Approche pluridisciplinaire de la sûreté des systèmes

Jean-François Aubry, Françoise Simonot-Lion

APPROCHE PLURIDISCIPLINAIRE DE LA SURETE DES SYSTEMES

AUBRY J.-F. * - SIMONOT-LION F.**
* CRAN – CNRS ESA 7039 - INPL tel : 03 83 59 55 78
** LORIA - CNRS UMR 7503 - INPL - tel : 03 83 59 55 79
ENSEM - 2, avenue de la Forêt de Haye - 54516 Vandoeuvre-lès-Nancy - France
aubry@ensem.u-nancy.fr - simonot@loria.fr
fax : 03 83 44 07 63

Résumé : *Nous présentons un sous-ensemble des travaux développés dans le cadre d'un Programme Fédérateur de Recherches sur la sûreté des systèmes industriels. Ils se placent dans le cadre du cycle spécification conception développement de systèmes de commande. L'objectif de ce programme est de rapprocher les équipes de différents laboratoires travaillant sur certaines étapes de ce cycle afin d'intégrer au mieux la sûreté de fonctionnement du système.*
Si on exclut les systèmes dédiés à la sécurité d'applications critiques, on peut confier au système de commande le soin de réagir aux défaillances du processus contrôlé. Cela implique en premier lieu d'être capable de diagnostiquer ces défaillances en ligne avant propagation irréversible et ce, de manière crédible, par la définition d'une instrumentation globale (commande + diagnostic) optimale en termes de précision, fiabilité et coût. En second lieu, il convient de définir les procédures de réaction aux défaillances identifiées, permettant soit de ramener le système dans un mode de fonctionnement normal, soit de l'arrêter en sécurité. La coopération de plusieurs spécialistes, l'homme process, l'automaticien (commande), l'instrumentiste et le spécialiste du diagnostic conduit, d'une part, à spécifier, indépendamment du support d'exécution, l'architecture fonctionnelle du système d'instrumentation, de commande et de réaction aux défaillances, et, d'autre part, à la valider. L'exploitation du formalisme des réseaux de Petri, permet de vérifier la conformité au cahier des charges et l'absence d'erreur.
Dans l'étape de conception, il faut définir une architecture informatique support (calculateurs, systèmes exécutifs, réseaux et protocoles), spécifier un placement des fonctions de l'Architecture Fonctionnelle sur l'architecture matérielle sous forme d'un ensemble de modules communicants, et enfin, prouver que le résultat vérifie toujours les propriétés de sûreté de fonctionnement c'est-à-dire que les hypothèses faites lors de la spécification ne sont pas violées. Les preuves doivent être faites au plus tôt et, si possible, avant l'implantation effective c'est-à-dire sur des modèles de cette implantation. Les techniques utilisées sont de deux types : analyse exhaustive de modèles d'automates temporisés lorsque cela est possible et approche stochastique et simulation dés que les systèmes deviennent trop complexes.

Mots - Clefs : Diagnostic, modes de marche, tolérances aux défaillances, temps réel, analyse de modèles

1. Introduction

La conception ancienne des systèmes industriels suivait une démarche séquentielle dans laquelle la mise en œuvre des moyens d'amélioration de la sûreté de fonctionnement du système et de la qualité des produits intervenait postérieurement à la conception du système de production, suivant elle-même la conception du produit. Après les efforts énormes d'automatisation des outils de production, les impératifs de rentabilité et de qualité ont entraîné la fusion des processus de conception du produit et de son système de production. Aujourd'hui, les gains de productivité et l'abaissement du coût des risques industriels peuvent encore s'obtenir par l'amélioration de la disponibilité des installations et de leur sécurité. Pour cela, l'intégration de ces objectifs doit se faire dès les premières étapes du cycle de vie de l'installation ; cahier des charges, spécification, conception, avec validation aussi systématique que possible des choix retenus. L'objectif est donc aujourd'hui de chercher à coordonner tous les métiers impliqués dans la conception d'un système industriel afin de rechercher une solution optimale satisfaisant les contraintes et

les objectifs de productivité et dans laquelle les défaillances sont des événements prévus et pris en compte.

Dans le cadre de son soutien à la recherche universitaire, le Conseil Régional de Lorraine a soutenu financièrement ce principe en créant le Programme Fédérateur de Recherches (PFR) « Sûreté Industrielle des Systèmes ». Ce programme associant 7 laboratoires Universitaires lorrains (LORIA, CRAN, GREEN, LRGSI, LSGC, LEMTA, LASC, LPMM), est intégré au contrat de plan Etat - Région 1993-1998 et contient deux opérations dont la principale Conception coordonnée de systèmes sûrs et de qualité" concerne les travaux présentés ici.

La maîtrise des systèmes industriels passe par l'automatisation de toutes les fonctions qui ne peuvent être confiées à l'opérateur humain pour des raisons de complexité, de performances, de sécurité ou de pénibilité. La relative fiabilité des systèmes de traitement de l'information utilisés pour réaliser les fonctions d'automatisation leur a longtemps interdit de prendre en compte directement les problèmes de sûreté de fonctionnement (sécurité en particulier) et a donc freiné le développement de l'approche globale que nous cherchons à promouvoir aujourd'hui. Commande et réaction aux fautes doivent être spécifiés conjointement et les moyens sûrs de leur réalisation doivent être recherchés. Ces deux propositions, bien que faisant l'objet des deux paragraphes ci dessous, ne sont pas sans interactions et les participants à ce thème ont mis en commun des moyens, confronté leurs approches et cherché leurs complémentarités à travers un certain nombre de réunions .

2. Prise en compte de la sûreté de fonctionnement dans la spécification d'un système industriel et de sa commande

En dehors des systèmes dédiés aux fonctions de sécurité dans lesquels les boucles de sécurité doivent être indépendantes des boucles de commande, dans la plupart des procédés industriels, la conception des systèmes de commande peut intégrer la prise en compte et la réaction aux défaillances. Cependant, cette démarche n'est bénéfique qu'à travers la coopération étroite des acteurs du processus de conception : le spécialiste du système à contrôler, l'automaticien et l'analyste de Sûreté de fonctionnement. La démarche conduit alors à une amélioration notable de la connaissance des phénomènes mis en jeu dans le système à contrôler. En effet, on sera amené à chercher des modèles plus fins de ce système afin de diagnostiquer les modes de fonctionnement et de défaillances, de contrôler tous les modes de fonctionnement et les passages d'un mode à l'autre, et de maîtriser le comportement en présence de défaillance par une réaction adéquate permettant la tolérance, le fonctionnement dégradé ou l'arrêt en sécurité.

Dans le processus menant à la spécification du système permettant d'assurer la production, nous nous intéressons ici à quelques aspects importants : comment disposer d'informations fiables au meilleur coût, comment établir un diagnostic crédible et rapide, comment spécifier le système de commande et de réaction aux défaillances et comment le valider.

2.1 Informations fiables, diagnostic crédible et rapide

- Dans le but de disposer d'informations sûres, il convient de concevoir un système d'instrumentation fiable et optimal. Les travaux de l'équipe du Pr. José Ragot du CRAN ont porté sur la recherche d'architectures optimales d'instrumentation incluant les critères de fiabilité et de coût (8).

- Disposant d'informations sûres, il convient alors de réaliser un diagnostic crédible et rapide de l'état du système, incluant l'état de son système d'instrumentation. Dans la même équipe, les travaux sur le diagnostic sont menés depuis de longues années. Ils portent par exemple sur le problème de la robustesse de la génération des résidus (11), indicateurs de défaillances, ou sur la validation des mesures fournies par les capteurs par comparaison à des estimations à partir de modèles. Les techniques récentes issues de la logique floue et de l'approche neuronales ont été explorées (3).

2.2 Spécification sûre du système de commande et de réaction aux défaillances

C'est l'approche hybride de la commande des systèmes, dans laquelle les défaillances sont considérées comme des événements discrets à prendre en compte au même titre que des changements de mode de marche par exemple. Ce travail est développé dans l'équipe du Pr JF. Aubry du CRAN avec une approche utilisant les Réseaux de Pétri Interprétés. Les transitions des réseaux sont synchronisées par les

événements issus du processus, de l'opérateur ou des horloges d'échantillonnage et les places contiennent les traitements discrets à réaliser sur les variables continues discrétisées. Dans ce modèle construit dans une approche déductive et par raffinements successifs (permettant de garantir a priori les bonnes propriétés du réseau (9)), on prend en compte toutes les hypothèses de défaillances du processus au niveau des événements de synchronisation, des conditions de franchissement de transition et de la cohérence de l'état du processus après action de la commande sur celui-ci (1). Cette analyse amène bien sûr à introduire dans la spécification du système de commande et de réaction aux fautes, un certain nombre de contraintes attachées aux différents modes identifiés.

- Nous avons appliqué la démarche à la commande de plusieurs processus électromécaniques. D'abord sur un groupe redresseur - onduleur où un certain nombre de défaillances et les procédures de reconfiguration propres à restaurer le fonctionnement normal ont été simulées et testées en vraie grandeur (14)(15). Ensuite nous avons abordé un système plus complexe: le cycloconvertisseur (alimentation de charges à forte puissance à très basse fréquence) (4)(5). La phase de spécification proprement dite a été faite avec le souci de rechercher une structure modulaire, compte tenu de l'architecture du convertisseur d'énergie utilisé et à définir les fonctions de coordination de la commande des trois modules.

Cette approche a permis de concevoir un système fonctionnant de manière sûre dans tous les modes possibles de fonctionnement, y compris la conduction discontinue que tous les dispositifs traditionnels évitent soigneusement à cause des problèmes qu'elle pose. De plus, la commande des interrupteurs du convertisseur est faite par impulsion unique, délivrée dans des conditions sûres d'effectivité, permettant ainsi le diagnostic de défaillance. Une méthode de reconfiguration du système de commande pour réaction à une défaillance d'interrupteur a été proposée, afin d'assurer la continuité de service de l'alimentation de la charge (moteur asynchrone par exemple) La phase de spécification de la commande a été validée par simulation. Une méthode simple a été proposée à cette fin (5).

Le travail a fait l'objet de deux maquettes expérimentales, d'abord sur un système mono-processeur puis, l'analyse de sûreté de l'architecture en ayant montré la nécessité, sur une structure multiprocesseur permettant de prendre en compte l'éventualité de parallèliser certaines fonctions. L'aspect fiabilité a pour sa part été pris en compte dans le recours à des processeurs spécialisés (type microcontrôleurs) Des approches de modélisation, par la méthode Marel, d'algorithmes microprogrammés dans les microcontroleurs, permettent notamment de garantir une meilleure sûreté du processus de traduction de la spécification en programmes. Ce travail est à relier en partie avec l'objet du §3.

- Nous avons commencé à appliquer ces méthodes dans le cadre des systèmes mécatroniques qui combinent des actionneurs mécaniques à une électronique de commande généralement localisée au plus près de l'actionneur (1), (13). L'augmentation des fonctions confiées à cette électronique entraîne inévitablement le recours à l'électronique programmée et la conception de ces systèmes est de plus en plus délicate, d'autant qu'ils sont fortement contraints en sûreté de fonctionnement. L'analyse du problème doit alors être menée dans le cadre d'une équipe associant les compétences de plusieurs spécialistes (automaticien, mécanicien, électronicien, analyste SdF). L'objectif est ici de réduire les coûts, d'améliorer la sûreté et de permettre une plus grande fluidité dans l'enchaînement des phases de spécification et de développement.

3. Prise en compte de la sûreté de fonctionnement dans le développement des systèmes de commande

Dans la section précédente, nous avons montré comment spécifier, de façon coordonnée, un système industriel et son système de commande afin de garantir la sûreté de fonctionnement de l'ensemble. Nous nous intéressons, dans cette section aux systèmes de commande réalisés sous forme d'une application informatique. Le résultat de leur spécification, telle qu'elle a été présentée ci-dessus, sera désigné sous le terme d'architecture fonctionnelle. Ce résultat définit les fonctions, les données et le comportement de l'application ainsi que les propriétés de sûreté qui ont été prouvées en faisant des hypothèses sur l'implantation et la distribution de cette architecture fonctionnelle. Il est donc indispensable de garantir que ces hypothèses sont bien respectées lors d'une implantation. C'est pourquoi, à l'étape de conception (appelée aussi analyse organique), il faut :

- définir une architecture informatique support (calculateurs, systèmes exécutifs, réseaux et protocoles)
- spécifier un partitionnement de l'AF en un ensemble de modules communicants et un placement de ces modules sur l'architecture matérielle,

- prouver que le résultat vérifie toujours les propriétés de sûreté de fonctionnement i.e. que les hypothèses faites lors de la spécification ne sont pas violées.

Pour des raisons économiques, les preuves doivent être faites le plus tôt possible lors du développement des systèmes et, si possible, avant son implantation effective c'est-à-dire sur des modèles de cette implantation (17). De plus, notons que cette activité de conception consiste non seulement en l'élaboration d'un système « correct », c'est-à-dire un système qui possède les propriétés requises de sûreté de fonctionnement, mais aussi en la construction du meilleur système au sens de critères à spécifier.

Les travaux que nous présentons dans cette section portent sur les moyens d'assurer cette étape de conception. Deux caractéristiques des systèmes y sont prises en compte : les problèmes induits par la distribution et les réseaux de communication, d'une part, et, d'autre part, les propriétés de sûreté de fonctionnement qui s'expriment sous la forme de contraintes de temps. Les résultats de ces travaux consistent en la définition et l'exploitation de modèles des systèmes. La pertinence et la précision des modèles sont liées aux propriétés (temporelles, pour cette étude) exigées des systèmes et aux critères de leur dimensionnement optimal. Les techniques mises en œuvre se situent en des phases différentes de la vie du système ; les premières consistent en une validation du système a priori, i.e. avant l'implantation tandis que les autres sont des vérifications en ligne, c'est-à-dire intégrées au système tout au long de son exploitation. Les dernières techniques permettent de mettre en œuvre des applications tolérant les fautes temporelles (non respect d'échéances, dérives temporelles).

Dans le cas des validations a priori, les points-clefs de la problématique sont illustrés à la figure 1 : il s'agit de définir comment exprimer les propriétés temporelles, comment modéliser l'application distribuée et enfin, comment exploiter le modèle pour prouver les propriétés.

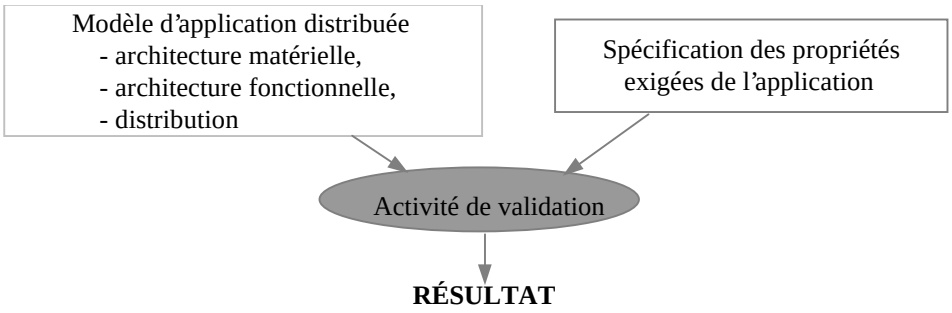

Figure 1 : validation a priori

3.1 Spécification des propriétés

Les propriétés temporelles auxquelles nous nous intéressons peuvent être qualitatives (propriétés s'exprimant sur l'ordre des occurrences d'événements) ou quantitatives (propriétés sur distances entre des occurrences d'événements).

Les résultats obtenus par l'équipe TRIO du LORIA, dans le contexte de ce projet portent sur l'expression des propriétés temporelles quantitatives et leur application aux interfaces entre couches adjacentes du modèle de communication (au sens modèle OSI) (20). Nous utilisons, pour les exprimer un formalisme reposant sur une logique temporelle à horloge explicite (12). La vérification du respect des contraintes de temps d' une application distribuée temps réel relève de l' observation des instants d' occurrence d' événements particuliers. Nous définissons un *événement* comme une condition logique qui représente un changement de condition physique du système. Une *occurrence* d' un événement est l' instant où la condition logique est vraie. Soit une fonction de datation d' occurrences d' événements est nécessaire, cette fonction est définie par rapport à un instant initial. Ces notions étant définies, nous avons proposé une classification des contraintes de temps : propriété sur la date d'une occurrence d'un événement (contrainte absolue), propriété sur l'intervalle séparant deux occurrences successives d'un même événement (contrainte relative), propriété sur l'intervalle séparant les occurrences homologues de deux événements (contrainte de causalité) et enfin propriétés sur l'inclusion d'occurrences d'un ensemble d'événements dans un intervalle de temps (contrainte de simultanéité) (21), (23).

3.2 Modélisations et exploitations des modèles

Dans le contexte des validations a priori, les techniques élaborées reposent sur l'exploitation de modèles de tout ou partie de l'application ; elles produisent deux types de résultats : un verdict sur le respect ou non de propriétés, ou une évaluation de certaines performances (temps de réponse, taux d'occupation de la mémoire, des processeurs ou du réseau …)

Pour obtenir le premier type de résultats, à savoir la preuve que l'application distribuée possède un ensemble de propriétés temporelles, nous exploitons des modèles de l'application exprimés soit dans le formalisme des réseaux de Petri temporels (2), soit dans celui des automates temporisés de type TIOSM (6). Nous avons, en particulier, développé des méthodes qui ajoutent un observateur neutre dans un modèle de l'application puis qui, par calcul exhaustif du graphe de comportement du modèle, fournissent le verdict pour une propriété (22). Pour maîtriser le problème de l'explosion combinatoire du graphe décrivant le comportement, nous proposons, également, une méthode de vérification de propriétés à la volée en appliquant une technique énumérative et un parcours de graphe en profondeur avec retour arrière en cas d'échec (7).

La deuxième approche est plus particulièrement utilisée dans le cas de systèmes complexes pour lesquels, soit le formalisme des réseaux de Petri ou des automates temporisés ne sont pas adaptés (modélisation d'ordonnancement, par exemple), soit les techniques d'analyse d'automates sont difficilement exploitables (taille du modèle trop important, …), ou dans le cas où des informations permettant une aide au dimensionnement de l'application (mémoire, taille de buffers, …) sont nécessaires. Nous utilisons le formalisme des réseaux de files d'attente et une approche stochastique. Notons que certains résultats peuvent être obtenus par une analyse du modèle sous des hypothèses fortes (16), mais dans la plupart des cas, nous validons l'application par évaluation de ses performances, et ce en simulant le modèle. Nous avons, en particulier, étudié la capacité de tolérances aux erreurs de transmission sur un bus embarqué dans l'automobile (bus CAN) (18), (10).

Enfin, ces deux techniques de validation (exhaustive par analyse de modèles –Model Checking- ou stochastique par simulation) sont implantées au sein d'un prototype d'atelier dans le cas de systèmes électroniques embarqués dans l'automobile et intégrant un réseau CAN (19). Ces travaux ouvrent deux voies de recherche à explorer : la première consiste à définir une méthodologie de validation de système, par application coordonnée des techniques d'analyse et de simulation et, ce par confinement des premières à des points clefs du système et itérations successives entre les deux méthodes. La deuxième voie de recherche doit apporter des solutions au problème de la pertinence des scénarios dans une technique de simulation. Pour ce faire, nous menons des études, en coordination entre les travaux présentés au paragraphe 2.2 et ceux exposés ici afin, en particulier, de modéliser l'environnement conformément à l'identification qui en a été faite par les automaticiens.

4. Conclusion

Dans ce projet, deux laboratoires se sont associés pour confronter leurs approches dans le domaine de la conception des systèmes de commande sûrs de fonctionnement. Ces approches complémentaires cherchent à apporter des méthodologies pour d'une part la spécification des systèmes d'instrumentation, de diagnostic et de commande et, d'autre part, le développement qui recherche l'architecture opérationnelle capable de respecter les propriétés précédemment spécifiées. Le souci des partenaires est de rechercher une solution de continuité dans ce processus de conception intégrant la sûreté de fonctionnement, depuis le cahier des charges jusqu'à la réalisation du prototype. La plupart de ces travaux ont été développés dans le cadre de collaborations industrielles tant régionales (domaine du diagnostic en particulier) que nationales (commande, réaction et développement), mais concernent très souvent des grands groupes industriels. Cette coopération se poursuit dans le cadre des actions soutenues par l'Institut de Sûreté Industrielle, organe du Pôle Européen Universitaire de Nancy-Metz. Un des rôles de cet institut est de chercher à mettre au service des PME PMI lorraines, le bénéfice des travaux menés par ces équipes de recherches avec les grands groupes industriels. Pour cela, il travaille en étroite collaboration avec toutes les instances régionales, associations, collectivités, chambres consulaires, dans le but d'informer, de former et de proposer des coopérations.

5. Bibliographie

(1) J-F. Aubry, C. Zanne, *Dependability of on board applications: an approach through the control system.* IEEE - AVCS, Amiens, juillet 98

(2) Berthomieu, B., Diaz, M. *Modeling and Verification of Time Dependant Systems Using Time Petri Nets*, IEEE Transactions on Software Engineering, 17(3), pp.259-273 (1991)

(3) Boukhris A., Giuliani S., Mourot G., Querelle R., Frank P.M. *Comparison of two fuzzy modelling approaches applied to the rainfall-runoff relationship.* 11th IFAC Symposium on System Identification, SYSID'97, Fukuoka, Japan, July 8-11, 1997.

(4) Elmasri A., Aubry J-F., *Conception and implementation of a cycloconverter digital control based on a MC 68332 microcontroller system* IEEE MEPCON, Alexandria, 4-6 January 1997 pp. 276 - 280

(5) Elmasri A., *Conception et réalisation de la commande numérique rapprochée d'un convertisseur électromécanique: application au cycloconvertisseur triphasé*, Thèse de Doctorat de l'INPL, (1997)

(6) Kaiser L., Koné O., *Une méthode de vérification d'interopérabilité temporelle*, Colloque francophone RENPAR'9, Lausanne (1997).

(7) Kaiser L. *Vérification de propriétés temporelles à la volée*, Colloque francophone RENPAR'10, Strasbourg (1998),.

(8) Luong M., Maquin D., Ragot J., *Sensor network design for failure detection and isolation.* IFAC Conference on Control of Industrial Systems, Belfort, France, May 20-22, 1997.

(9) Moitessier F., Aubry J-F., Derniame J-C., Zanne C., *A method for the conception of control systems for hybrid processes using Petri Nets*, Congrès ADPM - AFCET Paris janvier 92

(10) Navet N., Song Y.-Q. *On Fault Tolerance and Worst-Case Response Time Analysis in CAN*, 23nd IFAC/IFIP Workshop on Real-Time Programming, Chine(1998).

(11) Nuninger W., Kratz F., Ragot J., *Structural equivalence between direct residuals based on parity space and indirect residuals based on unknown input observers*, IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS'97, Hull, UK, (1997).

(12) Ostroff J.-S. *Temporal Logic fo Real-Time Systems*, Advanced Software Development Series. Research Studies Press Limited, John Wiley and Sons (1989).

(13) Rozière M., *Aide à la conception de stratégies de diagnostic et de reconfiguration dédiée aux systèmes hybrides*, Mémoire de DEA, INPL sept. 1997

(14) Sawicki J-P., Aubry J-F., Zanne C., *Sûreté d' un processus hybride parreconfiguration de sa commande. Exemple d' un convertisseur statique en défaut onduleur*,Congrès ADPM - AFCET Bruxelles novembre 94.

(15) Sawicki J-P., Zanne C., Aubry J-F., *Inverting mode failure recovery: application to the drive of a generator supplied by a three phase thyristor converter*, 4th IEEE Conference on Control Applications pp 383-388 Albany USA sept 28-29 1995.

(16) Simonot F., Song Y.-Q., Real-Time Communications using TDMA-based Multi-Access Protocol, Computer Communications 20, 6, Juillet 1997, pp.435-448.

(17) Simonot-Lion F., Thomesse JP., Bayart M., Staroswiecki M. *Dependable Distributed Computer Control Systems : Analysis of the Design Step Activities*, Proceedings of IFAC - DCCS' 95,Toulouse-Blagnac, (1997).

(18) Simonot-Lion F., Song Y.-Q., Raymond J., *Validating Real-Time Applications distributed over CAN : an Interoperability Verification*, 4th International CAN Conference, ICC'97, Berlin (1997).

(19) Song Y.Q., Simonot-Lion F., Belissent P., *VACANS – A Tool for the Validation of CAN-Based Applications*, Proceedings of 2nd IEEE International WFCS'97, Barcelone, Espagne (1997).

(20) Thomesse J.-P., Mammeri Z., Vega L, *Time in Distributed Systems Cooperation and Communication Models*, Proceedings 5th Workshop on FTDCS, IEEE Computer Society Press, Cheju Island, Korea (1996).

(21) Toussaint J., Vega L., Simonot-Lion F., *Formal Verification of Time Constrained Communications*, Proceedings of ISCA International Conference on Parallel and Distributed Computing Systems, pp.138-143, Dijon, France, 1996.

(22) Toussaint J., Simonot-Lion F., *Vérification formelle de propriétés temporelles d'une application distribuée temps réel*, Conférence Real-Time Systems'97, éditions Teknéa, Paris, 1997.

(23) Vega Saens L., *Modèles de coopération et de communication entre processus temps réel répartis : expression de contraintes de temps pour la vérification de propriétés temporelles*, thèse de doctorat de l'Institut National Polytechnique de Lorraine, 1996.