRIA, France, 1993

[Le Lann & al., 1994] Le Lann G., Rivierre N. Real time communications over broadcast networks: the CSMA-DCR and DOD/CSMA-CD protocols, RTS'94, pp. 67-84, Teknea, Toulouse France, 1994

[Lemoigne, 1994] Lemoigne, J-L., La théorie du système général- théorie de la modélisation, Editions Presses universitaires deFrance, 4ème édition, 1994

[Lepage & al., 1989] Lepage F., Afilal F., Antoine P., Bajic E., Bron JY., Divoux T., Les réseaux locaux industriels, Hermès, ISBN 2-86601-166-X, Paris, 1989

[Lepreux, 2003] Lepreux S., Abed M., Kolski C., A human-centred methodology applied to decision support system design and evaluation in a railway network context, Cogn Tech Work, 2003 (5), 248-271

[Ligeron, 2003] Ligeron, J.P, Les limites de la sûreté de fonctionnement, Présentation lors de la session d'ouverture, PENTOM'03, 26-28 Mars 2003, PUV 2003, ISBN-2-905725-51-6

[Lin, 1997] Lin, Y., Druzdzel, M.J., Computational Advantages of Relevance Reasoning in Bayesian Belief Networks, Proceedings of the Thirteenth Annual Conference on Uncertainty in Artificial Intelligence (UAI-97), pp342-350, Providence, Rhode Isalnd, August, 1997

[Lind, 1990] Lind, M. Representing Goals and Functions of Complex Systems : an introduction to Multilevel Flow Modelling. Technical Report 90-D-381. TU Danmark.

[Lorino, 1997] Lorini, P., Méthodes et pratiques de la performance - le guide du pilotage, Les éditions d'organisation, Paris, 1997

[Lyonnet, 2000] Lyonnet, P., La maintenance : Mathématiques et méthodes, Editions Tec & Doc, 2000

[Maccrimmon & al., 1986] Maccrimmon, K.R., Wehrung, D.A., Taking risks : the management of uncertainty, Collier Macmillan, Londres, 1986

[Mammeri & al., 1993] Mammeri, Z., Thomesse, J.P., Réseaux locaux industriels, Eyrolles, ISBN 2-212-09010, 1993

[Mandiau & al., 2002] Mandiau, R., Grislin, E., Systèmes multiagents, Techniques de l'ingénieur, Traité Informatique Industrielle, S 7 216, 2002, pp. 1-16

[Marty, 1996] Marty, C., Le Juste à temps : de la théorie à la pratique, Hermès, ISBN 2-86601-523-1

[Masten, 1997] Masten, M-K., Electronics : the intelligence in intelligent control, pp 1-11, Edited by L. Foulloy, Annecy, 9-11 Juin, 1997

[Mauris & al., 2002] Mauris, G., Foulloy, L., A fuzzy symbolic approach to formalize sensory measurements : an application to a comfort sensor, IEEE Transactions on instrumentation and measurement, vol. 51, n°4, Août 2002

[MESR, 1994] MESR 2033, Impact de l'émergence des réseaux de terrain et de l'instrumentation intelligente dans la conception des systèmes d'automatisation de processus, Ministère de l'Enseignement Supérieur et de la Recherche, Rapport final, 102 pages, Paris, 1994

[Meunier & al., 2000] Meunier, P., Denis, B., Lesage, J-J., Safety analysis during the control architecture design of automated systems, IFAC Safeprocess 2000, Budapest, Hungary, June 14-16 June, 2000

[Migge & al., 2000] Migge, J., Elloy, J-P., Embedded electronic architecture, 3th International Workshop on open systems in automotive networks, Bad Homburg, Germany, 02-03 February, 2000

[Millot, 2003]. Supervision et coopération homme-machine : app. In Sous La Direction De Guy Boy (Ed.), Ingénierie cognitive, Hermès-Lavoisier, Paris, pp. 35-70.

[Moncelet, 1998] Moncelet, G., Application des réseaux de Petri à l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile, Thèse de doctorat, Université Paul Sabatier, Toulouse, France

[Morgan, 1990] Morgan, C., Programming from specifications, Prentice Hall

[Morin, 1990] Morin, E., Introduction à la pensée complexe, Editions ESF, Paris, 1990

[Neumann & al., 2002] Neumann, P., Diedrich, C., Simon, R., Enginnering of field devices using device descriptions, Proceedings IFAC 2002, 15th Triennal World Congress, Barcelona, Spain

[NF C46602] AFNOR, Bus Fip pour échange d'informations entre transmetteurs, actionneurs et automates – Couche Application – Services périodiques et apériodiques, 1990

[NF C46603] AFNOR, Bus Fip pour échange d'informations entre transmetteurs, actionneurs et automates – Couche Liaison de Données, 1990

[NF C46604] AFNOR, Bus Fip pour échange d'informations entre transmetteurs, actionneurs et automates – Couche Physique en bande de base sur paire torsadée blindée, 1990

[Niel, 1998] Niel, E., Sécurité opérationnelle des systèmes de production, Techniques de l'ingénieur, R76401-8, 1998

[Niel & al., 2002] Niel, E., Craye, E., Maîtrise des risques et sûreté de fonctionnement des systèmes de production, Lavoisier 2002, ISBN 2-7462-0402-9

[Noyes, & al., 2001] Noyes, D., Gouriveau, R., Outils d'analyse des risques dans le processus de réponse à appel d'offre, Qualita 2001, 22-23 Mars 2001, Annecy France, pp106-111

[Noyes, 2002] Noyes D., Approche analytique par espace d'états Markov, in Maîtrise des risques et sûreté de fonctionnement des systèmes de production, Sous la direction de E. Niel, E. Craye, Hermès, ISBN 2-7462-0402-9, pp 239-269

[Pagès & al., 1980] Pagès, A., Gondran, M., Fiabilité des systèmes, Editions Eyrolles, 1980

[Pasquet, 1999] Pasquet, S., Analyses de sûreté de fonctionnement de systèmes dynamiques à l'aide de diagramme de flux et réseaux de neurones, Thèse de l'université technologique de Troyes, 1999

[Patchong & al., 1996] Patchong, A., Cauffriez, L., Willaeys, D., Defrenne, J., Diagnostic pour l'amélioration d'un atelier de production : application à l'atelier ferrage de Sevelnord, Rapport de contrat, LAMIH-Sevelnord, Juin 1996

[Patchong, 1997] Méthodes de modélisation, d'analyse et de diagnostic pour l'amélioration de l'efficacité d'un atelier de production, Thèse de doctorat, LAMIH, Université de Valenciennes et du Hainaut-Cambrésis, 1997

[Patchong & al., 1997] Patchong, A., Willaeys, D., Defrenne, J., Analysis of a transfer line with automated and manual stations and no intermediate storage, EDA'97, International Conference on Engineering Design and automation, Bangkok, 1997

[Pham, 2003] Pham, H., Handbook of Reliability Engineering, ISBN 1-85233-453-3, Springer-Verlag, 2003

[Piechowiak, 2001] Piechowiak, S., Raisonnement à base de contraintes : Application au diagnostic, Habilitation à diriger les recherches, Université de Valenciennes et du Hainaut-Cambrésis, 2001

[Philippe & al., 1999] Philippe, B. Cauffriez, L. Une architecture objet basée sur un réseau CAN : Application à la description d'un robot mobile, INNOCAP 99, European Symposium sensor networks and communications, (pp. 87-92). 28-29 Avril 1999, Grenoble, France, 1999

[Piechowiak, 2001] Piechowiak, S., Raisonnement à base de contraintes : Application au diagnostic, Habilitation à diriger les recherches, Université de Valenciennes et du Hainaut-Cambrésis, 2001

[Polet, 2002] Polet, P., Modélisation des franchissements de barrières pour l'analyse des risques des systèmes homme-machine, Thèse de doctorat, Université de Valenciennes et du Hainaut-Cambrésis, 2002

[Polet & al., 2002] Polet, P., Vanderhaegen, F., Wieringa, P.A., Theory of Safety-Related Violations of System Barriers, Cognition Technology & Work, 2002, 4 :171-179, Springer-Verlag, London

[Quintian, 2003] Quintian, L. Lahire, P. Vers une meilleure intégration des composants « sur l'étagère », OCM03, 2003

[Rafoux, 1995] Rafoux J.F., La sûreté des procédés industriels, 20 ans du SPI, Nancy, 1995

[Rasmussen, 1997] Rasmussen, J., Risk management in a dynamic society : a modelling problem, Safety science, Volume 27, Issues 2-3, Pages 183-213, Novembre 1997

[Reason, 1993] Reason, J., L'erreur humaine, traduction de Hoc, J.M., Presses universitaires de France, 1993

[Renard, 1998] Viabilité de l'information pour la prise de décision dans un site réparti de contrôle/commande, Rapport de DEA, LAMIH-Université de Valenciennes, Juillet 1998

[Renaux & al., 1999] Renaux, D., Cauffriez, L. Equivalent Failure Rate Assessment in case of Periodically Tested Systems, ESREL'99 Tenth European Conference on Safety and Reliability, (pp 1573-1578), September 13-17, Münich-Garching, Germany. ISBN 9058091090, 1999

[Renaux & al., 2001] Renaux, D., Cauffriez, L., Aramini, S. Application of the Cause-cost tree methodology for the evaluation of a failure cost. In (Ed.), International Conference European Safety and Reliability ESREL 2001. (pp. 293-300). September, Turin, Italie, ISBN 88-8202-099-1, Eds Zio Demichela Piccinini.

[Renaux & al., 2001b] Renaux, D., Cauffriez, L., Aramini, S., Quantification du coût des défaillances, Méthode de l'arbre de causes-coûts. In (Ed.), Qualita 2001 4ème congrés international pluridisciplinaire. (pp. 328-333). Mars, Annecy, France. ISBN 2-9516453-0-9, 22-23, Mars 2001

[Renaux & al., 2002] Renaux, D., Cauffriez, L., Benard, V. Towards an optimal production cost. In (Ed.), European Conference on System Dependability and Safety, ESREL 2002. (pp. 218-223). March, Lyon, France.

[Renaux & al., 2003] Renaux, D., Beugin, J., Cauffriez, L. Proposal for a neural network approach and ordering heuristic for the fault tree evaluation, European Safety and Reliability Conference ESREL 2003, pp.1301-1306, June, Maastricht, Nederland, ISBN 9058095517, Eds Bedford & van Gelder..

[Renaux & al., 2005] Renaux, D., Beugin, J., Cauffriez, L., Allocation et évaluation globale de la sécurité d'un système : Application aux systèmes guidés, Pentom 2005, Marrakech (Maroc), Avril 2005.

[Renpenning & al., 2002] Renpenning, F., Braband, J., Risk assessment of a novel railway signalling concept, Lambda-Mu Esrel 2002 European Conference, pp 251-257, Lyon, 18-21th, March 2002

[Robert & al., 1993] Robert, M., Marchandiaux, M., Porte, M., Capteurs intelligents et méthodologie d'évaluation, Editions Hermès, ISBN 2-86601-382-4

[Roy, 1993] Roy, B., Aide multicritère à la décision – méthodes et cas, Economica, Paris, 1993

[Royce, 1970] Royce, W.W, Managing the development of large software systems, Proc. Westcon, California, USA

[Salvatore, & al., 2002] Salvatore C., Salvatore, M., Tovar, E., Vasques, F., Multi-master Profibus-DP modelling and worst case analysis-based evaluation, IFAC 15th Triennal World Congress, Barcelona, Spain, 2002

[Senechal, 2004] Senechal, O., Pilotage des systèmes de production vers la performance globale, HDR de l'Université de Valenciennes, LAMIH, Septembre 2004

[Simonot-Lion, 1999] Simonot-Lion, F., Une contribution à la modélsiation et à la validation d'architectures temps réel, Habilitation à Diriger les Recherches, INPL, Nancy

[Son & al., 2003] Son, H-S., Seong, P-H., Development of a safety critical software requirements verification method with combined CPN and PVS : a nuclear power plant protection systems application, Reliability engineering and system safety, 80 (2003), pp19-32

[Sourisse & al.,1996] Sourisse C. , Boudillon, L., La sécurité des machines automatisées, Tome 1, Collection Technique Groupe Schneider, ISBN 2-907314-29-7

[Staroswiecki & al., 1994] Staroswiecki, M., Bayart, M., Actionneurs Intelligents, Editions Hermès, 1994, ISBN 2-86601-439-1

[Staroswiecki & al., 1994] Staroswiecki, M. Bayart, M., Actionneurs intelligents, Hermès, ISBN 2-86601-439-1, 1994

[Staroswiecki & al., 1996] Staroswiecki, M., Bayart, M., Models and languages for the interoperability of smarts intsruments, Automatica, Vol. 32, n°6, pp 859-873, 1996

[Terracol & al., 1987] Terracol C., David R., Performance d'une ligne composée de machines et stocks intermédiaires, RAIRO APII, vil. 21 , pp239-262, 1987

[Thiriet, 2004] Thiriet, J-M., Sûreté de fonctionnement des systèmes d'automatisation à intelligence distribuée, Habilitation à diriger les recherches, UHP, Nancy 1, 2004

[Thomesse, 1997] Thomesse, J-P., Interoperability : an overview, Sicica'97, 3th IFAC symposium on intelligent components and instruments for control application, pp 473-478, Edited by L. Foulloy, Annecy, 9-11 Juin, 1997

[Thomesse, 1999a] Thomesse, J-P., Open issues in fieldbus based systems, Proceedings IFAC 2002, 15th Triennal World Congress, Barcelona, Spain

[Thomesse, 1999b] Thomesse, J.P., Fieldbus and interoperability. Control Engineering Practice 7, Pergamon, pp81-94

[Tindell, & al., 1995a] Tindell K., Burns A., Welling J. Analysis of real time communication. The journal of real time systems, 9, pp. 147-171, 1995
[Tindell, & al., 1995b] Tindell K., Burns A., Welling J. Calculating controller area network message response times, Control Engineering Practice, vol 3, pp. 1163-1168, 1995

[Tindell & al., 1995c] Tindell K., Hansson H. Babbling Idiots, the Dual –Priority Protocol and Smart CAN Controllers, Proceeding of ICC'95, CiA/CAN in Automation, 1995

[Tolio & al., 2002] Tolio T., Gershwin S.B., Matta A., Analysis of two-machine lines with multiple failure modes, IIE Transactions, vol. 34, n°1, pp51-62, January, 2002.

[Trentesaux, 2002] Trentesaux, D., Pilotage hétérarchique des systèmes de production, Habilitation à diriger les recherches, Université de Valenciennes et du Hainaut-Cambrésis, 2002

[UGTMS, 2002] Deliverable D1, First report for a preliminary definition of UGTMS, 5th Framework Programme, Contract GRD2-2000-30090, 119 pages

[UGTMS, 2003] Deliverable D5, Functional requirement specification of ATP core functions, 5th Framework Programme, Contract GRD2-2000-3009, 42 pages

[Vanderhaegen, 2003] Vanderhaegen, F., Analyse et contrôle de l'erreur humaine dans les systèmes homme-machine, Habilitation à diriger les recherches, Université de Valenciennes et du Hainaut-Cambrésis, 2003

[Vargas, 1992] Vargas, A. R., Sur la modélisation et l'évaluation de performances de lignes de fabrication non-homogènes, Thèse de doctorat, INPG, 1992

[Verlinde, 1989] Verlinde, C., Contribution à l'étude des architectures de systèmes automatisés, Thèse de doctorat de l'Institut Polytechnique de Lorraine INPL, Université de Nancy I, 1989

[Villemeur, 1988] Villemeur A., Sûreté de fonctionnement des systèmes industriels : Fiabilité - Facteurs humains - Informatisation, Editions Eyrolles, 1988.

[Wintraecken, 1990] Wintraecken, J.J.V.R., The NIAM Information Analysis Method. Theory and practice. Kluwer Academic Publishers. Netherlands, ISBN 0-7923-0263-X, 1990

[Woltereck, 2001] Woltereck, M. Dynamic reliability analysis with quantification of epistemic uncertainty : A BWR application, Esrel 2001, pp1403-1410

[X60500, 1988] Norme AFNOR X60-500, Terminologie relative à la Fiabilité - Maintenabilité - Disponibilité, 1988

[Zaytoon, 2002] Zaytoon, J., Systèmes dynamiques hybrides, Traité IC2 série systèmes automatisés, Hermès, 2002

[Zwingelstein, 1996] Zwingelstein, G., La maintenance basée sur la fiabilité, guide pratique d'application de la RCM, Hermès, Paris, 1996

Publications majeures

Revues publiées ou acceptées

[Cauffriez, & al., 1995] Cauffriez, L., Defrenne, J. Viabilité de l'information et réseau à diffusion : deux atouts pour la prise de décision dans un système réparti de contrôle/commande tolérant les fautes. Revue Européenne de Sûreté de Fonctionnement et de Diagnostic, Vol 5/2, (pp. 219-247), Hermès. ISSN 1166-3049, 1995

[Cauffriez & al., 1997] Cauffriez, L., Willaeys, D., Defrenne, J., Mesure des indicateurs de performances de lignes de production : présentation d'une méthode et retour d'expérience. Journal Européen des systèmes Automatisés Vol. 31/8, (pp.1297-1310), Hermès. ISSN 0296-1598, Novembre, 1997

[Cauffriez & al., 2004] Cauffriez, L., Cicottelli, J., Conrard, B., Bayart, M., Design of intelligent distributed control systems: A Dependability point of view. Journal of Reliability Engineering and System Safety. pp.19-32.Vol 84/1, April, Elsevier. ISSN 0951-8320, 2004

[Cauffriez & al., 2005] Cauffriez, L., Willaeys, D. A predictive model for performance diagnosis of line production. IJAMT. The International Journal of Advanced Manufacturing Technology. Springer. Acceptée le 26 janvier 2005

[Cauffriez & al., 2005b] Cauffriez, L., Benard, V., Renaux, D. A new formalism for designing and specifying RAMS parameters for safe complex distributed control systems : the Safe-SADT formalism, IEEE Transactions on Reliability. Acceptée le 24 Août 2005

Revues soumises

[Cauffriez & al., 2003] Cauffriez, L., Willaeys, D. (Soumise en octobre 2003, révisée en septembre 2005 suite au reviewing). Towards a Predictive Model for Production Line Performance Diagnosis. Control Engineering Practice.

[Benard & al., 2005] Benard, V., Cauffriez, L., Renaux, D. (Soumise le 11 mai 2005) The Safe-SADT method for aiding designers to choose and improve dependable architectures for complex automated systems, Journal of Reliability Engineering and System Safety, Elsevier.

Ouvrage collectif

[Cauffriez & al., 1999c] Sous la direction de L. Cauffriez, Ciame, Tome 1 : Réseaux de terrain - Description et critères de choix. CIAME, 204 pages, Paris, Hermès. ISBN 286601-7242