Université Henri Poincaré Nancy 1

Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy

DFD Automatique et Production automatisée

Ecole Doctorale IAEM-Lorraine

CNRS UMR 7039

HABILITATION A DIRIGER DES RECHERCHES

Présentée par

Jean-Marc THIRIET

Ingénieur de l'Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy (ESSTIN)
Maître de Conférences à l'Université Henri Poincaré Nancy 1

Spécialité Automatique

SURETE DE FONCTIONNEMENT DE SYSTEMES D'AUTOMATISATION A INTELLIGENCE DISTRIBUEE

soutenue publiquement le 16 décembre 2004 devant la commission d'examen

Président :	Mireille BAYART Professeur à l'Université des Sciences et Technologies de Lille
Rapporteurs :	Guy JUANOLE Professeur à l'Université Paul Sabatier, Toulouse 3 Jean-Jacques LESAGE Professeur à l'Ecole Normale Supérieure de Cachan Daniel NOYES Professeur à l'Ecole Nationale d'Ingénieurs de Tarbes
Examinateurs :	Maria João MARTINS Professeur à l'Université Technique de Lisbonne (Portugal) Jean-François AUBRY Professeur à l'Institut National Polytechnique de Lorraine, Nancy Michel ROBERT Professeur à l'Université Henri Poincaré Nancy 1
Invité :	Joseph CICCOTELLI Directeur de Recherche, Docteur d'Etat, Institut National de Recherche et de Sécurité

SURETE DE FONCTIONNEMENT DE SYSTEMES D'AUTOMATISATION A INTELLIGENCE DISTRIBUEE

Ce mémoire est consacré à la modélisation et à l'évaluation des paramètres de sûreté de fonctionnement de systèmes d'automatisation à intelligence distribuée (SAID) ou systèmes commandés en réseau. Les systèmes d'automatisation à intelligence distribuée sont des systèmes qui sont composés de capteurs et actionneurs intelligents, architecturés autour d'un réseau de communication, typiquement un réseau de terrain. Les travaux développés traitent de l'évaluation de la sûreté de fonctionnement, notamment la fiabilité et la disponibilité de ces systèmes, en prenant en compte la normalisation. Cette approche s'applique à la fois à des grands systèmes et à des systèmes embarqués.
Dans le but de proposer une méthode pour d'aide à la conception des SAID, trois approches sont développées :
- une approche statique basée sur la topologie de l'architecture et traitant des fonctions à distribuer sur le SAID : diverses architectures sont évaluées, à l'aide notamment d'une extension des diagrammes de décision binaires,
- une approche temporelle ou dynamique mêlant les réseaux de Petri colorés à arcs probabilistes et les simulations de Monte-Carlo et permettant la prise en compte de l'évolution des modes de fonctionnement et états du système,
- une approche informationnelle, en cours de développement, par laquelle nous proposons d'aborder l'étude du SAID sous un autre angle, en nous affranchissant de l'architecture elle-même et en nous focalisant sur les informations circulant ainsi que leurs crédibilités.
Les autres aspects traités dans ce mémoire concernent l'évaluation du niveau de sécurité de réseaux de terrains de sécurité, ainsi que l'étude, en cours, d'une boucle de sécurité constituée d'instruments intelligents.

MOTS-CLEFS :
sûreté de fonctionnement – fiabilité – disponibilité – sécurité – système distribué – instrumentation intelligente – réseau de terrain – réseau de Petri stochastique – réseau de Petri coloré – diagramme de décision binaire – "*networked control system*" – système d'automatisation à intelligence distribuée – répartition de tâches – approche statique – approche dynamique – approche informationnelle

DEPENDABILITY OF INTELLIGENT DISTRIBUTED CONTROL SYSTEMS

This dissertation is dedicated to Intelligent Distributed Control Systems (IDCS) or Networked Control Systems (NCS). The IDCSs are systems composed of several smart or intelligent sensors or actuators distributed around a communication network, usually a Field Bus network. The dissertation deals with the dependability evaluation, mainly reliability and availability, of such systems. The work is done according to the standards. The purpose of the methodology is to be applied both on large-scale systems and embedded systems.
In order to propose a method for the design of IDCSs, three approaches are developed:
- a static approach based on the architecture topology and allowing distributing functions within the IDCS: various architectures are evaluated and compared, with the help of a binary decision diagram extension,
- a temporal or dynamic view based both on coloured Petri nets with probabilistic arcs and Monte-Carlo simulations: this method allows taking into account the system functioning modes and states evolution,
- an informational approach, presently in development, which allows studying IDCSs with another point of view: it is possible thanks to this method not to take into account the architecture and to focus on the actual information and its credibility.
The other aspects developed in this dissertation deal with the evaluation of the safety level of safe Field Buses and the study of an intelligent instruments-based safety loop.

KEYWORDS:
dependability – reliability – availability – safety – distributed system – smart, intelligent instrumentation – Field Bus network – stochastic Petri net – coloured Petri net – binary decision diagram – networked control system – intelligent distributed control system – task distribution – static approach – dynamical approach – informational approach

FUNKTIONSSICHERHEIT BEI AUTOMATISIERUNGSSYSTEMEN MIT VERTEILTER INTELLIGENZ

Die vorliegende Arbeit befasst sich mit der Modellierung und Evaluierung von Parametern zur Funktionssicherheit von Automatisierungssystemen mit verteilter Intelligenz (ASI), auch "Systeme mit netzbasierter Befehlsstruktur" genannt. Mit intelligenten Sensoren und Aktoren ausgestattet, werden ASI in Architekturen rund um ein Kommunikationsnetzwerk eingesetzt.
Die Arbeit beschäftigt sich mit der Evaluierung der Funktionssicherheit derartiger Systeme, insbesondere in Bezug auf Zuverlässigkeit und Verfügbarkeit und unter Berücksichtigung von Normalisierungsaspekten. Eine derartige Methode dürfte sowohl in großen stationären Anlagen, als auch in mobilen Bordsystemen Anwendung finden.
Mit dem Ziel, eine Methode zur Konzeptionsunterstützung von ASI vorzustellen, wurden drei Ansätze entwickelt:
- ein statischer Ansatz (architekturbasiert), welcher die über das ASI verteilten Funktionen untersucht: Evaluiert werden unterschiedliche Architekturen vor allem auf der Grundlage der erweiterten binären Entscheidungsdiagramme,
- ein zeitlicher Ansatz (dynamisch), welcher eine Mischung aus den gefärbten Petrinetzen mit statistisch gewichteten Zweigen und der Monte-Carlo-Simulationen darstellt. Dieser Ansatz berücksichtigt außerdem die zeitliche Entwicklung der Funktionsmodi und Systemzustände,
- ein informationeller Ansatz (derzeit noch in der Entwicklung), über den wir die ASI unter einem anderen Blickwinkel betrachten wollen. Dabei befreien wir uns von den Architekturaspekten und begrenzen uns auf die im System zirkulierenden Informationen sowie deren Glaubwürdigkeit.
Durchgeführt werden in dieser Arbeit ferner eine Evaluierung im Bereich der Sicherheit von ASI in sensiblen Bereichen, sowie eine noch laufende Studie zum Thema Sicherheitsschleifen, die aus intelligenten Instrumenten aufgebaut sind.

SCHLÜSSELWÖRTER:
Funktionssicherheit – Zuverlässigkeit – Verfügbarkeit – Sicherheit – verteiltes System – intelligente Instrumentierung – Bereichsnetz – statistisches Petrinetz – gefärbtes Petrinetz – binäre Entscheidungsdiagramme – "Networked Control System" – Automatisierungssystem mit verteilter Intelligenz – Aufgabenverteilung – statischer Ansatz – dynamischer Ansatz – informationeller Ansatz

SEGURIDAD DE FUNCIONAMIENTO DE SISTEMAS DE AUTOMATIZACIÓN CON INTELIGENCIA DISTRIBUIDA

Esta disertación está dedicada a la modelización y a la evaluación de los parametros de seguridad de funcionamiento de los sistemas de automatización con inteligencia distribuida (SAID), o "*networked control systems*". Los SAID se componen de captadores y actuadores inteligentes, distribuidos alrededor de una red de comunicación, clasicamente una red de terreno (*FieldBus*).
Los trabajos desarrollados tratan sobre la evaluación de la seguridad de funcionamiento, particularmente de la fiabilidad y de la disponibilidad, de este tipo de sistema, considerando la normalización. Estos métodos deben poder utilizarse tambien en grandes sistemas y en pequeños sistemas embarcados.
Con el fin de proponer un método por la concepción de los SAID, tres enfoques son desarrollados :
- un enfoque estática basado en la topología de la arquitectura y que trata de las funciones que deben distribuirse sobre el SAID: se evalúan distintas arquitecturas, con la ayuda, en particular, de extensiones de los diagramas de decisión binarios,
- un enfoque temporal, o dinámico, mezclando las redes de Petri coloreadas a arcos probabilistas y las simulaciones de Monte-Carlo, y permitiendo la consideración de la evolución de los modos de funcionamiento del sistema así como su estado,
- un enfoque informativo, en curso de desarrollo, por el cual proponemos abordar el estudio del SAID bajo otro ángulo, liberándonos de la arquitectura y concentrándonos en la información que circula así como su credibilidad.
Los otros aspectos tratados en esta disertación se refieren a la evaluación del nivel de seguridad de redes de terrenos de seguridad, así como el estudio, en curso, de un lazo de seguridad constituido de instrumentos inteligentes.

PALABRAS CLAVES :
seguridad de funcionamiento – fiabilidad – disponibilidad – seguridad – sistema distribuido – instrumentación inteligente – red de terreno – red de Petri estocástica – red de Petri coloreada – diagrama de decisión binario – "networked control system" – sistema de automatización con inteligencia distribuida – distribución de tareas – enfoque estática – enfoque dinámico – enfoque informativo

SEKURECO DE FUNKCIADO DE AŬTOMATAJ SISTEMOJ KUN DISPARTIGITA INTELIGENTECO

Tiu laboro estas ĉefe dediĉita al la modeligado kaj al la evoluo de la parametroj de funkciada sekureco de la sistemoj de aŭtomatigado kun distribuita inteligenteco, aŭ rete regitaj sistemoj. La sistemoj kun dispartigita inteligenteco estas sistemoj, kiuj konsistas el inteligentaj kaptiloj kaj inteligentaj ekfunciigiloj, distribuitaj en reto de komunikado, t.e./tipe laŭ reto de tereno (kampo). La laboroj klarigitaj pritraktas la taksadon de la funkciada sekureco, precipe la fidecon kaj la disponeblecon de tiu speco de sistemo, se oni konsideras la normigadon. Tia metodo povas esti aplikita samtempe al grandaj sistemoj kaj al eniŝipigitaj sistemoj.
Por proponi metodon por helpi la elpensadon de la SAID, tri eltraktadoj estas malvolvitaj :
- statika eltraktado bazita sur la arkitektura topologio kaj pritraktanta la funkciojn dispartigotajn al la SAID : diversaj arkitekturoj estas taksataj kun la helpo precipe de etendigo de la binaraj diagramoj de decidoj,
- tempa aŭ dinamika eltraktado, kiu unue miksas la retojn de Petri kolorigitaj kun probabl-arkoj kaj la simuladojn de *Monte Carlo*, kaj due, kiu ebligas la konsideradon de la evoluo de la modoj de funkciado de la sistemo same kiel ties staton,
- informada eltraktado disvolvifianta per kiu ni proponas ekstudi la SAID laŭ alia vidpunkto, liberigante nin de la arkitekturo mem kaj interesifiante pri la fluantaj informadoj kaj pri ties grado de kredindeco.
La aliaj aspektoj pritraktitaj en la memuaro rilatas la taksadon de la sekureca nivelo de retoj de sekurecaj terenoj (kampoj) same kiel la nuntempan studon de sekureca maŝo konsistanta el inteligentaj instrumentoj.

ĈEFVORTOJ :
funkciada sekureco – fideco – disponebleco – sekureco – distribuita sistemo – inteligenta instrumentado – reto de tereno/kampo – stokasta reto de Petri – kolorigita reto de Petri – binara diagramo de decido – « networked control system » – sistemo de aŭtomatigado kun distribuita inteligenteco – dispartigo de taskoj – statika eltraktado – dinamika eltraktado – informada eltraktado

Annick, Rémi, Léa

Mes parents

L'ambition nécessairement limitée de toute discipline scientifique l'oblige à définir dès le départ l'"univers" de son discours en précisant le domaine qu'elle s'efforce d'explorer et les méthodes qu'elle utilisera pour progresser : de quoi va-t-il être question ? Dans quel cadre les concepts utilisés dans les raisonnements sont-ils valables ? Quelles sont les définitions des paramètres introduits ? Par quels procédés d'observation ces paramètres sont-ils objets de mesure ? Comment les résultats théoriques obtenus sont-ils confrontés aux données fournies par le monde réel ? Ces précautions sont nécessaires pour que la réflexion scientifique nous permette de mieux discerner la réalité, de la décrire avec plus de précision, et peut-être un jour d'être capables de la modifier. Les oublier risque d'engager les raisonnements dans une impasse et de rendre impossibles les progrès de la compréhension et de l'action. (*De l'univers du discours, extrait de Albert Jacquard "La science à l'usage des non scientifiques"*)

L'ensemble des mathématiques auquel donne naissance le Calcul[1] incarne un mode de pensée flamboyant, tout à la fois hardi et spectaculaire, friand de grands gestes intellectuels et dans une large mesure indifférent à toute description détaillée du monde. C'est un style qui a façonné les sciences physiques mais non les sciences biologiques, et son succès en mécanique newtonienne, en relativité générale, et en mécanique quantique figure parmi les miracles de l'humanité. (*David Berlinski, "La vie des maths," p. 15*)

Il faut toujours se rappeler que, dans la prospection scientifique, les quelques pépites d'or de la vérité ne peuvent être obtenues qu'à force de lavages et de rejets incessants d'immenses quantités de cailloux et de sables inutiles. (*Bronislaw Malinowski*)

"Conversation was never begun at once, nor in a hurried manner. No one was quick with a question, no matter how important, and no one was pressed for an answer. A pause giving time for thought was the truly courteous way of beginning and conducting a conversation. Silence was meaningful with the Lakota, and his granting a space of silence to the speech-maker and his own moment of silence before talking was done in the practice of true politeness and regard for the rule that, “Thought comes before speech." (*"Native American Wisdom": Luther Standing Bear (1868?- 1939), Oglala Sioux Chef, pp.58-59*).

En 1843, **Fourier**, dans sa "théorie de l'unité universelle", annonçait l'apparition inévitable d'une nouvelle langue "digne d'une humanité unie et dans laquelle se trouverait incorporé le génie de toutes les nations" (*Georges Kersaudy, "Langues sans frontières", p. 251*)

[1] Calcul différentiel et intégral (*calculus* en anglais)

Avant-Propos

Remerciements

Avant d'aller plus avant dans le document, je souhaiterais remercier un certain nombre de personnes qui ont contribué, de près ou de loin et de manières très diverses, à différentes facettes de ce travail.

Concernant la **recherche** :

Tout d'abord je tiens à remercier très sincèrement et très chaleureusement Guy JUANOLE, qui a eu la double tâche d'officier d'abord en tant que rapporteur externe, nommé par le Conseil Scientifique de l'UHP (Université Henri Poincaré Nancy 1) pour accorder l'autorisation de soutenance à l'Habilitation à Diriger des Recherches, puis ensuite en tant que l'un des trois rapporteurs pour l'Habilitation à Diriger des Recherches elle–même : je tiens à dire que j'ai beaucoup apprécié les échanges téléphoniques et présentiel qui ont contribué à l'organisation actuelle du document.

Je souhaite remercier Jean-Jacques LESAGE, qui a sympathiquement accepté le travail de rapporteur. Il a également apporté un certain nombre de commentaires pertinents sur la manière d'appréhender l'exercice. Il a été un précieux conseiller.

Je voudrais remercier Daniel NOYES, qui a gentiment accepté d'être rapporteur et qui a apporté, par ses commentaires, un regard complémentaire permettant d'ouvrir la problématique. Je le remercie également pour les échanges téléphoniques et présentiel fructueux.

Je tiens à remercier très amicalement Maria João MARTINS*[2], avec qui nous travaillons intensément depuis sept ans sur les projets européens en Technologies de l'Information et de la Communication pour l'Enseignement (TICE). Je la remercie très chaleureusement d'être présente à ce jury.

Je voudrais amicalement et chaleureusement remercier Mireille BAYART*, avec qui nous travaillons activement dans le cadre du groupe de travail CIAME et de l'Action Spécifique. Je la remercie très vivement pour l'honneur qu'elle me fait d'avoir accepté d'être membre de ce jury. Je la remercie également pour les multiples discussions enrichissantes, notamment lors des réunions du groupe CIAME.

Je tiens à remercier Joseph CICCOTELLI*, avec lequel nous avons pu collaborer dans le cadre de travaux internes nancéiens ou de travaux au niveau du groupe national CIAME.

Je voudrais pouvoir remercier suffisamment Michel ROBERT*. Sans être 'flagorneur', pour reprendre une de ses épithètes préférées, il n'est pas facile pour moi de remercier Michel. Hormis des aspects d'amitié plus personnelle, je dois remercier Michel qui fut mon encadrant en thèse mais surtout je dois le remercier très vivement pour la confiance qu'il m'a accordée en 1994-95 en me donnant la possibilité d'orienter mes recherches, dans la poursuite des activités sur l'instrumentation intelligente, vers l'évaluation de systèmes d'automatisation à intelligence distribuée en intégrant les aspects de sûreté de fonctionnement. Il est en quelque sorte mon "père" scientifique. Je dois enfin le remercier très sincèrement pour la proposition qu'il m'a faite en 1996 de travailler avec lui sur les aspects liés à la prise en compte de la dimension européenne et de l'innovation pédagogique dans le cadre d'une activité européenne qui fut et demeure très riche et importante, pour moi.

[2] Dans cette partie, une étoile à côté d'un nom signifie que nous sommes co-auteurs d'au moins une communication.

Remerciements

Je le remercie pour cette confiance qui se traduit pour l'ensemble des dossiers recherche ou relations internationales que nous menons ensemble par un véritable fonctionnement en "binôme", où nous nous remplaçons mutuellement sans difficulté lorsque cela est nécessaire.

Je tiens à remercier très amicalement et chaleureusement Jean-François AUBRY*, avec qui j'ai commencé à travailler en 1999, en quelque sorte mon second père scientifique. Il me semble que nous nous sommes très rapidement accordés et que nous apprécions mutuellement de travailler ensemble. Je veux le remercier notamment pour l'apport scientifique significatif sur le thème de la sûreté de fonctionnement et les approches orientées information.

Je tiens à remercier très gentiment et sincèrement Claude HUMBERT* pour m'avoir fait confiance en me proposant un sujet de thèse, puis en ayant été ensuite mon directeur de thèse …

Naturellement, il est impératif mais c'est surtout un plaisir de remercier les cinq doctorants que j'ai eu ou ai le plaisir d'encadrer, Frédéric HERMANN*, Blaise CONRARD*, Pavol BARGER*, Abdelhak MKHIDA*, Rony GHOSTINE à qui je dois l'essentiel de ces travaux. Je remercie ici également Jana LIGUSOVA*, qui a travaillé trois mois avec nous, en 2003.

Je tiens à remercier très sincèrement Francis LEPAGE, Alain RICHARD, Thierry DIVOUX*, Gérard BLOCH* et Bernard HEIT. Je les remercie tous les cinq pour les discussions que nous avons pu avoir à différents moments, et je peux dire que je les considère à ce titre comme autant de mentors. Je remercie également très sincèrement Bernard pour la relecture de certaines parties du manuscrit.

Je remercie très amicalement Eric RONDEAU qui a accepté d'être rapporteur interne pour mon habilitation.

Je voudrais remercier Marc GABRIEL, avec lequel nous avons pu avoir des échanges fructueux à divers moments.

Je voudrais remercier également Françoise SIMONOT et Fabrice JUMEL*, pour la collaboration dans le cadre du groupe A, groupe de travail du contrat de plan Etat-Région.

Je remercie tout particulièrement les collègues du laboratoire, avec lesquels nous avons également pu avoir des discussions fructueuses mais également de bons moments de détente… : Frédérique BICKING*, Eric GNAEDINGER*, Eric LEVRAT, Gilles MILLERIOUX, Jean-Luc NOIZETTE*, Jean-Marie ORY, Jean Michel RIVIERE*, Christophe SIMON*, Marie-Christine SUHNER, Philippe WEBER. Je souhaite aussi remercier ici Didier THEILLIOL avec lequel nous coopérons de temps en temps, ainsi qu'Olaf MALASSE* avec lequel nous développons des activités de recherche communes.
Par ailleurs, je remercie Philippe THOMAS* (actuellement à l'UTBM) et Dimitri LEFEBVRE* (actuellement à l'Université du Havre) pour la coopération sur l'application de réseaux de neurones pour le traitement de données de trafic urbain. Je remercie également Philippe CHARPENTIER de l'INRS pour les collaborations communes.

En ce qui concerne **l'enseignement**, je tiens à remercier l'ensemble de mes collègues du département Génie des Télécommunications et Réseaux avec lesquels il fait bon travailler. Je souhaiterais citer en particulier Marie-Laure BESSON* et Didier FRADET pour le travail sur l'enseignement de Java, Hugues GARNIER* pour l'ensemble du travail commun sur le traitement du signal, Jean-Marie MOUREAUX pour l'informatique industrielle et tout le reste…
Je souhaite ici remercier très amicalement et chaleureusement Dominique RICHIER, avec lequel nous collaborons en informatique industrielle depuis de nombreuses années, et qui a également souhaité

reprendre la gestion des stages industriels des étudiants ; nous avons eu également un certain nombre de discussions très fructueuses et c'est pour moi toujours un plaisir de le retrouver.
Je remercie très chaleureusement Bénédicte FRANOUX, avec qui nous coopérons de manière sympathique pour les stages et autres activités.
Je tiens également et de manière appuyée à remercier ici Madeleine MANN qui est une collaboratrice hors pair, en particulier avec laquelle il m'est sympathique de coopérer notamment lorsque je gère les stages et qui a aussi, toujours avec beaucoup de gentillesse, émis chaque année un certain nombre d'ordres de mission …

Concernant les travaux liés aux **relations internationales et aux technologies de l'information et la communication pour l'enseignement (TICE)**, je dois remercier l'ensemble des partenaires impliqués dans les réseaux thématiques INEIT-MUCON puis THEIERE, je souhaiterais nommer en particulier les personnes suivantes : Pentti LAPPALAINEN* (Oulun Yliopisto / Université d'Oulu, Finlande), Maria João MARTINS* (Instituto Superior Técnico, Lisboa / Institut Supérieur Technique de Lisbonne, Portugal), Michael HOFFMANN* (Universität Ulm / Université de Ulm, Allemagne), Jan LIGUS (Technická univerzita Košice / Université Technique de Košice, Slovaquie).
Je tiens enfin à remercier amicalement et très chaleureusement Olivier BONNAUD*, de l'Université de Rennes 1, avec lequel nous avons pu passer de multiples moments de travail, de discussion et de détente dans divers endroits d'Europe, à chaque fois avec un plaisir renouvelé.

Pour tout le travail mené au sein de la Commission des Relations Internationales du Club EEA, je tiens à remercier l'ensemble des collègues, partenaires actifs de ce groupe de travail très sympathique. Je souhaiterais remercier en particulier les deux présidents avec lesquels il a fait et fait très bon travailler, Ludovic PROTIN (Université du Havre) et Bernard de FORNEL* (Institut National Polytechnique de Toulouse). Je tiens également à remercier en particulier Georges ZISSIS* (Université Paul Sabatier, Toulouse), Abdelaziz BENSRHAIR (Institut National des Sciences Appliquées, Rouen, actuel président de la Commission), Hamed YAHOUI* (Université Claude Bernard, Lyon 1) et Hélène FREMONT* (Université de Bordeaux 1) avec lesquels j'ai plus particulièrement été amené à travailler, à chaque fois avec sympathie et amitié.
Plus localement, je tiens à remercier Françoise CLERC avec qui je coopère en relations internationales à l'ESSTIN et qui accepte gentiment chaque année de donner des cours de français aux étudiants étrangers qui travaillent avec nous.
Je voudrais très sincèrement et personnellement remercier Corinne HUMBERT qui est une collaboratrice efficace et patiente pour la gestion des réseaux thématiques, ce qui n'est pas une tâche facile, mais qu'elle accomplit toujours avec le sourire.

Dans une rubrique particulière, je vais enfin remercier de tout cœur et amicalement Pascal GEND*, avec qui je collabore depuis près de six ans maintenant : nous avons mené ensemble plusieurs projets dans le cadre des nouvelles technologies pour la pédagogie et mis en place divers outils dans le cadre de l'organisation de conférences…

Je voudrais remercier Pierre IVANOVITZ, agent comptable de l'UHP, qui a toujours une solution lorsque nous sommes confrontés à un problème administratif ou financier, notamment vis-à-vis d'étudiants étrangers.

Mes remerciements vont également, à divers égards à Thierry DALSTEIN, David DEHLINGER, Stéphane DUGRAVOT, Guillaume FERRY, Patrick GAY, Geneviève RITTY, Christine JACQUE, Florence L'HOTE, Fabrice MALGLAIVE, Virginie MASSEL, Dominique MASSENOT, Claudie MATHIS, Hervé ORTEGA, Danièle SAXE, Jean-Claude TOUSSAINT, Sylvie VARLET, et toutes les autres personnes que j'aurais oubliées… toujours présentes pour nous rendre le travail plus agréable ou simplement possible…

Remerciements

Je remercie très amicalement Michael HOFFMANN pour la traduction allemande et Thierry SALADIN pour l'aide pour la traduction Esperanto sdu résumé.

Je voudrais enfin remercier ici Annick et Claudy DEMONGEOT pour les relectures du manuscrit.

Pour terminer, je remercie du fond du cœur Annick, Rémi et Léa, ainsi que mes parents.

SOMMAIRE

2ème PARTIE : PRESENTATION DES ACTIVITES DE RECHERCHE

Liste des abréviations

A3SI	Automatique et Simulation pour la Sécurité des Systèmes Industriels
AMDE	Analyse des Modes de Défaillance et de leurs Effets
AMDEC	Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
APD	Analyse Préliminaire des Dangers
API	Automate Programmable Industriel
AS-i	*Actuator – Sensor Interface* (réseau de terrain)
AS-i Safety at Work : extension de sécurité du réseau AS-i	
BDF	Blocs Diagrammes de Fiabilité
CAI	Composant d'Automatisme Intelligent
CAN	*Controller Area Network* (réseau de terrain)
CERTU	Centre d'Etudes sur les Réseaux, les Transports, l'Urbanisme et les constructions publiques (Ministère des Transports)
CGI	*Common Gateway Interface*
CIAME	Constituants Intelligents pour l'Automatisation et la Mesure (Groupe de travail SEE 18.04)
COTS	*Commercial Off-The Shelf Software* (brique logicielle sur étagère)
CPER	Contrat de Plan Etat-Région Lorraine
CPN	*Colored Petri Nets* (réseau de Petri coloré)
CRAN	Centre de Recherche en Automatique de Nancy
CSMA/CD	*Carrier Sense Multiple Access* / *Collisions Detection*
CSSF	Conception des Systèmes sûrs de Fonctionnement
DCS	*Discrete Control System* / Système de Commande discret/numérique ou *Distributed Control System* / Système d'Automatisation Distribué
DF	Diagramme fondamental
EAEEIE	*European Association for Education in Electrical and Information Engineering* (www.eaeeie.org)
EIE	*Electrical and Information Engineering*, équivalent français : Génie Electrique et STIC
ESSTIN	Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy
FIP	Flux Information Protocole ou *Factory Instrumentation Protocol*
FMDS	Fiabilité Maintenabilité Disponibilité Sécurité, *RAMS* en anglais
GTR	Génie des Télécommunications et Réseaux
HTML	*HyperText Mark-Up Language*
INEIT-MUCON	*Innovation for Education in Information Technology through Multimedia and Communication Networks* (www.eaeeie.org/ineit-mucon)
INERIS	Institut National de l'Environnement Industriel et des Risques
INPL	Institut National Polytechnique de Lorraine
INRS	Institut National de Recherche et de Sécurité
IUT	Institut Universitaire de Technologie
IUP	Institut Universitaire Professionalisé
LMD	Licence – Master – Doctorat (processus de Bologne)
MdC	Maître de Conférences
MDT	*Mean down time* (temps moyen d'indisponibilité)
ML	Langage de programmation ML standard [ULL 98]
MTBF	*Mean Time Between Failure* (temps moyen entre défaillance)
MTTF	*Mean Time To Repair* (temps moyen de remise en état)
MUT	*Mean up time* (temps moyen de disponibilité)
NCS	*Networked Control System*, voir aussi SAR
NTE	Nouvelles Technologies Educatives
Occ. Graphe	Graphe d'occurrence
OSA-TESMA	*Open System Architecture for Telematic Services in Municipal Applications*
OSI	*Open System Interconnection*
PCRD	Programme Cadre de Recherche et Développement (Union Européenne)

PFD	*Probability of Failure on Demand* / probabilité de défaillance sur sollicitation
PID	Correcteur Proportionnel Intégral Dérivé
PTP	Processus Thermique Pilote
QdS	Qualité de Service
RAMS	*Reliability Maintainability Availability Safety*, FMDS en français
RNIS	Réseau Numérique à Intégration de Service
ROM	*Read Only Memory*
RdP	Réseaux de Petri
RTC	Réseau Téléphonique Commuté
RTP	Réseau Thématique Pluridisciplinaire
SACSS	Systèmes Automatisés Contraints par la Sûreté de fonctionnement et la Sécurité
SADT	*Structure Analysis and Design Technique*
SAID	Système d'Automatisation à Intelligence Distribuée
SAP	Système Automatisé de Production
SAPID	Système Automatisé de Production à Intelligence Distribuée
SAR	Système d'Automatisation à Réseau (ou système d'automatisation via les réseaux), *NCS* en anglais
SART	*Structured Analysis for Real Time*
SdF	Sûreté de Fonctionnement
SDL	*Specification and Description Language*
SEE	Société de l'Electricité, de l'Electronique, et des Technologies de l'Information et de la Communication
SIL	*Safety Integrated Level*
SNMP	*Simple Network Management Protocol*
STIC	Sciences et Technologies de l'Information et de la Communication
SYDER	Systèmes distribués et embarqués réactifs aux fautes
TCP/IP	*Transmission Control Protocol/ Internet Protocol*
T_e, T_s	Période d'échantillonnage (*sampling period*)
THEIERE	*Thematic Harmonisation in Electrical and Information EngineeRing in Europe* (www.eaeeie.org/theiere)
TICE	Technologies de l'Information et de la Communication pour l'Enseignement
TNPN	*Thematic network programme networking* (http://cranmmx.esstin.u-nancy.fr/tnpn/tnpnt)
TTA	*Time-Triggered Architectures*
UHP	Université Henri Poincaré Nancy 1
XML	*Extensible Markup Language*, ou Langage Extensible de Balisage

Curriculum Vitae

1. Etat civil

Nom patronyme : **THIRIET** Prénoms : Jean-Marc Raymond André

Age : 42 ans Date et lieu de naissance : 21 février 1962 à Montbéliard (25)

Nationalité : Française

Adresses

Recherche	Enseignement
CRAN ESSTIN 2, rue Jean Lamour 54 519 Vandœuvre les Nancy cedex Tél.: 03.83.68.51.31	Institut Universitaire de Technologie de Nancy-Brabois (dépt. GTR) Le Montet 54 601 Villers les Nancy cedex Tél : 03.83.68.25.40
Courrier électronique : jean-marc.thiriet@esstin.uhp-nancy.fr, jean-marc.thiriet@iutnb.uhp-nancy.fr http://esstin.uhp-nancy.fr/~thiriet/	

Situation de famille : vivant maritalement.

Nombre d'enfants : 2 à charge.

Service national effectué (1987/88). Durée du service effectué : 12 mois

2. Cursus universitaire

1993	**Doctorat** en Automatique *mention Très Honorable et Félicitations* Université Henri Poincaré Nancy 1
1989	**DEA** Métrologie Automatique Electrotechnique *mention A-B* Université Henri Poincaré Nancy 1
1989	**Diplôme Ingénieur ESSTIN en Automatique** Université Henri Poincaré Nancy 1
1988	**DEUG Anglais** Université de Nancy II *(pendant le service national)*
1982	**B.T.S. Mécanique-Automatismes** Lycée d'Enseignement Technologique de Colmar
1980	**Baccalauréat de Technicien série F1** Lycée d'Enseignement technologique Viette de Montbéliard

3. Thèse & DEA

Ma formation par la recherche a commencé en 1988 lorsque j'ai intégré l'équipe d'Automatique et de Recherche Appliquée du Centre de Recherche en Automatique de Nancy (CRAN, CNRS URA n° 821 à cette époque, actuellement UMR 7039).

Durant l'année 1988-89, j'ai préparé mon D.E.A. sur le thème de l'Enseignement Assisté par Ordinateur et la Prévention à la Sécurité en collaboration avec l'I.N.R.S. (Institut National de Recherche et de Sécurité).

La partie pratique du DEA a consisté en la mise au point d'un logiciel qui soit un outil pédagogique pour la conception des circuits électromagnétiques à relais. Le logiciel, développé en Prolog, permettait la simulation des circuits ainsi que de certaines anomalies (court-circuit, coupure électrique, blocage d'une bobine...) [*DE89a*].

L'étude bibliographique associée était consacrée à l'Enseignement Assisté par Ordinateur en général [*DE89b*].

En décembre 1989, j'ai commencé une thèse [*TH93*] de l'Université de Nancy I (aujourd'hui Université Henri Poincaré Nancy 1) sous la direction du Pr. Claude HUMBERT et de Michel ROBERT sur les problèmes de trafic

urbain. La thèse s'est déroulée dans le cadre d'une convention avec la Ville de Nancy et a été soutenue le 5 février 1993.

Les résultats de cette recherche sont :

1) une étude de la situation de la régulation du trafic urbain dans le monde
Ce travail a consisté en une classification des stratégies de macro-régulation utilisées en régulation de trafic urbain. Diverses réflexions ont ensuite été développées et ont amené une proposition de système futur qui pourrait intégrer les fonctions de régulation, de guidage et de localisation de véhicules. Les résultats de ces recherches ont fait l'objet de la publication d'un rapport diffusé par l'ILGU (Institut Lorrain du Génie Urbain) [*Rc92b*] et d'un article publié dans la revue Transports Environnement Circulation [*RN91*].

Nous avons ensuite mis en œuvre la méthode SADT (Structured Analysis and Design Technics - IDEF0) pour effectuer une comparaison des fonctions d'un système de régulation de trafic avec un gardien de la paix qui régule la circulation dans un carrefour. L'objectif était de mettre en évidence les insuffisances respectives des deux "systèmes" [*CI93a*].

2) la détection d'anomalies dans le trafic urbain et la détermination de leurs causes
Deux démarches ont été adoptées parallèlement pour modéliser l'apparition d'une anomalie.

La première démarche est basée sur l'étude des variables macroscopiques, essentiellement les débits et propose un modèle qui estime les débits sortants du carrefour en fonction des entrées. Différents modèles ont été testés : régression pas à pas, ARX, famille PEM, réseaux neuronaux et un modèle de connaissance dérivé de la théorie des files d'attente. Leurs avantages et inconvénients sont analysés dans une hypothèse de détection et d'analyse d'anomalies en temps réel.

La seconde démarche observe le trafic à travers une fenêtre "stroboscopique" synchronisée sur l'évolution des cycles et des phases des feux tricolores. Elle peut être assimilée à une "déconvolution" des variables macroscopiques qui conduit à appréhender les paramètres microscopiques représentatifs du comportement des usagers. Nous montrons qu'il est possible par cette méthode d'analyser les anomalies en déterminant leur début, leur fin et par conséquent leur durée [*CI93b*] [*Rc92a*] [*CI92b*].

Doctorat de l'Université Henri Poincaré Nancy 1 en automatique.

- Titre "Contribution à la détection et à l'analyse d'anomalies de trafic en milieu urbain - regards sur l'existant en régulation du trafic urbain" (soutenue le 5 février 1993 à Nancy, directeurs de thèse : Claude HUMBERT & Michel ROBERT).

  Composition du jury : Président Claude HUMBERT (Professeur à l'ESSTIN/UHP), Rapporteur 1 : Jean LATERRASSE (Directeur de Recherche au C.N.R.S. à l'E.N.P.C. (Ecole Nationale des Ponts et Chaussées)), Rapporteur 2 : Gérard METZGER (Professeur à l'Université de Haute-Alsace), Michel ROBERT (Professeur à l'ESSTIN/UHP), Peter HÄCKELMANN (Docteur-Ingénieur au Stadtplanungsamt de Saarbrücken en Allemagne), Jean-Jacques DAVAINE (Ingénieur à la Communauté Urbaine du Grand Nancy/Directeur de l'I.L.G.U. (Institut Lorrain du Génie Urbain)).
  MENTION très honorable avec les félicitations du jury

4. Statut actuel

Grade : Maître de Conférences classe normale, 6ème échelon. Section : 61

Intitulé de la section : génie informatique, automatique et traitement du signal

Emploi : n° 6100 MCF 1198

Intitulé : Université Henri Poincaré Nancy 1 - U.F.R. : I.U.T. de Nancy-Brabois

Ancienneté : 12ème année Maître de Conférences (2004-2005) + 1 an ATER (demi poste) + 3 ans AER

Ancienneté de grade : titularisé le 1/9/94 comme Maître de Conférences 2ème Classe (nomination 1/9/93).
1ère Classe le 1/9/96.
Classe normale depuis le 1er juin 2001, 6ème échelon au 1er mai 2002.

Laboratoire : **CRAN** (Centre de Recherche en Automatique de Nancy, CNRS UMR 7039) :

- Groupe Thématique SURFDIAG (*Sûreté de Fonctionnement et Diagnostic*) à partir du 1er janvier 2005.
- Thème *Conception des Systèmes Sûrs de Fonctionnement* de 1999 à 2004.
- Equipe *Instrumentation Intelligente* jusqu'en 1999.

5. Emplois antérieurs

Dans l'enseignement supérieur

- 1992-93 : Attaché Temporaire d'Enseignement et de Recherche à l'ESSTIN (Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy) dépendant de l'Université Henri Poincaré Nancy 1 d'octobre 1992 à août 1993 (poste n° 61 ATER 1156).
- De 1989-90 à 91-92 : Allocataire d'Enseignement et de Recherche à l'ESSTIN/UHP d'octobre 1989 à septembre 1992 (poste n° 272 ALER 8010).
- Vacations à l'Université Henri Poincaré Nancy 1/ESSTIN de janvier à juin 87 : insertion d'un groupe d'étudiants indonésiens dans le système universitaire français.

Hors enseignement supérieur

- Vacations à l'INRS - Neuves-Maisons : environ 4 heures par semaine hors vacances universitaires entre décembre 1989 et décembre 1993 pour l'animation d'un club informatique orienté initiation, perfectionnement et jeux
- INRS : participation à quelques stages de formation et universités d'été dans la période 1989-93
- Automobiles Peugeot Sochaux "scolaire-ouvrier" de juin à septembre 87
- Automobiles Peugeot Vesoul "scolaire-ouvrier" de août à septembre 86
- CE Peugeot "personnel de service" en juillet 86 au Centre de vacances de Chamblay (39)
- CE Peugeot "personnel de service" en août 85 au Centre de vacances de Bussang (88)
- Automobiles Peugeot Sochaux "scolaire-ouvrier" de juin à septembre 83
- Vendanges 82 "Maurice Ecart - Savigny les Beaune"
- Automobiles Peugeot Sochaux "scolaire-ouvrier" de juin à septembre 82
- Animateur de centres aérés "FRANCA" à Valentigney (25) en 1979-80
- Manœuvre à la Ville de Valentigney (25) deux semaines en 1979
- Manœuvre à la Ville de Valentigney (25) deux semaines en 1978

6. Langues Etrangères

- Anglais "britannique" ou "américain" : lu, écrit, parlé. En possession d'un DEUG d'Anglais obtenu en 1988 par l'Université de Nancy II.
- Anglais "véhiculaire européen" : courant.
- Espagnol : lu, écrit. Niveau 4 du CNED (Centre National d'Enseignement à Distance de Vanves) d'"Espagnol industriel" suivi et validé en 1988/89.
- Niveau initiation en Allemand (collège), Portugais (1984), Chinois (1994) et Espéranto (1997).
- Acquisition de deux modules de Français Langue Etrangère (niveau licence de langues) en 1994.

7. Liste des références bibliographiques

La liste des références bibliographiques se trouve dans l'annexe B du présent document.

Introduction

Le développement des technologies numériques lors de la dernière décennie du vingtième siècle a entraîné la diffusion d'une part des processeurs de calcul et d'autre part des réseaux de communication.

La mise à disposition de ces technologies a permis le développement de l'**instrumentation intelligente**, capteurs ou actionneurs dotés de capacités de traitements numériques et d'une interface de communication. A partir d'une (ou plusieurs) mesure(s) effectuée(s) par un ou des transducteurs, l'objectif d'un capteur intelligent est d'obtenir une mesure opérationnelle validée. Celle-ci est dotée d'un certain intervalle de confiance combiné à une information concernant l'état de bon fonctionnement ou non de l'instrument. Ces possibilités ont été rendues possibles car l'instrument est capable d'effectuer localement des calculs plus ou moins complexes (de type redondance analytique par exemple) et de traiter plusieurs transducteurs physiques (redondance matérielle).

Par ailleurs, le fait de corréler ces informations locales à des informations complémentaires provenant de l'environnement, notamment grâce à l'interface de communication bidirectionnelle, permet de rendre plus robuste l'opération de validation.

Dans cette mouvance, j'ai contribué à participer à la définition d'un modèle informel de capteur intelligent dans le cadre des travaux de l'équipe et plus particulièrement, dans la suite de mes travaux de thèse, j'ai travaillé à la définition d'un capteur intelligent de trafic.

Le **réseau de communication** est devenu un moyen de communication bidirectionnel entre les divers composants constitutifs d'un système d'automatisation, ce qui n'était pas possible avec la traditionnelle ligne 4-20 mA. J'ai mené depuis quelques années des recherches sur l'utilisation de réseaux de terrain pour des architectures distribuées. Les aspects importants à prendre en compte sont d'une part l'aspect temps réel, développé par ailleurs dans plusieurs équipes au niveau national et international, et d'autre part les aspects sûreté de fonctionnement, qui deviennent fondamentaux pour les systèmes embarqués ou les systèmes complexes.

Divers travaux au niveau local ou dans le cadre du groupe national CIAME (Constituants Intelligents pour l'Automatisation et la Mesure (Groupe de travail SEE 18.04)) ont pu mettre en exergue un certain nombre de caractéristiques à prendre en compte pour soit évaluer le niveau de sûreté de fonctionnement du "système" de communication soit préciser les critères à évaluer pour qu'un réseau de terrain puisse être considéré comme un réseau de sécurité.

A partir de 1995, j'ai pris en charge au sein de l'équipe de recherche un axe concerné par les "**systèmes d'automatisation à intelligence distribuée**" (SAID), systèmes constitués de divers composants, dotés de capacités de calculs numériques, et distribués autour d'un réseau de communication. Il nous est apparu notamment que l'existence d'une intelligence distribuée devait nous permettre d'envisager une meilleure adaptation du système à son environnement, y compris en terme de sûreté de fonctionnement.

L'approche suivie est une approche ascendante partant du composant le plus bas, l'instrument intelligent, pour remonter vers une vision plus globale, le système d'automatisation à intelligence distribuée (SAID, puis systèmes commandés via des réseaux, NCS, "*Networked Control Systems*"). Le but est de faire collaborer tous ces composants intelligents pour que l'"intelligence" obtenue globalement soit supérieure à la somme des intelligences des composants constitutifs. Un des aspects qui nous intéresse depuis 1994 environ est la conséquence de l'utilisation d'architectures distribuées sur la sûreté de fonctionnement[3] des systèmes.

L'utilisation des systèmes numériques de calcul et de communication pose en effet un certain nombre de défis :
- la quantification de la sûreté d'une implantation logicielle sur un composant électronique numérique,
- la mise en place de méthodes d'évaluation permettant la prise en compte de ces aspects,

[3] Nous entendons par sûreté de fonctionnement (*dependability*) essentiellement la fiabilité et la disponibilité des systèmes. Dans une certaine mesure, nous nous intéressons également aux aspects sécurité (aux sens sécurité machine et environnement, tels qu'ils peuvent être employés par des organismes comme l'INRS ou l'INERIS). Il s'agit bien ici de la sécurité – innocuité (*safety* en anglais), au sens où il s'agit de se protéger vis-à-vis de défaillances catastrophiques, et non pas de la sécurité – intégrité (*security* en anglais).

- l'évaluation de la coopération de l'intelligence disponible un peu partout dans le système.

Cette idée a motivé nos recherches durant ces années et la démarche suivie consiste en la formalisation de ces systèmes à l'interface entre l'automatique traditionnelle et les réseaux de communication, support autour duquel s'architecturent les SAID. Nous avons notamment proposé des modèles fonctionnels de SAID, combinés à une étude des flux d'information, afin d'obtenir une liste de tâches élémentaires à implanter sur l'architecture opérationnelle. Nous avons ensuite mis en évidence les contraintes d'implantation avant de trouver, par des méthodes d'optimisation, la répartition la meilleure au sens du coût d'utilisation globale du système.

La **sûreté de fonctionnement** des SAID est un sujet délicat, à la fois sur le plan scientifique et sur le plan sociétal. Evaluer la sûreté consiste à donner une valeur permettant de quantifier le niveau de risque associé à l'utilisation d'une telle architecture en fonction de la mission qu'elle doit accomplir. Ce niveau de risque est caractérisé par la conséquence sur l'environnement humain ou matériel de situations dangereuses, ainsi que par la probabilité ou possibilité d'occurrence d'une telle situation.

Sur le plan sociétal, les systèmes automatisés ou informatisés sont présents partout. Les systèmes embarqués envahissent le quotidien : téléphones portables, jouets. Des systèmes plus complexes sont également présents avec de plus en plus d'informatique ou d'électronique numérique (automobile, électro-ménager), y compris pour des fonctions critiques comme c'est le cas généralement dans les transports.

Sur le plan scientifique, il nous faut trouver des méthodes permettant d'envisager les situations possibles, de les analyser et de quantifier leur niveau de sûreté. Puisque le travail a pour objet les systèmes d'automatisation à intelligence distribuée, systèmes d'automatisation intégrant des réseaux de communication, il nous faut envisager des méthodes permettant de représenter les diverses fonctions d'un SAID et capables de modéliser les divers comportements possibles.

Je propose donc dans ce mémoire d'habilitation de décrire les activités que j'ai menées dans ce but les années passées et propose un projet de recherche pour l'avenir, afin d'apporter une contribution à ces questions.

Depuis la soutenance de ma thèse, je poursuis mes activités de recherche au sein du CRAN (Centre de Recherche en Automatique de Nancy / CNRS UMR n° 7039), laboratoire dirigé actuellement par le Pr. Francis LEPAGE.

Durant la période 1993-1999, mes travaux de recherche se sont déroulés au sein de l'équipe "Instrumentation Intelligente" animée par le Pr. Michel ROBERT. Ces travaux concernaient généralement la recherche dite méthodologique, quelquefois technologique.

En 1999, le CRAN a été réorganisé dans le cadre de six thèmes de recherche pour la période 2000-2004. Mes travaux se sont naturellement intégrés dans l'action devenue ensuite le projet "Impact de la sûreté de fonctionnement dans la spécification, l'évaluation et le développement des systèmes automatisés" animé par le Pr. Jean-François AUBRY, au sein du thème "Conception des Systèmes sûrs de Fonctionnement".

Dans la structure proposée pour la période 2005-2008, mes travaux se dérouleront dans l'équipe-projet SACSS "Systèmes Automatisés Contraints par la Sûreté de fonctionnement et la Sécurité", animée par le Pr. Jean-François AUBRY. Ce projet est inscrit dans le groupe thématique "Sûreté de Fonctionnement et Diagnostic", sous la direction du Pr. Didier MAQUIN. Je participerai également à l'équipe-projet SYDER (Systèmes distribués et embarqués réactifs aux fautes), animé par le Pr. Dominique SAUTER, dans ce même groupe thématique.

Le travail que nous menons s'inscrit dans la stratégie du CNRS, à l'interface entre les RTP 20 (Fiabilité, diagnostic et tolérance aux fautes des systèmes complexes), 21 (Sûreté de fonctionnement des systèmes informatiques complexes ouverts) et 55 (Systèmes de Contrôle-commande et Réseaux de Communication).

Ce travail trouve des applications au sein du Contrat de Plan Etat-Région des universités lorraines, dans le PRST "Sûreté Industrielle et Déchets", projet "Automatisation et Prévention des Risques".

Ce mémoire propose enfin des axes pour un projet de recherche autour de l'évaluation de la sûreté de fonctionnement des systèmes enfouis ou systèmes complexes intégrant de l'intelligence distribuée et des réseaux de communication. Il est organisé en deux parties.

La **première partie** récapitule l'ensemble des activités menées en enseignement, en relations internationales et en recherche ; cette partie comprend les chapitres 1 à 3.

Le **chapitre 1** présente, sous forme de bilan assez classique, un résumé des enseignements (cf. figure 1) que j'ai dispensés depuis que je suis maître de conférences ainsi que les encadrements de projets-ingénieurs. Les activités administratives sont rappelées : en ce qui me concerne il s'agit surtout de la fonction de responsable des stages assurée pendant plusieurs années au département Génie des Télécommunications et Réseaux (GTR) de l'IUT de Nancy-Brabois.

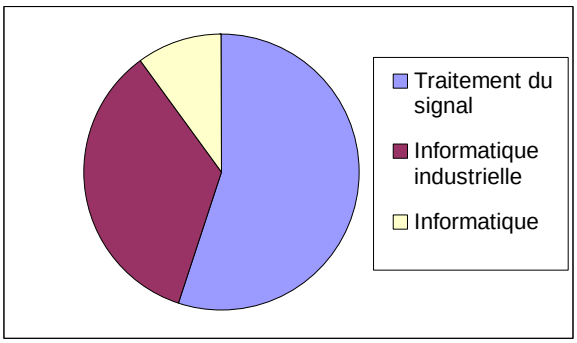


Figure 1 – Répartition des enseignements

Cette partie propose également la liste des implications administratives relatives à l'enseignement ou à la vie de nos structures universitaires.

Le **chapitre 2** effectue la synthèse d'une activité en relations internationales qui a été importante depuis fin 1996. Cette activité concerne deux points principaux :
- Depuis 1997, une première action concernant l'utilisation des TICE pour l'enseignement dans un cadre européen ; il s'agissait d'effectuer une veille sur l'évolution des technologies disponibles pour développer des enseignements accessibles par l'internet. Ceci nous a permis notamment de proposer un certain nombre de projets d'étudiants au département GTR, mais aussi à l'ESSTIN ou à l'IUP/GEII, pour la mise en forme de sites internet pédagogiques et le développement d'applets Java ou Multimédia de simulation/démonstration pédagogique.
- Depuis 2001, une seconde action relative à une réflexion approfondie sur l'implantation du LMD (licence, master, doctorat, processus de Bologne) dans les disciplines de l'EIE (*Electrical and Information Engineering*) dans un cadre européen.

Nous avons également participé au projet de développement d'un système d'information pour l'ensemble du programme de réseaux thématiques SOCRATES 1.
Ce chapitre contient un tableau récapitulatif des implications liées à ce domaine, notamment pour les aspects "gestion de projet" et participation à l'organisation de conférences.
Bien que nous soyons ici dans le cadre d'une habilitation à diriger des recherches, nous avons souhaité développer sur quatre pages ces aspects…

Le **chapitre 3** présente les co-encadrements doctoraux et autres co-encadrements, ainsi que plus généralement les implications liées à la recherche.

La **seconde partie** décrit ma contribution. Cette partie se compose des chapitres 4 à 7. Le chapitre 4 présente le contexte du travail, le fil conducteur envisagé concernant la problématique de l'évaluation de la sûreté de fonctionnement de systèmes d'automatisation à intelligence distribuée. Le chapitre 5 décrit synthétiquement un certain nombre d'actions ou de collaborations industrielles soit sur le thème de l'instrumentation intelligente soit sur le thème des réseaux de terrain ou réseaux de sécurité. Le chapitre 6 constitue le cœur de l'habilitation, autour principalement des thèses co-encadrées de Frédéric HERMANN, Blaise CONRARD et Pavol BARGER, pour la mise en place de méthodes d'évaluation du niveau de sûreté de fonctionnement de SAID. Le chapitre 7 est un projet de recherche pour les années prochaines.

Le **chapitre 4** introduit tout d'abord la notion de SAID (Système d'Automatisation à Intelligence Distribuée).

Ensuite sont abordées les notions de sûreté de fonctionnement d'abord de manière classique puis de plus en plus appliquées à notre problématique, les SAID, en mettant l'accent sur les composants de base de ces SAID : les instruments intelligents et les réseaux de communication.

Après avoir étudié les divers composants des SAID, il nous faut envisager l'agrégation ou intégration de ceux-ci pour former le système distribué et envisager l'évaluation de celui-ci comme un tout…

Par ailleurs, ce chapitre 4 propose une présentation de l'environnement de recherche, aux niveaux nationaux et internationaux.

Le **chapitre 5** présente le bilan d'activités menées dans la suite de la thèse et liées au développement de l'instrumentation intelligente. Dans la mouvance des travaux de l'équipe sur ce sujet, j'ai plus particulièrement contribué à la définition d'un capteur intelligent pour la mesure du trafic urbain.

Ce chapitre propose également une contribution à l'évaluation de la sûreté de fonctionnement de la fonction communication, élément central des SAID, ainsi qu'à l'étude des paramètres des réseaux de communication sur lesquels il est possible d'agir afin d'améliorer la sûreté de fonctionnement. Sont abordés dans ce chapitre les notions de temps réel et de déterminisme.

Ce chapitre présente également une contribution à la définition d'un système d'information pour les communautés urbaines, dans le cadre d'un projet du 4ème PCRD (Programme Cadre de Recherche et de Développement de l'Union Européenne).

Le **chapitre 6** traite de l'évaluation de la sûreté de fonctionnement des SAID.
Dans une première approche, nous envisageons l'étude des SAID en considérant leurs composants : les capteurs, les actionneurs, les unités de traitement et les réseaux de communication. Nous proposons une étude fonctionnelle de l'architecture conduisant à la décomposition de ces fonctions comme autant de tâches. Sous les contraintes de préférence et d'exclusion, il s'agit de minimiser les coûts mémoire, les coûts processeur et surtout les coûts de communication. La sûreté de fonctionnement en tant que telle n'est pas explicitement prise en compte dans ce travail.

La sûreté de fonctionnement, en particulier la fiabilité et la disponibilité, est ensuite prise en compte sous la forme d'un coût. Plusieurs architectures sont envisagées de la plus simple composée d'éléments standards communicant via des lignes 4 - 20 mA à la plus complexe où l'intelligence est véritablement répartie entre les composants intelligents communiquant par le réseau. La méthode proposée a pour but de comparer diverses architectures par le biais d'une transformation des niveaux de sûreté de fonctionnement en coûts.

La dernière partie aborde les aspects dynamiques en vue de l'évaluation du SAID. A l'évaluation de la topologie envisagée en tant que combinaison géographique et "connectique" de divers composants, nous proposons d'affiner cette évaluation en ajoutant la prise en compte de l'évolution temporelle et des modes de fonctionnement. En effet, le taux de défaillance des composants n'est pas indépendant mais fortement lié aux sollicitations que celui-ci reçoit en fonction de l'historique et de l'évolution, tandis que les conséquences de l'occurrence d'une défaillance peuvent être très différentes selon l'état courant du système.

Le **chapitre 7** propose un projet de recherche autour de méthodes de conception et d'évaluation de la sûreté de fonctionnement de systèmes d'automatisation à intelligence distribuée. Ce projet comprend des propositions plus personnelles et d'autres qui pourraient intégrer notamment des membres associés du laboratoire.
Les activités proposées abordent principalement :
- l'intégration des approches fonctionnelles et dynamiques envisagées dans le chapitre 6,
- l'évaluation de la sûreté de fonctionnement d'un SAID par une approche orientée information,
- l'évaluation d'une boucle de sécurité constituée de composants intelligents,
- une étude sur les réseaux de terrain et la sécurité.

Certaines de ces propositions pourraient être reprises ou faire partie d'un projet, dans un contexte régional plus large.

N.B. Tout au long du texte, les références bibliographiques sont présentées de la manière suivante :
- [CI98e], [OU03] ou [RI04a] sans espace dans la nomenclature en deux lettres suivies de l'année et en italique, renvoie à mes références bibliographiques dans l'annexe B.
- [BAY 95], [THO 02] *avec une espace et en trois lettres suivies de l'année, permet de citer une référence à d'autres travaux, l'ensemble se trouve dans l'annexe A.*
Les pages 12 et 13 présentent sous forme de tableaux les principales activités menées depuis 1994, avec en gras les activités majeures. Ce tableau présente les noms des personnes impliquées dans les projets, DEA et thèse, ainsi que les communications et publications (ces dernières sont présentées en blanc sur fond noir selon le codage décrit ci-dessus). Les contrats apparaissent également dans ce tableau. Enfin, nous avons fait apparaître dans les trois dernières lignes les aspects liés aux relations internationales dans la mesure où plusieurs projets ont été concernés.

Les annexes de ce mémoire sont les suivantes :
L'annexe A comprend l'ensemble des références bibliographiques citées tout au long du texte et l'annexe B liste l'ensemble de mes références bibliographiques.

	1994	1995	1996	1997	1998	1999
Instrumentation intelligente - Génie Urbain	Stage A. Filali **CONTRAT CERTU**	***CN95*** ***CI95d, CS95***	***RI96***	***CI97b***		
Réseau de terrain – Sécurité				Projet-stage N. Delahaye **CONTRAT CERTU**	***CI98d, CI98e***	***OU99***
Système d'information urbain (OSA-TESMA)		***CI95c***	***CI96a, CI96c***	***CI97a*** ***CN97***	CONTRAT-PROJET OSA-TESMA	
Analyse fonctionnelle de SAID		***CI95a, CI95b***	***CI96b*** ***CI96d***	***CI97c***	***CI98a, CI98c***	
		THESE F. HERMANN				
Evaluation de la SdF des SAID par une approche fonctionnelle		**THESE B. CONRARD**			***CI98b***	***CI99*** ***CN99c***
Evaluation de la SdF des SAID par une approche dynamique					DEA A. Azzam	**DEA P. Barger**
Fusion approches fonctionnelle et dynamique						
Analyse informationnelle de la SdT de SAID						
Ressources pédagogiques par Internet en EIE				***CP97*** ***CN97***	***CP98a, CP98b*** ***RN98***	**Administration INEIT** ***CP99***
			CONTRAT-PROJET INEIT-MUCON			**Dissémination INEIT-MUCON + Administration INEIT-MUCON**
				Projet Maria Lopez	Projets Luis et Maria	Projets Javier et José / 4 stagiaires ESSTIN et Bx-Arts
Contours de l'EIE en Europe, harmonisation						
Système d'information pour les réseaux thématiques					**CONTRAT-PROJET TNPN**	

	2000		2001		2002		2003		2004	
Instrumentation intelligente - Génie Urbain		***CI00b***	***CN01a***							
	Partenariat UTBM "Supervision de capteur de trafic à base de R.N."									
Réseau de terrain – Sécurité					***CN03a***	***CI03c***	Projet J. Ligusova	DEA A. Konaté	***CI04a, RI04a, OU04***	
						DEA A. Mkhida		**THESE A. MKHIDA**		
						Microthèse C. Brion	Projet S. Quentin	Microthèse M. Janson Muller		
		Ouvrage CIAME								
Système d'information urbain (OSA-TESMA)										
Analyse fonctionnelle de SAID										
Analyse fonctionnelle de la SdT de SAID		***CI00a***	***CN01b***			***CI02b***			***RI04b, RI04c***	
Analyse dynamique de la SdT de SAID					***CI02a***	***CI02c, CI02d***	***CI03a, CI03d, CI03e***		***CI04b***	
	DEA P. Barger	**THESE P. BARGER**								
Fusion approches fonctionnelle et dynamique									**THESE R. GHOSTINE**	
Analyse informationnelle de la SdT de SAID							***CI03b***			
					Travail du groupe A du Contrat de Plan Etat Région					
Ressources pédagogiques par Internet en EIE		CONTRAT-PROJET THEIERE								
	Dissémination INEIT-MUCON + Administration INEIT-MUCON	***CP00a, CP00c, CP00e***	Conférence EAEEIE Nancy + Congrès Club EEA		***CP02c***	***CP02d, RI02***				
	4 stagiaires ESSTIN et Bx-Arts	2 stages d'été	***RI01***	4 stages d'été		4 stages d'été				
Contours de l'EIE en Europe, harmonisation		***CN00***	***CP01***	***CN01c***	***CP02a***	***CP02e***	***CP03a***	***CP03b, OU03***	***CP04a, CP04b***	
		CONTRAT-PROJET THEIERE							Table ronde Club EEA Rouen	
							Projet C. Llanes	Stage N. Trotot	Projets D. Serrano et N. Miguez	Stage M. Cazanave
Système d'information pour les réseaux thématiques	**CONTRAT-PROJET TNPN**									
	Projet E. Dieguez									

1ère partie : Activités d'enseignement, relations internationales, résumé des implications en recherche

1. Activités d'enseignement et administratives

Mes activités pédagogiques se déroulent à l'IUT de Nancy-Brabois, au département Génie des Télécommunications et Réseaux. Les trois principales matières enseignées sont l'informatique industrielle, le traitement du signal (en fait les signaux et systèmes) et l'informatique web (enseignement des outils web, HTML, les CGI et JavaScript, Java).

A ces participations, il convient d'ajouter chaque année l'encadrement de deux ou trois binômes de projets tuteurés, la visite de quatre à cinq stagiaires en entreprise ainsi que la participation naturelle aux jurys de projet 1ère année, soutenances de stages, projets tuteurés 2ème année et aux jurys d'évaluation trimestriels et finaux de 1ère et 2ème année.

Ces implications pédagogiques au département Génie des Télécommunications et Réseaux (G.T.R.) sont décrites dans le premier paragraphe.

Le second paragraphe traite des autres implications pédagogiques depuis ma nomination à l'IUT.

Le troisième paragraphe rappelle les enseignements dispensés pendant la thèse de doctorat.

Le quatrième paragraphe récapitule les activités administratives liées au fonctionnement des structures universitaires.

1.1. Interventions au département GTR de l'IUT de Nancy-Brabois

1.1.1. Activités d'enseignement principales

Une moyenne de 245 heures annuelles équivalent TD, répartie en :

- cours magistraux, travaux dirigés et travaux pratiques dans les domaines de l'informatique industrielle en première année (rédaction d'un polycopié de TP), y compris le groupe qui est en formation par alternance en 2004-2005,
- traitement du signal (signaux et systèmes) en première et seconde années (rédaction de polycopiés de cours, TD et TP et médiatisation du cours de 1ère année dans le cadre de la politique de médiatisation des enseignements de notre université (http://www.cyber.uhp-nancy.fr/demos/GTRT-001/general/index.html)),
- quelques heures de TD et TP en informatique web,

caractérise les douze années d'enseignement au département GTR.

1.1.2. Administration pédagogique

Dans la structure IUT et dans le département GTR, j'ai eu les responsabilités suivantes :

- J'ai été élu chef du département GTR de l'IUT de Nancy-Brabois en octobre 2004 (en fonction à partir du 1er janvier 2005).
- Depuis la rentrée 94-95 jusqu'en 1998-99, et à nouveau depuis 2002-2003 jusqu'en décembre 2004, j'ai assuré la responsabilité des stages au département GTR de l'IUT. Il s'agit de la rédaction et du suivi des conventions, du contact avec les industriels, de l'adéquation entre les potentialités et intérêts des étudiants et les sujets possibles... Chaque année, il nous faut donc trouver entre 60 et 70 stages pour une période de 10 semaines.
- Depuis la rentrée 2001 jusqu'en 2004, j'ai assuré la coordination des projets tuteurés de 2nde année : il s'agit essentiellement de répartir les étudiants par projets puis de surveiller que les rencontres tuteurs-tuteurés s'effectuent de manière régulière pour l'ensemble des étudiants.
- Depuis septembre 2000 et jusque fin 2004, j'ai assuré les fonctions de correspondant TICE, ce qui implique d'être le contact entre ma composante (l'IUT de Nancy-Brabois) et la "cellule des Technologies de l'Information et de la Communication pour l'Enseignement" (TICE) de l'Université Henri Poincaré Nancy 1, afin de coordonner les actions qui sont menées concernant ce thème.

1.1.3. Encadrements de projets tuteurés

Je participe régulièrement à l'encadrement de deux ou trois projets tuteurés par an depuis la mise en place du nouveau programme pédagogique à la rentrée 95-96.

1.2. Autres interventions depuis ma nomination en 1993

1.2.1. Encadrement de Projets-Stages d'été

A partir de l'été 1999, j'ai encadré régulièrement entre deux et quatre étudiants quatre semaines chaque été dans le cadre des projets de réseaux thématiques, avec une bourse de 500 € par étudiant (cf. chapitre suivant). Il s'agit en général d'étudiants en 1ère année GTR.

Durant ces années, les deux aspects qui nous ont plus particulièrement intéressés sont les suivants :

- Développement d'applets Java pédagogiques comme autant de ressources de simulations/démonstrations pouvant s'intégrer dans des cours en ligne,

- Développement de projets de sites internet architecturés autour de bases de données qui ont été utilisés pour l'association européenne EAEEIE (European Association for Education in Electrical and Information Engineering, www.eaeeie.org) ainsi que pour les projets européens INEIT-MUCON (Innovation for Education in Information Technology through Multimedia and Communication Networks, www.eaeeie.org/ineit-mucon) et THEIERE (Thematic Harmonisation in Electrical and Information EngineeRing in Europe, www.eaeeie.org/theiere) (cf. également le chapitre suivant).

Mathieu CAZANAVE : finalisation et mise en exploitation du site-base de données "Recherche de cursus existant en *Electrical and Information Engineering* en Europe", http://www.eaeeie.org/theiereyp	Eté 2004
Nicolas TROTOT : participation à l'intégration de données dans le site "Recherche de cursus existant en *Electrical and Information Engineering* en Europe", http://www.eaeeie.org/theiereyp Mathieu CAZANAVE : finalisation et mise en exploitation du site-base de données de l'EAEEIE	Eté 2003
Bruno MARCELIN : mise à jour des sites capteur et internet package du projet THEIERE, utilisation des formats XML, http://www.eaeeie.org/theiere_isp Luu-Ly MAI : nouveau format XML pour le site "signal" et développement d'une animation Flash pour illustrer les phénomènes d'échantillonnage, pour le projet THEIERE, http://www.eaeeie.org/theiere_signal, http://www.eaeeie.org/theiere_signal/theiere_signal_fr/applet/applet_flash/temp/frameset.htm et http://www.eaeeie.org/theiere_signal/theiere_signal_fr/applet/applet_flash/freq/frameset.htm Benoît SLOTA, étudiant en maîtrise informatique : base de données THEIERE-D, http://www.eaeeie.org/theiere, encadrement technique assuré par Pascal GEND. Christophe ZGRZENDEK : médiatisation du module capteurs pour le projet THEIERE, http://www.eaeeie.org/theiere_sensor/	Eté 2002
Romuald HENRY & Benoît CROISSANT : formation à Java Rachid El OUAHABI & Christian HENRICH : Mise à jour des sites Signal et Capteurs de THEIERE, utilisation de formats XML	Eté 2001
ADAMUS-SUBRA : mise à jour du site INEIT-MUCON	Eté 2000

1.2.2. Autres encadrements

Dans cette partie se trouve la description de différents projets d'étudiants au niveau master 1 ou 2 (niveau IUP ou ingénieur) y compris dans le cadre d'échanges ERASMUS. Ces projets sont généralement liés au développement d'outils pédagogiques accessibles via l'internet ou liés à des aspects "réseaux de terrain et sécurité". J'ai encadré ou co-encadré (astérisque) ces différents projets.

Nom des stagiaires	Travail effectué	Dates	Provenance
David SERRANO & Nerea MIGUEZ	Développement de la zone privée du site theiereyp pour David (cf. ci-dessous C. LLANES). L'objectif était de permettre d'afficher le contenu de la base de données de manière intelligible par l'homme. Le second objectif était de générer le contenu des appendices A et B de la monographie papier en vue de pouvoir la rééditer. Proposition d'extensions sur le site de l'EAEEIE pour Nerea notamment autour de l'environnement de développement Xaraya. Elle a tout d'abord mis en œuvre un outil de gestion de conférences pour les conférences de l'EAEEIE. Ensuite elle a développé un outil qui permet l'aide à la traduction du site de l'EAEEIE et vérifie la compatibilité des diverses langues avec la base de données (codage en Unicode).	mars à août 2004	Université de Vigo (Espagne), ingénieurs ERASMUS
Mathieu JANSON-MULLER	Micro-thèse consacrée à l'étude des bus de sécurité : quels sont-ils ? Sur quels types d'application sont-ils disponibles ? La bibliographie consiste en une analyse des applications effectives des réseaux de terrain "sûrs" dans des systèmes sûrs ou de sécurité. La partie pratique concerne la modélisation de ProfiSafe à l'aide de l'outil de modélisation de réseaux ComNet.	septembre 2003 à février 2004	Microthèse IUP RNC
Carolina LLANES	Etude et développement d'une base de données de recherche des cursus et diplômes existant en "Electrical and Information Engineering" en Europe. Ce travail a été effectué dans le cadre du réseau thématique THEIERE. Pascal GEND a participé à l'encadrement.	février à juillet 2003	Université de Vigo (Espagne), ingénieur ERASMUS
Cyril BRION	Etude sur Ethernet, réseaux de terrain et sûreté de fonctionnement. Ce travail a consisté en une partie bibliographique sur Ethernet, temps réel et sécurité-sûreté de fonctionnement, ainsi qu'une partie pratique consistant en la modélisation d'un protocole de réseau Ethernet temps réel de sécurité.	septembre 2002 à février 2003	Microthèse IUP RNC
Emilio DIEGUEZ PAZO*	Participation au développement de la base de données du projet TNPN (Thematic network programme networking, http://cranmmx.esstin.u-nancy.fr/tnpn/tnpnt). Ce projet a été encadré avec Pascal GEND.	février à juin 2000	Université de Vigo (Espagne), ingénieur ERASMUS
Olivier COGNYÉ & Moustapha OULD EL BECHIR	Mise en place d'une nouvelle charte graphique pour le site INEIT-MUCON en partenariat avec des étudiants de l'Ecole des Beaux-arts : Stéphane NGOWDY & Jérôme HUGUENIN ont développé la charte graphique du site.	année 1999-2000	ESSTIN 3ème année
Javier GONZÁLEZ RODRÍGUEZ* & José CUPEIRO MARTÍNEZ*	- Contrôle d'un processus thermique via Internet, - Réalisation d'une passerelle entre Réseau de terrain et Internet. Ces projets ont été co-encadrés avec Blaise CONRARD.	avril à juin 1999	Université de Vigo (Espagne), ingénieurs ERASMUS
María Asuncíon CARRANZA FERNANDEZ et Luis Ángel VILLAR ESMORIS	Développement d'un outil pour créer et gérer des questionnaires d'évaluation d'étudiants, utilisables dans le cadre du projet INEIT-MUCON : - la première stagiaire a développé un outil permettant l'écriture simple de questionnaires d'évaluation pour les étudiants, - le second stagiaire s'est occupé de la gestion des réponses envoyées par l'étudiant via ce questionnaire couplée à une correction automatique.	avril à juin 1998	Université de Vigo (Espagne), ingénieurs ERASMUS
María José LÓPEZ PADÍN	Développement d'applets Java utilisables dans le cadre de modules d'enseignements développés pour le projet INEIT-MUCON. Le travail a consisté au développement d'une "applet" Java pour l'enseignement des problèmes d'échantillonnage et de repliement.	avril à juin 1997	Université de Vigo (Espagne), ingénieur ERASMUS

Liste des publications relatives à l'ensemble de ces travaux : *CP04b, OU03, CP03a, RI02, CP02d, CP02c, CP00e, CP00b, CP00a, CN00, Rc00b, Rc00a, CP99, CN99b, CP98b, CP98a, RN98, CN98.*

1.2.3. Master Réseau à Casablanca

Depuis l'année universitaire 1996-97 et jusqu'en 2002, nous avons enseigné une année sur deux avec Hugues GARNIER le module de Traitement du Signal qui était dispensé à Casablanca, Maroc, dans le cadre d'un master Réseau : Master Européen en Ingénierie des Technologies de l'Information et de la Communication. Il s'agit d'une trentaine d'heures d'enseignement dispensé sur une semaine. J'ai personnellement assuré ce module en 1997, 1999 et 2002.

1.2.4. Autres interventions et formation continue

J'ai participé certaines années à des jurys de soutenance de stages ou de projets de :
- 3ème, 4ème ou 5ème année à l'ESSTIN, diplôme d'Ingénieur,
- DEA,
- DUT Génie Electrique, au moins quatre fois,
- ENSEM, Ecole Nationale Supérieure d'Electricité et de Mécanique, en 1998,
- IUP RNC, Réseaux Numériques de Communication, en 2002, 2003 et 2004,
- ENSAM, Ecole Nationale Supérieure des Arts et Métiers, Metz, en 2002 et 2004,
- projets ERASMUS, pour des étudiants provenant principalement de l'Université de Vigo, Espagne, de 1997 à 2000 et depuis 2003.

1.2.4.1 DEA

En 2002-03 et 2001-02, j'ai assuré 2 heures d'enseignement "Capteurs intelligents" dans le cadre du module capteur du DEA CSC (Contrôle, Signaux, Communication), commun à l'UHP et à l'INPL.

1.2.4.2 Formation continue au GTR

- En 2003-04, 2002-03, 1998-99, 97-98 et 96-97 dans le cadre de la formation continue GTR, je suis intervenu pour des TD/cours de soutien dans l'enseignement de Traitement numérique du signal durant une dizaine d'heures en plus des enseignements traditionnels où les étudiants de formation continue sont intégrés aux enseignements de formation initiale de 2ème année.
- J'ai participé à l'élaboration du contenu pédagogique du module de "Traitement du signal" pour la formation "animateur développeur télétravail" organisée par le CITCOM (organisme de formation de France Telecom) en 1994-95.
- J'ai participé à l'Université d'été "la Physique des Télécommunications" organisée par l'Union des physiciens et le département GTR de l'IUT du 9 au 13 juillet 1994... Mes interventions ont concerné deux modules de deux heures avec rédaction de polycopiés (dérivés de celui utilisé à l'IUT) : "Numérisation du signal" et "Filtrage numérique et compression de données" ainsi que la présentation de huit heures de TP "Signaux discrets et filtrage numérique" : filtrage numérique non récursif et récursif, processeur de traitement numérique du signal (analyse spectrale, filtrage, génération de signaux).

1.2.4.3 Formation en anglais, pour un public international

- Juillet 2000 : j'ai présenté le réseau thématique INEIT-MUCON en français et anglais au Conseil Régional à Metz, dans le cadre de l'école d'été "Utilisation des Nouvelles Technologies de l'Information et de la Communication pour favoriser l'enseignement professionnalisé", devant une cinquantaine de participants européens :

  http://www.univ-ete.uhp-nancy.fr/2000/fr/flash/programme/mar18.html
- Avril 1999 : j'ai participé à l'organisation du "Thematic network programme networking" (TNPN). Cela concernait l'initiation aux serveurs web, HTML, Javascript, CGI… sous la forme d'une heure de conférence suivie de trois heures de travaux pratiques sur machine en anglais pour une quarantaine de participants européens de toutes disciplines.
- Juillet 1998 : j'ai participé à l'Ecole d'été TEMPUS (programme européen, Tempus Joint European Project S-JEP-11317-96) dont l'intitulé était : "Integrated Control Systems and Intelligent Control" organisé par l'université des Mines et de Métallurgie de Cracovie (Pologne), du 7 au 10 juillet 1998.
  Mon intervention a consisté en deux conférences de deux heures en anglais, la première sur l'instrumentation intelligente, la seconde sur les systèmes d'Automatisation à Intelligence Distribuée. Ces interventions étaient accompagnées d'un polycopié de 50 pages publié dans les actes de l'école d'été et

intitulé : J.M. THIRIET - "**Intelligent instruments and distributed systems**", in *Integrated control systems and intelligent control* - University of Mining and Metallurgy, Krakow, 1998, pp. 11-64. [*DC98*]

1.3. Activités pédagogiques antérieures (1989-93)

Avant ma nomination à l'IUT, j'ai été successivement AER puis à ATER à l'ESSTIN (Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy) où j'ai assuré mes enseignements en TP Physique, TP Matériaux Industriels, TP Productique et TD Optimisation, durant quatre années.

1.4. Activités administratives

Depuis plusieurs années, j'ai été et suis membre de diverses commissions tant au niveau national qu'au niveau local, et je suis responsable de la mise à jour des informations de plusieurs sites internet.

1.4.1. Commissions nationales

- Membre élu au Conseil National des Universités 61ème section de 1996 à 1999 au titre des Maîtres de Conférences.

1.4.2. Commissions locales

Celles-ci regroupent les commissions de spécialistes et de choix de l'UHP et de l'INPL.

1.4.2.1 Commissions de spécialistes

- Membre suppléant extérieur nommé de la Commission de Spécialistes 7-9-11-12-70-71ème section de l'UHP depuis 2003.
- Membre titulaire élu et vice-président Maître de Conférences de la Commission de Spécialiste 61ème section de l'Université Henri Poincaré Nancy 1 de 2001 à 2004. J'ai participé à ce titre plusieurs fois à des commissions d'audition.
- Membre suppléant élu de la Commission de Spécialiste 61ème section de l'Université Henri Poincaré Nancy 1 de 1998 à 2001.
- Membre titulaire extérieur nommé de la Commission de Spécialistes 61ème section de l'Institut National Polytechnique de Lorraine de 1998 à 2001. J'ai participé à deux commissions d'audition.

1.4.2.2 Commissions de choix

- Membre extérieur nommé de la Commission de Choix de l'IUT de Saint-Dié des Vosges depuis janvier 2004.
- Membre de la commission de choix de l'IUT de Nancy-Brabois de décembre 1994 à décembre 2001, et à nouveau depuis octobre 2004. A ce titre, j'ai participé deux fois à des commissions d'audition des Maîtres de Conférences (1995 en 61ème section, 1997 en 63ème section).

1.4.3. Autres activités administratives

Je m'occupe de l'administration des sites suivants :
- Commission des Relations Internationales du Club EEA (www.clubeea.org/relint), depuis l'origine (1997~),
- eaeeie (www.eaeeie.org) et gestion de la liste de diffusion depuis 1997,
- ineit-mucon (www.eaeeie.org/ineit-mucon) et gestion de la liste de diffusion de 1997 à 2000,
- theiere (www.eaeeie.org/theiere) et gestion de la liste de diffusion depuis 2000.

J'ai participé à l'équipe de mise en place du "serveur WWW du CRAN" (http://www.cran.uhp-nancy.fr) depuis 1996.

1.5. Conclusion

Ces années d'enseignement m'ont permis de développer quelques pratiques pédagogiques à l'IUT avec deux objectifs majeurs :
- le maintien d'un niveau "théorique" correct avec pour but de permettre aux étudiants de poursuivre vers des études plus longues dans de bonnes conditions,
- la mise à disposition d'outils "pratiques" (ex : interface Matlab-DSP, simulation Java et Flash) afin de valider les connaissances des étudiants sur des applications ou pseudo applications réelles ou réalistes.

Sur ce point, il semble inévitable dans le contexte actuel d'orientation de l'université vers un enseignement plus démocratisé, de renouer avec les spécialistes de la pédagogie et de la didactique de nos disciplines. En effet, la prise en compte de scénarios de navigation d'apprentissage est importante lors du développement de nouvelles ressources pédagogiques. Ces aspects sont intéressants tant pour l'enseignement à distance que pour l'enseignement initial à cause par exemple de l'hétérogénéité des profils étudiants ou de l'ouverture à l'international…

Cette réflexion est menée avec l'équipe pédagogique du département GTR et aussi par le biais des projets de réseaux thématiques européens. Le développement d'outils pédagogiques pour la simulation et les laboratoires virtuels, tels que le pilotage de processus réels à distance, est en effet l'un des axes de ces projets.

Les aspects liés aux projets européens sont succinctement décrits dans le chapitre suivant.

2. Implication en relations internationales et technologies de l'information et de la communication pour l'enseignement (TICE)

J'ai participé aux projets de réseaux thématiques européens INEIT-MUCON (*Innovation for Education in Information Technology through Multimedia and Communication Networks*, www.eaeeie.org/ineit-mucon) et THEIERE (*Thematic Harmonisation in Electrical and Information EngineeRing in Europe*, www.eaeeie.org/theiere) proposés par l'EAEEIE (*European Association for Education in Electrical and Information Engineering*, www.eaeeie.org) en réponse aux appels d'offres SOCRATES de la Commission Européenne.

En 1996, le Pr. Michel ROBERT avait, en tant que secrétaire de l'EAEEIE à cette époque, répondu à l'appel d'offres de la commission européenne et cette réponse avait été retenue. Le projet INEIT-MUCON est né. Le Pr. Michel ROBERT en était le coordinateur et j'ai assuré le secrétariat de la coordination en étroite collaboration avec lui de début 1997 à l'été 1999, date à laquelle je me suis occupé de la coordination du projet pour la dernière année et demie, c'est-à-dire les six derniers mois de INEIT-MUCON et l'année de dissémination obtenue pour 1999-2000 [*RI02, voir Annexe C papier 6*].

En 1999, en tant que coordinateur effectif du projet à cette époque, j'ai envoyé à la commission européenne une déclaration d'intention pour le projet de réseau thématique THEIERE. J'ai souhaité ne pas assurer la coordination de ce second réseau thématique afin de pouvoir me consacrer davantage à la recherche.

Cette proposition a été retenue. Nous avons ensuite, avec Maria João MARTINS de l'*Instituto Superior Técnico* de Lisbonne (Portugal), coordinatrice du nouveau projet, écrit la proposition de projet qui a été acceptée par la commission européenne pour une période de trois ans de 2000 à 2003.

Les deux premiers paragraphes de ce chapitre traitent des projets INEIT-MUCON et THEIERE. Le troisième paragraphe aborde ma participation aux travaux de la commission des relations internationales du Club EEA. Un quatrième paragraphe récapitule mes activités dans les domaines des TICE et des relations internationales.

2.1. Réseau thématique INEIT-MUCON (1996-2000)

L'objectif initial du réseau thématique INEIT-MUCON [*RI02, voir Annexe C papier 6*] [*DC00*] était de démontrer la faisabilité d'une université virtuelle européenne en *Electrical and Information Engineering* (EIE) qui s'appuierait sur le développement de modules d'enseignement accessibles à distance.

Le projet a débuté par un recensement des méthodes et outils utilisables ; cette étape a coïncidé avec l'expansion des technologies liées à l'internet tout au moins en France et a conduit au développement d'un site web spécifique permettant de mettre à la disposition de tous les partenaires un état de l'art sur le thème des outils utilisables en enseignement à distance. Cette "base de données" nous a également incités à restreindre notre champ d'application au développement de modules d'enseignement en EIE, accessibles via l'internet sans outils particuliers autres qu'un navigateur classique.

Le projet INEIT-MUCON a produit des modules d'enseignement accessibles via l'internet dans différentes disciplines de l'EIE ; il a encouragé et développé les échanges entre institutions européennes.

Le savoir-faire acquis dans la maîtrise des technologies liées à l'internet nous a conduit à nous impliquer en collaboration étroite avec la DG Education et Culture dans un programme baptisé *TNP Networking (Thematic network programme networking*, http://cranmmx.esstin.u-nancy.fr/tnpn/tnpnt) en 1998-99. Ce programme avait pour objectif la diffusion des "bonnes pratiques" en matière de NTIC et s'est concrétisé par notre participation à 2 séminaires de "formation" à l'attention des acteurs de l'ensemble des 43 réseaux thématiques qui couvrent des domaines très divers :

- les domaines académiques "classiques" en sciences économiques, sociales et humaines,
- les sciences et technologie,
- les domaines de spécialité,
- des domaines transversaux : philosophie et sciences humaines, éthique, enseignement ouvert et à distance, formation continue, administration et gestion des universités.

Ce programme a permis également la conception et le développement d'une base de données interactive recensant l'activité de l'ensemble de ces réseaux thématiques, dont nous avons été un acteur majeur avec Pascal GEND.

2.2. Réseau thématique THEIERE (2000-2003)

Ce second réseau a été lancé dans le cadre du programme SOCRATES 2 pour succéder au projet INEIT-MUCON [*CN01c*] (http://www.eaeeie.org/theiere/).

Le projet THEIERE est un projet de réseau thématique SOCRATES qui a été accepté par la Commission Européenne pour la période 2000-2003. Ce projet a pour objectifs une analyse des cursus proposés par les pays européens dans les domaines de l'EIE, ceci afin de mettre en évidence les points communs et les différences dans les enseignements proposés en Europe. Cette réflexion est une conséquence de la mise en place d'un espace européen de l'enseignement supérieur et de la recherche. Il s'agit d'aider les collègues qui réfléchissent pour proposer de nouveaux cursus dans l'esprit du schéma de Bologne.

Dans le cadre de ce projet une réflexion sur le LMD en Europe a été réalisée [*CN03b*]. Elle présente les résultats d'un recensement le plus exhaustif possible des formations disponibles dans les champs disciplinaires de l'EIE en Europe.

Comme résultat de ce travail, une monographie a été élaborée en 2003 [*OU03*]. Celle-ci se présente comme un document de référence à destination des enseignants et des institutions. Elle est accompagnée de la réalisation d'un portail internet (http://www.eaeeie.org/theiereyp/) couplé à un moteur de recherche plutôt destiné à des étudiants souhaitant enrichir leur cursus d'une dimension européenne.

Dans la suite du projet INEIT-MUCON, un autre aspect du projet THEIERE consiste à développer des ressources pédagogiques accessibles via l'internet et pouvant être utilisées par les enseignants dans les divers pays européens. J'ai plus particulièrement participé au module de traitement du signal et dans une moindre mesure au module de capteurs.

2.3. Commission des relations internationales du club EEA

Depuis 1996, je suis membre actif de la commission des relations internationales du club EEA. J'ai assuré de septembre 1997 à septembre 2000 la tâche de vice-président de cette commission. Depuis l'origine j'administre son site (http://www.clubeea.org/relint/). J'ai participé à la présentation des travaux de la commission des relations internationales lors des congrès du Club EEA de 1998 à Strasbourg, 1999 à Lyon, 2000 à Toulouse, 2001 à Nancy, 2002 à Perpignan, 2003 à Besançon et 2004 à Rouen.

En 2004, j'ai eu le plaisir de co-animer, avec H. FREMONT (de Bordeaux) la table ronde sur "La diversité du statut des enseignants chercheurs en Europe", avec la participation de : D. WEICHERT (Allemagne), M. JONES (Angleterre), F. FANTINI (Italie), A. SEOANE (Espagne), lors du congrès du Club EEA, à Rouen, le 3 juin 2004. Cette table ronde a été organisée avec l'aide de A. BENSRHAIR (Rouen) et H. YAHOUI (Lyon).

2.4. Implications liées aux relations internationales

Dans cette partie sont décrits les aspects plus particulièrement liés aux relations internationales et à l'innovation pédagogique. Les parties équivalentes plus liées à la recherche sont décrites dans le chapitre suivant.

2.4.1. Activités diverses

Activités	Mon rôle	Budget géré
CETSIS'2005 à Nancy	membre du comité d'organisation, trésorier	65 900 €uro
Réseau thématique THEIERE de 2000 à 2003.	coordinateur général de la tâche 1, rédacteur principal de la monographie "*Electrical and Information Engineering in Europe*" et développement du portail associé (http://www.eaeeie.org/theiereyp) avec l'aide d'étudiants.	

Activités	Mon rôle	Budget géré
Conférence de l'EAEEIE de 2001 à Nancy (110 participants)	trésorier et président du comité d'organisation	29 253,44 €uro
Meeting du projet THEIERE en mai 2001 à Nancy (50 participants)	organisateur	
Congrès du Club EEA en 2001 à Nancy	membre du comité d'organisation, trésorier adjoint	
Organisation de la réunion terminale du projet INEIT-MUCON à Nancy en octobre 2000 pour une quinzaine de participants	organisateur	
EAEEIE, association loi 1901	trésorier depuis 1999 (près de 180 membres européens à gérer par an)	
"INEIT-MUCON dissemination" de septembre 1999 à septembre 2000 : - prise en charge des déplacements et du logement dans le cadre du projet, - rédaction et diffusion de 5000 exemplaires d'une plaquette présentant le projet INEIT-MUCON en 12 langues.	coordinateur	66 509,74 €uro
Thematic Network Programme Networking : site pour presenter les réseaux thématiques SOCRATES de septembre 1998 à mars 2000	- gestion des informations de la base de données, - gestion des aspects financiers pour l'UHP. - participation aux réunions de définition du site à Bruxelles.	12 600 € pour l'UHP

2.4.2. Autres comités de programme

Ma participation concernant des conférences qui se sont déroulées hors de Nancy et qui étaient liées à l'innovation pédagogique et aux relations internationales est décrite ci-dessous :

- Comité scientifique de IBCE'2004 Workshop "Internet Based Control Education" en septembre 2004 à Grenoble.
- Président de session lors de la conférence ITHET'2004 à Istanbul en juin 2004.
- Président de session lors de la 8ème conférence annuelle de l'EAEEIE à Edimbourg en juin 1997 puis membre du comité de programme et président de session lors des conférences annuelles de l'EAEEIE depuis 1998.

2.4.3. Collaborations avec des chercheurs étrangers

Dans le cadre de l'implication dans les projets européens SOCRATES, nous avons eu l'opportunité de collaborer notamment avec les universités suivantes :

- l'Université de Ulm (D) *(M. HOFFMANN*[4]*)*,
- l'Université de Vigo (E) *(J.C. BURGUILLO & A. SEOANE*)*,
- l'Université de Valence (E) *(J.V. BENLLOCH & F. BUENDIA)*,
- l'Université de Oulu (FI) *(P. LAPPALAINEN*)*,
- l'Université de Limerick (IRL) *(C. BURKLEY)*,
- l'Université des mines et métallurgies de Cracovie (PL) *(W. GREGA)*,
- l'Université de de Rzseszów (PL) *(L. TRYBUS)*,
- l'Institut Supérieur Technique de Lisbonne (P) *(M.J. MARTINS* & J. ESTEVES)*,
- l'Université de Košice (SK) *(J. LIGUS)*,

ainsi que l'Université Claude Bernard Lyon 1 *(H. YAHOUI*)*, l'Université de Rennes 1 *(O. BONNAUD*)* et l'Université de Bordeaux 1 *(H. FREMONT*)*.

[4] Dans cette partie, une étoile à côté d'un nom signifie que nous sommes co-auteurs d'au moins une communication.

2.4.4. Expertise, review

J'ai eu l'occasion d'effectuer des tâches d'évaluation et d'expertise dans les contextes décrits ci-dessous :

- Activités de reviewing pour
  - IEEE trans. On Education,
  - le livre : "Innovations 2003: World Innovations in Engineering Education and Research", Editors Win Aung, M. H. W. Hoffmann, Ng Wun Jern, Robin W. King, Luis Manuel Sanchez Ruiz,
  - les congrès EAEEIE, IBCE'2004 …
- Expertise :
  - participation au Forum 2000 à Bruxelles organisé par la Commission Européenne en janvier 2000,
  - participation à la journée d'évaluation des réseaux thématiques à La Haye (CHEPS/NUFFIC : SOCRATES evaluation seminar on curriculum development and thematic network activities, 16-17 juin 2000).

2.5. Conclusion

L'ensemble des activités menées ces dernières années concernant les relations internationales et l'utilisation des TICE ont un double intérêt :

1) Le premier est bien sûr l'ouverture internationale, la possibilité d'avoir pu contribuer à la réflexion sur le futur de l'Université avec une vue européenne par le biais des réseaux thématiques. J'ai également participé au Forum 2000 fin janvier 2000 à Bruxelles en tant que représentant du réseau thématique INEIT-MUCON en compagnie des représentants des autres réseaux thématiques et de 300 présidents/recteurs d'universités d'Europe. Il s'agissait dans le cadre d'ateliers de réfléchir sur l'avenir de l'enseignement à distance, du métier d'enseignant-chercheur, des diplômes…

Concernant l'utilisation des TICE, naturellement très liée à la pédagogie, nous pouvons reprendre les deux aspects les plus intéressants :

- L'un concerne l'utilisation de simulations [MIC 98] et animations développées par le biais des nouvelles technologies (Applets Java, animation Flash) comme autant d'outils pédagogiques complémentaires aux outils plus classiques d'enseignement,
- L'autre est relatif au développement dans le cadre de plusieurs projets d'étudiants (IUT GTR, IUP, ingénieurs ESSTIN ou ENSEM, étudiants ingénieurs de Vigo (Espagne)) de ressources pédagogiques (cf. chap. précédent) accessibles par l'internet basées principalement soit sur des applets Java, soit sur des bases de données. Pour ces développements, les étudiants ont été amenés à travailler dans une véritable démarche "projet" à plusieurs, avec l'obligation de laisser à disposition une documentation technique pour permettre de futurs développements ; certains développements ont en effet nécessité l'intervention de plusieurs stagiaires pour être utilisables. Ce travail et cette démarche ont été pour eux, je pense, une bonne expérience de formation.

L'utilisation potentielle de ces divers outils est non seulement l'enseignement à distance, mais également :

- l'enseignement présentiel, en tant qu'outil pédagogique complémentaire ou alternatif, notamment comme support d'aide à l'homogénéisation des publics étudiants en terme de pré requis,
- la possibilité pour les étudiants de préparer leur mobilité avant de partir et aussi de garder le contact avec l'université d'origine,
- la possibilité pour les anciens étudiants de garder le contact avec leur université (formation continue, formation tout au long de la vie).

2) L'autre aspect très intéressant de cette activité concerne la réflexion approfondie sur l'implantation du LMD (licence, master, doctorat, conformément au processus de Bologne) dans les disciplines de l'EIE. La réflexion a débouché sur l'écriture d'une monographie proposant :

- un état des lieux des formations existant dans les domaines de l'EIE en Europe et le contour des disciplines de l'EIE,
- un état des lieux des réflexions et de l'implantation effective du LMD dans les divers pays européens,
- la proposition d'un cadre de cursus de licence en EIE autour duquel les diverses universités européennes pourraient construire leur offre.

Le but est naturellement de contribuer à favoriser la mobilité des étudiants et la reconnaissance des diplômes.

Concernant les perspectives, nous envisageons de poursuivre cette activité en partenariat avec les collègues européens afin de tendre vers des modèles de cursus dans nos disciplines, toujours avec l'esprit de favoriser la transparence et la reconnaissance des diplômes au niveau européen.

3. Co-encadrements, participations à des jurys de thèse, autres implications en recherche

Ce chapitre présente de manière synthétique les principales implications en recherche.

3.1. Co-encadrements de thèse

J'ai demandé l'autorisation de Co-encadrement de thèse, accepté par lettre du Président de l'Université Henri Poincaré Nancy 1 en date du 6 juin 1996 après avis favorable du département de la formation doctorale, afin de participer au co-encadrement de doctorants qui travaillent sur la problématique de la modélisation des SAID. Cette thématique a pour but de définir quels sont les critères et contraintes à prendre en compte pour parvenir à la distribution des commandes et du diagnostic. L'aspect sûreté de fonctionnement est un critère fondamental de cette démarche. Le conseil scientifique de l'INPL m'a également accordé l'autorisation à co-encadrer localement des thèses en date du 10 juin 2004.

3.1.1. Thèses en cours

Nom du diplômé : **Rony GHOSTINE** .....Diplôme : Thèse INPL .....
Titre du travail : Evaluation et vérification de paramètres de sûreté de fonctionnement d'un système distribué .....
Date début : septembre 2004.....Date fin : septembre 2007 .....encadrement : 70 % .....
Noms et % des co-directeurs : Pr Jean-François AUBRY 30 % .....
..... Situation actuelle du diplômé : Boursier MENSR .....

Un certain nombre de voies ont déjà été exploitées, ou plus précisément abordées, lors de travaux précédents. Les travaux de Raphaël Schoenig [SCH 03a] apportent une contribution dans le passage des spécifications vers l'évaluation probabiliste, par la proposition d'une réduction de modèle par une approche à la fois analytique et par simulation (les outils utilisés sont les réseaux de Petri interprétés et stochastiques et les graphes de Markov). Les travaux de Karim Hamidi [HAM 03], en cours, proposent une approche progressive par raffinement afin d'identifier toutes les séquences menant à l'événement danger, l'objectif étant l'évaluation d'une boucle de sécurité (les outils utilisés sont les réseaux de Petri et automates finis stochastiques). Le travail de Pavol Barger [BAR 03], thèse terminée, a montré l'influence d'un réseau de communication, sur l'évaluation de paramètres de sûreté de fonctionnement (les outils utilisés sont les réseaux de Petri colorés à arc probabiliste, et la simulation de Monte-Carlo). Une application de ce travail a montré comment, dans le cas d'un réseau de sécurité, une insuffisance de description des normes peut entraîner des interprétations diverses de certaines spécifications, impliquant un risque de non-conformité au niveau de sécurité requis.

Ces travaux récents et en cours serviront de base au travail à effectuer. Afin d'apporter une contribution, il est demandé de proposer un modèle de système distribué critique (c'est-à-dire où le paramètre de sécurité est fondamental, ex : direction automobile par réseau, *X by Wire*…), intégrant un réseau de communication, et de proposer l'évaluation de paramètres de sûreté de ce système, prenant en compte le réseau. L'idée est de regarder d'un peu plus près quels sont les points qui sont explicités dans la norme (principalement la 61508), et quels sont les points plus flous, afin d'avoir un regard critique et de voir comment et avec quels critères, il est possible d'aider les concepteurs de systèmes distribués critiques.

L'ensemble de ces travaux entre dans le cadre de la conception, optimisation et évaluation de systèmes distribués.

Nom du diplômé : **Abdelhak MKHIDA**.....Diplôme : Thèse INPL .....
Titre du travail : Evaluation de la sûreté de fonctionnement des boucles de sécurité constituées de Capteurs-actionneurs intelligents et de réseaux de terrain .....
Date début : septembre 2003.....Date fin : septembre 2006 .....encadrement : 70 % .....
Noms et % des co-directeurs : Pr Jean-François AUBRY 30 % .....
..... Situation actuelle du diplômé : Fonctionnaire de l'état marocain.....

Le travail s'inscrit dans la poursuite de travaux antérieurs sur les instruments intelligents. Les instruments sont essentiellement des capteurs et actionneurs, dotés de capacités de traitement numériques et d'une interface de communication, et capables à l'aide des traitements adéquats de donner en temps réel une image de leur environnement proche, de qualifier leurs fonctionnalités (incertitude instantanée ou moyennée de mesure) et leur état de fonctionnement (possibilité de fonctionner correctement, en marche dégradée, de ne plus fonctionner…). Dans ce cadre, il est demandé ici d'étudier le problème des capteurs et actionneurs de sécurité. Quels sont les critères à prendre en compte pour qu'un

capteur puisse être "de sécurité", même chose pour un actionneur? Comment effectuer l'implémentation ? Tous ces aspects doivent être pris en compte dans le cadre des normes en vigueur, et à venir.

Par ailleurs, le réseau de terrain, qui est le moyen de communication habituel autour duquel sont disposés et connectés les capteurs et actionneurs, peut-il être sûr ? Comment le qualifier ?

Ce travail se devra d'être à la fois de recherche et de veille technologique, afin d'avoir une connaissance des produits existants et des problèmes de normalisation.

Ce travail pourra le cas échéant faire l'objet d'un partenariat avec l'I.N.R.S. (Institut National de Recherche et de Sécurité) ainsi qu'avec Siemens, le travail pourra être validé « pratiquement » sur la plate-forme « sûre » mise en place à l'ENSAM de Metz.

Outre l'intégration au sein des projets du laboratoire et des objectifs du PRST du CPER, ce travail s'intègre au niveau national dans les travaux du SEE 18-04 CIAME (Constituants Intelligents pour l'Automatisation et la Mesure) ainsi que dans l'Action Spécifique "Méthode et modèle pour l'évaluation de la sûreté de fonctionnement des systèmes distribués" (RTP 55 Systèmes de contrôle-commande et réseaux de communication).

3.1.2. Thèses soutenues

Nom du diplômé : **Pavol BARGER** ..... Diplôme : Thèse UHP Nancy 1.....
Titre du travail : Evaluation et validation de la fiabilité et de la disponibilité des systèmes d'automatisation à intelligence distribuée, en phase dynamique.....
Date début : septembre 2000 ..... Date fin : 15 décembre 2003 ..... encadrement : 70 % .....
Noms et % des co-directeurs : Pr Michel ROBERT 30 % .....
..... Situation actuelle du diplômé : ATER .....
Publications relatives à ce travail *: CI04b, CI04a, CI03e, CI03d, CI03a, CN03a, CI02d, CI02c, CI02a*.

QUALIFIE en 2004

Jury : président Professeur Jean-François AUBRY (INPL, Nancy), Rapporteurs : MM. les Professeurs Robert VALETTE (LAAS, Toulouse) et Pascal YIM (ECL, Lille), Membres : Isabelle AUGE-BLUM (INSA, Lyon), Philippe CHARPENTIER (INRS, Vandœuvre), Prof. Michel ROBERT (UHP, directeur de thèse), Jean-Marc THIRIET (UHP, co-directeur de thèse)

Résumé :

Les systèmes d'automatisation actuels bénéficient de plus en plus du développement de l'informatique, ce qui permet l'augmentation de leur distribution (spatiale et/ou logique) et de leur niveau d'intelligence. L'étude de la sûreté de fonctionnement (fiabilité, disponibilité, prise en compte d'aspects liés à la sécurité) de tels systèmes est un sujet épineux parce qu'il est nécessaire de prendre en compte différentes caractéristiques telles que les modes de fonctionnement (reconfiguration), les dépendances entre les défaillances, la présence d'un réseau de communication, le vieillissement, etc. De nombreuses méthodes d'étude existent mais chacune a une portée limitée à un domaine ou un point de vue particulier et ne peut pas être appliquée avec une vue d'ensemble.

L'approche proposée dans la thèse consiste en une analyse du comportement dynamique, à la fois du point de vue fonctionnel et dysfonctionnel et la configuration dynamique du système est particulièrement visée. Les Réseaux de Petri colorés (CPN) sont utilisés pour la modélisation de chaque composant et l'analyse est faite principalement par une simulation de Monte Carlo à l'aide du logiciel Design/CPN. L'occurrence de défaillances est modélisée par la prise en compte de transitions stochastiques.

Les résultats principaux de cette étude sont tout d'abord la proposition de modèles des composants d'un système et ensuite leur analyse dynamique par la simulation. Une approche de la vérification formelle du protocole de communication AS-i, en regard de la norme, conclut la partie applicative de la thèse.

L'apport original de la thèse consiste en la proposition d'une approche permettant à la fois la conception des modèles des composants et de leur intégration pour constituer un système complet, par l'utilisation d'un outil unique permettant d'intégrer des points de vue à l'interface de trois communautés scientifiques : l'automatique, le génie informatique et la sûreté de fonctionnement.

Mots clés : système d'automatisation, systèmes commandés en réseau, réseau de Petri, sûreté dynamique, graphe d'occurrence.

Nom du diplômé : **Blaise CONRARD** .....Diplôme : Thèse UHP Nancy 1 .....
Titre du travail : Contribution à l'évaluation quantitative de la sûreté de fonctionnement des systèmes d'automatisation en phase de conception .....
Date début : septembre 1995.....Date fin : 24 septembre 1999.....encadrement : 50 % .....
Noms et % des co-directeurs : Pr Michel ROBERT 50 % .....
..... Situation actuelle du diplômé : Maître de Conférences à l'USTL de Lille (LAGIS) .....
Publications relatives à ce travail : *CI00a, OU99, CI99, CN99d, CN99c, CN99a, CI98e, CI98b*, puis après la thèse, dans le cadre de travaux conjoints au sein du groupe CIAME, les références suivantes : *RI04c, RI04b, CI03c, CI02b, CN01b*.

QUALIFIE en 2000.

Jury : président Professeur Marc GABRIEL (UHP Nancy 1), Rapporteurs : MM. les Professeurs Mireille BAYART (USTL Lille) et Daniel NOYES (ENIT Tarbes), Membres : André CHOVIN (CROUZET Automatismes, Valence), Joseph CICCOTELLI (INRS, Vandœuvre), Prof. Michel ROBERT (UHP, directeur de thèse), Jean-Marc THIRIET (UHP, co-directeur de thèse).

Résumé :
Les travaux exposés dans ce mémoire portent sur l'évaluation de la sûreté de fonctionnement explicitement utilisée comme un critère lors de la conception des systèmes d'automatisation. Ce document est organisé de la manière suivante :
Une première partie définit les différents termes relatifs aux systèmes d'automatisation et aux systèmes d'automatisation à intelligence distribuée puis la problématique générale de leur conception. Ensuite, la sûreté de fonctionnement et les principales notions s'y rattachant sont introduites.
Une deuxième partie présente les différentes représentations utilisées lors de la démarche de conception.
Une troisième partie aborde les principales méthodes employées pour quantifier les différents aspects de la sûreté de fonctionnement. Parmi celles-ci, celles relatives aux aspects disponibilité et fiabilité/sécurité sont plus particulièrement développées. Enfin, les arbres de décision binaire sont abordés comme outil pour la quantification de ces aspects.
Une quatrième partie présente la méthode proposée pour la conception des systèmes d'automatisation. Celle-ci s'appuie sur une recherche combinatoire afin d'optimiser l'architecture à concevoir prenant en compte ces critères relatifs à la sûreté de fonctionnement.
Une dernière partie illustre la démarche proposée en l'appliquant à deux exemples.

Mots clés : système d'automatisation, conception d'architectures, répartition de tâches, quantification de la sûreté de fonctionnement.

Nom du diplômé : **Frédéric HERMANN**.....Diplôme : Thèse UHP Nancy 1 .....
Titre du travail : Contribution à la répartition des traitements et des données sur une architecture distribuée équipée d'un réseau de terrain FIP : application à un processus thermique pilote .....
Date début : septembre 1993.....Date fin : 7 novembre 1997.....encadrement : 50% .....
Noms et % des co-directeurs : Pr Michel ROBERT 50 % .....
..... Situation actuelle du diplômé : Responsable informatique Région Est ASSEDIC.....
Publications relatives à ce travail : *Rc98b, CI98d, CI98c, CI98a, CI97c, CI96d, CI96b, CI95b*.

QUALIFIE en 1998

Jury : président Professeur Jean-Pierre THOMESSE (INPL Nancy), Rapporteurs : MM. les Professeurs Guy JUANOLE (UPS Toulouse) et Marcel STAROSWIECKI (USTL Lille), Membres : Didier PERINO (HLP Technologies, Paris), Prof. Michel ROBERT (UHP, directeur de thèse), Jean-Marc THIRIET (UHP, co-directeur de thèse).

Résumé :
Ce travail propose un placement des tâches d'un Système d'Automatisation à Intelligence Distribuée (SAID) sur une architecture matérielle équipée d'un réseau de terrain.
Une première partie met en évidence l'évolution du concept de Système d'Automatisation de Production (SAP) vers celui de Système d'Automatisation à Intelligence Distribuée (SAID). Cette évolution met en exergue principalement les progrès réalisés dans le domaine de l'instrumentation, des réseaux de terrain ainsi que des méthodes de conception.
Ensuite une approche méthodologique propose une modélisation fonctionnelle d'un SAID qui montre les fonctions essentielles d'un système d'automatisation et permet de dénombrer les tâches à implanter sur le SAID.
Dans un second temps, suite à une étude des différentes stratégies de répartition, une méthode est proposée afin de réaliser la projection de l'architecture fonctionnelle sur l'architecture matérielle. Il s'agit d'une méthode de programmation mathématique qui prend en compte certains critères et certaines contraintes de l'architecture fonctionnelle et matérielle telle que la taille mémoire, le temps d'exécution et également l'aspect communication avec le réseau de terrain FIP.
Enfin l'implémentation sur un processus thermique pilote (PTP) permet de valider l'architecture opérationnelle proposée.
Cette démarche s'inscrit dans une perspective de développement d'un ensemble d'outils pour la conception d'un SAID.

Mots-clés :
Système d'Automatisation à Intelligence Distribuée, conception d'architectures, architecture fonctionnelle, architecture matérielle, allocation de tâches, réseau de terrain FIP.

3.2. Participations à des jurys de thèse

Outre la participation aux trois jurys de thèses que j'ai co-encadrées, j'ai participé à deux jurys de thèse :

- 17 décembre 2003, à l'Université de Technologie de Belfort-Montbéliard, thèse de Nadhir MESSAI, "Surveillance de trafic urbain et interurbain à bases de modèles neuronaux", doctorat de l'Université de Technologie de Belfort-Montbéliard et de l'Université de Franche-Comté, Rapporteurs : R. LENGELLE et J. RAGOT, Président : D. LEFEBVRE, Examinateurs : A. ELMOUDNI, P. THOMAS, J.M. HENRIOUD et J.M. THIRIET,
- 20 septembre 2001, à l'Université Henri Poincaré Nancy 1, thèse de Philippe JEANJEAN, "Contribution à la définition et à la réalisation d'un atelier intelligent de génie du test d'ensembles électroniques", doctorat de l'UHP, Rapporteurs : P. FOUILLAT et E. NIEL, Examinateurs : J.F. AUBRY, M. NADI, J.L. NOIZETTE, M. ROBERT et J.M. THIRIET.

3.3. Accueil de doctorant étranger

Dans le cadre d'un partenariat mené avec la *Technická univerzita Košice* (Université Technique de Košice), Slovaquie, nous avons accueilli de février à avril 2003 Jana LIGUSOVA HORANSKA, étudiante en troisième année de thèse.

Cet échange s'inscrit dans le cadre d'un accord bilatéral entre nos deux universités. Cet accord a suivi le démarrage dans notre laboratoire (en septembre 2000) d'une thèse de doctorat par un étudiant originaire de l'université de Košice. Nous souhaitons profiter de conditions propices telle que la présence dans notre laboratoire d'un ancien doctorant provenant de Košice et l'existence de thématiques de recherche proches, pour mettre au point une coopération.

Une étude approfondie sur le choix de stratégies de synchronisation sur horloges ou sur événements extérieurs a été effectuée, combinée à une analyse de l'influence sur la sûreté de fonctionnement. Les résultats de cette étude ont été présentés et publiés à une conférence internationale [*CI04a, voir Annexe C papier 5*]. Jana LIGUSOVA HORANSKA a soutenu sa thèse de doctorat à Košice le 16 juin 2004.

3.4. Encadrements de Master recherche

Durant ces années, j'ai eu le plaisir de participer à l'encadrement de 8 étudiants en master recherche ou équivalent. Il s'agit de 5 DEA, 2 étudiants-ingénieurs avec un stage fortement ancré recherche, 1 post-DEA.

3.4.1. Evaluation des propriétés de sécurité du protocole de réseau de sécurité "Profisafe" (DEA, 2004)

Nom du diplômé : Ahmadou KONATE.....Diplôme : DEA.....
Titre du travail : Evaluation des propriétés de sécurité du protocole de réseau de sécurité "Profisafe"
Date début : septembre 2003 ……Date fin : septembre 2004.....encadrement : 20 %
Noms et % des co-directeurs : Pr. Jean-François AUBRY, 30 %, Pavol BARGER 50 %

Dans la suite du travail de Sébastien QUENTIN l'année précédente, il s'agit ici de voir comment il est possible de proposer un modèle de ProfiSafe. A partir des spécifications, un modèle à base de réseaux de Petri est réalisé pour l'évaluation des propriétés de sûreté de fonctionnement de ce réseau de sécurité.

3.4.2. Capteurs intelligents pour des applications de sécurité (DEA, 2003)

Nom du diplômé : Abdelhak MKHIDA.....Diplôme : DEA.....
Titre du travail : Capteurs intelligents pour des applications de sécurité
Date début : septembre 2002 ……Date fin : septembre 2003.....encadrement : 50 %
Noms et % des co-directeurs : Pr. Jean-François AUBRY, 30 %, Olaf MALASSE 20 %
Situation actuelle du diplômé : En 1ère année de thèse. Enseignant, ENSAM (Ecole Nationale Supérieure des Arts et Métiers) à Meknès (Maroc), passe un semestre de recherche par an en France.

Ce travail a montré comment les caractéristiques des instruments intelligents pouvaient être évaluées, en regard de la norme 61508 et a proposé une analyse de l'utilisation des instruments intelligents dans des applications de sécurité. Ce travail s'est poursuivi par une thèse.

3.4.3. Évaluation du niveau de sécurité d'une architecture distribuée à l'aide d'une modélisation par réseaux de Petri (diplôme d'ingénieur ENSEM, 2003)

Nom du diplômé : Quentin SEBASTIEN.....Diplôme : diplôme d'ingénieur ENSEM, stage orientation recherche en partenariat avec l'INRS
Titre du travail : Evaluation du niveau de sécurité d'une architecture distribuée à l'aide d'une modélisation par réseaux de Petri
Date début : septembre 2002 ……Date fin : septembre 2003.....encadrement : 30 %
Noms et % des co-directeurs : Pr. Jean-François AUBRY, 30 %, Pavol BARGER 40 %
Situation actuelle du diplômé : dans la vie professionnelle.

Ce travail a concerné l'évaluation du réseau de terrain ASISafe en regard de la description faite par la norme.

3.4.4. Modélisation et analyse de performances de systèmes d'automatisation à intelligence distribuée (DEA, 2000)

Nom du diplômé : Pavol BARGER….....Diplôme : DEA
Titre du travail : Modélisation et analyse de performances de systèmes d'automatisation à intelligence distribuée
Date début : septembre 1999 ……Date fin : septembre 2000.....encadrement : 80 %
Noms et % des co-directeurs : Pr. Michel ROBERT, 20 %
Situation actuelle du diplômé : Docteur, ATER.

L'objectif général de ce travail de DEA consistait à identifier les difficultés lors de la modélisation d'un système d'automatisation à intelligence distribuée, constitué de capteurs, actionneurs, unités de traitement, autour d'un réseau de communication. L'outil de modélisation proposé était les réseaux de Petri. Ce travail s'est poursuivi par une thèse.

3.4.5. Modélisation par approche hybride d'un processus thermique pilote (DEA, 1999)

Nom du diplômé : Ameziane AZZAM.....Diplôme : DEA.....
Titre du travail : Modélisation par approche hybride d'un processus thermique pilote
Date début : septembre 1998 ……Date fin : septembre 1999.....encadrement : 30 %
Noms et % des co-directeurs : Pr. Michel ROBERT, 20 %, Jean Michel RIVIERE 50 %
Situation actuelle du diplômé : En doctorat, contrat industriel.

L'objectif général de ce travail de DEA consistait à mettre en place une stratégie de commande-supervision hybride pour un processus thermique pilote disponible au laboratoire.

3.4.6. Protocoles et architectures de systèmes de régulation de trafic urbain (ingénieur ESSTIN, orientation recherche, 1998)

Nom du stagiaire ESSTIN (diplôme ingénieur, stage en laboratoire orientation recherche) : Nicolas DELAHAYE.....
Titre du travail : Etude des caractéristiques des Systèmes de régulation de trafic urbain : architecture et protocoles de transmissions - performances et possibilités d'évolution
Date début : octobre 1997…….Date fin : juin 1998.....encadrement avec Pr. Michel ROBERT et Frédéric HERMANN
Situation actuelle du diplômé : travail dans l'industrie
Publications relatives à ces travaux : *Rc98b, CI98d*.

Cette étude a fait l'objet d'un contrat entre le laboratoire et le CERTU (Centre d'Etudes sur les Réseaux, les Transports, l'Urbanisme et les constructions publiques) qui dépend du Ministère des Transports.
Le travail a consisté à effectuer une étude des principaux systèmes de régulation de trafic urbain et de les comparer en terme d'architecture et de protocoles de transmission afin de dégager pour l'utilisateur potentiel des

critères de performances et de modularité. Ces résultats ont fait l'objet d'un rapport d'étude confidentiel pour le CERTU. Contrat n° UNI 97-071, 1er octobre-31 décembre 1997, juin 1998.

3.4.7. Recueil de données du trafic routier (post-DEA, 1994)

Nom : Abid FILALI.....Post-DEA.....
Titre du travail : Recueil de données dans le domaine routier. .....
Date début : octobre 1993..... Date fin : septembre 1994 ..... % encadrement : 50% .....
Noms et % des co-directeurs : Pr Michel ROBERT 50% .....
Situation actuelle du diplômé : travail dans l'industrie .....
Publications relatives à ce travail : *Rc94*

Cette étude a fait l'objet d'un contrat entre le laboratoire et le C.E.T.U.R. (Centre d'Etudes des Transports Urbains) qui dépend du Ministère des Transports. Il s'agissait d'étudier avec quels moyens est assurée la fonction "Recueil de données" dans les systèmes routiers et de voir les insuffisances en regard de la manière dont cette fonction est assurée dans les procédés industriels. Nous avons également analysé le degré d'intelligence atteint par ces systèmes et dégagé les améliorations qui peuvent être envisagées. Ce travail se présentait comme une application au domaine routier de notre thématique de recherche. Ces résultats ont fait l'objet d'un rapport d'étude confidentiel pour le C.E.T.U.R. (devenu depuis le CERTU). Contrat n° UNI 93-102, 1er Octobre-31 décembre 1993, juin 1994.

3.4.8. Analyse de trafic (DEA, 1991)

Nom du diplômé : Sandrine ROTH.....Diplôme : DEA.....
Titre du travail : Analyse de trafic : coefficients d'encombrement statique et dynamique permettant de caractériser des quartiers urbains en vue de leur modélisation. .....
Date début : octobre 1990..... Date fin : septembre 1991 ..... % encadrement : 50% .....
Noms et % des co-directeurs : Pr Michel ROBERT 50% .....
Situation actuelle du diplômé : Docteur, travaille dans l'industrie

Cette étude consistait à définir des coefficients d'encombrement statique et dynamique sur une zone de manière à isoler la proportion d'usagers en transit de celle des usagers en stationnement : origine ou destination dans la zone considérée. Les informations utilisées pour cela étaient les débits comptés à partir de boucles électromagnétiques installées dans la chaussée. Ce travail a fait l'objet d'un contrat entre le CRAN et la Ville de Nancy.

3.5. Participation à la gestion de projets, contrats, ouvrages

Ce paragraphe récapitule les participations à des contrats ainsi qu'à la rédaction d'un ouvrage.

Projet	Mon rôle	Budget géré
Ouvrage rédigé par le groupe CIAME de 2000 à 2004.	rédacteur principal du chapitre 1 et coordinateur du chapitre 5 [*OU04*]	
Etude des caractéristiques des systèmes de régulation du trafic urbain : Architecture et protocoles de transmissions, performances et possibilités d'évolution" - CERTU/CRAN/Université Henri Poincaré Nancy 1, 1998, Confidentiel. Contrat n° UNI 97-071, 1er octobre-31 décembre 1997	responsable	15 244 € (100 000 FRF)

Projet	Mon rôle	Budget géré
European Commission TELEMATICS project UR 1020, OSA-TESMA Open System Architecture for Telematic Services in Municipal Applications, de début 1996 à début 1999.	gestion assurée par T. DIVOUX pour la partie française, je l'ai assisté en participant à tous les meetings d'évaluation à Bruxelles et en le remplaçant quelques fois à certaines phases de négociation avec Karl Heinz KAPP de l'Université de Karlsruhe. Je suis l'un des principaux rédacteurs du "*deliverable*" [*Rc98a*].	
Le recueil de données dans le domaine du trafic routier et urbain : les besoins, l'existant, les perspectives" - CERTU/CRAN/Université Henri Poincaré Nancy 1, 1994, Confidentiel. Contrat n° UNI 93-102, 1er octobre-31 décembre 1993	responsable	7 622 € (50 000 FRF)
Contrat sur ma thèse avec la Ville de Nancy de janvier 1990 à décembre 1991	co-responsable	27 414 € (179 824,10 FRF)
Contrat sur le DEA de Sandrine Roth en 1991	co-responsable	

3.6. Participation à la gestion d'équipe

- En 1999-2000, j'ai co-animé avec le professeur Michel ROBERT l'équipe Instrumentation Intelligente du CRAN, notamment en vue de la réorganisation du laboratoire qui a eu lieu à cette période et j'ai participé en 2000 à la rédaction des rapports d'activité (1996-99) et de perspectives (2001-2004) du CRAN pour la partie "Conception de systèmes sûrs de fonctionnement" (CSSF).
- J'ai eu également l'opportunité de participer à la rédaction de rapports d'activités et de perspectives à mi-parcours de 2002 et en 2003 pour le laboratoire sur des aspects liés au thème CSSF et les "NTE" (nouvelles technologies éducatives).
- Par le biais du groupe A du CPER, nous travaillons avec des membres associés du laboratoire avec pour objectif leur intégration.
- Je participe à la gestion des crédits du ministère et des crédits de contrat pour l'équipe depuis 1999 et à la gestion des crédits CNRS pour le thème CSSF depuis 2000.

3.7. Comités de programmes ou d'organisation de conférences

J'ai participé aux comités d'organisation ou comités de programme des conférences suivantes liées à la recherche :

Evénement	Mon rôle
MMM'2004 en septembre 2004 à Nancy, 11th IFAC Symposium on Automation in Mining, Mineral and Metal processing	membre du comité d'organisation
AIAI'2003 en juin 2003 à Montréal (Canada)	- membre des comités d'organisation et scientifique - design du site web http://www.aiai3.etsmtl.ca/ - président de session
QUALITA'2003, 5ème Congrès International Pluridisciplinaire Qualité et Sûreté de Fonctionnement, en mars 2003 à Nancy	membre du comité d'organisation et du comité scientifique, président de session
Congrès du Club EEA à Nancy en mai 2001	membre du comité d'organisation, trésorier adjoint
AIAI'99 (Troisième Conférence Internationale sur l'Automatisation Industrielle) à Montréal en 1999	président de session

3. Co-encadrements, jurys de thèse, autres implications en recherche

Evénement	Mon rôle
AIAI'95 (Seconde Conférence Internationale sur l'Automatisation Industrielle) à Nancy en 1995	membre du comité d'organisation, en charge du secrétariat général de la conférence, vice-président de session
Colloque FIRTECH (pôle de formation des ingénieurs par la recherche dans les technologies diffusantes) en 1994 à Nancy	membre du comité d'organisation

3.8. Sociétés savantes

Je suis membre des sociétés savantes suivantes, où je précise mon rôle pour chacune d'entre elles :

- RUFEREQ (Réseau des Universitaires Francophone pour l'Enseignement et la REcherche En Qualité et sûreté de fonctionnement) depuis 2003.
- IEEE depuis 2001 (societies Measurement, Reliability, Education …) : je suis signataire des "pétitions" pour la création de chapitres français des sociétés *Reliability* et *Education*.
- EAEEIE (European Association for Education in Electrical and Information Engineering) depuis 1996 : je suis membre du conseil depuis juin 1997 et trésorier depuis juin 1999.
- SEE (Société de l'Electricité, de l'Electronique, et des Technologies de l'Information et de la Communication) depuis 1995 : je suis membre actif du groupe de travail CIAME (Constituants Intelligents pour l'Automatisation et la Mesure) depuis septembre 1999.
- Club EEA depuis 1994 : je suis membre du conseil d'administration depuis mai 2001, réélu en 2004, j'ai été vice-président de la commission des relations internationales de novembre 1997 à septembre 2000 et demeure membre actif de cette commission depuis 1995.

3.9. Groupes de recherche et conseils scientifiques

3.9.1. Groupes nationaux

- Je participe aux travaux du groupe CIAME - groupe SEE 18-04 CIAME (Constituants Intelligents pour l'Automatisation et la Mesure), depuis septembre 1999. Un exposé intitulé "Evaluation et validation de la fiabilité et de la disponibilité dynamique des systèmes d'automatisation distribués" a été présenté le 6 juin 2002. Ce groupe est à l'origine de l'**Action Spécifique** "Méthode et modèle pour l'évaluation de la sûreté de fonctionnement des systèmes distribués" qui a été acceptée et a commencé à fonctionner au début 2004 dans le cadre du RTP 55 "Systèmes de contrôle-commande et réseaux de communication"…
- J'ai participé aux travaux du groupe de travail "Systèmes dynamique hybrides" de septembre 1998 à début 2000.
- Je participe occasionnellement aux travaux du groupe "Réseaux de Petri" : une présentation des travaux du doctorant P. BARGER a eu lieu.
- Je participe occasionnellement aux travaux de l'IMdR-SdF (Institut pour la Maîtrise des Risques et la Sûreté de Fonctionnement) "Groupe de Travail: Recherches Méthodologiques". Les travaux des doctorants P. BARGER et B. CONRARD ont été présentés dans ce groupe.

3.9.2. Groupes locaux

- Depuis septembre 2001, je suis membre des groupes A (Automatique et génie informatique : de l'architecture fonctionnelle à l'architecture opérationnelle; comment garantir la Sûreté de fonctionnement) et B (Automatique, psychologie, ergonomie, économie, évaluation du risque) du Pôle de Recherche Scientifique et Technique "Sûreté industrielle et déchets", projet "Automatisation et prévention des risques" dans le cadre du contrat de plan Etat – Région lorraine. J'assure la fonction d'animateur du groupe A depuis septembre 2002.
- De 1993 à 1996, j'ai participé aux travaux du groupe A.M.I. (Actionnement et Mesure Intelligents), groupe interne du CRAN, qui avait pour but l'élaboration d'un modèle générique et consensuel susceptible de représenter tout type d'instrument intelligent, qu'il s'agisse d'actionneur ou de capteur. Les réflexions de ce groupe de travail ont été synthétisées à l'aide de la méthode SADT.

3.9.3. Conseils scientifiques

- Je suis membre du conseil scientifique du Pôle de Recherche Scientifique et Techniques "Sûreté industrielle et déchets" du contrat de plan Etat-Région (région Lorraine) depuis 2001.
- J'ai été membre du Conseil Scientifique de l'ESSTIN de début 1997 jusqu'en 1999.

3.10. Valorisation de la recherche

3.10.1. Collaborations avec d'autres chercheurs

A l'extérieur du CRAN, nos collaborations en recherche sont avec :

- l'IMA (*Institut für Mikrorechner und Automation*) et l'IPF (*Institut für Photogrammetrie und Fernerkundung*) *(K.H. KAPP[5]*)* de l'Université de Karlsruhe, Allemagne, dans le cadre du projet européen OSA-TESMA de 1996 à 2000,
- l'Ecole de Technologie Supérieure, Université du Québec - Canada, dans le cadre de l'AIAI (Association Internationale pour l'Automatisation Industrielle) depuis 1995 *(G. BOGDADI)*. 4 conférences ont été organisées en 10 ans,
- le LAGIS (ex LAIL) de Lille dans le cadre de travaux communs relatifs aux instruments intelligents et aux systèmes distribués depuis 1994 *(M. BAYART*, B. CONRARD*)*,
- le LISTIC (ex LAMII) d'Annecy *(E. BENOIT)*, le LAMIH de Valenciennes *(L. CAUFFRIEZ*)*, l'INSA de Lyon *(I. BLUM)*, l'INRETS de Villeneuve d'Ascq *(M. WAHL),* dans le cadre des travaux du groupe CIAME,
- l'Université de Technologie de Belfort-Montbéliard : D. LEFEBVRE* (maintenant à l'Université du Havre) et P. THOMAS* dans la période 1999-2003 sur la régulation de trafic urbain,
- le CERTU (Centre d'Etudes sur les réseaux, les transports, l'urbanisme et les constructions publiques), organisme du Ministère des Transports, principalement de 1993 à 1998 *(Y. ROBIN-PREVALLEE*)*,
- l'INRS (Institut National de Recherche et de Sécurité, Equipe S.S.A. Sûreté des Systèmes Automatisés) depuis 2002 *(Ph. CHARPENTIER, J. CICCOTELLI*)*.

3.10.2. Expertise, review

- J'ai analysé des documents techniques dans le domaine du trafic urbain pour le compte du CERTU (activité de consultant) en 1994.
- J'ai évalué des communications pour les congrès AIAI, Qualita'2003, LFA'2005…

[5] Dans cette partie, une étoile à côté d'un nom signifie que nous sommes co-auteurs d'au moins une communication.

2ème partie : Présentation des activités de recherche

4. Présentation du contexte de travail : Systèmes d'Automatisation à Intelligence Distribuée & Sûreté de fonctionnement

Depuis 1995 environ, dans la poursuite des travaux de thèse liés, d'une part, à l'utilisation de capteurs pour la régulation de trafic urbain et, d'autre part, à la classification d'architectures de systèmes de régulation de trafic urbain, j'ai développé, au sein de l'équipe "instrumentation intelligente" du CRAN et avec le professeur Michel ROBERT, un axe appelé "Conception de système d'automatisation à intelligence distribuée". Ces systèmes d'automatisation sont définis comme étant composés d'instruments, capteurs et actionneurs, généralement intelligents, d'unités de traitement intégrées ou pas aux instruments et de media de communication, typiquement des réseaux de terrain ; ces systèmes sont appelés dans la suite SAID.

Le terme de SAID provient de SAP (Système Automatisé de Production) auquel ID (Intelligence Distribuée) a été ajouté dans les années quatre-vingt-dix avec l'apparition des unités de traitement numérique et des réseaux de communication. Le P de production a ensuite été enlevé pour tendre à plus de généricité. Plus récemment, la communauté anglophone parle de NCS (*Networked Control System* / système commandé en réseau, ou système commandé via les réseaux), évolution de DCS (*Discrete Control System* / Système de Commande discret/numérique ou *Distributed Control System* / Système d'Automatisation distribué), même si ces notions ne recoupent pas tout à fait les mêmes réalités.

Ce chapitre présente tout d'abord les méthodes classiques de sûreté de fonctionnement et la problématique afférente. Le second paragraphe introduit les systèmes d'automatisation à intelligence distribuée et la dernière partie envisage la sûreté de fonctionnement de ces systèmes.

4.1. Méthodes d'évaluation de la sûreté de fonctionnement

La sûreté de fonctionnement [LAP 95] [NUN 02] [VIL 88] est la science des défaillances et de leur analyse.

Les propriétés les plus couramment étudiées ou quantifiées sont décrites figure 4.1 [PEY 94] [50191]:

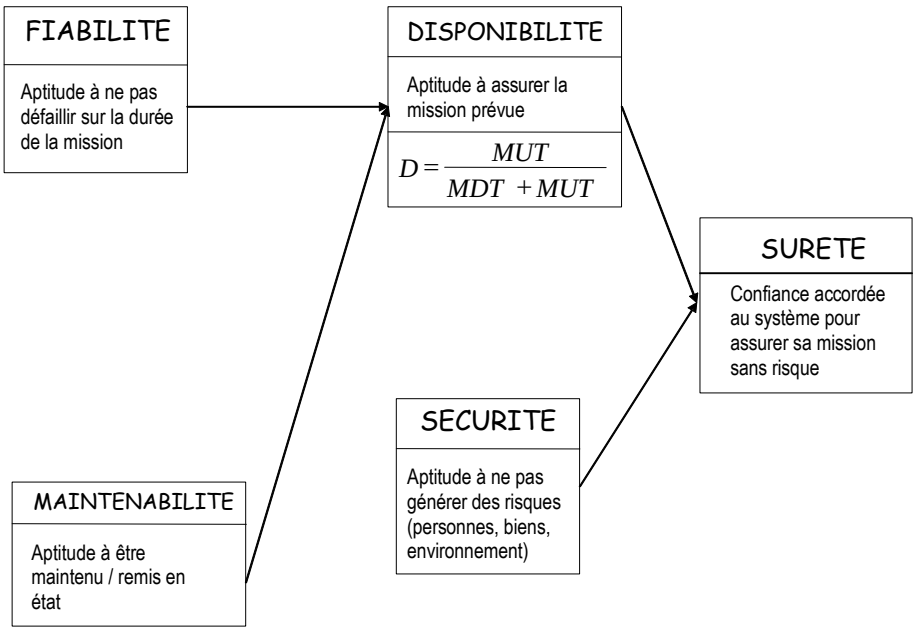


Figure 4.1 – Positionnement des divers concepts de sûreté de fonctionnement

La sûreté telle qu'elle est envisagée sur la figure 4.1 correspond aux notions de FMDS (Fiabilité Maintenabilité Disponibilité Sécurité) ou *RAMS (Reliability Maintainability Availability Safety)*. Le *MUT (mean up time)* caractérise le temps moyen de disponibilité, le *MDT (mean down time)* est le temps moyen d'indisponibilité.

Comme cela a été rappelé dans l'introduction du présent document, les aspects sécurité considérés dans notre travail s'entendent principalement aux sens sécurité machine et environnement, tels qu'ils peuvent être employés par des organismes comme l'INRS ou l'INERIS. Il s'agit bien ici de la sécurité – innocuité (*safety* en anglais), au sens où il s'agit de se protéger vis-à-vis de défaillances catastrophiques, et non pas de la sécurité – intégrité (*security* en anglais), même si celle-ci peut avoir des conséquences sur celle-là.

Les méthodes classiques de la sûreté de fonctionnement sont les méthodes qualitatives (AMDEC) qui permettent une analyse explicite basée sur une intervention d'experts et les méthodes quantitatives (blocs-diagrammes de fiabilité, arbres des défaillances, graphes de Markov) [DHA 02] [LAP 95] [PAR 01] [VAU 96] [VIL 88]. Ces méthodes sont généralement basées sur les caractéristiques de composants constitutifs plus simples connues par retour d'expérience ou par les documentations des fournisseurs.

4.1.1. Markov

Les graphes de Markov basés sur les processus stochastiques [DHA 02] permettent de quantifier la fiabilité, la disponibilité et la maintenabilité d'un système ou d'un matériel. Les graphes représentent les différents états du système ainsi que les transitions entre ces états. Les états envisagés sont l'état nominal, l'état dégradé, la panne et la réparation. Un taux de transition est associé à la probabilité de défaillance ou de remise en état ou tout simplement de changement d'état, pour chaque transition. Ces diagrammes sont adaptés pour les systèmes réparables ; les principales limitations sont le fait que les taux de transition sont supposés constants et que les aspects temporels et les séquencements d'états ne sont pas modélisables à cause de l'impossibilité de prendre en compte les effets mémoire.

Nous proposons ci-dessous un rappel des définitions des systèmes markoviens [NUN 02] :

- Un système est markovien lorsque les taux de transitions entre les états sont constants ; dans ce cas, les temps de séjour dans les états sont distribués exponentiellement.
- Un système est semi-markovien lorsque les temps de séjour dans les états sont des variables aléatoires non exponentielles mais les transitions entre les états sont conformes à une chaîne de Markov.
- A contrario, un système est non markovien lorsque l'effet mémoire joue, que les lois de probabilités ne sont pas réinitialisées lorsqu'on entre dans un état.

Les travaux de R. SCHOËNIG [SCH 03] proposent une méthode d'agrégation de graphes de Markov pour l'analyse de systèmes hybrides. Ces travaux s'inscrivent dans le contexte de la "Fiabilité dynamique et des systèmes hybrides" où cohabitent des processus à temps continus modélisés par des équations différentielles et des processus événementiels représentés par des graphes d'états. L'intérêt est de pouvoir modéliser un système complexe comme étant composé d'un ensemble de sous-systèmes indépendants. La difficulté est naturellement de bien diviser le système en sous-systèmes indépendants. La chaîne de Markov liant les sous-systèmes peut ensuite être établie et évaluée.

L'approche privilégiée par NOURELFATH [NOU 03] a pour but d'évaluer la fiabilité d'un système reconfigurable en prenant en compte divers modes de fonctionnement, notamment dégradés.

Nous pouvons terminer cette partie en rappelant qu'il est possible d'obtenir des équivalences entre des modèles à base de graphes de Markov et des modèles à base de réseaux de Petri stochastiques dans certains cas [SIG 02].

4.1.2. Aspects normatifs

Les travaux menés dans le domaine de la sûreté de fonctionnement doivent s'appuyer sur les normes [61069] [61508] [61511] [62061] [POU 98]. Il existe également des normes de modélisation de systèmes distribués telles que la 61499 [61499].

Ces normes définissent en général un certain nombre de contraintes à respecter sans donner de moyens pour vérifier celles-ci. Cela entraîne l'existence dans ces normes d'un certain nombre d'ambiguïtés et d'imprécisions permettant diverses interprétations, quelquefois aux dépens de la sécurité…

D'après Peycurat par exemple [PEY 04], un fournisseur qui dispose d'un relai avec un PFD (Probability of Failure on Demand / probabilité de défaillance sur sollicitation) compris entre 10^{-3} et 10^{-2} peut faire certifier ce relai au

niveau SIL2. Le problème soulevé est que l'accumulation de composants certifiés n'entraîne pas obligatoirement la sûreté du système. Il est important de définir les modes de fonctionnement du système dans son ensemble et la façon dont il se comporte en fonction des circonstances.

4.2. Systèmes d'Automatisation à Intelligence Distribuée

4.2.1. Problématique

La notion de système [DUR 79] d'automatisation à intelligence distribuée a été élaborée par la communauté de chercheurs travaillant sur la modélisation des instruments intelligents et réseaux de terrain dans le milieu des années 1990 [BAY 94] [CHO 98] [ROB 92] [SIM 95] [SIM 99]. Cette notion regroupe des systèmes temps réel composés de composants[6] intelligents[7] répartis autour d'un réseau de communication tel qu'un réseau de terrain. L'adjonction de l'intelligence sur ce type de systèmes a pour but notamment de favoriser la sûreté de fonctionnement. Toutefois, la complexité engendrée par ce type d'architecture fait qu'il n'est pas aisé d'évaluer la sûreté de fonctionnement, la complexité elle-même pouvant être à l'origine de failles ou de difficultés supplémentaires de sûreté de fonctionnement [HEC 03] [TOU 01].

Nos travaux ont pour objectif d'aider à effectuer la synthèse entre des recherches faites sur la conception de SAID, autrement dit la recherche de l'architecture la plus adaptée au sens d'un critère de coût intégrant à la fois le cycle de vie du système[8] avec une prise en compte d'aspects liés à la sûreté de fonctionnement et plus particulièrement la fiabilité-disponibilité du processus, la recherche également de la meilleure répartition des tâches et/ou des processus de calcul en vue d'obtenir une architecture opérationnelle la plus efficace, toujours au sens de ce critère de coût et de la disponibilité-fiabilité.

Par ailleurs, les aspects sécurité[9] sont une partie que nous développons, d'une part, parce que la sécurité a naturellement sa place parmi les attributs de la sûreté de fonctionnement mais également parce que la proximité géographique de l'INRS (Institut National de Recherche et de Sécurité) ouvre des perspectives d'application.

L'idée générale tend vers une méthode d'aide à l'évaluation des architectures obtenues afin de déterminer le niveau de sûreté et d'efficacité au sens des besoins exprimés et de la normalisation.

4.2.2. Outil, fondement

Afin de pouvoir représenter les différents composants du système d'automatisation, nous travaillons depuis 1999 autour des réseaux de Petri et de leurs extensions (colorés, stochastiques, continus/hybrides...) [DAV 02] [MOR 02] qui permettent une modélisation apte à la simulation et l'analyse de performances de tous les composants du système. Les capteurs et actionneurs, intelligents ou non, les régulateurs et autres fonctions de "supervision et/ou prise de décision", les moyens de communication et le processus lui-même peuvent être formalisés de la sorte, avec un point de vue à la fois continu et discret, en fonction des nécessités. En effet, les SAID tels que nous les avons définis peuvent être considérés comme des systèmes hybrides intégrant des parties continues (capteurs, process…), discrètes (capteur échantillonné, unités de calcul) et événementielles (réseau de communication). Par ailleurs, non seulement le système sur lequel nous travaillons est par essence hybride, mais en plus, la démarche de modélisation pourrait être considérée elle aussi comme hybride dans la mesure où, considérant un système plus classique que le SAID, au modèle "classique" de l'automatique continue vient se greffer un modèle sur "événements" nécessaire pour la prise en compte de l'occurrence de défaillances. Comme il a été rappelé par P. BARGER [BAR 03], il est également possible de considérer trois dynamiques avec des échelles de temps très différentes qui cohabitent dans le SAID ou NCS : la dynamique très rapide du réseau, la dynamique des constantes de temps du système automatisés normalement beaucoup plus lentes et enfin la dynamique de l'occurrence des défaillances encore beaucoup plus rares [61508].

Les réseaux de Petri ont été introduits par C.A. Petri au début des années 1960 [DAV 92]. Sans effectuer un descriptif complet, très répandu dans la littérature, nous pouvons rappeler qu'un réseau de Petri est un graphe composé de places, arc et transitions. Des jetons peuvent stationner dans les places, et se déplacent d'une place à une autre en franchissant les transitions, via les arcs. Les arcs lient les places aux transitions. Des règles pour

[6] capteurs, actionneurs, unités de traitement

[7] numériques, dotés de capacité de calcul et de communication

[8] coût d'installation, d'utilisation, de démantèlement

[9] sécurité-innocuité

le franchissement des transitions peuvent être établies (temporisation, franchissement stochastique) de même que les arcs peuvent être "pondérés", permettant le franchissement simultané de plusieurs jetons, ou permettant d'en générer ou d'en absorber [DIA 01] [TRI 03].

Afin de pouvoir modéliser des systèmes ayant des caractéristiques hybrides, les réseaux de Petri ont acquis des extensions leur permettant de prendre en compte des aspects continus [FLA 98b] [HAN 01] [MOS 99] [NEV 98] [RIE 99] [SIF 98] [TOM 03] [ZAY 02] par le biais de transitions continues, validées continûment sur taux de franchissement ou fréquence, ou par l'adjonction aux places d'équations algébro-différentielles permettant de maintenir un jeton dans une place comme une fonction du comportement "continu" du système durant cette "phase".

Les réseaux de Petri colorés permettent quant à eux de caractériser les jetons par des caractéristiques (données associées, propriétés particulières) avec les règles de franchissement associées [DAV 92]. L'intérêt de cette coloration est qu'elle permet à la fois de construire un modèle qui soit plus parlant puisque plus explicite mais aussi d'obtenir un modèle plus "compact". La difficulté souvent rappelée est celle de l'évaluation d'un tel modèle.

Les réseaux de Petri non autonomes, c'est-à-dire fonctionnant sur une sollicitation extérieure et intégrant de ce fait des propriétés temporelles, peuvent être utilisés pour modéliser des processus de Markov, comme nous l'avons vu dans le paragraphe précédent (RdP stochastiques [BOB 98] [DIA 01] [JEL 02]). Cela donne une application intéressante des réseaux de Petri pour la sûreté de fonctionnement ou la supervision [DAV 92 p. 168] [CHA 02b] [FLA 98a] [KHA 02] [MAC 98] [SIG 02] [VOL 04b]. Les réseaux de Petri vieillissants ('*Aging Petri Nets*') sont également utilisés [VOL 04a].

Les évaluations exhaustives utilisant toutes les propriétés des réseaux de Petri, en tout cas celles qui correspondent à la version de réseaux de Petri utilisée, ne sont pas toujours possibles. Dans ce cas, les simulations de Monte-Carlo [LAB 02] [MAR 04] [ROC 02] sont un complément intéressant avec pour propriétés l'évaluation des processus stochastiques ou complexes et l'obtention de résultats dans des situations où les méthodes plus formelles ne fonctionnent pas.

4.2.3. Application

Les applications envisagées sont très diverses puisqu'elles concernent potentiellement à la fois tous les systèmes à haute disponibilité et/ou haute sécurité :

- Les grands systèmes ou systèmes complexes peuvent être analysés comme étant un ensemble de constituants coopérant, chacun ayant la possibilité de s'adapter. C'est dans ce cas la sûreté de fonctionnement du système en tant que tel qui nous intéresse (ex : processus industriel, système de régulation de trafic urbain, avion...).
- Les systèmes isolés (embarqués, enfouis, dormants) sont des systèmes pour lesquels il faut envisager différents cas de dysfonctionnements, s'assurer de leur réponse lors d'une sollicitation rare, notamment à l'issue d'un phénomène catastrophique (système dormant), et pour lesquels la possibilité d'intervention une fois le système mis en fonctionnement dans son environnement n'est plus envisageable (robot en centrale nucléaire, applications spatiales...).

Le modèle doit servir à l'évaluation de l'ensemble architecture – composant – répartition (architecture opérationnelle) retenu. Il doit permettre également de simuler le fonctionnement normal mais surtout de mettre en évidence les dysfonctionnements et les risques de fonctionnements dangereux ou catastrophiques.

Le modèle conçu, intégrant les points de vue de l'Automatique, du Génie Informatique et de la Sûreté de Fonctionnement, simulera certaines évolutions de la dynamique du processus.

L'évaluation s'inscrit à différents niveaux du système :

- au niveau du composant où il est possible de s'appuyer sur les méthodes classiques d'évaluation, tout au moins pour les systèmes "analogiques" (physique, mécanique, électronique, optique…),
- au niveau des composants "numériques", typiquement les composants intégrant des unités de calcul, où il est possible d'envisager une évaluation du composant "hors ligne" par retour d'expériences ou de connaissances fournies par les constructeurs, dans les cas les plus favorables,
- au niveau du réseau de communication, par une approche consistant à évaluer la probabilité d'occurrences d'erreurs sur les messages (trames) transmis ou les approches plus globales qui évaluent la probabilité de défaillir de nœuds appartenant à un grand réseau et la reconfiguration conséquente de ce dernier [HO 04]. Les travaux en rapport avec ce travail se focalisent en général sur ce que nous pouvons appeler la fonction

"communication" [*CI03c*]. A ce sujet, nous pouvons citer les approches consistant à évaluer le réseau lui-même en regard de la norme 61508 par exemple [CHA 02a] [FRO 03].
- à un niveau global permettant de prendre en compte l'état, l'évolution, du système.

Les objectifs consistent en la quantification de la sûreté de fonctionnement et de la sécurité de ces systèmes.

4.3. Sûreté de fonctionnement et SAID

A priori, la solution qui consiste à distribuer les traitements semble plus efficace du point de vue de la sûreté de fonctionnement [LAP 95] [VIL 88] qu'une architecture centralisée classique. En effet, la défaillance d'une unité de commande n'entraîne pas nécessairement l'arrêt de l'installation si une redistribution efficace de ses traitements vers les autres unités est réalisée.

Ce mécanisme de reprise est d'ailleurs facilité par l'emploi des réseaux de terrain capables de diffuser les informations vers tous les équipements. De même, de par la mise en place de certains traitements au plus près du processus (au niveau du capteur ou de l'actionneur intelligent), ces architectures pourraient être plus réactives à l'occurrence d'incidents et renforcer la fiabilité globale de l'installation. Enfin, les possibilités d'interrogation à distance sur l'état des composants apportent un plus grand confort dans le diagnostic et la surveillance de l'installation.

En revanche, de par leur complexité, ces systèmes peuvent également être sources de défaillances. Ainsi, la perte d'un message à un moment critique peut conduire à un arrêt indésirable du système.

Enfin la recherche d'une architecture optimale au sens de la plus grande disponibilité et faillibilité pour le moindre coût complexifie le problème de la conception. Le choix pertinent des fonctions et traitements à "redonder" est en effet délicat et doit s'appuyer sur une analyse des différents modes possibles de défaillances.

Les travaux portent sur le développement d'une méthodologie permettant d'établir l'architecture opérationnelle à partir des spécifications fonctionnelles. Ils requièrent, d'une part, une représentation informatique des traitements et de leur organisation et, d'autre part, des critères de jugement permettant une optimisation des architectures envisagées.

4.4. Sûreté de fonctionnement des constituants des SAID

Nous avons vu que sur le plan topologique, le SAID peut être considéré comme composé de divers instruments, unités de traitement et réseaux de communication. Par essence, ces constituants sont numériques donc à l'interface entre le monde de la physique ou de l'électronique analogique et le monde abstrait de l'informatique. Tour d'abord, nous pouvons dire que la prise en compte de cette interface n'est pas triviale. De plus, ces constituants devront être analysés dans les deux domaines, chacun de ces domaines pouvant apporter des risques de défaillances.

4.4.1. Réseau et sûreté de fonctionnement

Les réseaux sont une composante essentielle des systèmes distribués [ADO 01] [CIA 99] [JUA 02] [JUA 01] [JUA 99] [KRO 02] [*RI04a*] [*OU04*] [*CI98b*]. Différents aspects liés à la sûreté de fonctionnement peuvent être étudiés dans ce cadre et nécessitent d'être évalués : les aspects liés au respect temporel [HAN 98] [THO 00] [WIL 00] et à la notion de qualité de service appliquée aux réseaux de terrain [CHA 00], les critères évalués étant les temps de transfert des messages, la périodicité, le "*jitter*" (variation autour de la période spécifiée), la qualité de service [CHA 01].

Des comparaisons sont faites dans la littérature entre les principaux réseaux de terrain et l'Ethernet industriel pour des applications de type NCS (*Networked Control System* ou système commandé via des réseaux) [GEN 03] [JAS 01] [LIA 01] [POU 04].

4.4.1.1 Réseaux de terrain

Les réseaux de terrain sont des réseaux dédiés aux applications industrielles [CIA 99] [*OU04*], intégrant la plupart du temps des contraintes de temps réel bienvenues pour ce type d'applications. Sans entrer dans les détails, rappelons que les réseaux de terrain se sont développés à partir de la fin des années 1980, par la conjonction des développements de la technologie et des besoins des utilisateurs et en parallèle de l'évolution de l'électronique numérique, notamment ce que l'on a commencé à appeler à cette époque "composants intelligents" [BAY 94] [ROB 92] [SIM 99] [*CI97b*]. Après une tentative de normalisation des réseaux de terrain, les consortia ont finalement abouti à la norme 61158 [61158]. Cette norme est un catalogue de plusieurs milliers de pages

regroupant les spécifications des réseaux de terrain les plus connus : TS61158, ControlNet, Profibus, P-Net, Foundation Fieldbus [WIL 00], SwiftNet, WorldFIP [CAR 00] [TOV 00], Interbus [CHA 00] [PEY 00].

D'autres réseaux de terrain sont très répandus dans l'industrie, même s'ils ne font pas partie de cette norme [CIA 99], tels que CAN [ALM 00] [CAR 00] [CIS 01] [GAU 02] [KAI 00] [TRY 98].

4.4.1.2 Réseau Ethernet

Il est séduisant d'intégrer les technologies issues de l'internet dans une problématique "terrain", le principal avantage étant leur expansion et leur interopérabilité. L'inconvénient des protocoles standard de l'internet est la non garantie d'arrivée des messages dans une fenêtre temporelle bornée. Cela peut éventuellement être acceptable dans certaines applications industrielles mais est rédhibitoire dans des applications de sécurité ou à forte contrainte de criticité [DEC 04] [KRO 02] [LAN 02] [WAL 03].

Les switches, ou commutateurs, Ethernet [GRO 04] permettent d'introduire du déterminisme dans les réseaux Ethernet (principe CSMA/CD de la norme IEEE 802.3), ce qui peut satisfaire aux critères requis par certaines applications temps réel. Deux méthodes de commutation sont utilisées par ce type de switches :

- la méthode "*store and forward*" qui stocke une trame complète et la vérifie avant de la réémettre vers son destinataire,
- la méthode "*cut through*", ou méthode de commutation "à la volée", pour laquelle le switch commence à réémettre le début de la trame avant d'avoir reçu la totalité de celle-ci.

La première méthode est plus sûre, la seconde plus rapide mais sature davantage le réseau car de mauvaises trames peuvent être émises.

Le principe de base de ces switches est d'éviter les problèmes de collisions qui sont la cause du non déterminisme de l'ethernet en isolant des "domaines de collision", domaine à l'intérieur desquels le risque d'occurrence d'une collision entre deux trames est soit faible soit inexistant. Il faut se souvenir qu'il s'agit d'un déterminisme relatif, fortement lié à l'importance du trafic et à l'application.

Certaines équipes utilisent les réseaux de Petri colorés pour modéliser ce type de réseau [POU 04].

4.4.2. Capteurs et actionneurs

Les capteurs et actionneurs intelligents [BAY 94] [FRA 00] [ROB 93] [ROB 92] [TIA 01] (voir aussi chapitre suivant) peuvent jouer un rôle stratégique car :

- les capteurs, en intégrant de l'intelligence, sont capables de s'autodiagnostiquer et de fournir une information plus crédible [MKH 03],
- les actionneurs, en utilisant des procédures d'autotest, de tests externes ou de micro sollicitations (électrovanne de sécurité…) peuvent être plus sûrs.

Les systèmes commandés en réseaux [JUA 98] [WAL 01] [ZHA 01] [*CI03e, voir Annexe C papier 4*] [*CI98b*] ou NCS (Networked Control System) sont des systèmes pour lesquels la boucle de régulation intègre un réseau de communication. Dans l'approche SAID que nous privilégions, nous considérons que les composants sont distants du régulateur et que le réseau relie l'ensemble de ces composants.

4.4.3. Matériel et logiciel

Une approche qui est envisagée lorsqu'on aborde la modélisation d'un système est en général une approche qui consiste à avoir, d'une part, les spécialistes de la micro- ou nanoélectronique qui vont travailler sur l'évaluation et le test de cartes électroniques [CHU 99] [DAS 03] [JON 03] [LAL 03] [UPA 97] [*CI01*], d'autre part, des spécialistes du logiciel [ARL 00] [BLA 04] [CRA 03] [DWY 04] [FOU 93] [GUE 00] [GUL 04] [GUT 04] [SWA 04] [YIN 04] [YU 03] qui vont tester ou prouver les propriétés du logiciel. L'évaluation de l'implantation (ou implémentation), autrement dit de l'ensemble logiciel tel qu'il est implanté sur la machine reste à ce jour un problème ouvert qui se trouve également être dans les objectifs du RTP 21 (Sûreté de fonctionnement des systèmes informatiques complexes ouverts, animé par Jean ARLAT de Toulouse). Le RTP 21 se propose de travailler et de fédérer les deux communautés concernées par les thèmes de recherche ci-dessus. Ces approches ont pour limite le fait que le matériel et le logiciel sont traités séparément, des approches globales prenant en compte l'ensemble de ces aspects [AUB 99] semblent nécessaires.

4.5. Environnement des activités de recherche

Les activités que nous menons, à l'interface entre diverses communautés et problématiques –l'automatique, les systèmes d'information et la sûreté de fonctionnement– trouvent leur place dans le cadre local, régional, national, européen et international.

4.5.1. Au niveau local

Au niveau local, nos travaux se déroulent au CRAN au sein du groupe thématique SURFDIAG. Nous utilisons également des aspects développés dans le cadre du groupe thématique SYMPA (Systèmes de Production Ambiants) en particulier les projets liés aux réseaux ou aux systèmes à événements discrets.

Par ailleurs et par le biais du contrat de plan Etat-Région notamment, nous avons également des relations avec le LORIA (Laboratoire lorrain de recherche en informatique et ses applications), équipe TRIO (Temps Réel et InterOpérabilité) notamment.

4.5.2. Au niveau régional

Notre travail est directement appliqué au sein du Contrat de Plan Etat-Région des universités lorraines, dans le projet « Automatique et Prévention des Risques » pôle de recherches scientifique et technologique (PRST) “Sûreté Industrielle et Déchets“ du 4ème Contrat de Plan Etat Région Lorraine, où nous coopérons plus particulièrement avec le LORIA, mais également avec l'équipe ETIC (Equipe Transdisciplinaire sur l’Interaction et la Cognition) de Metz.

4.5.3. Au niveau national

Nous entretenons des relations avec l'ensemble des équipes qui participent aux travaux du groupe CIAME - groupe SEE 18-04 CIAME (Constituants Intelligents pour l'Automatisation et la Mesure) et à l'Action Spécifique "Méthode et modèle pour l’évaluation de la sûreté de fonctionnement des systèmes distribués". Cette action spécifique a été acceptée et a commencé à fonctionner début 2004 dans le cadre du RTP 55 "Systèmes de contrôle-commande et réseaux de communication"… Il s'agit des laboratoires suivants :

- LAGIS (ex LAIL) de Lille (M. BAYART, B. CONRARD), qui travaille sur les modèles de capteurs et actionneurs intelligents, ainsi que sur la modélisation de SAID, avec une vision proche de la nôtre,
- LISTIC (ex LAMII) d'Annecy (E. BENOIT, G. MAURIS, R. DAPOIGNIE), qui utilise notamment les théories floues et possibilistes ainsi que l'approche UML pour la modélisation et l'implantation de capteurs intelligents,
- LAMIH de Valenciennes (L. CAUFFRIEZ) qui travaille sur l'évaluation de la sûreté de fonctionnement, notamment appliquée à la fonction communication des réseaux,
- INSA de Lyon (I. BLUM) qui travaille sur des modèles de réseaux de communication,
- LCIS de Valence (D. GENON-CATALOT) qui implante des applications à base de réseaux de terrain et réseaux sans fil.

Les principales autres équipes françaises qui, d'une manière ou d'une autre, travaillent sur des thèmes proches des nôtres, sont :

- le LGP de Tarbes (D. NOYES) qui travaille notamment sur le développement de modèles conceptuels de données pour l'analyse de risques,
- le LAAS de Toulouse (R. VALETTE & G. JUANOLE) qui travaille entre autre sur la modélisation à base de réseaux de Petri, de protocoles de communication et de systèmes à événements discrets,
- le LURPA, de Cachan (J.J LESAGE et J.M FAURE) qui a proposé des travaux autour des automates programmables et travaille également sur la modélisation à base de réseaux de Petri colorés de réseaux Ethernet,
- le LAP, équipe ADS de Bordeaux (Y. DUTUIT) qui utilise également les réseaux de Petri dans une problématique de fiabilité dynamique,
- le LASQUO, d'Angers (B. DUMONT) qui travaille sur l'accélération de tests (vieillissement accéléré),
- le LAI de Lyon (E. NIEL),
- l'ISTIT, équipe M2S de Troyes (E. CHATELET, C. BERENGUER), qui travaille sur les aspects fiabilistes et la maintenance,
- le LAB de Besançon (N. ZERHOUNI), utlise des réseaux de Petri flous pour la surveillance,

- les RTP 20 (Fiabilité, diagnostic et tolérance aux fautes des systèmes complexes) et 21 (Sûreté de fonctionnement des systèmes informatiques complexes ouverts), en plus du RTP 55,
- …

4.5.4. Au niveau européen (PCRD)

Ci-dessous sont présentés succinctement quelques projets européens du 5ème ou 6ème PCRD :

- DEPAUDE : Dependability for embedded automation systems in dynamic environments with intra-site and inter-site distribution aspects (Geert Deconinck, Leuven, B) : ce projet traite des architectures de grands systèmes (type usine) plutôt sur le plan informatique et aborde des notions de qualité de service.
- DBENCH : Dependability Benchmarking (Karama Kanoun, Toulouse, F) : il s'agit du développement d'un cadre conceptuel pour l'étude (benchmark) des COTS (Commercial Off-The Shelf Software) et systèmes composés de COTS,
- DSOS : Dependable Systems Of Systems (Cliff JONES, Newcastle upon Tyne, GB) : il s'agit de construire un "système de systèmes" (ou macro-système) sûr à partir d'un ensemble de composants informatiques largement autonomes,
- FIT : Fault Injection for TTA (Herbert GRUENBACHER, Technikum Kärnten - Verein zur Errichtung der Fachhochschule Kärnten, School of Electronics, Spittal An der Drau, A) : ce projet a pour but la validation expérimentale de concepts d'architectures TTA (Time-Triggered Architectures) ; il est basé sur le chip TTP/C (time-triggered communication protocol), développé dans le cadre du projet ESPRIT TTA,
- NEXT TTA - high-confidence architecture for distributed control applications (Hermann KOPETZ, Technische Universität Wien) : il s'agit ici de développer la structure, les fonctionalités et la sûreté de fonctionnement de l'architecture TTA,
- SAFEGUARD: Intelligent AGents organisation to enhance Dependability and SUrvivAbility of large complex critical inFrastructurE (John BIGHAM, University of London, UK) : le but de ce projet est d'améliorer la sûreté de fonctionnement et la survivabilité de LCCIs (Large Complex Critical Infrastructures), telles que les réseaux de télécommunication et les réseaux de distribution électrique. Il s'agit de voir dans quelle mesure il est possible d'automatiser les fonctions de surveillance et de sécurité dans les grands systèmes automatisés pour lesquels ces fonctions sont souvent manuelles.

Les équipes européennes travaillant sur des sujets proches ou pouvant nous intéresser sont les suivantes :

- Université Libre de Bruxelles (Pierre-Etienne LABEAU) sur la fiabilité dynamique et la simulation de Monte-Carlo,
- *Politecnico de Milano* (Italie) (Marzio MARSEGUERRA et Enrico ZIO) sur la simulation de Monte-Carlo [MAR 04] [ZIO 04].
- *Dipartimento di Informatica (DI), Università del Piemonte Orientale* (Andrea BOBBIO) [BOB 99] sur les Réseaux de Petri,
- *České vysoké učení technické v Praze (ČVUT)* (Université technique de Prague) (Zdenek HANZALEK) (CZ), sur les réseaux de Petri,
- *Technická univerzita Košice* (Université Technologique de Košice) (Jan LIGUS) (SK) sur la modélisation des NCS,
- *Politechnika Rzeszowska* (Université de de Rzseszów) (Leszek *TRYBUS*) (PL) sur les réseaux de terrain et la modélisation des systèmes a événements discrets.

Nous avons principalement des relations avec Košice et quelques-unes avec Rzseszów.

4.5.5. Au niveau international

Un certain nombre d'équipes internationales travaillent sur des sujets connexes :

- *Department of Electrical and Computer Engineering, Duke University, Durham, NC* (USA) (Kishor S. TRIVEDI (US) [TRI 03], qui propose des modèles à base de réseaux de Petri stochastiques et des chaînes de Markov,
- *Troy State University Montgomery* (USA) (Mehmet ŞAHINOGLU) [ŞAH 04] qui a propose une méthode permettant d'estimer la fiabilité et la disponibilité d'un réseau,
- *Georgia Institute of Technology* (USA) (Vitali VOLOVOI) [VOL 04a] [VOL 04b] sur les RdP stochastiques appliqués à la SdF, et sur l'utilisation des "réseaux à jetons vieillissants" (*Ageing Petri nets*) pour la modélisation des systèmes à plusieurs modes de fonctionnement,
- *Department of Computer Science*, *Oklahoma State University* (USA) (Nohpill PARK) [CHO 02a] [CHO 02b] qui travaille principalement sur les aspects de tests de circuits électroniques.

- *Curtin University of Technology* (Australia) (Halit EREN) effectue de la mesure par traitement du signal.

J'ai eu l'occasion de rencontrer, de manière informelle, Kishor S. TRIVEDI, Mehmet ŞAHINOGLU, Nohpill PARK et Halit EREN.

4.6. Conclusion

Conformément à ce qui a été décrit précédemment, nous pouvons dire que les méthodes de sûreté de fonctionnement d'"architectures" un tant soit peu complexes se focalisent en général sur l'analyse des topologies comme étant des combinaisons série ou parallèle de composants de base, chacun ayant son propre comportement. Divers problèmes se posent liés à l'interopérabilité [THO 94], aux "liaisons" et "connexions" entre les composants et ces problèmes n'ont pas de solution triviale.

Si nous considérons une simple boucle ouverte au sens de l'automatique, intégrant un réseau de communication [ALI 02] entre le capteur et le contrôleur, puis entre le contrôleur et l'actionneur, le réseau apparaît deux fois dans l'architecture et l'évaluation doit prendre en compte cet aspect, les aspects modes communs étant en ce cas importants [BER 02] [CHA 02c].

De plus, l'évaluation de la boucle fermée, y compris sans réseau d'ailleurs, n'est pas un problème trivial, à cause des phénomènes de rebouclage.

Concernant les méthodes d'évaluation, les approches privilégient en général une coopération entre les méthodes formelles, qui présentent l'intérêt de pouvoir être exhaustives mais sont souvent peu compatibles avec la complexité des systèmes réels, et les approches liées à la simulation, qui permettent de mettre en évidence des situations rares mais ne peuvent jamais prétendre à l'exhaustivité [BOD 98]. Ces méthodes peuvent toutefois être combinées à des injections de défaillances [ROD 02]. Il nous faudra par conséquent tenter de mettre en œuvre une combinaison de méthodes.

En prenant en compte l'ensemble des problèmes décrits dans ce chapitre, il est possible d'avoir une idée de l'ampleur du problème de la modélisation des SAID. Utiliser la modélisation à des fins d'évaluation, soit exhaustive dans les cas les plus favorables, soit par le *biais* de la simulation, n'est pas une idée nouvelle. La progression continue des méthodologies et des outils [SIG 96] a en effet ouvert la porte à une telle démarche.

Nous avons également considéré dans ce chapitre l'environnement scientifique local, national et international dans lequel notre recherche se déroule.

5. Contributions dans les domaines de l'instrumentation intelligente et des réseaux

Ce chapitre présente des activités de recherche qui ont été menées ces dernières années dans les domaines de l'instrumentation intelligente et des réseaux. Les contributions décrites ici n'ont pas fait l'objet de co-encadrements doctoraux et sont donc des contributions plus mineures que celles du chapitre suivant, autour de la thématique de recherche à laquelle nous travaillons.

Les instruments intelligents et les réseaux sont les composants de base autour desquels se construisent les SAID. Les activités les plus anciennes, autour de l'instrumentation intelligente et des applications dans le domaine du génie urbain, ont été développées dans la poursuite de mes travaux de thèse et dans la mouvance de travaux d'actualité à l'époque [BAY 95]. Les travaux plus récents, autour des concepts de réseau de sécurité et de l'utilisation de réseaux de communication ou de réseaux de terrain pour des applications critique ou de sécurité, ont quant à eux été développés dans la mouvance de discussions avec l'INRS et des travaux du groupe de travail national CIAME.

Ce chapitre se compose de trois parties :
- une partie traitant de l'instrumentation intelligente,
- une partie développant les contributions sur l'utilisation de réseaux,
- une dernière partie traitant d'une contribution sur la définition d'un système d'informations urbain.

Dans la poursuite de mes travaux de thèse, qui concernaient l'étude et l'analyse d'anomalies de trafic en milieu urbain, et à titre d'application des concepts **d'instrumentation intelligente** développés dans l'équipe, j'ai participé à la définition d'un capteur de trafic intelligent. Une contribution, en partenariat avec le CERTU (Centre d'Etudes sur les Réseaux, les Transports, l'Urbanisme et les constructions publiques) a permis de montrer l'intérêt et les limites de l'utilisation d'instruments intelligents dans le domaine du trafic urbain. Ce travail a fait l'objet d'un contrat avec le CERTU (1994) [*Rc94*] ainsi que du co-encadrement d'un étudiant sur ce projet après son DEA (A. FILALI).

Beaucoup plus récemment (2000-2003), une coopération avec l'UTBM (Université de Technologie de Belfort-Montbéliard) a permis de proposer un modèle neuronal de supervision du trafic. Ce travail m'a permis de contribuer au travail de thèse de N. MESSAI [MES 03] ; pour ma part relative à ce travail, je suis co-auteur d'une communication [CI00b] et ai été invité à participer au jury de thèse de N. MESSAI.

La seconde partie regroupe les divers travaux que j'ai pu menés, dans le cadre local ou au sein du groupe CIAME, sur les **réseaux de terrain**, leurs sûreté de fonctionnement, autrement dit la sûreté de fonctionnement de la fonction communication, ainsi que les réseaux de terrain de sécurité.

Une contribution en partenariat avec le CERTU a permis de montrer l'intérêt et les limites de l'utilisation de réseaux de terrain dans le domaine du trafic urbain. Cette contribution a donné lieu à un contrat avec le CERTU (1998) et au co-encadrement du stage orienté recherche de N. DELAHAYE (1998) [*Rc98b*]. Cette étude a permis la rédaction d'une communication internationale [*CI98d*].

L'utilisation de réseaux de terrain dans des applications "sûres", de même que l'utilisation de réseaux de terrain directement dans des applications de sécurité est une démarche intéressante lorsqu'on envisage la conception de SAID. De plus, une convergence d'intérêt a émergé de discussions avec l'I.N.R.S. (Institut National de Recherche et de Sécurité) relatifs à l'évaluation du niveau de sécurité des réseaux de terrains dits de sécurité ou *safe* [REI 01] [SCH 99]. Nous avons effectué dans ce cadre une étude du réseau de terrain de sécurité ASi-Safety at Work. Ce travail a fait l'objet du co-encadrement du stage orienté recherche de S. QUENTIN en 2003 et du stage de DEA de A. KONATE en 2004, sur ProfiSafe.

Un partenariat avec l'université de Košice (Slovaquie), matérialisé par la visite de trois mois de J. LIGUSOVA à Nancy en 2003 et une communication [*CI04a, voir Annexe C papier 5*] a permis d'entrevoir l'interaction entre les composants et le réseau, dans une vision SAID, cette étude propose une étude de l'influence du mode d'initialisation du réseau sur la sûreté de fonctionnement.

Ce chapitre se termine par une étude effectuée dans le cadre d'un projet européen [*Rc98a*], pour la définition d'un **système d'information** utilisable pour tous types d'utilisateurs internes et externes et fournissant diverses informations concernant la ville. Il s'agit ici d'une approche plus orientée réseau régional et système d'information.

5.1. Contributions relatives à l'instrumentation intelligente

5.1.1. Intelligence dans un capteur

En France, des chercheurs, en collaboration avec des utilisateurs et des fabricants ont écrit un livre blanc [CIA 87] qui contient ce qui doit être fait pour rendre un capteur intelligent. L'utilisateur a besoin d'un capteur idéal qui devrait posséder les propriétés suivantes [ROB 93] [*CS95*] :

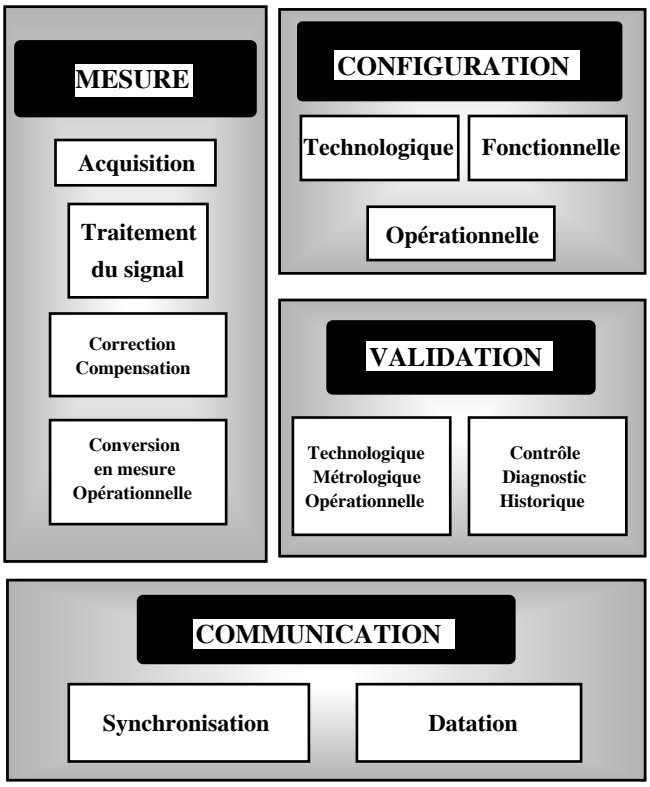


Figure 5.1 – Fonctionnalités d'un capteur intelligent

- être crédible [DEL 92], cela signifie que le capteur est capable de reconnaître et de renseigner sur son état (correct ou non),
- fournir une mesure datée,
- être interopérable : différentes unités sont capables d'échanger et d'interpréter des données sans nécessiter de transcriptions particulières,
- être interexploitable : deux composants sont suffisamment similaires pour pouvoir être remplacés l'un par l'autre, même si leurs fonctionnements internes sont différents,
- être interchangeable : l'équipement d'un fabricant peut être remplacé par le composant d'un autre fabricant sans altérer les comportements prévus,
- préserver une compatibilité ascendante.

Les quatre services attendus d'un capteur intelligent sont liés à quatre domaines représentés figure 5.1 [ROB 93] :

5.1.1.1 Mesure

Cette fonction ne signifie pas simplement effectuer la mesure mais implique également de prendre en compte la gestion de l'information, c'est-à-dire :

- produire de l'information : recueillir des données provenant du transducteur, les traiter, élaborer les paramètres les plus pertinents,
- stocker l'information dans une base de donnée et fournir aux utilisateurs autorisés un accès aisé à ces données,
- distribuer de manière astucieuse l'information là où elle est nécessaire, quand elle est nécessaire,
- mettre à jour les bases : gérer des bases de données afin de détruire les information obsolètes, soit parce qu'elles sont trop anciennes, soit parce qu'elles ne présentent plus d'intérêt.

Le mesurande est la quantité que l'on veut effectivement mesurer, les grandeurs d'influence sont des mesures secondaires effectuées afin de corriger le mesurande, les grandeurs d'auto-contrôle permettent de caractériser le fonctionnement du capteur, le temps permet la datation de la mesure.

De ces grandeurs, on peut extraire les mesures suivantes, chacune d'entre elles devant être datée :
- la mesure primaire (information fournie par le transducteur : par exemple la température),
- la mesure auxiliaire (par exemple l'âge du transducteur qui peut altérer la mesure),
- la mesure technologique (ex : test de l'alimentation),
- la mesure fonctionnelle est une mesure intermédiaire tenant compte des grandeurs d'influence (ex : température corrigée par la pression mesurée),
- la mesure validée prend en compte tous les événements mesurés (ex : température corrigée par la pression mesurée après avoir vérifié que l'alimentation est correcte).

Cette information produit une mesure opérationnelle. Cette mesure opérationnelle est la quantité significative pour le système, élaborée avec sa propre unité et, si nécessaire, à partir de plusieurs points de mesure, en tout état de cause dans le référentiel désiré par l'utilisateur.

5.1.1.2 Validation

D'après le livre blanc [CIA 87], la fonctionnalité validation est indissociable de la fonctionnalité mesure, cette particularité étant la principale différence avec un capteur classique. Une contribution à l'intelligence est la connaissance, à tout instant, des conditions dans lesquelles se sont déroulées les mesures. Le problème reste la détermination du moment où on stoppe la validation, avec un certain niveau de confiance.

Valider la mesure signifie lui attribuer un certain niveau de crédibilité et de confiance. La validation peut concerner une mesure par elle-même (contrôle des connexions électriques, alimentation, ...) ou peut être réalisée avec un point de vue plus global (corrélations ou opérations statistiques avec des mesures issues d'autres sources ...).

5.1.1.3 Configuration

Cette fonctionnalité peut être requise par le constructeur, l'installateur ou l'utilisateur dans les différentes phases du cycle de vie d'un capteur. La configuration est le résultat d'un ensemble d'actions et de leurs validations.
- la configuration technologique a pour but d'intégrer le capteur dans son environnement physique (alimentation),
- la configuration fonctionnelle permet de donner aux capteurs la possibilité de mesurer et de communiquer (choix de protocoles ...),
- la configuration opérationnelle dédie le capteur à une application particulière (choix d'unité, référentiel de l'utilisateur).

5.1.1.4 Communication

Les capteurs intelligents disposent d'une interface de communication [GEH 94] qui permet la communication avec divers interlocuteurs, d'autres capteurs, avec une base de données, avec un ordinateur, ... Ces aspects sont développés plus en détail dans le chapitre suivant.

5.1.2. Définition d'un capteur intelligent de trafic

Il s'agit d'extraire et d'améliorer des paramètres à partir de l'information brute émise par les capteurs de trafic, en particulier les boucles inductives qui sont de loin le capteur de trafic le plus répandu. La méthode proposée permet d'envisager une stratégie de commande plus fine des carrefours en milieu urbain. Ces travaux avaient fait l'objet d'un contrat avec le CERTU (Centre d'Etudes sur les Réseaux, les Transports, l'Urbanisme et les constructions publiques, dépendant du Ministère français des Transports), intitulé "Le recueil de données dans le domaine du trafic routier et urbain : les besoins, l'existant, les perspectives" [*CS95*] [*Rc94*].

La poursuite de ces travaux a fait l'objet d'une communication en 2001 [*CN01a, voir Annexe C papier 3*] et d'une soumission dans une revue.

Les principaux résultats concernent la définition d'une fenêtre temporelle calibrée sur les cycles de feux tricolores en fonction de la topologie des carrefours. Cette fenêtre temporelle est subdivisée en diverses parties pouvant être caractérisées par des comportements typiques de trafic. L'intérêt de cette fenêtre est que, grâce à ces parties, il est possible de détecter divers comportements et dysfonctionnements de trafic et, par conséquent, de déduire l'existence d'anomalies de trafic, avec une bonne performance et un temps de réaction très court, en fait plus court qu'un temps de cycle…

5.1.2.1 Présentation

Dans les systèmes actuels de régulation de trafic urbain, la boucle électromagnétique noyée dans la chaussée demeure de loin le capteur le plus répandu. Les principales raisons sont la facilité de mise en œuvre et d'utilisation.

Cependant, l'exploitation des données issues de ce capteur présente quelques insuffisances principalement liées au manque de pertinence et de validité de l'information obtenue.

Sans accroître la complexité technologique de ces capteurs, il est possible d'envisager des améliorations significatives de l'information perçue, reposant sur le concept d'instrumentation intelligente.

5.1.2.2 Boucle électromagnétique et détecteur associé

Une boucle électromagnétique est composée d'un transducteur, généralement associé à un détecteur.

Le transducteur est un fil noyé dans la chaussée et enroulé de manière à constituer des spires (cf. figure 5.2).

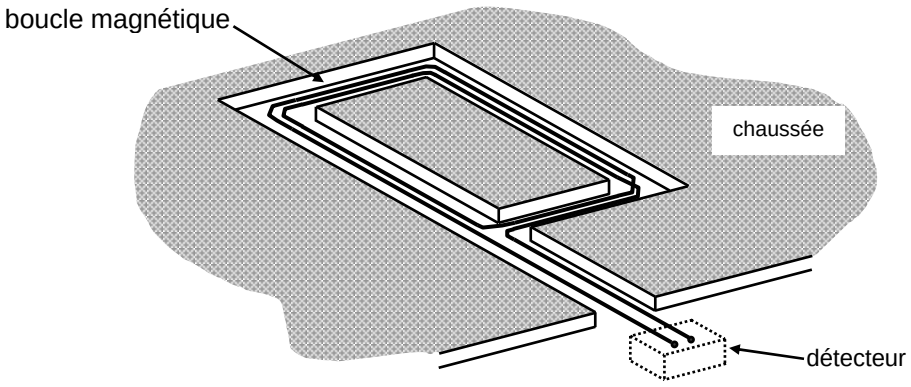


Figure 5.2 – La boucle électromagnétique et le détecteur associé

Un courant circulant dans ces spires crée un champ magnétique modifié lors du passage d'un véhicule au-dessus de la boucle (cf. figure 5.3).

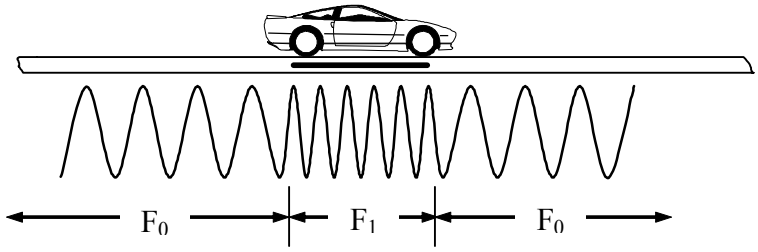


Figure 5.3 – Modification du champ magnétique lors du passage d'un véhicule

Un détecteur récupère et limite le signal lié à la modification du champ magnétique afin d'obtenir une donnée d'occupation ou de non-occupation instantanée de la boucle.

La position des boucles électromagnétiques est fonction du rôle qui leur est assigné :
- boucle de micro-régulation,
- boucle de limitation de vitesse et de sélection véhicule léger/poids lourd,
- boucle destinée à l'analyse de trafic.

D'autres configurations de boucles sont également possibles en fonction des objectifs visés [COH 90].

Enfin, il est important de noter que les boucles électromagnétiques sont des capteurs ponctuels : cela signifie qu'elles ne " voient " que ce qui se passe en un point, contrairement aux caméras par exemple.

5.1.2.3 Etats des lieux : la boucle face aux autres capteurs

Différents types de capteurs peuvent être utilisés en régulation de trafic. Les capteurs les plus courants [BLO 96] [COH 99] sont soit posés ou implantés au sol, soit installés en l'air. Dans la première catégorie, outre les tubes pneumatiques utilisés pour effectuer des comptages pour des durées limitées, se trouvent le capteur piézo-électrique et la fibre optique qui permettent de discriminer les véhicules par type. La seconde catégorie regroupe les détecteurs acoustiques à ultrasons, les radars à effet Doppler-Fizeau, les détecteurs infrarouges ou les émetteurs-récepteurs à hyperfréquences.

Les autres techniques sont basées sur le traitement d'images ou n'utilisent pas directement des capteurs (au sens traditionnel du terme), telles que les " véhicules flottants " et l'utilisation de la photographie aérienne.

5.1.2.4 Capteur intelligent pour la régulation du trafic

Nous avons vu que l'instrumentation intelligente apporte une solution aux nombreux problèmes rencontrés dans la conduite des procédés industriels [*RI96*] :
- quelle crédibilité accordée aux informations issues des capteurs ?
- quel est l'état de fonctionnement du capteur ?
- l'actionneur a-t-il correctement exécuté une requête ?
- quel est l'état de fonctionnement de l'actionneur ?

…

Les améliorations attendues de l'utilisation de l'instrumentation intelligente sur la boucle électromagnétique et le détecteur associé [*CI98d*] sont, d'une part, une amélioration de la crédibilité de l'information perçue au niveau des systèmes de régulation et, d'autre part, l'obtention d'informations supplémentaires représentatives de l'état du trafic.

Les nouvelles fonctionnalités de ce capteur intelligent sont donc :
- donner une information opérationnelle, c'est-à-dire directement exploitable, plutôt que des mesures brutes [ROB 93]. Il est possible de tirer avantage de la nature différente des informations délivrées par les détecteurs mentionnés précédemment ou même de les mettre à contribution dans le but d'améliorer la mesure.
- indiquer une défaillance et pouvoir s'auto-diagnostiquer. Là aussi, plusieurs approches sont couplées, une approche simple de test de la réponse de la boucle au passage d'un courant afin de valider le transducteur lui-même, couplé à une méthode d'analyse des données reçues pour mettre en évidence certains modes de dysfonctionnement de la boucle.

5.1.2.5 Traitement des données

Les données obtenues sur le système de régulation de trafic de la Ville de Nancy consistent en l'acquisition en temps réel avec une période d'acquisition de 0,1 seconde de l'état des feux tricolores ainsi que de l'occupation instantanée des capteurs électromagnétiques. Environ 140 carrefours et 200 boucles électromagnétiques sont ainsi surveillés. Les systèmes étant basés habituellement sur l'acquisition des données brutes vers les centraux d'acquisition, il s'agit ici d'accroître les capacités de traitement local afin, par exemple, de mettre en place des stratégies de micro-régulation et de tendre ainsi vers une structure autonome remontant des données utiles à la surveillance et à la supervision.

L'exploitation des mesures a pour objectifs essentiellement la surveillance et l'analyse de trafic. L'apport de la démarche consiste en l'élaboration de paramètres pertinents et validés représentatifs de l'évolution du trafic.

Ainsi, dans les phases de surveillance et d'analyse du trafic, il est possible à partir de la vitesse estimée des véhicules, de distinguer différents comportements de trafic :

- phase de démarrage des véhicules,
- phase où les véhicules ont atteint leurs vitesses de croisière,
- phase de décélération,
- phase pendant laquelle quelques véhicules franchissent la boucle pendant le temps de rouge (fonction de l'implantation relative du feu et de la boucle).

5.1.2.6 Etats de trafic et mise en évidence d'anomalies

Les comportements de trafic décrits dans le paragraphe précédent permettent de caractériser des régimes de trafic.

Ces différents régimes sont illustrés sur la figure 5.4. Cet exemple a été tracé à partir d'une acquisition de données de trois minutes, soit la durée de deux cycles de feux. Les valeurs numériques caractérisant les régimes (appelée Re) sont arbitraires et ont pour but simplement d'aider à les distinguer.

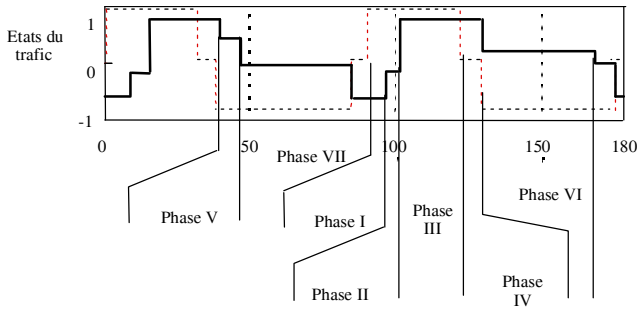


Figure 5.4 – Différents régimes de trafic

Re = -0,7 :	début de cycle, temps de décalage	Phase I
Re = -0,2 :	phase de démarrage	Phase II
Re = 0,9 :	régime établi	Phases III & IV
Re = 0,7 :	phase de ralentissement	Phase V
Re = 0,2 :	remplissage du sas	Phase VI
Re = 0 :	sas rempli	Phase VII

En fonction de ces différents régimes, il est possible de détecter des dysfonctionnements de manière beaucoup plus pertinente en temps quasi-réel car le résultat peut être élaboré et obtenu avant la fin du cycle.

Le tableau 5.1 propose une description des types de situations détectables par phase.

5.1.2.7 Intérêt de la méthode

Comme cela a été montré, il est possible d'améliorer l'information perçue provenant des boucles électromagnétiques, le tout sans avoir trop de dépenses d'infrastructure. En effet, la méthode proposée s'appuie sur l'existant, surtout dans le cas de la micro-régulation.

Les progrès récents des technologies liées à l'utilisation des instruments intelligents apportent, grâce à un traitement local adapté, l'élaboration de paramètres plus pertinents pouvant servir en micro-régulation ou pour une stratégie plus globale.

Le capteur intelligent de trafic fournit une information plus riche permettant l'élaboration de paramètres dynamiquement par l'amélioration de la confiance accordée aux variables. De ce fait, il est possible d'envisager un système de traitement de cette information plus performant et, notamment dans le domaine urbain, une stratégie de régulation de trafic temps réel qui puisse prendre en compte ces informations plus riches.

Les phases	Situations détectables par phase
I) DECALAGE Attente après le début de vert que le véhicule qui est sur la boucle la quitte.	Si le taux d'occupation = 1 alors la circulation dense. Si l'occupation <> 0 et <> 1, ce cas signifie que pendant le décalage, un ou plusieurs véhicules sont passés sur la boucle mais ne sont pas restés dessus. Si l'occupation = 0 alors la circulation est relativement fluide car le sas n'est pas rempli en fin de cycle.
II) PHASE DE DEMARRAGE Existe si l'occupation = 1 à la fin du décalage, sinon facultative.	Si l'occupation = 1 à la fin du décalage et que le véhicule ne quitte pas la boucle, nous sommes en présence de la source d'une anomalie de trafic possible accidentelle si seule cette boucle est concernée ou si la boucle reste bloquée à 1. Si les boucles adjacentes ou aval sont également concernées, nous sommes en présence d'une congestion. La vitesse augmente pendant cette phase. Si la durée est trop longue avec un passage de véhicules, alors les conditions de circulation ne sont pas bonnes, il peut s'agir d'une anomalie accidentelle si seule cette boucle est concernée, ou d'une congestion ou de mauvaises conditions de circulation si les boucles adjacentes ou aval sont dans le même cas. Si la durée est trop longue parce qu'il n'y a pas de véhicule, nous ne pouvons rien conclure. L'étude du temps mis par le véhicule qui est bloqué sur la boucle au feu rouge pour quitter celle-ci après que le feu soit passé au vert peut donner des information complémentaires ; cette notion est fonction de la distance boucle-feu.
III & IV) REGIME ETABLI Evolution de la vitesse moyenne => À la fin du régime établi, nous obtenons la vitesse moyenne en régime établi. Les phases III et IV sont en réalité une même phase en terme de comportement des véhicules, seul l'état du feu explique le changement.	Etude de la dégradation du carrefour par observation de la dégradation de la vitesse moyenne mesurée pendant la période de régime établi. Il existe en effet une corrélation directe entre la vitesse moyenne en régime établi et la fluidité du carrefour. Etant donné notre manière de calculer la vitesse, nous ne pouvons tenir compte que de la vitesse moyenne calculée sur plusieurs véhicules.
V) DECELERATION VI) REMPLISSAGE DU SAS	En phase de ralentissement ou de remplissage de sas, nous pouvons avoir une idée de la fluidité du trafic en mesurant le temps mis pour remplir le sas ou en mesurant le taux d'occupation pendant ce temps.
VII) SAS REMPLI	Si les phases V et VI sont courtes => circulation dense.

Tableau 5.1 – Situations détectables en fonction des régimes de trafic

5.1.3. Modèle de supervision de trafic à base de réseaux neuronaux

Dans ce cadre, nous avons travaillé avec Dimitri LEFEBVRE (actuellement à l'Université du Havre) et Philippe THOMAS de l'UTBM (Université de Technologie de Belfort-Montbéliard) à une étude sur la "modélisation et la surveillance du trafic urbain par réseaux de neurones" qui a fait l'objet d'un DEA puis d'une thèse préparés à l'UTBM par Nadhir MESSAI. Il s'agissait d'appliquer les techniques des réseaux de neurones maîtrisées par les partenaires belfortains au contexte des données trafic sur lequel j'ai apporté mon savoir-faire. Ce travail a débouché sur une communication commune [*CI00b*]. La thèse de Nadhir MESSAI, intitulée "Surveillance de trafic urbain et interurbain à bases de modèles neuronaux" a été soutenue le 17 décembre 2003 et j'ai eu le plaisir d'avoir été invité au jury de la thèse.

La principale contribution concerne la proposition d'un réseau de supervision statique basé sur le diagramme fondamental (DF) flux-densité. Différents modèles de diagrammes fondamentaux ont été utilisés dans ce travail et l'analyse de ces modèles indique que tous les DF obtenus convergent vers une forme de type STRADA [BUI 96] [MES 93].

Ce résultat est conforme à la littérature [BUI 96] et indique que le DF de STRADA est bien adapté aux carrefours complexes et montre la pertinence de l'approche de modélisation proposée. De plus, l'estimation des paramètres de l'infrastructure, à partir de ces DF, montre que malgré la forte dispersion des données, les vitesses libres, les débits maximaux, les densités critiques et les densités maximales possèdent généralement des valeurs

cohérentes avec la largeur des voies du carrefour et les normes de sécurité en France. Cependant, il est remarquable que le DF de la boucle B1 (cf. les représentations fig. 5.5) possède une densité maximale inadmissible physiquement. Ce problème est en effet dû au fait que le jeu d'apprentissage contient uniquement deux données en régime saturé et que ces deux mesures qui correspondent vraisemblablement à des défauts n'ont pas été considérés, lors de l'apprentissage, comme étant des valeurs aberrantes.

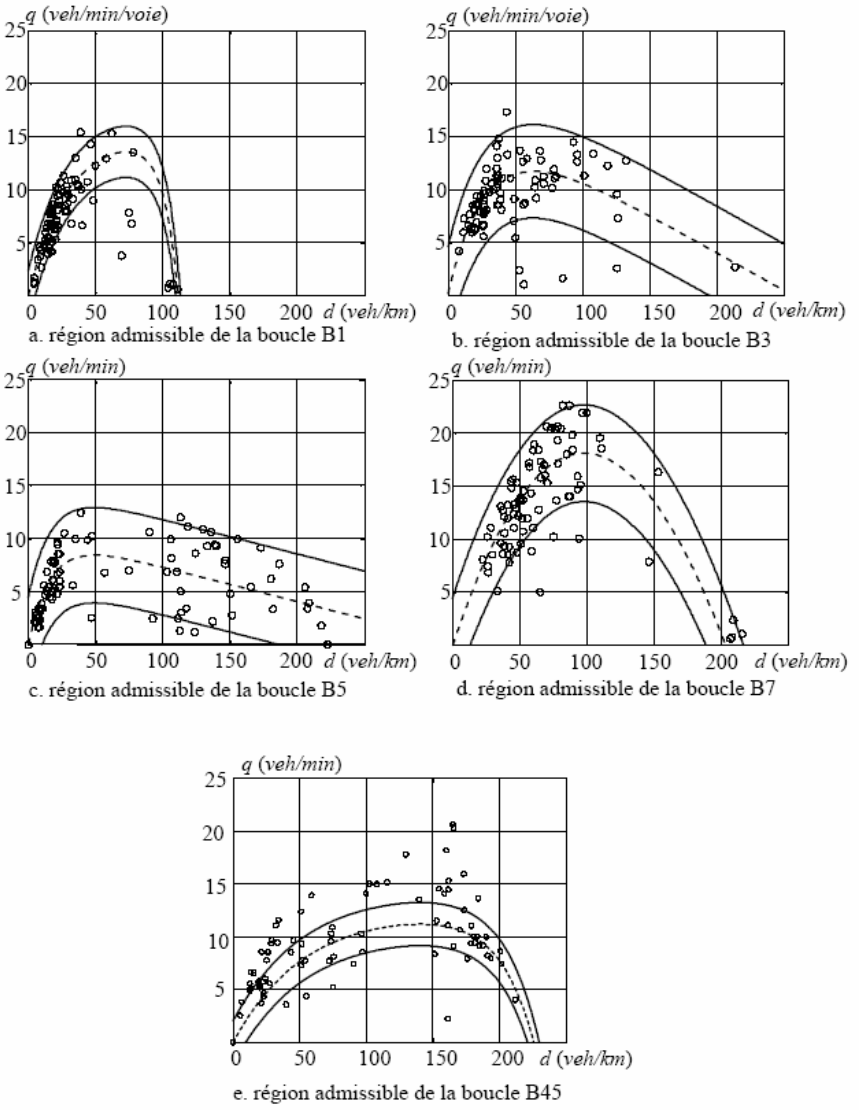


Figure 5.5 – Régions admissibles des boucles de carrefour C38

Une région admissible centrée autour de ce diagramme a été définie. Les variables de flux et de densité mesurées ont été reportées dans l'espace flux-densité dans le but de détecter et d'isoler les incidents qui perturbent le trafic. Le principal intérêt de la méthode proposée est de permettre une supervision locale de chaque capteur. Il n'est donc pas nécessaire d'avoir plusieurs capteurs. La supervision a été définie tout d'abord comme une simple fonction logique puis un réseau de neurones a été utilisé. Les avantages majeurs de ce dernier concernent le parallélisme massif ainsi que les propriétés de classification qui ont été utilisées pour satisfaire les contraintes de temps réel de ces applications de supervision.

Diverses publications sont disponibles sur ce sujet : [CRE 81] [JAY 94] [LEF 99] [LEU 88] [WID 90], [*CN95*].

5.2. Réseaux de terrain et sécurité

5.2.1. Réseaux de terrain et transports

La problématique de la distribution des traitements et des informations présente des similitudes tant dans les systèmes d'information de certains systèmes de régulation de trafic urbain que dans les systèmes d'information des procédés industriels intégrant des réseaux de terrain et des instruments intelligents. Cette problématique est : comment distribuer les informations et les traitements sous les contraintes temporelles, matérielles, de sûreté de fonctionnement, etc. [*CI98d*, *CI96d*, *CI96b*, *CI95a*]... C'est ainsi que les connaissances acquises antérieurement ont été mises à profit en vue d'utiliser le système de régulation du trafic urbain ou un système intégré de gestion et de régulation du trafic comme terrain d'expérimentation de cette problématique SAID. Nous avons travaillé, dans le cadre d'un contrat avec le CERTU sur une "Etude des caractéristiques des Systèmes de régulation de trafic urbain : architecture et protocoles de transmissions - performances et possibilités d'évolution". L'objectif consistait à effectuer une étude des principaux systèmes de régulation de trafic urbain et de les comparer en terme d'architecture et de protocoles de transmission afin de dégager pour l'utilisateur potentiel des critères de performances et de modularité. Ce travail a fait l'objet d'un rapport de contrat et d'une communication [*CI98d*, *Rc98b*].

5.2.1.1 Résultats obtenus

Les principaux manques des systèmes de régulation du trafic urbain sont en général les suivants [*CI98d*] :

- interopérabilité des composants : il n'est souvent guère possible de remplacer un composant ancien par un composant plus récent ou provenant d'un autre constructeur,
- interopérabilité des protocoles de communication : la communication n'est pas aisée entre différents systèmes provenant de différents constructeurs, par exemple entre un système de régulation de trafic et un système d'aide à l'exploitation pour les transports en commun,
- architecture : une architecture fermée de type liaisons point à point ne permet pas facilement d'ajouter un nouveau composant : nouveau carrefour, intégration d'un nouveau Système d'Aide à l'Exploitation des transports publics, intégration d'un système dédié au traitement de la saturation.

Ces aspects entraînent l'impossibilité pour le système d'évoluer aussi vite que la technologie. Les collectivités locales ont alors le choix entre remplacer la totalité du système ou se contenter d'évolutions limitées.

Après cette analyse, nous pouvons mettre en évidence certaines propriétés de ce que devrait être l'architecture fonctionnelle et matérielle d'un système de régulation du trafic urbain prenant en compte les remarques précédentes.

- Réseau : mise en place d'un réseau basé sur un trafic périodique pour pouvoir répondre à la contrainte de temps réel. Une solution intéressante peut être l'installation dans la ville d'un réseau métropolitain global capable de transmettre différents types d'information : information sur le trafic, stations de mesures, télévision par câble, téléphone …
- Architecture : une architecture distribuée propose l'addition ou la suppression de n'importe quel composant sans altérer le fonctionnement global du système. Un besoin de standardisation se fait sentir pour tendre vers l'interopérabilité de composants d'origines diverses. Des travaux sont en cours tant dans l'Union Européenne qu'aux Etats-Unis ou en Australie sur ce sujet.
- Protocole : il est nécessaire de standardiser également les protocoles de communication afin de favoriser les échanges entre différents systèmes : système de régulation, système de transport public, guidage, panneaux à messages variables… Une norme française est utilisée pour le recueil de données (TEDI) et des programmes européens se sont également intéressés au problème (STRADA).

5.2.1.2 Commentaires

Les principaux résultats ont montré les problèmes d'interopérabilité des systèmes de régulation de trafic urbain existants, ce qui oblige en général les collectivités locales à se lier à un constructeur. Par ailleurs, l'autre grande difficulté concerne l'obsolescence des matériels et la difficulté à évoluer en regard des progrès technologiques. Ces constatations nous ont amenés à proposer quelques solutions basées sur des approches développées dans d'autres contextes.

L'utilisation d'une telle approche peut également nous entraîner à proposer une stratégie plus pertinente pour le système de régulation de trafic, améliorant la détection des anomalies de trafic.

Concernant la communication, les normes existantes ont montré leur insuffisance pour permettre une réelle communication entre les systèmes provenant de différents fabricants. Toutefois, la tendance aussi bien dans l'Union Européenne qu'aux Etats-Unis est de proposer des normes adaptées aux besoins de la gestion et de la régulation du trafic, qui soient utilisées par tous les constructeurs ; ces normes utilisent les protocoles de l'internet (TCP/IP, SNMP…).

La remarque générale que l'on peut faire par comparaison entre l'état de l'art dans le domaine du trafic et le domaine industriel est l'existence d'un certain retard dans le domaine urbain conséquence vraisemblable d'un marché plus restreint et de la nécessité de travaux d'infrastructure importants pour faire évoluer les systèmes.

5.2.2. Evaluation de réseaux de terrain de sécurité

Faire bénéficier les applications dédiées sécurité des avancées des systèmes de commande distribués à intelligence répartie exige de maîtriser la sûreté de fonctionnement de ces derniers. Un premier pas doit donc être franchi pour fournir des modèles d'évaluation de performances des réseaux de terrain en terme de sécurité fonctionnelle [*CN03a*].

Un groupe de travail CRAN INRS s'est mis en place pour y travailler. Un étudiant-ingénieur, Quentin SEBASTIEN [SEB 03], en partenariat avec P. BARGER, a proposé en 2002-03 une "Evaluation du niveau de sécurité d'une architecture distribuée à l'aide d'une modélisation par réseaux de Petri". Il s'agissait d'évaluer le réseau de terrain *ASISafe*, en regard de la description faite par la norme. Le travail a montré les "limites" et "insuffisances" des spécifications de la norme et a ouvert la voie à une réflexion relative à l'apport d'une approche de modélisation-simulation pour la vérification de ces spécifications.

Une seconde application a concerné le réseau de sécurité *ProfiSafe* ; elle a montré encore davantage de difficultés à quantifier de manière évidente ces propriétés de sécurité [KON 04].

5.2.2.1 Discussion sur les réseaux de terrain de sécurité

L'utilisation des réseaux de communication a de nombreux avantages. Néanmoins, leur implémentation industrielle dans des installations à forte criticité ou dans des installations de sécurité est limitée par l'approbation d'organismes indépendants. L'Institut National de Recherche et de Sécurité (INRS) [CIC 99] fait partie de ces organismes, particulièrement dans le domaine des machines. Nous avons eu l'occasion de coopérer avec l'INRS afin de vérifier les spécifications techniques du réseau de sécurité *AS-i Safety at Work*, en regard des contraintes de sécurité attendues.

Dans cette étude, nous présentons tout d'abord les concepts de base du protocole *AS-i* et son extension *AS-i Safety at Work*. Une partie du protocole est ensuite modélisée par l'approche des RdP colorés et le modèle est analysé grâce au graphe d'occurrence construit à partir du modèle [BAR 03]. Par rapport aux études proposées chapitre 6, cette étude est différente en plusieurs points :

- le but n'est pas d'estimer les caractéristiques par simulation de Monte Carlo car cette méthode n'est pas adaptée pour l'étude de la sécurité,
- les modèles construits doivent correspondre intégralement à la spécification de la norme, avec une possibilité de vérification de cette correspondance à tout moment,
- il est impératif que le graphe d'occurrence puisse être analysé. En définissant les critères d'évaluation, il faut donc limiter l'explosion combinatoire. Dans notre cas, ceci est réalisé grâce à une séquence d'excitation déterministe.

Il est à noter que modéliser une norme avec des Réseaux de Petri n'est pas une idée novatrice, elle est largement abordée [BLA 00]. L'avantage de notre approche est l'utilisation d'un outil logiciel existant et ensuite l'intégration du modèle dans le reste du système d'automatisation.

5.2.2.2 AS-i et AS-i Safety at Work

AS-i, une abbréviation pour *Actuator – Sensor interface*, appartient à la catégorie des réseaux de terrain. Déjà, par son appellation il est clair que le domaine de son application principale est l'interconnexion des capteurs et des actionneurs aux régulateurs.

La topologie du réseau est soit un bus, soit un arbre, soit une étoile et elle doit contenir un maître unique et un nombre d'esclaves : 62 pour *AS-i* et 31 pour *AS-i Safety at Work*. Tous les échanges d'informations sont initiés par le maître auquel répondent potentiellement les esclaves. La réponse de l'esclave contient une information codée sur quatre bits.

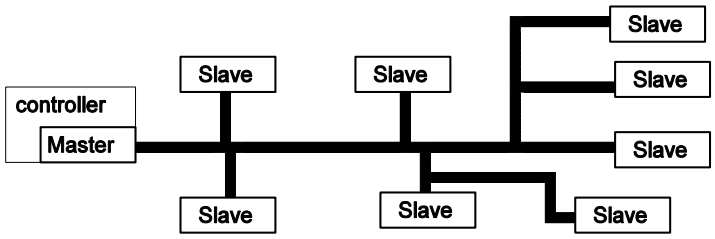


Figure 5.6 – Un exemple de topologie AS-i

Une couche supplémentaire est ajoutée au protocole *AS-i* pour former *AS-i Safety at Work*. Ainsi, le protocole *AS-i* devient une partie centrale dans un réseau de communication dédié à la sécurité. Selon sa présentation par le consortium, toutes les fonctions de sécurité peuvent y être implantées puisque *AS-i Safety at Work* est certifié pour être conforme à la catégorie 4 de la EN (Norme Européenne) 954 – 1 [954]. L'un des avantages principaux est la possibilité d'acheminer les données standard et de sécurité sur le même médium.

Ce travail est un exemple de modélisation et d'analyse d'une partie du protocole de communication *AS – i*, tel qu'il est décrit dans la référence principale NF EN 50295 [50295].

5.2.2.3 Méthode d'analyse

Après avoir créé le modèle [BAR 03] [*CN03a*], survient la phase de son analyse. Ceci signifie l'observation des réactions du modèle et l'évolution de l'état d'esclave en fonction des signaux extérieurs comme, par exemple, la présence d'un bit sur le bus. Le choix de l'ensemble des événements observés est un facteur crucial pour le concepteur. En effet, ce choix est une fonction du savoir-faire du concepteur et son 'intuition' est un facteur déterminant pour la valeur de l'analyse.
Pour observer le comportement de l'esclave-récepteur, un modèle d'émetteur est nécessaire. A ce stade de notre travail, l'émetteur maître n'est pas un modèle conforme aux spécifications *AS-i* mais seulement un émetteur simplifié qui envoie une séquence pseudo-aléatoire de requêtes de communication. L'envoi sur le bus est modélisé en plaçant la trame de communication dans une place appelée BUS. Les auteurs sont conscients qu'il s'agit ici d'une approximation grossière, mais elle est entièrement suffisante pour le but de l'étude.
La séquence pseudo-aléatoire de requêtes envoyée par le maître est conçue pour mettre en évidence le comportement de l'esclave dans le plus grand nombre de situations et elle comporte :

- des requêtes standard adressées à l'esclave observé (avec l'adresse de destination correspondante), par exemple *data_exchange* ou *write_parameter*,
- des trames standard adressées à un autre esclave que celui observé pour vérifier les réactions de l'esclave observé,
- des messages corrompus, par exemple un bit de parité non valide ou la longueur de trame mal formée.

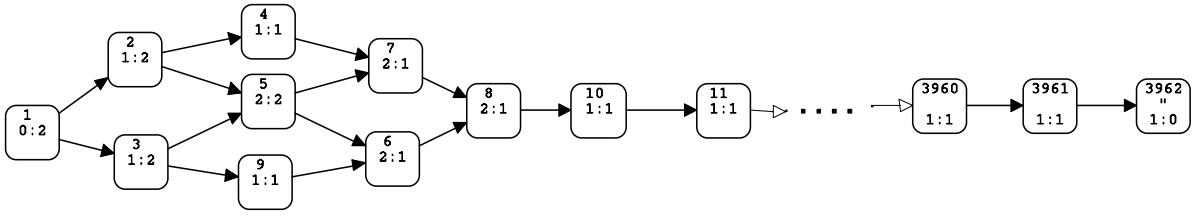


Figure 5.7 – Graphe d'occurrence

Design/CPN [DESIGN] [JEN 97] (voir aussi chap. 6) permet une génération automatique du graphe d'occurrence (cf. figure 5.7). Après l'avoir créé, plusieurs requêtes sont prédéfinies pour son analyse. Il est possible également de construire des requêtes selon les spécifications de l'utilisateur.

La première information fournie par le logiciel est la présence d'un état puits dans le graphe d'occurrence. Un état puits est un état à partir duquel le modèle ne peut plus évoluer [DAV 92] [DIA 01]. Bien sûr, la présence d'un tel état est indésirée dans la mesure où l'esclave doit toujours continuer à réagir sur les requêtes du maître. Pour trouver le nombre d'états puits, il faut parcourir chaque état du graphe d'occurrence et vérifier le nombre de ses successeurs. Si ce nombre est égal à 0, alors un état puits peut être présent.

Dans cette expérience, un état puits parmi plus de 3900 états atteints à été trouvé. Mais si nous examinons cet état en détail, nous trouvons qu'il s'agit du dernier état calculé et, pour lui, les successeurs ne sont pas encore calculés. Alors, la valeur par défaut 0 est utilisée. Les successeurs peuvent être calculés facilement ; cela ne résout pas le problème mais le décale simplement. En conclusion, il faut dire que si seulement une coupe du graphe d'occurrence est calculée, il faut toujours vérifier si les places puits le sont réellement ou s'il s'agit seulement des limites de la coupe calculée.

La présence d'un seul état puits peut renseigner sur le comportement du système communiquant ; son comportement est presque toujours déterministe. La seule exception à cette règle est l'instant d'initialisation du modèle où plusieurs actions sont effectuées quasi simultanément pour initialiser tous les composants. Après ce bref intervalle, le comportement du système converge rapidement vers une évolution complètement déterministe. Ce propos est encore confirmé par le nombre d'arcs, qui est légèrement supérieur (de moins de 10) au nombre des états atteignables. Dans le cas d'un comportement purement déterministe (séquence linéaire des états), le nombre d'arcs est inférieur d'une unité au nombre des états.

Toutes ces informations peuvent être obtenues du compte-rendu standard établi automatiquement par le logiciel. Entre autre, il y a aussi des renseignements sur la "bornitude" ou la vivacité. Une information est également donnée, concernant le fait que le graphe a été calculé en intégralité ou seulement en partie (c'est le cas de cette étude).

Toutes les informations résumées dans le compte-rendu standard restent très générales. Mais le potentiel de l'analyse de graphe d'occurrence est beaucoup plus important. Les critères définis par l'utilisateur peuvent être effectués moyennant la capacité de programmation de ces requêtes. Le passage entre les états *TRANSMIT* (cf. figure 5.8) et *INIT* est un exemple d'une telle analyse. Selon EN 50295, ce passage doit exclusivement avoir lieu si la trame *reset_AS-i_slave* a été correctement reçue par l'esclave. Alors, pour vérifier que chaque demande de reset est traitée correctement, il suffit de comparer le nombre de passages entre *TRANSMIT* et *INIT* avec le nombre d'apparitions de cette requête sur le BUS. Rappelons qu'aucune corruption des messages sur le bus n'est considérée à ce stade de l'étude.

Après avoir appelé la fonction *SearchNodes* qui parcourt tous les états du graphe d'occurrence, 106 états contenant les demandes de reset sont trouvés. Il reste à déterminer les passages entre *TRANSMIT* et *INIT*. Pour cela, il faut répertorier tous les états où l'esclave se trouve dans l'état *TRANSMIT* et ensuite examiner les successeurs directs de ces états. Il faut compter seulement les cas où *INIT* suit immédiatement le *TRANSMIT*. 53 cas sont ainsi recensés.

Il est évident que même si les deux résultats ne sont pas identiques, ils sont fortement corrélés. Dans la suite de l'analyse, il a été découvert que les 106 états avec la trame reset sur le BUS se produisent toujours en couples de deux états successifs. Il est relativement facile à démontrer que la répétition de ces états est due aux tests effectués sur le BUS. Ainsi, nous pouvons conclure que toutes les demandes *reset_AS-i_slave* sont reconnues et traitées correctement.

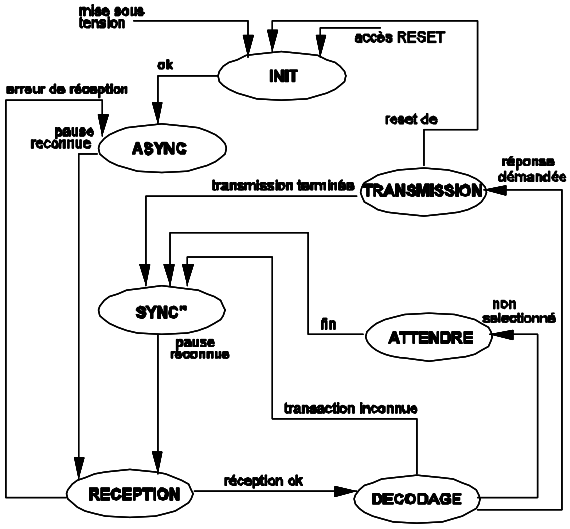
5.2.2.4 Conclusion de cette étude

La plus grande partie de cette étude porte sur la modélisation et l'analyse d'un protocole de communication réel. Les réseaux de Petri colorés ont montré leur potentiel dans ce type d'application. Le problème le plus important dans la phase de modélisation est l'absence d'une spécification suffisamment approfondie. En présence d'ambiguïtés, le concepteur doit interpréter la spécification et introduit ainsi une subjectivité dans le modèle, ce qui peut nuire à une analyse objective. Répertorier les ambiguïtés et les incohérences permet à son tour d'améliorer la qualité de la spécification [BLA 00].

Un modèle CPN peut être analysé de deux façons : 1.) performance et critères QdS et 2.) graphe d'occurrence, qui est approprié pour les études de sûreté/sécurité et peut être considéré comme une méthode d'analyse formelle.

Un modèle constitué d'un esclave et d'un maître est présenté dans cette étude. Mais la méthode n'est pas limitée à la modélisation des composants seuls. Chaque sous-système modélisé peut être utilisé ensuite comme une brique à intégrer dans un système plus complexe. Tous les composants peuvent d'abord être vérifiés séparément et après une analyse du système complet est toujours possible. Ceci est un atout majeur de la composition hiérarchique d'un modèle CPN et peut amplement faciliter le travail avec des systèmes de tailles conséquentes.

Le protocole complet n'est pas modélisé dans son intégralité à l'état actuel, puisque le but est de vérifier la faisabilité d'une analyse d'une norme par les CPN et de préparer une étude plus poussée.



Après mise sous tension ou après reset de l'esclave par l'accès RESET ou après réception d'une requête reset_AS-i_slave l'esclave doit être mis à l'état INIT.

Dans l'état INIT les fonctions suivantes doivent être exécutées:

- charger les registres de sortie de données et de sortie de paramètres avec la valeur par défaut 0xF;
- remettre le registre d'état à 0x0;
- charger l'adresse, la configuration E/S et le code identification de la mémoire non volatile dans les registres appropriés et contrôler les erreurs de lecture;
- mettre la marque data_exchange_disable (rendre échange de données inutilisable) à TRUE (vrai);
- passer à l'état ASYNC.

Figure 5.8 – Extrait de la version française de la norme EN 50295 présentant ASI-Safe

La vérification d'absence de blocage, telle qu'elle est présentée ici, ne peut pas être considérée comme une preuve formelle. Une preuve par induction pour toute taille de la portion calculée serait nécessaire. Mais il est possible qu'en faisant usage des caractéristiques structurelles, ce problème puisse être évité [CHR 01]. Ceci notamment par une transformation du graphe infini vers un graphe fini.

Ce travail a été repris dans [SEB 03] pour son stage ingénieur. Son travail comprend, d'une part, l'extension des modèles existant et, d'autre part, une proposition de méthodes d'évaluation de la sécurité du protocole de communication.

Les résultats obtenus sont les suivants :

- CPN et Design/CPN permettent la conception d'un modèle formel d'une spécification comme EN 50295.
- Le modèle peut être simulé et permet ainsi au concepteur d'acquérir une meilleure compréhension du modèle et de son comportement.
- La simulation de Monte Carlo permet l'analyse des performances.
- Un graphe d'occurrence peut être généré automatiquement. Dans l'exemple présenté, le graphe est infini et, par conséquent, seule une partie est calculée.
- L'absence de blocage (états puits) est vérifiée d'une manière non exhaustive.
- La différence entre le nombre d'arcs et d'états procure des renseignements sur la structure du graphe.
- Les fonctions de recherche définies par l'utilisateur offrent une grande souplesse pour l'analyse des nombreux critères sur le graphe d'occurrence (ex. : *reset_AS-i_slave*).
- La liste des ambiguïtés et incohérences de la norme et, par conséquent, la liste des choix que nous avons fait pour aboutir à des modèles finaux est documentée.
- Les modèles de différents composants du réseau *AS-i* sont disponibles et le graphe d'occurrence est prêt pour une analyse. Dans notre cas, la séquence d'excitation de l'esclave est périodique et donc infinie. C'est pourquoi seule une partie du graphe est construite.

5.2.3. Influence de l'initialisation du réseau sur la sûreté de fonctionnement

Ce travail avait pour but de montrer comment le mode d'initialisation d'un réseau, le choix dans la détermination des horloges et la stratégie de synchronisation ou non-synchronisation des composants pouvaient avoir des conséquences très importantes sur les performances du système, au sens de l'automatique, ainsi que sur la sûreté de fonctionnement de ce système [*CI04a, voir Annexe C papier 5*]. Ceci a été montré dans le cas de la régulation d'une cuve de liquide, pilotée via un réseau (dans un contexte de *Networked Control System*). Ces travaux peuvent être considérés dans une certaine mesure comme la continuation de travaux menés antérieurement [*CI98b*].

Le NCS sur lequel nous avons travaillé est représenté figure 5.9. Le réseau apparaît deux fois dans la boucle et il impose une contrainte de communication (seul un nœud peut transmettre sa donnée à la fois) qui est la cause des délais τ_{sc} entre le capteur et le contrôleur et τ_{ca} entre ce dernier et l'actionneur [LIG 02] [*CI02a*].

Les types de retard dans les NCS peuvent être classés en deux groupes : les temps de calcul et les retards dus à la communication. Il est possible dans une première approximation de considérer les temps de calcul comme fixes, dans la mesure où ceux-ci peuvent être connus, pour un calcul donné. Les temps de transmission sont fonction du nombre de nœuds connectés, du type de réseau ou d'ordonnancement et du niveau de partage des ressources. Pour certains protocoles tels les protocoles à jetons, les délais de transmission sont bornés ; dans d'autres cas, tels qu'Ethernet avec des mécanismes CSMA/CD, les temps de transmission sont non bornés. Cela implique que les performances du système ne sont pas fonction uniquement des performances des composants individuels, mais également très liées au choix du medium de communication.

Trois types de délais peuvent être envisagés dans un NCS [NIL 03] (cf. figure 5.9) :

- délai lié au réseau entre le capteur et le contrôleur τ_k^{sc},
- délai de calcul pour l'élément τ_k^{c},
- délai lié au réseau entre le contrôleur et l'actionneur τ_k^{ca}.

Le délai total lié au NCS est la somme de ces trois délais.

Concernant les durées de ces délais, elles obéissent aux caractéristiques suivantes :

- délais plus petits ou égaux à la période d'échantillonnage $\tau \leq T_s$,
- délais plus grands que la période d'échantillonnage $\tau > T_s$.

τ représente le délai du réseau et T_s la période d'échantillonnage du système commandé.

5.2.3.1 Description des stratégies d'initialisation du NCS

No.	Capteur	Retard	Contrôleur	Retard	Actionneur
1.	T	τ^{sc}	T	τ^{ca}	T
2.	T	τ^{sc}	T	τ^{ca}	E
3.	T	τ^{sc}	E	τ^{ca}	T
4.	T	τ^{sc}	E	τ^{ca}	E
5.	E	τ^{sc}	T	τ^{ca}	T
6.	E	τ^{sc}	T	τ^{ca}	E
7.	E	τ^{sc}	E	τ^{ca}	T
8.	E	τ^{sc}	E	τ^{ca}	E

Tableau 5.2 – Combinaisons possibles des comportements des noeuds de commande (*E – event driven, T – time driven*) pour un NCS simple à trois éléments

Le NCS illustré figure 5.9 est composé de trois éléments : un capteur, un contrôleur et un actionneur. Chacun de ces éléments peut être soumis à deux types d'initialisation, soit une initialisation sur horloge, périodique (*T-initialization*) soit une initialisation sur événement ou interruption (*E-initialization*).

Dans les modèles NCS traités, l'événement extérieur sera un événement de communication, concrètement une information qui doit être traitée immédiatement par le nœud de réception. Ce nœud enverra l'information traitée à

l'élément suivant au moyen d'une séquence de contrôle. Dans le cas du système à trois éléments, cette séquence sera *capteur vers le contrôleur puis l'actionneur.* Toutes les combinaisons possibles des initialisations des nœuds de ces trois éléments reliés au réseau sont proposées dans le tableau 5.2.
Dans la partie suivante ne sont envisagées que les quatre premières combinaisons. Nous considérerons donc que le capteur est sollicité sur horloge (*T-driven*) uniquement, même si une initialisation sur événement peut avoir une forte implication sur l'utilisation du réseau et la congestion [OTA 02]. Dans la suite seront donc envisagées les combinaisons TTT, TTE, TET et TEE.

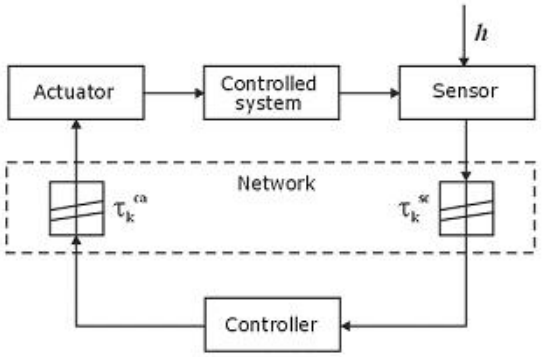


Figure 5.9 – Schéma général d'un NCS

5.2.3.2 Effet de l'initialisation sur le NCS

Avec la stratégie TTT, tous les éléments du réseau sont synchronisés et échantillonnés au même moment. Dans ce cas idéal, le système est conforme à la théorie des systèmes échantillonnés. Si les composants sont strictement synchronisés, la séquence de contrôle est décrite par les étapes suivantes :

- la mesure est échantillonnée au temps *k*,
- à cause du temps de communication, le contrôleur traitera cette information au temps *k+1*,
- et finalement toujours à cause du temps de communication, l'actionneur n'agira qu'au temps *k+2*.

Donc normalement, sans retards liés au temps de calcul, deux périodes d'échantillonnage sont nécessaires pour parcourir la chaîne, autrement dit le temps de retard global est de deux périodes d'échantillonnage. L'utilisation de déclenchements sur événement (*Event initialization*) permet de réduire ces retards, causés par la synchronisation et les retards de transfert. Tout retard compris entre 0 et T_s (période d'échantillonnage) est équivalent à un retard d'une période d'échantillonnage. Finalement, chaque nœud de réception (soit le contrôleur, soit l'actionneur) qui est déclenché sur horloge (*T-driven*) dans un NCS synchronisé apportera donc un retard d'une période d'échantillonnage.

Facteur de qualité	Sans réseau	TTT	TTE	TET	TEE
T_{reg} [su]	175	175	119	164	129
σ_{max} [%]	0	8,69	2.59	5.43	0
T_d [su]	0	10	7	10	4
RSDE [%]	0	0	17.5	34	14

Tableau 5.3 – Résumé des résultats de simulation

5.2.3.3 Conclusion

Toutes les simulations ont utilisé les mêmes périodes d'échantillonnage, la même architecture et le même type de contrôleur. Le type d'initialisation affecte la qualité de la commande. Si l'on compare à la boucle de commande sans réseau, les résultats montrent que l'initialisation TEE est la meilleure. Chaque nœud de réception (soit le contrôleur, soit l'actionneur) qui est "*T-driven*" causera un retard d'une période d'échantillonnage. Il est évident que si le contrôleur est T-initialisé, cela dégrade la qualité de la commande. En fait, la somme des retards

aléatoires τ_k^{sc} et τ_k^{ca} est plus grande que la période d'échantillonnage, l'actionneur qui est *T-driven* applique sa valeur de la commande à la période d'échantillonnage suivante.

Dans le tableau 5.3, le paramètre RSDE (*relative standard deviation error /* erreur de déviation standard relative) est calculé à chaque pas d'échantillonnage comme le rapport en % entre l'écart-type maximal et la réponse indicielle moyenne.

$$RSDE = \max(sde(k)/xm(k)) * 100\%.$$

où sde(k) est l'écart-type calculé au temps k, xm(k) est la valeur moyenne sur l'historique des initialisations pour tous les échantillons k.

Cette erreur donne des informations sur l'influence des retards aléatoires dans chaque cas d'initialisation. De ces résultats de simulation, notons que le cas de d'initialisation TEE est le plus robuste car l'influence des retards aléatoires est la moins perceptible sur la qualité. Nous pouvons donc en déduire qu'il est possible d'améliorer le NCS en modifiant la stratégie de commande.

Ce travail a été réalisé par Jana LIGUSOVA, étudiante en 3ème année de thèse à l'Université Technique de Košice (Slovaquie), lors de son stage de trois mois dans notre équipe, au printemps 2003.

5.3. Système d'information pour une communauté urbaine

De janvier 1996 à mars 1999, j'ai participé à un projet européen dans un contexte de système d'information. Il s'agissait du projet européen OSA-TESMA (4ème PCRD/TELEMATICS/ Open System Architecture for TElematicS in Municipal Applications / TELEMATICS UR1020) qui concernait le développement d'une interface multimédia avec une base de données urbaines reliée à un système d'information géographique pouvant être consulté par différents media (web, RNIS, RTC) et terminaux.

Le contractant principal était l'*Institut für Mikrorechner und Automation* - Karlsruhe (membre de l'IAR : Institut Franco-Allemand pour les Applications de la Recherche).

Les autres contractants étaient :
- le CRAN,
- la Communauté Urbaine du Grand Nancy,
- l'Institut Lorrain du Génie Urbain
- l'Institut de l'Audiovisuel et des Télécommunications.

Les autres partenaires étaient :
- l'*Institut Photogrammetrie und Fernerkundung-Karlsruhe*,
- le *Vermessungs- und Liegenschaftsamt der Stadt - Karlsruhe (VLA-KA)*,
- *Kreutler GmbH* en Allemagne,
- *VIEWROPE* à Luleå en Suède,
- *EPSILON International SA* à Marousi en Grèce.

J'ai participé à Bruxelles à certaines phases de négociations lors de la rédaction du contrat avec K.H. KAPP (Université de Karlsruhe), le coordinateur et j'ai présenté les résultats de notre travail lors des trois évaluations annuelles à Bruxelles. J'ai travaillé à la définition et à la modélisation de l'architecture du système avec T. DIVOUX (responsable de ce « Work package »), S. ROTH, M.L. BESSON et E. GNAEDINGER. Le développement du prototype a été réalisé par M.L. BESSON. Deux communications dans des conférences internationales ont été présentées dans la période 1997-98 et un rapport de contrat (« deliverable »), dans lequel je me suis très fortement impliqué, a été rédigé pour notre partie du travail.

La figure 5.10 présente l'architecture générale du système étudié.

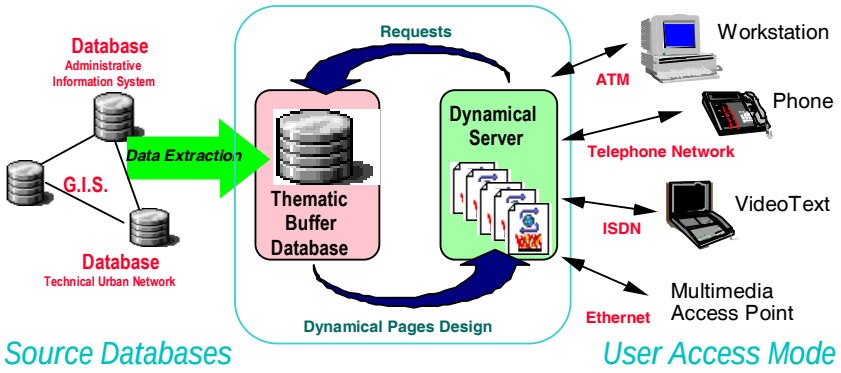


Figure 5.10 – Architecture du système proposé avec la base de données tampon et le serveur dynamique

5.3.1. Base de données tampon

Le système d'information multimédia proposé est basé sur un modèle universel de base de données tampon. L'idée est à la fois de protéger le réseau interne et le système d'information géographique en ne permettant l'interrogation extérieure que de cette base de données tampon. Divers moteurs d'extraction doivent être envisagés, ayant pour rôle la mise à jour du contenu de cette base de données tampon en fonction de la périodicité et de la criticité des informations envisagées.

La base de données tampon propose ces diverses informations avec des formats compatibles avec les terminaux utilisés par les utilisateurs finaux (ordinateur, téléphone, terminal, téléphone portable). L'autre idée force de cette base de données tampon est l'optimisation, au sens où elle ne contient que les informations les plus à même d'être utilisées, à l'image d'un site miroir, et que ces informations sont organisées en fonction de listes thématiques.

5.3.2. Serveur dynamique

Le serveur dynamique a pour finalité l'affichage sur l'écran du terminal retenu des informations pertinentes encapsulées dans une page de présentation appelée page de résultats.

Un autre aspect intéressant est la 'navigation'. En effet, au moment de l'entrée dans le système, l'utilisateur s'est défini grâce à une fiche d'identité le concernant ; le système peut donc choisir les items à afficher ainsi que la façon de les afficher en fonction du profil de l'utilisateur. Pour cela, à chaque profil utilisateur sont associées des listes d'arguments qualifiant les items.

Le mécanisme d'extraction permettant la mise à disposition des informations dans la base de données tampon est divisé en plusieurs phases. La première étape concerne la recherche de l'information correcte mise à jour dans le système d'information géographique ou dans une autre base de données urbaine. Ensuite, le moteur d'extraction a pour tâche d'adapter le format d'origine du document en un format compatible avec le terminal de l'utilisateur [RAG 94]. Finalement, le document est complété par une liste d'arguments décrivant le contenu de ce document et les informations potentiellement intéressantes aux utilisateurs pour faciliter toute recherche future.

5.3.3. Modèle de base de données

Le modèle de base de données proposé est conforme à une liste de règles qui doivent être respectées par les utilisateurs et le système. Ce modèle donne la définition du modèle conceptuel de communication et du modèle conceptuel de données [*Rc98a*] [*Cl96c*]. Plus précisément, ce modèle contient les descriptions des :

- utilisateurs et transactions,
- entités continues dans la base de données : il s'agit pour l'essentiel des éléments de base provenant du système d'information géographique,
- entités et sous-types d'un élément : il s'agit ici de caractériser les champs ou attributs d'un élément en fonction du type d'utilisateur ou du scénario envisagé.

5.3.4. Résultats

Les principaux résultats de ce travail sont les suivants :

- la définition d'une architecture générique pour un système temps réel d'information municipal facilement installable dans diverses villes européennes par le biais d'une base de données tampon indépendante des bases de données des systèmes urbains,
- une réflexion sur le pré-formatage de documents,
- un moteur de recherche permettant une recherche "intelligente" définie autour du concept de définition de profils type d'utilisateurs finaux par le biais de questionnaires.

L'intérêt principal a été de nous initier sérieusement aux nouvelles technologies à une époque où elles l'étaient encore. L'autre intérêt était bien sûr l'ouverture internationale.

Les points qui restent vraiment d'actualité dans les propositions qui ont été faites sont l'aspect lié à l'utilisation de la carte d'identité de profil utilisateur ainsi que l'adaptation de la présentation des informations au type de terminal utilisé par l'usager.

Diverses publications sont disponibles sur le sujet : [CHR 91], [COM 94], [FOR 96], [HAE 96], [HOW 96], [RAG 94], [ROT 96], [WIE 96].

5.4. Conclusion

Dans la poursuite des travaux de thèse, nous avons apporté quelques résultats concernant l'utilisation des capteurs intelligents pour la régulation de trafic urbain, ces instruments intelligents faisant partie des composants de base constitutifs des SAID. Ces travaux ont permis de mettre en application des concepts développés, notamment au sein de l'équipe.

Ce chapitre a également amené quelques réflexions nécessaires lorsqu'on veut utiliser les réseaux de terrain qui sont par essence la colonne vertébrale des SAID. Selon le niveau de criticité requis pour le SAID, il peut être en effet important, d'une part, d'évaluer ce réseau afin d'obtenir un niveau de certitude sur l'accomplissement de la fonction communication et, d'autre part, d'étudier les interactions entre le réseau et les composants (type d'initialisation par exemple) qui peuvent entraîner des conséquences sur le niveau de sûreté du SAID.

Dans le cadre de cette action, nous sommes également un partenaire actif depuis 1999 du groupe de travail CIAME (18.04, Constituants Intelligents pour l'Automatisation et la Mesure) - groupe de travail de la SEE, (Société de l'Electricité, de l'Electronique et des Technologies de l'Information et de la Communication), ainsi que de l'action spécifique "Méthode et modèle pour l'évaluation de la sûreté de fonctionnement des systèmes distribués" qui a démarré en janvier 2004. Dans le cadre du groupe CIAME, un ouvrage intitulé "Critères de choix de réseaux de terrains, prise en compte de la sûreté de fonctionnement" sera publié cette année [*OU04*] [*RI04a*]. Dans la contribution proposée par le groupe de travail CIAME [*CI03c*] [*RI04a*], les résultats de la fonction "communication" sont présentés avec la caractérisation des différents modes de défaillances, de leurs causes et de leurs effets à tous les niveaux OSI (Open System Interconnection) du réseau. Cette AMDEC (Analyse des Modes de Défaillances, de leurs Effets et de leurs Criticités) permet de présenter différents moyens à mettre en œuvre pour éviter ou minimiser les conséquences de l'occurrence de tels modes de défaillances.

Nous avons également apporté une contribution sur la définition d'un système d'information pour les communautés urbaines européennes.

Nous proposons un récapitulatif des communications et publications concernant ces activités :
- définition d'un capteur intelligent de trafic : *CN01a (voir Annexe C papier 3), CI97b, RI96, CN95, CS95, Rc94 (rapport de contrat),*
- modèle de supervision de trafic à base de réseaux neuronaux : *CI00b.*
- réseaux de terrain et transports : *CI98d, Rc98b (rapport de contrat), CI96d, CI95a,*
- réseaux de terrain et sécurité : *RI04a, CI04a (voir Annexe C papier 5), CI03c, CI02a, CI98b*.
- systèmes d'information pour une communauté urbaine : *Rc98a* (rapport de contrat européen), *CN97, CI97a, CI96c, CI96a, CI95c*.

6. Evaluation de la SdF des SAID

Ce chapitre constitue, avec le chapitre suivant proposant un projet de recherche futur, le cœur de l'habilitation, proposant une démarche d'évaluation du niveau de sûreté de fonctionnement des SAID qui intègre bien les propriétés particulières des éléments intelligents constitutifs de ces systèmes, ainsi qu'une prise en compte la plus pertinente possible de l'existence du réseau de communication, comme colonne vertébrale de ce système. Ce chapitre correspond également au travail de trois thèses que j'ai co-encadrées.

Le premier travail proposé consiste à envisager l'intégration des composants intelligents décrits dans le chapitre précédent afin d'obtenir une architecture distribuée. Dans la mouvance de travaux d'actualité à l'époque, il s'agissait de prendre en main des outils et méthodes concernant la répartition des tâches et de proposer une répartition des tâches sur un SAID, la meilleure possible au sens des coûts et en respectant les contraintes de tailles mémoire, de vitesse d'exécution des processeurs et de disponibilité du réseau. Dans ce travail, la sûreté de fonctionnement en tant que telle n'était pas encore vraiment prise en compte. Le premier paragraphe rappelle l'ensemble de ces travaux qui constituent la thèse de Frédéric HERMANN, que j'ai co-encadrée.

Un second travail propose l'utilisation d'algorithmes génétiques pour la répartition des tâches sur le SAID. Ce travail a été le fruit d'un partenariat avec F. BICKING, maître de conférences, et a fait l'objet de plusieurs communications et d'une publication [*RI04b, voir Annexe C papier 2*] [*CI02b*] [*CI00a*] [*CN99c*] [*CI98c*].

Dans un troisième travail, nous montrons comment l'intégration de composants intelligents peut influer sur la sûreté de fonctionnement. Les critères de sûreté de fonctionnement pris en compte sont la disponibilité et la fiabilité. Une modélisation fonctionnelle de l'architecture est effectuée, suivie d'une analyse des dysfonctionnements sous la forme d'une recherche des événements perturbateurs et des états dégradés. Une évaluation est finalement réalisée à partir d'une méthode basée sur les arbres de décision binaires. Le second paragraphe de ce chapitre resitue une bonne part des activités de la thèse de Blaise CONRARD, que j'ai co-encadrée.

Dans le quatrième travail, il s'agit d'aller encore plus loin dans la prise en compte des caractéristiques du système (intelligence, aspect dynamique). Pour cela, nous avons souhaité compléter l'approche envisagée dans les travaux de B. CONRARD d'aspects liés à l'évolution temporelle du système, c'est-à-dire d'une part simuler l'évolution du système en fonction d'un modèle permettant la prise en compte des aspects temporels, d'autre part intégrer dans les caractéristiques évolutives de sûreté de fonctionnement des composants les sollicitations réelles de ceux-ci en fonction des stratégies de commande, des modes de fonctionnement, de l'architecture. Le quatrième paragraphe de ce chapitre décrit les activités de la thèse de Pavol BARGER, que j'ai co-encadrée.

6.1. Répartition des données et traitements sur un SAID

6.1.1. Recherche d'un modèle

La mise en place d'une démarche de développement de SAP soulève de nombreux problèmes ; l'un des plus représentatifs est lié au choix des moyens et méthodes à employer en conception [HER 97]. Dans ce domaine, nous nous sommes inspirés du modèle 3-axes qui classe les fonctions de base du système d'information d'un SAP en quatre grandes catégories de fonctions [SIM 92]. Ce modèle informel est représentatif des besoins d'exploitation et surtout correspond à des finalités distinctes bien définies [DEL 89] :

- La fonction **Conduire** est destinée à contrôler le comportement futur et immédiat du processus de production, pour atteindre les objectifs de production exprimés en termes de qualité et de productivité. Cette fonction recouvre aussi bien les automatismes séquentiels que les asservissements ou les régulations.
- La fonction **Maintenir** est destinée à assurer une disponibilité maximale du processus de fabrication. Pour atteindre cet objectif, il est nécessaire d'intégrer un niveau de sûreté de fonctionnement satisfaisant.
- La fonction **Suivre** est destinée à recueillir et à synthétiser les informations relatives à l'état présent et passé du processus ainsi qu'à l'état et la position des produits.
- La fonction **Sécuriser** est destinée à assurer la non occurrence de défaillances catastrophiques qui pourraient mettre en danger le personnel d'exploitation, l'environnement, les installations de production et les produits.

6.1.2. Représentation de l'architecture des traitements

Avant de répartir les traitements sur une architecture matérielle, ceux-ci doivent être inventoriés et leur relations identifiées. Ces relations sont les flux de données qui interconnectent les différents traitements. Une représentation possible pourrait donc être un graphe où les nœuds représenteraient les traitements et les arcs les flux de données.

Cette représentation doit cependant répondre à une autre contrainte : la possibilité d'associer à celle-ci des informations relatives au comportement de l'installation en présence de défaillance. Nous préférons ainsi utiliser une représentation hiérarchisée. En effet, ce type de représentation est plus facile à établir grâce à l'emploi de méthodes telles que SADT [IGL 89] ou SA/RT [PER 90]. Mais de plus elle permet d'établir plus simplement les relations concernant l'influence des défaillances sur chaque système et sous-système de l'installation.

La représentation proposée est la suivante. Elle consiste à décomposer chaque fonction en sous-fonctions pour aboutir globalement à une décomposition hiérarchique et arborescente du système. Une fonction est considérée ici comme l'association d'un ensemble de traitements destinés à rendre un service. Le raffinement s'achève lorsqu'on atteint des fonctions suffisamment élémentaires pour être considérées comme des traitements suffisamment élémentaires pour être "supportables" par un des composants du système. In fine, nous obtenons une décomposition hiérarchique des fonctions du système avec au sommet la mission de l'installation et à la base les traitements élémentaires (cf. figure 6.1) que nous appelerons tâches.

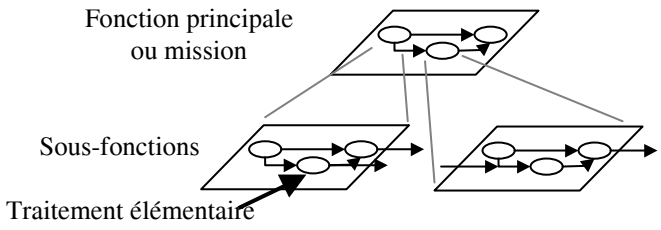


Figure 6.1 – Décomposition hiérarchisée des fonctions et traitements

6.1.3. Allocation des tâches sur l'architecture matérielle

Les fonctions à implanter vont devenir des tâches à répartir sur l'ensemble des CAI (Composants d'Automatisme Intelligent). Ces derniers sont reliés entre eux par le réseau de terrain FIP, dans le cas d'une application que nous avons développée sur le processus thermique pilote du laboratoire (PTP) (cf. figure 6.2) :

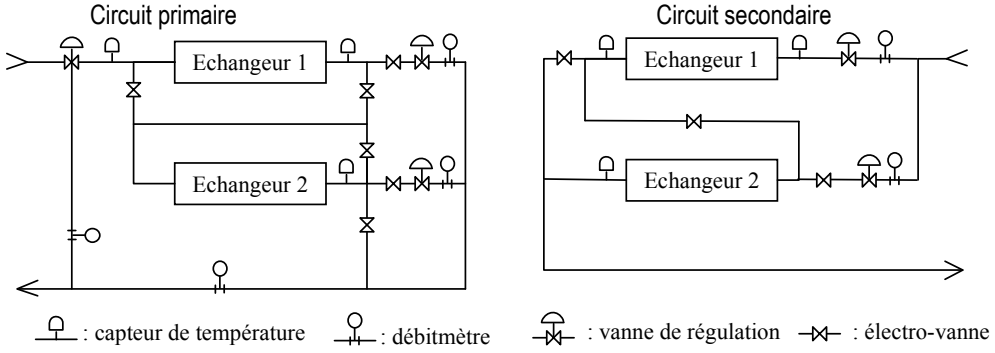


Figure 6.2 – Schéma du processus thermique

Deux circuits ouverts parcourus par de l'eau constituent le processus. Le premier est alimenté par un fluide chaud dont l'énergie thermique est transférée à un circuit secondaire grâce à deux échangeurs. La fonction ou mission de ce processus est donc de contrôler la quantité de fluide traversant le circuit secondaire ainsi que sa température de sortie.

Ce système pilote étudié était un processus thermique commandé par plusieurs stations PC qui assurent la régulation de température du fluide et qui permettaient la configuration du système. Six boucles de régulation de débit et de température étaient implantées. Le processus thermique se composait :

- d'un générateur thermique : une chaudière à gaz à circulation d'eau chaude,
- d'un récepteur thermique constitué de deux échangeurs de chaleur à faisceaux tubulaires rectilignes à contre courant,
- de capteurs de débits et de températures,
- de vannes de régulation pneumatiques,
- d'électrovannes tout ou rien.

Globalement cette mission consiste pour le système d'automatisation à réguler en débit le circuit secondaire grâce aux vannes de régulation et à réguler sa température de sortie en contrôlant le débit d'eau chaude dans les échangeurs du circuit primaire.

L'affectation des tâches aux CAI doit tenir compte des contraintes ressources matérielles et des coûts correspondant à la somme des coûts d'exécution et de communications entre les tâches. Nous cherchons à déterminer une affectation de coût minimal, c'est-à-dire un placement des tâches sur les CAI qui utilise au mieux les ressources systèmes : les CAI et le réseau de terrain. Nous savons qu'il n'existe pas d'algorithme non déterministe pour la résolution du problème en un temps polynomial [MEL 94].

Le placement des traitements sur une architecture matérielle nécessite d'effectuer déjà des choix sur le matériel à employer comme le nombre de CAI (API, ordinateurs, capteurs, actionneurs...) à utiliser, la taille mémoire ROM, le temps de cycle et le nombre maximal de tâches par CAI.

En pratique, il y a toujours un choix sur l'infrastructure de départ tels que les capteurs, actionneurs et réseaux de terrain [GAL 98]. Au niveau des unités de traitement, il y a le choix entre API et ordinateurs industriels. Par contre leur nombre reste à déterminer.

Le résultat de cette projection est appelé architecture opérationnelle [BAY 95]. Les méthodes de placement des tâches peuvent être de deux catégories : statique ou dynamique [MUN 91]. Pour un placement statique, il existe deux types de méthode : la méthode exacte et la méthode heuristique. En fait, les méthodes heuristiques dérivent des méthodes exactes. Ces dernières permettent d'intégrer un plus grand nombre de critères et de contraintes, mais sont plus consommatrices en temps de calcul. Par contre, les méthodes heuristiques ne permettent pas d'obtenir la solution optimale.

6.1.4. Programmation mathématique

Les méthodes utilisant la programmation mathématique formulent le problème comme un problème d'optimisation combinatoire et le principe de ces méthodes est de ramener ce problème à l'optimisation d'une fonction non linéaire exprimant le coût du placement, soumise à plusieurs contraintes : c'est une énumération "implicite" de toutes les solutions possibles.

La formulation du problème est de minimiser une fonction coût f_i [1], tout en respectant un ensemble de contraintes [2] :

$$S = \text{Min. } f_i(X_1, X_2, \ldots X_k) \qquad [1]$$

$$G_i (X_1, X_2, \ldots X_k) \leq B_i \qquad [2]$$

Les variables X_i sont des variables bivalentes ; les fonctions f_i et G_i sont des fonctions polynomiales en X_i à coefficients constants. Les B_i sont des constantes et S est la solution du problème. Les fonctions coûts représentent un moyen de mesure de performance d'une répartition obtenue. Nous donnons dans la suite du paragraphe les fonctions de coûts et de contraintes proposées dans le cas de l'application PTP.

Plusieurs fonctions du coût sont proposées. Le choix d'une fonction coût dépend du type d'architecture utilisée. Dans notre cas, nous avons une architecture hétérogène (processeurs de puissances de traitements différentes) sans mémoire commune. Dans le but d'allouer nos tâches aux différents CAI (machines ou processeurs), nous utilisons une matrice d'affectation X :

$$x(i,k)=\{1 \text{ si la tâche est affectée au processeur k / sinon } 0)$$

6.1.4.1 Fonctions coûts

Coût de communication :

Le coût de communication dépend notamment du type de l'architecture cible. Il existe deux types de coûts de communication : les coûts de communication entre deux tâches et les coûts de communications entre deux processeurs. Le premier type de coût de communication correspond à l'échange de données entre deux processus. Nous considérons que ce coût entre deux tâches placées sur un même processeur est négligeable. Le second coût correspond aux échanges d'information entre deux processeurs. Ce coût fait intervenir le réseau de communication.

A partir de la matrice de communication entre les tâches et la matrice d'affection X, nous calculons le nombre de variables produites (nbvarprod), ainsi que la taille de ces variables (varprod) pour chaque machine.

$$f_1 = \Sigma \text{ varprod}(i) \times 8 + 2 \times \text{nbvarprod}(i) \times (61+TR),\ i = 1, \ldots n$$

où n est le nombre de machines, varprod(i) correspond à la quantité d'octets transitant sur le réseau FIP pour une machine i et nbvarprod(i) correspond au nombre de variables nécessaires pour effectuer le transit de varprod(i). Enfin TR est le temps de retournement, il dépend des caractéristiques physiques du réseau FIP comme notamment la longueur du bus de terrain (valeur courante 40ms).

De plus, nous calculons également le nombre de variables consommées (nbvarcons(i)) par chaque machine i, afin de savoir exactement les variables produites et consommées par chaque station du réseau. En effet l'écriture ou la lecture d'une variable FIP entraîne un surcoût au niveau du coût d'exécution qu'il convient de connaître.

Coût d'exécution :

Le coût d'exécution d'une tâche à implanter sur un processeur varie en fonction de la puissance du processeur.

$$f_2 = \Sigma \text{ u}(i).x(i,j) + \Sigma \text{ nbvarprod}(i) \times TE + \Sigma \text{ nbvarcons}(i) \times TE$$

où u(i) représente le temps d'exécution de la tâche i. La lecture ou l'écriture des variables FIP engendre un délai qui est variable suivant le logiciel utilisé comme FIPToolbox ou LabVIEW avec la librairie (Hlp Technologies). Ce délai est représenté par TE qui vaut 55 millisecondes dans le cas de notre application avec LabVIEW.

Coût de la taille mémoire :

Le coût de la taille mémoire représente dans notre application l'encombrement des tâches sur le support de stockage de chaque machine (ROM).

$$f_3 = \Sigma \text{ m}(i).x(i,j)$$

où m(i) représente la taille mémoire ROM de la tâche i.

6.1.4.2 Contraintes

Nous distinguons deux types de contraintes : la contrainte d'affectation obligatoire ou matrice de préférences et la contrainte d'exclusion. Elles peuvent être représentées par une matrice booléenne.

Nous pouvons considérer la matrice de préférence ou d'affectation obligatoire entre les tâches et les processeurs :

$$P = \{p(i,j)\},\ i = 1, \ldots n,\ j = 1, \ldots m$$

où n est le nombre de processeurs. Si p(i,j) = 0, alors la tâche i ne peut pas être allouée au processeur j : par exemple les valeurs issues des capteurs ne peuvent être implantées uniquement que sur les concentrateurs.

Une matrice d'exclusion E entre les tâches est définie par :

$$E = \{e(i,j)\},\ i = 1, \ldots e,\ j = 1, \ldots m$$

où e est le nombre d'exclusion et m le nombre de tâches. Si e(i,20)=1 et e(i,21)=1 alors les tâches 20 et 21 ne doivent pas être sur le même processeur.

A titre d'exemple, sur le processus PTP la fonction "Conduire" est dupliquée dans le but d'augmenter la sûreté de fonctionnement. Dans la même optique, la fonction "choisir" est implantée sur une machine différente. Ces choix sont représentés par la matrice E.

L'équilibrage de charge réseau se fait au travers des contraintes. Ces contraintes sont la charge sur une machine, la taille mémoire, la contrainte temps réel sur les CAI.

La charge machine est représentée par la contrainte suivante :

$$\Sigma\, x(i,j) \leq R_k,\ k = 1, \ldots n$$

où la somme des tâches ne doit pas dépasser le maximum toléré R_k par la machine k.

La taille mémoire est représentée par la contrainte suivante :

$$\Sigma\, m(i).x(i,j) \leq M_k,\ k = 1, \ldots n$$

où m(i) représente le taille mémoire de la tâche i et M_k représente la capacité mémoire de la machine k. Cette équation montre la mémoire totale utilisée par toutes les tâches assignées à une machine. Et ce montant ne doit pas excéder la capacité mémoire assignée à cette machine.

La contrainte temps réel est exprimée par l'équation suivante :

$$\Sigma\, u(i).x(i,j) \leq U_k,\ k = 1, \ldots n$$

où u(i) représente le temps d'exécution de la tâche i et U_k représente le temps limite imposé au processeur k.

Cette équation montre le temps d'exécution total utilisé par toutes les tâches assignées à une machine. Ce montant ne doit pas excéder le temps limite assigné à cette machine.

6.1.5. Résultats

6.1.5.1 Présentation

Sans entrer dans les détails développés ailleurs [HER 97], nous montrons ci-dessous un exemple de résultat où la répartition permet de définir le nombre de variables échangées entre les CAI ainsi que leur taille (cf. figure 6.3). La figure 6.3 fait le récapitulatif des différentes répartitions sur le PTP.

Afin de déterminer la table d'arbitre de bus, il faut définir le temps du macrocycle. Nous proposons de définir le temps du macrocycle inférieur au temps d'exécution du CAI le plus rapide. Toutefois, ceci n'est possible que si la charge réseau périodique est intégrable dans le temps imparti. Le tableau 6.1 donne un ordre d'idée sur le nombre de variables FIP scrutables pour obtenir un trafic périodique de 60%.

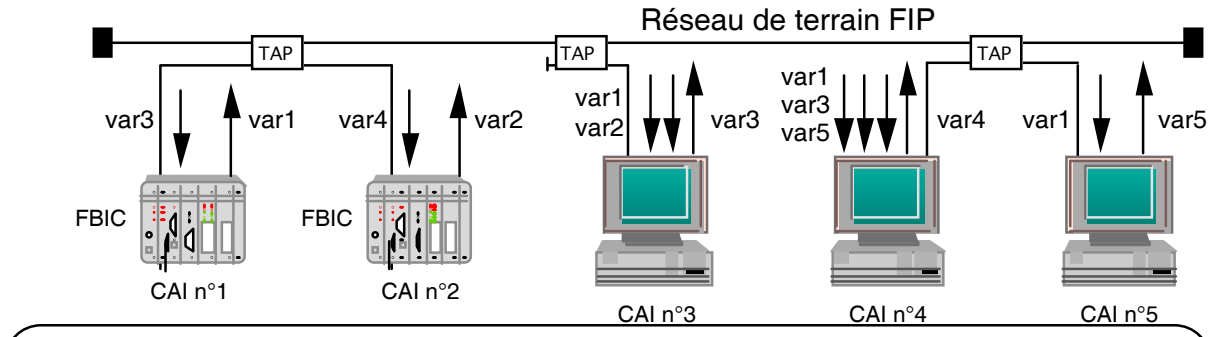
La première ligne du tableau 6.1 signifie que la scrutation de 48 variables FIP nécessite 100 ms et que ce trafic périodique encombre le réseau à 60 %.

Dans cet exemple, nous obtenons cinq variables avec un macrocycle de 120 ms lié au temps d'exécution le plus rapide (CAI 5). La charge réseau minimale possible est de 8 % ; elle correspond à la scrutation de chaque variable FIP au moins une fois. La quantité d'informations échangée est encore faible dans le cas envisagé. Toutefois, si l'on intègre par la suite une partie des notions d'interopérabilité, d'interfonctionnement comme la sémantique, alors la quantité d'informations échangées devient rapidement très importante. Dans notre application, la taille des variables du processus est limitée à deux octets. En intégrant ces notions, la taille des variables FIP peut atteindre 27 octets en respectant la norme EN 50170.

6.1.5.2 Validation de l'architecture opérationnelle

Après l'implantation des tâches, il convient de valider cette répartition en effectuant différents tests. L'ensemble de ces vérifications doit conduire à une architecture opérationnelle validée :

- Vérifier le respect de la taille mémoire sur chaque CAI.
- Vérifier le respect du temps d'exécution sur chaque CAI. Il est possible de placer un "chien de garde" sur chaque CAI afin de détecter un dépassement du temps d'exécution.



Variables FIP (taille)	var1 : 12 octets	var2 : 16 octets	var3 : 12 octets	var4 : 18 octets	var5 : 2 octets
Ordre des tâches	T1,T2, T3, T4, T5, T6	T7, T8, T9, T10	T11, T13, T19, T20, T23	T12,T14, T15, T16, T17, T18, T22, T24	T21
Temps d'exécution	170 ms	150 ms	195 ms	275 ms	130 ms
Taille mémoire	110 koctets	90 koctets	700 koctets	300 koctets	75 koctets

Figure 6.3 – Schéma de l'implantation des tâches

Charge réseau (trafic périodique)	Temps d'exécution du CAI	Nombre de variables scrutables
60 %	100 ms	48 variables FIP de 128 octets
60 %	200 ms	96 variables FIP de 128 octets
60 %	300 ms	146 variables FIP de 128 octets

Tableau 6.1 – Charge réseau admissible

- Vérifier que les variables FIP sont bien transmises à l'aide du statut de promptitude et de rafraîchissement. Afin de constater un défaut de promptitude ou de rafraîchissement, des compteurs sont implantés pour évaluer le nombre de défauts. Les tâches pour les compteurs ont une taille et un temps d'exécution négligeables.
- Vérifier les principales fonctions exigées comme la puissance fournie à la charge (radiateur).
- Vérifier la sûreté de fonctionnement concernant la défaillance du correcteur PID (Proportionnel Intégral Dérivé) qui est dupliqué. Nous avons simulé une panne du correcteur PID dupliqué (cf. figure 6.4). Le défaut est détecté. L'information est envoyée à la tâche de sélection qui réalise le choix du correcteur PID n'ayant pas de défaut. Le changement du correcteur PID défaillant au correcteur PID dupliqué est signalé par le départ défaut sur la figure 6.4. Lorsque "la panne est réparée" (fin défaut sur la figure 6.4), le correcteur PID défaillant est réactivé. La sûreté de fonctionnement est ainsi assurée par une tâche redondante.

Il peut exister une légère différence de fonctionnement entre les correcteurs, même avec des valeurs PID identiques car ces correcteurs ne sont pas initialisés de la même façon. Cette différence s'exprime par une légère oscillation (cf. figure 6.4) et s'estompe au bout de quelques secondes.

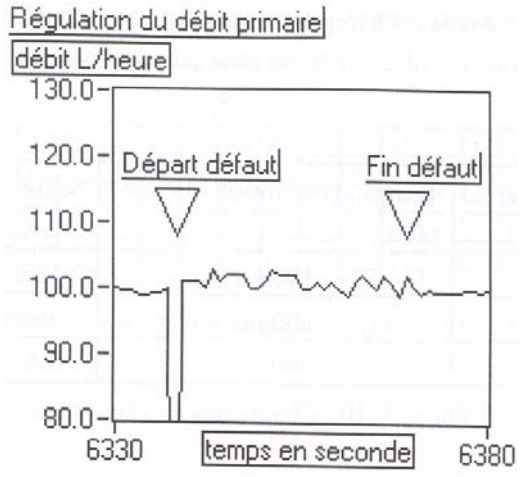


Figure 6.4 – Simulation d'une panne du correcteur PID

6.2. Affectation de traitements par approche génétique

Nous présentons l'utilisation d'un algorithme d'inspiration génétique appliqué à l'allocation de fonctions dans le cadre d'un système d'automatisation et utilisant des critères de disponibilité et de fiabilité dans l'évaluation des solutions envisagées [*CN99c*].

6.2.1. Architecture du système d'automatisation

L'objectif de l'étude est de déterminer l'architecture opérationnelle du système d'automatisation. L'architecture matérielle choisie se compose de trois automates interconnectés par un réseau de terrain. Chaque automate est directement connecté à un certain nombre d'actionneurs et de capteurs qu'il convient de déterminer. Par l'allocation des fonctions élémentaires "commander l'automate i" ou "effectuer la mesure y", le choix des instruments connectés aux automates est indirectement réalisé.

Cette architecture reprend celle couramment proposée par les constructions où un réseau principal fédère un ensemble d'automates et où chaque automate dialogue avec ses capteurs et ses actionneurs par un autre réseau spécialisé pour la communication avec ce type d'instrument ou par des lignes "point-à-point" (ex : 4 - 20 mA, 0 - 10 V…).

La nature des actionneurs permet de spécifier une position de repli lorsqu'un défaut est détecté. Cette particularité peut être prise en compte dans l'algorithme de recherche. Ceci permet de déterminer pour les vannes quelle est la meilleure position à prendre lorsque l'automate qui les commande vient à tomber en panne.

L'objectif global de la recherche consiste donc à déterminer pour chaque automate quels capteurs et actionneurs leur sont dédiés et plus particulièrement pour chaque actionneur quelle est sa position de repli en cas de défaillance détectée de l'automate le commandant.

6.2.2. Caractéristiques de sûreté de fonctionnement des instruments

Avant de pouvoir évaluer les paramètres de disponibilité et de fiabilité du système d'automatisation, le comportement des composants doit être connu. Arbitrairement, les caractéristiques suivantes ont été choisies :

- Pour les automates, deux états sont considérés : "disponible", où l'automate assure sa mission, et "indisponible", où l'automate n'est pas en état d'assurer sa mission et toutes ses sorties ont une valeur par défaut. Deux modes de défaillances sont pris en compte : "l'arrêt intempestif" dont les conséquences sont une mise à défaut de toutes les valeurs des sorties de l'automate et "le comportement incohérent" pour lequel les valeurs des sorties ne correspondent pas à celles spécifiées par sa programmation, dû par exemple à une défaillance du système de traitement de l'automate.
- Pour les vannes, trois états sont considérés : "disponible" où la vanne peut être ouverte ou fermée sur commande, "indisponible fermée" où la vanne reste bloquée dans une position fermée, et "indisponible ouverte" (bloquée en position ouverte). Pour les vannes de régulation, l'état "indisponible intermédiaire" est ajouté et caractérise le blocage de la vanne dans une position intermédiaire correspondant à un grippage. Les modes de défaillance pris en compte sont : "retour intempestif à la position par défaut" caractérisant un

défaut de la commande de la vanne, celle-ci revenant à une position de défaut, "mouvement intempestif" caractérisant comme défaut un mouvement de la vanne vers l'autre position extrême que celle par défaut, et enfin pour les vannes de régulation, "blocage dans une position intermédiaire" caractérisant le grippage de la vanne lorsque celle-ci est utilisée en régulation.

- Pour les capteurs, seuls deux états sont considérés : disponible et indisponible, selon que l'instrument est en état de fournir ou non sa mesure. Leurs modes de défaillance sont : "arrêt" correspondant à la cessation d'activité de mesurer et "mauvaise mesure" correspondant à la fourniture d'une valeur de la mesure ne correspondant pas à la réalité.

6.2.3. Mode de fonctionnement et disponibilité

De par son architecture, le processus offre de nombreuses configurations possibles pour satisfaire sa mission. Ainsi, le circuit primaire comme le circuit secondaire peuvent avoir une configuration série ou parallèle dans le cas d'un fonctionnement avec deux échangeurs. De même, un fonctionnement avec un seul échangeur répond aux objectifs du système même si la quantité d'énergie transmissible est réduite. Nous recensons ainsi six configurations possibles. Enfin, pour une même configuration du parcours des fluides, différents modes de marche peuvent être employés selon la ou les vannes utilisées pour la régulation. Globalement seize modes de fonctionnement ont été répertoriés [*CN99c*].

Comme il a été précisé précédemment, l'étude de la disponibilité s'appuie sur l'identification d'un ensemble de modes de fonctionnement. En accord avec la mission traitée qui est la régulation en débit et en température de la sortie du fluide du secondaire, quatre états de disponibilité ont été choisis. Le premier dit "disponible nominal" correspond à un état des composants permettant au système un fonctionnement dans les six configurations : parallèle, série ou utilisation d'un seul échangeur. Dans le second état de disponibilité dit "disponible dégradé-1", seule une partie des configurations peut être employée mais au moins une de ces configurations utilise les deux échangeurs. Dans le troisième état "disponible dégradé-2", seul un fonctionnement avec un échangeur est possible. Enfin, dans le dernier état dit "indisponible", l'état des composants ne permet pas l'accomplissement de la mission.

L'évaluation consiste donc à estimer la part du temps de chacun de ces états de disponibilité, selon les taux de disponibilité individuel de chaque composant.

6.2.4. Défaillance et fiabilité

L'étude de la fiabilité consiste ici à évaluer la probabilité d'occurrence de défaillances affectant la mission du système. Les modes de défaillance choisis en accord avec ceux des composants sont au nombre de trois. Le premier nommé "micro-arrêt" correspond à un arrêt intempestif du système suite à la défaillance d'un composant mais avec une possibilité de reprise dans la configuration dans laquelle le processus était utilisé avant la défaillance grâce à une intervention mineure : réinitialisation d'un automate, débranchement de l'alimentation en puissance d'un actionneur pour qu'il revienne à sa position par défaut. Le second nommé "arrêt" correspond lui aussi à un arrêt intempestif du système mais avec l'impossibilité de redémarrer dans la configuration initiale sans remplacer ou réparer le composant défaillant. Enfin, le dernier mode de défaillance considéré est un "mauvais fonctionnement" du système pour lequel, suite à une défaillance, il n'assure plus sa mission de régulation mais sans le détecter et sans se mettre dans une position de repli.

L'évaluation du critère de fiabilité revient à établir la probabilité d'occurrence de chacun de ces modes de défaillance.

6.2.5. Recherche de la meilleure architecture

La recherche de la meilleure architecture s'appuie sur l'utilisation d'une méthode génétique qui envisage un certain nombre de solutions d'architecture pour ne retenir que celles ayant obtenu la meilleure évaluation. Les architectures envisagée sont définies grâce à une valeur désignant pour chaque instrument (capteur ou actionneur) l'automate auquel il est associé et grâce à une valeur définissant pour chaque actionneur sa position par défaut prise lors d'une défaillance détectée de l'automate pilotant l'actionneur considéré.

La phase d'évaluation estime les deux critères de sûreté de fonctionnement c'est-à-dire les taux de disponibilité et les probabilités d'occurrence des modes de défaillance pour la fiabilité. Ces estimations s'appuient sur l'utilisation de diagrammes de décision permettant la détermination des probabilités de présence dans chaque

état selon les disponibilités respectives de chacun des composants. La transformation de ces critères en une unique valeur est réalisée à l'aide des correspondances suivantes qui les ramènent à un seul critère à caractère économique.

Critères	*Etats ou événement*	*Correspondance*		
Disponibilité	Disponible nominal	1 %	→	150
	Disponible dégradé I	1 %	→	140
	Disponible dégradé II	1 %	→	50
	Indisponible	1 %	→	-10
Fiabilité	Micro-arrêt	1 occurrence	→	-1
	Arrêt	1 occurrence	→	-10
	Mauvais fonctionnement	1 occurrence	→	-25

Tableau 6.2 – Correspondance entre les états ou événements et les coûts

L'allocation de la commande de chaque instrument à un automate est soumise à certaines contraintes matérielles. Ainsi, un automate possède quatre sorties analogiques, huit entrées analogiques, huit sorties de type "tout-ou-rien". Ces valeurs correspondent aux équipements utilisés réellement sur le processus.
Après traitement, l'architecture suivante a été trouvée comme maximisant les critères de sûreté de fonctionnement ramenés à un unique critère économique.

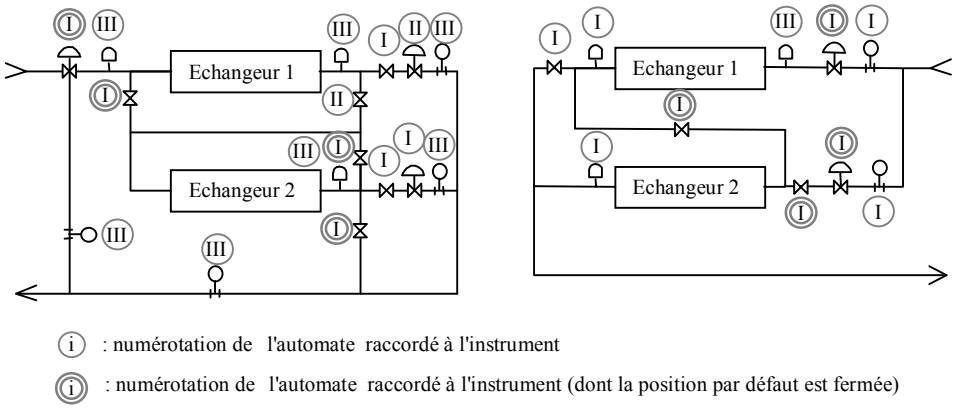


Figure 6.5 – Comparaison d'architectures du processus thermique pilote

L'étude de la solution montre que l'automate I est principalement chargé de la commande du processus et est éventuellement aidé par l'automate II pour certaines configurations de parcours des fluides. L'automate III n'a en revanche qu'un rôle de surveillance et a pour mission la détection des défauts. Ainsi, les valeurs des critères choisis et celles des caractéristiques des automates semblent, pour un tel processus, privilégier une répartition des traitements selon qu'ils participent à une fonction de commande ou de surveillance.

L'évaluation de la sûreté de fonctionnement pour cette solution a fourni les valeurs suivantes :

Critère de disponibilité
- Disponible nominal: 74.2525 %
- Disponible dégradé-I: 17.6305 %
- Disponible dégradé-II: 3.9057 %
- Indisponible : 4.2114 %

Critère de fiabilité
- Micro-arrêt : 6,37
- Arrêt : 53,47
- Mauvais fonctionnement : 0,45

(exprimé en nombre d'occurrence sur la durée de vie du système)

6.3. Evaluation de la SdF des SAID par une approche statique

6.3.1. Critères de sûreté de fonctionnement

Comme nous l'avons vu auparavant, évaluer la sûreté de fonctionnement d'un système d'automatisation est une activité délicate puisque par définition ce concept est difficilement quantifiable [CON 99].

Cependant, dans une optique de production et de rentabilité industrielles, certains attributs de la sûreté de fonctionnement peuvent être évalués sous forme de coût financier et s'intégrer à l'estimation d'un coût global de possession. Dès lors, la comparaison d'architectures devient réalisable sur la base d'une grandeur unique obtenue par l'association de plusieurs critères de coût.

6.3.1.1 Critère lié à la disponibilité

Dans le cadre de la conception d'un système d'automatisation, nous proposons de prendre en compte deux critères. Le premier est relatif à la disponibilité du système et traduit sa capacité à produire. Le second, relatif à la fiabilité/sécurité, est représentatif des conséquences induites par les défaillances.

La disponibilité et plus spécialement son corollaire l'indisponibilité sont cruciales au sein d'un système de production. Elles se traduisent par des pertes financières rapidement élevées dues à l'arrêt de production. La disponibilité est définie comme l'aptitude d'un dispositif à assurer sa mission à un instant donné, dans des conditions données (X 60-010). Elle est quantifiée par un taux qui est le rapport entre le temps utile, où il y a production effective et le temps d'ouverture où on souhaiterait produire.

Par l'estimation de ce taux et son application à une durée de production, nous estimons le coût de production.

6.3.1.2 Critère lié à la fiabilité/sécurité

L'adjonction d'un second critère de fiabilité/sécurité enrichit l'évaluation par la prise en compte des conséquences possibles des défaillances. En s'inspirant de la méthode de l'AMDEC, il s'agit de considérer l'effet des défaillances sur le système en terme de gravité et de probabilité d'occurrence. Globalement, nous identifions un ensemble d'événements susceptibles de se produire dont chacun est associé à un couple gravité/probabilité.

Leur probabilité d'occurrence est estimable à partir des probabilités de défaillance des composants susceptibles d'engendrer cet événement néfaste, de l'état du système, évalué de manière probabiliste lors de l'étude précédente de disponibilité, et son mode de fonctionnement (ex : marche nominale, marche lente ou en arrêt). Nous relions ainsi les modes de défaillances des composants à ceux du système. Le couple probabilité/gravité peut être finalement quantifié, dans la mesure où il est possible d'attribuer un coût à chaque conséquence : perte d'une partie de la production, de quelques équipements…

En conclusion, la quantification de la sûreté de fonctionnement, nécessaire pour une comparaison entre différentes solutions, repose sur une estimation a priori sous forme de coûts, d'une part, du taux de disponibilité et, d'autre part, d'un ensemble d'événements présentés par un couple probabilité/gravité.

6.3.1.3 Critère de coût du système

Aux critères précédents relatifs à la sûreté de fonctionnement, un critère coût du système est adjoint pour obtenir une évaluation globale du système. D'une manière simpliste, ce coût peut être la somme des coûts des composants. Cependant, comme le critère lié à la disponibilité tient compte d'une période de fonctionnement, il est préférable de considérer la somme du coût de base des composants et de leur coût d'entretien sur la période considérée.

6.3.2. Formalisation du problème

Cette partie présente la manière dont le problème d'allocation des traitements peut être formulé en vue de l'optimisation de l'architecture opérationnelle d'un système d'automatisation prenant en compte les contraintes de sûreté de fonctionnement qui viennent d'être précisées.

6.3.2.1 Modélisation des composants élémentaires

Pour chaque composant (capteur, actionneur… ou réseau de communication), un ensemble de paramètres est attribué permettant l'évaluation des trois critères précédents.

1- Concernant le critère lié au coût du système

Une valeur unique définit le coût du composant (investissement, installation, entretien…) qui, s'il est employé, est additionné pour obtenir le coût global du système.

2- Concernant le critère lié à la disponibilité

Pour chaque composant, un ensemble d'états peut être identifié et qualifie l'aptitude du composant à accomplir sa ou ses fonctions. Souvent réduit à deux états (disponible et indisponible), il peut cependant parfois inclure des états dégradés où seule une partie des services est susceptible d'être rendue. Un tel cas de figure se rencontre

généralement avec l'emploi d'instruments intelligents capables de traiter des défaillances partielles. En vue d'une quantification, un taux de probabilité est associé à chaque composant et dépend de la qualité de celui-ci, peu fiable ou très robuste, et de la politique de maintenance qui lui est affectée : échange ou réparation plus ou moins rapide. Globalement, ces données peuvent être représentées sous forme d'un tableau (cf. tableau 6.3).

3- Concernant le critère lié à la fiabilité/sécurité

Il s'agit ici de définir les modes de défaillance des composants. A chacun, nous associons un ensemble d'événements en fonction de la nature des services que peut rendre le composant considéré. En vue d'une évaluation plus globale des défaillances du système, une quantification de ces événements est indispensable et une probabilité d'occurrence doit leur être affectée, nécessitant d'avoir à disposition des données de retours d'expérience. La méthode proposée se limite à n'utiliser qu'un seul paramètre exprimé sous forme d'un nombre de défaillances par unité de temps. Finalement, nous définissons pour chaque composant une table de probabilité de défaillance (cf. tableau 6.3).

Etat	Probabilité
Disponible	97 %
Dégradé	2 %
Indisponible	1 %

Tableau 6.3 – Représentation des données relatives à la SdF d'un composant

Mode de défaillance	Probabilité
Mode 1 (ex : Blocage)	10^{-3}
Mode 3 (ex : Arrêt intempestif)	10^{-4}
Mode 2 (ex : Rupture)	10^{-5}
…	…

En vue d'effectuer une allocation des traitements sur ces composants, les contraintes matérielles doivent être prises en compte. Les deux contraintes suivantes ont été retenues dans la méthode proposée :

- La première est la charge limite que peut supporter chaque composant. Selon la nature du composant, la charge limite représente pour une unité de calcul la quantité de mémoire disponible, le nombre maximal d'opérations réalisables par unité de temps (équivalent à la vitesse de traitement) ou pour un réseau la quantité maximale d'informations transmissibles par unité de temps.
- La seconde est relative au problème d'interopérabilité. Il s'agit de vérifier que le composant choisi et le réseau qui le connecte sont compatibles. En effet, il est par exemple impossible de relier un capteur "Asifié" (c'est-à-dire "connectable" au réseau de terrain *AS-Interface*) à un réseau de type CAN ou une liaison de type 4 - 20 mA.

Ces contraintes permettent de contrôler les choix d'allocation des fonctions élémentaires en vue d'obtenir une architecture effectivement réalisable.

6.3.2.2 Modélisation de l'architecture matérielle

Toutes ces données concernant les composants sont absolues dans la mesure où elles sont indépendantes du processus à automatiser. En vue d'effectuer l'allocation des fonctions élémentaires, il convient de proposer une architecture matérielle préliminaire. Plus explicitement, il s'agit de définir l'ensemble et l'organisation des éléments susceptibles d'être employés pour un processus déterminé. Aux données précédentes (disponibilité, fiabilité, charge…), un paramètre de topologie est adjoint à chaque composant. Ce dernier est une position pour un composant ou un ensemble de points de connexion pour un réseau. Le résultat obtenu est une architecture matérielle préliminaire.

Plusieurs possibilités d'allocation des traitements élémentaires sont tentées sur l'architecture matérielle préliminaire. Seuls les composants auxquels au moins une fonction élémentaire a été affectée sont conservés. Le meilleur couple *allocation des traitements-architecture matérielle* est finalement retenu et forme l'architecture matérielle finale (cf. figure 6.6).

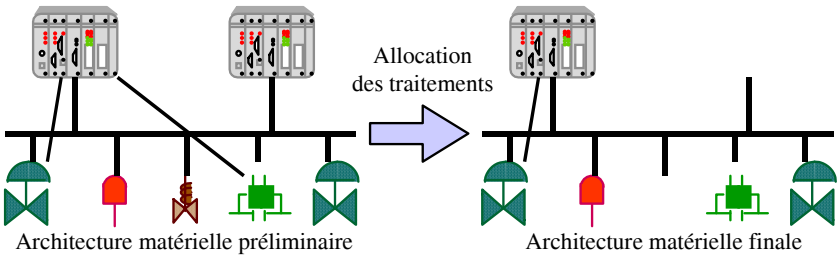


Figure 6.6 – Sélection de l'architecture matérielle

6.3.2.3 Modélisation des traitements élémentaires

Les traitements élémentaires sont les éléments qui par leur affectation vont déterminer l'architecture finale du système d'automatisation. La sélection du composant supportant chaque traitement est effectuée à partir d'un ensemble fini de composants. Celui-ci est établi à partir de l'architecture préliminaire et est soumis aux contraintes de topologie du processus à automatiser, les positions respectives des capteurs, actionneurs et consoles de commande étant dépendantes du processus.

Outre cette contrainte de localisation, la charge engendrée par chaque traitement élémentaire doit être spécifiée. Elle permet lors de l'affectation de contrôler que la charge limite de chaque composant n'est pas atteinte. Elle doit être exprimée par une grandeur compatible avec celle décrivant les limites du composant (Ko, bits/s,…). Enfin, les besoins en communication doivent être identifiés. Chaque traitement peut posséder plusieurs flux de données entrants ou sortants. A chacun, il convient d'affecter un ensemble de supports possibles de communication tirés de l'architecture préliminaire, dont un sera sélectionné lors de l'allocation.

A ces contraintes, des informations liées à l'évaluation des critères de SdF (sûreté de fonctionnement) doivent être adjointes. Comme pour les composants matériels, des états peuvent être associés aux traitements et décrivent la manière dont leur service est rendu. La forme de ces états est semblable à celle des composants et peut prendre des valeurs "disponible", "indisponible", "dégradé"… Il s'agit donc de définir la relation entre l'état du composant et celui résultant pour le traitement qu'il supporte. Une table de correspondance permet cette description (cf. tableau 6.4). De même, la défaillance d'un composant est modélisée par l'occurrence d'un événement. Pour exprimer la propagation de cet événement à travers la décomposition (utile à l'évaluation du critère de fiabilité/sécurité), une correspondance entre événements est appliquée comme pour les états (cf. tableau 6.4).

Etat du composant	Etat résultant pour le traitement élémentaire
Disponible	Disponible
Dégradée	Disponible
Indisponible	Indisponible
…	…

Evénement lié au composant	Evénement résultant sur le traitement élémentaire
Evénement A (ex : Blocage)	Pas de propagation
Ev. B (ex : Arrêt intempestif)	Ev. 1 (ex : Arrêt du service)
Ev. C (ex : Rupture)	Ev. 2 (ex : Mise en repli)
…	…

Tableau 6.4 – Correspondance des états et des événements

6.3.2.4 Modélisation des fonctions

Chaque fonction est l'association d'une ou plusieurs sous-fonctions ou traitements élémentaires. Leur organisation a été définie lors de la décomposition hiérarchisée. A l'inverse des traitements élémentaires que l'on associe à des composants matériels, ces fonctions n'ont pas de relation directe avec l'architecture matérielle (uniquement par l'intermédiaire de traitements élémentaires). Les seules informations à leur adjoindre concernent donc l'évaluation des critères.

Concernant le critère de disponibilité, il s'agit de définir les états que peut prendre chaque fonction. En définissant la relation entre ces états et ceux des ressources (sous-fonctions et traitements élémentaires), il est alors possible de calculer le taux de probabilité de chacun des états en fonction de ceux des composants utilisés, par l'intermédiaire des traitements élémentaires. Une table de vérité semble être un bon outil pour exprimer cette relation (cf. tableau 6.5). Une telle représentation permet d'exprimer assez simplement diverses formes de redondance.

Concernant le critère de fiabilité, il s'agit de décrire la propagation des événements au sein des fonctions. Dans la modélisation présentée, l'événement est généré par la défaillance d'un composant matériel et se propage de

manière ascendante à travers la décomposition fonctionnelle. Ainsi, pour chaque fonction, nous définissons l'événement induit pour toute occurrence d'événement sur une de ses ressources. Cette propagation à travers une fonction est cependant liée à son état. Selon les ressources disponibles, telles que la présence ou non de mécanisme de sécurité, de redondance…, les conséquences et donc la nature des événements induits diffèrent. Par ailleurs, tous les événements des ressources n'ont pas forcément un événement correspondant au niveau de la fonction par exemple dans le cas où une redondance pallie la défaillance d'une des ressources. Dans un tel cas, la propagation de l'événement initiateur est stoppée et n'atteint pas la mission principale du système. Globalement, cela revient à associer à chaque cas de la table d'état une table de correspondance relative à la propagation des événements (cf. tableau 6.5).

Table d'état :

Fonction		Sous-fonction 2		
		Dispo.	Dégradé	Indisp.
Sous-fonction 1	Dispo.	Dispo. ①	Dispo. ①	Dispo. ②
	Dégradé	Dispo. ①	Dégradé②	Dégradé②
	Indisp.	Dispo. ②	Dégradé②	Indisp. ③

Table de correspondance :

① événement 1 ➔ événement A
événement 2 ➔ événement B

② événement 1 ➔ événement C
événement 2 ➔ événement B

③ événement 1 ➔ événement D
événement 3 ➔ événement E

Tableau 6.5 – Table des états et de la propagation des événements

La description de chacune des fonctions de la décomposition hiérarchique du système permet de définir une relation entre les traitements élémentaires du système d'automatisation et sa mission, en terme d'états et d'événements. L'association finale des traitements élémentaires à des composants matériels dont les caractéristiques sont connues permet une quantification probabiliste et une évaluation des critères de sûreté de fonctionnement.

6.3.3. Mécanisme d'allocation des fonctions élémentaires

La méthode de recherche de l'architecture optimale revient à étudier différentes combinaisons où chaque traitement élémentaire est associé à un composant matériel. Cette technique peut être améliorée pour permettre un choix adéquat des fonctions à "redonder".

La démarche consiste à définir lors de l'établissement de la décomposition hiérarchisée un nombre important de redondances variées parmi lesquelles une sélection sera appliquée au sens de notre coût. Celle-ci est réalisée lors de l'allocation où seule une partie des traitements est associée à des composants matériels.

L'évaluation des critères de sûreté de fonctionnement s'effectue alors comme si tous les traitements avaient été alloués à des composants. Cependant, ceux n'ayant pas été affectés sont qualifiés d'indisponibles lors de la démarche d'évaluation. Pour que la solution demeure admissible, il est nécessaire que ces traitements soient des traitements "redondés".

6.3.4. Algorithmes employés

La modélisation proposée a été choisie en partie pour sa relative facilité à pouvoir être traitée de manière informatique.

6.3.4.1 Algorithmes d'évaluation des critères

Si de nombreuses méthodes permettent une évaluation quantitative et probabiliste des états d'un système (ex : graphe de Markov) ou de l'occurrence d'événements (arbre de défaillance, diagramme de succès/échec), l'utilisation d'une méthode inspirée des diagrammes de décision binaire [XIN 04a] [XIN 04b] [ZAN 99] ordonnés semble la plus adaptée. Il s'agit de graphes orientés acycliques où chaque nœud est lié à une variable [CHE 94].

Ils s'adaptent aussi bien à l'évaluation probabiliste des états qu'à celle de l'occurrence d'événements (cf. figure 6.7).

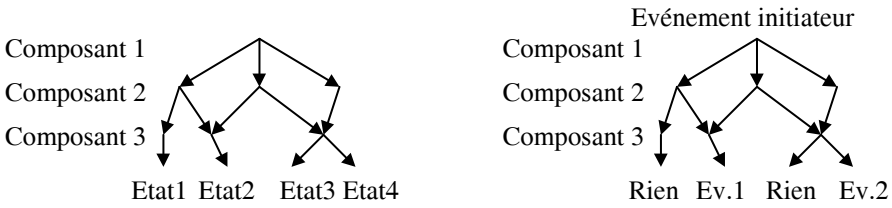


Figure 6.7 – Utilisation des arbres de décision

La construction de ces arbres est facilitée par la décomposition hiérarchisée et offre même s'il n'est pas optimal un ordonnancement correct des variables par les regroupements successifs des fonctions élémentaires. Elle consiste à établir en premier lieu l'arbre de la fonction principale où les nœuds sont ses ressources. Puis de manière similaire en développant chaque fonction, nous obtenons après plusieurs itérations un arbre représentatif de l'état de la mission du système en fonction de celui des composants.

Le même principe peut être appliqué pour chaque événement où l'arbre décrit l'événement résultant sur la mission en fonction de l'état des composants.

6.3.4.2 Algorithmes d'allocation

De nombreux algorithmes d'allocation ont été employés face à ce type de problème (Branch & Bound, recuit simulé, gradient…) [MEU 98] [HER 97]. Cependant l'emploi d'algorithmes d'inspiration génétique [MAR 94] (cf. § précédent) semble très adapté à ce type de problème d'allocation. En effet, ces algorithmes permettent d'effectuer une recherche parmi un très grand ensemble de solutions possibles. De plus, même s'ils n'aboutissent pas toujours rapidement à une solution optimale, ils sont capables de fournir des solutions intermédiaires acceptables aux concepteurs de ce type d'architecture.

6.4. Evaluation de la SdF des SAID par une approche dynamique

A l'issue des travaux précédents, il nous a semblé nécessaire de mettre l'accent sur les outils de modélisation et d'évaluation, y compris temporelle, des SAID. En effet, dans les études effectuées auparavant, nous nous sommes centrés sur la conception "a priori", comme résultant finalement de l'assemblage de composants ayant chacun leurs caractéristiques, afin d'en évaluer les performances globales.

Deux problèmes se sont posés à nous :

- le premier est que l'évaluation de la sûreté de fonctionnement globale était effectuée a priori ou de manière structurelle autrement dit comme une combinaison des sûretés des différents composants en prenant en compte essentiellement la topologie de l'architecture…
- le second est le besoin d'un outil de modélisation nous permettant de représenter les différents constituants (capteurs et actionneurs potentiellement intelligents, réseau de communication, unités de traitement telles que microprocesseurs, automates programmables, processeurs de traitement numérique du signal…) afin de pouvoir mesurer les performances de ces systèmes.

Il nous a semblé intéressant à partir de ces résultats d'aller plus loin, d'évaluer le comportement et les performances du SAID à l'aide de simulations notamment ou de méthodes formelles mais qui intègrent des aspects temporels ou dynamiques. Il est en effet indispensable de prendre en compte les sollicitations réelles des différents éléments dans le cycle de vie du SAID, pour pouvoir évaluer la fiabilité globale. Dans ce but, nous avons participé en 1999-2000 à certaines réunions du groupe de travail "Systèmes dynamiques hybrides" (groupe de travail SEE-EEA, actuellement GT du GDR Automatique) [AZZ 99] [FLA 98b] [MOS 99] [NEV 98] [RIE 99] [SIF 98] [TOM 03] [ZAY 02] à la recherche d'outils pour ces SAID qui sont par essence composés d'éléments à temps continu, à temps discret et d'éléments à événements discrets. Le but était de nous aider à effectuer un état de l'art des méthodes existantes. Nous pouvons en effet considérer une architecture distribuée de commande d'un processus via un réseau de communication comme un système hybride.

Depuis 2000, dans le cadre d'abord d'un DEA et puis dans le cadre d'une thèse de doctorat (DEA et thèse de Pavol BARGER), nous avons commencé la modélisation du SAID par réseau de Petri "étendus", à partir

notamment d'une bibliographie tant nationale (laboratoires participant aux groupes de travail RdP et SdH) qu'internationale (TRIVEDI (US) [TRI 03], BOBBIO (I) [BOB 00] [BOB 99] [BOB 98], HANZALEK (CZ) ...). Nous évaluons les propriétés, les compatibilités et les limitations de certaines extensions des réseaux de Petri (stochastique, coloré, selon JENSEN [JEN 97] par l'utilisation de l'outil Design CPN [DESIGN], arc inhibiteur...) [BAR 03] [JUA 02] [MEU 00] pour résoudre ce problème de la modélisation du fonctionnement et des dysfonctionnements en phase dynamique des SAID. La coloration permet, à l'aide des jetons, la représentation des modes de fonctionnement et/ou le contenu des trames de communication, en fonction de l'analyse effectuée et du niveau de granularité désiré. L'aspect probabiliste est pris en compte pour l'intégration d'événements aléatoires (défaillances, pannes…) [*CI03e, voir Annexe C papier 4*] [*CI03d*] [*CI03a*].

L'outil Réseau de Petri présente également l'intérêt d'être connu des spécialistes de la sûreté de fonctionnement et de pouvoir par conséquent servir non seulement pour modéliser la commande mais également pour évaluer les performances de la sûreté de fonctionnement, ces raisons ont guidé notre choix. Les capteurs et actionneurs (intelligents ou non), les régulateurs et autres fonctions de "supervision et/ou prise de décision", les moyens de communication, le processus lui-même peuvent être formalisés de la sorte, avec un point de vue à la fois continu et discret, en fonction des nécessités.

Le modèle a pour but l'évaluation de l'ensemble architecture – composant – répartition (architecture opérationnelle) retenu. Il permet également de simuler le fonctionnement normal et la mise en évidence des dysfonctionnements et des risques de fonctionnements dangereux ou catastrophiques.

Pour ces travaux, nous avons une approche "boîte grise", dans le sens où nous partons d'une analyse assez exhaustive de l'ensemble de l'architecture distribuée, par opposition à une approche intégralement probabiliste. Cet aspect nous paraît intéressant du point de vue de l'évaluation.

En conséquence, la démarche devra s'appuyer sur une rigueur en conception, afin d'obtenir une "robustesse" suffisante de la démarche, l'idée étant de pouvoir appliquer la démarche en regard notamment de la norme 61508 [61508]. Les outils à base de réseaux de Petri que nous utilisons doivent nous permettre d'évaluer des probabilités d'atteignabilité d'états critiques ou dangereux, en prenant en compte ces évolutions de l'information et des modes de fonctionnement du système.

Nous proposons dans ce chapitre de montrer quelques résultats obtenus en prenant en compte les aspects dynamiques pour un SAID ou NCS. Le premier paragraphe pose le problème. Le second paragraphe décrit l'application choisie concernant la régulation du niveau dans une cuve pour laquelle nous souhaitons pour des raisons de sécurité éviter le débordement. Le troisième paragraphe aborde l'étude effectuée tandis que le quatrième effectue un bilan des scénarios recensés et les résultats correspondants. Le cinquième paragraphe propose une discussion critique sur la généralisation des résultats.

6.4.1. Présentation de la méthode

Un problème important lorsqu'on évalue ce type de système est l'influence mutuelle qui peut exister entre des événements présents à des moments différents sur plusieurs composants. La propagation temporelle de ces événements n'est pas facile à spécifier et peut modifier considérablement le comportement du système.

Nous considérons dans la suite un système composé de capteurs, d'un actionneur et d'un régulateur, le tout relié par un réseau.

Une mesure analogique est prise par le capteur. Sa valeur est envoyée via le réseau de communication au régulateur qui détermine la nouvelle commande et la communique à l'actionneur. Une perturbation supplémentaire peut agir également sur le système mais elle n'est pas mesurée.

La communication entre les composants du SAID s'effectue naturellement par l'intermédiaire du réseau. L'importance accordée aux trames de communication peut être variable. En effet, une trame peut à un moment donné contenir une alarme de sécurité tandis que la trame suivante véhiculera une information non cruciale. Le degré d'importance ou de criticité de ladite trame est donc fonction de la donnée transportée mais également de l'historique du système et de son état courant.

Nous proposons l'utilisation d'un modèle à base de réseaux de Petri colorés selon Jensen [JEN 97] et utilisant l'outil Design/CPN [DESIGN] [SON 03]. Le modèle développé devra intégrer à la fois les aspects fonctionnels et dysfonctionnels de chaque composant.

Concernant l'étude des défaillances, il est possible d'intégrer au modèle des défaillances permanentes (système non réparable), des défaillances ponctuelles (erreur réseau) et des défaillances à durée limitée. Les modes de

défaillance pris en compte par les composants peuvent être des défaillances fréquentielles ou des défaillances sur événement.

6.4.2. Application

Nous proposons comme application la commande du niveau du liquide dans une cuve (cf. figure 6.8). La mission du SAID est de remplir et de maintenir le niveau désiré dans la cuve.
Pour pouvoir assurer son fonctionnement, le système (cf. figure 6.8) est composé de :

- un capteur analogique de niveau,
- deux capteurs binaires de sécurité,
- un régulateur,
- un actionneur (pompe),
- un réseau de communication,
- d'autres composants éventuels générant un trafic supplémentaire sur le réseau de communication, permettant de valider le modèle.

L'actionneur est une pompe placée à l'entrée de la cuve qui agit sur celle-ci. Une perturbation supplémentaire (fuite ou évaporation) peut agir également sur le système mais elle n'est pas mesurée. Dans l'état initial, la cuve est vide et donc prête à être remplie.

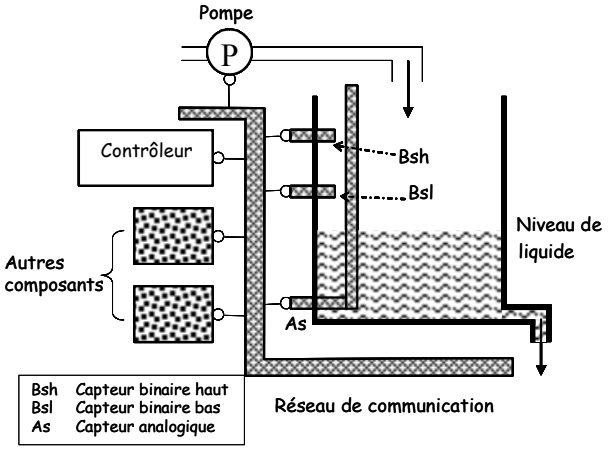


Figure 6.8 – Exemple de système : la cuve

La communication entre les composants du SAID s'effectue naturellement par l'intermédiaire d'un réseau. L'importance accordée aux trames de communication peut être variable. En effet, une trame peut à un moment donné contenir une alarme de sécurité tandis que la trame suivante véhiculera une information non cruciale. Le degré d'importance ou de criticité de ladite trame est donc fonction de la donnée transportée mais également de l'historique du système et de son état courant.

Un modèle à base de réseaux de Petri colorés selon Jensen et utilisant l'outil Design/CPN a été proposé pour le système schématisé figure 6.8 [*CI03e, voir Annexe C papier 4*] [*CI04b*].

Huit types de défaillances ou erreurs possibles sont considérés (cf. tableau 6.6) :

Code	Nom de l'événement	Taux d'occurrence moyen
1	Sensor_low_failure	1/1800 sec
2	Sensor_high_failure	1/1800 sec
3	Sensor_analog_failure	1/1800 sec
4	Controller_failure	1/1800 sec
5	Actuator_blocked	1/100 starts
6	Actuator_wearout	1/100 sec
7	Frame_alternation	1/50 frames
8	Frame_loss	1/25 frames

Tableau 6.6 – Liste des défaillances prises en compte

Les événements 1 à 6 sont des défaillances permanentes. Leurs réparations ne sont pas considérées. Les événements 7 et 8 sont des erreurs liées au réseau ; elles sont instantanées et affectent une seule trame de communication à la fois – cela peut correspondre à une courte perturbation électromagnétique par exemple.
Les événements 1 à 4 et 6 sont fonctions de la durée (*time-triggered*), alors que les événements 5, 7 et 8 sont fonctions de sollicitations extérieures (*event-triggered*). Les probabilités de défaillance utilisées ici sont plus grandes que la réalité permettant ainsi d'accélérer les méthodes de test et par conséquent de vérifier la faisabilité de la méthode.

Deux autres événements sont liés à la sûreté de fonctionnement :

Code	Nom de l'événement
9	Alarm_activated
10	Alarm_applied

Tableau 6.7 – Evénements liés à la sûreté de fonctionnement

Ces deux cas illustrent le fonctionnement du mécanisme de sécurité. L'alarme est activée lorsque l'information qui a le plus haut niveau (délivrée par le capteur binaire) arrive au contrôleur. La valeur de l'alarme est appliquée lorsque la commande de sûreté atteint l'actionneur.

Deux missions sont prises en compte pour l'analyse du système : le remplissage et le maintien du niveau. Par conséquent, deux types de défaillances pourront être identifiées :
- défaillance lors du remplissage,
- défaillance lors du maintien.

En ne prenant en considération que la phase de remplissage, le système fonctionne de la manière suivante : le démarrage se produit avec la cuve vide et est considéré comme terminé lorsque $\sum_{k=1}^{n} abs(y_k - \overline{y}) < \varepsilon$. y_k représente le niveau du liquide à l'instant k, $\overline{y}$ est le niveau à atteindre défini par l'utilisateur (400 unités de hauteur dans la suite) et ε est un écart toléré entre le niveau désiré et le niveau mesuré. Lors du fonctionnement nominal, le capteur analogique fournit des mesures qui sont utilisées par le contrôleur pour élaborer la valeur de commande et l'envoyer à l'actionneur. Si le niveau de liquide atteint le capteur binaire de sécurité, ce dernier envoie une alarme au contrôleur qui arrête immédiatement l'actionneur, une pompe. Celle-ci ne peut pas redémarrer tant que le capteur binaire indique que le niveau est trop élevé. Si pour n'importe quelle raison, le niveau continue de croître et atteint la valeur Max, la cuve est considérée en débordement et la mission a échoué…

Un des critères utilisés pour considérer que la mission a échoué est le fait que le niveau de liquide n'a toujours pas atteint 50 % de la consigne après 10 périodes d'échantillonnage. Ce type de défaillance est appelé *Not_started*.

La simulation s'arrête lorsque :
- la phase de remplissage est stabilisée,
- le niveau de la cuve déborde (niveau de liquide supérieur à Max),
- le niveau de liquide n'a toujours pas atteint 50 % de la consigne, après 10 périodes d'échantillonnage.

Le tableau 6.8 résume ces différents états.

Numéro	Nom	Condition	Commentaire
1	Successful	400 < niveau < Max	Désiré
2	Started_not_finished	niveau < 400	Non désiré, non dangereux
3	Overflow	niveau > Max	Non désiré, dangereux
4	Not_started	niveau (4*)Ts <20	Non désiré, non dangereux
5	Forced_stop	non stabilisé	Non dangereux

Tableau 6.8 – Etats finaux des simulations

6.4.3. Etude effectuée

Une question se pose concernant le succès de la stabilisation. En fait, l'obtention d'une simulation stabilisée n'implique pas forcément que le remplissage a réussi. Par exemple, il est possible d'envisager un cas de figure où le remplissage commence correctement puis, après l'occurrence d'une défaillance, le système se stabilise à un autre niveau que celui désiré… Pour cette étude, l'intervalle d'acceptabilité est compris entre la valeur de la consigne et la valeur Max de sécurité. Conformément à la définition, si la valeur finale est plus grande que la valeur Max, la cuve déborde. Si le niveau est plus bas que la valeur désirée, la défaillance s'appelle *Started_not_finished*.

La première question concerne l'influence du mécanisme de sécurité sur la fiabilité du système. Pour tenter d'y répondre, nous pouvons déterminer le pourcentage de scénarios amenant au succès lors des simulations de Monte-Carlo. 78 % des simulations aboutissent au succès sans le mécanisme, et 83 % avec. Nous pouvons considérer que le mécanisme de sécurité améliore la fiabilité de 5 points.

Même si le mécanisme de sécurité améliore les caractéristiques du système, nous sommes loin de la sûreté absolue. Nous pouvons en effet noter que plus de 6 % des scénarios défaillants ont au moins une fois activé le mécanisme de sécurité.

Ceci nous amène à nous poser dans la partie suivante une seconde question sur les causes de la défaillance.

Nombre total de scénarios	10000
Nombre de scénarios menant au succès	8218
Nombre de scénarios menant à l'échec	1782
Nombre de scénarios menant à l'événement "*Started_not_finished*"	150
Nombre de scénarios menant au débordement	1412
Nombre de scénarios menant à l'événement "*Not_started*"	156
Nombre de scénarios menant à l'événement "*Forced_stop*"	64
Scénarios vides (ne contenant aucun événement)	94

Tableau 6.9 – Résultats des simulations de Monte Carlo avec fonction de sécurité

6.4.4. Scénarios défaillants

Dans cette partie ne sont pris en compte que les scénarios qui conduisent à l'état de débordement. D'après le tableau 6.9, il existe 1412 scénarios de ce type. Le tableau 6.10 montre la distribution des longueurs[10] des scénarios défaillants.

Un tiers des scénarios défaillants ne contient qu'un seul événement et presqu'un autre tiers n'en contient que deux. Très peu de scénarios sont plus longs que six événements.

Nous allons maintenant analyser plus en détail les scénarios composés d'un seul événement (466). Nous pouvons nous demander quel événement a précédé le débordement. Le tableau 6.11 synthétise ces scénarios.

Avant d'entrer plus en détail dans les événements qui sont la cause des débordements, nous allons nous intéresser aux autres scénarios contenant un seul événement. 866 de ces scénarios sont envisagés et leurs états finaux sont décrits dans le tableau 6.12.

[10] La longueur d'un scénario se mesure au nombre d'événements qui le composent.

Longueur de scénario	Nombre de séquences	%
1	466	33.00
2	422	29.89
3	289	20.47
4	131	9.28
5	49	3.47
6	15	1.06
7	8	0.57
8	10	0.71
9	4	0.28
10	4	0.28
11	2	0.14
12	6	0.42
13	1	0.07
14	2	0.14
15	0	0.00
16	1	0.07
17	0	0.00
18	1	0.07
19	0	0.00
20	0	0.00
21	1	0.07

Tableau 6.10 – Distribution des longueurs des scénarios défaillants

Scénarios défaillants à un seul événement	Nombre
Sensor_low_failure	0
Sensor_high_failure	0
Sensor_analog_failure	2
Controller_failure	1
Actuator_blocked	0
Actuator_wearout	5
Frame_alternation	143
Frame_loss	315
Alarm_activated	0
Alarm_applied	0
Nombre total	*466*

Tableau 6.11 – Distribution des événements pour les scénarios défaillants ayant seulement un événement

Etat final	Nombre
Successful	345
Started_not_finished	2
Overflow	466
Not_started	53
Forced_stop	0
Nombre total	*866*

Tableau 6.12 – Etats finaux des scénarios à un seul événement

Nous pouvons constater que le nombre de scénarios à un seul événement qui mène au succès est comparable au nombre de scénarios menant au débordement. Le tableau 6.13 présente les événements qui mènent aux scénarios à succès.

Scénarios menant au succès comportant un seul événement	Nombre
Sensor_low_failure	1
Sensor_high_failure	1
Sensor_analog_failure	0
Controller_failure	2
Actuator_blocked	1
Actuator_wearout	6
Frame_alternation	113
Frame_loss	221
Alarm_activated	0
Alarm_applied	0
Nombre total	*345*

Tableau 6.13 – Distribution des événements pour les scénarios menant au succès comportant un seul événement

Les erreurs dues au réseau sont les plus fréquentes pour les deux types de scénarios. Il n'est pas possible de savoir quelle erreur de réseau conduit à la défaillance et quelle erreur ne conduit pas à la défaillance. Pour cette raison, nous avons enregistré les trames de communication corrompues pendant la simulation de Monte-Carlo.

334 scénarios comportant un seul événement et contenant une seule erreur de réseau ont conduit à un succès tandis que 458 autres ont conduit à un échec. L'étape suivante consiste à classer les trames de communication et à observer si ces classes conduisent uniquement à l'état final "échec" ou si elles peuvent conduire à un état final de succès.

Les informations majeures prises en compte pour la classification des trames sont : 1) les adresses de l'émetteur et du récepteur, 2) la date de l'émission et 3) le type de donnée transportée. Les trames dans les scénarios menant à l'échec sont échangées principalement entre le capteur analogique et le contrôleur. Les échanges entre le contrôleur et l'actionneur sont moins fréquents.

Les trames envoyées depuis le capteur analogique au contrôleur sont envoyées à la 2nde, la 3ème et la 4ème période d'échantillonnage du système. Les données qu'elles contiennent dépendent du moment de l'émission. La recherche de trames similaires dans l'ensemble des scénarios menant au succès et comportant un seul événement a montré qu'aucune trame similaire n'existe.

La simulation est légèrement différente pour le second groupe de trames, envoyé du contrôleur à l'actionneur. La principale différence est que si deux erreurs de trame apparaissent lors des deux premières périodes d'échantillonnage, alors le débordement s'ensuit. Si l'erreur apparaît à la troisième période, le débordement ne s'ensuit pas. Et s'il apparaît à la quatrième ou à la cinquième période, alors nous pouvons obtenir un débordement, mais ce n'est pas certain.

Ces résultats sont importants. Ils mettent en exergue la principale difficulté liée à l'évaluation de la sûreté de fonctionnement des systèmes intelligents. En fait, cela montre qu'aucun événement ne peut être analysé par lui-même et que le contexte global doit être pris en compte. Dans ce cas particulier, cela signifie qu'il faut étudier non seulement l'erreur de réseau mais également l'instant d'occurrence ainsi que le contenu de la trame corrompue. C'est seulement par ce type d'étude que l'on sait si une erreur de réseau est susceptible d'être suivie d'un débordement de la cuve ou non.

La question de savoir si les résultats obtenus à partir des scénarios contenant un seul événement peuvent être généralisés est abordée dans la partie suivante.

6.4.5. Généralisation des résultats

Après avoir obtenu les deux groupes de trames provenant des scénarios comportant un seul événement, il est important d'examiner si ces résultats se retrouvent dans d'autres scénarios. Cette vérification est faite sur l'exemple suivant : 130 scénarios comportant un événement conduisant au débordement sont composés de trames altérées ou perdues envoyés du capteur au contrôleur lors de la 2ème période d'échantillonnage. Les mesures communiquées varient de 155 à 200 unités de hauteur. Les 130 scénarios envisagés ici représentent un tiers de l'ensemble des scénarios défaillants comportant un événement (466).

La perte ou la modification de cette trame a été observée 565 fois (cf. tableau 6.14).

Etat final	Occurrence de l'événement
Successful	239
Started_not_finished	2
Overflow	323
Not_started	0
Forced_stop	1
Nombre total	*565*

Tableau 6.14 – Occurrence d'un événement particulier et son état final

D'après ce tableau, il est évident que la corruption de la trame donnée ci-dessus n'implique pas forcément que le scénario aboutira à un débordement. Seuls un peu plus de 57 % de ces événements se retrouvent dans les scénarios menant au débordement. Par conséquent, même si cette corruption est souvent présente dans les scénarios menant au débordement, et par ailleurs jamais présente dans les scénarios comportant un seul événement et menant au succès, il n'est en général pas possible de conclure que l'événement considéré est la cause du débordement.

Il est donc évident que les résultats obtenus à partir des scénarios comportant un événement ne peuvent pas être généralisés. En fait nous n'avons trouvé aucun événement qui peut par lui-même être considéré comme une cause de débordement. Les causes réelles sont donc fonction d'une suite d'événements, il nous faut donc prendre en considération les séquences comportant plus d'un événement. Une première approche de cette étude a été présentée dans [*CI03e, voir Annexe C papier 4*].

6.5. Conclusion

Dans un premier travail de thèse (F. HERMANN) et dans la mouvance d'autres travaux locaux effectués notamment au sein du projet MESR (convention MESR 92-P-0239) intitulé « Impact de l'émergence des réseaux de terrain et de l'instrumentation intelligente dans la conception des architectures des systèmes d'automatisation de processus » [BAY 95], nous nous sommes attachés à définir une architecture composée de capteurs et d'actionneurs intelligents, d'unités de traitement éventuellement intégrées aux composants, distribués autour d'un réseau de terrain.

A partir des missions que le système distribué doit assurer, une décomposition fonctionnelle utilisant la méthode SADT permet la définition de tâches élémentaires pouvant être implantées sur les unités de traitement.

Le but de ce travail était triple et a donné les résultats suivants :

- Démonstration de la faisabilité de mise en place d'un SAID composé de capteurs, d'actionneurs, d'interfaces homme machine et autres CAI autour d'un réseau de terrain. Le prototype développé est un processus thermique pilote composé d'une chaudière, d'un circuit d'eau primaire et d'un circuit secondaire interfacés par deux échangeurs [*CI99*].
- Modélisation dans un contexte de systèmes automatisés de production (SAP) des fonctions de contrôle commande, de suivi de production, de maintenance et de supervision-diagnostic implémentées ensuite sous forme de tâches sur le système distribué [*CI95b*]. L'étude fonctionnelle met en évidence les relations des différentes fonctions de conduite, de supervision et de suivi de production et de sélection. Cette étude permet également de montrer l'intérêt de concevoir une architecture distribuée afin d'améliorer la sûreté de fonctionnement, l'interconnexion des différents CAI et les possibilités d'évolutions.
- Développement d'un algorithme de répartition afin de distribuer au mieux les tâches sur les unités de traitement du système distribué afin de minimiser les coûts liés au temps d'exécution, à la consommation en mémoire et surtout les coûts de communication dus à l'utilisation d'un réseau de terrain [*CI98a, CI97c*]. Dans une première phase, l'algorithme de répartition était basé sur une méthode énumérative ; ceci pour deux raisons qui sont la facilité de mise en œuvre, l'absolue convergence et l'obtention d'une solution optimale. Dans le but d'améliorer cet algorithme, notamment pour des questions de temps nécessaire pour obtenir une répartition satisfaisante, nous avons proposé une amélioration basée sur les algorithmes génétiques et les stratégies d'évolution [*CI98c*]. La méthode proposée donne la possibilité d'allouer les tâches sur

l'architecture matérielle avec une solution optimale. Les critères et les contraintes définis permettent d'obtenir un dimensionnement de cette architecture. Avec le calcul du coût de communication pour le réseau WorldFIP, il est possible de dimensionner également les variables périodiques à configurer. D'autres algorithmes de répartitions comme la méthode Branch and Bound [CHE 90], la méthode du recuit simulé [KIR 83] ou les méthodes heuristiques ont été testées au cours de ce travail.

Ces travaux se sont concrétisés par la soutenance de la thèse de Frédéric HERMANN le 7 novembre 1997, dont le titre était : "Contribution à la répartition des traitements et des données sur une architecture distribuée équipée d'un réseau de terrain FIP : application à un processus thermique pilote".

Diverses perspectives ont été ouvertes par ce travail : l'automatisation du passage du modèle fonctionnel vers le modèle de tâches avec prise en compte des aspects spatiaux et temporels, la recherche d'une méthode de répartition plus efficace, la répartition dynamique...

Un second travail de thèse (B. CONRARD) avait pour but l'intégration des contraintes liées à la sûreté de fonctionnement et plus particulièrement la disponibilité et la fiabilité, en plus des aspects temps réel vus précédemment. Ce travail a conduit à des propositions pour une méthode et des outils associés afin de répartir au mieux les données et les traitements au sein d'un système d'automatisation distribué.

Nous prenons en compte dès la conception du système les paramètres liés aux défaillances prévisibles de chaque équipement et leur influence sur le comportement global de l'installation.

- Le premier aspect est relatif aux problèmes de sûreté de fonctionnement dans les SAID pris dans une double approche : d'une part, l'amélioration de la sûreté de fonctionnement induite par la distribution, d'autre part, les spécificités de la distribution en terme de sûreté de fonctionnement, les travaux s'appuient sur une méthodologie de décomposition hiérarchique et arborescente du système qui permet une évaluation a priori de la fiabilité et de la disponibilité [*CN01b, CI99, CN99d*]. Diverses stratégies de répartition prenant en compte les aspects Communication sont alors évaluées et classées en fonction de critères qui quantifient le comportement global du système en termes de sûreté de fonctionnement. Une méthode a été développée à partir des arbres de décision binaires.
- Le second aspect concerne la prise en compte de l'influence temporelle due à l'utilisation de réseaux de communication dans une boucle de régulation [*CI98b*]. Ces travaux ouvrent la voie à la prise en compte du réseau de communication utilisé dans la formalisation de la boucle de régulation. Cet aspect s'intègre dans la problématique de boîte à outil de conception de systèmes d'automatisation à intelligence distribuée.
- Le troisième aspect apporte une contribution à l'évaluation de la sûreté de fonctionnement de réseaux de terrain [*OU99, CI98e*].

Cette méthode d'aide à la conception permet de comparer diverses architectures possibles, sans envisager d'importants investissements lors de la réponse à un appel d'offres, par exemple…

L'informatisation de cette méthode, même si elle ne remplit qu'une part du travail de conception, est susceptible d'apporter une aide notable dans la détermination d'une architecture matérielle d'un SAID. Elle nécessite cependant l'utilisation de moyens informatiques requis par une recherche combinatoire assez vaste. De plus, elle doit être associée à une base de donnée précise sur les caractéristiques (fiabilité, disponibilité…) des composants d'automatisation disponibles.

La validation et l'explicitation de la méthode sur un cas concret consistent en l'application au PTP.

Ces travaux se sont concrétisés par la soutenance de la thèse de Blaise CONRARD le 24 septembre 1999, dont le titre était : "Contribution à l'évaluation quantitative de la sûreté de fonctionnement des systèmes d'automatisation en phase de conception".

Le troisième travail de thèse a permis d'enrichir les approches précédentes de caractéristiques liées à la dynamique du système et à l'évolution des modes de fonctionnement. Divers scénarios ont été pris en compte dans l'étude, ceux décrits dans le paragraphe précédent ainsi que d'autres scénarios [*CI04b*].

Cette méthode permet une estimation du taux de défaillance globale lorsque l'on ne connaît que les taux de défaillance des composants et que leurs corrélations ne sont pas estimées. La méthode permet également une classification dynamique des événements en fonction de leur influence sur les critères de sûreté. Dans une certaine mesure, nous pouvons considérer cette méthode comme une contribution, à approfondir lors de travaux futurs, à la détermination d'erreurs de causes communes [CHA 02c].

L'ensemble de ces travaux s'est concrétisé par la soutenance de la thèse de Pavol BARGER le 15 décembre 2003, dont le titre est : "Evaluation et validation de la fiabilité et de la disponibilité des systèmes d'automatisation à intelligence distribuée, en phase dynamique".

Les principaux résultats obtenus sont les suivants :

- Dans une approche de sûreté dynamique, nous avons montré comment les modes de fonctionnement et le choix d'une stratégie de commande pouvaient entraîner des dégradations plus ou moins rapides d'un actionneur, à cause par exemple d'une plus grande sollicitation donc d'une usure plus rapide. Cela implique une plus grande probabilité d'occurrences de défauts et donc une plus grande probabilité de mise en mode dégradé ou en panne [*CI03e, voir Annexe C papier 4*] [*CI02a*]. Une autre étude a été appliquée aux modes de pannes d'un capteur [*CI02c*].
- Nous avons proposé un tutoriel de modélisation des composants d'automatisation dans le logiciel Design/CPN : divers modèles de base du système d'automatisation à intelligence distribuée sont présentés, notamment le système discrétisé, un capteur "intelligent" communicant et potentiellement défaillant et un canal de communication.
- Nous avons apporté d'autres résultats concernant l'influence du réseau de communication, notamment des temps aléatoires de transmission, sur la plus ou moins grande sollicitation d'actionneurs, ce qui peut entraîner une plus ou moins grande probabilité de dégradation de ceux-ci [*CI02d*].

Nous proposons un récapitulatif des communications et publications concernant ces activités :

- répartition des données et traitements sur une architecture : *CI99, CI98d, CI98c, CI98a, CI97c, CI96d, CI96b, CI95b, CI95a.*
- évaluation du niveau de sûreté de fonctionnement d'une architecture distribuée et aspects réseau : *RI04c, RI04b (voir Annexe C papier 2), CI02b, CN01b, CI00a, OU99, CI99, CN99d, CN99c, CI98e, CI98c, CI98b*.
- évaluation en phase dynamique de la sûreté de fonctionnement des SAID : *CI04a (voir Annexe C papier 5), CI03e (voir Annexe C papier 4), CI03d, CI03a, CN03a, CI02d, CI02c, CI02a.*

7. Projet de recherche: méthodes d'aide à la conception et à l'évaluation de la sûreté de fonctionnement de SAID

Le projet de recherche que nous proposons ici s'inscrit dans la politique actuelle et future du laboratoire, étant entendu que j'ai eu la possibilité en 2004 de préparer le projet de recherche SACSS (Systèmes Automatisés Contraints par la Sûreté de fonctionnement et la Sécurité) avec le Pr. Jean-François AUBRY et, dans une moindre mesure, j'ai pu apporter une contribution au projet SYDER (Systèmes distribués et embarqués réactifs aux fautes) proposé par le Pr. Dominique SAUTER.

Je propose donc dans le premier paragraphe de rappeler mon implication dans les projets du laboratoire.

Le second paragraphe propose le projet de recherche que je souhaite mener dans les années à venir, présentant à la fois des aspects de recherche plus fondamentale et un souci de transfert technologique.

Les paragraphes suivants décrivent des actions plus précises à court terme, certaines d'entre elles ayant fait l'objet de travaux préliminaires ou étant en phase de démarrage. Les principales activités concernent l'intégration des approches fonctionnelles et dynamiques décrites dans les chapitres précédents, l'évaluation de la sûreté de fonctionnement d'une architecture distribuée par une méthode orientée information, l'évaluation d'une boucle de sécurité constituée d'instruments intelligents et de réseaux de terrain et une contribution sur l'évaluation de réseaux de sécurité. Les deux premiers travaux peuvent être considérés comme une contribution à l'évaluation de la sûreté de fonctionnement des SAID d'une manière générale, tandis que les deux autres sont plus proches de la recherche appliquée et concernent la sécurité.

La conclusion de ce chapitre apporte des perspectives d'équipe, dans la mesure où, outre les doctorants, un post-doctorant travaille avec moi. Quelques membres associés du CRAN ont également manifesté le désir de se rapprocher de nos activités de recherche, autour du groupe de travail A du contrat de plan Etat-Région et du projet SACSS, ce qui est déjà concrétisé par quelques communications communes, au moins soumises.

7.1. Implication dans les équipes-projet du CRAN

7.1.1. Participation au projet SACSS

Ma participation principale concerne le projet SACSS (Systèmes Automatisés Contraints par la Sûreté de fonctionnement et la Sécurité). L'objectif de ce projet est de rechercher des méthodes pour la conception des futurs systèmes automatisés sûrs de fonctionnement. Les caractéristiques fonctionnelles et dysfonctionnelles de ces systèmes sont prises en compte, de la spécification à la mise en service. Nous cherchons à fusionner les activités de spécification du système (l'architecture fonctionnelle, ce que nous voulons réaliser, le point de vue de l'automaticien) et d'évaluation de la sûreté de fonctionnement, afin d'aider à la décision du choix de l'architecture matérielle (avec quoi le faire).

Ce choix fait, il reste à étudier la projection de l'architecture fonctionnelle/dysfonctionnelle sur l'architecture matérielle afin de définir l'architecture opérationnelle du système automatisé, notamment le problème de la répartition des fonctions sur des entités coopérantes distribuées. Là encore, la sûreté de fonctionnement doit être un critère essentiel du choix, toute solution devant satisfaire aux exigences de performances et de sûreté. La recherche de modèles génériques associant les objectifs de spécification fonctionnelle et d'évaluation de la sûreté est un objectif prioritaire.

Dans ce projet, les réseaux de Petri (RdP) constituent un bon modèle pour jouer un tel rôle. Sous l'une de leurs formes, ils permettent de modéliser le fonctionnement des parties opératives des systèmes (discrets ou hybrides). Pour la simulation, ils permettent de spécifier la partie commande (RdP interprétés) et permettent par couplage avec celle de la partie opérative d'accéder à la simulation du fonctionnement global. L'aspect dysfonctionnel peut quant à lui être pris en charge par la variante stochastique des RdP, par passage au modèle Markovien par exemple ou par simulation de type Monte Carlo.

Quelle représentation minimale du système peut alors constituer le noyau duquel par déclinaison il soit possible d'aborder simultanément les trois aspects de spécification, d'évaluation et de simulation ?

Quelques inconvénients sont cependant inhérents à ces modèles. Citons en particulier la difficulté d'une représentation hiérarchisée et le risque d'explosion combinatoire encore aggravé lorsque nous cherchons à évaluer les performances de l'architecture opérationnelle du système, notamment avec l'introduction des systèmes à intelligence distribuée pour lesquels les possibilités de reconfigurations sont élevées.

7.1.2. Participation au projet SYDER

Le projet SYDER (Systèmes distribués et embarqués réactifs aux fautes) est un projet transversal du CRAN. Nous contribuerons, par une application des approches et méthodes que nous développons ou utilisons dans le projet SACSS, à la définition d'une architecture distribuée commandée via un réseau de communication. La modélisation du système distribué, par diverses approches (fonctionnelle, informationnelle…) peut être envisagée.

Le modèle obtenu aurait pour objectif de permettre une évaluation des paramètres de la sûreté de fonctionnement prenant en compte les divers modes de fonctionnement du système, sachant que les méthodes existantes ne permettent pas une évaluation aisée des systèmes intégrant de l'intelligence (capacité de traitement et de communication), aussi bien pour de grands systèmes distribués que des systèmes embarqués autonomes.

Une stratégie pourra consister à tenter de borner le fonctionnement du système dans un espace maîtrisé intégrant les modes nominaux et les modes dégradés (replis) et d'estimer la probabilité que le système sorte de cet espace.

Les réseaux de Petri, colorés ou stochastiques, peuvent contribuer à cette évaluation.

Les normes d'évaluation de la sûreté de fonctionnement ou de la sécurité (61508, 511) ne donnent pas de méthode d'évaluation de ce type de système mais sont le cadre dans lequel nous devrons travailler.

7.2. Projet : Evaluation du niveau de sûreté de fonctionnement de systèmes d'automatisation à intelligence distribuée

Notre but est de répondre aux besoins sociétaux identifiés dans l'introduction du présent mémoire, relatifs à la sûreté de fonctionnement des systèmes intégrant de l'automatique ou de l'informatique embarquées. A ce besoin sociétal se rattachent un besoin scientifique et un besoin de transfert. Le besoin scientifique consiste à développer des méthodes permettant d'évaluer la sûreté de fonctionnement. Le besoin de transfert, quant à lui, est lié à la nécessité de transférer vers le milieu industriel des méthodes et des outils permettant, d'une part, la prise en compte des aspects normatifs dans la conception des SAID et, d'autre part, l'évaluation d'architectures plus ou moins complexes, pouvant aller jusqu'à la quantification du niveau de SIL desdites architectures.

7.2.1. Réponse à un besoin scientifique

Le besoin scientifique auquel nous souhaitons répondre dans les années à venir est donc relatif à l'évaluation de la sûreté de fonctionnement de SAID. Pour cela, les points durs que nous avons pu identifier sont les suivants :

- Etre capable, en phase de conception, de comparer diverses architectures possibles avec, pourquoi pas, la quantification d'un niveau de SIL global, éventuellement de niveaux de SILs par sous-ensembles (ce point implique d'être capable d'isoler des sous-ensembles suffisamment indépendants les uns des autres pour pouvoir les traiter séparément), et également d'identifier les points sensibles, ou les fragilités de l'architecture, à surveiller de plus près.

- Pouvoir valider ensuite, en phase de prototypage, les choix faits en phase de conception, en comparant les résultats obtenus au niveau des essais sur le prototype aux résultats obtenus par le modèle.

La démarche, aussi bien pour la quantification en conception que pour la validation en phase de prototypage peut combiner plusieurs approches : des approches d'évaluation des composants (capteurs, actionneurs intelligents, unités de traitement, réseaux) et des approches d'évaluation de l'intégration.

La problématique de l'évaluation des composants implique les points suivants :

- les composants physiques peuvent être évalués avec les méthodes traditionnelles, les résultats peuvent être obtenus par des tests constructeurs ou des retours d'expériences,
- les composants numériques nécessitent la prise en compte de l'interface entre le monde physique et le monde numérique, la prise en compte de l'architecture numérique, la prise en compte du logiciel embarqué

(avec deux aspects qui sont le test de l'algorithme et le test de l'implémentation, autrement dit de la manière dont le logiciel est codé pour être implanté sur le processeur) ; comme nous l'avons dit auparavant (cf. chap. 4), cet aspect est traité par le RTP 21 qui fédère les communautés du test électronique et de la prouvabilité logicielle,

- les réseaux, cœurs de la fonction communication, où diverses propriétés matérielles (tests de compatibilité électro-magnétique) ou logicielles et fonctionnelles (déterminisme, temps réel, qualité de service), peuvent être évaluées,
- les aspects interfaces entre les composants et le réseau de communication doivent aussi être pris en compte.

La partie sur laquelle nous comptons mettre l'accent est basée sur l'approche système, c'est-à-dire l'évaluation de l'ensemble, supposé être un système dynamique, évoluant au cours du temps. L'évolution du système est fonction de l'ensemble de ses constituants et interfaces. Nous pouvons considérer être doublement en "fiabilité dynamique" (ou sûreté de fonctionnement dynamique), d'une part, parce que nous devons prendre en compte par cette approche les séquencements de défaillances (certaines mises en situation de dysfonctionnement sont en effet le résultat d'un séquencement d'erreurs) et, d'autre part, parce que nous prenons en compte le vieillissement des constituants comme étant une conséquence des sollicitations et donc dépendant de l'évolution du système.

Afin d'atteindre ces objectifs, il nous faut mettre en œuvre des méthodes et des outils.

A l'image d'un réseau de Petri coloré qui nous semble donc un bon outil de départ, surtout s'il peut accepter des temporalités et intégrer des aspects stochastiques, nous pouvons caractériser trois aspects dans l'évaluation d'architectures. En effet, les places peuvent représenter la topologie de l'architecture, les jetons la dynamique d'évolution et la coloration, le contenu informationnel qui circule sur le système. Les approches fonctionnelles et dynamiques développées dans le présent mémoire sont des contributions aux deux premiers points, l'approche informationnelle abordée plus loin dans ce chapitre contribuera au troisième point.

Nous pensons en effet qu'il sera difficile d'envisager une évaluation exhaustive des SAID par des méthodes intégralement formelles dès que la dynamique est forte bien que cette piste soit à creuser afin de pouvoir l'utiliser au mieux. Par contre, essayer d'analyser le SAID sous différents aspects afin de contribuer à son évaluation nous paraît réaliste, même si cette hypothèse est limitée de fait par l'explosion combinatoire.

Divers méthodes et outils peuvent être envisagés. La caractéristique de ces outils est qu'ils devront pouvoir modéliser des aspects temporels et des aspects stochastiques, qu'il serait intéressant aussi qu'il puissent intégrer plusieurs bases de temps et, enfin, qu'il faut pouvoir représenter du temps discret et des événements discrets. Nous comptons approfondir les aspects liés à l'utilisation des réseaux de Petri colorés, stochastiques, temporisés.

Il nous paraît intéressant par ailleurs de comparer les réseaux de Petri à d'autres outils de modélisation tels que les réseaux bayésiens dynamiques [WEB 03], par exemple.

Le problème de l'évaluation est également à prendre en compte. Les réseaux de Petri permettent, lorsque l'on respecte certaines contraintes, de vérifier certaines propriétés (bornitude, vivacité …) et certains outils, tels DesignCPN avec MLStandards, permettent d'envisager l'évaluation des modèles, grâce notamment à la possibilité de programmation.

Sur ces aspects d'évaluation, qui n'a pas toujours été très approfondi dans les travaux passés, nous pensons qu'il peut être intéressant d'utiliser des techniques d'analyses afin de classer les scénarios obtenus par simulations de Monte-Carlo. Pour cela, nous pensons que des approches floues ou l'utilisation de techniques possibilistes pourraient présenter un intérêt.

Quant aux travaux que nous pensons développer, certains d'entre eux sont dans la poursuite de travaux déjà abordés :

- Intégration, complémentarité et opposition des approches statiques et dynamiques : il s'agit de voir comment ces deux approches peuvent être complémentaires. L'approche statique nous permet de mettre en évidence plusieurs architectures opérationnelles possibles. C'est une approche de conception, elle permet de mettre à plat tous les aspects concernant les différentes fonctions que le système doit accomplir et ces potentialités de défaillances. L'approche dynamique prend en compte l'évolution temporelle. Le travail consiste à voir

comment il va être possible d'intégrer ces deux approches, en terme de démarche et en terme de validation des résultats sur des applications. L'idée pourrait être de développer de cette manière l'embryon d'une boîte à outil de conception-évaluation de la SdF de SAID.

- Sur l'approche statique : nous pensons la compléter par des méthodes d'analyse de graphes, d'optimisation d'architectures, afin de voir l'applicabilité de ces méthodes sur les SAID, pour lesquels les composants sont des composants matériels, et les contraintes de temps réel sont différentes des systèmes informatiques.
- Approche dynamique : nous pensons la compléter par une approche d'évaluation de typologies de scénarios (dans le cadre d'un DEA, par exemple).
- Approche informationnelle : cette approche, sur laquelle nous avons commencé à réfléchir, traite de l'analyse de la dynamique du système en prenant en compte l'évolution de l'information en son sein. Cet aspect est décrit plus en détail dans le paragraphe 7.4.
- Approfondissement de la notion d'interface, interface entre un système échantillonné, qui constitue le composant matériel intelligent, et le réseau de communication.

Un dernier aspect qui nous intéresse, belle illustration de l'interface entre l'Automatique, le Génie Informatique et la Sûreté de Fonctionnement, est l'Evaluation du niveau de SIL d'une boucle de régulation en fonction de l'algorithme de commande. L'évaluation de la boucle fermée n'est en effet pas triviale et voir l'influence de l'algorithme de commande sur le niveau de SIL de la boucle nous paraît un travail pertinent à mener.

7.2.2. Réponse à un besoin de transfert

Le type de recherche sur lequel nous travaillons a des applications évidentes dans la société. Paradoxalement, ce besoin de la société n'est pas clairement identifié. En effet, la prise en compte de la sûreté de fonctionnement et de la sécurité implique des coûts non directement liés à la productivité, tout au moins tant que la législation n'a pas transformé en coût les dégradations sur l'environnement et la société.

La normalisation existe mais elle est souvent partielle, voir partiale, et ne fournit pas de méthodes d'évaluation et encore moins d'outils, elle préconise simplement certaines règles à respecter et valeurs à atteindre.

Notre travail a pour but de répondre à ce besoin, en proposant des méthodes permettant d'aider à l'évaluation des SAID. Nous souhaiterions, pourquoi pas, dans les années à venir participer à la mise en place d'une boîte à outils ou d'un outil logiciel, intégrant plusieurs méthodes et approches permettant l'évaluation de SAID, le choix de l'architecture la meilleure intégrant les contraintes de coût, d'évolutivité, d'interopérabilité, de sûreté de fonctionnement.

Les aspects plus particulièrement dédiés à la sécurité nous intéressent également, et les deux aspects sur lesquels nous souhaitons progresser sont les suivants :

- Modèle d'une boucle de sécurité avec un réseau de terrain ASi-Safe (modèle du capteur de sécurité, de son interface, du réseau de sécurité, de l'actionneur de sécurité, de son interface),
- Etude d'un réseau de sécurité : définir le cahier des charges d'un réseau de sécurité, en voyant comment prendre en compte les aspects interfaces avec l'extérieur, et voir si l'on peut définir des contraintes à respecter sur ces interfaces pour que le réseau soit utilisé dans des conditions correctes, et donc être effectivement considéré comme un réseau de sécurité.

Une application potentiellement intéressante pourrait être la commande via réseau d'un coussin gonflable automobile. Est-ce réaliste ? Peut-on envisager cela et sous quelles conditions ?

Ce paragraphe avait pour but de situer le projet de recherche, les axes de recherche plus fondamentaux ou appliqués que je souhaite développer dans l'avenir, dans le cadre du projet de recherche SACSS et également dans le cadre de projets transversaux tels que SYDER. Les points forts de ce projet sont la recherche du niveau de SIL d'un système de type SAID mais également l'identification des risques d'occurrence de défaillances rares mais dangereuses ou critiques, même s'il est en ce cas impossible de quantifier une probabilité, seulement de donner une possibilité ou plausibilité...

7.3. Action 1 : Modélisation d'un SAID et évaluation de la sûreté de fonctionnement par intégration des approches fonctionnelles et dynamiques

7.3.1. Description de l'action

Evaluer la sûreté de fonctionnement d'un système automatisé, dont la commande, distribuée, transite via un réseau de communication, n'est pas simple. Les méthodes classiques de la sûreté de fonctionnement, fort bien adaptées aux systèmes à mode de fonctionnement unique et pour lesquelles la coopération entre les différents composants du système relève de la mise en série ou en parallèle, ne conviennent pas ici.

Dans la poursuite de travaux précédents, il est proposé d'appréhender la modélisation d'un système distribué intégrant divers éléments (capteurs, actionneurs, contrôleurs) répartis autour d'un réseau de communication, afin de définir et de proposer une ou des méthodes de modélisation satisfaisantes.

L'objectif recherché de la modélisation est l'évaluation, de manière formelle ou en simulation, de paramètres de sûreté de fonctionnement, en prenant en compte les différents modes de fonctionnement du système. Comme cela a été précisé précédemment, il pourra s'agir de borner le fonctionnement du système dans un espace maîtrisé intégrant les modes nominaux et les modes dégradés (replis) et d'estimer la probabilité que le système sorte de cet espace.

7.3.2. Sujet de thèse : Evaluation et vérification de paramètres de sûreté de fonctionnement d'un système distribué

Problématique

Le sujet de thèse s'inscrit dans le cadre de l'évaluation de la disponibilité et de la fiabilité des systèmes d'automatisation à intelligence distribuée, systèmes composés de capteurs, d'actionneurs et d'unités de traitement (régulateurs, superviseurs...) architecturés autour d'un medium de communication.

Dans le cycle de conception de ces systèmes, une rupture existe dans l'intégration des contraintes de sûreté de fonctionnement entre les étapes de spécification de l'automatisation d'un processus et d'implantation sur une architecture matérielle. Dans la première, nous pouvons intégrer les mécanismes de réaction aux défaillances du processus et en évaluer les performances. Dans la seconde, nous nous contentons souvent d'une évaluation de la fiabilité de l'architecture matérielle indépendamment de l'application.

L'évaluation globale de la sûreté de l'architecture opérationnelle incluant le matériel et l'ensemble des fonctions qui y sont réparties, se heurte au problème de l'interaction entre ces deux entités. Le travail de thèse sera une contribution à l'élaboration de méthodes permettant l'évaluation de tels systèmes d'automatisation, pour lesquels il est difficile de prendre en compte tous les aspects liés à la dynamique et aux changements de modes de fonctionnement (reconfigurations notamment), par le biais des méthodes classiques de sûreté de fonctionnement.

Outil, fondement

Un tel système, pouvant être vu sous différents points de vue (celui de l'automaticien, celui du spécialiste en sûreté de fonctionnement, celui du spécialiste des réseaux), se doit d'être décrit de manière compréhensible selon ces divers points de vue. Idéalement, un modèle unique pour la spécification, l'intégration et l'évaluation du système, devrait pouvoir intégrer ces points de vue en permettant son évolution en terme de granularité et d'objectif.

Aucun formalisme n'est imposé a priori. Les réseaux de Petri ou les automates finis stochastiques seront évalués ainsi que d'autres outils, dans des approches aussi bien analytiques que par simulation. Afin de réduire la complexité attendue, nous tendrons d'emblée vers une généricité dans les modèles ainsi qu'une construction hiérarchique.

Travail demandé

Un certain nombre de voies ont déjà été exploitées, ou plus précisément abordées, lors de travaux précédents. Les travaux de Raphaël SCHOENIG apportent une contribution dans le passage des spécifications vers l'évaluation probabiliste, par la proposition d'une réduction de modèle par une approche à la fois analytique et par

simulation (les outils utilisés sont les réseaux de Petri interprétés et stochastiques et les graphes de Markov). Les travaux de Karim HAMIDI, en cours, proposent une approche progressive par raffinement afin d'identifier toutes les séquences menant à l'événement danger, l'objectif étant l'évaluation d'une boucle de sécurité (les outils utilisés sont les automates finis stochastiques). Le travail de Pavol BARGER a montré l'influence d'un réseau de communication sur l'évaluation de paramètres de sûreté de fonctionnement (les outils utilisés sont les réseaux de Petri colorés à arc probabiliste, et la simulation de Monte-Carlo). Les travaux de Blaise CONRARD ont montré comment il était possible d'évaluer une architecture distribuée a priori en utilisant une méthode basée sur les arbres de décision binaire, et permettant de propager les événements (défaillance) et les états (fonctionnement ou dysfonctionnement) dans le modèle du SAID.

Ces travaux récents et en cours serviront de base au travail à effectuer. Il est demandé dans ce travail de proposer un modèle de système distribué critique (c'est-à-dire où le paramètre de sécurité est fondamental, ex : direction automobile par réseau, X by Wire…), intégrant un réseau de communication, et de proposer l'évaluation de paramètres de sûreté de ce système, prenant en compte le réseau. L'idée est de regarder d'un peu plus près quels sont les points qui sont explicités dans la norme (principalement la 61508), et quels sont les points plus flous, afin d'avoir un regard critique et de voir comment et avec quels critères il est possible d'aider les concepteurs de systèmes distribués critiques. Une première approche pourra consister à effectuer la synthèse des approches statiques et dynamiques décrites dans le présent document afin de voir dans quelle mesures ces approches peuvent être complémentaires et de mettre en évidence leurs insuffisances.

L'ensemble de ces travaux entre dans le cadre de la conception, l'optimisation et l'évaluation de systèmes distribués.

Les travaux de recherche ou autres documents dont nous pouvons nous inspirer sont les suivants :
[61508], [AUB 99], [AUB 02], [AUB 03], [BEE 03], [BAR 03], [BLA 04], [DIA 01], [HAM 03], [JAM 01], [JAM 02], [NOU 03], [POU 98], [ŞAH 04], [SCH 03a], [SHA 98], [SIG 96], [TRI 03], [ZIO 04]
[*CI03b*], [*CI03e, voir Annexe C papier 4*], [*CI04a, voir Annexe C papier 5*]

7.4. Action 2 : Modélisation d'un système distribué par une approche orientée information

7.4.1. Description de l'action

Il s'agit d'une voie nouvelle pour l'évaluation de la fiabilité d'un système partant de la notion d'information manipulée [DAI 03]. Un modèle de définition a été proposé [*CI03b*], dans le cadre d'un partenariat avec l'équipe TRIO (Temps Réel et InterOpérabilité) du LORIA (Laboratoire lorrain de recherche en informatique et ses applications) [JUM 03].

La méthode proposée consiste à considérer l'information circulant dans un SAID. Deux problèmes se posent alors :

- Evaluer les parcours des différentes données, mesures, échantillons… utilisés pour élaborer les variables de commande du système. L'intérêt est de prendre en compte la manière dont ces diverses données sont élaborées, émises, transmises, "agglomérées" ou "fusionnées" en intégrant les aspects temporels (retards de transmission, délais de calcul, stockage plus ou moins long dans des tampons ou mémoires…) et leur obsolescence courante, afin de pouvoir leur attribuer un caractère de crédibilité.
- Evaluer la criticité des variables par une analyse de risques, afin de mettre cette criticité en relation avec la crédibilité des variables correspondantes. En remontant, à partir des variables critiques, à la manière dont lesdites variables ont été élaborées, il est possible de mettre en évidence les différents composants utilisés et d'étudier leur influence vis-à-vis des variables critiques. Ceci doit nous permettre d'isoler les points critiques de l'architecture.

Les résultats actuels de cette activité sont la proposition d'un modèle de fiabilité d'une boucle ouverte, publiée dans [*CI03b*]. Cette méthode se veut une alternative aux méthodes d'évaluation probabilistes traditionnelles [DAV 02b] [BIE 02].

Comme nous avons déjà pu le constater, le réseau, qui apparaît à différents endroits de la boucle ou de l'architecture, peut être considéré comme une source potentielle de défaillances de mode commun [CHA 02c]. Ceci doit bien sûr être pris en compte, en particulier lorsque plusieurs boucles de commande partagent le même réseau.

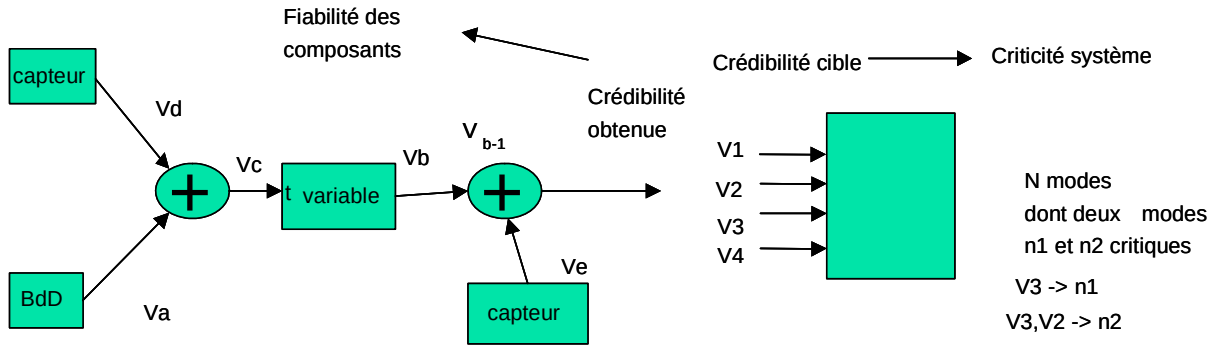


Figure 7.1 – Figure générale présentant l'approche orientée "information"

L'étude proposée à titre d'illustration concerne la commande en boucle ouverte d'un système échantillonné simple utilisant une seule horloge. Si l'on suppose que ce système est une cuve, telle que décrite dans le chapitre précédent par exemple, nous proposons de regarder plus en détail le temps d'ouverture, appelé TO, déterminé par un contrôleur PI et d'analyser les modes de défaillance de cette variable.

Calculons le temps d'ouverture. TO_n est le temps d'ouverture au temps n, ε_n représente l'écart entre la mesure et la consigne au temps n.

Les modes de défaillance pour la variable TO_n sont les suivants :

1) temps d'ouverture moyen excessif
- Si TO_n est plus grand que le temps de cycle alors le temps d'ouverture est excessif ;
- Si $TO_{n\_requis} < TO_n < T_{cycle}$ alors le temps d'ouverture est excessif, mais moins grand que précédemment.

Les conséquences de ce mode de défaillance peuvent être un débordement dû au temps moyen d'ouverture excessif.

2) temps d'ouverture moyen insuffisant alors la résistance n'est pas couverte par le liquide.

Ces deux modes de défaillance peuvent être pris en compte, par le maximum des deux en gravité.

Les causes de dysfonctionnement de la vanne sont principalement le blocage à l'ouverture et le blocage à la fermeture. Le débordement toléré est un débordement tous les 100 ans (7.10^6 heures) donc $\lambda = \frac{1}{7.10^6}$. Ces contraintes doivent être prises en compte dans la définition de l'architecture requise.

La question qui se pose est comment fabrique-t-on TO_n, à partir de deux données ε_n et ε_{n-1} qui n'ont pas le même âge (cf. figure 7.1 et la formule 1 ci-dessous). Est-il possible de quantifier la fiabilité de cette variable de commande ?

L'équation pour la détermination de la variable TO_n est la suivante :

$$TO_n = (K_1 + K_2)\varepsilon_n - K_2\varepsilon_{n-1} \quad (1)$$

Supposons que la fiabilité de la commande soit une fonction de la fiabilité des capteurs, ainsi que de celles des matériels et logiciels utilisés par les composants pour les opérations de calcul et la communication. Avec un algorithme de commande de type MLI (Modulation de largeurs d'impulsion), nous pouvons représenter le système de la manière suivante (cf. figure 7.2) :

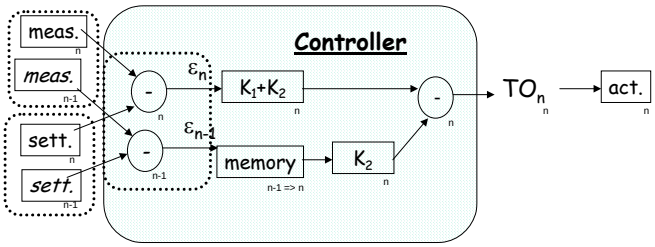


Figure 7.2 – Exemple d'architecture

La figure 7.2 est orientée fiabilité. Cette figure "plate" représente ce qui va se passer pendant les diverses valeurs du temps (périodes d'échantillonnage), pour cet exemple au niveau du $n^{ème}$ échantillon, avec le $(n - 1)^{ème}$ échantillon. Pour ne pas perdre complètement la dimension temporelle, la valeur du temps (n ou n – 1) est mentionnée en bas à droite de chaque opérateur, et un cadre pointillé les entoure pour que l'on n'oublie pas qu'il s'agit bien du même composant assurant la même opération, mais à un autre moment (par exemple $meas_n$ et $meas_{n-1}$).

Pour simplifier la démonstration, nous allons dans la suite nous intéresser à la plus simple équation de récurrence qui soit (cf. formule 2 et figure 7.3) :

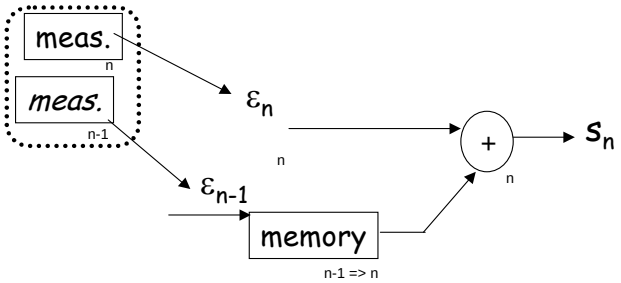


Figure 7.3 – Une architecture simple

$$s_n = \varepsilon_n + \varepsilon_{n-1} \quad (2)$$

Dans ce cas, nous considérerons que la sortie s_n est la variable critique. Nous allons évaluer la probabilité globale de défaillance.

Appelons fi l'occurrence d'une défaillance de la variable i, ce qui entraîne le fait que cette variable soit en défaut. Dans ce système, nous avons :

- fs la défaillance de s (la sortie),
- fa la défaillance de l'additionneur (A),
- fm la défaillance de la mémoire (M),
- $f\varepsilon_n$ la défaillance de ε_n,
- $f\varepsilon_{n-1}$ la défaillance de ε_{n-1},

où m représente la mémoire en charge de stocker et de conserver sans erreur la valeur de ε_{n-1} durant une période d'échantillonnage, et a représente l'unité de calcul en charge des opérations (ici simplement une addition).

Nous pouvons écrire :

$$fs = fm \cup fa \cup f\varepsilon_n \cup f\varepsilon_{n-1}. \quad (3)$$

Dans ce cas et en prenant en compte l'architecture réelle du système simplifié, nous obtenons l'expression suivante de la probabilité :

$$p(fs) = p(fm) + p(fa) + p(f\varepsilon_n \cup f\varepsilon_{n-1}). \quad (4)$$

En utilisant le théorème de l'indépendance entre les probabilités, il est possible d'écrire :

$$p(fs) = p(fm) + p(fa) + p(f\varepsilon_n) + p(f\varepsilon_{n-1}) - p(f\varepsilon_n \cap f\varepsilon_{n-1}). \qquad (5)$$

Dans l'équation (5), nous avons $p(f\varepsilon_n \cap f\varepsilon_{n-1}) = p(f\varepsilon_{n-1})$ car si une défaillance apparaît au moment du calcul de la valeur ε_{n-1}, la chaîne de calcul sera hors service au moment de calculer ε_{n-1}, et le défaut demeurera (système non réparable) pour le calcul de toutes les valeurs futures, et donc en particulier pour le calcul de ε_n. La probabilité peut finalement s'écrire :

$$p(fs) = p(fm) + p(fa) + p(f\varepsilon_n) \qquad (6)$$

Cela signifie que cet exemple est équivalent à une mise en série de la mémoire, de l'unité de calcul et du capteur. Ce modèle est en effet celui généralement utilisé dans le cas de l'évaluation de la fiabilité d'un système d'information élémentaire. C'est la conclusion que l'on peut tirer dans le cas d'une simple boucle ouverte dans laquelle les défaillances du réseau n'ont pas été considérées.

Il s'agit ici de poursuivre cette action, considérée comme une approche complémentaire de celles des approches fonctionnelles et dynamiques vues précédemment.

L'idée est donc d'effectuer une analyse de la façon dont l'information est élaborée dans ce que nous pouvons finalement considérer comme étant le système d'information. Indépendamment de la structure du système, l'idée est ici d'identifier les sources d'information (capteurs, bases de données) et de caractériser les diverses informations émises (périodicité, obsolescence ou caducité, c'est-à-dire durée de vie, précision et confiance, date…).

Ensuite il nous faut regarder à qui, quand et de quelle manière chaque information est utilisée. Nous pourrons montrer que les informations de base vont pouvoir être agglomérées pour créer des informations plus pertinentes, ou macro-informations.

Quelles règles pouvons-nous utiliser pour effectuer cette agglomération ? Il nous faut en effet faire attention, intégrer dans l'élaboration des paramètres la précision connue, l'obsolescence constatée, afin d'accorder une certaine confiance à cette information et d'avoir une estimation de la confiance, ou crédibilité, que nous pouvons accorder à l'information nouvellement créée. Dans le cas d'une information critique, nous pourrions même envisager que cette information soit transmise dans une trame intégrant des paramètres d'obsolescence (et donnant la possibilité au système de mettre à jour les caractéristiques de confiance, ou de crédibilité, accordées à la variable ou à l'échantillon considéré) permettant au système d'avoir un état "instantané" et courant de la qualité de l'information. Concernant ce dernier point de vue, nous pourrions imaginer que le système évacue de lui-même des informations non critiques devenues non crédibles…

Lorsque la vue de l'ensemble des informations sera terminée, il sera possible de mettre en évidence des modes communs, indépendamment de l'architecture, lorsqu'une information est utilisée pour élaborer plusieurs variables du système. Il sera possible de mettre ensuite en évidence des modes communs liés à l'implantation, lorsque des informations a priori indépendantes partageront des unités de calcul, de la mémoire ou des capacités réseau. Finalement le but sera de voir dans quelle mesure les méthodes classiques de sûreté de fonctionnement sont ou ne sont pas applicables pour l'évaluation des points critiques du système…

7.4.2. Sujet de thèse : Evaluation de la sûreté de fonctionnement d'une architecture distribuée par une méthode orientée information

Problématique

Ce travail tente de définir une méthodologie nouvelle, qui s'inscrit dans la problématique de l'évaluation des architectures de commande distribuée, en terme de sûreté de fonctionnement, principalement fiabilité et disponibilité.

La méthode proposée consiste, en partant de l'information circulant sur un système d'automatisation distribuée, et prenant en compte l'architecture réelle du système, à :

- Evaluer les parcours des différentes données, mesures, échantillons, …, utilisés pour élaborer les variables de commande du système. L'intérêt est de prendre en compte la manière dont ces diverses données sont élaborées, émises, transmises, "agglomérées" ou "fusionnées", en prenant en compte notamment les aspects temporels (retards de transmission, délais de calcul, stockage plus ou moins long dans des tampons ou mémoires…) et leur obsolescence courante, afin de pouvoir leur attribuer un caractère de crédibilité.

- Evaluer sur le système la criticité des variables, par une analyse de risques, afin de mettre cette criticité en relation avec la crédibilité des variables correspondantes. En remontant, à partir des variables critique, à la manière dont lesdites variables ont été élaborées, il est possible de mettre en évidence les différents composants utilisés et d'étudier leur influence vis-à-vis des variables critiques ou à évaluer les exigences de fiabilité sur les informations d'entrées issues des capteurs. Ceci doit nous permettre de mettre en évidence les points critiques de l'architecture.

Une piste intéressante pourrait consister à accompagner l'information par une procédure (orientée objet par exemple) permettant de modéliser le vieillissement. Il nous paraît intéressant de regarder d'un peu plus près les "réseaux de Petri à jetons vieillissants" (*Aging Petri Nets*) [VOV 04a] pour caractériser la crédibilité de l'information pour les systèmes distribués. Il pourrait être intéressant dans ce cadre d'associer du code au jeton du réseau de Petri.

Une autre approche vise le même but, à savoir rechercher les points faibles d'un système complexe distribué, il s'agit d'une approche ayant pour but d'identifier les points faibles du système afin de se focaliser sur ces parties pour améliorer la fiabilité globale [BEE 03], ce type de système est appelé non cohérent.

Outil, fondement

Aucun formalisme n'est imposé. Les réseaux de Petri ou les automates finis stochastiques seront évalués ainsi que d'autres outils, dans des approches aussi bien analytiques que par simulation. Afin de réduire la complexité à laquelle nous pouvons nous attendre, nous chercherons d'emblée une généricité dans les modèles ainsi qu'une construction hiérarchique.

Travail demandé

Un certain nombre de résultats ont été obtenus, concernant cette méthode [*CI03b*]. Nous avons évalué dans ces travaux préliminaires un système tout simple consistant en une équation de récurrence en boucle ouverte du premier ordre.

Pour s'approprier la méthode, le premier travail concernera l'évaluation d'un système en boucle ouverte un peu plus sophistiqué, du second ordre par exemple. Le but est de déterminer l'équation donnant les probabilités de défaillance du système global en fonction des probabilités de défaillance des différents composants qui interviennent pour l'élaboration et le transport de l'information.

Ensuite, en fonction des difficultés envisagées et de l'intérêt des personnes impliquées, plusieurs pistes pourront être tentées :

- Etude d'une boucle fermée du premier ordre,
- Démonstration de la faisabilité de la méthode par une application sur un système un peu plus complexe, intégrant l'ensemble des éléments décrits figure 7.1,
- Intégration de différents types de protocoles de communication et types d'initialisation (voir aussi le chapitre 6),
- Caractérisation de la manière de qualifier la crédibilité d'une information circulant sur un SAID.

L'objectif est d'apporter une contribution à la définition d'une boîte à outil d'aide à l'évaluation de la sûreté de fonctionnement en phase de conception des SAID.

Les travaux de recherche ou autres documents dont nous pouvons nous inspirer sont les suivants :
[61508], [BAR 03], [BEE 03], [BLA 04], [DAV 92], [DIA 01], [FRO 03], [JON 03], [PEY 94], [ŞAH 04], [SHA 98], [SIG 96]
[*CI03b*],

Pour conclure sur ces aspects liés à la crédibilité, nous rappelons qu'il faut prendre en compte pour commencer les notions d'erreurs et d'incertitudes telles qu'elles sont envisagées déjà par les gens de la mesure [CAR 02], [CHI 02], [CRI 03], [DEL 92], [FER 03], [IUC 02], [LOC 02], [MAU 02], [NUC 02], [RUS 02], [SCH 03c], [VRI 02].

7.5. Action 3 : Vers une «Sécurité Intelligente »

7.5.1. Evaluation de la sûreté de fonctionnement des boucles de sécurité constituées de Capteurs-actionneurs intelligents et de réseaux de terrain

Cette étude s'inscrit dans la poursuite de travaux antérieurs sur les instruments intelligents. Nous avons vu que les instruments intelligents sont essentiellement des capteurs et actionneurs dotés de capacités de traitement numériques et d'une interface de communication. Ils sont capables à l'aide des traitements adéquats de donner en temps réel une image de leur environnement proche, de qualifier leurs fonctionnalités (incertitude instantanée ou moyennée de mesure) et de préciser leur état de fonctionnement (possibilité de fonctionner correctement, en marche dégradée, de ne plus fonctionner…).

Dans ce cadre, il est demandé ici d'étudier le problème des capteurs et actionneurs de sécurité. Quels sont les critères à prendre en compte pour qu'un capteur puisse être "de sécurité", même chose pour un actionneur ? Comment effectuer l'implémentation ?

Par ailleurs, le réseau de terrain, qui est le moyen de communication habituel autour duquel sont disposés et connectés les capteurs et actionneurs, peut-il être sûr ? Comment le qualifier ?

Ce travail se doit d'être à la fois de recherche et de veille technologique, afin d'avoir une connaissance des produits existants et des problèmes de normalisation.

Actuellement, les réseaux disposent d'exigences spécifiques à savoir l'indépendance de la communication liée à la sécurité et de la communication standard destinée au contrôle/commande. Pour l'évaluation de la sûreté de fonctionnement, et suivant l'architecture des SAID, il est nécessaire de se conformer à la norme CEI 61508 [61508] qui traite de la sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité et constitue un véritable guide de conception de fonctions de sécurité. Le développement du profil satisfait à des exigences de sécurité sur une seule voie de communication, la redondance étant utilisée pour accroître la fiabilité. La norme CEI 61508 présente de nombreux atouts : Il s'agit de la seule norme multisectorielle traitant spécifiquement de la problématique des systèmes intégrant de l'électronique et du logiciel, elle permet de traiter tant les problèmes de pannes aléatoires que les défaillances de type systématique (non aléatoire), elle apporte des lignes directrices quant aux architectures de sécurité acceptables en fonction du besoin de sécurité, elle apporte des éléments de mesure en regard d'objectifs prédéfinis, de l'efficacité des méthodes utilisées pour spécifier ou justifier la sécurité.

Dans l'étude en cours, nous proposons une analyse pour les capteurs intelligents dédiés à la sécurité tels que les transmetteurs à sortie analogique de l'industrie du process et les détecteurs tout ou rien qui possèdent tous des liaisons avec l'unité logique. Les modes de défaillances sont décrits en terme fiabiliste uniquement. L'architecture 1oo1 (1 out of 1) montre que l'on peut considérer que le capteur se compose de deux composants, l'un ayant un taux de défaillances dangereuses λ_{DU} résultant des défaillances non détectées et l'autre un taux de défaillances dangereuses λ_{DD} résultant des défaillances détectées. Il est possible de calculer un temps d'indisponibilité équivalent t_{CE} s'appliquant au capteur en additionnant les temps d'indisponibilité individuels des deux composants t_{c1} et t_{c2} proportionnellement à la contribution respective de chaque composant au risque de défaillance du capteur.

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Pour une architecture 1oo1 par exemple, la probabilité moyenne de défaillance sur demande est :

$$PFD = (\lambda_{DU} + \lambda_{DD})\, t_{CE}$$

Ces résultats sont les premiers issus du DEA, en 2002-03, poursuivi par la thèse à partir de septembre 2003, de A. MKHIDA.

A l'issue de la première année de thèse, le candidat a pris en main les outils "réseaux de Petri", a commencé l'étude de modèles et effectué de la bibliographie sur les composants intelligents, les boucles de sécurité, l'usure…

Ce travail pourra être validé « pratiquement » sur la plate-forme « sûre » de l'ENSAM de Metz (A3SI - Automatique et Simulation pour la Sécurité des Systèmes Industriels). Des matériels relatifs à des entrées-sorties distantes via réseau, ainsi qu'une électrovanne de sécurité vont être acquises dans ce but.

Notre but est de pouvoir donner une méthode d'évaluation du niveau de SIL de la boucle de sécurité intelligente.

7.6. Action 4 : Modélisation et analyse de réseaux de terrain de sécurité et vérification des spécifications normatives

7.6.1. Description de l'action

Alors que les machines et systèmes de production profitent de la distribution des capacités de traitement pour tendre vers des architectures à base d'équipements "intelligents" (capables de s'auto- surveiller, d'optimiser leur comportement, de gérer leurs données, d'assister leur propre exploitation, maintenance, …), la sécurité reste traitée de manière centralisée.

Profitant de cette évolution des équipements, une étude pourrait être menée sur des équipements sécuritaires plus "intelligents", aptes à communiquer avec les équipements de production et, pourquoi pas, avec l'homme, de manière à optimiser leur comportement (optimisation de la sécurité, sécurité "intelligente", sécurité "agile", …), et/ou l'intégration aux équipements "intelligents" d'une fonction sécuritaire apte à appréhender son environnement et à réagir localement en fonction du rôle de l'équipement auquel elle est associée.

Le domaine des réseaux de communication est très intéressé également par ces problèmes, même si dans ce cas la notion de sûreté de fonctionnement est très fortement liée à celle de qualité de service, sans trop de relations avec la sûreté de fonctionnement du système, au sens où nous l'entendons [HAY 04] [ROC 04] [SAH 04] [XIN 04b] [ZIO 04].

Cette action a pour objectif de voir dans quelle mesure les réseaux dits de sécurité le sont effectivement, et également de voir comment un tel réseau de sécurité pourrait servir de colonne vertébrale à un système de sécurité ou un système critique…

7.6.2. Sujet de thèse

Problématique

Le sujet de thèse s'inscrit dans la problématique de l'évaluation de la sécurité des systèmes d'automatisation à intelligence distribuée, systèmes composés de capteurs, d'actionneurs et d'unités de traitement (régulateurs, superviseurs...) architecturés autour d'un medium de communication.

Il s'agit plus particulièrement dans ce travail de se focaliser sur la définition d'un modèle de représentation d'un réseau de terrain de sécurité, modèle de comportement et d'évaluation, en partant de la norme. L'objectif est de voir comment, à partir de la norme (par exemple la 50295 dans le cas de Asi-Safe), il est possible de décrire les spécifications du réseau et de pouvoir en élaborer le modèle.

Les réseaux de sécurité font partie des systèmes assurant la sécurité des installations. Actuellement plusieurs concepts sont développés et proposés sur le marché (ASiSafe, ProfiSafe, CAN-OPEN Safe, SafetyBus…). Le sujet du présent travail est de comparer la philosophie de ces différents concepts et de proposer leur classification.

Après avoir ainsi fait connaissance avec les réseaux de sécurité, le candidat est amené à développer un modèle d'un réseau selon soit une norme soit une spécification constructeur. Pendant cette modélisation un recensement des ambiguïtés présentes dans le document de référence sera effectué, en suivant la démarche proposée dans le cadre de travaux préliminaires de niveau DEA [SEB 03] [KON 04]. L'outil proposé pour la création du modèle est les Réseaux de Petri colorés, néanmoins le choix de l'outil pourra faire objet d'une discussion.

Le modèle créé va permettre son analyse formelle aussi bien qu'une analyse par simulation. L'étude formelle indique notamment la présence des états de blocage du protocole ainsi que les chemins qui mènent vers les états non désirés.

Le but global de ce travail est de tendre vers un outil de conception en vue de l'évaluation de réseaux de terrain de sécurité.

Outil, fondement

Afin de représenter les différents composants du système d'automatisation, le travail pourra s'effectuer autour des réseaux de Petri et de leurs extensions (colorés, stochastiques, continus/hybrides...) permettant ainsi une modélisation apte à la simulation et à l'analyse de performances de tous les composants d'un système d'automatisation distribué. Le réseau de terrain peut quant à lui être modélisé avec différents points de vue ou résolutions (granularité).

Application

Les applications concernent essentiellement les systèmes de sécurité et systèmes critiques (commandes de coussins gonflables automobiles, X by wire…).

Travail demandé

Le travail proposé se déroulera en deux temps.

La première partie va consister à prendre en main le sujet en s'inspirant des travaux de DEA décrits plus haut. Dans cette partie, nous proposons de faire une analyse la plus exhaustive possible des caractéristiques à prendre en compte pour que le réseau de terrain de sécurité soit un réseau de sécurité. Ces travaux pourront être menés en parallèle des travaux menés dans le groupe CIAME et l'Action Spécifique "Méthode et modèle pour l'évaluation de la sûreté de fonctionnement des systèmes distribués". Nous pouvons dire que cette activité pourrait consister à quantifier le niveau de sécurité de la fonction communication, prise indépendamment du système ou de l'application. Peut-on développer une méthode de conception/évaluation de tels réseaux de sécurité ?

La seconde partie du travail consistera à intégrer le réseau de terrain de sécurité dans une application et de proposer une méthode permettant de qualifier un niveau de sécurité variable du réseau, en fonction du type d'information véhiculée et de son niveau de criticité.

L'objectif de ces travaux est de montrer dans quelle mesure un réseau de terrain de sécurité peut être utilisé dans une application de sécurité et de voir dans quelles mesures il est possible de faire cohabiter les applications de commandes et les applications de sécurité autour d'un même réseau unique à condition de pouvoir évaluer cet ensemble. Ce type d'architecture n'est actuellement pas toléré, au plan de la normalisation.

Les travaux de recherche ou autres documents dont nous pouvons nous inspirer sont les suivants :
[50295], [61508], [AUB 99], [BAR 03], [BAY 95], [CIA 99], [DAV 92], [DIA 01], [FRO 03], [NOU 03], [POU 98], [REI 01], [ŞAH 04], [SEB 03], [SIG 96], [SIM 99], [TRI 03], [ZIO 04], [*CN03a*], [*CI03c*], [*CI03e, voir Annexe C papier 4*], [*CI04a, voir Annexe 5 papier 5*]

7.7. Conclusion

Ce chapitre a permis de montrer quelques résultats en cours sur les deux aspects de recherche que nous souhaitons développer dans l'avenir et qui concernent :

- l'étude plus fondamentale de l'évaluation de la sûreté de fonctionnement des SAID en prenant en compte le maximum de points de vue possibles et en confrontant plusieurs approches, avec pour objectif à terme de proposer une boîte à outils d'aide à la conception de SAID,
- l'évaluation plus appliquée de la sécurité de systèmes basés sur des réseaux de terrain de sécurité, en commençant par ces derniers eux-mêmes.

Le projet de recherche affiché s'oriente clairement vers l'utilisation de systèmes d'automatisation à intelligence distribuée ou de systèmes commandés en réseau comme architecture de base de systèmes de sécurité ou de systèmes à forte criticité.

Aux méthodes statiques et dynamiques déjà envisagée dans les travaux présentés dans ce document, nous proposons de développer une nouvelle approche informationnelle permettant d'aborder le SAID sous un autre angle. Il nous faut maintenant envisager la comparaison de ces méthodes, mettre en évidence leurs complémentarités et les intégrer.

Utilisant principalement les réseaux de Petri et la simulation de Monte-Carlo, nous suivons également les travaux menés par les équipes qui travaillent sur les aggrégations ou simplification de graphe ainsi que sur les méthodes d'accélération et changements d'échelle pour les simulations.

Sur un aspect plus appliqué, nous souhaitons aprofondir les études commencées en partenariat avec l'INRS, sur l'utilisation et l'évaluation des réseaux de sécurité dans les applications critiques ou de sécurité.

Concernant l'environnement local, ces travaux font partie des projets SACSS et SYDER proposés par le CRAN pour la période 2005-2008.

L'intérêt de proposer un projet de recherche finalisée est aussi d'envisager l'intégration de membres associés du laboratoire, grâce à l'ouverture que ce type de projet permet. En effet, certains membres associés ont commencé à travailler avec nous, notamment dans le cadre du groupe A (groupe de travail du contrat de plan Etat-Région). Les aspects qui sont en cours de développement par ces collègues et dans lesquels je suis également impliqué sont les suivants :

- les aspects possibilistes appliqués au SAID [*CI05b*], un premier travail concerne l'utilisation de ces techniques pour la classification automatique de scénarios pour la méthode dynamique décrite dans le chapitre 6,
- les aspects probabilistes plus classiques et les algorithmes génétiques [*RI04b, voir Annexe C papier 2*] [*CI02b*] [*CI00a*],
- l'instrumentation intelligente [*CN01a, voir Annexe C papier 3*] [1 revue en révision] et les chaînes de Markov cachées.

Ces travaux pourront bien sûr être partie prenante du Contrat de Plan Etat-Région Lorraine dans la suite du CPER existant, et la sûreté de fonctionnement des systèmes commandés en réseau est un sujet d'avenir. De plus, les méthodes peuvent être concrètement validées ou testées sur la plate-forme A3SI (Automatique et Simulation pour la Sécurité des Systèmes Industriels) de Metz.

Au niveau européen, où nous sommes peu présents en recherche, nous pourrions envisager de réfléchir au projet d'une étude, en partenariat avec des industriels, sur les méthodes mises en œuvre lorsqu'il s'agit d'évaluer des paramètres liés à la sûreté de fonctionnement pour des applications transport par exemple : ferroviaire, automobile, *X by wire* puis "*X without wire*", ou la sécurité machine. Ce type de projet pourrait s'architecturer autour d'associations (RUFEREQ).

Il semble que cette double dimension régionale et européenne pourrait effectivement être la manière, dans le futur, de gérer la recherche, d'après E. BANDA[11]…

Nous proposons un récapitulatif des communications et publications concernant
- la méthode orientée information : *CI03b.*
- les réseaux de terrain et la sécurité : *RI04a, CI04a (voir Annexe C papier 5), CI03c, CI02a.*

[11] Enric BANDA, Confier la science à l'Europe et l'innovation aux régions, La Recherche, n° 375, mai 2004, pp. 63-66.

Conclusion

Contribuer à évaluer la fiabilité et la disponibilité d'un système d'automatisation constitué de plusieurs unités de calcul et d'un réseau de communication, être capable de garantir le niveau de sécurité d'une telle installation : tels sont les objectifs que je me suis fixés globalement ces dernières années et ces objectifs seront poursuivis pour les années futures, car ce problème est un problème sociétal important et un défi scientifique d'envergure.

Ma recherche pour la décennie passée peut être scindée en trois étapes.

La première partie, importante jusque 1999, moindre ensuite, a consisté à appliquer les connaissances acquises par l'équipe dans les domaines de l'instrumentation intelligente et des SAID/Réseaux de terrain, au domaine du trafic urbain. Dans la poursuite des travaux de thèse, cette activité se présente comme de la recherche appliquée. Nous pouvons intégrer dans cette partie également une contribution, dans le cadre d'un contrat européen (4ème PCRD), à la définition et la modélisation d'un système d'informations urbaines pour divers profils d'utilisateurs et par le biais de divers types de terminaux.
Les résultats de cette première partie sont publiés dans une revue internationale (et une en révision), une revue nationale, huit conférences internationales, trois colloques nationaux, un rapport de contrat et un rapport de contrat européen.

La seconde partie concerne une contribution sur la modélisation de la structure ou de la topologie d'un système d'automatisation à intelligence distribuée, que nous avons appelée approche statique.

L'essentiel des travaux s'est déroulé dans la période 1995-2002. Le travail présenté propose une démarche pour la conception des systèmes d'automatisation. Cette démarche procède de la façon suivante :

- une modélisation de l'architecture fonctionnelle traduit les spécifications attendues et détermine une organisation de traitements élémentaires que devront réaliser les composants du système final,
- un enrichissement de cette architecture fonctionnelle par des informations relatives à la sûreté de fonctionnement décrit le comportement du système lors ou en présence de défaillances des traitements élémentaires,
- une architecture matérielle préliminaire établie par le concepteur définit un ensemble de composants susceptibles d'accueillir les traitements élémentaires identifiés précédemment,
- la projection des traitements élémentaires sur cette architecture matérielle consiste en une optimisation combinatoire où l'emploi d'algorithmes d'allocation est nécessaire. L'évaluation des solutions envisagées est réalisée par l'association de critères en une métrique unique. Ces critères rendent compte du coût des équipements utilisés, de la capacité du système à accomplir sa mission et de l'estimation du nombre d'incidents susceptibles de survenir. Le mécanisme d'allocation a ici un double objectif : outre décider du choix de la répartition des traitements, il détermine indirectement l'architecture matérielle convenant le mieux.

Les résultats de cette seconde partie sont publiés dans deux thèses de doctorat, deux revues internationales, neuf conférences internationales, quatre conférences nationales, un rapport de contrat.

La troisième partie a pour but d'intégrer les aspects dynamiques ou temporels dans l'étude, ainsi que les aspects liés aux modes de fonctionnement, en complément de l'approche précédente. Le travail a permis de vérifier la pertinence d'une approche orientée RdP pour les systèmes d'automatisation à intelligence distribuée, notamment les systèmes comprenant un réseau de communication pour en estimer les critères de la sûreté de fonctionnement.

La méthode utilisée est constituée des étapes suivantes :

- le développement des modules des composants,
- l'association des composants pour former un système complet,
- l'analyse du système par simulation de Monte Carlo de certaines propriétés et par utilisation des graphes d'occurrence pour d'autres.

La modularité de cette approche permet de créer des bibliothèques de composants et ensuite d'alléger la conception d'un système aussi bien en terme de temps d'analyse qu'en terme de coût. Elle s'inscrit alors

pleinement dans notre projet d'étude qui traite du développement d'un outil d'aide à la conception des systèmes distribués.

En l'état actuel, un recensement des problèmes a été effectué. Il a permis de mettre en évidence de nombreuses facettes du problème de synthèse et d'analyse des systèmes d'automatisation distribués. Ces problèmes vont de la conception d'un régulateur via le choix des composants et des architectures jusqu'à la certification des installations.

La méthode utilisée a permis d'évaluer des applications distribuées aussi bien au niveau des performances de commande que du point de vue de la sûreté de fonctionnement. L'usure des composants ainsi que des scénarios défaillants peuvent être estimés. Ce travail présente aussi une méthodologie détaillée de modélisation des composants des systèmes distribués et s'intéresse au problème de cohabitation de sous-ensembles à événements discrets avec des sous-ensembles échantillonnés.

Ce travail a mis en évidence les avantages et les inconvénients d'une telle méthode ainsi que certaines des limites. Parmi les avantages nous pouvons inclure l'uniformité de l'approche de modélisation tout au long de l'étude ou encore la finesse des modèles CPN. Mais la finesse a un coût qui est celui d'une lenteur de simulation. Le choix final du niveau de détail sera un compromis entre un modèle qui, exhaustif, sera nécessairement plus lent et un modèle dont les temps de simulation sont plus acceptables.
Les résultats de cette troisième partie sont publiés dans une thèse de doctorat, une revue internationale en révision, sept conférences internationales, une conférence nationale, et un partenariat avec l'INRS.

Dans la poursuite des travaux effectués ces dernières années, un certain nombre d'actions sont actuellement en cours. Ces actions se répartissent en deux grands domaines.

Tout d'abord dans le domaine de l'évaluation de la sûreté de fonctionnement des SAID, des travaux concernent une troisième approche, informationnelle, qui vient en complément des approches statiques et dynamiques envisagées précédemment.

Les autres travaux en cours concernent plus particulièrement les aspects sécurité. Une première étude tente de proposer un modèle d'évaluation d'une boucle de sécurité intégrant un réseau de sécurité. Une seconde contribution, en relation avec l'INRS, concerne l'évaluation de réseaux de terrain de sécurité, rendu nécessaire car ceux-ci sont la colonne vertébrale des SAID.

A cet égard, je participe à un groupe de travail local (groupe de travail A du CPER Lorraine : Automatique et génie informatique: de l'architecture fonctionnelle à l'architecture opérationnelle; comment garantir la SdF), à un groupe de travail national (CIAME, groupe SEE 18-04: Constituants Intelligents pour l'Automatisation et la Mesure) ainsi qu'à l'Action Spécifique CNRS "Méthode et modèle pour l'évaluation de la sûreté de fonctionnement des systèmes distribués".
Les résultats des travaux en cours sont publiés dans une participation à ouvrage, deux revues internationales, trois conférences internationales. Une thèse démarre sur ce sujet.

Un projet de recherche est proposé pour les années à venir. Dans ce projet, des actions de recherche plus fondamentale liée à l'évaluation de la sûreté de fonctionnement pourront cohabiter avec des actions plus appliquées liées à la sécurité. Concrètement à court terme, nous proposons de lancer trois actions, deux relatives à l'évaluation de la sûreté de fonctionnement et une sur la sécurité.

La première action concerne la modélisation d'un SAID et a pour objectif de mettre en place les premières briques d'une boîte à outils de conception de SAID, en effectuant la synthèse des approches statiques et dynamiques.

La deuxième action concerne l'approche informationnelle décrite précédemment. Dans ce travail, il est prévu de développer cette approche en envisageant divers cas de figures : l'évaluation de la boucle fermée, la comparaison de divers protocoles pour l'étude d'un système complexe et la prise en compte de la crédibilité des informations.

La troisième action, plus appliquée, concerne l'évaluation du niveau de SIL d'une boucle de sécurité et l'évaluation du niveau de sécurité d'un réseau de sécurité.

Les autres aspects de mon implication concernent l'enseignement, naturellement, qui, outre la participation "normale" liée à mon poste, se traduit en plus par une activité administrative (responsable de stages du département GTR, diverses commissions) ainsi que par l'encadrement durant plusieurs étés de stages

d'étudiants qui effectuent des développements informatiques (Applets Java, bases de données), principalement dans le cadre de projets européens.
La dernière contribution importante concerne les relations internationales et les technologies de l'information et de la communication pour l'Enseignement, où j'ai été un acteur important depuis 1996 dans le cadre des réseaux thématiques INEIT-MUCON et THEIERE.
Les résultats des travaux liés aux relations internationales et aux TICE sont publiés dans une participation à ouvrage, deux revues internationales, une revue nationale, vingt conférences internationales, six conférences nationales, deux rapports de contrat européens et plusieurs participations en "diffusion de la connaissance".

J'ai voulu exposer ici une thématique de recherche, avec les résultats obtenus sur la décennie passée, les activités de recherche actuelle et mon projet de recherche pour les années prochaines.

J'ai également voulu montrer ce qu'étaient les différents aspects du métier d'enseignant-chercheur avec des aspects aussi diversifiés qu'un fort investissement en recherche à certains moments, couplés à un investissement dans certains projets à d'autres moments, et à un développement d'activités d'innovations pédagogiques. Ces différentes activités se sont doublées d'implications dans divers groupes locaux, nationaux et internationaux, non seulement en recherche et liées à une thématique précise, mais aussi dans des groupes de réflexion pour l'avenir de l'enseignement, de l'université, de la recherche.

J'envisage pour le futur de conserver cette dimension pédagogique et internationale, au côté d'une activité de recherche qui a atteint une certaine maturité, tant en terme de résultats, qu'en terme d'équipe par le nombre de personnes impliquées.

Cette recherche pourra de ce fait s'approfondir, d'autant qu'elle correspond à un besoin réel des entreprises et de la société. Ce besoin n'est actuellement pas toujours explicitement formalisé, par manque d'outil législatif et d'outils d'évaluation. Nous pensons que ce besoin ira en s'amplifiant à l'avenir étant donné l'évolution de la normalisation et des besoins sociétaux, et nous souhaitons contribuer au développement de méthodes et outils d'évaluation…

Annexe A : Références bibliographiques générales

[954] Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1. Principes généraux de conception, AFNOR, 38 p., 1997.

[50170] norme européenne regroupant en fait des normes nationales DSF 21906, DIN 19245-1 à 4, NFC 46602/3/6, soit P-Net, Profibus, WorldFip, FF-H1 (Fieldbus Foundation) et ControlNet, remplacée par 61158.

[50191] Installation et exploitation des équipements électriques d'essais – Norme NF EN 50191

[50295] Norme française, Norme européenne, NF EN 50295, Appareillage à basse tension, Systèmes d'interface appareil de commande – mars 1999.

[61069] Mesure et commande dans les processus industriels - appréciation des propriétés d'un système en vue de son évaluation – Norme EN 61069.

[61158] Fieldbus Standard for use in industrial control systems – Norme internationale pour les bus de terrain (P-Net, Profibus, WorldFip, FF-HSE (Fieldbus Foundation), ControlNet, SwiftNet et Interbus-S).

[61499] Modelling control systems using IEC 61499: applying function blocks to distributed systems, par Robert Lewis, 2001.

[61508] Norme 61508, Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité, 1998.

[61511] Sécurité fonctionnelle. – Systèmes instrumentés de sécurité pour le domaine de la production par processus, 2004.

[62061] Safety of machinery: Functional Safety of Electrical, Electronic and Programmable Electronic Systems for Machinery – 2002 (FDIS CEI 62061 publiée en juin 2004, 95 pages).

[63850] Norme française homologuée NF C63-850, octobre 1982 : appareillage industriel à basse tension – automates programmables.

[ADO 01] H. ADOUD, E. RONDEAU, T. DIVOUX – Configuration of Communication Networks By Analysing Co-operation Graphs – *Computer Communications*, vol. 24, n° 15-16, octobre 2001.

[ALI 02] I. ALIEV, Z. KARA – Online reliability analysis of network information systems – *ESREL'2002-lambda-mu'2002*, Lyon, 19-21 mars 2002.

[ALM 00] L. ALMEIDA, J.A. FONSECA – FTT-CAN: a network-centric approach for can-based distributed systems – *4th IFAC International Symposium SICICA'2000*, Buenos Aires, Argentine, 13-15 septembre 2000.

[AND 01] P. ANDRE, A. VAILLY – *Conception des systèmes d'information, panorama des études et techniques* – Ellipses, Paris, 2001.

[ARL 00] J. ARLAT – *Composants logiciels et sûreté de fonctionnement intégration de COTS (components off the shelf)* – Hermes, juin 2000, ISBN, 2-7462-0146-1.

[AUB 03] J.F. AUBRY, E. GUILHEM, T. HUTINET, R. SCHOENIG – A design methodology for embeded control systems including safety assessment studies – *Congrès Européen ESREL'2003,* Maastricht, 15-18 juin 2003.

[AUB 02] J.F. AUBRY – Automated systems: from the control to the dependability. Few answers, some opened questions. – *International Conference on Quality, reliability and maintainability CCF'02,* Sinaia, Roumanie, 18-20 septembre 2002.

[AUB 99] J.F. AUBRY, F. SIMONOT-LION – Approche pluri-disciplinaire de la sûreté des systèmes – *Qualita'99, 3ème congrès international pluridisciplinaire Qualité et Sûreté de Fonctionnement*, Paris, France, 25-26 mars 1999.

[AZZ 99] A. AZZAM – *Modélisation par approche hybride d'un processus thermique pilote* – Rapport de DEA, Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy, UHP, 1999.

[BAC 96] J.P. BACONNET – Certification des bus de terrain : un bilan très contrasté – REE n° 11, décembre 1996.

[BAR 03] P. BARGER – *Evaluation et validation de la fiabilité et de la disponibilité des systèmes d'automatisation à intelligence distribuée, en phase dynamique* – thèse de l'Université Henri Poincaré Nancy 1, 15 décembre 2003.

[BAY 95] M. BAYART, F. SIMONOT – *Impact de l'émergence des réseaux de terrain et de l'instrumentation intelligente dans la conception des architectures des systèmes d'automatisation de processus* – convention MESR 92 P 0239, 1995.

[BAY 94] M. BAYART – *Instrumentation intelligents, systèmes automatisés de production à intelligence distribuée* – Habilitation à Diriger des Recherches, USTL, Lille, 21 décembre 1994.

[BEE 03] S. BEESON, J.D. ANDREWS – Importance measures for non-coherent-system analysis – *IEEE transactions on reliability*, vol. 52, n° 3, septembre 2003.

[BEL 00] R. BELHASSINE-CHERIF, A. GHEDAMSI – Diagnostic des fautes multiples pour des systèmes distribués modélisés par des machines à états finis communicantes – *CFIP'00, Colloque Francophone sur l'Ingénierie des Protocoles*, Toulouse, France, 17-20 octobre 2000.

[BER 02] H.P. BERG, R. GÖRTZ, E. SCHIMETSCHKA – A process oriented simulation model for common cause failures in systems of redundant components – *ESREL'2002-lambda-mu'2002*, Lyon, 19-21 mars 2002.

[BIE 02] D. BIED-CHARRETON – La sécurité probabiliste et ses limites – *ESREL'2002-lambda-mu'2002*, Lyon, 19-21 mars 2002.

[BLA 04] C. L. BLACKMON, M.L. YIN – A Design Tool for Large Scale Fault-Tolerant Software Systems – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[BLA 01] J.C. BLAISE, P. LHOSTE, J. CICCOTELLI – Vers un Outil d'Assistance à la prise en compte de Normes en Conception : Application à la Sécurité des Presses Mécaniques – *2ème Conférence Annuelle d'Ingénierie Système, AFIS*, Toulouse, 26-28 juin 2001.

[BLA 00] J.-C. BLAISE – *Apport d'une modélisation de l'information normative à l'intégration des règles de sécurité des machines en conception* – thèse de doctorat, Université Henri Poincaré, Nancy 1, 2000.

[BLO 96] J.M. BLOSSEVILLE – Recueil de données de trafic pour la régulation et l'information routière – *séminaire télématique des déplacements urbains*, INRETS, mars 1996.

[BOB 00] A. BOBBIO, A. PULALIAFITO, M. TEKEL – A modeling framework to implement preemption policies in non-markovian SPNs – *IEEE transactions on software engineering*, vol. 25, n° 1, janvier 2000.

[BOB 99] A. BOBBIO, G. FRANCESCHINIS, R. GAETA, L. PORTINALE – Exploiting Petri nets to support fault tree based dependability analysis – *International workshop on Petri Nets and Performance models*, 1999.

[BOB 98] A. BOBBIO, M. TELEK – Non-exponential stochastic Petri nets: an overview of methods and techniques – *Computer System Science and Engineering*, vol. 6, 1998.

[BOD 98] C. BODENNEC, C. JOURDAIN, C. MAZUET, R. GARNIER, D. PEREZ – Dependability of safety critical systems: complementary of probabistic and formal methods – *INCOM'98/IFAC, 9th symposium on information control in manufacturing*, Nancy, 24-26 juin 1998.

[BOU 03] J.L. BOULANGER – Validation des données liées à la sécurité – *Qualita'03, Congrès Qualité et Sûreté de Fonctionnement*, Nancy, France, 18-20 mars 2003.

[BUC 02] G. BUCCI, E. FIORUCCI, C. LANDI, G. OCERA – The use of wireless networks for distributed measurement applications – *IEEE Instrumentation and Measurement Technology Conference*, Anchorage, Alaska, 21-23 mai 2002.

[BUI 96] C. BUISSON, J.P. LEBACQUE, J.B. LESORT, H. MONGEOT – The STRADA dynamic assignment model – *3rd World Congress on Intelligent Transport Systems*, Orlando, USA, 1996.

[CAR 02] P. CARBONE, D. MACII, D. PETRI – Management of measurement uncertainty for effective statistical process control – *IEEE/IMTC'02, Anchorage*, Alaska, USA, 21-23 mai 2002.

[CAR 00] C. CARDEIRA – Using fieldbuses for industrial applications – *4th IFAC International Symposium SICICA'2000*, Buenos Aires, Argentine, 13-15 septembre 2000.

[CHA 03] J.M. CHARTRES – Réseaux sans fil, mais en sécurité – *J'automatise*, n° 30, septembre-octobre 2003.

[CHA 02c] P. CHARPENTIER, J.F. AUBRY – Consideration of common mode failures in the design of safety dedicated programmable controller architecture – *8th International Conference on Quality, reliability and maintainability CCF02*, Sinaia, Roumanie, 18 - 20 sept 2002.

[CHA 02b] E. CHATELET, C. BÉRENGUER, O. JELLOULI – Performance assessment of complex maintenance policies using stochastic Petri nets – *ESREL'2002-lambda-mu'2002, Lyon*, 19-21 mars 2002.

[CHA 02a] P. CHAUSSIS, P. TEXEIRA – CEI 61508 : un outil pour la construction de la sécurité des systèmes électroniques automobiles ? – *ESREL'2002-lambda-mu'2002*, Lyon, 19-21 mars 2002.

[CHA 01] M.L. CHÁVEZ – Quality of services and fieldbuses –

[CHA 00] M.L. CHÁVEZ, J.P. THOMESSE – Fieldbuses and real-time MAC protocols – *4th IFAC International Symposium SICICA'2000*, Buenos Aires, Argentine, 13-15 septembre 2000.

[CHE 94] M. CHEVALIER, Y. DUTUIT, A.M. LAPASSAT, A. LAVIRON, I. MORLAES, A. RAUZY, J.P. SIGNORET – Arbres des défaillances et diagrammes de décision binaires – *conférence de Qualité et Sûreté de fonctionnement*, Compiègne, 1994.

[CHE 90] G.H. CHEN, J-S. YUR – A branch and bound with underestimates algorithm for the task assignment problem with precedence constraint – *The 10th Int. Conf. on Distributed Computing Systems*, Paris, France, mai 1990.

[CHO 02b] M. CHOI, N. PARK, F. J. MEYER, F. LOMBARDI – Performance analysis of fault tolerant multistage interconnection networked parallel instrumentation with concurrent testing and diagnosis – *18th IEEE/IMTC Instrumentation and Measurement Technology Conference*, Anchorage, Alaska, USA, 21-23 mai 2002.

[CHO 02a] M. CHOI, N. PARK, F. J. MEYER, F. LOMBARDI, V. PIURI – Reliability Measurement of Fault-tolerant onboard memory system under fault clustering – *18th IEEE/IMTC Instrumentation and Measurement Technology Conference*, Anchorage, Alaska, USA, 21-23 mai 2002.

[CHO 98] E. CHOTIN, E. BENOIT, L. FOULLOY – An approach for cooperation in distributed architectures – *INCOM'98/IFAC, 9th symposium on information control in manufacturing*, Nancy, 24-26 juin 1998.

[CHI 02] G. CHIORBOLI – Uncertainty of mean value and variance obtained from quantized data – *IEEE/IMTC'02, Anchorage*, Alaska, USA, 21-23 mai 2002.

[CHR 01] S. CHRISTENSEN, K. JENSEN, T. MAILUND, L. M. KRISTENSEN – State-Space Methods for Timed Coloured Petri Nets –*2nd International Colloquium on Petri Net Technologies for Modeling Communication Based Systems*, Berlin, Allemagne, 14-15 septembre 2001.

[CHR 91] P. CHRISTIANSSON – Next generation knowledge-based multimedia systems – *La citta'interattiva congress*, Milano, 1991.

[CHU 99] J. CHUBB – Flying Probers Circumvent Loss of Tess Access – *Test & Measurement Europe*, vol. 7, n° 5, octobre-novembre 1999.

[CIA 99] Groupe CIAME – *Réseaux de terrain, description et critères de choix* – Hermes, Paris, 1999.

[CIA 87] CIAME – *Livre blanc : les capteurs intelligents, réflexions des utilisateurs* – CIAME-AFCET, 1987.

[CIC 99] J. CICCOTELLI, J.P. BUCHWEILER – Evaluation du niveau de sécurité des bus de communication dans les composants de sécurité – *J'Automatise*, n° 4, juin 1999.

[CIS 01] J. CISEK, W. MIKLUSZKA, Z. SWIDER, L. TRYBUS – A low-cost DCS with multifunction instruments and CAN bus – *6th IFAC symposium on Cost Oriented Automation (Low cost AUtomation)*, Berlin, Allemagne, 8-9 octobre 2001.

[COH 99] S. COHEN – *Etude prospective dans le domaine du recueil de données du trafic* – CERTU, Lyon, 1999.

[COH 90] S. COHEN – *Ingénierie du trafic routier* – Presses des Ponts et Chaussées, Paris, 1990.

[COM 94] C. COMPAROT-POUSSIER, C. CHRISTMENT – Hyperbase for electronic technical document management, Engineering of Information Systems – *Ingénierie des systèmes d'information*, vol. 2, n° 5, Hermès, 1994.

[CON 99] B. CONRARD – *Contribution à l'évaluation quantitative de la sûreté de fonctionnement des systèmes d'automatisation en phase de conception* – thèse de l'Université Henri Poincaré Nancy 1, 24 septembre 1999.

[CRA 03] J. H. CRAIG – A Software Reliability Methodology Using Software Sneak Analysis, SW FMEA and the Integrated System Analysis Approach – *RAMS'03, Annual Reliability and Maintainability Symposium*, Tampa, Floride, janvier 2003.

[CRE 81] M. CREMER, M. PAPAGEORGIOU – Parameter identification for a traffic flow model – *Automatica*, n° 17, 1981.

[CRI 03] L. CRISTALDI, A. FERRERO, C. MUSCAS, S. SALICONE, R. TINARELLI – The impact of internet transmission on the uncertainty in the electric power quality estimation by means of a distributed measurement system – *IEEE transactions on instrumentation and measurement*, vol. 52, n° 4, août 2003.

[DAI 03] Y.S. DAI, M. XIE, K.L. POH, G.Q. LIU – A study of service reliability and availability for distributed systems – *Reliability Engineering and System Safety*, n° 79, 2003.

[DAS 03] S.R. DAS, M. SUDARMA, M.H. ASSAF, E.M. PETRIU, W.B. JONE, K. CHAKRABARTY, M. ŞAHINOĞLU – Parity bit signature in response data compaction and built-in self-testing of VLSI circuits with nonexhaustive test sets – *IEEE transactions on instrumentation and measurements*, vol. 52, n° 5, octobre 2003.

[DAV 02b] B. DAVIDIAN, C. TOURNIAIRE – Une approche opérationnelle pour la conception des chaînes instrumentées de sécurité pour les installations de procédés – *ESREL'2002-lambda-mu'2002*, Lyon, 19-21 mars 2002.

[DAV 02a] B. DAVIDIAN, C. TOURNIAIRE – L'IEC 61508, un bon guide pour la sécurité – *Mesures*, juin 2002.

[DAV 92] R. DAVID, H. ALLA – *Du Grafcet aux réseaux de Petri* – Hermes, Paris, 1992, 1997.

[DEC 04] J.D. DECOTIGNIE – "Ethernet industriel ? Soyez prudents quand même" – Mesures, pp. 24-27, novembre 2004.

[DEC 02] J.D. DECOTIGNIE – Wireless fieldbuses, a survey of issues and solutions – *IFAC World Congress*, Barcelone, 2002.

[DEI 84] D. DEI-SVALDI, J.P. VAUTRIN – Les automates programmables, nouvelles technologies, nouveaux risques, principes de sécurité à appliquer – *Cahier de note documentaire*, n° 117, 4ème trimestre 1984.

[DEL 92] G. DELMAS – Les techniques d'injection de pannes dans le contexte sûreté de fonctionnement défini par la CEI – *Automation*, 1992.

[DEL 89] J.L. DELCUVELLERIE – *Ingénierie des systèmes d'automatisation de production : connaissance en conception des architectures de systèmes informatisés, d'automatisation et outil d'analyse de la robustesse aux défaillances d'architectures réparties* – Thèse de doctorat en informatique INPL, Nancy, 1989.

[DESIGN] http://www.daimi.aau.dk/designCPN

[DHA 02] M. DHAUSSY – Les méthodes de la sûreté de fonctionnement et leur utilisation – *REE*, n° 1, janvier 2002.

[DIA 01] M. DIAZ – *Les réseaux de Petri, modèles fondamentaux* – Hermes, Paris, 2001.

[DUF 02] F. DUFOUR, Y. DUTUIT – Dynamic reliability: a new model – *ESREL'2002-lambda-mu'2002*, Lyon, 19-21 mars 2002.

[DUR 79] D. DURAND – *La systémique* – Que sais-je ? Presses Universitaires de France, Paris, 1979.

[DWY 04] D. DWYER – Software Reliability Estimations/Projections, Cumulative & Instantaneous – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[FAG 00] G. FAGES – Sécurité machine – *J'automatise*, n° 10, mai-juin 2000.

[FER 03] A. FERRERO, S. SALICONE – An innovative approach to the determination of uncertainty in measurements based on fuzzy variables – *IEEE transactions on instrumentation and measurement*, vol. 52, n° 4, août 2003.

[FIP 92] AFNOR-UTE – *Bus FIP pour échange d'informations entre transmetteurs, actionneurs et automates, guide de rédaction des normes d'accompagnement* – C46-645, 7 août 1992.

[FLA 98b] J.M FLAUS, H. ALLA – Modélisation, analyse et commande de systèmes dynamiques hybrides – *Ecole d'été d'Automatique de Grenoble*, Grenoble, 7-11 septembre 1998.

[FLA 98a] J.M FLAUS – Discrete supervisor synthesis for a class of continuous system – *CDC'98, Conference on Decision and Control*, Tampa, Floride, 16-18 décembre 1998.

[FOR 96] L. FORTUNATI – *GeoData Server on WWW* – Palacio de Congresos, Barcelone, 27-29 mars 1996.

[FOU 93] J.P. FOURNIER – *Fiabilité du logiciel, concepts, modalisation, perspectives* – Hermes, collection "Traité des Nouvelles Technologies", 1993.

[FRA 00] R. FRANK – *Understanding smart sensors* – second edition, Artech House, Boston, London, 2000.

[FRI 02] H.T. FRITZSCHE – Standardising machine safety with SafetyBus p – *Control Engineering Europe*, avril/mai 2002.

[FRO 03] J.P. FROIDEVAUX, O. NICK, M. SUZAN – Use of fieldbus in safety related systems, an evaluation of WorldFIP according to proven-in use concept of IEC 61508 – *Qualita'03, Congrès Qualité et Sûreté de Fonctionnement,* Nancy, France, 18-20 mars 2003.

[GAL 98] F. GALLON – Critères de choix des réseaux de terrain – *REE* n° 3, mars 1998.

[GAU 02] B. GAUJAL, N. NAVET – Fault confinement mechanisms on CAN: analysis and improvements – *IEEE transactions on vehicular technology*, 2002.

[GEH 94] A.L. GEHIN – *Analyse fonctionnelle et modèle générique des capteurs intelligents, application à la surveillance de l'anesthésie* – Université de sciences et technologies de Lille, thèse de l'université, Lille, 1994.

[GEN 03] M.A. El-GENDY, A. BOSE, K.G. SHIN – Evolution of the internet QoS and support for soft real-time applications – *Proceedings of the IEEE*, vol. 91, n° 7, juillet 2003.

[GOK 04] S.S. GOKHALE, V.B. MENDIRATTA, K.S. TRIVEDI – Software reliability engineering techniques – tutorial, *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[GOU 04] R. GOURIVEAU, D. NOYES – Data structuring for dependability CASE tool – *Qualita'03, Congrès Qualité et Sûreté de Fonctionnement*, Nancy, France, 18-20 mars 2003.

[GRO 04] C. GROEPPELIN – Performances des switches Ethernet – *J'Automatise,* n° 33, mars-avril 2004.

[GUE 00] A. LE GUENNEC – Méthodes formelles avec UML – *CFIP'00, Colloque Francophone sur l'Ingénierie des Protocoles*, Toulouse, 17-20 octobre 2000.

[GUL 04] L. J. GULLO, R. J. DAVIS – Accelerated Stress Testing to Detect Probabilistic Software Failures – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[GUT 04] V. H. GUTHRIE, P. B. PARIKH – Software Safety Analysis: Using the Entire Risk Analysis Toolkit – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[HAE 96] M. HAEGELI, R. BOSCH and J. WEY – *Connecting WWW, GIS and RDBMS* – Palacio de Congresos, Barcelone, 27-29 mars 1996.

[HAM 03] K. HAMIDI, J-F. AUBRY, O. MALASSÉ – SILKEY: A Tool for the automatic evaluation of safety and availability of multi-level Redundancies Architecture – *21st ISSC: International System Safety Conference*, Ottawa, 4-9 août 2003.

[HAN 01] L. HAN-XIONG, G. SHOUPING – Hybrid intelligent control strategy – *IEEE Control Systems Magazine*, juin 2001.

[HAN 98] H. HANSSON, M. SJÖDIN, A. ERMEDAHL – Response time guarantees for networked control systems – *INCOM'98/IFAC, 9th symposium on information control in manufacturing*, Nancy, 24-26 juin 1998.

[HAY 04] M. HAYASHI, T. ABE – An Efficient Factoring Algorithm for Computing the Failure-Frequencies of Telecommunications Networks – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[HEC 03] R. HECKMANN, M. LANGENBACH, S. THESING, R. WILHELM – The influence of processor architecture on the design and the results of WCET (worst case execution time) tools – *Proceedings of the IEEE*, vol. 91, n° 7, juillet 2003.

[HEN 97] J.J HENRY – Les nouvelles régulation temps réel : PRODYN – *Séminaire les nouvelles techniques de la régulation de trafic*, Paris, 26 septembre 1997 (34 transparents).

[HER 97] F. HERMANN – *Contribution à la répartition des traitements et des données sur une architecture distribuée équipée d'un réseau de terrain FIP : Application à un processus thermique pilote* – Thèse de l'Université Henri Poincaré Nancy 1, 1997.

[HO 04] P. H. HO, J. TAPOLCAI, H.T. MOUFTAH – On achieving optimal survivable routing for shared protection in survivable next-generation internet – *IEEE transactions on Reliability*, vol. 53, n° 2, juin 2004.

[HO 03] S. Ho HONG, I.H. CHOI – Experimental evaluation of a bandwidth allocation scheme for foundation fieldbus – *IEEE transactions on Instrumentation and Measurement*, vol. 52, n° 6, décembre 2003.

[HOW 96] N. HOWIND et al. – *User Requirements Report for HCN and MIS* – Deliverable D01 TELEMATICS OSA-TESMA UR1020, Commission Européenne, avril 1996.

[IGL 89] *SADT: Un langage pour communiquer* – IGL Technology, Edition Eyrolles, 1989.

[IUC 02] G. IUCULANO, A. LAZZARI, G. PELLEGRINI, A. ZANOBINI – Measurement uncertainty in a multivariate model: a novel approach – *IEEE/IMTC'02, Anchorage*, Alaska, USA, 21-23 mai 2002.

[IUN 02] B. IUNG – *Contribution à l'automatisation des systèmes intelligents de production : ineropérabilité des processus de contrôle, maintenance et gestion technique* – Habilitation à diriger des recherches, CRAN, Université Henri Poincaré Nancy 1, Nancy, 17 décembre 2002.

[IUN 00] B. IUNG, D. MOREL, P. LHOSTE – Interoperable component-based emulation for distributed automated control validation – *IFAC Symposium on Manufacturing, Modeling, Management and Control, MIM'2000*, Patras, Grèce, 12-14 juillet 2000.

[JAM 02] D. JAMPI, J.-F. AUBRY – The reliability assessment of an automated system from the specification of its digital control part – *International Conference on Quality, reliability and maintainability, CCF'02,* Sinaia, Roumanie, 18-20 septembre 2002.

[JAM 01] D. JAMPI, J-F. AUBRY, E. GUILHEM – Spécification de systèmes de contrôle commande embarqués et évaluation de sûreté de fonctionnement : fusion de deux activités – *4ème congrès international pluridisciplinaire Qualité et Sûreté de Fonctionnement, Qualita'2001*, Annecy, 2001.

[JAU 02] Numéro spécial de *Terrain/J'Automatise*, n° 10 "Sécurité et bus de terrain", AS - interface SAFETY AT WORK, Safeguard, DeviceNet Safety, ProfiSafe, SafetyBus, mai-juin 2002.

[JAY 94] R. JAYAKRISHNAN, H.S. MAHMASSANI, T.Y. HU – An evaluation tool for advanced traffic information and management systems in urban networks – *Transportation Research*, n° 2C, 1994.

[JEL 02] O. JELLOULI, E. CHÂTELET, P. LALLEMENT – Application of stochastic synchronized Petri Nets in supply chain inventory management – *ESREL'2002-lambda-mu'2002*, Lyon, 19-21 mars 2002.

[JAS 01] J. JASPERNEITE, P. NEUMANN – Performance evaluation of switched ethernet in realtime applications – *4th IFAC conference "Fieldbus systems and their applications",* Nancy, France, 15-16 novembre 2001.

[JEN 98] K. JENSEN – A brief introduction to colored Petri nets – *Proc. Workshop on the Applicability of Formal Models*, Århus, Danemark, juin 1998.

[JEN 97] K. JENSEN – Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use – Monographs in *Theoretical Computer Science*, Springer-Verlag, 2nd corrected printing 1997.

[JEN 90] F. V. JENSEN, K. G. OLESEN, S. K. ANDERSEN – An Algebra of Bayesian Belief Universes for Knowledge-Based Systems – *Networks*, vol. 20, 1990.

[JOH 01] R. JOHNSONBAUGH – *Discrete Mathematics* – Prentice Hall, New Jersey, 2001.

[JON 03] W.B. JONE, D.C. HUANG, S.R. DAS – An efficient BIST method for non-traditional faults of embedded memory arrays – *IEEE transactions on instrumentation and measurements*, vol. 52, n° 5, octobre 2003.

[JUA 02] G. JUANOLE – Quality of service of communication networks and distributed automation: models and performances – *IFAC World Congress*, Barcelone, 2002.

[JUA 01] G. JUANOLE – Réseaux de communication et automatique – *Journées "Automatique et Communication"*, 13-14 mars 2001.

[JUA 99] G. JUANOLE, I.BLUM – Quality of service of real time networks and performances of distributed applications – *4th International Workshop on Electronics, Control, Measurement and Signals (ECMS'99)*, Liberec, République Tchèque, 31 mai-1er juin 1999.

[JUA 98] G. JUANOLE, I. BLUM – *Sur la complémentarité des modélisations type "informatique" et type "automatique" pour l'étude globale d'un système* – rapport interne LAAS 98200, mai 1998.

[JUM 03] F. JUMEL – *Définition et gestion d'une qualité de service pour les applications temps réel* – Thèse de l'INPL, Nancy, 27 novembre 2003.

[KAI 00] J. KAISER – Real-time communication on the CAN-bus for distributed applications with decentralized control – *4th IFAC International Symposium SICICA'2000*, Buenos Aires, Argentine, 13-15 septembre 2000.

[KHA 02] S. KHALFAOUI, E. GUILHEM, H. DEMMOU, R. VALETTE – Une méthode pour obtenir des scénarios critiques dans les systèmes mécatroniques – *ESREL'2002-lambda-mu'2002*, Lyon, 19-21 mars 2002.

[KHO 90] L. KHOUDOUR, J.B. LESORT, J.L. FARGES – PRODYN : trois ans d'expérimentation sur la ZELT, *Recherche Transports Sécurité* "Spécial Gestion du Trafic" – n° 28, décembre 1990.

[KIR 83] S. KIRKPATRICK, C. D. GELATT, M.P. VECCHI – Optimization by simulated annealing – *Science*, vol. 220, n° 4598, 1983.

[KON 04] A. KONATE – *Evaluation des propriétés de sécurité du protocole de réseau de sécurité "ProfiSafe"* – Rapport de DEA, Ecole Nationale Supérieure d'Electricité et de Mécanique, INPL de Lorraine, Nancy, 2004.

[KOP 02] H. KOPETZ – Time-triggered real-time computing – *15th IFAC World Congress*, Barcelone, 2002.

[KRO 03] A. KROLO and B. BERTSCHE – An Approach for the Advanced Planning of a Reliability Demonstration Test Based on a Bayes Procedure – *RAMS'03, Annual Reliability and Maintainability Symposium*, Tampa, Floride, janvier 2003.

[KRO 02] N. KROMMENACKER, J.P. GEORGES, E. RONDEAU, T. DIVOUX – Designing, modelling and evaluating switched ethernet networks in factory communication systems – *RTLIA'2002, 14th IEEE Euromicro Conference on Real Time Systems*, 1st Workshop on Real Time LAN's in the Internet Age, Vienne, Autriche, 18 juin 2002.

[LAB 02] P.E LABEAU., E. ZIO – Procedures of Monte Carlo transport simulation for applications in system engineering – *Reliability Engineering and System Safety*, 2002.

[LAL 03] P.K. LALA, A.L. BURRESS – Self-checking logic design for FPGA implementation – *IEEE transactions on instrumentation and measurements*, vol. 52, n° 5, octobre 2003.

[LAV 04] J.Z. LAVI, D. DALCHER, M. MANNION, R. GALLON – Engineering of Computer-Based systems : A proposed curriculum for a degree program at bachelor level – *IEEE transactions on Education*, vol. 47, n° 2, mai 2004

[LEP 91] F. LEPAGE, F. AFILAL, P. ANTOINE, E. BAJIC, J.Y. BRON, T. DIVOUX – *Les réseaux locaux industriels* – Edition Hermes, 1991.

[LIA 01] F.L. LIAN, J.R. MOYNE, D.M. TILBURY – Performance evaluation of control networks: Ethernet, ControlNet, DeviceNet – *IEEE control Magazine*, février 2001.

[LIG 02] J. LIGUŠOVÁ – Modeling of Network Control Systems Based on Coloured Petri Nets – *Internal scientific conference of TU Košice*, mai 2002.

[LIS 98] V. LIST, A. CHOVIN, P. COAT, G. RENARD, P. SOETERS – Safety integration in distributed automation systems fieldbus-dependability – *INCOM'98*, Nancy, 1998.

[LAN 02] S. LANKES, A. JABS, M. REKE – A time-triggered Ethernet protocom for Real-Time CORBA – *5th IEEE International Symposium on Object-Oriented Real-Time Distributed Computing (ISORC 2002)*, Washington DC, USA, avril 2002.

[LAP 95] J.C. LAPRIE & al. – *Guide de la sûreté de fonctionnement* – Cépaduès, 1995.

[LAU 97] B. LAURENS, P.Y. TEXIER P.Y. – Doit-on rougir de nos feux ? – *Transports Environnement Circulation*, 1997.

[LEF 99] D. LEFEBVRE – Failure detection and isolation for manufacturing systems – *Int. J. of Mech. Prod. Syst. Eng.*, n° 2, 1999.

[LEL 04] D. LELIEVRE – Fiabiliser, ça peut rapporter gros ! (3) – *Mesures*, n° 764, avril 2004.

[LEU 88] W. LEUTZBACH – *Introduction to the theory of traffic flow* – Springer-Verlag, 1988.

[LOC 02] N. LOCCI, C. MUSCAS, L. PERETTO, R. SASDELLI – A numerical approach to the evaluation of uncertainty in nonconventional measurements on power systems – *IEEE transactions on instrumentation and measurement*, vol. 51, n° 4, août 2002.

[MAC 98] P. MACIEL, E. BARROS, W. ROSENSTIEL – A based on Petri net approach for quantifying mutual exclusion degree – *INCOM'98/IFAC, 9th symposium on information control in manufacturing*, Nancy, 24-26 juin 1998.

[MAR 04] M. MARSEGUERRA, E. ZIO – Monte-Carlo sampling and simulation – tutorial, *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[MAR 94] Y. MARTIN, G. HERBIN, J. FAUCHON, D. PLAY – Allocation de fiabilité : démarche "expérimentale" par algorithme génétique – *Conférence de Qualité et Sûreté de fonctionnement*, Compiègne, 1994.

[MAU 02] G. MAURIS, L. FOULLOY – 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.

[McD 95] A. MCDERMID, M. NICHOLSON, D.J. PUMFREY, P. FENELON – Experience with the application of HAZOP to computer-based systems – *10th Annual IEEE Conference on COMPuter ASSurance (COMPASS '95),* 1995.

[MEL 94] N. MELAB – *Synthèse des méthodes de distribution statique et dynamique de la charge sur architectures MIMD* – Publication AS-94-160, © LIFL USTL, octobre 1994.

[MEU 00] P. MEUNIER, B. DENIS and J.J. LESAGE – Safety Analysis During the Control Architecture Design of Automated Systems – *Safeprocess 2000 (IFAC)*, Budapest, Hongrie, 14-16 juin 2000.

[MES 03] N. MESSAI – Surveillance de trafic urbain et interurbain à base de modèles neuronaux – Thèse de l'Université de Technologie de Belfort-Montbéliard et de l'Université de Franche-Comté, Belfort, 17 décembre 2003.

[MEU 98] F. MEUNIER, H. DESILLE, M. O'CONNOR, A. RAUZY, P. THOMAS – Sherloc : Outil d'allocation d'indisponibilité pour les arbres de défaillance – *Textes des conférences de $\lambda\mu$11*, Arcachon, 1998.

[MEY 02] K. MEYER-GRÄFE – Solutions for safety technology using Interbus Safety – *Control Engineering Europe*, juin-juillet 2002.

[MIC 98] F. MICHAU – *Contribution de Nouvelles Technologies Educatives à la Formation en Automatique* – Habilitation à Diriger des Recherches, I.N.P.G., Grenoble, 15 avril 1998.

[MKH 03] A. MKHIDA – *Capteurs intelligents pour des applications de sécurité* – Mémoire de DEA, CRAN, Nancy, 2003.

[MON 98] G. MONCELET – *Application des réseaux de Petri à l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile* – Thèse de l'Université Paul Sabatier, Toulouse, France, 1998.

[MOR 02] J.Y. MOREL, M. BARREAU, A. TODOSKOFF – Petri nets: a tool adapted to computer system dependability and safety – *ESREL'2002-lambda-mu'2002*, Lyon, 19-21 mars 2002.

[MOR 01] G. MOREL, J.F. PETIN, P. LAMBOLEY – Formal specification for manufacturing systems automation – *IFAC - INCOM'01 Conference on Information Control problems in Manufacturing*, Vienne, Autriche, 20-22 septembre 2001.

[MOS 99] M. MOSTEFAOUI, I. DEMONGODIN, N. SAUER – Vivacité des graphes d'événements continus valués – *JDA'99, Journées doctorales d'automatique*, Nancy, 21-23 septembre 1999.

[MUL 03] A. MULLER, M.C. SUHNER, P. WEBER, G. PERROUD – Modélisation par réseaux bayésiens du processus de fiabilisation de produits, application à l'automobile – *Qualita'03, Congrès Qualité et Sûreté de Fonctionnement*, Nancy, France, 18-20 mars 2003.

[MUN 91] T. MUNTEAN, E.G. TALBI – Méthodes de placement statique des processus sur architectures parallèles – *T.S.I*, vol. 10, n° 5, 1991.

[NAV 00] N. NAVET, Y-Q. SONG, F. SIMONOT – Worst-Case Deadline Failure Probability in Real-Time Applications Distributed over CAN (Controller Area Network) – *Journal of Systems Architecture*, Elsevier Science, vol. 46, n° 7, 2000.

[NEV 98] F. NEVES Junior, J.A. MARTIN – Reachability in hybrid systems by control inclusion – *INCOM'98/IFAC, 9th symposium on information control in manufacturing*, Nancy, 24-26 juin 1998.

[NIL 03] J. NILSSON, B. BERNHARDSSON, B. WITTENMARK – Stochastic analysis and control of real-time systems with random time delays – *Automatica,* vol. 34, n° 1, 2003.

[NOU 03] M. NOURELFATH, D. AIT-KADI, I. SORO – Performance evaluation of reconfigurable manufacturing systems – *Qualita'03, Congrès Qualité et Sûreté de Fonctionnement*, Nancy, France, 18-20 mars 2003.

[NUC 02] S. NUCCIO, C. SPATARO – Can the effective number of bits be useful to assess the measurement uncertainty? – *IEEE/IMTC'02, Anchorage*, Alaska, USA, 21-23 mai 2002.

[NUN 02] E. NUNES, J. FARIA, M. MATOS – A comparative analysis of dependability assessment methodologies for markovian and non markovian systems – *ESREL'2002-lambda-mu'2002*, Lyon, 19-21 mars 2002.

[OTA 02] P. G. OTANEZ, J. R. MOYNE, D. M. TILBURY – Using Deadbands to Reduce Communication in Network Control Systems –*2002 American Control Conference,* 2002.

[PAR 01] I. PARISSIS, J. VASSY – Test de propriétés de sûreté – *MSR'01, Modélisation des systèmes réactifs*, Toulouse 17-19 octobre 2001.

[PER 90] J. PEREZ – *Systèmes Temps Réel* – Edition Dunod, 1990.

[PEY 04] J.F. PEYRUCAT – Les systèmes de sécurité face au choix des normes – *Mesures*, n° 764, avril 2004.

[PEY 00] J.F. PEYRUCAT – La norme IEC 61158 est sortie mais on n'est guère plus avancé – *Mesures*, n° 722, février 2000.

[PEY 94] J.F. PEYRUCAT – Sûreté de fonctionnement, une confiance difficile à mesurer – *Forum*, 1994.

[POL 98] S. POLEDNA – The time-triggered communication Protocol TTP/C – *Real-Time magazine*, 1998-4.

[POU 04] G. POULARD, B. DENIS, J.-M. FAURE – Modélisation par réseau de Petri coloré des architectures de commande distribuées sur réseau de terrain Ethernet et TCP/IP – *5ème Conférence francophone de MOdélisation et SIMulation, MOSIM04*, Nantes (France), pp. 405-412, septembre 2004.

[POU 98] J. POUEYO, J.P. DALZON – Mastering safety of open & distributed systems in compliance with IEC 61508 – *INCOM'98/IFAC, 9th symposium on information control in manufacturing*, Nancy, 24-26 juin 1998.

[RAG 94] D. RAGGETT – A review of the HTML+ document format – *First International World-Wide-Web Conference*, mai 1994.

[RAO 03] J.P. RAOULT, L. SMAIL – Algorithmes des restrictions successives – *Qualita'03, Congrès Qualité et Sûreté de Fonctionnement*, Nancy, France, 18-20 mars 2003.

[RAS 97] R. RASCALON – Des langues et des langages pour spécifier, modéliser et enseigner en ingénierie des systèmes complexes – *REE*, n° 3, mars 1997.

[REI 01] D. REINERT, M. SCHAEFER – Sichere Bussysteme für die Automation – Hüthig Verlag Heidelberg, 2001.

[RIE 99] P. RIEDINGER, F. KRATZ, C. ZANNE – Commande optimale des systèmes dynamiques hybrides : synthèse d'une loi de commande – *AIAI'99, 3ème conférence internationale sur l'automatisation industrielle*, Montréal, Canada, 7-9 juin 1999.

[ROB 93] M. ROBERT, M. MARCHANDIAUX, M. PORTE – *Capteurs Intelligents et Méthodologie d'Evaluation* – Hermès, 1993.

[ROB 92] M. ROBERT – *Contribution à l'évolution de l'instrumentation industrielle : capteurs intelligents et détections de défauts* – Habilitation à Diriger des Recherches, UHP, Nancy, 29 septembre 1992.

[ROC 04] C. M. ROCCO S. – Approximate Reliability Expressions Using a Decision Tree Approach – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[ROC 02] C.M. ROCCO S., J.A. MORENO – System reliability evaluation using Monte Carlo simulation and cellular automata – *ESREL'2002-lambda-mu'2002*, Lyon, 19-21 mars 2002.

[ROD 02] M. RODRIQUEZ, J.C. FABRE, J. ARLAT – Assessment of real-time systems by fault injection – *ESREL'2002-lambda-mu'2002*, Lyon, 19-21 mars 2002.

[ROT 96] S. ROTH – *Compte-rendu sur les Serveur Web-GIS et Municipaux* – compte-rendu scientifique, CRAN-UHP, Nancy, 1996.

[ROT 91] S. ROTH – *Analyse de trafic* – Rapport de DEA, Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy, UHP, 1991.

[RUS 02] H. RUSER, V. MAGORI, H.R. TRÄNKLER – Correlated microwave-ultrasonic multi-sensor for reliable measurements of velocity and range – *IEEE/IMTC'02, Anchorage*, Alaska, USA, 21-23 mai 2002.

[ŞAH 04] M. ŞAHINOĞLU, C. V. RAMAMOORTHY, A. E. SMITH, B. DENGIZ – A Reliability Block Diagramming Tool to Describe Networks – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[SCH 03c] C. SCHERRER, A. STEININGER – Dealing with dormant faults in an embedded fault-tolerant computer system – *IEEE transactions on reliability,* vol. 52, n° 4, décembre 2003.

[SCH 03b] R. SCHOËNIG, J.F. AUBRY, E. GUILHEM, T. HUTINET – An example of reliability assessment by an aggregation method of Markov graphs for hybrid systems*, Qualita'03, Qualité et Sûreté de Fonctionnement*, Nancy, France, 18-20 mars 2003.

[SCH 03a] R. SCHOËNIG, J.F. AUBRY, E. GUILHEM, T. HUTINET – An aggregation method of Markov graphs for the reliability analysis of hybrid systems, *Qualita'03, Qualité et Sûreté de Fonctionnement*, Nancy, France, 18-20 mars 2003.

[SCH 99] M. SCHAEFER – New concepts for safety-related bus systems – *Safe PLC systems*, Cologne, Allemagne, 1999.

[SEB 03] Q. SEBASTIEN – *Evaluation du niveau de sécurité d'une architecture distribuée à l'aide d'une modélisation par réseaux de Petri* – Rapport de stage ingénieur, Ecole Nationale Supérieure d'Electricité et de Mécanique, INPL de Lorraine, Nancy, 2003.

[SHA 98] I. SHAGAEV, S. PLIASKOTA – The concept of dynamic safety – *9th symposium on information control in manufacturing*, *IFAC/INCOM'98*, Nancy, 24-26 juin 1998.

[SIF 98] J. SIFAKIS – Hybrid systems – *Ecole d'été d'Automatique de Grenoble*, Grenoble, 7-11 septembre 1998.

[SIG 02] J.P. SIGNORET, J.L. CHABOT, T. HUTINET – Comment cacher un réseau de Petri derrière un bloc diagramme de fiabilité ? – *ESREL'2002-lambda-mu'2002*, Lyon, 19-21 mars 2002.

[SIG 96] J.P. SIGNORET – Modélisation et simulation dans le domaine de la sûreté de fonctionnement – *REE*, n° 8, septembre 1996.

[SIM 99] F. SIMONOT – *Une contribution à la modélisation et à la validation d'architectures temps réel* – Habilitation à Diriger des Recherches, INPL, Nancy, 10 août 1999.

[SIM 92] F. SIMONOT, C. VERLINDE – Importance d'un cadre de référence dans la mise en place d'une démarche de développement d'un système automatisé de production – *Conférence Canadienne sur l'automatisation industrielle AIAI'92*, Montréal, juin 1992.

[SON 03] H.S. SON, P.H. SEONG – Development of a safety critical software requirements verification method with combined CPN and PVS: a nuclear power plant protection system application – *RESS*, 80, 2003.

[SON 99] Y. Q. SONG, F. SIMONOT-LION, N. NAVET – De l'évaluation de performances du système de communication à la validation de l'architecture opérationnelle – *Ecole d'été temps réel*, Poitiers, septembre 1999.

[STA 94] M. STAROSWIECKI, M. BAYART – *Actionneurs Intelligents* – Hermès Paris, Collection Automatique, 1994.

[SWA 04] S. S. GOKHALE – Cost Constrained Reliability Maximization of Software Systems – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[TAN 04] Z. TAN, J. BECHTA DUGAN – Minimal cut set/sequence generation for dynamic fault trees – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[THO 02] J.P. THOMESSE – Open issues in fieldbus based systems – *IFAC World Congress*, Barcelone, 2002.

[THO 00] J.P. THOMESSE – The research and a possible future for fieldbuses – *4th IFAC International Symposium SICICA'2000*, Buenos Aires, Argentine, 13-15 septembre 2000.

[THO 94] J.P. THOMESSE – Conformité, interopérabilité, interfonctionnement, interchangeabilité – *CiMax, édition Terrain*, n° 2, janvier-février 1994.

[TIA 01] G.Y. TIAN – Design and implementation of distributed measurement systems using fieldbus-based intelligent sensors – *IEEE transactions on instrumentation and measurement*, vol. 50, n° 5, octobre 2001.

[TOM 03] C.J. TOMLIN, I. MITCHELL, A.M. BAYEN, M. OISHI – Computational techniques for the verification of hybrid systems – *Proceedings of the IEEE*, vol. 91, n° 7, juillet 2003.

[TOU 01] J.P. TOURRES – *L'entreprise intégrée intelligente* – TOP Editions, Paris, 2001.

[TOV 00] E. TOVAR, F. VASQUES, L.M. PINHO – Engineering real-time applications with WorldFIP: analysis and tools – *4th IFAC International Symposium SICICA'2000*, Buenos Aires, Argentine, 13-15 septembre 2000.

[TRI 03] K.S. TRIVEDI, S. RAMANI, R. FRICKS – Recent advances in modeling response-time distributions in real-time systems – *Proceedings of the IEEE*, vol. 91, n° 7, juillet 2003.

[TRY 98] L. TRYBUS, W. MIKLUSZKA – Introduction to CAN communication – *Integrated control systems and intelligent control, Summer School 98,* Tempus joint European project S-JEP-11317-96, Cracovie, PL, 7-10 juillet 1998.

[ULL 98] J. D. ULLMAN – *Elements of ML programming* – ML97 edition, Prentice Hall, New Jersey, 1998.

[UPA 97] S. J. UPADHYAYA – *VLSI Testing* – Tutoriel, Department of Electrical and Computer Engineering, Université de New York, 1997.

[VAU 96] J.P. VAUTRIN, P. CHARPENTIER, C. VIGNERON – La sécurité en machinerie, introduction au concept de catégorie – *Cahiers de notes documentaires*, n° 163, 2ème trimestre 1996.

[VIL 88] A. VILLEMEUR – *Sûreté de fonctionnement des systèmes industriels* – Editions Eyrolles, Paris, 1988.

[VOL 04b] V. VOLOVOI – Modeling of system reliability with stochastic Petri nets – tutorial, *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[VOL 04a] V. VOLOVOI – Modeling multiphased missions using stochastic Petri nets with aging tokens – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[VRI 02] B. VRIELYNCK, H. CLOSON – Les process mieux maîtrisés grâce à la réconciliation des données – *Mesures,* janvier 2002.

[WAH 03] M. WAHL – *Les réseaux de terrain embarqués dans les transports guidés* – Les collections de l'INRETS, synthèse n° 45, juillet 2003.

[WAL 03] C. WALTER – Les technologies internet dans les systèmes de contrôle-commande – *J'automatise*, n° 28, mai-juin 2003.

[WAL 01] G.C. WALSH, H. YE – Scheduling of networked control systems – *IEEE control Magazine*, février 2001.

[WAL 99] G. C. WALSH, H. YE, L. BUSHNEL – Stability analysis of networked control systems –*American Control Conference*, San Diego (CA), juin 1999.

[WAN 04b] W. WANG, M. JIANG – Generalized Decomposition Method for Complex Systems – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[WAN 04a] W. WANG, J. LOMAN, P. VASSILIOU – Reliability importance of components in a complex system – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[WEB 03] P. WEBER, L. JOUFFE – Reliability modelling with dynamic bayesian networks – *IFAC/SafeProcess'2003*, Washington, juin 2003.

[WEB 02] P. WEBER, M.C. SUHNER – An application of bayesian networks to the performance analysis of processes – *ESREL'2002-lambda-mu'2002*, Lyon, 19-21 mars 2002.

[WID 90] B. WIDROW, M.A. LEHR – 30 years of adaptative neural networks: Perceptron, Madaline, and backpropagation - *IEEE Proceedings*, vol. 78, n° 9, 1990.

[WIE 96] J. WIESEL, W. HAGG, A. KOSCHEL, R. KRAMER and R. NIKOLAI – A Client/Server Map Visualization Component for an Environmental Information System based on WWW – Vienne, Autriche, *ISPRS'1996*.

[WIL 00] R. WILD, C.E. PEREIRA – Validating temporal behavior of communication in foundation fieldbus – *4th IFAC International Symposium SICICA'2000*, Buenos Aires, Argentine, 13-15 septembre 2000.

[WOR 03] *WorldFIP Fieldbus* – Iss.31, mars 2003.

[WOR 02] *WorldFIP Fieldbus* – Iss.30, juillet 2002.

[XIN 04b] L. XING – Fault-tolerant network reliability and importance analysis using binary decision diagrams – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[XIN 04a] L. XING, J.B. DUGAN – A separable ternary decision diagram based analysis of generalized phase-mission reliability – *IEEE transactions on Reliability*, vol. 53, juin 2004.

[XU 04] H. XU, J. BECHTA DUGAN – Combining dynamic fault trees and event trees for probabilistic risk assessment – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[YAL 03] A. YALAOUI, E. CHÂTELET, C. CHU – Overview of reliability optimization and models for a new reliability and redundancy allocation problem in a parallel-series system – *Qualita'03, Qualité et Sûreté de Fonctionnement*, Nancy, France, 18-20 mars 2003.

[YIN 04] M.-L. YIN, J. PETERSON, R. R. ARELLANO – Software Complexity Factor in Software Reliability Assessment – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

[YU 03] Y. YU and B.W. JOHNSON – A BBN Approach to Certifying the Reliability of COTS Software Systems Approach – *RAMS'03, Annual Reliability and Maintainability Symposium*, Tampa, Floride, janvier 2003.

[ZAN 99] X. ZANG, H. SUN, K.S. TRIVEDI – A BDD-based algorithm for reliability analysis of phased-mission systems – *IEEE transactions on Reliability*, vol. 48, mars 1999.

[ZAY 02] J. ZAYTOON – Systèmes *dynamiques hybrides* – traité ic2 série systèmes automatisés, Hermes, 2002.

[ZHA 01] W. ZHANG, M.S. BRANICKY, S.M. PHILIPS – Stability of networked control systems – *IEEE control Magazine*, février 2001.

[ZIO 04] E. ZIO, L. PODOFILLINI – A Monte Carlo Approach to the Estimation of Importance Measures of Multi-State Components – *RAMS'04, Annual Reliability and Maintainability Symposium*, Los Angeles, janvier 2004.

Annexe B : Mes références bibliographiques

Les références bibliographiques sont classées de manière assez classique.

Les communications à caractère pédagogique sont séparées des communications liées à la recherche.

Toutes les références ont une classification de type *M* pour la recherche Méthodologique, *T* pour la recherche Technologique et *P* pour la recherche Pédagogique.

Note sur la politique de publication : concernant les noms d'auteur, les communications liées aux travaux des doctorants ont toujours le doctorant comme premier auteur, sachant qu'il est généralement le rédacteur principal.

Pour les conférences, le nom souligné est le nom de la personne qui a fait la présentation. Les communications en italique ont fait l'objet d'une reprise étendue en ouvrage ou revue. Pour information, nous avons fait mention des revues liées à la recherche actuellement en révision en note de bas de page.

DEA, THESE, HABILITATION

[*HA04*] Habilitation à Diriger des Recherches de l'Université Henri Poincaré Nancy 1 en Automatique : "*Sûreté de fonctionnement de systèmes d'automatisation à intelligence distribuée*" – CRAN, UHP, Nancy, 2004.

[*TH93*] Thèse de l'Université Henri Poincaré Nancy 1 en Automatique : "*Contribution à la détection et à l'analyse d'anomalies de trafic en milieu urbain – Regards sur l'existant en régulation du trafic urbain*" – CRAN, UHP, Nancy, 1993.

[*DE89a*] Rapport pratique de DEA : *Création d'un logiciel en Prolog pour la formation à la sécurité des personnels concepteurs de circuits de commande électromécaniques à relais et diagnostic de ces circuits par les méthodes de l'intelligence artificielle* (avec l'I.N.R.S., Institut National de la Recherche et de la Sécurité) – ESSTIN-CRAN-INRS, Nancy, 1989.

[*DE89b*] Rapport bibliographique de DEA : *les logiciels d'enseignement "intelligemment" assistés par ordinateur* – ESSTIN-CRAN, Nancy, 1989.

PARTICIPATION A OUVRAGES

Participation à ouvrages liés à la recherche

[*OU04*] Groupe de travail CIAME (…, Jean-Marc THIRIET, …) – *Réseaux de terrain, critères de sûreté de fonctionnement* – Hermès (à paraître, automne 2004). *M*

[*OU99*] Blaise CONRARD, Jean-Marc THIRIET, Michel ROBERT – A tool for the evaluation of fieldbuses reliability for intelligence distributed automation system design – in S.G. TZAFESTAS, *Advanced in manufacturing, decision, control and information technology*, Springer, 1999, ISBN 1-85233-126-7, pp. 157-167. *M*

Participation à ouvrage lié aux relations internationales et à l'innovation pédagogique

[*OU03*] Under the co-ordination of Jean-Marc THIRIET & Maria João MARTINS – *Monograph: Towards the harmonisation of Electrical and Information Engineering Education in Europe* – Ed. EAEEIE, août 2003, 380 pages, (ISBN, book version: ISBN 972-97738-2-3, ISBN: CD-ROM version: ISBN 972-97738-3-1).

REVUES INTERNATIONALES AVEC COMITE DE LECTURE

Revues internationales acceptées ou publiées, liées à la recherche[12]

[*RI04c*] Blaise CONRARD, Jean-Marc THIRIET, Michel ROBERT – Distributed system dependability evaluation: a case study on a pilot thermal process – *Reliability Engineering and System Safety*, acceptée pour publication, en 2004 ('article in press'). *M*

[12] Revues internationales avec comité de lecture, en révision (à titre d'information)

[REV2] Jean-Marc THIRIET, Jean-Michel RIVIERE, Michel ROBERT – Improvement of an inductive loop-based measurement system for the determination of urban traffic parameters – soumise à *IEEE transactions on Instrumentation and Measurement*, juillet 2001, en révision, novembre 2002, resoumission janvier 2004. T

[REV1] Pavol BARGER, Jean-Marc THIRIET, Michel ROBERT – Dependability Analysis of a Distributed Control or Measurement Architecture – soumis à *IEEE transactions on Instrumentation and Measurement*, juillet 2003, en révision, juillet 2004. M

[*RI04b*] Frédérique BICKING, Blaise CONRARD, Jean-Marc THIRIET – Integration of dependability in a task allocation problem – *IEEE transactions on Instrumentation and Measurement*, Vol. 53, n°6, December 2003, pp. 1455 - 1463. *M*

[*RI04a*] Laurent CAUFFRIEZ, Joseph CICCOTELLI, Blaise CONRARD, Mireille BAYART, Eric BENOIT, Guy BENOIT, André CHOVIN, Eric FAE, Michel ROBERT, Jean-Marc THIRIET, Martine WAHL (Groupe CIAME) – Design of intelligent distributed control systems: a dependability point of view – *Reliability Engineering & System Safety*, vol. 4, n 1, 2004, pp. 19-32. *M*

[*RI96*] Jean Michel RIVIERE, Mireille BAYART, Jean-Marc THIRIET, Adam BOURAS, Michel ROBERT – Intelligent instruments: some modelling approaches – *Measurement and Control*, juillet-août 1996, vol. 29, pp. 179-186. *M*

Revues internationales liées à l'innovation pédagogique

[*RI02*] Jean-Marc THIRIET, Michel ROBERT, Pentti LAPPALAINEN, Michael HOFFMANN, Maria João MARTINS, Anselmo SEOANE – Toward a pan-European virtual university in Electrical and Information Engineering – *IEEE transactions on Education*, mai 2002, vol. 45, n° 2, pp. 152-160. *P*

[*RI01*] Maria João MARTINS, Michel ROBERT, Jean-Marc THIRIET – An Internet project to achieve curricula harmonisation – *Acta Scientiarum*, vol. 22, nº 5, décembre 2001, pp. 1327-1331. *P*

REVUES NATIONALES AVEC COMITE DE LECTURE

Revue nationale liée à la recherche

[*RN91*] Jean-Marc THIRIET, Michel ROBERT, Claude HUMBERT, Jean-Jacques DAVAINE – Cinq générations de stratégies de régulation du trafic urbain de par le monde – *TEC, Transport Environnement Circulation,* n° 109, novembre-décembre 1991, pp 32-36. *M*

Revue nationale liée à l'innovation pédagogique

[*RN98*] Michel ROBERT, Jean-Marc THIRIET – Le réseau thématique SOCRATES INEIT-MUCON : des modules d'enseignement en EEA via Internet – *Revue pédagogique CETSIS EEA numéro 001 (version prototype de JEEEA),* papier numéro 5, 1998 (support électronique). *P*

CONFERENCES INTERNATIONALES AVEC ACTES ET COMITE DE LECTURE

Conférences internationales avec actes et comité de lecture liées à la recherche

[*CI05b*] Christophe SIMON, Jean-Marc THIRIET, Jean-François AUBRY – Credibility of reliability evaluation of Networked Control System – accepté pour la conférence *ESREL'2005 (European safety and reliability conference*, Gdansk-Gdynia (Pologne), 27-30 June 2005.

[*CI05a*] Abdelhak MKHIDA, Pavol BARGER, Jean-Marc THIRIET, Jean-François AUBRY – Influence of the control strategy choice on the safety level of a distributed automation system – accepté pour la conférence *ESREL'2005 (European safety and reliability conference*, Gdansk-Gdynia (Pologne), 27-30 June 2005.

[*CI04b*] Pavol BARGER, Jean-Marc THIRIET, Michel ROBERT, Jean-François AUBRY – 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. *M*

[*CI04a*] Jana LIGUŠOVA, Jean-Marc THIRIET, Jan LIGUŠ, Pavol BARGER – Effect of Element's Initialization in Synchronous Network Control System to Control Quality – *RAMS/IEEE conference 2004 (Annual Reliability and Maintainability Symposium)*, Los Angeles, janvier 2004, 6 pages (format électronique, ISBN: 0-7803-8216-1). *M*

[*CI03e*] Pavol BARGER, Jean-Marc THIRIET, Michel ROBERT – Safety analysis and reliability estimation of a networked control system – *IFAC/SafeProcess'2003*, Washington, juin 2003, pp. 1047-1052. *M*

[*CI03d*] Jean-Marc THIRIET, Pavol BARGER, Michel ROBERT – Dynamic evaluation of dependability for distributed intelligence automation systems – *4ème conférence de l'AIAI*, Montréal (Québec, Canada), 9-11 juin 2003, 4 pages (CD-ROM). *M*

[*CI03c*] Laurent CAUFFRIEZ, Blaise CONRARD, Jean-Marc THIRIET, Mireille BAYART – Fieldbuses and their Influence on Dependability – *20th IEEE Instrumentation and Measurement Technology Conference (IEEE/IMTC'2003)*, Vail (Colorado, Etats-Unis), 20-22 mai 2003, pp. 83-88. *M*

[*CI03b*] Fabrice JUMEL, Jean-Marc THIRIET, Jean-François AUBRY, Olaf MALASSÉ – Towards an information-based approach for the dependability evaluation of distributed control systems – *20th IEEE Instrumentation and Measurement Technology Conference (IEEE/IMTC'2003)*, Vail (Colorado, Etats-Unis), 20-22 mai 2003, pp. 270-275. *M*

[*CI03a*] Pavol BARGER, Jean-Marc THIRIET, Michel ROBERT – Dependability Analysis of a Distributed Control or Measurement Architecture – *20th IEEE Instrumentation and Measurement Technology Conference (IEEE/IMTC'2003)*, Vail (Colorado, Etats-Unis), 20-22 mai 2003, pp. 473-477. *M*

[*CI02d*] Pavol BARGER, Jean-Marc THIRIET – Evaluation of networked control systems thanks to a dynamical reliability approach – *8th International Conference Quality, Reliability, Maintenability, CCF'2002*, Sinaia, Roumanie, 18-20 septembre 2002, pp. 190-196, *M*.

[*CI02c*] Pavol BARGER, Jean-Marc THIRIET, Michel ROBERT – Dynamical reliability and availability evaluation and validation of distributed control systems – *19th IEEE Instrumentation and Measurement Technology Conference (IEEE/IMTC'2002)*, Anchorage (Alaska, Etats-Unis), 21-23 mai 2002, pp. 837-842. *M*

[*CI02b*] Frédérique BICKING, Blaise CONRARD, Jean-Marc THIRIET – Integration of dependability in a task allocation problem – *19th IEEE Instrumentation and Measurement Technology Conference (IEEE/IMTC'2002)*, Anchorage (Alaska, Etats-Unis), 21-23 mai 2002, pp. 1461-1466. *M*

[*CI02a*] Pavol BARGER, Jean-Marc THIRIET, Michel ROBERT – Performance and dependability evaluation of distributed dynamical systems – *European Conference on System Dependability and Safety (ESRA'2002/lambda-Mu13)*, Lyon (France), 19-21 mars 2002, pp. 16-22. *M*

[*CI01*] Philippe JEANJEAN, Jean-Luc NOIZETTE, Jean-Marc THIRIET – Test strategies of an intelligent instrument – *6th IFAC symposium on Cost Oriented Automation (Low cost Automation, COA'2001)*, Berlin (Allemagne), 8-9th octobre 2001, pp. 58-63. *M*

[*CI00b*] Dimitri LEFEBVRE, Philippe THOMAS, Jean-Marc THIRIET, Nadhir MESSAI, Abdellah EL MOUDNI – Model-based traffic monitoring by means of neural networks – *39th IEEE Conference on Decision and Control (CDC'00)*, Sydney (Australie), 12-15 décembre 2000, pp. 3541-3546. *M*

[*CI00a*] Blaise CONRARD, Jean-Marc THIRIET, Frédérique BICKING – Dependability as a criterion for distributed systems design – *4th IFAC International Symposium on Intelligent Components and Instruments for Control Applications (SICICA'00)*, Buenos Aires , Argentine, 13-15 septembre 2000, pp. 45-50. *M*

[*CI99*] Blaise CONRARD, Frédéric HERMANN, Jean-Marc THIRIET, Michel ROBERT – Vers une boîte à outils pour la conception de systèmes intégrés distribués – *3ème Conférence de l'Association Internationale de l'Automatisation Industrielle (AIAI'99)*, Montréal (Canada), juin 1999, pp. 20.9 - 20.12. *M*

[CI98e] Blaise CONRARD, Jean-Marc THIRIET, Michel ROBERT – A tool for the evaluation of fieldbuses reliability for intelligence distributed automation system design – EURISCON'98, juin 1998, Athènes. M [voir OU99]

[*CI98d*] Frédéric HERMANN, Nicolas DELAHAYE, Jean-Marc THIRIET, Michel ROBERT – Problems of genericity for the architectures and protocols used for UTCSs – *31st ISATA Conference*, Düsseldorf, juin 1998, pp. 21-28. *T*

[*CI98c*] Frédéric HERMANN, Frédérique BICKING, Jean-Marc THIRIET, Michel ROBERT – Development of a genetic method for optimal allocation of tasks in a Distributed Intelligence Base Automation System (DIBAS) context: Application to a pilot thermal process using field-bus – *ETIMVIS'98/IEEE International Workshop on Emerging Technologies*, St-Paul, Minnesota, mai 1998, pp. 114-123. M

[*CI98b*] Blaise CONRARD, Jean-Marc THIRIET, Michel ROBERT – Problems of precision for control loops implanted on Distributed Automation System – *CESA'98 (Computational Engineering in Systems Applications)/IMACS/IEEE*, Hammamet/Nabeul (Tunisie), avril 1998, pp. 180-185, vol. 1. *M*

[*CI98a*] Frédéric HERMANN, Jean-Marc THIRIET, Michel ROBERT – A tasks allocation strategy for the design of distributed architecture in automation systems: application to a pilot thermal process using field-bus – *CESA'98 (Computational Engineering in Systems Applications)/IMACS/IEEE*, Hammamet/Nabeul (Tunisie), avril 1998, pp. 70-74, vol. 1. *M* (présentée par B. CONRARD).

[*CI97c*] Frédéric HERMANN, Jean-Marc THIRIET, Michel ROBERT – Task allocation for the design of distributed architecture in automation systems: application to a pilot thermal process using a fieldbus network – 3rd IFAC/SICICA Conference, Annecy (France), juin 1997, pp. 459-464. *M*

[*CI97b*] Michel ROBERT, Jean-Marc THIRIET – Instrumentation intelligente, état de l'art et perspectives – *2nd Symposium International sur "les capteurs et leurs applications industrielles"*, Gabès (Tunisie), mai 1997, pp. 41-50, sur invitation. *M*

[*CI97a*] Sandrine ROTH, Marie-Laure BESSON, Eric GNAEDINGER, Jean-Marc THIRIET, Thierry DIVOUX – Proposition of a model for the M.I.S. (multimedia information system) database connected to a G.I.S. – *JEC Conference 97*, Vienne, avril 1997, pp. 1079-1088. *M*

[*CI96d*] Jean-Marc THIRIET, Frédéric HERMANN, Michel ROBERT – Development in simulation of an architecture for an Integrated Traffic Control and Management System (I.T.C.M.S.) – *CESA'96 (Computational Engineering in Systems Applications)/IMACS/IEEE*, Lille, juillet 1996, pp. 867-872. *M*

[*CI96c*] Sandrine ROTH, Jean-Marc THIRIET, Eric GNAEDINGER, Michel ROBERT, Thierry DIVOUX – Proposition for a multimedia information system (M.I.S.) to display information about public transport and traffic states – *29th ISATA Conference*, Florence, Italie, juin 1996, pp. 157-163. *T*

[*CI96b*] Jean-Marc THIRIET, Frédéric HERMANN, Blaise CONRARD, Michel ROBERT – Towards an architecture for a distributed traffic control and guidance system (I.T.C.M.S.) in an urban context – *29th ISATA Conference,* Florence, Italie, juin 1996, pp. 393-400. *M*

[*CI96a*] Sandrine ROTH, Eric GNAEDINGER, Jean-Marc THIRIET, Thierry DIVOUX & Karl Heinz KAPP – Proposition of a multimedia information system (M.I.S.) about the urban services for the citizens – *JEC'Conference 96*, Barcelone, mars 1996, Espagne, pp. 1036-1045. *T*

[*CI95d*] Jean-Marc THIRIET, Jean-Luc NOIZETTE, Michel ROBERT, Jean Michel RIVIERE – A smart or intelligent sensor for road and urban traffic – *28th ISATA Conference*, Stuttgart, septembre 1995, pp. 383-392. *T*

[*CI95c*] Eric GNAEDINGER, Jean-Marc THIRIET, Sandrine ROTH, Michel ROBERT – Integrated communication architecture to inform citizens about urban services with telematic application: proposition for an urban information system – *Neties Conference 95*, Athènes, Grèce, 1995. *T*

[*CI95b*] Frédéric HERMANN, Jean-Marc THIRIET, Michel ROBERT – Architecture distribuée et réseaux de terrain, répartition des traitements et des données : application à un processus thermique – *2ème Conférence AIAI*, Nancy, juin 1995, pp. 225-230. *M*

[*CI95a*] Jean-Marc THIRIET, Eric GNAEDINGER, Michel ROBERT, Frédéric HERMANN – Automatic Production Systems and Integrated Traffic Control and Management Systems – *28th ISATA Conference*, Stuttgart, septembre 1995, pp. 247-256. *M*

[*CI93b*] Jean-Marc THIRIET, Michel ROBERT, Eric GNAEDINGER, Claude HUMBERT – Towards an algorithm for automatic supervision of traffic sensors – *26th ISATA International Symposium Automotive Technology and Automation*, Aix-la-Chapelle, Allemagne, 13-17 septembre 1993, pp. 663-669. *M*

[*CI93a*] Jean-Marc THIRIET, Michel ROBERT, Claude HUMBERT, Jean-Jacques DAVAINE – Comparison of functions between a policeman controlling traffic flows at a crossroad and a UTCS, using the SADT method – *26th ISATA International Symposium Automotive Technology and Automation*, Aix-la-Chapelle, Allemagne, 13-17 septembre 1993, pp. 323-329. *M*

[*CI92b*] Jean-Marc THIRIET, Michel ROBERT, Jean-Pierre JOUANNET, Claude HUMBERT, Jean-Jacques DAVAINE – Parameters for modelisation and fault detection at a crossroad – *25th ISATA Silver Jubilee International Symposium Automotive Technology and Automation*, Florence, Italie, 1-5 juin 1992, pp. 229-236. *M*

[*CI92a*] Eric GNAEDINGER, Jean-Marc THIRIET, Michel ROBERT, Gérard BLOCH – Traitement de l'information, réseau industriel et génie urbain – *Conférence sur l'Automatisation Industrielle (AIAI'92)*, Montréal, 1-3 juin 1992, pp. 4-9, 4-12. *M* (présentée par C. HUMBERT).

Conférences internationales avec actes et comité de lecture liées à l'innovation pédagogique et aux relations internationales

[*CP04b*] Jean-Marc THIRIET, Maria João MARTINS, Pascal GEND, Michel ROBERT – THEIERE project: a study about curricula available in Europe in Electrical and Information Engineering and reflections on the BMD process – *ITHET'2004*, juin 2004, Istanbul (Turquie), ISBN 0-7803-8597-7, paper 307 (electronic support). *P*

[*CP04a*] Jean-Marc THIRIET, Maria João MARTINS, Pascal GEND, Michel ROBERT – A monograph and a portal: curricula available in Europe in Electrical and Information Engineering and reflections on the BMD process, *EAEEIE'2004*, 27-29 mai 2004, Sofia (Bulgarie), pp. 133-136. *P*

[*CP03b*] Maria João MARTINS, Michel ROBERT, J.M. THIRIET – A thematic network contribution to education and training in electrical and information engineering in Europe – *4th International Conference on Information Technology Based Higher Education and Training ITHET'2003*, 7-9 juillet 2003 Marrakech, Maroc (electronic support). *P*

[*CP03a*] Jean-Marc THIRIET, Pascal GEND, Michel ROBERT, Maria João MARTINS, Carolina LLANES – A tool to help students and colleagues understanding European Higher education systems and diploma in EIE – *14th annual EAEEIE Conference*, Gdansk, Pologne, 16-18 juin 2003, 5 pages (electronic format), ISBN. *P*

[*CP02e*] Maria João MARTINS, Michel ROBERT, Jean-Marc THIRIET – New technologies and harmonisation of curricula: a thematic network approach – *Vienna International Working Conference (Viewdet 2002)*, Vienne (Autriche), 4-6 décembre 2002, pp. 179-183, invitation. *P*

[*CP02d*] Jean-Marc THIRIET, Michel ROBERT, Pascal GEND – Development of pedagogical resources for teaching signal processing and sensors: some issues – *Vienna International Working Conference (Viewdet 2002)*, Vienne (Autriche), 4-6 décembre 2002, pp. 193-200, invitation. *P*

[*CP02c*] Jean-Marc THIRIET, Michel ROBERT, Maria João MARTINS, Michael HOFFMANN – Pedagogical resources reachable via internet for teaching intelligent instruments: developments within a European Thematic Network – *19th IEEE Instrumentation and Measurement Technology Conference (IEEE/IMTC'2002)*, Anchorage (Alaska, Etats-Unis), 21-23 mai 2002, pp. 1475-1480 [poster]. *P*

[*CP02b*] Pascal GEND, Jean-Marc THIRIET – THEIERE pedagogical resources, pertinence and limits of statistics on a web site – *13th annual EAEEIE Conference*, York, Royaume-Uni, 8-10 avril 2002, 6 pages (electronic format), ISBN 1-85911-009-6. *P*

[*CP02a*] Jean-Marc THIRIET, Georges ZISSIS, Michel ROBERT, Maria João MARTINS, Hamed YAHOUI – Some considerations on the actual implementation of the 358 scheme in Europe – *13th annual EAEEIE Conference*, York, Royaume-Uni, 8-10 avril 2002, 5 pages (electronic format), ISBN 1-85911-009-6. *P*

[*CP01*] Maria João MARTINS, Michel ROBERT, Jean-Marc THIRIET – THEIERE: A thematic Network focused on harmonisation of curricula – *12th annual EAEEIE Conference*, Nancy, France, 14-16 mai 2001, pp. 1-5. *P*

[*CP00e*] Jean-Marc THIRIET, Michel ROBERT, Blaise CONRARD – Curricula reachable via Internet for teaching intelligent instruments – *4th IFAC International Symposium on Intelligent Components and Instruments for Control Applications (SICICA'00)*, Buenos Aires , Argentine, 13-15 septembre 2000, pp. 189-194. *P*

[*CP00d*] Maria João MARTINS, Michel ROBERT, Jean-Marc THIRIET – Linking teachers and students via WWW – *GIREP'2000*, Barcelone, Espagne, 27 août-1er septembre 2000, résumé/abstract 1 page. *P*

[*CP00c*] Michel ROBERT, Jean-Marc THIRIET, Pascal GEND – INEIT-MUCON: A SOCRATES European thematic network in electrical and Information Engineering – *International Conference on Information Technology Based Higher Education and Training (ITHET'00)*, Istanbul, 3-5 juillet 2000, Turquie, pp. 7-12. *P*

[*CP00b*] Pascal GEND, Jean-Marc THIRIET, Michel ROBERT – An internet site allowing to federate a set of persons and projects in a multidisciplinary and multilingual context – *11th annual EAEEIE Conference*, Ulm, Allemagne, avril 2000, pp. 94-98. *P*

[*CP00a*] Jean-Marc THIRIET, Michel ROBERT – Curricula reachable via internet for teaching intelligent instruments and signal processing: validation and dissemination – *11th annual EAEEIE Conference*, Ulm, Allemagne, avril 2000, pp. 250-254. *P*

[*CP99*] Jean-Marc THIRIET, Michael HOFFMANN, Hugues GARNIER, M. PRUTSCHER – Evaluation of internet-based tools to help students in understanding concepts of digital signal processing – *10th annual EAEEIE Conference*, Capri, Italie, mai 1999, pp. 28-31. *P*

[*CP98b*] Michel ROBERT, Jean-Marc THIRIET – The SOCRATES INEIT-MUCON Thematic Network: curricula in EIE via Internet – *9th symposium on information control in manufacturing, IFAC/INCOM*, 24-26 juin 1998, Nancy, pp. 223-228. *P*

[*CP98a*] Jean-Marc THIRIET, Michel ROBERT – Development of virtual educational tools for teaching and through teaching – *9th annual EAEEIE Conference*, Lisbonne, Portugal, mai 1998, pp. 161-166. *P*

[*CP97*] Jean-Marc THIRIET, Hugues GARNIER – Design of digital filters and test on a DSP: an example of teaching using new tools – *8th annual EAEEIE Conference*, Edimbourg, juin 1997, pp. E1.14-E1.20. *P*

[*CP95*] Jean Michel RIVIERE, Michel ROBERT, Jean-Marc THIRIET, Jean-Luc NOIZETTE – How technology transfer can be a motor for more conceptual research – *6th annual EAEEIE Conference*, Bologne, mai-juin 1995. *P*

CONFERENCES NATIONALES AVEC ACTES ET COMITE DE LECTURE

Conférences nationales liées à la recherche

[*CN03a*] Pavol BARGER, Jean-Marc THIRIET, Michel ROBERT – Modeling and analyzing safety criteria of a real communication protocol – *5ème congrès international pluridisciplinaire "Qualité et süreté de fonctionnement" QUALITA'2003*, Nancy, France, 18-20 mars 2003, pp. 36-43. *M*

[*CN01b*] Blaise CONRARD, Jean-Marc THIRIET, Michel ROBERT – Conception d'architecture de systèmes d'automatisation par allocation des traitements sous des contraintes de sûreté de fonctionnement – *Congrès QUALITA'2001 "Qualité et sûreté de fonctionnement"*, Annecy, 22-23 mars 2001, pp. 442-447. *M*

[*CN01a*] Jean-Marc THIRIET, Jean Michel RIVIERE, Michel ROBERT – Amélioration de l'information perçue par les systèmes de régulation de trafic urbain – *Colloque C2I'2001 "Colloque interdisciplinaire en instrumentation"*, CNAM, Paris, 31 janvier - 1er février 2001, in "*Instrumentation pour les mesures physiques – C2I 2001, volume 1*", sous la direction de F. Lepoutre, D. Placko, Y. Surrel, Hermes, 2001, pp. 461-469. *M*

[*CN99d*] Blaise CONRARD, Michel ROBERT, Jean-Marc THIRIET – Prise en compte de la sûreté de fonctionnement dans la conception des systèmes d'automatisation à intelligence distribuée – *3ème congrès international pluridisciplinaire "Qualité et sûreté de fonctionnement", QUALITA'99*, Paris, 25-26 mars 1999, pp. 231-241. *M*

[*CN99c*] Frédérique BICKING, Blaise CONRARD, Jean-Marc THIRIET – Affectation des traitements par approche génétique pour la conception de systèmes distribués intégrant la sûreté de fonctionnement – *IAR ICD'99 Workshop "Techniques intelligentes pour le traitement de l'information et applications"*, Nancy, 10 décembre 99, pp. 41-48. *M*

[*CN99a*] Blaise CONRARD, Jean-Marc THIRIET, Michel ROBERT – Répartition des traitements dans la conception de systèmes d'automatisation architecturés autour de réseaux de terrain – *Colloque européen "Réseaux de capteurs et communications /INNOCAP 99"*, Grenoble, 28/29 avril 99, pp. 43-49. *M*

[*CN97*] Marie-Laure BESSON, Thierry DIVOUX, Jean-Marc THIRIET & Karl Heinz KAPP – OSA - TESMA: Open System Architecture for TElematic Systems in Municipal Applications – *IAR Kolloquium*, Duisburg (Allemagne), novembre 1997, 5 pages. *T*

[*CN95*] Jean-Luc NOIZETTE, Abdallah KHOURY, Jean-Marc THIRIET, Michel ROBERT – Un transmetteur intelligent de température au service de l'environnement – *Conférence SEE : "Des capteurs pour l'environnement"*, Grenoble, mars 1995, pp. 35-40. *M*

Conférences nationales liées à l'innovation pédagogique

[*CN03b*] Jean-Marc THIRIET, Maria João MARTINS, Michel ROBERT, Hamed YAHOUI, Olivier BONNAUD, Pascal GEND, Carolina LLANES – THEIERE : un réseau thématique, force de proposition pour l'Université de demain – *Colloque sur l'Enseignement des Technologies et des Sciences de l'Information et des Systèmes en Electronique, Electrotechnique et Automatique /CETSIS'03*, Toulouse, 13-14 novembre 2003. *P* (poster)

[*CN01c*] Jean-Marc THIRIET, Maria João MARTINS, Michel ROBERT – Le réseau thématique THEIERE : nouvelles technologies et harmonisation des cursus pour l'université de demain – *Colloque sur l'Enseignement des Technologies et des Sciences de l'Information et des Systèmes en Electronique, Electrotechnique et Automatique /CETSIS'01*, Clermont-Ferrand, 29-30 octobre 01, pp. 349-352. *P* (poster)

[*CN00*] Michel ROBERT, Jean-Marc THIRIET, Pascal GEND – Vers un cursus européen en ingénierie électrique et de l'information, le réseau thématique SOCRATES INEIT-MUCON – *Colloque international TICE'2000*, Troyes, 18-20 octobre 2000, résumé/abstract p. 285 (papier complet sur le CD-ROM). *P*

[*CN99b*] Jean-Marc THIRIET, Michael HOFFMANN – Développement et évaluations d'outils pédagogiques en EEA, dans un contexte européen – *Colloque sur l'Enseignement des Technologies et des Sciences de l'Information et des Systèmes en Electronique, Electrotechnique et Automatique /CETSIS'99*, Montpellier, 4/5 novembre 99, pp. 57-60. *P* (poster)

[*CN98*] Jean-Marc THIRIET, Michel ROBERT – Utilisation du web comme outil de formation, dans un contexte européen – *Forum NTICF'98*, Rouen, novembre 1998, 8 pages. *P*

[*CN97*] Jean-Marc THIRIET, Michel ROBERT – Le réseau thématique SOCRATES INEIT-MUCON : des modules d'enseignement en EEA via Internet – *CETSIS-EEA*, Orsay (France), novembre 1997, pp. 307-310. *P* (poster)

COLLOQUES NATIONAUX AVEC ACTES, SANS COMITE DE LECTURE

[*CS95*] Yves ROBIN-PREVALLEE, Jean-Marc THIRIET, Michel ROBERT – La mesure de trafic, vers un capteur intelligent – *Colloque Club EEA / CNRS / ATT "20 ans du SPI / L'automatique et les transports"*, Nancy, octobre 1995. *T*

[*CS90*] Michel ROBERT, Jean-Marc THIRIET, J.P. JOUANNET, J.J. DAVAINE – Positionnement automatique de caméras en environnement urbain pour la visualisation et l'analyse des anomalies de trafic – *"Rencontre Nationale de Génie Urbain "*, Lyon, mars 1990. *T*

RAPPORTS DE CONTRATS INDUSTRIELS ET EUROPEENS

Rapports de contrats industriels et européens liés à la recherche

[*Rc98b*] Jean-Marc THIRIET, Frédéric HERMANN, Nicolas DELAHAYE, – *Etude des caractéristiques des systèmes de régulation du trafic urbain : Architecture et protocoles de transmissions, performances et possibilités d'évolution* – CERTU/CRAN/Université Henri Poincaré Nancy 1, 1998, Confidentiel. Contrat n° UNI 97-071, 1er octobre-31 décembre 1997, septembre 1998, 65 pages.

[*Rc98a*] Marie-Laure BESSON, Thierry DIVOUX, Jean-Marc THIRIET, Eric GNAEDINGER, Sandrine ROTH – *Presentation pre-standard proposition for MIS (Multimedia Information System)* – Deliverable n° 6 European Commission TELEMATICS project UR 1020, OSA-TESMA Open System Architecture for Telematic Services in Municipal Applications, février 1998, 45 pages.

[*Rc94*] Abid FILALI, Jean-Marc THIRIET, Michel ROBERT – *Le recueil de données dans le domaine du trafic routier et urbain : les besoins, l'existant, les perspectives* – CERTU/CRAN/Université Henri Poincaré Nancy 1, 1994, Confidentiel. Contrat n° UNI 93-102, 1er octobre-31 décembre 1993, juin 1994, 40 pages.

[*Rc92b*] Jean-Marc THIRIET, Michel ROBERT – *Etude bibliographique : les systèmes de régulation du trafic urbain Version 2* – Rapport CRAN ESSTIN Ville de Nancy, Institut Lorrain du Génie Urbain, Nancy, septembre 1992 (première version en septembre 1990 – les deux versions sont diffusées par l'Institut Lorrain du Génie Urbain).

[*Rc92a*] Jean-Marc THIRIET – Rapports de contrats durant la thèse, CRAN/Ville de Nancy, Nancy, 1991-92 :
Etat d'avancement des travaux en octobre 1992 - 37 pages.
Etat d'avancement des travaux en février 1992 - 16 pages.
Etat d'avancement des travaux en octobre 1991 - 20 pages.

Rapports de contrats européens liés à l'innovation pédagogique

[*Rc00b*] Mícheál Ó'hÉIGEARTAIGH, Michel ROBERT, Jean-Marc THIRIET, Pascal GEND, Bernard GOLDBACH – *Final report on the Thematic Network Programme Networking project* – European Commission DG Education & Culture, février 2000, 35 pages.

[*Rc00a*] Michel ROBERT, Jean-Marc THIRIET – SOCRATES Programme: Final Report form, thematic network projects "*INnovations for Education in Information Technology through MUltimedia and COmmunication Networks (Dissemination)*" – EU reference: 26173-CP-1-99-1-FR-ERASMUS-ETN, novembre 2000, 100 pages + annexes.

DIFFUSION DES CONNAISSANCES

Diffusion des connaissances liées à la recherche

[*DC98*] Jean-Marc THIRIET – *Intelligent instruments and distributed control, in Integrated control systems and intelligent control* – Summer School 98, Tempus joint European project S-JEP-11317-96, Cracovie (Pologne), 7-10 juillet 1998, pp. 9-64.

Diffusion des connaissances liées aux relations internationales et à l'innovation pédagogique

[*DC04c*] Hélène FREMONT, Jean-Marc THIRIET, Hamed YAHOUI – Table ronde, animée par H. FREMONT et J. M THIRIET, "La diversité du statut des enseignants chercheurs en Europe (Allemagne D. WEICHERT, Angleterre M. JONES, Italie Fausto FANTINI, Espagne Anselmo SEOANE)", *Congrès du Club EEA*, Rouen, 3 juin 2004. *P*

[*DC04b*] Hélène FRÉMONT, Jean-Marc THIRIET, Hamed YAHOUI – Comparative presentation of the status of teacher-researcher in different countries of Europe – *EAEEIE'2004*, 27-29 mai 2004, Sofia (Bulgarie), pp. 123-128. P

[*DC04a*] Hamed YAHOUI, Hélène FREMONT, Jean-Marc THIRIET, Maria João MARTINS, Olivier BONNAUD – From the two-tier degree structure of the Bologna process to the Erasmus Mundus European master – *EAEEIE'2004*, 27-29 mai 2004, Sofia (Bulgarie), pp. 110-113. *P*

[*DC03*] Jean-Marc THIRIET, Hamed YAHOUI – THEIERE : activités du réseau européen, réflexions pour l'Université de demain – présentation effectuée pendant le "*43ème congrès annuel du Club EEA*", Besançon (France), 14-16 mai 2003. *P*

[*DC02*] Jean-Marc THIRIET, Hamed YAHOUI & al. – European Curricula in Electrical and Information Engineering – présentation effectuée pendant le "*42ème congrès annuel du Club EEA*", Perpignan (France), 29-31 mai 2002.

[*DC01c*] Publication dans "*La Informilo*" n° 116 de décembre 2001 "INEIT-MUCON, benvenon en la retejon de INEIT-MUCON, novigaĵoj por instruado en la informteknologioj per informilaro kaj komunikretoj", p. 37, trad. J.L. Thibias & J.M. Thiriet.

[*DC01b*] Bernard de FORNEL, Jean-Marc THIRIET, Olivier BONNAUD – The French Club EEA Commission for International relationships – *12th annual EAEEIE Conference*, Nancy, France, 14-16 mai 2001, pp. 7-10. *P*

[*DC01a*] Jean-Marc THIRIET, Georges ZISSIS – Towards a Unique European Higher Education Scheme: Dream or Reality? – Communication présentée pendant le jour commun entre la *12th annual EAEEIE Conference*, Nancy, France, 14-16 mai 2001, et le *41ème congrès du Club EEA*, Nancy, France, 16-18 mai 2001. *P*

[*DC00*] Michel ROBERT, Jean-Marc THIRIET – Réseau international : outils pédagogiques en EEA dans un réseau européen – *Rencontres 2000 des Ecoles Universitaires d'Ingénieurs "Stratégies de Réseaux"*, Saint-Etienne, 10-11 mai 2000, pp. 8-12. *P*

[*DC99*] Michel ROBERT, Jean-Marc THIRIET – Développement et évaluation d'outils pédagogiques en EEA dans un contexte européen – *8èmes journées d'enseignement des télécommunications "Les systèmes mobiles de 3ème génération"*, Nice, 24-25 novembre 1999, pp. 169-174. *P*

Annexe C : Publications ou communications significatives

1. [RI04c] Blaise CONRARD, Jean-Marc THIRIET, Michel ROBERT, *Distributed system dependability evaluation: a case study on a pilot thermal process*, "Reliability Engineering and System Safety", acceptée pour publication (*'article in press'*), en 2004.

2. [RI04b] Frédérique BICKING, Blaise CONRARD, Jean-Marc THIRIET, *Integration of dependability in a task allocation problem*, "IEEE transactions on Instrumentation and Measurement", Vol. 53, n°6, décembre 2004, pp. 1455 - 1463.

3. [CN01a] Jean-Marc THIRIET, Jean Michel RIVIERE, Michel ROBERT, *Amélioration de l'information perçue par les systèmes de régulation de trafic urbain*, Colloque C2I 2001 "Colloque interdisciplinaire en instrumentation", CNAM, Paris, 31 janvier – 1er février 2001, in "Instrumentation pour les mesures physiques – C2I 2001, volume 1", sous la direction de F. Lepoutre, D. Placko, Y. Surrel, Hermes, 2001, pp. 461 - 469.

4. [CI03e] Pavol BARGER, Jean-Marc THIRIET, Michel ROBERT, *Safety analysis and reliability estimation of a networked control system*, "IFAC/SafeProcess'2003", Washington, juin 2003, pp. 1047 - 1052.

5. [CI04a] Jana LIGUŠOVA, Jean-Marc THIRIET, Jan LIGUŠ, Pavol BARGER, *Effect of Element's Initialization in Synchronous Network Control System to Control Quality*, "RAMS/IEEE conference 2004 (Annual Reliability and Maintainability Symposium)", Los Angeles, janvier 2004, 6 pages (format électronique, ISBN: 0-7803-8216-1).

UNE PUBLICATION SIGNIFICATIVE EN INNOVATION PEDAGOGIQUE

6. [RI02] Jean-Marc THIRIET, Michel ROBERT, Pentti LAPPALAINEN, Michael HOFFMANN, Maria João MARTINS, Anselmo SEOANE, *Toward a pan-European virtual university in Electrical and Information Engineering*, "IEEE trans. on Education", mai 2002, vol. 45, n°2, pp. 152 - 160.