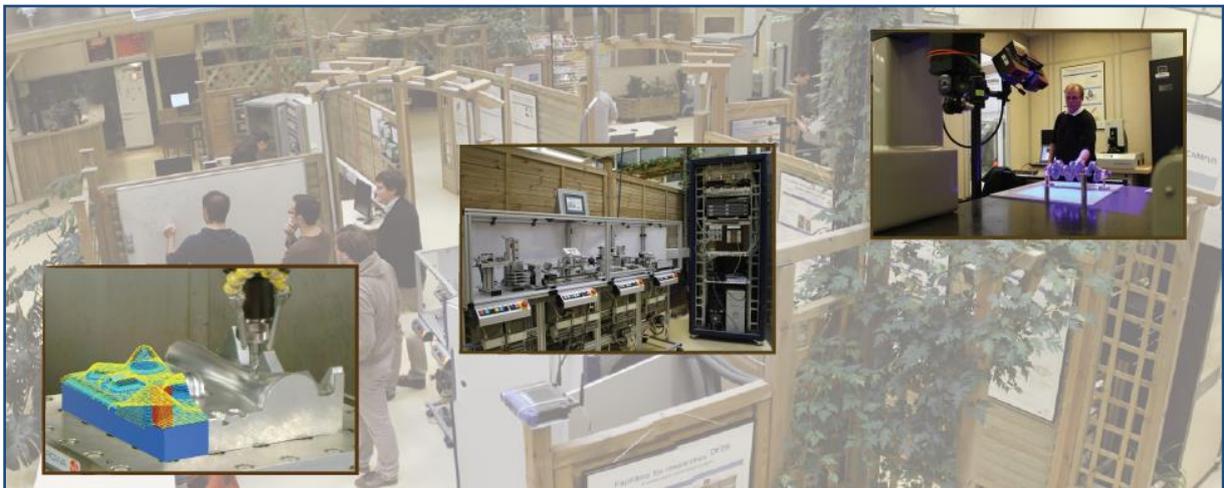




LABORATOIRE UNIVERSITAIRE DE RECHERCHE EN PRODUCTION AUTOMATISEE



Rapport d'activité janvier 2008 – juin 2013 de l'Équipe ISA Ingénierie des Systèmes Automatisés

Créé en 1981, le **LURPA** (Laboratoire Universitaire de Recherche en Production Automatisée) est un laboratoire de Recherche de l'**École Normale Supérieure de Cachan**. Il a le statut d'Équipe d'Accueil du Ministère de l'Enseignement Supérieur et de la Recherche depuis 1994 (EA 1385). Il est, depuis 2004, placé sous la co-tutelle de l'**Université Paris-Sud**.

Le LURPA est structuré en deux équipes :

- **Équipe Géo3D** : Géométrie tridimensionnelle des pièces et des mécanismes,
- **Équipe ISA** : Ingénierie des Systèmes Automatisés,

Ce document correspond au **Rapport scientifique de l'Équipe ISA pour la période Janvier 2008 à juin 2013**.

Avant-propos

Le thème général des recherches de l'Équipe ISA est la **commande sûre des Systèmes à Événements Discrets (SED)** ou **Dependable Control of Discrete event Systems**. Dans ce rapport, les résultats de ces recherches pour la période janvier 2008 / juin 2013 sont présentés selon quatre thématiques :

- Test et vérification formelle des contrôleurs logiques,
- Approches algébriques pour la synthèse et l'analyse formelles,
- Identification des SED,
- Approches SED pour l'analyse de sûreté.

Les trois premières thématiques regroupent des travaux relevant des problématiques classiques de l'Automatique des SED : **Analyse**, **Synthèse** et **Identification**. Dans la quatrième thématique, il s'agit plutôt d'étudier dans quelle mesure l'utilisation des paradigmes, modèles et méthodes des SED permet de formaliser les modèles utilisés en sûreté de fonctionnement et d'en rigorer la construction et l'analyse.

Ce document a été rédigé en considérant qu'il sera principalement exploité de manière électronique. Différents renvois ont donc été insérés pour permettre d'en prolonger la lecture en offrant la possibilité d'aller plus loin via notre nouveau site WWW. Cela est particulièrement le cas pour les publications dont des liens hypertextes permet d'accéder directement au contenu diffusé sur HAL :

- <http://hal.archives-ouvertes.fr/lab/lurpa/>

LURPA

<http://www.lurpa.ens-cachan.fr/>

Équipe ISA

<http://www.lurpa.ens-cachan.fr/version-francaise/recherche/equipe-isa/>

Table des matières

Table des matières.....	1
1. Présentation générale de l'Équipe ISA	3
1.1. Composition de l'équipe.....	3
1.2. Objectif des recherches.....	3
1.3. Mots-clés	4
2. Thématique « Test et vérification formelle des contrôleurs logiques »	5
2.1. Test de conformité des contrôleurs logiques	5
2.1.1. Objectifs des travaux	5
2.1.2. Principaux résultats obtenus.....	5
2.1.3. Commentaires.....	7
2.1.4. Références externes au LURPA.....	7
2.2. Évaluation des bornes des performances temporelles par preuves itératives de propriétés logiques	7
2.2.1. Objectifs des travaux	7
2.2.2. Principaux résultats obtenus.....	7
2.2.3. Commentaires.....	9
2.2.4. Références externes au LURPA ou antérieures à 2008.....	9
2.3. Modélisation réaliste et multi-échelles des systèmes bouclés temporisés	9
2.3.1. Objectifs des travaux	9
2.3.2. Principaux résultats obtenus.....	9
2.3.3. Commentaires.....	11
2.3.4. Références externes au LURPA ou antérieures à 2008.....	11
3. Thématique « Approches algébriques pour la synthèse et l'analyse formelles »	12
3.1. Approches algébriques pour la synthèse formelle des contrôleurs logiques.....	12
3.1.1. Objectifs des travaux	12
3.1.2. Principaux résultats obtenus.....	13
3.1.3. Commentaires.....	14
3.1.4. Références externes au LURPA.....	14
3.2. Évaluation de performance par algèbre (Max, +).....	15
3.2.1. Objectifs des travaux	15
3.2.2. Principaux résultats obtenus.....	15
3.2.3. Commentaires.....	16
3.2.4. Références externes au LURPA	17
4. Thématique « Identification des SED »	18
4.1. Identification des SED par Automates finis	18
4.1.1. Objectifs des travaux	18
4.1.2. Principaux résultats obtenus.....	19
4.1.3. Commentaires.....	20
4.2. Identification des SED par Réseaux de Petri.....	20
4.2.1. Objectifs des travaux	20
4.2.2. Principaux résultats obtenus.....	20
4.2.3. Commentaires.....	21
4.2.4. Références externes au LURPA ou antérieures à 2008.....	21
5. Thématique « Approches SED pour l'analyse de sûreté »	23
5.1. Formalisation des outils pour l'analyse de sûreté	23
5.1.1. Objectifs des travaux	23
5.1.2. Principaux résultats obtenus.....	24
5.1.3. Commentaires.....	26
5.1.4. Références extérieures	27
5.2. Allocation des fonctions de contrôle-commande des systèmes critiques par analyse d'atteignabilité.....	27
5.2.1. Objectifs des travaux	27
5.2.2. Principaux résultats obtenus.....	28
5.2.3. Commentaires.....	29
5.2.4. Références extérieures	29
5.3. Analyse de sûreté des architectures de contrôle/commande	29
5.3.1. Objectifs des travaux	30

5.3.2. Principaux résultats obtenus	30
5.3.3. Commentaires	31
5.3.4. Références externes au LURPA.....	31
6. Collaborations nationales et internationales	32
6.1. Collaborations nationales	32
6.2. Collaborations internationales.....	32
7. Activités d’animation et de rayonnement national et international.....	33
7.1. Activités au plan national.....	33
7.2. Activités au plan international.....	35
8. Activités contractuelles et valorisation.....	37
8.1. Projets de recherche nationaux	37
8.2. Collaborations industrielles	38
8.3. Collaboration au sein de l’ENS Cachan.....	38
9. Formation par la recherche	40
9.1. Formation initiale.....	40
9.2. Formation en Master Recherche	40
10. Publications, thèses, masters	43
10.1. Articles dans des revues à comité de lecture à diffusion internationale	43
10.2. Brevets	44
10.3. Conférences plénières ou invitées	44
10.4. Communications dans des congrès internationaux avec actes	44
10.5. Communications dans des congrès francophones avec actes	47
10.6. Thèses	48
10.7. Masters	49

1. Présentation générale de l'Équipe ISA

1.1. Composition de l'équipe

Au 1^{er} janvier 2013, l'équipe **Ingénierie des Systèmes Automatisés – ISA** - comprend 6 permanents, à savoir 2 Professeurs des Universités et 4 Maîtres de Conférences. Durant la période de référence, l'équipe a été dirigée par Bruno Denis, puis par Jean-Marc Roussel qui en assure la direction depuis le 1^{er} novembre 2010.

- **Professeurs des Universités**

- Jean-Marc Faure SUPMECA
- Jean-Jacques Lesage ENS Cachan

- **Maîtres de Conférences**

- Saïd Amari Université Paris-Nord 13
- Bruno Denis ENS Cachan
- Gregory Faraut¹ ENS Cachan
- Jean-Marc Roussel ENS Cachan

Au 1^{er} janvier 2013, l'équipe accueille également 8 doctorants :

- **Doctorants de 1^{ère} année :**

- Pierre-Antoine Brameret Contrat Doctoral spécifique pour Normalien
- Pierre-Yves Piriou Financement lié au projet BGLE Connexion

- **Doctorants de 2^{ème} année :**

- Anaïs Guignard Financement lié à l'ANR VACSIM

- **Doctorants de 3^{ème} année et au-delà :**

- Damien Aza-Vallina Contrat Doctoral spécifique pour Normalien
- Mickaël Danancher Contrat Doctoral spécifique pour Normalien
- Pierre-Yves Chaux Financement CIFRE, thèse soutenue le 15 avril 2013
- Ana-Paula Estrada-Vargas Financement mexicain, thèse soutenue le 20 février 2013
- Thibaut Lemattre Financement CIFRE, soutenance prévue le 9 juillet 2013

1.2. Objectif des recherches

Le thème général des recherches de l'Équipe ISA est **la commande sûre des Systèmes à Événements Discrets (SED) ou Dependable Control of Discrete event Systems**. Ce thème de recherche, reconnu par l'IFAC (International Federation of Automatic Control), correspond aujourd'hui au cycle de workshops Dependable Control of Discrete event Systems (DCDS) initié par l'Équipe en 2007 :

- DCDS 07 : 1^{ère} édition en juin 2007 à Cachan,
- DCDS 09 : 2^{ème} édition en juin 2009 à Bari (Italie),
- DCDS 11 : 3^{ème} édition en juin 2011 à Saarbrücken (Allemagne),
- DCDS 13 : 4^{ème} édition en septembre 2013 à York (Angleterre),

Les recherches de l'Équipe ISA visent à **développer des méthodes, techniques et outils permettant** d'améliorer la conception, l'implantation et l'exploitation des systèmes de commande majoritairement discrets, afin d'en **accroître la sûreté de fonctionnement**. Si, initialement, nos travaux ne concernaient que les systèmes mécatroniques complexes, nous nous intéressons aujourd'hui aux **systèmes critiques** présents tout aussi bien dans les systèmes de production de biens ou de services comme **l'énergie** et le **transport**. De ce fait, les architectures de commande étudiées par l'Équipe vont de l'électronique embarquée jusqu'au contrôle via des réseaux locaux industriels, en passant par les architectures distribuées conventionnelles.

¹ Grégory Faraut a rejoint l'Équipe ISA en septembre 2011.

À l'intérieur de ce thème général, pour la période considérée, nos recherches se sont structurées selon les quatre thématiques suivantes :

- Test et vérification formelle des contrôleurs logiques,
- Approches algébriques pour la synthèse et l'analyse formelles,
- Identification des SED,
- Approches SED pour l'analyse de sûreté.

Les trois premières thématiques regroupent des travaux relevant des problématiques classiques de l'Automatique des SED : **Analyse**, **Synthèse** et **Identification**. Dans la quatrième thématique, il s'agit plutôt d'étudier dans quelle mesure l'utilisation de nos compétences acquises dans le domaine des SED permet de formaliser les modèles utilisés en sûreté de fonctionnement et d'en rigorer la construction et l'analyse.

D'une manière générale, les recherches de l'Équipe ISA ont pour but **de proposer des apports formels ou méthodologiques à des outils de modélisation issus de l'industrie en répondant à des besoins industriels déjà présents ou sur le point de le devenir**. Elles intègrent le plus souvent une part importante d'expérimentations réalisées sur des systèmes réels ou d'exemples tirés de tels systèmes.

Vouloir **confronter les résultats théoriques de recherche à des expérimentations réalisées sur des systèmes réels** est une spécificité de l'Équipe comme du laboratoire. C'est un objectif ambitieux dont l'aspect chronophage est plus qu'évident puisqu'il exige de coûteux développements informatiques et de nombreuses expérimentations avant de conduire à des résultats concrets. Cependant cette démarche scientifique est très formatrice car elle permet d'asseoir une culture technologique forte nécessaire à ce type de travaux tout en obligeant d'intégrer, dès l'étude théorique du problème, les nécessaires contraintes de la mise en œuvre.

Si le cœur scientifique de l'Équipe ISA demeure les **Systèmes à Événements Discrets (SED)**, la démarche scientifique suivie intégrant la confrontation des nouveaux résultats théoriques acquis à des expérimentations réalisées sur des systèmes réels, comme le transfert vers d'autres domaines scientifiques constituent certainement l'un des atouts majeurs des bonnes relations liant l'Équipe à ses partenaires académiques ou industriels.

Pour la période considérée, l'Équipe ISA a eu différents partenaires académiques et industriels :

- **Partenaires académiques en France**
 - Équipe Sympa du CRAN, Université de Lorraine (Nancy)
 - Équipe Sysmo du LIX, École Polytechnique (Palaiseau)
 - Équipe AC SED de l'IRCCyN (Nantes)
- **Principaux partenaires académiques à l'International**
 - Institute of automatic control AT+, University of Kaiserslautern (Kaiserslautern, Allemagne)
 - Équipe SED, Unité Guadalajara du Cinvestav (Guadalajara, Mexique)
 - Dipartimento di Informatica, Università del Piemonte Orientale (Alessandria, Italie)
 - Laboratoire de Conception et Conduite des Systèmes de Production, Université Mouloud MAMMERI (Tizi Ouzou, Algérie)
- **Principaux partenaires industriels**
 - EDF Recherche et développement
 - Équipe STEP (site de Chatou) : Simulation et Traitement de l'information pour l'Exploitation des systèmes de Production,
 - Équipe MRI (site de Clamart) : Management des Risques Industriels
 - Société Dassault Systèmes
 - Société EADS, IW Suresnes et Eurocopter Marignane

1.3. Mots-clés

Les mots-clés qui caractérisent l'Équipe ISA sont : Systèmes à Événements Discrets (SED), Sûreté de fonctionnement, Méthodes formelles, Contrôle-commande, Systèmes d'automatisation.

Concernant les modèles utilisés : Automates finis, Théorie des langages, Réseaux de Petri, Algèbre (max,+), Chaînes de Markov.

2. Thématique « Test et vérification formelle des contrôleurs logiques »

Garantir que le système de commande pilotera de manière sûre l'installation qu'il contrôle est une contrainte de plus en forte à laquelle sont confrontés tous les industriels. C'est particulièrement le cas des systèmes critiques comme l'énergie et le transport. Pour mener à bien cette activité, il existe 2 stratégies complémentaires :

- Le **test du contrôleur réel**, une fois celui-ci programmé,
- La **vérification formelle du modèle de comportement de ce contrôleur**.

La vérification formelle des contrôleurs logiques a été une importante activité de recherche durant le précédent contrat quadriennal (2004-2007). Plusieurs résultats importants ont été obtenus dans le domaine de la vérification de propriétés qualitatives. Pour cette période quinquennale, nous nous sommes principalement intéressés à la vérification de **propriétés quantitatives** de systèmes temporisés. Plus précisément, ces travaux ont concerné :

- l'évaluation des bornes des performances temporelles des architectures d'automatisation en réseau,
- la modélisation réaliste et multi-échelles des systèmes bouclés temporisés.

En complément de la vérification formelle, nous avons également travaillé autour du test de conformité des contrôleurs logiques, seule technique garantissant que l'exécution des lois de commandes sur un matériel donné est conforme à ce qui est spécifié.

2.1. Test de conformité des contrôleurs logiques

Le test de conformité est une technique de test **fonctionnel**, et non structurel, qui a pour objectif de s'assurer que le comportement d'une implantation, considérée comme une boîte noire dont on peut observer les entrées/sorties, est identique au comportement spécifié. De manière générale, le test de conformité d'une implantation comporte deux phases :

- Construction d'une séquence de test à partir de la spécification, chaque élément de cette séquence étant composé d'un vecteur d'entrée et du vecteur de sortie escompté en réponse au vecteur d'entrée associé. La construction de cette séquence nécessite que la spécification soit exprimée sous la forme d'un modèle formel et qu'un taux de couverture de ce modèle ait été préalablement défini.
- Exécution proprement dite du test de conformité. Durant cette phase, pour chaque élément de la séquence précédemment élaborée, la réponse produite par l'implantation est comparée à celle attendue. La non-conformité de cette réponse conduit à un verdict de test négatif.

De nombreux résultats théoriques ont été obtenus dans ce domaine, en se basant pour ce qui concerne les systèmes non temporisés sur des modèles de spécification sous la forme de machines de Mealy [Lee and Yannakakis, 1996], de systèmes de transitions [Jéron, 2004], [Tretmans, 2008] ou de certaines classes de réseaux de Petri [von Bochmann and Jourdan, 2009]. Ces travaux ont permis de formaliser des méthodes efficaces de construction de la séquence de test et d'utilisation de cette séquence sur un modèle de l'implantation, en mettant en évidence en particulier les cas de test non-concluants. Quel que soit l'intérêt de ces contributions, elles ont cependant toutes supposées que la spécification était représentée dans un formalisme complètement défini, ce qui n'est pas le cas dans la quasi-totalité des applications industrielles où la spécification d'un contrôleur est décrite dans un langage métier, bien adapté à l'ingénieur automaticien mais dont le formalisme est le plus souvent défini sous forme textuelle ou à l'aide d'exemples illustratifs. D'autre part, la limitation de l'analyse de l'exécution sur un modèle de l'implantation, et non sur un contrôleur logique réel, ne permet pas de prendre en compte l'influence des caractéristiques technologiques de ce contrôleur sur le verdict du test de conformité.

2.1.1. Objectifs des travaux

L'objectif des travaux de la thèse de Julien Provost [TH 8] a été de contribuer à combler les lacunes des travaux décrits ci-dessus afin de faciliter l'acceptation des techniques de test de conformité par l'industrie. Plus précisément, ces travaux ont concerné le test de conformité de contrôleurs logiques industriels à **scrutation cyclique des entrées** dont la spécification du comportement est décrite dans le **langage Grafcet** (norme IEC 60848). Ces travaux se sont déroulés dans le cadre du [Projet ANR TESTEC \(07-TLOG 022\)](#) « **T**Est des **S**ystèmes Temps réel **E**marqués **C**ritiques ».

2.1.2. Principaux résultats obtenus

Le premier résultat majeur de ces travaux est une méthode de traduction, sans perte de sémantique, d'un modèle Grafcet en une machine de Mealy équivalente [ACL 9], [CAI 33]. Cette traduction repose sur un modèle intermédiaire,

dénoté Automate des Localités Stables, qui exprime formellement l'ensemble des états stables du modèle initial ; ce modèle intermédiaire peut être traduit aisément en une machine de Mealy en explicitant les conditions logiques qui étiquettent ses transitions. Sur la base de ce résultat et des résultats antérieurs sur la génération d'une séquence de test de longueur minimale assurant la couverture de toutes les transitions d'une machine de Mealy [Naito and Tsunoyama, 1981], une méthode de construction d'une telle séquence à partir d'un modèle de spécification Grafcet a été développée [CAI 12], [CAI 25], [CAI 29], [CAN 5], et implantée dans le logiciel TELOCO, disponible à l'adresse :

- <http://www.lurpa.ens-cachan.fr/-211030.kjsp>

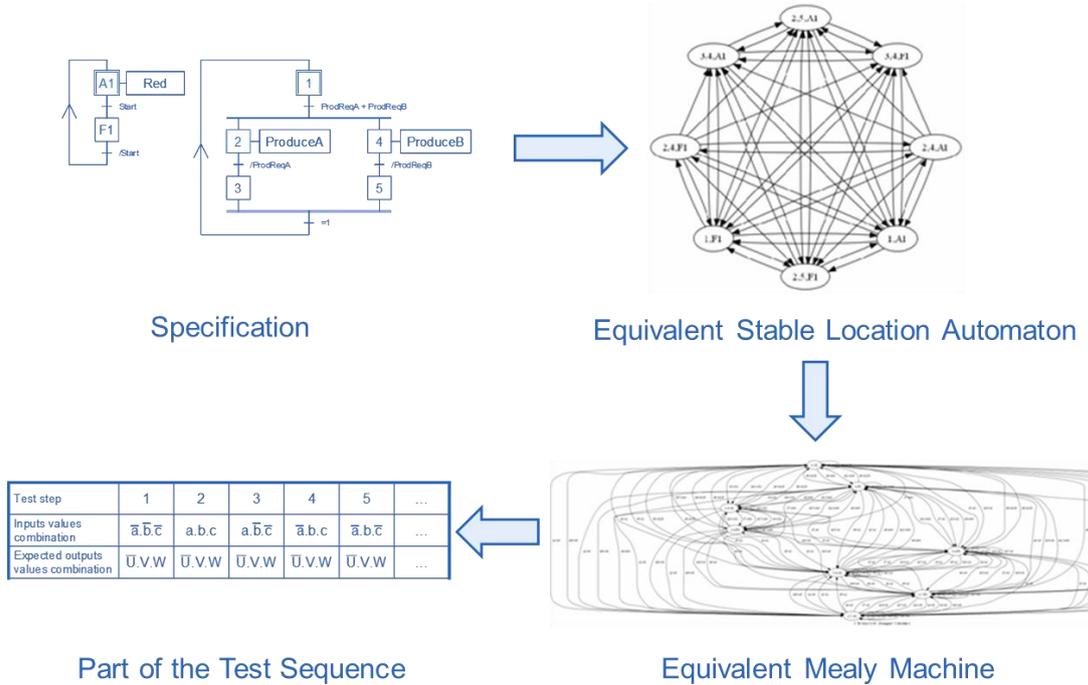


Figure 1 Construction d'une séquence de test à partir d'une spécification en langage IEC 60848

Plusieurs expérimentations sur banc de test ont montré que l'exécution de cette séquence pour le test de conformité d'un contrôleur réel pouvait conduire à des verdicts erronés [CAN 7]. L'analyse de ces erreurs de verdict a montré qu'elles se produisaient toujours lorsque les valeurs de plusieurs entrées étaient simultanément modifiées d'un pas de test au suivant. En effet, la lecture des entrées d'un contrôleur logique ne se fait en un temps strictement nul et durant cette phase de lecture **des événements synchrones** (changements de valeurs d'entrées simultanés) **peuvent être perçus comme asynchrones**.

Ceci nous a conduit à introduire le concept de **SIC-testabilité** [CAI 21], capacité d'une spécification à pouvoir être testée sans erreur de verdict, c.à.d. à l'aide d'une séquence de test de type SIC (Single Input Change), telle que la valeur d'une seule entrée est modifiée d'un pas de test au suivant. Cette propriété n'étant pas vérifiée dans la plupart des cas, nous avons ensuite proposé le concept de **taux de couverture garanti sans erreur de verdict**, qui indique le pourcentage d'un modèle de spécification formelle que l'on peut tester par une séquence SIC. Des algorithmes de construction de la séquence de test pour ces deux cas de figure (spécification SIC-testable ou non) ont été ensuite développés.

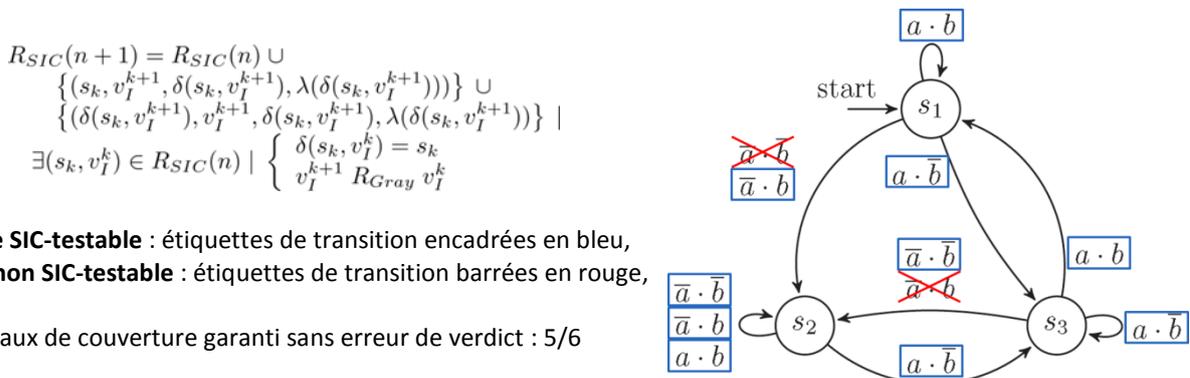


Figure 2 Principe de la recherche de la partie SIC-testable

2.1.3. Commentaires

Ces travaux visant à la validation d'un contrôleur réel et non d'un modèle de ce contrôleur, par comparaison aux approches de vérification précédemment exposées, ont combiné efficacement contributions théoriques et expérimentations. Ils se poursuivent dans le cadre de la thèse d'Anaïs Guignard, financée par le [Projet ANR VACSIM \(11-INSE 0004\)](#) « **VA**lvalidation de la commande des systèmes critiques par **CO**uplage **SI**mulation et **M**éthodes d'analyse formelle ». L'accent est mis sur l'observation des séquences d'entrée/sortie du contrôleur couplé au processus commandé, afin de diminuer la durée nécessaire à la validation par réduction de l'espace d'état à explorer.

2.1.4. Références externes au LURPA

T. Jéron. Contribution à la génération automatique de tests pour les systèmes réactifs. Habilitation à diriger des recherches, Université de Rennes 1, France, 2004.

D. Lee and M. Yannakakis. Principles and methods of testing finite state machines - a survey. *Proceedings of the IEEE*, 84(8), 1996, pp. 1090–1123.

S. Naito and M. Tsunoyama. Fault detection for sequential machines by transitions tours. *Proceedings of the IEEE fault tolerant computer symposium*, 1981, pp. 238–243.

J. Tretmans. Model based testing with labeled transition systems. *Formal Methods and Testing*, LNCS 4949, 2008, pp. 1–38.

G. von Bochmann and G.V. Jourdan. Testing k-safe Petri nets. LNCS 5826, 2009, pp. 33–48.

2.2. Évaluation des bornes des performances temporelles par preuves itératives de propriétés logiques

Même si l'évaluation des délais de bout en bout, à l'aide de méthodes telles que le calcul réseau [Cruz, 1991], [Georges, 2005] ou la méthode des trajectoires [Bauer, 2010], offrent des perspectives importantes pour la conception des architectures d'automatisation en réseau, il n'en demeure pas moins vrai que ces méthodes ne considèrent que les délais introduits par les composants du réseau et non ceux résultant de traitements et/ou de synchronisations au sein des composants de contrôle/commande, tels que modules d'entrée/sortie et contrôleurs industriels. Ce sont pourtant les performances temporelles globales de l'architecture qui intéressent l'automaticien. L'évaluation de ces performances, comme le temps de réponse ou la différence de temps de réponse, requiert de prendre en compte l'ensemble des mécanismes de consommation de temps dans tous les composants de l'architecture.

Il convient en outre de souligner qu'une performance temporelle est caractérisée non pas par une valeur unique mais par une loi de distribution de valeurs, les mécanismes de consommation de temps au sein de l'architecture induisant des délais variables. Nos travaux antérieurs [Marsal, 2006], [Meunier, 2006], avaient permis de proposer des méthodes d'obtention de la distribution d'une performance qui s'appuyaient sur la simulation de modèles d'architecture sous la forme de réseaux de Petri temporisés et colorés. Quel que soit l'intérêt de ces résultats, ce sont les bornes de la distribution qui importe lorsque des applications critiques sont envisagées et une approche par simulation ne permet malheureusement pas de connaître ces bornes avec certitude mais seulement des valeurs minimale et maximale les approximant avec un certain niveau de confiance.

2.2.1. Objectifs des travaux

Ceci explique que nous avons entrepris dans le cadre de la thèse de Silvain Ruel [TH 4], soutenue en juillet 2009, des recherches visant à proposer une méthode d'évaluation des bornes des performances temporelles des architectures d'automatisation en réseau, en considérant le cas particulier des architectures basées sur le protocole Modbus TCP/IP. Ce protocole est un exemple de solution de type Ethernet industriel reposant sur des mécanismes de communication clients/serveurs, les contrôleurs industriels étant les clients et les modules d'entrées-sorties distribués les serveurs. On notera enfin qu'une partie de ces travaux a été effectuée dans le cadre du [Projet Farman SIMOP](#), en collaboration avec le Laboratoire Spécification et vérification (LSV – UMR 8643).

2.2.2. Principaux résultats obtenus

Le premier résultat des travaux de thèse de Sylvain Ruel est une méthode de détermination des bornes d'une performance temporelle par preuves itératives de propriétés d'atteignabilité [CAI 15]. Cette méthode s'appuie sur un modèle formel de l'architecture, sous la forme d'un réseau d'automates temporisés communicants, où chaque automate modélise un composant de l'architecture de contrôle/commande. Les propriétés d'atteignabilité sont définies sur un automate observateur paramétré, dont certaines gardes sont fonction d'un paramètre temporel. A l'issue de chaque itération, les

résultats des preuves permettent de définir la valeur de ce paramètre pour la prochaine itération, au moyen d'un algorithme de recherche par dichotomie assurant la convergence des itérations.

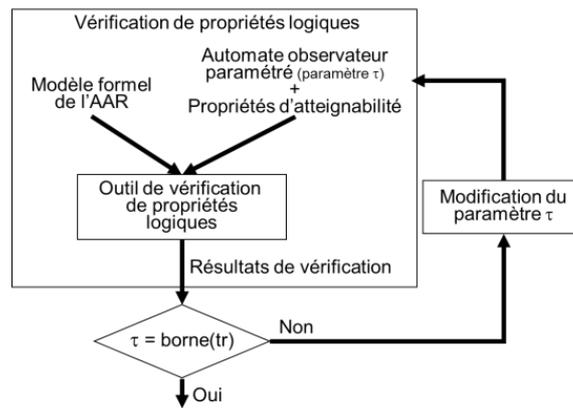


Figure 3 Stratégie de recherche de bornes

Des problèmes d'explosion combinatoire étant apparus lors de la mise en œuvre de cette méthode sur des exemples non triviaux, une technique d'abstraction du modèle formel de l'architecture a été proposée [CAI 4], [CAI 8]. Cette technique comporte deux étapes :

- simplification de la structure du modèle initial d'architecture,
- modification des modèles de composants subsistant dans la structure simplifiée.

L'objectif de la première étape est de supprimer les modèles des composants qui n'influencent pas directement sur la performance temporelle étudiée ; la seconde étape vise à prendre en compte dans les modèles de composants conservés l'impact potentiel des modèles supprimés. Il a également été démontré lors de ces travaux que cette abstraction est conservative, c.à.d. que la borne inférieure et la borne supérieure, obtenues toute deux avec le modèle abstrait, minimise et maximise respectivement les bornes inférieure et supérieure obtenues avec le modèle détaillé.

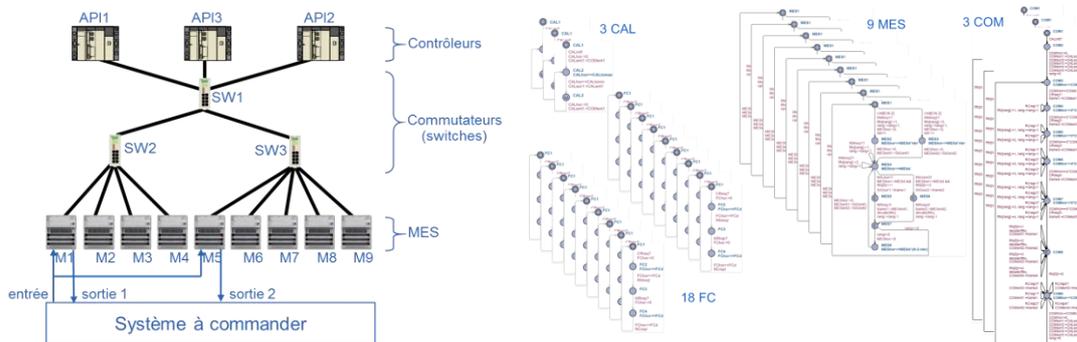


Figure 4 Exemple d'architecture d'automatisation en réseau et Modèle formel détaillé correspondant

Enfin, la méthode d'évaluation proposée a été validée expérimentalement, sur la base de six cas d'étude de complexité croissante. Cette validation a montré en particulier :

- que la technique d'abstraction développée lors de ces travaux augmente très nettement les possibilités de passage à l'échelle,
- que les valeurs de bornes obtenues par preuves itératives de propriétés sur un modèle formel sont très proches de celles mesurées sur une architecture réelle et encadrent ces mesures de façon très peu pessimiste, ce qui valide nos apports.

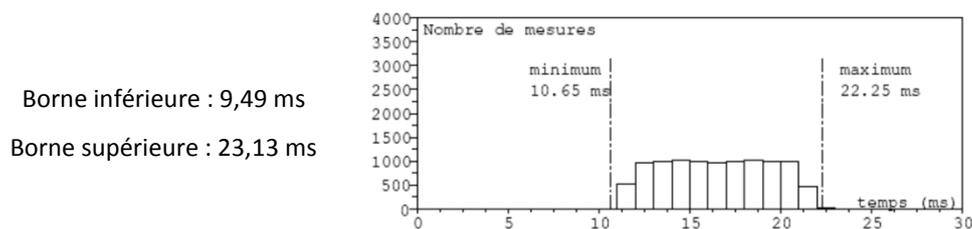


Figure 5 Résultats théoriques obtenus par preuves itératives et Résultats expérimentaux

2.2.3. Commentaires

Les résultats de ces travaux complètent utilement ceux obtenus antérieurement à partir de techniques de simulation en permettant de déterminer, en sus de la distribution d'une performance temporelle, des valeurs réalistes de ses bornes.

2.2.4. Références externes au LURPA ou antérieures à 2008

H. Bauer, J.-L. Scharbag and C. Fraboul. Improving the worst-case delay analysis of an AFDX network using an optimized trajectory approach. *IEEE Transactions on Industrial Informatics*, 6(4), 2010, pp. 521–533.

R. L. Cruz. A calculus for network delay. *IEEE Transactions on Information Theory*, 37, January 1991.

J.P. Georges. Systèmes contrôlés en réseau : Evaluation de performances d'architectures Ethernet commuté. Thèse de l'Université Henri Poincaré Nancy 1, novembre 2005.

G. Marsal. Evaluation of time performances of Ethernet-based automation systems by simulation of high-level Petri nets. Thèse de l'ENS Cachan et de l'Université de Kaiserslautern (Germany), December 2006.

P. Meunier. Evaluation de performances d'architectures de commande de systèmes automatisés industriels. PhD thesis, Thèse de l'ENS Cachan, mars 2006.

2.3. Modélisation réaliste et multi-échelles des systèmes bouclés temporisés

De nombreux résultats théoriques ont été obtenus dans le domaine de la vérification de propriétés quantitatives de modèles temporisés depuis une quinzaine d'années. Ces résultats sont cependant peu ou pas utilisés dans l'industrie. Ceci provient selon nous de deux problèmes :

- Des difficultés à mettre en œuvre la méthode d'analyse. L'écriture de propriétés formelles est en effet une tâche très difficile pour l'ingénieur automaticien et nécessite l'introduction de mécanismes adaptés (Campos, 2009). De plus, l'analyse de résultats, en particulier en cas de preuve négative, requiert beaucoup de compétences et de temps.
- Des difficultés à construire des modèles formels qui soient tout à la fois réalistes, c.à.d. ne contenant que des états et des évolutions trouvant leurs correspondances dans le système réel, et traitables par les méthodes d'analyse existantes, sans explosion combinatoire. On peut à ce niveau remarquer que la quasi-totalité des propositions de modèles issus de la communauté de l'informatique théorique considère un système isolé, plongé dans un environnement générateur d'événements ou de variables, mais jamais un **système bouclé Procédé/Contrôleur** qui est pourtant le modèle de base de l'automaticien.

Les travaux décrits ci-après visent à contribuer à la résolution du second problème, ce verrou nous paraissant devant obligatoirement être levé pour une meilleure diffusion des techniques de vérification de propriétés quantitatives. On pourra d'ailleurs remarquer que le développement de méthodes de construction de modèles réalistes et analysables dans des temps réalistes n'est pas un thème propre à l'automatique des systèmes discrets mais se retrouve dans toutes les sciences de l'ingénieur.

2.3.1. Objectifs des travaux

La thèse de Matthieu Perin [TH 9], réalisée dans le cadre d'une [convention CIFRE avec la société Dassault Systèmes](#) et soutenue en juin 2012, avait pour objectif de proposer une méthode de modélisation d'un système de production manufacturier, système bouclé composé d'un contrôleur interagissant avec un procédé, sous la forme d'un modèle temporisé réaliste et multi-échelles. Ce travail se différencie de ceux présentés dans (Machado, 2006), (Philippot, 2009), (Rohée, 2009) qui se limitent à des modèles non temporisés et ne permettent donc pas la vérification de propriétés quantitatives. De plus, l'aspect multi-échelles a été introduit afin d'améliorer les possibilités de passage à l'échelle. La vérification de propriétés quantitatives sur un modèle complexe est en effet facilitée si tout ou partie du système est modélisé avec un niveau de granularité plus grossier ; cependant, cette approche suppose que les comportements des modèles détaillés et abstraits sont équivalents pour la propriété à vérifier, ce qui doit bien entendu avoir été prouvé auparavant.

2.3.2. Principaux résultats obtenus

La première contribution issue de cette recherche [ACL 15] est une méthode de construction d'un modèle temporisé représentant un système de production et composé d'un modèle de contrôleur communiquant avec un modèle de procédé. Le formalisme retenu pour la modélisation est celui des Automates Temporisés à Variables Discrètes (ATVD) proposé par (Janowska, 2006). Ce formalisme propose des mécanismes de modélisation de l'urgence qui sont bien adaptés au

problème considéré ; nous avons de plus montré que tout modèle en ATVD pouvait être transformé, sans perte de sémantique, en un modèle analysable par l'outil UPPAAL.

Le modèle de procédé est construit par instanciation de modèles génériques de composants. Cette approche correspond bien à une démarche industrielle de conception par assemblage de composants sur étagère mais peut introduire des évolutions irréalistes ; l'introduction de mécanismes d'urgence adéquats dans le modèle global du procédé permet de supprimer ces évolutions [CAI 14]. Des mécanismes de blocage (deadlocks) étant apparus lors du couplage entre le modèle de procédé et celui du contrôleur, déduit directement d'une spécification Grafcet, nous avons ensuite proposé [CAI 45] un nouveau modèle de contrôleur garantissant les propriétés de stabilité et de réactivité de la commande tout en supprimant ces blocages. L'ensemble des états et des évolutions du modèle du système bouclé est représentatif de comportements pouvant être observés en réalité.

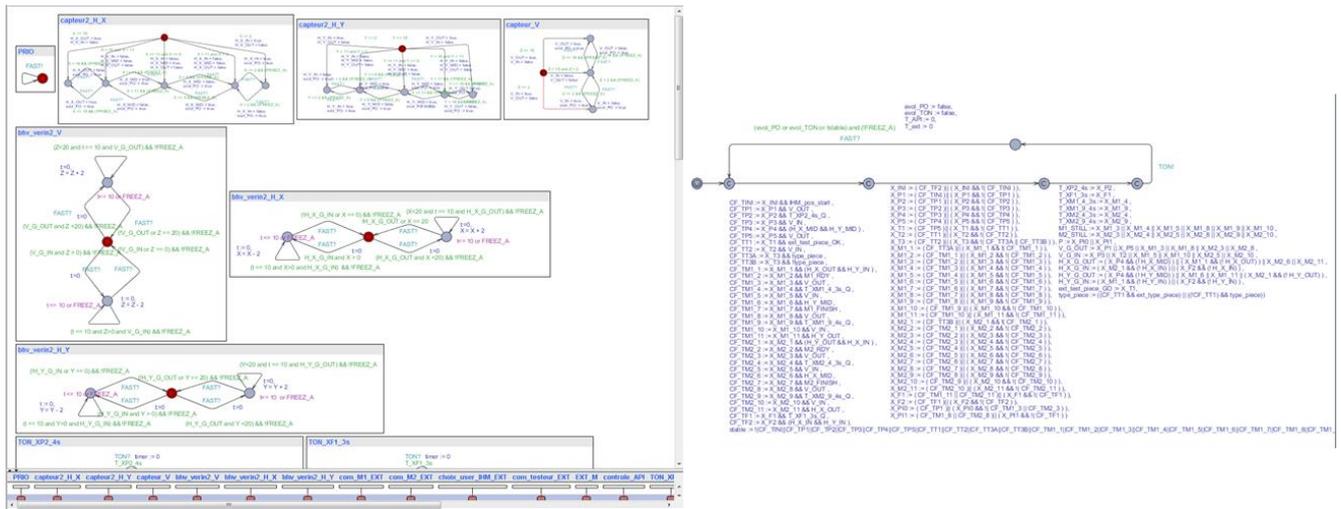


Figure 6 Modèle du système bouclé

Le deuxième résultat majeur de ces recherches concerne la modélisation multi-échelles d'un même système, afin d'améliorer les possibilités de passage à l'échelle. La construction automatique du modèle abstrait à partir du modèle détaillé paraissant très difficile en raison des nombreuses possibilités d'évolutions concurrentes dans ce dernier modèle, nous avons opté pour une approche de preuve d'équivalence entre deux modèles de granularité différente et conçus avec des points de vue différents (par exemple le point de vue de l'automaticien et celui du logisticien).

Modèle détaillé du préhenseur

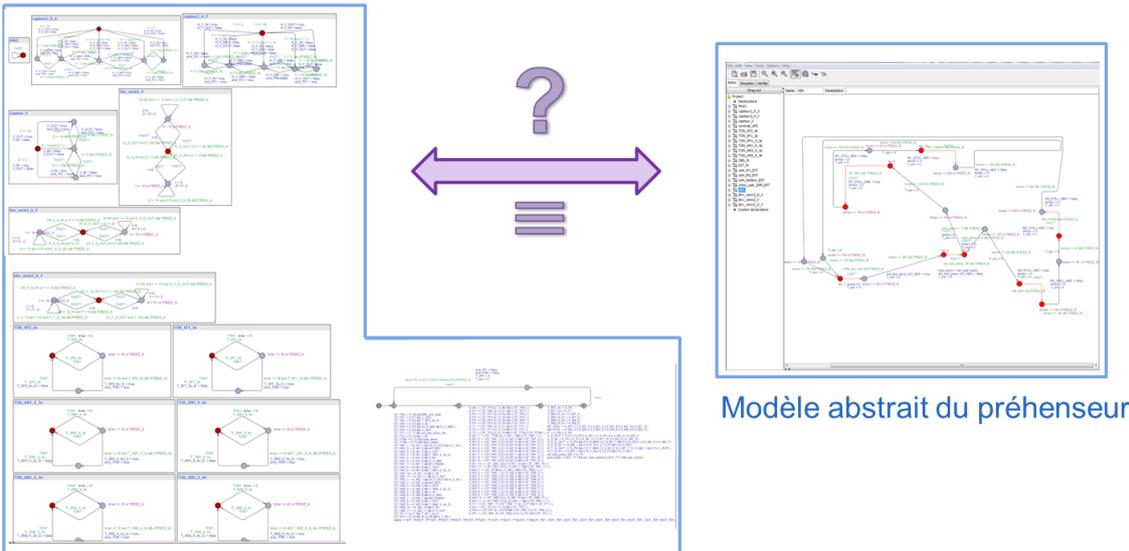
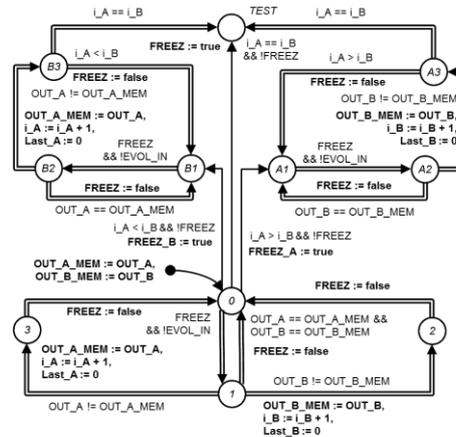


Figure 7 Modèle du système bouclé

Une relation d'équivalence en trace (Rabinovich, 1997) entre modèles en ATVD a donc été définie, sous la forme d'une expression en logique CTL* ; cette relation porte sur les seuls comportements observables communs aux deux modèles,

les évolutions internes étant forcément différentes. L'équivalence stricte, tant en valeur qu'en temps, étant en pratique peu fréquente et donc difficile à prouver, nous avons ensuite introduit une relation d'équivalence avec tolérances sur les valeurs et les dates. Ces deux relations ont pu être prouvées en introduisant un automate observateur qui assure également la cohérence entre les observations.



$E \leftrightarrow (AOS.TEST \ \&\& \ (OUT_A \neq OUT_B \ || \ Last_A \neq Last_B))$

Figure 8 Automate observateur et propriété d'équivalence en trace

2.3.3. Commentaires

Nous pensons que les résultats de ces travaux constituent des contributions solides permettant de rendre les techniques de vérification formelle plus accessibles à l'ingénieur automatique. Il n'en demeure pas moins vrai que d'autres contributions visant à éliminer (réduire) les problèmes d'écriture de propriétés et d'analyse des résultats doivent être proposées pour que ces techniques soient réellement répandues.

2.3.4. Références externes au LURPA ou antérieures à 2008

J. C. Campos, J. Machado. Pattern-based analysis of automated production systems. INCOM 2009.

A. Janowska, P. Janowski. Slicing of timed automata with discrete data. Fundamenta Informaticae, 72(1-3), pp. 181-195, 2006.

J. Machado. Influence de la prise en compte d'un modèle de processus en vérification formelle des Systèmes à Evénements Discrets. Thèse de doctorat de l'École Normale Supérieure de Cachan et de l'Université du Minho (Portugal), 2006.

A. Philippot, M. Sayed Mouchaweh et V. Carré-Ménétrier. Modelling of a discrete manufacturing system by parts of plant. INCOM 2009.

A. Rabinovich. Complexity of equivalence problems for concurrent systems of finite agents. Information and computation (139), pp.111-129, 1997.

B. Rohée, B. Riera, V. Carré-Ménétrier et J.-M. Roussel. A methodology to design and check a plant model. DESDes'06, pp. 246-250, 2006.

3. Thématique « Approches algébriques pour la synthèse et l'analyse formelles »

L'Équipe ISA a développé depuis plus de 15 ans des compétences réelles en matière de modélisation algébrique des SED. Il s'agit, aujourd'hui, d'une des spécificités de l'Équipe qui est appliquée à deux des problématiques générales classiques de l'Automatique des SED : l'Analyse, et la Synthèse de modèles.

3.1. Approches algébriques pour la synthèse formelle des contrôleurs logiques

La conception du programme de contrôle-commande d'une installation automatisée est une tâche difficile qui repose encore aujourd'hui le plus souvent sur la seule expertise des équipes de conception. Depuis toujours, le monde industriel a cherché à fiabiliser son processus de conception de programme de contrôle-commande. Pour limiter les effets désastreux des erreurs de programmation, certaines sociétés se sont dotées de méthodologies très strictes pour le développement de leurs installations. On peut à ce titre citer par exemple les recommandations CNOMO¹ définies les constructeurs automobiles français.

Pour les systèmes critiques, les normes actuelles, comme la norme *IEC 61308 : Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*, recommandent l'utilisation de méthodes formelles. Ces techniques ont cependant du mal à pénétrer le secteur industriel, en raison de la forte expertise qu'elles demandent. Elles se limitent principalement aux techniques de vérification de modèles et abordent très peu les méthodes de synthèse.

Dans le cadre de l'automatique des SED, la recherche académique explore, depuis plus de 25 ans la *Supervisory Control Theory* (Ramadge, 1989) proposée par Ramadge and Wonham en 1989 afin de disposer d'un cadre formel pour la synthèse de modèles SED. Si les résultats théoriques obtenus sont remarquables, il convient de souligner que le transfert vers le monde industriel est limité, voir expérimental seulement.

Nos propres expérimentations de cette théorie [CAI 2] ont montré que cette approche s'appliquait très difficilement au cas du contrôle-commande d'équipements industriels de bas niveau (vérins, moteurs, ...) en raison de la nécessité :

- de manipuler les signaux échangés entre contrôleur et processus et non des événements théoriques dénués de sens physique,
- d'intégrer les algorithmes de traitement des contrôleurs industriels (Automates Programmables Industriels (API),...) et leur incidence sur le traitement des informations échangées avec le procédé, ...
- de l'extrême difficulté d'établir un modèle du procédé représentatif du système à contrôler.

Contrairement à la SCT qui propose un cadre générique pour les SED, les travaux du LURPA ont été spécifiquement développés pour la synthèse de la commande des systèmes logiques (entrées et sorties à valeurs booléennes) composés d'équipements industriels de bas niveau (vérins, moteurs, ...).

3.1.1. Objectifs des travaux

L'objectif des travaux est d'obtenir le programme de contrôle-commande à implanter dans un contrôleur industriel à partir de ses spécifications formalisées de manière algébrique (figure 9).

Nous nous sommes principalement intéressés aux systèmes de contrôle-commande de systèmes du domaine de la production manufacturière. L'état de ces systèmes physiques peut être partiellement reconstruit à partir des informations fournies par les détecteurs présents sur le système. En s'appuyant sur la connaissance de l'état de la partie opérative et de l'état des produits manipulés, le fonctionnement global de ces systèmes peut être obtenu à partir d'une commande locale, parfois élémentaire, de chaque actionneur qui le compose. Il s'agit d'ailleurs d'une des recommandations CNOMO.

Pour les applicatifs étudiés, ces spécifications s'expriment principalement :

- des attentes fonctionnelles relatives à la commande du système, comme la séquence des opérations à réaliser,
- des règles de sécurité liées aux modes de marche,
- des règles de sécurité ou de programmation liées à la technologie des composants commandés,
- des règles de sécurité liées aux positionnements des composants commandés.

D'une manière générale, la spécification d'un système est le plus souvent composée de fragments de spécification représentant des exigences attendues pour le système. Ces fragments sont le plus souvent donnés dans des formalismes différents de manière formelle ou informelle. Pour certains projets, les concepteurs peuvent par ailleurs disposer d'une

¹ Des informations complémentaires sont disponibles sur : <http://www.cnomo.org/>

solution générique de tout ou partie de la loi de commande à implanter. Ce sont ces types de données que notre méthode accepte en entrée.

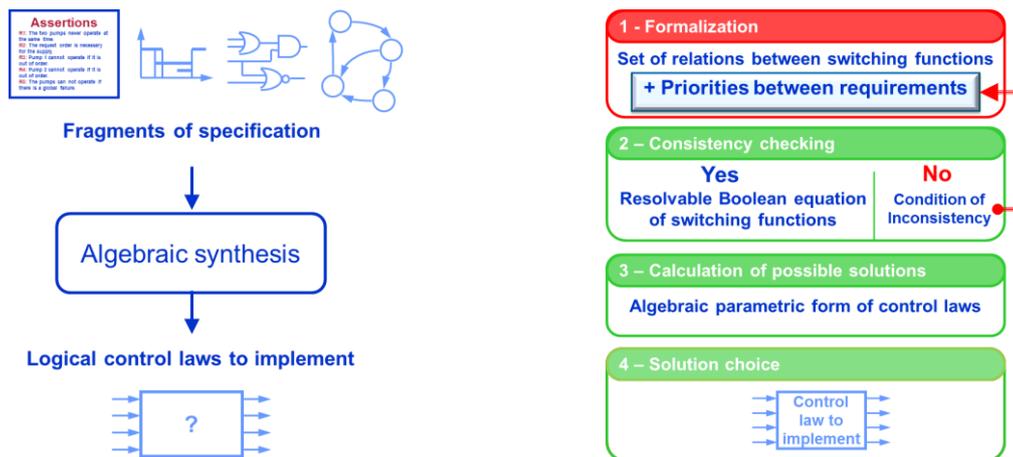


Figure 9 Synthèse formelle d'un contrôleur logique : Données d'entrées et étapes de la méthode

Sur le plan mathématique, nous avons retenu de ne manipuler que des fonctions booléennes (Switching functions) d'une dimension n donnée. Ces fonctions booléennes sont donc de la forme :

$$f : B^n \rightarrow B \text{ avec } B = \{b0, b1\}$$

La figure 10 présente le modèle que nous avons retenu pour exprimer la commande d'un système logique comportant p entrées logiques u_i , q sorties logiques y_j , et r variables internes logiques x_l . Ces variables internes sont introduites afin d'exprimer le comportement séquentiel du système. Le temps est considéré comme discret : $[k]$ représente l'instant présent et $[k - 1]$ l'instant précédent. Dans cette modélisation, le comportement est décrit par la définition de $(q + r)$ fonctions booléennes de $(p + q)$ variables.

Cette description compacte, est cependant très expressive puisque le modèle décrit figure 10 admet 2^p combinaisons différentes des variables d'entrée, peut émettre jusqu'à 2^q combinaisons différentes des variables de sortie et permet de modéliser $(2^{2^{(p+r)}})^{(q+r)}$ comportements différents.

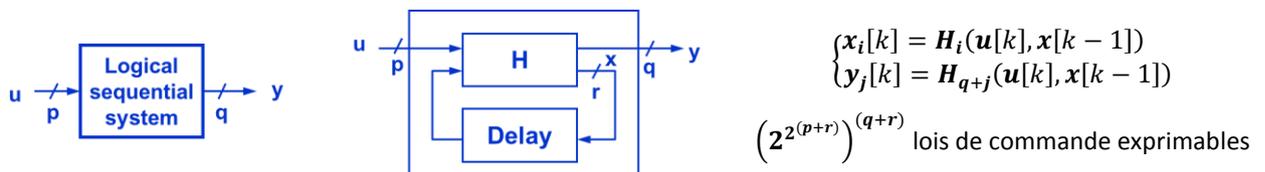


Figure 10 Modèle retenu pour la loi de commande d'un système logique

Proposé initialement par D.-A. Huffman en 1954 (Huffman, 1954), ce modèle a été rapidement supplanté par les modèles de Moore ou de Mealy car il est extrêmement difficile à élaborer sans erreur de manière manuelle dès que le nombre des variables augmente de manière significative. Cependant, grâce aux récents résultats mathématiques obtenus sur les algèbres de Boole (Rudeanu, 2001), (Brown, 2003), la synthèse automatique de fonctions booléennes par résolution d'un système d'équations est maintenant possible.

3.1.2. Principaux résultats obtenus

Nous sommes aujourd'hui en mesure **d'obtenir automatiquement la loi de commande d'un système logique à partir de ses spécifications formalisées de manière algébrique** sous forme de relations entre des compositions booléennes de fonctions booléennes.

Dans [TH 3], nous avons montré comment la recherche d'une loi de commande pour un système logique séquentiel pouvait se ramener à la résolution d'un système d'équations dans l'algèbre de Boole des fonctions booléennes quelques soient le nombre d'inconnues, la forme des équations et leur nombre. Les principaux résultats sont les suivants :

- Grâce à la relation d'ordre partiel qui existe dans cette algèbre, nous avons montré qu'il est possible d'exprimer formellement des conditions nécessaires ou suffisantes entre des combinaisons de ces fonctions. C'est cette caractéristique qui permet de formaliser simplement les attentes exprimées dans un cahier des charges.
- En nous appuyant sur les travaux de Rudeanu (2001) et Brown (2003), nous avons établi à quelle condition un système d'équations dans l'algèbre de Boole des fonctions booléennes admettait des solutions. Cette condition correspond au produit des discriminants de la forme canonique de l'équation équivalente au système initial.
- Nous avons également établi une forme paramétrée de l'ensemble des solutions lorsque ces solutions existent. À notre connaissance, la recherche de cette forme paramétrée n'avait pas été étudiée auparavant.

Les derniers développements mathématiques ont été obtenus afin de faciliter le travail de formalisation des exigences attendues pour la commande :

- Il est maintenant possible d'obtenir les solutions qui satisfont des critères d'optimisation donnés : [M 12] [CAI 44]. Grâce à la relation d'ordre partiel qui existe dans une algèbre de Boole, il est en effet possible de comparer les solutions existantes et de choisir une solution optimale lorsque celle-ci existe.
- Lorsque les spécifications sont incohérentes entre-elles, il nous est maintenant possible de les hiérarchiser afin de tenir compte de leur priorités relatives pour l'établissement de la loi de commande [CAI 46]. Lorsqu'une incohérence est détectée entre plusieurs spécifications, la spécification la moins prioritaire est automatiquement reformulée afin d'éliminer les cas de conflit. Pour illustrer notre propos, considérons 2 ensembles A et B donnés et pour lesquels il est recherché un ensemble X qui doit satisfaire à la fois les spécifications R1: $A \subset X$ et R2: $(B \cap X) = \emptyset$. Lorsque A et B sont quelconques, ce système n'admet pas de solutions. En supposant maintenant que R1 est plus prioritaire que R2 ($R1 \gg R2$), il existe différentes solutions pour X qui peuvent s'obtenir après reformulation de la spécification R2.

$$\left\{ \begin{array}{l} R1: A \subset X \\ R2: (B \cap X) = \emptyset \\ \text{Priority rules:} \\ R1 \gg R2 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} R1: A \subset X \\ R2: (B \cap X) \subset \underbrace{(A \cap B)}_{\text{ic}} \end{array} \right.$$

Afin de simplifier la lecture des modèles ainsi établis, nous avons également développé un module permettant de les représenter automatiquement sous forme d'un automate à états [M 11] [CAN 17].

3.1.3. Commentaires

Nous disposons aujourd'hui d'un outil logiciel BESS (Boolean Equations System Solver), développé en Python, permettant d'assister le concepteur pour cette activité de synthèse. Tous les calculs symboliques nécessaires à cette approche sont réalisés automatiquement.

Différentes études de cas traitées avec cet outil ont été conduites et le résultat de la synthèse expérimentée dans un équipement industriel lorsque cela nous a été possible. Le détail de ces expérimentations est disponible depuis le site WWW du laboratoire à l'adresse : <http://www.lurpa.ens-cachan.fr/-171294.kjsp>

Pour des raisons d'efficacité, il nous a fallu développer notre propre module de calcul symbolique d'expressions booléennes en raison du grand nombre de calculs symboliques à effectuer. Ce module est basé sur un codage BDD des expressions et intègre également des manipulations ensemblistes de BDD afin de limiter les calculs à effectuer.

3.1.4. Références externes au LURPA

- Brown, F.M. (2003). Boolean Reasoning: The Logic of Boolean Equations. Dover Publications.
- Huffman, D.A. (1954). The synthesis of sequential switching circuits. J. of the Franklin Institute, 257(3-4), pp. 161-190 and pp. 275-303.
- Rudeanu, S. (2001). Lattice Functions and Equations (Discrete Mathematics and Theoretical Computer Science). Springer.
- Ramadge, P.J.G. and Wonham, W.M. (1989). The control of discrete event systems. Proceedings of the IEEE Transactions on Automatic Control, 77(1), ppp. 81-98.

3.2. Évaluation de performance par algèbre (Max, +)

Les architectures d'automatisation distribuées sur des réseaux offrent un ensemble de services très diversifié pour les industriels. Cependant, ce type de systèmes de commande introduit des phénomènes de partage de ressources et d'asynchronisme entre les composants nécessaires à la communication des informations. Ces situations génèrent des retards, qui peuvent être considérables, entre l'occurrence d'un événement généré par un contrôleur et celle de sa conséquence sur le processus physique (ou vice versa), ce qui affecte le bon fonctionnement du système automatisé. Ce problème est amplifié avec les nouvelles technologies comme pour les réseaux Ethernet qui ne sont à la base pas conçus pour garantir des performances temporelles et qui pourtant deviennent incontournables dans les systèmes critiques (transport ou énergie par exemple). L'évaluation a priori des performances temporelles, avant la mise en service de ces systèmes de commande, est donc nécessaire.

3.2.1. Objectifs des travaux

Dans ces travaux, on s'intéresse plus particulièrement à la détermination des délais d'acheminement des événements au travers ces systèmes et au calcul des bornes minimale et maximale de la réactivité de ces architectures de commande distribuées sur des réseaux. L'enjeu est d'apporter des méthodes formelles et des moyens d'analyse pour garantir des temps de réaction (ou temps de réponse D_r) du système pour chaque occurrence d'événement critique qui se produit pendant le fonctionnement. Les systèmes de commande en réseau (SCR) qui nous concernent fonctionnent suivant le protocole client/serveur où le contrôleur (PLC : Programmable Logic Controller) est le client et les modules d'entrées/sorties (RIOMs : remote input output modules) sont les serveurs. Le PLC retenu dispose de deux modules, le CPU pour le traitement des programmes et le coupleur réseau Ethernet ETHb (carte de communication) pour l'envoi des requêtes et la scrutation des RIOMs. Ces deux modules fonctionnent de manière cyclique mais asynchrone, ce qui rend l'évaluation des performances difficile et pose un problème quant aux valeurs des périodes du CPU et l'ETHb à fixer pour atteindre un niveau de performance désiré. Le processeur de traitement exécute périodiquement les tâches : lecture, traitement et écriture avec comme seule contrainte temporelle, la période de cycle à ne pas dépasser. Le coupleur réseau ETHb de son côté, et de manière complètement asynchrone, copie puis envoie des requêtes aux RIOMs et attend que les réponses reviennent. Si avant de terminer le temps de cycle toutes les réponses sont arrivées, il se met en attente ou sinon il recommence directement un nouveau cycle de scrutation.

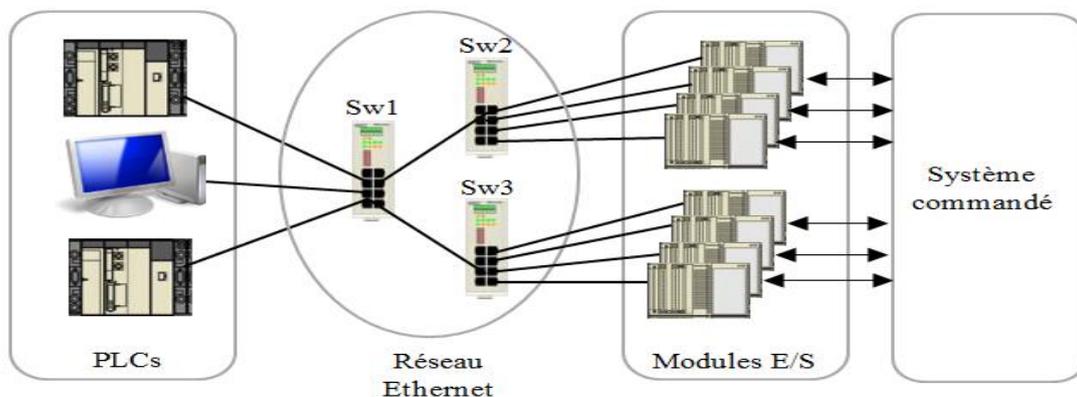


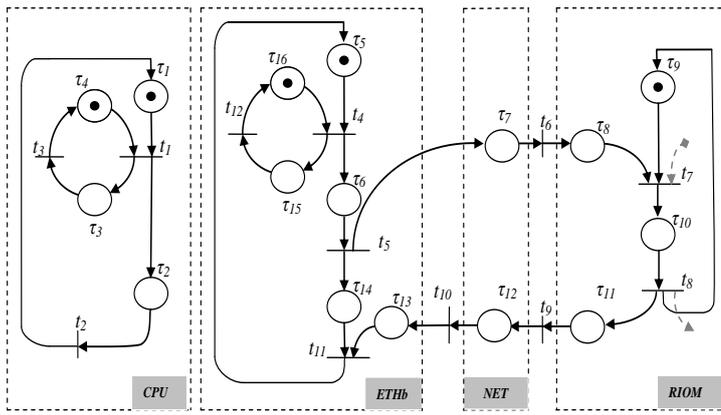
Figure 11 Système de Commande en Réseau (SCR)

Pour mieux aborder le problème de détermination des bornes du temps de réactivité, nous considérons le cas relativement simple d'un SCR avec seul PLC et un seul module RIOM puis on étend l'étude pour des architectures de commande plus générale. Dans les travaux de la thèse de B. Addad [TH 7], nous avons proposé une méthode de calcul des bornes et de la distribution du temps de réponse des architectures d'automatisation en réseaux client/serveur en utilisant les graphes d'événements temporisés (GET) et le formalisme de l'algèbre (Max, +).

3.2.2. Principaux résultats obtenus

Notre contribution dans ces travaux est de proposer une nouvelle approche analytique à base du formalisme de l'algèbre (Max,+) afin de remédier aux problèmes des méthodes existantes comme l'explosion combinatoire de la vérification formelle ou la non exhaustivité des scénarios envisagés par simulation. Notre démarche débute par une modélisation des composants du SCR client/serveur à l'aide des Graphes d'Événements Temporisés (Murata, 1989) puis une représentation par des équations (Max, +) linéaires de leur dynamique (Bacelli et al, 1992). Après résolution de ce système

d'équations linéaires, nous obtenons des formules de calcul direct des bornes et la forme de la distribution du temps de réponse [ACL 3].



Modèles Graphes d'événements temporisés du SCR

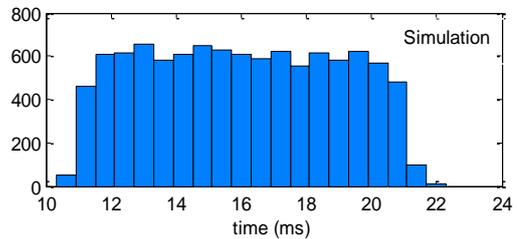
$$\begin{cases} \theta_1(k) = (\theta_2(k-1) \otimes \tau_1) \oplus (\theta_3(k-1) \otimes \tau_4) \\ \theta_2(k) = \theta_1(k) \otimes \tau_2 \\ \theta_3(k) = \theta_1(k) \otimes \tau_3 \end{cases}$$

$$\begin{cases} \theta_4(l) = (\theta_{11}(l-1) \otimes \tau_5) \oplus (\theta_{12}(l-1) \otimes \tau_{16}) \\ \theta_5(l) = \theta_4(l) \otimes \tau_6 \\ \theta_6(l) = \theta_5(l) \otimes \tau_7 \\ \theta_7(l) = (\theta_6(l) \otimes \tau_8) \oplus (\theta_8(l-1) \otimes \tau_9) \\ \theta_8(l) = \theta_7(l) \otimes \tau_{10} \\ \theta_9(l) = \theta_8(l) \otimes \tau_{11} \\ \theta_{10}(l) = \theta_9(l) \otimes \tau_{11} \\ \theta_{11}(l) = (\theta_5(l) \otimes \tau_{14}) \oplus (\theta_{10}(l) \otimes \tau_{13}) \\ \theta_{12}(l) = \theta_4(l) \otimes \tau_{15} \end{cases}$$

Equations (Max, +) linéaires de la dynamique

$$\begin{cases} D_{MIN} = q \cdot T_{SCR} + T_{NETf} - T_{NETb} + T_{I/O} + d_f \\ D_{MAX} = (q+1) \cdot T_{SCR} + T_{NETf} - T_{NETb} + T_{I/O} + d_f \\ D_r(p) = \theta_8(l+q) - v(p) \end{cases}$$

Formules de calcul du temps de réponse



Histogramme du temps de réponse

Figure 12 Démarche d'évaluation du temps dans un système de commande en réseau

À la suite de cette approche déterministe pour calculer les bornes, minimale et maximale, du temps de réponse, nous avons introduit une analyse stochastique et obtenu une formule de calcul direct de la fonction de densité de probabilité du temps de réponse [ACL 7].

De plus, nous prenons en compte dans nos travaux tous les délais élémentaires qui composent le temps de réponse, y compris les délais de bout-en-bout, dus à la traversée du seul réseau de communication. Ce dernier étant naturellement composé de ressources partagées, rendant l'utilisation des modèles (Max,+) classiques impossibles, nous introduisons une nouvelle approche de modélisation à base du formalisme (Max,+) mais prenant en compte le concept de conflit ou ressource partagée. L'exemple d'un réseau de type Ethernet est considéré pour évaluer ces délais de bout-en-bout [ALC 8]. Pour ce faire, nous avons étudié une classe des réseaux de Petri, les RGETC (Réseaux de Graphes d'Événements Temporisés avec Conflits), et avons réussi à les représenter grâce à des modèles (Max,+), assez similaires aux modèles classiques. L'avantage majeur des RGETC est qu'ils sont adéquats pour l'étude des réseaux de communication mais qu'ils permettent également d'appréhender de nombreux systèmes (production, transport, etc) comme nous l'avons montré sur différents exemples pratiques [ACL 14].

Enfin, pour vérifier la validité des résultats obtenus des travaux, notamment la formule de la borne maximale du temps de réponse, une campagne de mesures expérimentales a été menée sur la plateforme expérimentale de l'équipe ISA. Différentes configurations et conditions de trafic dans un réseau Ethernet ont été considérées [CAI 34].

Pour ces travaux, Boussad Addad a obtenu un prix :

- Prix 2011-2012 des meilleures thèses en automatique du GDR MACS et de la section automatique du Club EEA, dans la catégorie « Systèmes à Événements Discrets et Systèmes hybrides ».

3.2.3. Commentaires

Les systèmes de commande en réseau traités dans nos travaux fonctionnent suivant le protocole Client/serveur. Il serait intéressant de se pencher sur les possibilités d'étendre les résultats à des SCR fonctionnant suivant d'autres protocoles comme Producteur/consommateur. Sans trop de difficultés, nous pensons que cela devrait être réalisable, puisque les modèles des composants ne devraient pas être trop affectés et que la difficulté liée à la non synchronisation entre les PLCs et les modules E/S n'est pas présente dans le cas du protocole Producteur/consommateur. Concernant le réseau de

communication, nous nous sommes penchés sur Ethernet commuté standard. Il serait également utile de considérer par exemple la classification de service, implémentée de plus en plus dans les commutateurs afin d'améliorer les performances des applications temps-réel. Il est vrai que cela pourrait se révéler difficile puisque le principe même de la méthode proposée dans [ACL 8] pour l'évaluation des délais de bout-en-bout est basé sur la politique FIFO (Bauer et al, 2010), (Cruz, 1991). Dans un contexte plus général de recherche fondamentale, l'extension de la représentation des systèmes à événements discrets impliquant des ressources partagées à l'aide d'équations $(\max,+)$, nous semble une perspective intéressante. En effet, plusieurs hypothèses plus au moins fortes ont été posées. Par exemple, la capacité à relaxer l'hypothèse que certains circuits dans les GETC sont saufs nous permettrait d'envisager d'appréhender des systèmes qui comportent des ressources multiserveurs. Par ailleurs, la généralisation de la notion de séquence d'évolution d'un GETC cyclique, commune à toutes les ressources partagées, à une séquence propre à chaque ressource paraît aussi une bonne piste à explorer.

3.2.4. Références externes au LURPA

F. Baccelli, G. Cohen, G.-J. Olsder, and J.-P. Quadrat (1992). *Synchronization and Linearity: An Algebra for Discrete Event Systems*. New York: Wiley.

H. Bauer, J.-L. Scharbarg, and C. Fraboul, (2010). Improving the Worst-Case Delay Analysis of an AFDX Network Using an Optimized Trajectory Approach, *IEEE Trans. on Industrial Informatics*, vol. 6(4), pp. 521-533.

R. L. Cruz (1991). A calculus for network delay, Part I: Network in isolation, *IEEE Trans. Inf. Theory*, vol. 37(1), pp. 114–131.

T. Murata (1989), Petri nets properties analysis and applications, *Proc. IEEE*, vol. 77, no. 4, pp. 541–580.

4. Thématique « Identification des SED »

L'identification consiste à rechercher un modèle mathématique d'un système dynamique à partir de données expérimentales et de connaissances disponibles a priori. Dans le cas des Systèmes à Événements Discrets (SED), les modèles recherchés sont des machines à états (Automates Finis (AF), Réseaux de Petri (RdP),...). On parle d'identification *boîte noire* lorsque l'on ne dispose d'aucune connaissance a priori concernant le système à identifier ; l'identification est dite *passive* lorsque le processus d'identification se déroule pendant le fonctionnement normal du système, qui n'est alors soumis qu'aux sollicitations ambiantes. **Dans nos travaux, nous nous intéressons à l'identification passive et de type boîte noire des SED.**

Ce n'est que récemment que la communauté scientifique internationale s'est intéressée à la recherche d'algorithmes d'identification spécifiquement dédiés aux SED. Une revue détaillée de la littérature dans ce domaine peut être trouvée dans [ACL 2], nous en présentons ci-dessous une synthèse non exhaustive.

Plusieurs des approches proposées sont assez analogues aux techniques d'apprentissage de langages, développées dans le domaine de l'informatique depuis les années 1960 (Gold 1967). Ainsi, dans (Cabasino, 2007) et (Cabasino, 2008) on construit un RdP qui génère le même langage que celui généré par le SED identifié. Plusieurs hypothèses retenues dans ces travaux en limitent cependant fortement la praticabilité. Tout d'abord il est supposé que le langage généré par le SED est connu dans sa totalité (hypothèse qui a été invalidée dans [CAI 19]). Par ailleurs, toutes les transitions du RdP sont supposées connues, ce qui nécessite une connaissance a priori du comportement du système incompatible avec une approche d'identification de type boîte noire. Dans (Ould El Medhi, 2006) plusieurs algorithmes sont proposés pour synthétiser un RdP par propagation d'un ensemble d'événements. Aucune distinction n'étant faite entre les événements d'entrée et de sortie du SED, le RdP ainsi construit ne peut donc traduire les relations causales d'entrées-sorties qui sont le propre de tout système réactif. Une construction incrémentale d'un RdP interprété (RdPI) à partir d'une séquence observée des sorties du contrôleur est proposée dans (Meda-Campaña, 2005). Par hypothèse, cette approche n'est valide que pour les systèmes dont le comportement peut être caractérisé par la seule évolution de leurs sorties, ce qui ne correspond pas aux besoins pour l'identification des systèmes réactifs. Dans (Dotoli, 2008) et (Dotoli, 2011), un RdPI est construit de manière à reproduire une séquence d'événements et les sorties correspondantes. La relation de causalité entre la séquence d'événements et les sorties doit être déterministe. De plus, l'ensemble des événements à prendre en compte doit être connu a priori, ce qui encore une fois n'est pas compatible avec une approche d'identification de type boîte noire.

Il résulte de ce rapide état de l'art que l'identification des SED est un domaine de recherche récent dans lequel des premiers résultats théoriques prometteurs ont été obtenus. Notre objectif est de prolonger ces premiers résultats, de manière à faire de l'identification une technique expérimentale performante, offrant une réelle alternative à la modélisation par connaissance. Pour cela, les challenges à relever portent pour l'essentiel sur deux aspects :

- 1) la capacité à prendre en compte les contraintes physiques et technologiques des SED industriels. Il faut donc :
 - manipuler les signaux échangés entre contrôleur et processus et non des événements théoriques dénués de sens physique,
 - prendre en compte l'impossibilité d'observer la totalité de l'espace d'état du SED ou du langage qu'il génère en un temps fini,
 - intégrer les algorithmes de traitement des contrôleurs industriels (Automates Programmables Industriels (API),...) et leur incidence sur le traitement des informations échangées avec le procédé, ...
- 2) la proposition d'algorithmes qui permettent d'identifier des systèmes de taille réaliste (plusieurs dizaines ou centaines d'E/S) en un temps acceptable, même si les algorithmes d'identification sont classiquement exécutés hors ligne, à partir de données expérimentales acquises en temps réel.

4.1. Identification des SED par Automates finis

4.1.1. Objectifs des travaux

Nous avons abordé pour la première fois l'identification des SED par AF dans le cadre d'une thèse réalisée en co-tutelle avec le Prof. Litz de l'Université de Kaiserslautern – Allemagne (Klein, 2005a). Dans ces travaux, dont l'objectif était d'identifier un modèle sur lequel a été construite une technique de diagnostic par méthode du modèle, nous avons choisi de restituer le résultat de l'identification sous la forme d'un Automate Fini (AF). Les résultats obtenus (Klein, 2005b) ont notamment permis :

- de montrer que les algorithmes d'apprentissage des langages ne pouvaient être utilisés car ils sont basés sur des hypothèses non vérifiées par les SED automatisés industriels (non occurrence d'événements simultanés, connais-

sance - le plus souvent exhaustive - du langage généré par le système observé, connaissance de contre-exemples, ...),

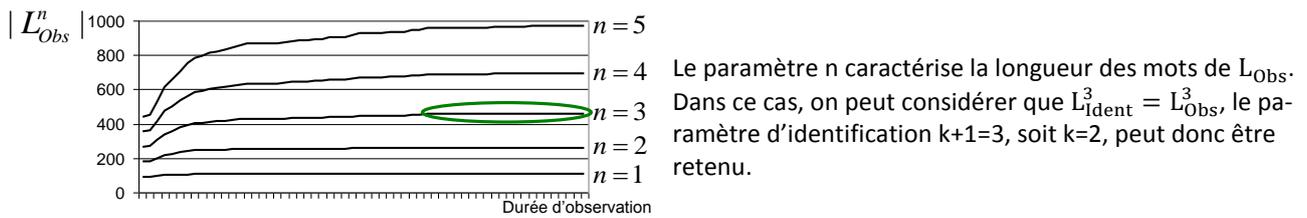


Figure 13 Allure typique de l'évolution du cardinal du langage observé (L_{Obs}) en fonction de la durée d'observation

- de proposer un algorithme d'identification performant et spécifiquement adapté aux SED réactifs, paramétré par la longueur (k) des mots du langage construit à partir des séquences d'événements observés,
- de proposer un théorème de complétude, qui établit qu'une fois un paramètre k choisi, tout langage de longueur inférieur ou égale à $k+1$ généré par l'AF identifié (L_{Ident}^n) est exactement le langage observé sur le SED (L_{Obs}^n) :

$$\forall n \leq k + 1, L_{Ident}^n = L_{Obs}^n$$

4.1.2. Principaux résultats obtenus

Dans la période de référence, cette propriété de $(k+1)$ complétude a été prolongée dans la thèse de Matthias Roth [TH 6] par la démonstration d'un second théorème, très important pour le diagnostic car il permet de prouver qu'aucune fausse alarme ne sera générée en appuyant la méthode de diagnostic sur l'AF identifié par notre approche :

$$\text{Si } L_{Orig}^{k+1} = L_{Obs}^{k+1}, \text{ alors } L_{Ident}^{k+n} \supseteq L_{Orig}^{k+n}, \forall n \geq 1$$

Ce théorème indique que si l'on peut faire l'hypothèse que tous les mots de longueur $(k+1)$ que peut générer le SED (L_{Orig}^{k+1}) ont été observés (L_{Obs}^{k+1}), le langage généré par l'AF simule le langage originel. Dans la pratique, cette hypothèse d'observation complète du langage généré pour une longueur donnée est généralement vérifiée pour les systèmes peu complexes, mais reste difficile à vérifier pour les systèmes massivement concurrents. C'est pourquoi dans cette seconde thèse réalisée en co-tutelle avec le Prof. Litz de l'Université de Kaiserslautern [TH 6] nous avons proposé une approche pour l'identification distribuée.

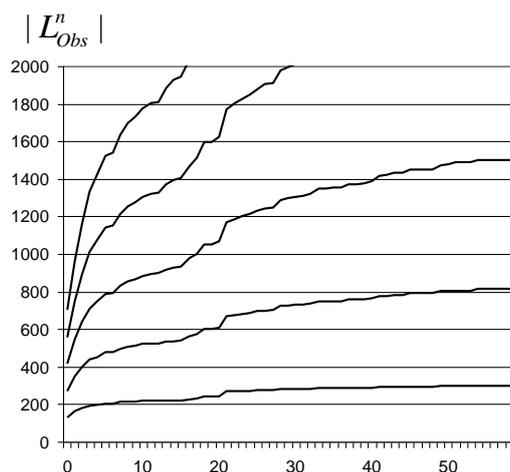


Figure 14 Allure typique de l'évolution du cardinal du langage observé pour un système fortement concurrent

Deux techniques de partitionnement d'un SED en sous-systèmes concurrents ont également été proposées : l'une, experte, est basée sur des heuristiques ; l'autre, automatique, est basée sur l'algorithme du recuit simulé [CAI 20]. Dans ces deux thèses, l'AF obtenu par identification constitue le modèle exempt de faute sur lequel est basée une approche de diagnostic centralisé [ACL 10] ou distribué [ACL 13].

Dans les deux cas (centralisé ou décentralisé), une approche originale a été retenue pour le diagnostic. Elle est basée sur l'utilisation de « résidus » qui, à l'instar des systèmes continus représente l'écart de comportement entre celui prévu par le modèle et celui réellement observé sur le système en exploitation .

Pour ces travaux, Matthias Roth a obtenu deux prix :

- le "Best paper Award of the track Discrete Event Systems" du 13th IFAC Symposium on Information Control Problems in Manufacturing (INCOM'09), Moscow (Russia), en Juin 2009,
- le "Best paper Award of the track Discrete Event Systems" de l'American Control Conference (ACC'10), Baltimore (USA), en Juillet 2010.

4.1.3. Commentaires

Dans ces travaux, le modèle identifié sous la forme d'un AF s'est révélé parfaitement adapté aux objectifs de diagnostic. Cependant, un AF est sémantiquement trop pauvre pour offrir à un ingénieur automatique une représentation performante et explicite des comportements d'un SED complexe, ce qui est par exemple attendu dans un contexte où l'identification est utilisée dans un objectif de réingénierie. Ainsi, les comportements parallèles du SED observé sont « mis à plat » dans l'AF identifié ou, dans l'approche distribuée proposée dans [CAI 20] ils sont répartis dans les AF associés aux différents sous-systèmes. Dans aucun cas ils ne sont mis en évidence dans le modèle identifié et ne sont rendus lisibles par un expert. Par ailleurs, il convient de souligner que seuls les SED ayant un comportement cyclique ont été considérés dans ces deux approches.

4.2. Identification des SED par Réseaux de Petri

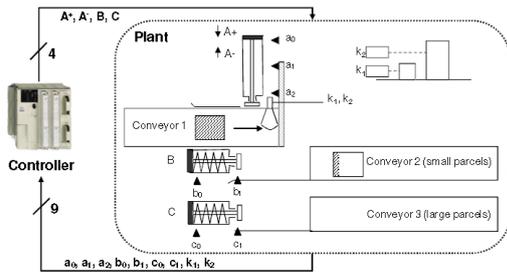
4.2.1. Objectifs des travaux

C'est pour remédier aux inconvénients mentionnés ci-dessus que l'identification des SED sous la forme de Réseaux de Petri Interprétés (RdPI) a été explorée dans le cadre d'une thèse réalisée en co-tutelle avec le Prof. E. L. Mellado du Cinvestav – Guadalajara – Mexique [TH 10]. Dans cette thèse, nous avons développé deux techniques d'identification par RdP.

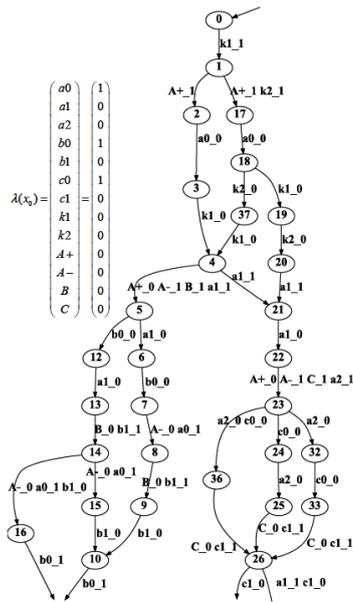
4.2.2. Principaux résultats obtenus

La première méthode [CAI 18], [CAI 27] permet de construire progressivement un modèle RPI à partir d'une seule séquence d'entrées/sorties représentant le comportement observable du SED. Cette technique paramétrique est proche de celle développée par S. Klein, mais l'hypothèse de cyclicité du SED a pu être levée [CAI 36], [ACL 16].

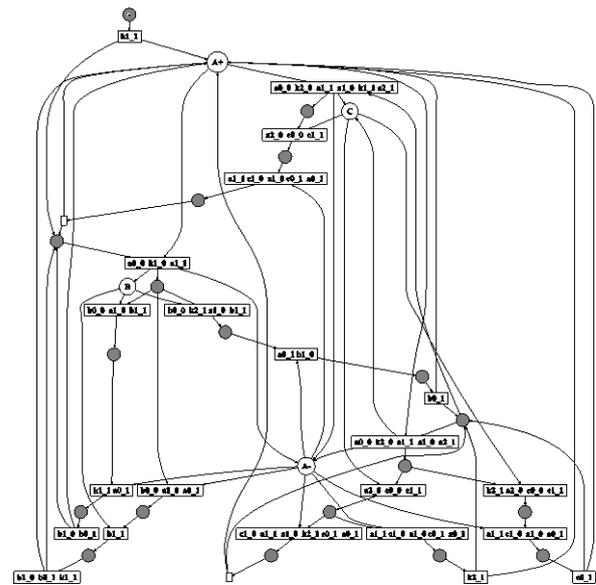
La seconde méthode, [CAI 40] [CAI 47] est basée sur une exploitation statistique des données observées qui permet la construction de modèles RPI compacts et expressifs. Elle est composée de deux étapes ; la première calcule à partir de la séquence entrée-sortie, la partie réactive observable du modèle, traduite dans le RdPI par des places et des transitions observables. La deuxième étape permet d'inférer le comportement non-observable du SED, en ajoutant au RdP obtenu à l'issue de la première étape des places non observables de manière à permettre le tir de la séquence d'entrées-sorties observée.



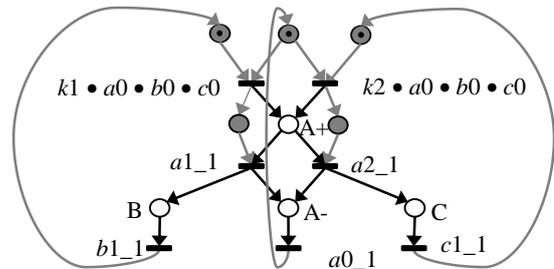
SED à Identifier (9 entrées et 4 sorties)



Automate Fini identifié avec k=2 (S. Klein)
(partiel, l'AF complet a 38 états et 44 trans



RdP identifié avec k=2
(A.-P. Vargas, 1ère méthode : constructive)



RdP identifié
(A.-P. Vargas – 2ème méthode : statistique)

Figure 15 Comparaison des résultats procurés par trois techniques d'identification sur un même exemple

Pour ces travaux, Ana Paula Estrada a obtenu un prix :

- le "Best paper Award" de la 16th IEEE Int. Conf. on Emerging Technologies and Factory Automation (ETFA'11), Toulouse (France), en Septembre 2011.

Les algorithmes proposés dans ces deux thèses sont de complexité polynomiale, [TH 6], [TH 10]. Ils ont été implémentés dans des outils expérimentaux et testés à la fois sur des cas d'école et sur des systèmes réels en fonctionnement. La figure ci-dessus donne une image des résultats obtenus sur un même cas d'étude. Elle permet d'illustrer, même sur un cas simple, la complexité de l'AF ou du RdP obtenus dans le cas d'une identification centralisée par des algorithmes paramétriques. Le RdP obtenu par approche statistique est plus compact, mieux à même de répondre aux besoins de la réingénierie.

4.2.3. Commentaires

Bien qu'opérationnelle et performante, cette dernière approche d'identification par RdPI se heurte à la difficulté de reconstituer, par inférence, les comportements concurrents non observables. C'est pourquoi nous souhaitons à court terme étudier les apports de l'identification distribuée par RdPI.

4.2.4. Références externes au LURPA ou antérieures à 2008

Cabasio M.P., Giua A., Seatzu C. (2007), Identification of Petri Nets from Knowledge of Their Language, Discrete Event Dynamic Systems, 17(4), pp. 447-474
 Cabasio M.P., Giua A., Seatzu C. (2008), Linear Programming Techniques for the Identification of Place/Transition Nets, IEEE Int. Conf. on Decision & Control, Cancun, Mexico, pp. 514-520
 David R. and Alla H. (1994), Petri Nets for Modeling of Dynamic Systems, a survey, Automatica, 30(2), pp. 175-202

- Dotoli M., Fanti M.P., Mangini A.M. (2008), Real time identification of discrete event systems using Petri nets, *Automatica*, 44(5), pp. 1209-1219
- Dotoli M., Fanti M.P., Mangini A.M., Ukovich W. (2011), "Identification of the Unobservable Behaviour of Industrial Automation Systems by Petri Nets", *Control Engineering Practice*, 19(9), pp. 958-966,
- Gold E.M. (1967), Language identification in the limit, *Information and Control*, 10(5), pp. 447-474
- Klein S. (2005a), Identification of Discrete Event Systems for Fault Detection Purposes, PhD thesis, ENS de cachan & UniV; Kaiserslautern, 150 pages
- Klein S., Litz L., Lesage J.-J. (2005b), Fault detection of Discrete Event Systems using an identification approach, 16th IFAC World Congress, 6 pages, Praha, Czech Rep.
- Meda-Campaña M., López-Mellado E. (2005), Identification of Concurrent Discrete Event Systems Using Petri Nets, IMACS'05 World Congress, Paris, France, pp.1-7
- Ould El Medhi S., Leclercq E., Lefebvre D. (2006), Petri nets design and identification for the diagnosis of discrete event systems, IAR Annual Meeting, Nancy, France

5. Thématique « Approches SED pour l'analyse de sûreté »

5.1. Formalisation des outils pour l'analyse de sûreté

L'analyse de sûreté d'un système complexe repose aujourd'hui principalement sur l'utilisation d'outils et de méthodes issues du monde industriel. Ces outils et méthodes sont variés tant sur le plan des possibilités offertes que sur les modèles mathématiques sur lesquels ils reposent.

Le groupe de travail M2OS (Management, Méthodes, Outils, Standards) de l'IMdR¹ (Institut pour la Maîtrise des Risques) propose un [recueil](#) de 30 fiches synthétiques détaillant certains outils et méthodes utilisés pour une analyse de sûreté. À la lecture de ces fiches, il apparaît clairement que l'analyse de sûreté d'un système est une activité complexe nécessitant à la fois une culture pluridisciplinaire pour intégrer les différents aspects à prendre en compte et une culture très pointue pour établir le modèle d'analyse avec le niveau de détails adéquat.

Conçus initialement pour ne prendre en compte que des comportements élémentaires, les outils utilisés en analyse de sûreté reposent généralement sur des modèles mathématiques simples. Pour répondre aux attentes pressantes des utilisateurs, de nouvelles primitives ont été progressivement introduites dans ces outils. Dans certains outils, l'ajout de ces nouvelles primitives s'est malheureusement fait sans remettre en cause le choix initial des modèles mathématiques sous-jacents. Cela a conduit à des définitions informelles de ces primitives, et pouvant remettre en cause les résultats obtenus avec ces outils de sûreté.

5.1.1. Objectifs des travaux

Les travaux menés au LURPA pour la thématique « Formalisation des outils pour l'analyse de sûreté » ont pour objectif de renforcer les fondements mathématiques sur lesquels reposent ces outils métiers afin d'en éliminer les possibilités d'incohérence et de permettre de pratiquer des analyses formelles des modèles établis par les experts.

Pour mener à bien ces travaux, l'équipe ISA utilise les compétences acquises dans le domaine des SED. Nous nous focalisons donc sur les outils d'analyse de sûreté qui font référence aux évolutions discrètes des systèmes.

Pour la période considérée, nous nous sommes principalement intéressés à :

- La modélisation algébrique des arbres de défaillance dynamiques,
- La formalisation de la cohérence et au calcul des séquences de coupe minimales pour les systèmes dynamiques réparables.

Les arbres de défaillances sont largement utilisés dans l'industrie pour conduire des études prévisionnelles de fiabilité d'un système. Ils sont établis par les experts fiabilistes pour identifier les différentes causes qui conduisent à la défaillance du système analysé. Leur construction suit un processus itératif partant de l'événement redouté placé à la racine de l'arbre. Il consiste à décomposer chaque événement étudié en événements intermédiaires jusqu'à ce que cette décomposition soit impossible ou jugée superflue. Les événements non décomposés sont les événements de base de la modélisation. Ils forment les feuilles de l'arbre de défaillances et doivent correspondre à des processus stochastiques indépendants. Une fois établis, ces arbres de défaillances sont exploités pour déterminer les conditions minimales pour que la défaillance ait lieu (étude qualitative) ou quantifier la probabilité d'occurrence de cette défaillance (étude quantitative) en fonction des événements de base.

Lorsque chaque décomposition est décrite à l'aide d'une porte OU ou d'une porte ET, l'arbre de défaillances est dit statique (ADS). La forme simplifiée de la fonction booléenne qu'il décrit est la fonction de structure de cet arbre de défaillance. Sa connaissance permet de mener efficacement les analyses qualitatives ou quantitatives à l'aide de BDD. Pour compléter le pouvoir d'expression des ADS, de nouvelles portes ont été ajoutées. Les arbres de défaillances les utilisant sont dits dynamiques (ADD) (Dugan, 1992) puisqu'il est fait non seulement référence à la présence ou non d'un événement de base mais également à l'ordre d'apparition de ces événements. La modélisation des arbres de défaillances par de simples fonctions booléennes devient impossible.

Dans bon nombre d'études prévisionnelles de sûreté, les systèmes étudiés sont considérés comme étant non réparables durant tout le temps de mission considéré. Cette hypothèse simplificatrice n'est aujourd'hui plus tolérable dans bon nombre de secteurs industriels qui, pour des raisons techniques et/ou économiques, se doivent de prendre en compte la réparabilité des composants. L'hypothèse de l'unicité de la défaillance d'un composant ne peut donc dans ce cas plus être conservée et il devient nécessaire d'utiliser de nouveaux modèles mathématiques pour formaliser les modèles de sûreté. C'est particulièrement le cas des Boolean logic Driven Markov Processes (BDMP) qu'a développé EDF

¹ <http://www.imdr.fr/>

pour la modélisation de ses équipements électriques (Boussiou, 2003). Dans ce modèle, qui a été spécifiquement développé pour la modélisation des systèmes dynamiques réparables, les événements de base sont remplacés par des processus stochastiques représentés par des chaînes de Markov. Ces processus stochastiques sont également synchronisables entre eux pour décrire les interactions entre les composants, induites par le contrôle des commutations entre équipements redondants.

5.1.2. Principaux résultats obtenus

Modélisation algébrique des arbres de défaillance dynamiques

Dans le travail de thèse de Guillaume Merle [TH 5], nous nous sommes particulièrement intéressés à la modélisation algébrique des arbres de défaillance dynamiques afin de pouvoir conduire des analyses qualitatives ou quantitatives sans nécessiter une représentation exhaustive de l'espace d'état, représentation fortement sensible à l'explosion combinatoire (figure 16).

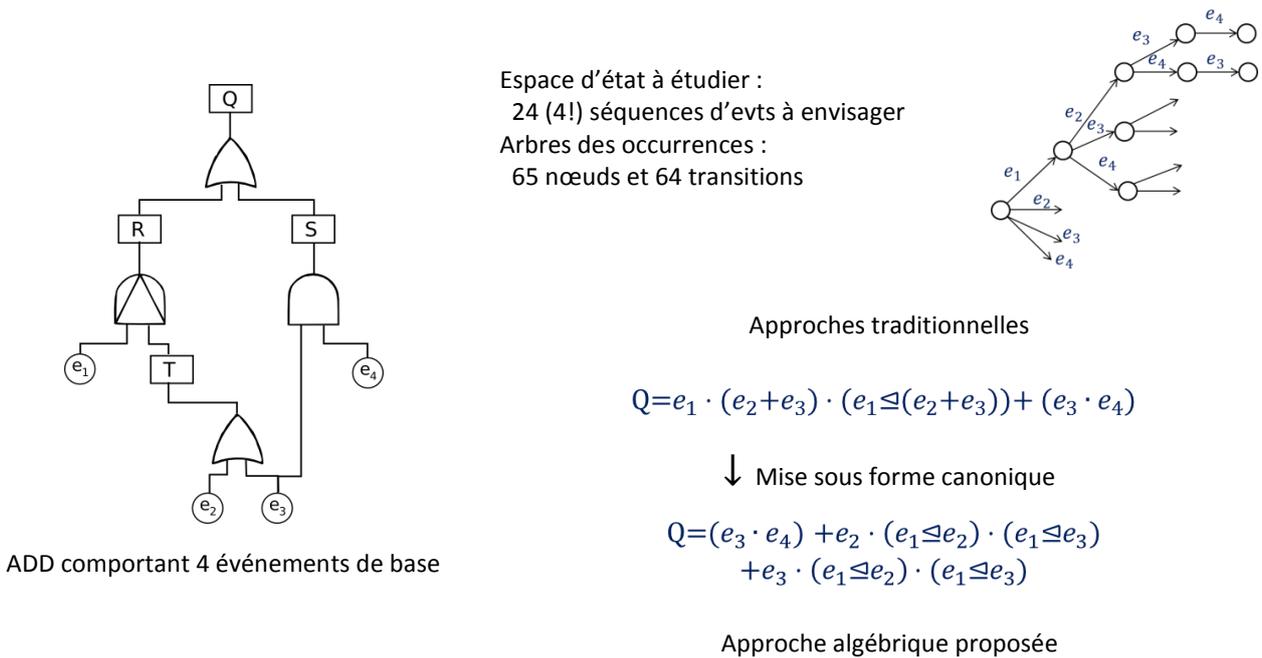


Figure 16 Modélisation d'état, vs. algébrique, d'un ADD

La contribution majeure des travaux de thèse de Guillaume Merle a été la définition d'un cadre algébrique homogène permettant d'établir la fonction de structure d'un ADD et ainsi d'étendre les méthodes analytiques utilisées pour analyser les ADS aux ADD. Ce cadre algébrique est fondé sur un modèle temporel des événements présents dans un ADD et des différentes portes qui les manipulent [CAI 11] [CAI 23] [CAI 24]. Il se compose de cinq opérateurs permettant d'associer les événements en tenant compte de la séquentialité de leur occurrence. Il est ainsi possible d'exprimer les situations temporelles suivantes :

- e_i : l'événement e_i est apparu,
- $e_i \prec e_j$: l'événement e_i est apparu strictement avant e_j
- $e_i \preceq e_j$: l'événement e_i est apparu avant ou au même instant que e_j

Grâce à ce cadre algébrique, nous avons pu, d'une part, proposer un modèle algébrique pour tous les types de portes d'un ADD, et, d'autre part établir tous les théorèmes nécessaires à la manipulation symbolique d'expressions construites à l'aide de ces opérateurs. Il nous est possible d'exprimer et simplifier la fonction de structure d'un ADD [CAI 28]. Nous avons également démontré que cette fonction de structure peut être toujours ramenée à une forme canonique, puis à une forme minimale grâce à la définition d'un critère de minimisation [ACL 1].

$$Q = \sum \left(\prod b_i \cdot \prod (b_j \prec b_k) \right), j \notin \{i, k\}$$

Cette forme canonique décrit l'ensemble des conditions suffisantes pour que la défaillance de l'événement redouté ait lieu. Ces conditions font référence à l'occurrence des événements de base (b_i) et si nécessaire à des contraintes sur leur ordre d'occurrence ($b_j \prec b_k$). Elle correspond exactement aux besoins des fiabilistes pour conduire leurs analyses qualitatives.

Cette forme canonique peut également être exploitée pour mener les analyses quantitatives car elle permet de calculer également la probabilité de défaillance de l'événement redouté à l'instant t ($Pr\{Q\}(t)$) en fonction des probabilités de défaillances des événements de base ($Pr\{b_i\}(t)$) et de leur combinaisons ($Pr\{b_j \triangleleft b_k\}(t)$ ou $Pr\{b_k \cdot (b_j \triangleleft b_k)\}(t)$) [ACL 5] [ACL 17].

$$Pr\{Q\}(t) = f\left(Pr\{b_i\}(t), Pr\{b_j \triangleleft b_k\}(t), Pr\{b_k \cdot (b_j \triangleleft b_k)\}(t)\right)$$

Pour ces travaux, Guillaume Merle a obtenu un prix :

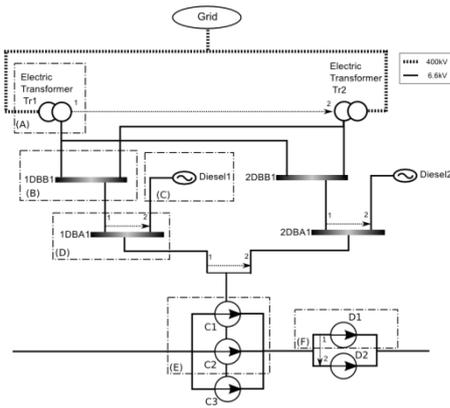
- Prix 2009-2010 des meilleures thèses en automatique du GDR MACS et de la section automatique du Club EEA, dans la catégorie « Systèmes à Événements Discrets et Systèmes hybrides ».

Formalisation de la cohérence et calcul des séquences de coupe minimales pour les systèmes dynamiques réparables

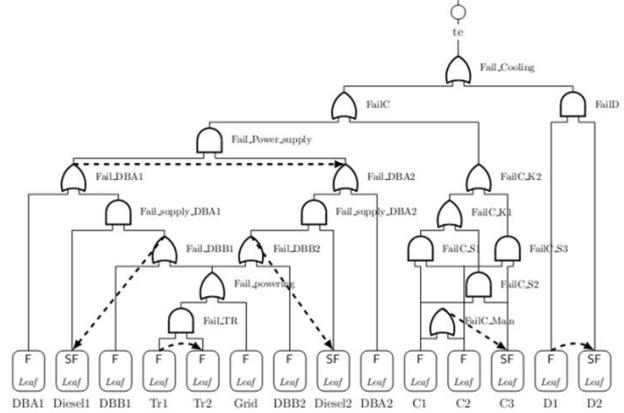
L'objectif des travaux de thèse de Pierre-Yves Chaux [TH 11], réalisé dans le cadre d'une [convention CIFRE avec la société EDF R&D, département MRI](#), est de proposer une définition et une technique de calcul des séquences de coupe minimales pour les systèmes dynamiques réparables. Il convient d'insister sur le fait que l'absence d'une formalisation précise de ces séquences de coupe minimales a favorisé l'émergence de définitions propres à certains outils de modélisation et de nombreuses définitions informelles. Il arrive même que pour certaines études de sûreté, deux outillages distincts donnent des résultats différents.

Les travaux de thèse de Pierre-Yves Chaux [TH 11] ont permis de proposer :

- une définition formelle des séquences de coupe minimales, indépendant du modèle d'analyse préliminaire de sûreté utilisé, basée sur :
 - **la théorie des langages** et sur une extension aux systèmes dynamiques du paradigme de **cohérence**, préalablement défini pour les systèmes statiques (Birbaum, 1961). Le comportement dynamique dysfonctionnel du système est alors représenté par le **langage dysfonctionnel** \mathcal{L}_D . Le **langage défaillant** \mathcal{L}_F comprend l'ensemble des séquences d'événements de panne et de réparation des composants conduisant à la défaillance du système ($\mathcal{L}_F \subset \mathcal{L}_D$). Dans le cadre des travaux, ces deux langages sont manipulés à travers un automate à états finis dont \mathcal{L}_D est le langage généré et \mathcal{L}_F est le langage marqué.
- une méthode permettant le calcul des séquences de coupe minimales, basée sur des propriétés déduites de leur définition.
 - Cette méthode procède par élimination des séquences non minimales à partir d'un sous-ensemble suffisant de séquences de \mathcal{L}_D . Les travaux théoriques conduits ont pu démontrer que cet ensemble initial est bien un sur-ensemble de l'ensemble recherché.
- l'extension des premières définitions aux composants multimodes. Ce cadre permet le calcul des séquences de coupe minimales pour des installations décrites avec les Boolean logic Driven Markov Processes (BDMP), outil de description mise en place par EDF (figure 17).



Installation électrique modélisée



Modèle BDMP de l'installation

16 384 états ($=2^{14}$) dont 13 300 défaillants
229 376 transitions

Automate équivalent

136 séquences de coupe minimales
de longueur inférieure ou égale à 6

Séquences de coupes minimales

Figure 17 Étude qualitative d'une installation électrique à l'aide de BDMP

Sous l'hypothèse que l'ensemble des scénarios représentés implicitement via le modèle de sûreté établi peut être modélisé à l'aide d'un automate fini, **ces travaux définissent donc la notion de cohérence des systèmes dynamiques et réparables comme le moyen de définir et obtenir une représentation minimale de l'ensemble des scénarios menant à la défaillance du système.**

Pour ce faire, il a été introduit une représentation minimale du langage défaillant ($\mathcal{Kern}(\mathcal{L}_{\mathcal{F}})$) et une application (\mathcal{CR}_4) permettant de reconstruire entièrement $\mathcal{L}_{\mathcal{F}}$ à partir de $\mathcal{Kern}(\mathcal{L}_{\mathcal{F}})$. L'application (\mathcal{CR}_4) résulte de la formalisation des règles de cohérences appliquées aux systèmes dynamiques réparables.

$$\left\{ \begin{array}{l} \mathcal{Kern}(\mathcal{L}_{\mathcal{F}}) \xrightarrow{\mathcal{CR}_4} \mathcal{L}_{\mathcal{F}} \\ \exists P \subset \mathcal{Kern}(\mathcal{L}_{\mathcal{F}}) (P \neq \mathcal{Kern}(\mathcal{L}_{\mathcal{F}})), P \xrightarrow{\mathcal{CR}_4} \mathcal{L}_{\mathcal{F}} \end{array} \right.$$

Pour le traitement des BDMP, il a été montré, dans [CAN 13], qu'il était possible d'établir algébriquement la fonction de structure d'une sous-classe de BDMP ainsi qu'un modèle combinatoire décrivant le fonctionnement de chaque composant en fonction des défaillances des composants en interaction. Cependant, dans le cas des systèmes réparables fortement interconnectés, la connaissance du modèle algébrique de la fonction de structure ne suffit pas à l'ingénieur fiabiliste pour mener à bien ses études qualitatives. Il a également besoin de connaître les différents scénarios qui conduisent à la panne de son système. Pour ce faire, une modélisation des BDMP à l'aide d'automates finis a été également proposée [CAI 37]. Des mécanismes propres à la théorie des langages pour extraire automatiquement les informations nécessaires à une analyse qualitative à partir de cette modélisation ont été ensuite définis [CAI 41], [CAI 52].

5.1.3. Commentaires

Au travers des résultats de thèses de Guillaume Merle [TH 5] et de Pierre-Yves Chauv [TH 11], nous avons pu montrer que les compétences acquises dans le domaine des SED, pouvaient être exploitées avec profit pour la formalisation des outils pour l'analyse de sûreté.

Aujourd'hui, pour certaines études de sûreté, les fiabilistes doivent tenir compte des nécessaires interactions entre les composants d'un système afin d'être représentatif du système étudié. Dans les modèles qu'ils doivent établir, la part du comportement dynamique est de plus en plus importante (Boiteau, 2006), (Gudemann, 2011). Cet état de fait rend le recours aux approches développées pour les SED de plus en plus nécessaire.

La [collaboration avec l'Équipe Sysmo du LIX](#), École Polytechnique (Palaiseau) dans le cadre de la thèse de Pierre-Antoine Brameret s'inscrit dans ce cadre.

5.1.4. Références extérieures

- Birnbaum, Z., Esary, J., and Saunders, S. (1961). Multicomponent systems and structures and their reliability. *Technometrics*, 3(1), 55-77.
- Bouissou, M. and Bon, J. (2003). A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes. *Reliability Engineering & System Safety*, 82(2), 149 – 163
- Boiteau, M., Dutuit, Y., Rauzy, A., and Signoret, J.P.(2006). The altarcica data-flow language in use: Assessment of production availability of a multistates system, *Reliability Engineering and System Safety*, 91, 747 - 755.
- Dugan, J., Bavuso, S., and Boyd, M. (1992). Dynamic fault-tree models for fault-tolerant computer systems. *Reliability, IEEE Transactions on*, 41(3), 363 - 377.
- Gudemann, M. and Ortmeier, F. (2011). Towards model-driven safety analysis. In *Dependable Control of Discrete Systems (DCDS)*, 2011 3rd International Workshop on, 53 - 58. IEEE.

5.2. Allocation des fonctions de contrôle-commande des systèmes critiques par analyse d'atteignabilité

La conception de l'architecture opérationnelle d'un système de contrôle-commande consiste formellement à projeter l'architecture fonctionnelle, qui décrit les échanges de données entre les fonctions de contrôle-commande, sur l'architecture matérielle (ou physique), qui décrit la structure du système matériel, constitué d'automates programmables, de calculateurs industriels, de SNCC, ... reliés par des réseaux de communication, sur lequel seront implantées les fonctions précédemment identifiées. Deux approches de conception sont théoriquement possibles :

- conception bonne a priori, ou synthèse automatique ;
- conception basée sur l'expertise puis évaluation des performances et validation a posteriori.

La seconde approche est souvent privilégiée en pratique car la première approche nécessite d'élaborer puis de résoudre un système de contraintes souvent très complexe car intégrant de nombreux paramètres caractéristiques des composants de l'architecture matérielle.

En se plaçant donc dans cette dernière approche, le principal problème à résoudre est l'allocation de l'ensemble des fonctions de l'architecture fonctionnelle aux composants de l'architecture matérielle. Cette opération d'allocation doit bien entendu respecter des contraintes liées aux capacités des composants matériels ; il n'est par exemple pas possible d'allouer à un composant qui ne dispose que de N entrées deux fonctions qui utilisent au total un nombre supérieur d'entrées. De plus, quand on s'intéresse à des architectures de commande de systèmes critiques, des contraintes de sûreté, comme la non-allocation au même composant matériel de deux fonctions assurant une redondance fonctionnelle, doivent également être introduites. La complexité de ce problème d'allocation de fonctions explique qu'à l'heure actuelle cette opération est réalisée par des experts et nécessite un temps très important.

Comme pour tout problème de satisfaction de contraintes, plusieurs types de résultats peuvent être recherchés lors de l'allocation :

- une seule solution réalisable (ou faisable), c.à.d. qui satisfait le système de contraintes,
- un ensemble borné de solutions faisables,
- l'ensemble des solutions faisables,
- une solution optimale.

Le dernier cas suppose qu'un critère d'optimisation ait été précédemment défini, ce qui n'est pas forcément une tâche triviale. Le deuxième type de résultat est très souvent apprécié par les concepteurs industriels car il permet en effet de comparer, à l'aide des techniques d'évaluation de performances décrites ci-dessus, plusieurs solutions qui respectent toutes les contraintes fondamentales de projection.

5.2.1. Objectifs des travaux

L'objectif des travaux de thèse de Thibault Lemattre, réalisée dans le cadre d'une convention CIFRE avec la société EDF R&D, département STEP, soutenue le 9 juillet 2013, est de proposer une méthode d'allocation sous contraintes de capacité et de sûreté d'un ensemble connu de fonctions, les caractéristiques externes de ces fonctions et des contrôleurs pouvant accueillir ces fonctions étant connues. Trois types de résultats sont proposés : une solution réalisable, un ensemble borné de solutions réalisables, ou une solution optimale, le critère d'optimisation retenu étant le nombre minimum de contrôleurs dans l'architecture finale.

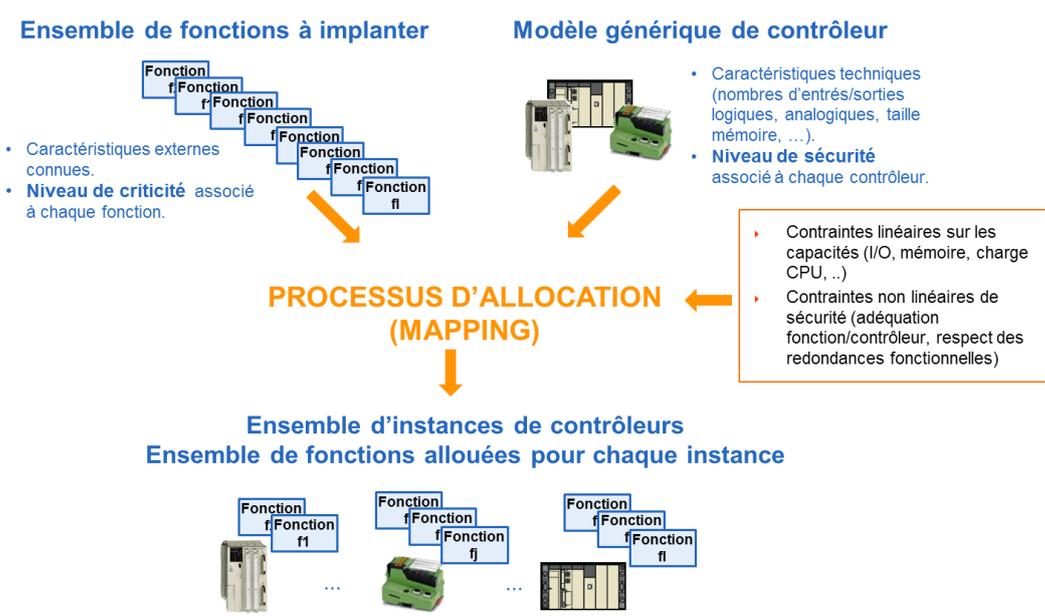


Figure 18 Allocation de fonctions sous contraintes

5.2.2. Principaux résultats obtenus

La première contribution originale de ces recherches [CAI 32], [CAI 35], [CAN 15] a consisté en la modélisation du problème d'allocation par un ensemble de mécanismes de type requête/réponse concurrents dans un réseau d'automates communicants à variables entières. Ce réseau comporte autant d'automates émetteurs de requêtes qu'il y a de fonctions à allouer et un nombre d'automates répondant à ces requêtes égal au nombre de contrôleurs que l'on souhaite utiliser. Il convient de noter que cette contribution a été inspirée des résultats du [projet AMETIST](#), (Behrmann, 2005), (Subbiah, 2010), où des problèmes d'ordonnancement ont été résolus par recherche d'atteignabilité dans un réseau d'automates communicants ; s'intéressant à des problèmes d'ordonnancement, ces propositions étaient basées sur un réseau d'automates temporisés ce qui n'est pas le cas pour nos travaux, le problème d'allocation ne nécessitant pas la prise en compte du temps.

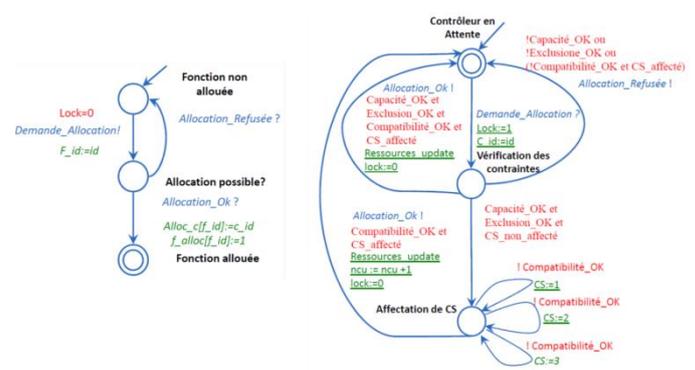


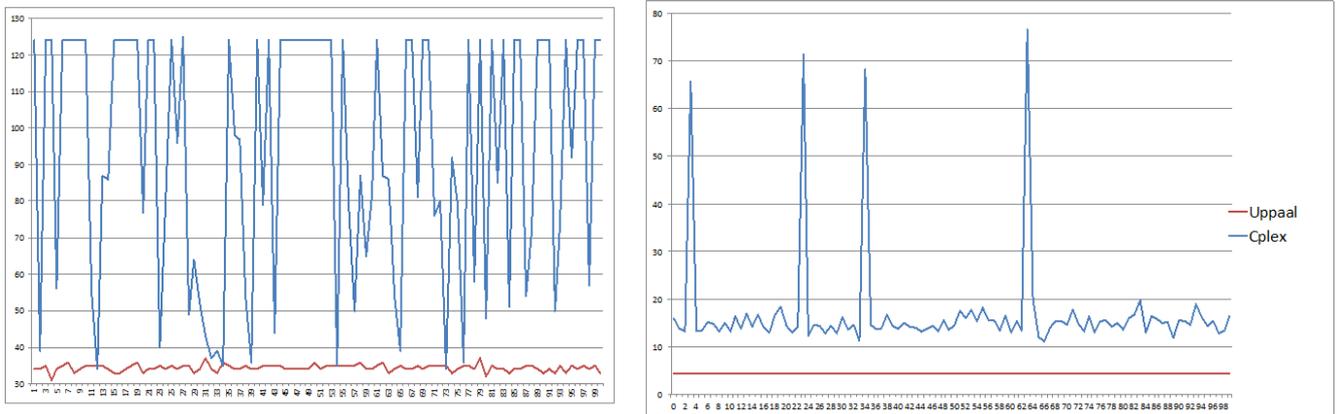
Figure 19 Modèles génériques d'émission de requête d'allocation et d'acceptation/refus de requêtes

Une solution réalisable est alors obtenue en recherchant un état atteignable depuis l'état initial qui satisfait une propriété formelle exprimant que toutes les fonctions ont été allouées. En itérant cette recherche d'atteignabilité à partir d'un état initial différent, il est possible d'obtenir un ensemble de solutions réalisables, ou une solution optimale.

Cette méthode d'allocation par recherche d'atteignabilité a ensuite été comparée à une méthode de résolution par programmation linéaire en nombres entiers (ILP), sur la base d'études de cas représentatives comportant chacune 200 fonctions ; cette comparaison a nécessité de linéariser les contraintes initialement non-linéaires pour pouvoir appliquer l'approche ILP. Les résultats de cette comparaison ont nettement mis en évidence l'intérêt de notre proposition :

Les solutions minimales, étant donné des limitations de mémoire et de temps de calcul, sont comparables.

Par contre, l'approche par recherche d'atteignabilité fournit beaucoup plus rapidement une solution réalisable très proche d'une solution minimale. Cette caractéristique permet donc d'avoir en un temps réduit un ensemble de solutions réalisables qui pourront être évaluées par un expert ou à l'aide de techniques d'évaluation de performances.



En rouge, résultats de la recherche d'atteignabilité ; en bleu, résultats de l'approche ILP

Figure 20 Nombre de contrôleurs nécessaires dans la première solution faisable et temps d'obtention de cette solution

5.2.3. Commentaires

Les résultats de ces travaux sont très encourageants sur plusieurs points. D'un pont de vue méthodologique, ils ouvrent la voie à des approches de résolution de problèmes de satisfaction de contraintes couplant recherche d'atteignabilité et ILP, la première méthode fournissant rapidement une solution réalisable qui pourrait ensuite être analysée par ILP à des fins d'optimisation. L'introduction de nouvelles contraintes de capacité ou de sûreté est aussi une voie prometteuse.

En dernier lieu, les résultats de ces travaux constituent la base des recherches de [l'Action de Recherche Concertée 2.2 du projet BGLE \(Briques Génériques du Logiciel Embarqué\) CONNEXION](#) qui s'intéresse à l'évaluation des performances temporelles et de sûreté, par exemple en termes de disponibilité, d'une architecture opérationnelle de contrôle-commande.

5.2.4. Références extérieures

G. Behrmann et al. Production scheduling by reachability analysis - a case study. *Parallel and Distributed Processing Symposium, International*, 3:140–147, 2005.

S. Subbiah and S. Engell. Short-Term Scheduling of Multi-Product Batch Plants with Sequence-Dependent Changeovers Using Timed Automata Models. *20th European Symposium on Computer Aided Process Engineering*, volume 28, pp. 1201–1206, 2010.

5.3. Analyse de sûreté des architectures de contrôle/commande

Dans de très nombreux domaines d'application, les bus de terrain ont remplacé les traditionnelles connections point-à-point pour assurer les communications entre les composants des systèmes de contrôle-commande ; cette évolution technologique a permis en particulier de réduire le coût et le poids du câblage. Cependant, pour des communications relatives à des fonctions critiques, cette évolution n'est possible que si la fiabilité de la nouvelle solution est au moins égale à celle de la précédente.

Plusieurs types de fautes peuvent se produire dans un réseau de terrain (Cauffriez, 2004). Les premières à considérer sont celles se produisant dans la couche physique car leur analyse permet de définir les mécanismes de tolérance aux fautes des couches OSI supérieures. De manière synthétique, et si on ne considère que la logique des communications, et non les fautes sur les valeurs numériques des données ou relatives au temps, qui peuvent trouver leur origine dans d'autres couches ou dans l'environnement, les fautes restantes peuvent se ranger dans l'une ou l'autre des deux catégories suivantes :

- absence intempestive de données,
- présence intempestive de données.

Les composants du réseau doivent donc être modélisés comme des composants à deux états de défaillance (un cas particulier de ‘multi-state components’ (Ramirez-Marquez, 2006)), le premier représentant une défaillance locale et le second une défaillance propagée (Xing, 2010) ; lorsqu’un composant du réseau émet de manière intempestive des données, le bus n’est en effet plus disponible pour d’autres communications. Les méthodes traditionnelles d’analyse prévisionnelle des fautes (arbre de défaillances, diagrammes de fiabilité, ...) ont été développées pour des composants binaires, à un seul état de défaillance, et supposent que les événements élémentaires sont indépendants ; elles ne peuvent donc pas être employées pour le calcul de la fiabilité des communications. Il est par contre possible d’utiliser à cette fin des modèles de composants sous forme de chaînes de Markov.

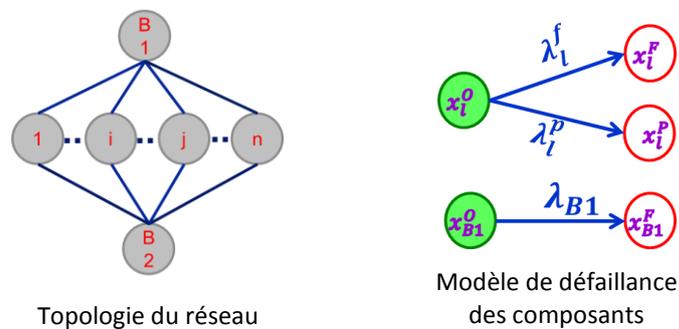
Le modèle du réseau de terrain peut alors être obtenu par composition de ces chaînes de Markov élémentaires. Néanmoins, cette composition donne lieu très rapidement à des modèles comportant un très grand nombre d’états qui ne peuvent être analysés que par simulation. Ceci limite l’intérêt de cette modélisation car il serait préférable de disposer d’une expression analytique de la fiabilité, prenant en compte les probabilités de se trouver dans les différents états de défaillance, et qui pourrait être utilisée par le concepteur du réseau pour comparer rapidement différentes solutions de communication.

5.3.1. Objectifs des travaux

Les travaux de la thèse de Damien Aza-Vallina, qui a débuté en octobre 2010, visent donc à proposer une méthode permettant d’obtenir une expression analytique de la fiabilité d’une transmission entre deux terminaux (two-terminal problem) d’un réseau de terrain, à partir de modèles multi-états des composants du réseau et de la connaissance de la topologie. Cette méthode doit être capable de passer à l’échelle et donc éviter, ou tout au moins limiter, l’explosion combinatoire.

5.3.2. Principaux résultats obtenus

La détermination de cette expression [CAI 38], [CAN 14] s’appuie sur la recherche des combinaisons d’états admissibles, combinaisons d’états qui autorisent la transmission. Ces combinaisons sont obtenues par analyse des chemins entre les deux terminaux considérés dans le graphe représentant la topologie du réseau, les nœuds situés sur ces chemins devant être non-défaillants et les nœuds adjacents ne devant pas être dans un état de défaillance propagée. Lorsque ces combinaisons d’états sont déterminées, l’expression analytique s’obtient en remplaçant les états de composants par leurs probabilités d’occupation.



$$C_{1N}^{P1N} = X_1^0 \times \left[\prod_{l=2}^{N-1} (X_l^0 \cup X_l^F) \right] \times X_N^0 \times X_{B1}^0 \times (X_{B2}^0 \cup X_{B2}^F)$$

Combinaisons autorisées d’états

$$\pi_{1N}(t) = e^{-(\lambda_1^f + \lambda_1^p)t} \cdot \left[\prod_{l=2}^{N-1} \frac{\lambda_l^f + \lambda_l^p \cdot e^{-(\lambda_l^f + \lambda_l^p)t}}{\lambda_l^f + \lambda_l^p} \right] e^{-(\lambda_N^f + \lambda_N^p)t} \cdot \left[(e^{-\lambda_{B1}t} \cdot e^{-\lambda_{B2}t}) + (e^{-\lambda_{B1}t} \cdot (1 - e^{-\lambda_{B2}t}) + ((1 - e^{-\lambda_{B1}t}) \cdot e^{-\lambda_{B2}t})) \right]$$

Expression de la fiabilité (taux de défaillance supposés constants)

Figure 21 Étapes du calcul de l’expression analytique de la fiabilité

L’expression analytique permet alors d’évaluer l’influence des fautes propagées. La Figure 22a) représente l’évolution de la fiabilité d’une transmission au cours du temps pour plusieurs tailles de réseau. On constate aisément que la fiabilité diminue lorsque le nombre de terminaux augmente, les possibilités d’émission intempestive s’accroissent. D’autre part, la

comparaison avec une analyse sans prise en compte des fautes propagées (un seul mode de défaillance) montre que cette modélisation est trop optimiste et justifie clairement l'intérêt des travaux.

Ces résultats ont été ensuite étendus à la modélisation de réseaux de terrain à plusieurs partitions [CAI 42], l'objectif étant de fournir au concepteur des outils d'aide au partitionnement. Deux types de transmissions doivent alors être étudiés : transmissions intra- et inter-partitions.

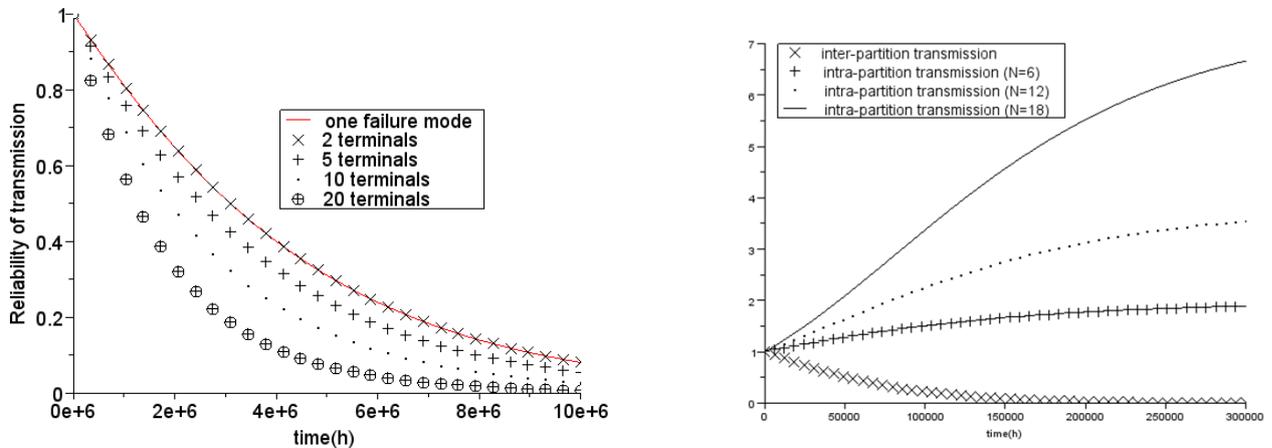


Figure 22 Évolution de la fiabilité d'une transmission
et Évolution du rapport de la fiabilité entre des solutions à plusieurs partitions

Les trois courbes du haut dans la figure ci-contre représentent l'évolution au cours du temps du rapport entre la fiabilité d'une transmission entre deux terminaux se trouvant dans la même partition d'un réseau à deux partitions et celle de la même transmission dans un réseau non-partitionné, pour différentes valeurs du nombre N de terminaux. Il est clair que le partitionnement améliore nettement la fiabilité des transmissions intra-partition, et ceci d'autant plus que le nombre de terminaux du réseau est grand.

On notera par contre (courbe inférieure) que le partitionnement diminue la fiabilité des transmissions inter-partitions, l'expression de cette fiabilité comportant un terme supplémentaire qui correspond à la défaillance du commutateur reliant les partitions.

En dernier lieu, des travaux récents [CAI 54] ont montré que les résultats obtenus à partir de modèles de composants sous la forme de chaînes de Markov peuvent être étendus à une modélisation des composants du réseau par automates de mode (Rauzy, 2002), cette représentation regroupant les comportements fonctionnels (émission, transmission ou réception de données) et dysfonctionnels (défaillance avec ou sans propagation) des composants. L'algorithme d'obtention des combinaisons d'états admissibles a donc été adapté à cette modélisation.

5.3.3. Commentaires

Cette recherche s'est déroulée dans le cadre d'Inno'campus, structure de recherche collaborative entre l'ENS de Cachan et EADS Innovation Works. Les résultats ont été appréciés du partenaire industriel ; un brevet [BRE 1] au nom des personnels des deux partenaires ayant contribué a été publié en décembre 2012. De plus, une maquette logicielle développée durant sur la base de ces résultats est en cours d'évaluation dans les services techniques de l'entreprise.

Les perspectives scientifiques offertes par ces travaux concernent l'extension à la modélisation des mécanismes de tolérance aux fautes dans une perspective d'analyse prévisionnelle des fautes, par exemple sous la forme de recherche de séquences minimales, lors de reconfiguration de l'architecture du réseau de terrain.

5.3.4. Références externes au LURPA

Cauffriez L., Ciccotelli J., Conrard B., Bayart M., the members of the working-group CIAME (2004), Design of intelligent distributed control systems: a dependability point of view, *Reliability Engineering & System Safety*, 84 (1), pp. 19-32

Ramirez-Marquez A. et al. (2006), New insights on multi-state component criticality and importance, *Reliability Engineering & System Safety*, 91 (8), pp. 894-904

Rauzy A. (2002), Mode automata and their compilation into fault-trees, *Reliability Engineering & System Safety*, 78 (1), pp. 1-12

Xing L., Levitin G. (2010), Combinatorial analysis of systems with competing failures subject to failure isolation and propagation effects, *Reliability Engineering & System Safety*, 95 (11), pp. 1210-1215

6. Collaborations nationales et internationales

Pour la période considérée, les membres de l'Équipe ISA ont mené à bien différentes collaborations nationales ou internationales. Dans ce document, seules les collaborations ayant donné lieu à au moins une publication ou un encadrement de thèse sont mentionnées.

6.1. Collaborations nationales

Nos partenaires universitaires de recherche dans le cadre de l'[ANR TESTEC](#), de l'[ANR VACSIM](#) et du [Cluster CONNEXION](#) sont listés au paragraphe « 8.1 Projets de recherche nationaux ».

Équipe Sympa du CRAN, Université de Lorraine (Nancy)

La thèse de Thibault Lemattre [TH 12] est co-dirigée par Jean-Marc Faure et Jean-François Pétin (CRAN). Les résultats obtenus dans ce cadre ont donné lieu aux publications communes [CAN 15], [CAI 32], [CAI 35].

Équipe Sysmo du LIX, École Polytechnique (Palaiseau)

La thèse de Pierre-Antoine Brameret est co-dirigée par Jean-Marc Roussel et Antoine Rauzy (LIX). Les résultats obtenus dans ce cadre ont donné lieu à plusieurs publications communes [CAN 19], [CAI 53], [CAI 55].

Équipe AC SED de l'IRCCyN (Nantes)

Collaboration scientifique avec Jean-Jacques Loiseau, DR CNRS et responsable de l'équipe ACSED à l'RCCyN de Nantes, et Claude Martinez, Maître de conférences au laboratoire IRCCyN de Nantes. Thème de recherche : Commande des systèmes à événements discrets sous contraintes temporelles en utilisant l'algèbre des dioïdes ([ACL 11], [ACL 12]).

6.2. Collaborations internationales

Institute of automatic control AT+, University of Kaiserslautern (Allemagne)

La thèse de Matthias Roth [TH 6] a été réalisée en co-tutelle entre l'ENS de Cachan et l'Univ. Kaiserslautern, co-dirigée par Jean-Jacques Lesage et Lothar Litz.

Équipe SED, Unité Guadalajara du Cinvestav (Mexique)

La thèse d'Ana Paula Estrada Vargas [TH 10] a été réalisée en co-tutelle entre l'ENS de Cachan et le CINVESTAV- Guadalajara, co-dirigée par Jean-Jacques Lesage et Ernesto Lopez-Mellado.

Dipartimento di Informatica, Università del Piemonte Orientale (Italie)

Collaboration scientifique avec Andrea Bobbio dans le cadre de la modélisation des arbres de défaillances dynamiques. Cette collaboration a donné lieu aux publications communes [ACL 1] et [CAI 11].

Laboratoire de CCSP, Université Mouloud MAMMERI de Tiri-Ouzou (Algérie)

Saïd Amari encadre avec Rédouane Kara (MdC - HdR) deux thèses de doctorat (K. Tebaniet, L. Mameri). Thèmes de recherche : Commande temps-réel des architectures d'automatisation en réseau, Modélisation et analyse des réseaux de Graphes d'Événements Temporisés en Conflits dans l'algèbre Max-Plus.

Institute of Automation and Information Systems, Technische Universität München, (Allemagne)

Le projet de recherche MITPES « Modelling, Implementation and Test of PLC-based Embedded Systems » (Modélisation, Implantation et Test des Systèmes Embarqués à base d'API) a été mis en place avec le Professeur Birgit Vogel-Heuser. Il visait à étendre les résultats de thèse de Julien Provost [TH 8] à d'autres langages de spécification. Ce projet a été financé dans le cadre du PHC Procope en 2009 et 2010.

7. Activités d'animation et de rayonnement national et international

Animé d'une volonté affirmée de contribuer aux actions visant à accroître la visibilité de la communauté scientifique, les enseignants-chercheurs de l'Équipe ISA de participent régulièrement à des jurys de thèse et d'HdR, à l'évaluation d'entités, à des comités de recrutement, à des groupes de travail nationaux et internationaux et sont impliqués dans l'organisation de manifestations scientifiques nationales et internationales.

7.1. Activités au plan national

Participation à des instances d'animation

Pour la période considérée, l'Équipe ISA a participé, au travers de ces membres, aux instances d'animation suivantes :

- **Conseil National des Universités, section 61 :**
 - J.-J. Lesage : membre élu rang A pour le mandat 2008/2011
 - S. Amari : membre élu rang B pour le mandat 2012/2015
 - J.-M. Faure : membre élu rang A pour le mandat 2012/2015
- **GDR MACS (Modélisation, Analyse et Conduite des Systèmes dynamiques) :**
 - J.-M. Faure : membre du comité de Direction pour les périodes 2006/2009 et 2010/2013
 - J.-M. Faure : animateur du prix des meilleures thèses
- **Club EEA :**
 - J.-M. Faure : président de la section Automatique du Club EEA pour le mandat 2010/2013

Participation à des jurys de thèses ou d'HdR

Dans la période de référence, les permanents de l'équipe ISA ont participé à **18 jurys de thèse hors ENS Cachan** (10 en tant que Rapporteur et 2 en tant que Président) :

- J.-M. Faure (Rap.) 06/2008 : Thèse de R. Ghostine, dirigée par J.-F. Aubry, Université Nancy 1 - CRAN
- J.-M. Faure (Pré.) 07/2008 : Thèse de D. Evrot, dirigée par G. Morel, Université Nancy 1 - CRAN
- J.-J. Lesage (Rap.) 10/2008 : Thèse de A. Allahham, dirigée par H. Alla, Université Joseph Fourier - GIPSA
- J.-J. Lesage (Exa.) 12/2008 : Thèse de X. Pucel, dirigée par L. Trave-Massuyes, Université Paul Sabatier - LAAS
- J.-M. Roussel (Exa.) 12/2008 : Thèse de B. Rohée, dirigée par B. Riera, Université Reims - CRESTIC
- J.-J. Lesage (Rap.) 01/2009 : Thèse de F. Chiron, dirigée par A. Quillot, Université Blaise Pascal - LIMOS
- J.-M. Faure (Rap.) 02/2009 : Thèse de R. Awedikian, dirigée par B. Yannou, Ecole Centrale Paris - LGI
- J.-J. Lesage (Rap.) 11/2009 : Thèse de P. David, dirigée par F. Cratz, ENSI Bourges - PRISME
- J.-M. Faure (Rap.) 12/2009 : Thèse de H.-X. Hu, dirigée par M. Bayart, Ecole Centrale Lille - LAGIS
- J.-J. Lesage (Pré.) 10/2010 : Thèse de E. Chauvet, dirigée par P. Castagna, Université Nantes - IRCCyN
- J.-J. Lesage (Exa.) 10/2010 : Thèse de M. Hemour, dirigée par B. Riera, Université Reims – CRESTIC
- B. Denis (Exa) 11/2010 : Thèse de M. Hemour, dirigée par T. Divoux, Université Nancy 1 - CRAN
- J.-J. Lesage (Rap.) 11/2011 : Thèse de E. Le Corronc, dirigée par L. Hardouin, Université Angers - ISTIA
- J.-M. Faure (Rap.) 02/2012 : Thèse de A. Vasiliu, dirigée par H. Alla, Université Joseph Fourier - GIPSA
- J.-J. Lesage (Rap.) 03/2012 : Thèse de T. Ferrandiz, dirigée par C. Fraboul, INP Toulouse
- J.-J. Lesage (Exa.) 06/2012 : Thèse de C. Hamon, dirigée par J. Lebeaume, Université Paris 5
- J.-M. Faure (Rap.) 12/2012 : Thèse de R. Cressent, dirigée par F. Kratz, ENSI Bourges – PRISME
- G. Faraut (Exa.) 01/2013 : Thèse de J. Yang, dirigée par E.-M. El-Koursi, Université de Lille- IFFSTAR

Il y a eu également **4 jurys de d'HdR** (2 en tant que Rapporteur et 1 en tant que Président) :

- J.-J. Lesage (Rap.) 12/08 : HdR de M. Sayed Mouchaweh, Université de Reims Champagne Ardennes - LAM
- J.-J. Lesage (Exa.) 11/09 : HdR de R. Bouyekhf, Université Technologique Belfort Montbelliard - SET
- J.-J. Lesage (Rap.) 10/10 : HdR de M. Yeddes, Université Paris 6 - LIP6
- J.-J. Lesage (Pré.) 11/11 : HdR de S. Lahaye, Université d'Angers - ISTIA

Participation à des évaluations de projets ou d'unités de recherche

Pour la période considérée, l'AERES a sollicité l'Équipe ISA pour 4 évaluations :

- J.-J. Lesage (01/2008) : [CRAN](#), UMR 7039 - Centre de Recherche en Automatique de Nancy
- J.-J. Lesage (02/2010) : [GSCOP](#), UMR 5272 - Laboratoire des Sciences pour la Conception, l'Optimisation et la Production de Grenoble

- J.-J. Lesage (11/2010) : [LISA](#), EA 4094 - Laboratoire d'Ingénierie des Systèmes Automatisés
- J.-J. Lesage (02/2011) : [CReSTIC](#), EA 3804 - Centre de Recherche en STIC

Pour la période considérée, les membres de l'Équipe ISA ont été sollicités pour différentes évaluations :

- J.-M. Faure (2008) : Participation au comité national pour l'attribution de la Prime d'Encadrement Doctoral et de Recherche
- J.-J. Lesage (depuis 2008) : Président du groupe thématique « Information, Communication, Organisation et Sécurité des Systèmes » (ICOS), au Conseil Scientifique et Stratégique pour l'Innovation de la région Champagne Ardennes
- J.-M. Faure (2011) : Participation au comité national pour l'attribution de la Prime d'Excellence Scientifique
- J.-J. Lesage (2011) : Participation au comité pour l'attribution de la PES de l'Université Bordeaux 1

Participation à des comités de sélection

Dans la période de référence, les permanents de l'Équipe ont participé à **15 comités de sélection** :

- 61 MCF 0422, [Université de Reims Champagne Ardennes](#), 05/2009 : J.-M. Roussel
- 61 MCF 0352, [Université Paul Sabatier de Toulouse](#), 04/2010 : J.-J. Lesage
- 60 PR 0008, [ENS Cachan](#), 05/2010 : J.-M. Faure
- 60/61 MC 0242, [Université de Technologie de Compiègne \(UTC\)](#), 05/2010 : J.-J. Lesage
- 61 MCF 027, [SupMeca](#), 05/2010 : J.-M. Faure
- 61 MCF 0698, [Université de Nancy 1](#), 05/2010 : J.-M. Faure
- 61 MCF 0422, [Université de Reims Champagne Ardennes](#), 05/2011 : J.-M. Roussel
- 61 MCF 074, [ENS Cachan](#), 05/2011 : J.-M. Faure, J.-J. Lesage, J.-M. Roussel (Président)
- 61 PR 0631, [Université de Reims Champagne Ardennes](#), 05/2011 : J.-M. Faure
- 61 PR 0556, [Université Paul Sabatier de Toulouse](#), 04/2012 : J.-J. Lesage
- 61 PR 1260, [Université Paul Sabatier de Toulouse](#), 04/2012 : J.-J. Lesage
- 61 MCF 0693, [Université de Lorraine](#), 05/2012 : J.-M. Faure
- 61 PR XXXX, [SupMeca](#), 05/2012 : J.-M. Faure
- 61 MCF 0817, [Université de Reims Champagne Ardennes](#), 05/2013 : J.-M. Roussel
- 61 MC 2191, [Université Aix-Marseille](#), 05/2013, S. Amari

Participation à des comités de programmes de conférences nationales ou francophones (10+2)

- CIFA 2008, 5ème Conférence Internationale Francophone d'Automatique, Bucarest (Roumanie), 09/2008 : J.-M. Faure, J.-J. Lesage
- [JD/JN MACS 2009](#), 3ièmes Journées Doctorales du GDR MACS, Angers, 03/2009 : J.-M. Faure, J.-J. Lesage
- [MSR 2009](#), 7ème colloque francophone sur la Modélisation des Systèmes Réactifs, Nantes, 11/2009 : J.-M. Faure, J.-J. Lesage (Président du Comité de Pilotage)
- CETSIS 2010, 8ième Colloque Enseignement des Technologies et des Sciences de l'Information et des Systèmes, Grenoble, 03/2010 : J.-J. Lesage
- [CIFA 2010](#), 6ème Conférence Internationale Francophone d'Automatique, Nancy, 06/2010 : J.-M. Faure, J.-J. Lesage
- [JD/JN MACS 2011](#), 4ièmes Journées Doctorales du GDR MACS, Marseille, 06/2011 : J.-M. Faure, J.-J. Lesage
- CETSIS 2011, 9ième Colloque Enseignement des Technologies et des Sciences de l'Information et des Systèmes, Trois Rivières (Canada), 10/2011 : J.-J. Lesage
- [MSR 2011](#), 8ème colloque francophone sur la Modélisation des Systèmes Réactifs, Lille, 11/2011 : J.-M. Faure, J.-J. Lesage (Président du Comité de Pilotage)
- [CIFA 2012](#), 7ème Conférence Internationale Francophone d'Automatique, Grenoble, 07/2012 : J.-M. Faure, J.-J. Lesage
- [CETSIS 2013](#), 10ième Colloque Enseignement des Technologies et des Sciences de l'Information et des Systèmes, Caen, : J.-M. Roussel

Pour information, congrès planifiés à l'issue de la période de référence

- [JD/JN MACS 2013](#), 5ièmes Journées Doctorales du GDR MACS, Strasbourg, 07/2013 : J.-M. Faure
- [MSR 2013](#), 9ème colloque francophone sur la Modélisation des Systèmes Réactifs Rennes, 011/2013 : J.-M. Faure, J.-J. Lesage

7.2. Activités au plan international

Participation à des instances d'animation

Pour la période considérée, l'Équipe ISA a participé, au travers de ces membres, aux instances d'animation suivantes :

- **IFAC Technical Committee 1.3 "Discrete event and hybrid systems"** :
 - J.-J. Lesage : Vice- Chair
 - J.-M. Faure : Représentant national
- **IFAC Technical Committee 3.1 "Computers for control"** :
 - J.-M. Roussel : Représentant national
- **IFAC Technical Committee 5.1 "Manufacturing Plant Control"** :
 - J.-M. Faure : Vice- Chair
- Revue **"IEEE Transactions on Automation Science and Engineering"** :
 - J.-M. Faure, J.-J. Lesage : Editeurs associés

Participation à des jurys de thèses

Les permanents de l'Équipe ont participé à **4 jurys de thèse** soutenue à l'étranger (3 en tant que rapporteur) :

- S. Amari (Exa.) 06/2009 : Thèse de R. Kara, dirigée par S. Djennoune et J.-J. Loiseau, Université Tizi-Ouzou (Algérie)
- J.-J. Lesage (Rap.) 09/2011 : Thèse de M. Güdeman, dirigée par F. Ortmeier, University of Magdebourg (Allemagne)
- J.-M. Faure (Rap.) 09/2012 : Thèse de N. Mahmud, dirigée par Y. Papadopoulos, University of Hull (UK)
- J.-J. Lesage (Rap.) 03/2013 : Thèse de Y. Nke, dirigée par J. Lunze, Université Bochum (Allemagne)

Organisation ou co-organisation de manifestations scientifiques internationales (2+1)

- [CASE 2011](#), 7th IEEE Int. Conf. on Automation Science and Engineering, 09/2011 :
 - J.-J. Lesage : Chair du track "Foundation of Automation"
- [WODES 2012](#), 11th International Workshop on Discrete Event Systems, 10/2012 :
 - J.-J. Lesage : Co-Chair de la conference
- [ECC 2013](#), 10th European Control Conference, Zurich (Switzerland), 07/2013 :
 - J.-J. Lesage : Associate editor

Participation à des comités de programmes de congrès internationaux (22+3)

- [WODES 2008](#), 9th International Workshop On Discrete Event Systems, Göteborg (Sweden), 05/2008 : J.-M. Faure, J.-J. Lesage
- [INDIN 2008](#), 6th IEEE Conf. on Industrial Informatics, track Distributed Embedded and Networked Control, Daejeon (Korea), 07/2008 : J.-J. Lesage
- CoSME 2008, 2nd International Conference on Computing and Solution in Manufacturing Engineering, Brasov (Romania), 09/2008 : J.-J. Lesage
- [DCDS 2009](#), 2nd IFAC Workshop on Dependable Control of Discrete Systems, Bari (Italy), 06/2009 : J.-M. Faure, J.-J. Lesage, J.-M. Roussel
- [INCOM 2009](#), 13th IFAC symposium on Information Control Problems in Manufacturing, Moscow (Russia), 06/2009 : J.-M. Faure, J.-J. Lesage
- [ADHS 2009](#), 3rd IFAC International Conference on Analysis and Design of Hybrid Systems, Saragoza (Spain), 09/2009 : J.-J. Lesage
- [VECoS 2009](#), 3rd International Workshop on Verification and Evaluation of Computer and Communication Systems, Rabat (Morocco), 09/2009 : J.-J. Lesage
- [VECoS 2010](#), 4th International Workshop on Verification and Evaluation of Computer and Communication Systems, Paris (France), 04/2010 : J.-M. Roussel
- [ETFA 2010](#), 15th IEEE International Conference on Emerging Technologies and Factory Automation, Bilbao (Spain), 09/2010 : J.-M. Faure
- [WODES 2010](#), 10th International Workshop On Discrete Event Systems, Berlin (Germany), 09/2010 : J.-M. Faure, J.-J. Lesage
- [DCDS 2011](#), 3rd IFAC Workshop on Dependable Control of Discrete Systems, York (United Kingdom), 06/2011 : J.-M. Faure, J.-J. Lesage, J.-M. Roussel
- [CASE 2011](#), 7th IEEE Int. Conf. on Automation Science and Engineering, Trieste (Italy), 09/2011 : J.-J. Lesage
- [ETFA 2011](#), 16th IEEE International Conference on Emerging Technologies and Factory Automation, Toulouse (France), 09/2011 : J.-M. Faure

- [VECoS 2011](#), 5th International Workshop on Verification and Evaluation of Computer and Communication Systems, Tunis (Tunisia), 09/2011 : J.-M. Rousset
- [ADHS 2012](#), 4th IFAC International Conference on Analysis and Design of Hybrid Systems, Eindhoven (the Netherlands), 06/2012 : J.-J. Lesage
- [INCOM 2012](#), 14th IFAC symposium on Information Control Problems in Manufacturing, Bucarest (Romania), 06/2012 : J.-M. Faure
- [CASE 2012](#), 8th IEEE Int. Conf. on Automation Science and Engineering, Seoul (Korea), 08/2012 : J.-M. Faure
- [VECoS 2012](#), 6th International Workshop on Verification and Evaluation of Computer and Communication Systems, Paris (France), 08/2012 : J.-M. Rousset
- [ETFA 2012](#), 17th IEEE International Conference on Emerging Technologies and Factory Automation, KraKow (Poland), 09/2012 : J.-M. Faure
- [SAFECOMP 2012](#), 31th International Conference on Computer Safety, Reliability and Security, Magdeburg (Germany), 09/2012 : J.-J. Lesage
- [WODES 2012](#), 11th International Workshop on Discrete Event Systems, Guadalajara (Mexico), 10/2012 : J.-M. Faure, J.-J. Lesage
- [IWMBSA 2013](#), 3rd International Workshop on Model Based Safety Assessment, Versailles (France), 03/2013 : J.-M. Rousset

Pour information, congrès planifiés à l'issue de la période de référence

- [ECC 2013](#), 10th European Control Conference, Zurich (Switzerland), 07/2013 : J.-J. Lesage
- [CASE 2013](#), 9th IEEE Int. Conf. on Automation Science and Engineering, Madison (USA), 08/2013 : J.-M. Faure, J.-J. Lesage
- [DCDS 2013](#), 4th IFAC Workshop on Dependable Control of Discrete Systems, York (United Kingdom), 09/2013 : J.-M. Faure, J.-J. Lesage, J.-M. Rousset

8. Activités contractuelles et valorisation

Les recherches menées dans l'Équipe ISA s'inscrivent dans le domaine des Sciences de l'Ingénierie. Elles contribuent donc à la résolution de défis industriels. Pour la période considérée, les membres de l'Équipe se sont investis dans 3 projets de recherche financés par l'État suite à un appel d'offres national, **4 collaborations industrielles et 3 collaborations locales au sein de l'ENS Cachan**.

8.1. Projets de recherche nationaux

Les projets de recherche nationaux auxquels a répondu l'Équipe ISA sont financés par l'ANR ou par les investissements d'avenir géré par le cabinet du Premier Ministre.

- L'**ANR, Agence Nationale de la Recherche**, a pour mission d'augmenter la dynamique du système français de recherche et d'innovation en mettant en œuvre le financement de la recherche sur projets.
- Les **investissements d'avenir** ont été lancés par le Président de la République le 14 décembre 2009 pour dynamiser l'économie française.

ANR Testec

Le projet 07-TLOG-022 TESTEC (TEst des Systèmes Temps réel Embarqués Critiques) s'est déroulé de mars 2008 à août 2011. Il réunissait deux industriels (EDF R&D et Geensoft (entreprise acquise par Dassault Systèmes en 2010)) et quatre laboratoires (I3S, INRIA Rennes, LaBRI, LURPA) ; le coordinateur du projet était le LURPA. Ce projet, le budget global étant de 1 M€, dont 150 k€ pour le LURPA.

Les résultats scientifiques obtenus lors de ce projet ont permis la soutenance de deux thèses portant sur le test de conformité des contrôleurs logiques [TH 8], le test des systèmes temporisés et l'apport des techniques de programmation par contraintes au test fonctionnel. Un certain nombre des résultats de ce projet sont en cours d'intégration dans les processus de conception et validation des systèmes de contrôle-commande des centrales de production d'énergie.

ANR Vacsim

Le [projet 11-INS-004 VACSIM](#) (VALIDation de la commande des systèmes critiques par Couplage Simulation et Méthodes d'analyse formelle) se situe dans la continuité du projet TESTEC. Il a démarré en octobre 2011, pour une durée de 42 mois, réunit les mêmes partenaires et est toujours coordonné par le LURPA, le budget global étant de 1 M€, dont 150 k€ pour le LURPA. L'objectif général de ce projet est de proposer des techniques complémentaires au test de conformité, en s'appuyant en particulier sur les nouvelles potentialités des environnements de modélisation et simulation des processus physiques.

Au niveau du LURPA, le financement de la thèse d'Anaïs Guignard est assuré par ce projet.

Cluster Connexion

Le [Cluster Connexion](#) a été élaboré par **9 partenaires industriels et 6 partenaires académiques** pour participer à l'appel à projet « **Briques génériques du logiciel embarqué** » clos le 29 avril 2011.

Depuis Janvier 2011, les partenaires industriels et académiques de la filière nucléaire française se sont unis pour élaborer un programme de travail de R&D ambitieux afin d'intégrer des innovations majeures dans la conception et la réalisation des systèmes de contrôle-commande des centrales nucléaires. Ce programme a été construit dans une logique de filière industrielle, à travers la mise en place d'un « Cluster » de projets à fort effet de levier, en cohérence avec les recommandations du Conseil de Politique Nucléaire du 21/02/2011, avec pour enjeux de :

- développer l'innovation et conserver la compétitivité de l'industrie nucléaire française sur le territoire et à l'export,
- renforcer la crédibilité et le rayonnement scientifique des acteurs du domaine,
- capitaliser les connaissances pour préparer le renouvellement des générations en conservant l'attractivité de la filière nucléaire.

Ce programme appelé **Cluster CONNEXION (CONtrôle Commande Nucléaire Numérique pour l'EXport et la rénovation)** a pour ambition de proposer et de valider une architecture innovante de plateformes de contrôle-commande adaptée aux centrales nucléaires en France et à l'International.

Cette architecture intègre un ensemble de briques technologiques développées par les partenaires académiques (CEA, INRIA, CNRS/CRAN, ENS Cachan, LIG, Telecom ParisTech) et reposant sur des collaborations entre des grands intégrateurs

comme AREVA et ALSTOM, l'opérateur EDF en France et des « techno-providers » de logiciels embarqués (Atos Worldgrid, Rolls-Royce Civil Nuclear, CORYS TESS, Esterel Technologies, All4Tec, Predict).

Parmi les axes de recherche du Cluster, on peut citer les dispositifs de **vérification et de validation des systèmes numériques**, l'affichage des informations pour faciliter la conduite, l'échange d'informations sans fil entre la salle de commande et les autres services (notamment avec les équipes de maintenance) ou encore la gestion des modifications du Contrôle-Commande dans le temps.

Enfin, le Cluster CONNEXION se matérialisera par la mise en place, sur le site d'EDF R&D à Chatou, d'un laboratoire d'expérimentation (comprenant notamment des systèmes de Contrôles-Commandes représentatifs des paliers 900 MWe et 1300 MWe) dans lequel les partenaires du Cluster pour tester en conditions réelles les briques technologiques développées.

Ce projet a été lancé le 12 avril 2012 pour une durée de 4 ans. Le coordinateur du projet est EDF R&D. Des informations complémentaires sur ce projet peuvent être trouvées sur le site WWW du projet : <http://www.cluster-connexion.fr>

Au niveau du LURPA, le financement de la thèse de Pierre-Yves Piriou est assuré par ce projet.

8.2. Collaborations industrielles

Collaboration avec l'Équipe STEP d'EDF R&D

Cette collaboration avec l'Équipe STEP « Simulation et Traitement de l'information pour l'Exploitation des systèmes de Production » s'est déroulée de décembre 2009 à novembre 2012. Elle concernait la **conception et validation des architectures de contrôle-commande des systèmes de production d'énergie**. La thèse de Thibault Lemattre [TH 12] se situe dans le cadre de cette collaboration (financement CIFRE).

Collaboration avec l'Équipe MRI d'EDF R&D

Cette collaboration s'est déroulée avec l'Équipe MRI « Management des Risques Industriels » de septembre 2009 à août 2012. Elle concernait la **formalisation de la cohérence et calcul des séquences de coupe minimales pour les systèmes dynamiques réparables**. Les travaux de thèse de Pierre-Yves Chauv [TH 11] se situent dans le cadre de cette collaboration (financement CIFRE).

Collaboration avec la société Dassault Systèmes

Cette collaboration s'est déroulée d'avril 2008 à mars 2011 et portait sur concernait la **modélisation et analyse multi-échelles des systèmes automatisés de production**. Les travaux de thèse de Matthieu Perin [TH 9] se situent dans le cadre de cette collaboration (thèse CIFRE).

Collaboration avec la société EADS

Cette collaboration se situe dans le cadre d'Inno'campus, structure de recherche collaborative entre l'ENS de Cachan et EADS Innovation Works. Elle concerne l'**analyse de la fiabilité des communications dans les systèmes embarqués en réseau**. Elle a débuté en octobre 2010 et se terminera en novembre 2013 lors de la soutenance des travaux de thèse de Damien Aza-Vallina.

8.3. Collaboration au sein de l'ENS Cachan

L'ENS Cachan a créé en décembre 2006 l'[Institut Farman](#) pour associer les compétences de cinq de ses laboratoires (le CMLA, le LMT, le LSV, le LURPA et le SATIE) dans le domaine de la modélisation, simulation et validation des systèmes complexes.

Pour la période considérée, l'Équipe ISA a participé à 3 projets portés et financés par cet institut.

Projet SIMOP : Synergie Simulation et Model-Checking Paramétré

L'objectif de ce projet collaboratif entre le LSV et LURPA était d'évaluer les performances d'une architecture de commande distribuée sujette à panne et d'estimer la plage de valeur des paramètres de fonctionnement de l'architecture qui garantit les performances attendues. Les différents modes de fonctionnement (mode nominal, différentes configurations de mode dégradé) seront pris en compte.

Pour atteindre cet objectif il a été utilisé le model-checking temporisé paramétré pour sa capacité à fournir des résultats à la fois quantitatifs et garantis sur les paramètres de fonctionnement recherchés. Comme sa mise en œuvre est limitée par la complexité intrinsèque du problème, il a été utilisé au préalable des observations issues de simulation pour limiter l'espace de recherche du model-checking. La méthode de model-checking temporisé et paramétré est dirigée par des résultats issus de simulation.

- **Caractéristiques du projet :**
- Durée du projet :
 - 2 ans : du 1/01/2007 au 31/12/2008
- Responsables :
 - Olivier De Smet¹ (LURPA)
 - Laurent Fribourg (LSV)

Projet EMOTICON : Equivalences between Models with Time and Concurrency

L'objectif de ce projet était de formaliser et systématiser la traduction de modèles de la famille des formalismes temporisés à états en s'attachant particulièrement aux paradigmes de concurrence et de temps. Pour ces formalismes, les transformations recherchées doivent préserver non seulement la sémantique séquentielle, mais aussi la concurrence. Il est ainsi nécessaire de formaliser la notion de préservation de la concurrence en définissant un critère d'équivalence qui devra permettre la comparaison de modèles issus de formalismes différents. Ce critère d'équivalence doit faire intervenir une sémantique temporisée concurrente pour les modèles, qui sera plus précise que la sémantique séquentielle. Cette sémantique concurrente doit utiliser des ordres partiels pour représenter les exécutions. Lors de la définition des transformations, nous nous attendions à devoir faire le constat que pour un formalisme d'origine, un formalisme cible et un critère d'équivalence donnés, il n'existait pas de transformation qui s'applique à tous les modèles du formalisme d'origine. Il a donc été nécessaire d'identifier des restrictions pertinentes du formalisme d'origine pour permettre la transformation, ou alternativement d'affaiblir le critère d'équivalence pour qu'une transformation soit possible. Les trois formalismes retenus pour le projet sont les automates temporisés, les réseaux de Petri T-temporels et le formalisme de l'ingénieur SFC.

- **Caractéristiques du projet :**
- Durée du projet :
 - 2 ans : du 1/09/2008 au 31/08/2010
- Responsables :
 - Saïd Amari (LURPA)
 - Thomas Chatain (LSV)

Projet CRAFT : Critical Risks Analysis by Fault Trees

L'objectif global du projet est de coupler des approches déterministes et des approches stochastiques pour améliorer l'efficacité des techniques d'analyse des défaillances critiques des systèmes industriels, basées sur des arbres de défaillance dynamiques.

Ce projet visait à explorer une approche originale, combinant des outils et des modèles déterministes et stochastiques, qui pourrait constituer une alternative performante aux approches existantes dans ce domaine. Il s'agit d'une part d'explorer l'apport du model-checking pour la détermination des séquences de coupes de l'arbre de défaillance, et d'autre part d'explorer comment des méthodes récentes issues de la théorie de l'apprentissage, telles le boosting ou les Support Vector Machines, permettraient de calculer la probabilité de défaillance du système à partir de la connaissance de ces séquences de coupe et de la donnée des probabilités de défaillances des composants élémentaires.

- **Caractéristiques du projet :**
- Durée du projet :
 - 2 ans : du 1/09/2008 au 31/08/2010
- Responsables :
 - Jean-Jacques Lesage (LURPA)
 - Laurent Fribourg (LSV)
 - Nicolas Vayatis (CMLA)

¹ Olivier De Smet a quitté le LURPA le 1^{er} janvier 2012 pour intégrer le Laboratoire de Mécanique des Structures et des Systèmes Couplés du CNAM, son établissement de rattachement.

9. Formation par la recherche

9.1. Formation initiale

Les enseignants-chercheurs de l'Équipe ISA sont rattachés à 3 établissements d'enseignement distincts : l'ENS Cachan, SupMéca à Saint-Ouen et l'IUT de Saint-Denis. Ils participent à la formation en premier, second et troisième cycle en assurant une part importante des enseignements en automatique des Systèmes à Événements Discrets dispensés dans ces établissements :

- **Au département Génie Mécanique de l'ENS Cachan :**
 - Au niveau Licence L3 « Sciences Appliquées en PHysique et Ingénierie pour la Recherche et l'Enseignement »,
 - au niveau Master M1 « Ingénierie Numérique de la Production » et Master M1 « Mécanique des matériaux et des structures »
 - au niveau Master M2P « Formation des enseignants pour le supérieur ».
- **Au département EEA (Électronique, Électrotechnique et Automatique) de l'ENS Cachan :**
 - au niveau Master M2P « Formation des enseignants pour le supérieur ».
- **À SupMéca :**
 - au niveau L3 (tronc commun) et M1, spécialités «Systèmes de Production et Logistique» et «Mécatronique»
- **Au département GMP de l'IUT de Saint-Denis :**
 - Au niveau DUT et en licence professionnelle

9.2. Formation en Master Recherche

Pour l'ENS Cachan, la formation à, et par, la recherche est une priorité. L'un des objectifs principaux de formation de ses départements est l'orientation de très bons élèves issus de classes préparatoires aux grandes écoles vers les carrières de la recherche et de l'enseignement supérieur.

L'Équipe ISA est naturellement fortement impliquée dans un master Recherche porté par l'ENS Cachan. Il s'agit du **Master Recherche ISC « Ingénierie des Systèmes Complexes »** proposé par l'Université de Lorraine et co-habilité par l'ENS Cachan.

D'un point de vue administratif, seul le parcours Recherche de la **spécialité S3A « Spécialité Sûreté et Sécurité active des systèmes »** est ouvert à l'ENS Cachan.

Pour la période considérée, Jean-Jacques Lesage est le responsable de la formation pour l'ENS Cachan tandis que Jean-Marc Roussel assure la responsabilité pédagogique.

Habilitations du Master Recherche

Pour la période considérée, le master Recherche dans lequel l'Équipe ISA est impliquée, a naturellement évolué au rythme des différentes habilitations de l'Université de Lorraine. Il s'est nommé :

- **Master IS en EEAPR (Ingénierie Système en EEA et Production & Réseaux) :**
 - Habilitation pour 4 ans pour les années universitaires 2005/2006 à 2008/2009.
- **Master ISC, Spécialité S3A :**
 - Habilitation pour 4 ans pour les années universitaires 2009/2010 à 2012/2013,
 - Habilitation pour 4 ans pour les années universitaires 2013/2014 à 2016/2017.

Formation dispensée

Les enseignements de ce parcours Recherche sont principalement dispensés en visio-conférence entre Cachan et Nancy selon l'origine de l'enseignant qui les dispense. Toute la formation est dispensée en français. Pour les étudiants inscrits à Cachan en septembre 2012, les 60 ECTS de la formation se sont répartis de la manière suivante :

- **Cours en visio-conférence depuis Cachan (6 ECTS)**
 - MAIC3U37 - Dependable systems design and analysis (3 ECTS)
 - MAIC3U39 - Dependable control of discrete event systems (3 ECTS)

- **Cours en visio-conférence depuis Nancy (15 ECTS)**
 - MAIC3C03 - Real-Time Systems and Scheduling Theory (3 ECTS)
 - MAIC3C09 - Network modelling (3 ECTS)
 - MAIC3C11 - Quality of Service (3 ECTS)
 - MAIC3U32 - Formal Systems Engineering (3 ECTS)
 - MAIC3U36 - Probabilistic model in reliability analysis for multi-components (3 ECTS)
- **Cours dispensés à Cachan (21 ECTS)**
 - MAIC3U17 - Learning Research by Doing (12 ECTS)
 - MAIC4U01 - Scientific communication in English (6 ECTS)
 - MAIC3UZ - Algebraic approaches to the design and analysis of dependable system (3 ECTS)
- **Stage de recherche (18 ECTS)**
 - Le stage peut avoir lieu au sein du LURPA, dans un autre laboratoire de Recherche ou en entreprise.

Équipements de visio-conférence dédiés

Tous les enseignements se font au sein des locaux du LURPA. Le laboratoire dispose de sa propre salle de visio-conférence mis à la disposition du Master ISC en priorité. Les équipements informatiques de cette salle sont identiques à ceux du CRAN, notre partenaire à Nancy¹. Cette salle est équipée :

- d'un tableau numérique interactif pour :
 - l'animation des supports de cours,
 - les travaux sur tableaux blancs,
- de caméras pour filmer :
 - l'enseignant lorsque le cours est dispensé depuis Cachan,
 - les étudiants lors le cours est dispensé depuis Nancy,
- de différents équipements de prise de son,
- de deux logiciels de visio-conférence :
 - le logiciel StarBoard pour la synchronisation des tableaux numériques,
 - le logiciel Connect Pro d'Adobe pour la gestion du son et de l'image : Le master dispose de son propre salon virtuel hébergé sur le serveur de l'ENS Cachan.

Devenir des étudiants

Le devenir des étudiants à l'issue du master Recherche est une préoccupation de toute l'équipe pédagogique. Une page du site WWW du Master est d'ailleurs consacrée à [ce suivi](#). Pour la période considérée, sur les **23 étudiants** inscrits à Cachan, nous avons eu :

- 1 abandon lors de l'année universitaire 2008/2009,
- 1 redoublement² à l'issue de l'année universitaire 2011/2012,
- **21 poursuites en thèse :**
 - 10 au sein du LURPA,
 - 9 au sein d'un autre laboratoire français :
 - au CITI à Lyon,
 - au MIPS à Mulhouse,
 - au LIRMM à Montpellier,
 - au LIP6 à Paris,
 - au ERPI à Nancy,
 - au CRAN à Nancy après un stage de recherche prédoctoral au Department of Electrical Engineering and Computer Science, University of Michigan (USA),
 - au LIASD à Paris,
 - à l'iFSTTAR à Lille,
 - à l'INRIA à Grenoble.
 - 2 à l'étranger :

¹ La salle de visio-conférence à Nancy est hébergée par le pôle AIP-Priméca lorrain.

² Les résultats de l'étudiant lors de l'année universitaire 2012/2013 lui ont permis d'obtenir son diplôme en juillet 2013.

- au Département de génie électrique et informatique de l'Université du Kentucky (USA),
- au Department 7.4 Mechatronics Engineering, Saarland University (Allemagne).

Sur la période considérée, tous les étudiants ayant eu une scolarité sans incident sont aujourd'hui docteurs ou inscrits en thèse.

10. Publications, thèses, masters

10.1. Articles dans des revues à comité de lecture à diffusion internationale

Le facteur d'impact indiqué est celui du « **ISI Web of Knowledge, Journal Citation Report** » à la date de constitution ce dossier.

- [ACL 1] [Probabilistic algebraic analysis of Fault Trees with priority dynamic gates and repeated events](#), G. Merle, J.-M. Roussel, J.-J. Lesage, A. Bobbio, IEEE Trans. on Reliability, **59(1)**, pp. 250-261, DOI: 10.1109/TR.2009.2035793, March 2010, (IF JCR: 1,285)
- [ACL 2] [A comparative analysis of recent identification approaches for discrete-event systems](#), A.-P. Estrada-Vargas, E. Lopez-Mellado, J.-J. Lesage, Mathematical Problems in Engineering, Vol. 2010, Article ID 453254, 21 pages, DOI: 10.1155/2010/453254, April 2010, (IF JCR: 0,777)
- [ACL 3] [Analytic calculus of response time in networked automation systems](#), B. Addad, S. Amari, J.-J. Lesage, IEEE Trans. on Automation Science and Engineering, **7(4)**, pp. 858-869, DOI: 10.1109/TASE.2010.2047499, October 2010, (IF JCR: 1,461)
- [ACL 4] [Verification of a timed multitask system with Uppaal](#), H. Bel Mpkadem, B. Berard, V. Gourcuff, O. De Smet, J.-M. Roussel, IEEE Trans. on Automation Science and Engineering, **7(4)**, pp. 921-932, DOI: 10.1109/TASE.2010.2050199, October 2010, (IF JCR: 1,461)
- [ACL 5] [Algebraic determination of the structure function of Dynamic Fault Trees](#), G. Merle, J.-M. Roussel, J.-J. Lesage, Reliability Engineering and System Safety, **96(2)**, pp. 267-277, DOI: 10.1016/j.ress.2010.10.001, February 2011, (IF JCR: 1,77)
- [ACL 6] [Genetic algorithms for delays evaluation in networked automation systems](#), B. Addad, S. Amari, J.-J. Lesage, Engineering Applications of Artificial Intelligence, **24(3)**, pp. 485-490, DOI: 10.1016/j.engappai.2010.10.017, April 2011, (IF JCR: 1,665)
- [ACL 7] [Client-Server networked automation systems reactivity: deterministic and probabilistic analysis](#), B. Addad, S. Amari, J.-J. Lesage, IEEE Trans. on Automation Science and Engineering, **8(3)**, pp. 540-548, DOI: 10.1109/TASE.2011.2116118, July 2011, (IF JCR: 1,461)
- [ACL 8] [A virtual queuing based algorithm for delays evaluation in networked control systems](#), B. Addad, S. Amari, J.-J. Lesage, IEEE Trans. on Industrial Electronics, **58(9)**, pp. 4471-4479, DOI: 10.1109/TIE.2010.2098358, September 2011, (IF JCR: 5,16)
- [ACL 9] [Translating Grafcet specifications into Mealy machines for conformance test purposes](#), J. Provost, J.-M. Roussel, J.M. Faure, Control Engineering Practice, **19(9)**, pp. 947-957, DOI: 10.1016/j.conengprac.2010.10.001, September 2011, (IF JCR: 1,481)
- [ACL 10] [The concept of residuals for fault localization in discrete event systems](#), M. Roth, J.-J. Lesage, L. Litz, Control Engineering Practice, **19(9)**, pp. 978-988, DOI: 10.1016/j.conengprac.2011.02.008, September 2011, (IF JCR: 1,481)
- [ACL 11] [Control of discrete event systems with respect to strict duration: Supervision of an industrial manufacturing plant](#), A. Atto, C. Martinez, S. Amari, Computers & Industrial Engineering, **61(4)**, pp. 1149-1159, DOI: 10.1016/j.cie.2011.07.004, September 2011, (IF JCR: 1,589)
- [ACL 12] [Max-Plus Control Design for Temporal Constraints Meeting in Timed Event Graphs](#), S. Amari, I. Demongodin, J.J. Loiseau, C. Martinez, IEEE Trans. on Automatic Control, **57(2)**, pp. 462-467, DOI: 10.1109/TAC.2011.2164735, February 2012
- [ACL 13] [Fault detection and isolation in manufacturing systems with an identified discrete event model](#), M. Roth, S. Schneider, J.-J. Lesage, L. Litz, Int. Journal of Systems Science, **43(10)**, pp. 1826-1841, DOI: 10.1080/00207721.2011.649369, October 2012, (IF JCR: 0,991)
- [ACL 14] [Networked conflicting timed event graphs representation in \(Max,+\) algebra](#), B. Addad, S. Amari, J.-J. Lesage, Discrete Event Dynamic Systems, **22(4)**, pp. 429-449, December 2012, (IF JCR: 0,641)
- [ACL 15] [Building meaningful timed models of closed-loop DES for verification purposes](#), M. Perin, J.M. Faure, Control Engineering Practice, 20 pages, DOI: 10.1016/j.conengprac.2012.05.002,, available online since August 2012, (IF JCR: 1,481)

- [ACL 16] *Input-output identification of controlled discrete manufacturing systems*, A.-P. Estrada-Vargas, J.-J. Lesage, E. Lopez-Mellado, *Int. Journal of Systems Science*, 16 pages, DOI: 10.1080/00207721.2012.724098, available online since September 2012, (IF JCR: 0,991)
- [ACL 17] *Quantitative Analysis of Dynamic Fault Trees based on the Structure Function*, G. Merle, J.-M. Roussel, J.-J. Lesage, *Reliability Engineering International*, **29(8)**, 14 pages, DOI: 10.1002/qre.1487, available online since January 2013, (IF JCR: 0,7)

10.2. Brevets

- [BRE 1] [Procédé pour la conception et la fabrication d'une chaîne de composants en réseau et réseau obtenu par un tel procédé](#), D. Aza-Vallina, N. Chevassus (EADS), B. Dantin (EADS), B. Denis, J.M. Faure, 14 décembre 2012

10.3. Conférences plénières ou invitées

- [CINV 1] *Conformance test of logic controllers*, J.-M. Faure, *Workshop on Model Integrated Mechatronics, University of Saarbrücken (Germany), January 2011*
- [CINV 2] *Improving dependability of controlled systems: a challenge for automation science and engineering*, J.-M. Faure, J.-J. Lesage, *8th Int. Conf. on Informatics in Control Automation and Robotics (ICINCO'11), Noordwijkerhout (The Netherlands), July 2011*
- [CINV 3] *Tailor-made vs. formal languages: how to reconcile effectiveness and rigor of modelling for automation engineering*, J.-J. Lesage, *Plenary keynote paper, 5th Int. Workshop on Verification and Evaluation of Computer and Communication Systems (VECOS'11), Tunis (Tunisia), September 2011*
- [CINV 4] *Equipment of tailor-made languages with formal framework: the case of two industrial tools for Safety Analysis*, J.-J. Lesage, *Invited talk, Annual Research Seminary of the Faculty of Informatics, Univ. Magdeburg (Germany), September 2011*

10.4. Communications dans des congrès internationaux avec actes

- [CAI 1] [Algebraic Synthesis of Transition Conditions of a State Model](#), Y. Hietter, J.-M. Roussel, J.-J. Lesage, *9th International Workshop On Discrete Event Systems (WODES 2008), Göteborg (Sweden), pp. 187-192, May 2008*
- [CAI 2] [Reactive control system design using the Supervisory Control Theory: evaluation of possibilities and limits](#), M. Cantarelli, J.-M. Roussel, *9th International Workshop On Discrete Event Systems (WODES 2008), Göteborg (Sweden), pp. 200-205, May 2008*
- [CAI 3] [Supervision of an industrial plant subject to a maximal duration constraint](#), A. Atto, C. Martinez, S. Amari, *9th International Workshop On Discrete Event Systems (WODES 2008), Göteborg (Sweden), pp. 254-259, May 2008*
- [CAI 4] [Building effective formal models to prove time properties of networked automation systems](#), S. Ruel, O. de Smet, J.M. Faure, *9th International Workshop On Discrete Event Systems (WODES 2008), Göteborg (Sweden), pp. 334-339, May 2008*
- [CAI 5] [Response time evaluation in Ethernet-based automation architectures](#), B. Addad, S. Amari, *2nd International Workshop on Verification and Evaluation of Computer and Communication Systems (VECOS 2008), Leeds (England), 11 pages, July 2008*
- [CAI 6] [Algebraic synthesis of dependable logic controllers](#), Y. Hietter, J.-M. Roussel, J.-J. Lesage, *17th IFAC World Congress, Seoul (Korea), pp. 4132-4137, July 2008*
- [CAI 7] [Improving large-sized PLC programs verification using abstractions](#), V. Gourcuff, O. de Smet, J.M. Faure, *17th IFAC World Congress, Seoul (Korea), pp. 5101-5106, July 2008*
- [CAI 8] [Efficient representation for formal verification of time performances of networked automation architectures](#), S. Ruel, O. de Smet, J.M. Faure, *17th IFAC World Congress, Seoul (Korea), pp. 5119-5124, July 2008*
- [CAI 9] [Modelling and Response Time Evaluation of Ethernet-based Automation Architectures using Max-Plus Algebra](#), B. Addad, S. Amari, *4th IEEE Int. Conf. on Automation Science and Engineering (CASE 2008), Washington DC (USA), pp. 418-423, August 2008*
- [CAI 10] [Delay Evaluation and Compensation in Ethernet-Networked Control Systems](#), B. Addad, S. Amari, *16th International Conference on Real-Time and Network Systems (RTNS 2008), Rennes (France), 10 pages, October 2008*

- [CAI 11] [Algebraic expression of the structure function of a subclass of Dynamic Fault Trees](#), G. Merle, J.-M. Roussel, J.-J. Lesage, A. Bobbio, *2nd IFAC Workshop on Dependable Control of Discrete Systems (DCDS 2009), Bari (Italy)*, pp. 129-134, June 2009
- [CAI 12] [Test sequence construction from SFC specification](#), J. Provost, J.-M. Roussel, J.M. Faure, *2nd IFAC Workshop on Dependable Control of Discrete Systems (DCDS 2009), Bari (Italy)*, pp. 341-346, June 2009
- [CAI 13] [A residual inspired approach for fault localization in DES](#), M. Roth, J.-J. Lesage, L. Litz, *2nd IFAC Workshop on Dependable Control of Discrete Systems (DCDS 2009), Bari (Italy)*, pp. 347-352, June 2009
- [CAI 14] [Building meaningful timed plant models for verification purposes](#), M. Perin, J.M. Faure, *13th IFAC symposium on Information Control Problems in Manufacturing (INCOM 2009), Moscow (Russia)*, pp. 970-975, June 2009
- [CAI 15] [Finding the bounds of response time of networked automation systems by iterative proofs](#), S. Ruel, O. de Smet, J.M. Faure, *13th IFAC symposium on Information Control Problems in Manufacturing (INCOM 2009), Moscow (Russia), June 2009*
- [CAI 16] [An FDI Method for Manufacturing Systems Based on an Identified Model](#), M. Roth, J.-J. Lesage, L. Litz, *13th IFAC symposium on Information Control Problems in Manufacturing (INCOM 2009), Moscow (Russia)*, pp. 1389-1394, June 2009, **Best paper Award of the track "Discrete Event Systems"**
- [CAI 17] [Distributed identification of concurrent discrete event systems for fault detection purposes](#), M. Roth, J.-J. Lesage, L. Litz, *10th European Control Conference 2009 (ECC 2009), Budapest (Hungary)*, pp. 2590-2595, August 2009
- [CAI 18] [Off-line identification of concurrent discrete event systems exhibiting cyclic behaviour](#), A.-P. Estrada-Vargas, E. Lopez-Mellado, J.-J. Lesage, *IEEE Int. Conf. on Systems Man and Cybernetics (SMC 2009), San Antonio (USA)*, pp. 181-186, October 2009
- [CAI 19] [Identification of discrete event systems: Implementation issues and model completeness](#), M. Roth, L. Litz, J.-J. Lesage, *7th Int. Conf. on Informatics in Control Automation and Robotics (ICINCO 2010), Funchal (Portugal)*, pp. 73-80, June 2010
- [CAI 20] [Black-box identification of discrete event systems with optimal partitioning of concurrent subsystems](#), M. Roth, J.-J. Lesage, L. Litz, *American Control Conference (ACC 2010), Baltimore (USA)*, pp. 2601-2606, July 2010, **Best paper Award of the track "Discrete Event Systems"**
- [CAI 21] [SIC-testability of sequential logic controllers](#), J. Provost, J.-M. Roussel, J.M. Faure, *10th International Workshop On Discrete Event Systems (WODES 2010), Berlin (Germany)*, pp. 203-208, September 2010
- [CAI 22] [Linear time-varying \(max,+\) representation of conflicting timed event graphs](#), B. Addad, S. Amari, J.-J. Lesage, *10th International Workshop On Discrete Event Systems (WODES 2010), Berlin (Germany)*, pp. 310-315, September 2010
- [CAI 23] [Analytical Calculation of Failure Probabilities in Dynamic Fault Trees including Spare Gates](#), G. Merle, J.-M. Roussel, J.-J. Lesage, N. Vayatis, *19th European Safety & Reliability Conf. (ESREL 2010), Rhodes (Greece)*, pp. 794-801, September 2010
- [CAI 24] [Improving the Efficiency of Dynamic Fault Tree Analysis by Considering Gates FDEP as Static](#), G. Merle, J.-M. Roussel, J.-J. Lesage, *19th European Safety & Reliability Conf. (ESREL 2010), Rhodes (Greece)*, pp. 845-851, September 2010
- [CAI 25] [Conformance test of logic controllers of critical systems from industrial specifications](#), F. Chériaux, L. Picci, J. Provost, J.M. Faure, *19th European Safety & Reliability Conf. (ESREL 2010), Rhodes (Greece)*, pp. 1569-1576, September 2010
- [CAI 26] [Control of Time-Constrained Dual-Armed Cluster Tools Using \(max, +\) Algebra](#), R. Attia, S. Amari, C. Martinez, *Conference on Control and Fault-Tolerant Systems (SysTol 2010), Nice (France)*, 6 pages, October 2010
- [CAI 27] [An identification method for PLC-based automated discrete event systems](#), A.-P. Estrada-Vargas, E. Lopez-Mellado, J.-J. Lesage, *49th IEEE Conf. on Decision and Control (CDC 2010), Atlanta (USA)*, pp. 6740-6746, December 2010
- [CAI 28] [Dynamic Fault Tree analysis based on the structure function](#), G. Merle, J.-M. Roussel, J.-J. Lesage, *Annual Reliability and Maintainability Symposium 2011 (RAMS 2011), Lake Buena Vista (USA)*, pp. 462-467, January 2011
- [CAI 29] [Testing Programmable Logic Controllers from Finite State Machines Specification](#), J. Provost, J.-M. Roussel, J.M. Faure, *3rd IFAC Int. Workshop on Dependable Control of Discrete Systems (DCDS 2011), Saarbrücken (Germany)*, pp. 3-8, June 2011

- [CAI 30] [A comparative study of three model-based FDI approaches for Discrete Event Systems](#), M. Danancher, M. Roth, J.-J. Lesage, L. Litz, 3rd IFAC Int. Workshop on Dependable Control of Discrete Systems (DCDS 2011), Saarbrücken (Germany), pp. 29-34, June 2011
- [CAI 31] [Timed Residuals for Fault Detection and Isolation in Discrete Event Systems](#), S. Schneider, L. Litz, M. Danancher, 3rd IFAC Int. Workshop on Dependable Control of Discrete Systems (DCDS 2011), Saarbrücken (Germany), pp. 35-40, June 2011
- [CAI 32] [Designing operational control architectures of critical systems by reachability analysis](#), T. Lemattre, B. Denis, J.M. Faure, J.-F. Pétrin, P. Salaün, 7th IEEE Int. Conf. on Automation Science and Engineering (CASE 2011), Trieste (Italy), pp. 12-18, August 2011
- [CAI 33] [A formal semantics for Grafcet specifications](#), J. Provost, J.-M. Roussel, J.M. Faure, 7th IEEE Int. Conf. on Automation Science and Engineering (CASE 2011), Trieste (Italy), pp. 488-494, August 2011
- [CAI 34] [Measures vs. Analytic Evaluation of Response Time of Networked Automation Systems](#), B. Addad, S. Amari, J.-J. Lesage, B. Denis, 7th IEEE Int. Conf. on Automation Science and Engineering (CASE 2011), Trieste (Italy), pp. 576-581, August 2011, **Best paper Award finalist**
- [CAI 35] [Using a meta-model to build operational architectures of automation systems for critical processes](#), T. Lemattre, B. Denis, J.M. Faure, J.-F. Pétrin, P. Salaün, 16th IEEE Int. Conf. on Emerging Technologies and Factory Automation (ETFA 2011), Toulouse (France), Paper n°175, 6 pages, September 2011
- [CAI 36] [Stepwise Identification of Automated Discrete Manufacturing Systems](#), A.-P. Estrada-Vargas, J.-J. Lesage, E. Lopez-Mellado, 16th IEEE Int. Conf. on Emerging Technologies and Factory Automation (ETFA 2011), Toulouse (France), Paper N°4-6, 8 pages, September 2011, **Best paper Award of the conference**
- [CAI 37] [Qualitative analysis of a BDMP by finite automata](#), P.-Y. Chaux, J.-M. Roussel, J.-J. Lesage, G. Deleuze, M. Bouissou, 20th European Safety & Reliability Conf. (ESREL 2011), Troyes (France), In "Advances in Safety Reliability and risk management", Taylor & Francis Ed., pp. 2055-2057, September 2011
- [CAI 38] [Communications reliability analysis in networked embedded systems](#), D. Aza-Vallina, B. Denis, J.M. Faure, 20th European Safety & Reliability Conf. (ESREL 2011), Troyes (France), In "Advances in Safety Reliability and risk management", Taylor & Francis Ed., pp. 2639-2646, September 2011
- [CAI 39] Translation from Petri nets into Boolean equations for the algebraic design of logic controllers, M. Diaz-Rodriguez, E. Lopez-Mellado, P.-A. Brameret, J.-M. Roussel, 8th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE 2011), Merida (Mexico), 6 pages, October 2011
- [CAI 40] [Identification of Industrial Automation Systems: Building Compact and Expressive Petri Net Models from Observable Behavior](#), A.-P. Estrada-Vargas, J.-J. Lesage, E. Lopez-Mellado, American Control Conference (ACC 2012), Montreal (Canada), pp. 6095-6101, June 2012
- [CAI 41] [Systematic extraction of Minimal Cut Sequences from a BDMP model](#), P.-Y. Chaux, J.-M. Roussel, J.-J. Lesage, G. Deleuze, M. Bouissou, 21th European Safety & Reliability Conf. (ESREL 2012), Helsinki (Finland), Paper 16B-We4-3 8 pages, June 2012
- [CAI 42] [Influence of bus partitioning on the reliability of transmissions](#), D. Aza-Vallina, B. Denis, J.M. Faure, 21th European Safety & Reliability Conf. (ESREL 2012), Helsinki (Finland), Paper 02-Mo2-4 10 pages, June 2012
- [CAI 43] [Indoor Location Tracking based on a Discrete Event Model](#), M. Danancher, J.-J. Lesage, L. Litz, 10th Int. Conf. On Smart homes and health Telematics (ICOST 2012), Artimino (Italy), Lecture Notes in Computer Science 7251, pp. 262-265, June 2012
- [CAI 44] [Algebraic synthesis of logical controllers with optimization criteria](#), H. Leroux, J.-M. Roussel, 6th International Workshop on Verification and Evaluation of Computer and Communication Systems (VECOS 2012), Paris (France), pp. 103-114, August 2012
- [CAI 45] [Coupling timed plant and controller models with urgent transitions without introducing deadlocks](#), M. Perin, J.M. Faure, 17th IEEE Int. Conf. on Emerging Technologies & Factory Automation (ETFA 2012), Krakow (poland), September 2012
- [CAI 46] [Algebraic synthesis of logical controllers despite inconsistencies in specifications](#), J.-M. Roussel, J.-J. Lesage, 11th Int. Workshop on Discrete Event Systems (WODES 2012), Guadalajara (Mexico), pp. 307-314, October 2012
- [CAI 47] [Determination of Timed Transitions in Identified Discrete-Event Models for Fault Detection](#), S. Schneider, L. Litz, J.-J. Lesage, 51st IEEE Annual Conference on Decision and Control (CDC 2012), Grand Wailea Maui HI (USA), pp. 5816-5821, December 2012

Pour information, communications acceptées et planifiées à l'issue de la période de référence

- [CAI 48] [Automated Modeling of Reactive Discrete Event Systems from External Behavioral Data](#), A.-P. Estrada-Vargas, J.-J. Lesage, E. Lopez-Mellado, *23rd Int. Conf. on Electronics, Communications and Computing (CONIELECOMP 2013)*, Cholula Puebla (Mexico), pp. 120-123, March 2013
- [CAI 49] [A meta-model for integrating safety concerns into systems engineering processes](#), P.Y. Piriou, J.M. Faure, G. Deleuze, *7th IEEE International Systems Conference (SysCon 2013)*, Orlando (USA), pp. 298-304, April 2013
- [CAI 50] [A Discrete Event Model for Multiple Inhabitants Location Tracking](#), M. Danancher, J.-J. Lesage, L. Litz, G. Faraut, *9th IEEE Int. Conf. on Automation Science and Engineering (CASE 2013)*, Madison-Wisconsin (USA), pp 922-927, August 2013
- [CAI 51] Comparing detailed and abstract timed models of automated discrete manufacturing systems, M. Perin, J.M. Faure, *9th IEEE Int. Conf. on Automation Science and Engineering (CASE 2013)*, Madison-Wisconsin (USA), pp 928-933, August 2013
- [CAI 52] [Towards an unified definition of Minimal Cut Sequences](#), P.-Y. Chauv, J.-M. Roussel, J.-J. Lesage, G. Deleuze, M. Bouissou, *4th IFAC Workshop on Dependable Control of Discrete Systems (DCDS 2013)*, York (United Kingdom), Paper n°1, 6 pages, September 2013
- [CAI 53] [Preliminary System Safety Analysis with Limited Markov Chain Generation](#), P.-A. Brameret, J.-M. Roussel, A. Rauzy, *4th IFAC Workshop on Dependable Control of Discrete Systems (DCDS 2013)*, York (United Kingdom), Paper n°3, 6 pages, September 2013
- [CAI 54] [An analytic expression of the reliability of transmissions in fieldbuses with propagated failures](#), D. Aza-Vallina, J.M. Faure, *4th IFAC Workshop on Dependable Control of Discrete Systems (DCDS 2013)*, York (United Kingdom), Paper n°18, 6 pages, September 2013
- [CAI 55] [The AltaRica 3.0 Project for Model-based Safety Assessment](#), T. Prosvirnova, M. Batteux, P.-A. Brameret, L. Kloul, A. Cherfi, T. Friedlhuber, J.-M. Roussel, A. Rauzy, *4th IFAC Workshop on Dependable Control of Discrete Systems (DCDS 2013)*, York (United Kingdom), Paper n°22, 6 pages, September 2013
- [CAI 56] Identification of Partially Observable Discrete Event Manufacturing Systems, A.-P. Estrada-Vargas, E. Lopez-Mellado, J.-J. Lesage, *18th IEEE Int. Conf. on Emerging Technologies and Factory Automation (ETFA 2013)*, Cagliari (Italy), Paper n°83, 7 pages, September 2013
- [CAI 57] [Enforcing I/O sequences for PLC validation purposes](#), A. Guignard, J.M. Faure, *18th IEEE Int. Conf. on Emerging Technologies and Factory Automation (ETFA 2013)*, Cagliari (Italy), Paper n°89, 6 pages, September 2013
- [CAI 58] [A DES Simulator for Location Tracking of Inhabitants in Smart Home](#), M. Danancher, G. Faraut, J.-J. Lesage, L. Litz, *8th EUROSIM Congress on Modelling and Simulation (EUROSIM'13)*, Cardiff-Wales (United Kingdom), pp. 330-335, September 2013

10.5. Communications dans des congrès francophones avec actes

- [CAN 1] [Calcul des conditions de transition d'un Réseau de Petri par synthèse algébrique](#), Y. Hietter, J.-M. Roussel, J.-J. Lesage, *5ème Conférence Internationale Francophone d'Automatique (CIFA 2008)*, Bucarest (Roumanie), Papier n°83 6 pages, Septembre 2008
- [CAN 2] [Commande d'un système de production à temps critique](#), S. Amari, C. Martinez, *5ème Conférence Internationale Francophone d'Automatique (CIFA 2008)*, Bucarest (Roumanie), Papier n°269 6 pages, Septembre 2008
- [CAN 3] [Analyse prévisionnelle des fautes des systèmes embarqués discrets par vérification model-based](#), M. Perin, J.M. Faure, *5ème Conférence Internationale Francophone d'Automatique (CIFA 2008)*, Bucarest (Roumanie), Papier n°381 6 pages, Septembre 2008
- [CAN 4] [Réseaux d'automates hybrides à synchronisations typées pour la modélisation des SDH](#), Z. Juarez Orozco, B. Denis, J.-J. Lesage, *5ème Conférence Internationale Francophone d'Automatique (CIFA 2008)*, Bucarest (Roumanie), Papier n°396 6 pages, Septembre 2008
- [CAN 5] [Construction d'une séquence de test minimale à partir d'une spécification GRAFCET](#), J. Provost, J.-M. Roussel, J.M. Faure, *3ièmes Journées Doctorales du GDR MACS 2009*, Angers, Papier n°19 6 pages, Mars 2009
- [CAN 6] [Modélisation et évaluation temporelle des architectures de commande en réseau](#), B. Addad, S. Amari, *3ièmes Journées Doctorales du GDR MACS 2009*, Angers, Papier n°25 6 pages, Mars 2009
- [CAN 7] [Test exhaustif de contrôleurs logiques spécifiés en Grafcet : apports et limites d'une modélisation par machines de Mealy](#), J. Provost, J.-M. Roussel, J.M. Faure, *7ème colloque francophone sur la Modélisation des Systèmes*

Réactifs (MSR 2009), Nantes, Dans N° spécial du Journal Européen des Systèmes Automatisés, 43(7-8-9), pp. 889-904, Novembre 2009

- [CAN 8] [Evaluation de délais dans les systèmes de communication temps-réel en utilisant des files d'attente virtuelles](#), B. Addad, S. Amari, J.-J. Lesage, 7ème colloque francophone sur la Modélisation des Systèmes Réactifs (MSR 2009), Nantes, Dans N° spécial du Journal Européen des Systèmes Automatisés, 43(7-8-9), pp. 985-1000, Novembre 2009
- [CAN 9] [Modélisation de réseaux de graphes d'événements temporisés avec conflits dans l'algèbre \(Max,+\)](#), B. Addad, S. Amari, J.-J. Lesage, 6ème IEEE Conférence Internationale Francophone d'Automatique (CIFA 2010), Nancy, Papier n°22 6 pages, Juin 2010
- [CAN 10] *Comparaison de deux méthodes dynamiques d'évaluation de la sureté de fonctionnement :BDMP et DFM*, P.-Y. Chauv, 17ème Congrès de Maîtrise des Risques et Sûreté de Fonctionnement (LambdaMu 17), La Rochelle, Papier n° 4C-2 9 pages, Octobre 2010
- [CAN 11] [Un démonstrateur pour le test de conformité de contrôleurs logiques](#), J. Provost, J.-M. Roussel, J.M. Faure, 3èmes Journées Démonstrateurs du club EEA, , 10 pages, Novembre 2010
- [CAN 12] [Diagnostic des SED basé sur un modèle : trois approches évaluées sur une même étude de cas](#), M. Danancher, M. Roth, J.-J. Lesage, L. Litz, 4ièmes Journées Doctorales du GDR MACS 2014, Marseille, pp. 165-170, Juin 2011
- [CAN 13] [Formalisation des scénarios de défaillance d'un BDMP par automate fini](#), P.-Y. Chauv, J.-M. Roussel, J.-J. Lesage, 4ièmes Journées Doctorales du GDR MACS 2011, Marseille, pp. 459-464, Juin 2011
- [CAN 14] [Prise en compte de différents modes de défaillance des composants réseau dans l'évaluation de la fiabilité des transmissions](#), D. Aza-Vallina, B. Denis, J.M. Faure, 4ièmes Journées Doctorales du GDR MACS 2012, Marseille, pp. 263-268, Juin 2011
- [CAN 15] [Aide à la conception d'architectures opérationnelles de commande de systèmes critiques par analyse d'atteignabilité](#), T. Lemattre, B. Denis, J.M. Faure, J.-F. Pétin, P. Salaun, 4ièmes Journées Doctorales du GDR MACS 2013, Marseille, pp. 447-452, Juin 2011
- [CAN 16] *Modélisation et commande d'une architecture d'automatisation en réseau sous contrainte temporelle en utilisant l'algèbre Min-Plus*, K. Tebani, S. Amari, R. Kara, 9th International Conference on Modeling, Optimization & SIMulation (MOSIM 2012), Bordeaux, Papier n°173, Juin 2012
- [CAN 17] [Génération d'une machine de Mealy à partir de spécifications algébriques à des fins de test de conformité](#), A. Guignard, J.-M. Roussel, J.M. Faure, 7ème IEEE Conférence Internationale Francophone d'Automatique (CIFA 2012), Grenoble, pp. 907-912, Juillet 2012
- [CAN 18] [Identification de SED au moyen de réseaux de Petri : une approche pour la représentation structurelle des comportements observés](#), A.-P. Estrada-Vargas, J.-J. Lesage, E. Lopez-Mellado, 7ème IEEE Conférence Internationale Francophone d'Automatique (CIFA 2012), Grenoble, pp. 919-924, Juillet 2012
- [CAN 19] *Assessing the Dependability of Systems with Repairable and Spare Components*, P.-A. Brameret, J.-M. Roussel, A. Rauzy, 18ème Congrès de Maîtrise des Risques et Sûreté de Fonctionnement (LambdaMu 18), Tours, Papier 3D-6 9 pages, Octobre 2012

Pour information, communications acceptées et planifiées à l'issue de la période de référence

- [CAN 20] *Commande (Max, +) pour garantir un temps de réponse dans les systèmes de commande en réseau*, K. Tebani, S. Amari, R. Kara, Conférence Internationale sur La Conception & Production Intégrées (CPI 2013), Tlemcen (Algérie), Papier n°246, Octobre 2013
- [CAN 21] *Modélisation et évaluation de performances d'un système d'aiguillage par des graphes d'événements temporisés en conflit*, L. Mameri, S. Amari, R. Kara, Conférence Internationale sur La Conception & Production Intégrées (CPI 2013), Tlemcen (Algérie), Papier n°311, Octobre 2013

10.6. Thèses

- [TH 1] [Vérification de propriétés quantitatives des systèmes logiques par model-checking hybride](#), Z. Juarez-Orozco, Thèse de l'ENS Cachan, 135 pages, 20 juin 2008
- [TH 2] [Architectures de contrôle-commande redondantes à base d'Ethernet Industriel : Modélisation et validation par model-checking temporisé](#), S. Limal, Thèse de l'ENS Cachan, 122 pages, 8 janvier 2009

- [TH 3] [*Synthèse algébrique de lois de commande pour les systèmes à événements discrets logiques*](#), **Y. Hietter**, Thèse de l'ENS Cachan, 162 pages, 28 mai 2009
- [TH 4] [*Evaluation des bornes des performances temporelles des Architectures d'Automatisation en Réseau par preuves itératives de propriétés logiques*](#), **S. Ruel**, Thèse de l'ENS Cachan, 148 pages, 9 juillet 2009
- [TH 5] [*Algebraic modelling of Dynamic Fault Trees, contribution to qualitative and quantitative analysis*](#), **G. Merle**, Thèse de l'ENS Cachan, 218 pages, 7 juillet 2010, **Prix 2009-2010 des meilleures thèses en automatique du GDR MACS et de la section automatique du Club EEA, dans la catégorie « Systèmes à Événements Discrets et Systèmes hybrides »**
- [TH 6] [*Identification and fault diagnosis of industrial closed-loop discrete event systems*](#), **M. Roth**, Thèse en co-tutelle ENS Cachan / Université de Kaiserslautern (Allemagne), 225 pages, 8 octobre 2010
- [TH 7] [*Evaluation analytique du temps de réponse des systèmes de commande en réseau en utilisant l'algèbre \(max,+\)*](#), **B. Addad**, Thèse de l'ENS Cachan, 141 pages, 1 juillet 2011, **Prix 2011-2012 des meilleures thèses en automatique du GDR MACS et de la section automatique du Club EEA, dans la catégorie « Systèmes à Événements Discrets et Systèmes hybrides »**
- [TH 8] [*Test de conformité de contrôleurs logiques spécifiés en Grafcet*](#), **J. Provost**, Thèse de l'ENS Cachan, 170 pages, 8 juillet 2011
- [TH 9] [*Contribution à la modélisation réaliste et multi-échelles des systèmes bouclés temporisés*](#), **M. Perin**, Thèse de l'ENS Cachan, 178 pages, 22 juin 2012
- [TH 10] [*Black-box identification of automated discrete event systems*](#), **A.-P. Estrada-Vargas**, Thèse en co-tutelle ENS Cachan / Cinvestav (Mexique), 122 pages, 20 février 2013
- [TH 11] *Formalisation de la cohérence et calcul des séquences de coupe minimales pour les systèmes dynamiques réparables*, **P.-Y. Chaux**, Thèse de l'ENS Cachan, 148 pages, 15 avril 2013

Pour information, thèses soutenues à l'issue de la période de référence

- [TH 12] *Allocation de fonctions de commande de systèmes critiques par recherche d'atteignabilité dans un réseau d'automates communicants*, **T. Lemattre**, Thèse de l'ENS Cachan, 160 pages, 9 juillet 2013

10.7. Masters

- [M 1] Modeling and Response Time Evaluation of Ethernet-based Control Architectures using Timed Event Graphs and Max-Plus Algebra, **B. Addad**, Mémoire du Master IS en EAAPR de l'ENS Cachan, juillet 2008
- [M 2] Du modèle logique séquentiel à la machine de Mealy à base d'alphabet : une transcription adaptée aux techniques de test, **J. Provost**, Mémoire du Master IS en EAAPR de l'ENS Cachan, juillet 2008
- [M 3] *Apport du model-checking pour l'analyse qualitative de BDMP*, **P.-Y. Chaux**, Mémoire du Master IS en EAAPR de l'ENS Cachan, juillet 2009
- [M 4] Une approche modulaire pour la formalisation en UPPAAL du comportement du SFC, **T. Lemattre**, Mémoire du Master IS en EAAPR de l'ENS Cachan, juillet 2009
- [M 5] *Test des capacités de surveillance d'un contrôleur logique*, **T. Antignac**, Mémoire du Master ISC de l'ENS Cachan, juillet 2010
- [M 6] Commande des systèmes à événements discrets à temps critiques en utilisant l'algèbre des dioïdes et Applications, **R. Attia**, Mémoire du Master ISC de l'ENS Cachan, juillet 2010
- [M 7] *Analyse de fiabilité d'une architecture réseau*, **D. Aza-Vallina**, Mémoire du Master ISC de l'ENS Cachan, juillet 2010
- [M 8] Comparison of three model-based diagnosis methods for Discrete Event Systems, **M. Danancher**, Mémoire du Master ISC de l'ENS Cachan, juillet 2010
- [M 9] Vérification du comportement d'une commande logique implantée dans un FPGA, **M. Quignon**, Mémoire du Master ISC de l'ENS Cachan, juillet 2010
- [M 10] Determining the availability of a system built with repairable components, **P.A. Brameret**, Mémoire du Master ISC de l'ENS Cachan, juillet 2011
- [M 11] Symbolic generation of the automaton representing an algebraic description of a logic system, **A. Guignard**, Mémoire du Master ISC de l'ENS Cachan, juillet 2011

- [M 12] Algebraic synthesis of logical controllers with optimization criteria, **H. Leroux**, Mémoire du Master ISC de l'ENS Cachan, juillet 2011
- [M 13] *Containing Byzantine Failures with Control Zones*, **A. Maurer**, Mémoire du Master ISC de l'ENS Cachan, juillet 2011
- [M 14] Étude des propriétés spectrales des Réseaux de Graphes d'Événements Temporisés en conflits dans l'algèbre Max-Plus, **W. Boussahel**, Mémoire du Master ISC de l'ENS Cachan, juillet 2012
- [M 15] Apport de la Supervisory Control Theory pour l'établissement d'un modèle de maison intelligente, **A. Butez**, Mémoire du Master ISC de l'ENS Cachan, juillet 2012
- [M 16] Génération d'AMDEC et d'Arbres de défaillances à partir de modèles établis en Ingénierie des Systèmes, **P. Mauborgne**, Mémoire du Master ISC de l'ENS Cachan, juillet 2012
- [M 17] Expérimentation d'interopérabilité entre les études fonctionnelles et les études de sûreté de fonctionnement, **P.-Y. Piriou**, Mémoire du Master ISC de l'ENS Cachan, juillet 2012
- [M 18] Algèbre (max, +) pour l'évaluation de performances temporelles des systèmes de commande en réseau producteur/consommateur, **R. Ammour**, Mémoire du Master ISC de l'ENS Cachan, juillet 2013
- [M 19] Réalisation d'un Model-Checker pour la vérification formelle des circuits logiques synchrones en VHDL, **A. Boussif**, Mémoire du Master ISC de l'ENS Cachan, juillet 2013
- [M 20] Délais Pire cas dans les réseaux Ethernet commutés-network calculs, **A. Bouzakaria**, Mémoire du Master ISC de l'ENS Cachan, juillet 2013
- [M 21] Causality analysis for the execution of synchronous data-flow programs, **Y. Geoffroy**, Mémoire du Master ISC de l'ENS Cachan, juillet 2013
- [M 22] Modelling of activities of daily living for online recognition and prediction, **J. Saives**, Mémoire du Master ISC de l'ENS Cachan, juillet 2013