Important
Ce document, hors annexes, ne doit pas dépasser 40 pages, corps de texte en police de taille 11. Ce point constitue un critère de recevabilité de la proposition de projet. Les propositions de projets ne satisfaisant pas aux critères de recevabilité ne seront pas évaluées.

Acronyme / Acronym	**VACSIM**		
Titre du projet	Validation de la commande des systèmes critiques par couplage simulation et méthodes d'analyse formelle		
Proposal title	Validation of critical systems control by coupling simulation and formal analysis methods		
Axe(s) thématique(s) / theme(s)	☐ 1 ☒ 2 ☐ 3 ☒ 4 ☐ 5		
Type de recherche / Type of research	☐ Recherche Fondamentale / Basic Research ☒ Recherche Industrielle / Industrial Research ☐ Développement Expérimental : Experimental Development		
Coopération internationale (si applicable) / International cooperation (if applicable)	Le projet propose une coopération internationale / International cooperation with : ☐ avec un ou des pays spécifiquement mentionnés dans l'appel à projets / countries explicitely cited in the call for proposal ☐ autres pays / other countries		
Aide totale demandée / Grant requested	959 460 €	**Durée du projet / Projet duration**	36 mois

1. RESUME DE LA PROPOSITION DE PROJET / EXECUTIVE SUMMARY

Le projet VACSIM (Validation de la commande des systèmes critiques par couplage simulation et méthodes d'analyse formelle) réunit deux industriels, un concepteur et exploitant de systèmes critiques (EDF R&D) et un éditeur de logiciels d'ingénierie numérique (Dassault Systèmes), et quatre laboratoires : un relevant de l'automatique (LURPA) et trois de l'informatique (I3S, INRIA Rennes, LaBRI). Ce partenariat pluridisciplinaire est nécessaire pour résoudre le problème posé dans ce projet qui consiste à tirer profit des avantages respectifs des techniques de simulation, en incluant des modèles des processus commandés, et des méthodes d'analyse formelles, pour la validation de la commande des systèmes critiques.

Ce projet fait suite au projet ANR TESTEC (TEst des Systèmes Temps réel Embarqués Critiques – 07 TLOG 022) dont le consortium était le même. Ce projet a fourni de nombreux et importants résultats tant académiques qu'industriels. Il a également montré que les seules approches formelles de test et de vérification n'étaient pas suffisantes pour la validation de commandes de systèmes critiques, mais qu'il convenait de s'intéresser à leur couplage avec des approches de simulation, ces deux approches ayant des avantages complémentaires, notamment en termes de capacité à passer à l'échelle et de maîtrise du taux de couverture de l'analyse.

Le nouveau projet vise à développer des contributions de nature à la fois méthodologique (définition de nouveaux modes d'utilisation des simulateurs, règles de couplage simulation/ méthodes formelles) et formelle (adaptation, extension ou création de méthodes formelles) qui permettront la réalisation d'un démonstrateur, sur la base de l'outil ControlBuild, outil d'ingénierie numérique de la société Dassault Systèmes, illustrant, sur la base d'études de cas industriels, les bénéfices du couplage.

Le but ultime du projet est de proposer un **continuum de validation** durant le cycle de vie de la commande des systèmes critiques basé sur des environnements d'ingénierie numérique.

2. CONTEXTE, POSITIONNEMENT ET OBJECTIFS DE LA PROPOSITION / CONTEXT, POSITION AND OBJECTIVES OF THE PROPOSAL

Le projet VACSIM est un projet de recherche industrielle visant à montrer les bénéfices du couplage entre techniques de simulation et méthodes d'analyse formelles pour la validation de la commande des systèmes critiques. Le démonstrateur développé durant le projet, sur la base de l'outil ControlBuild, outil d'ingénierie numérique de la société Dassault Systèmes, permettra d'illustrer ces bénéfices en proposant différents modes de couplage.
La réalisation de ce démonstrateur nécessite des contributions de nature méthodologique (définition de nouveaux modes d'utilisation des simulateurs, règles de couplage simulation/ méthodes formelles) et formelle (adaptation, extension ou création de méthodes formelles). Afin de relever ce challenge, le projet VACSIM réunit deux industriels, un concepteur et exploitant de systèmes critiques (EDF R&D) et un éditeur de logiciels d'ingénierie (Dassault Systèmes) et quatre laboratoires. Parmi ces derniers, un relève de l'automatique (LURPA) et trois de l'informatique (I3S, INRIA Rennes, LaBRI) ; étant donné le problème posé dans ce projet, ce partenariat pluridisciplinaire nous paraît garant de propositions à la fois originales et solides.

2.1. CONTEXTE ET ENJEUX ECONOMIQUES ET SOCIETAUX / CONTEXT, SOCIAL AND ECONOMIC ISSUES

D'après le Rapport du Ministère de l'Economie, des Finances et de l'Industrie (auteur Dominique Potier) «BRIQUES GÉNÉRIQUES DU LOGICIEL EMBARQUÉ», du 7 octobre 2010, un système critique peut avoir des conséquences graves sur la sécurité de l'environnement, des personnes, des entreprises ou des biens. Toujours d'après ce rapport, la production d'énergie électrique, la production et le raffinage de produits pétroliers ou de produits chimiques dangereux, les transports aériens et ferroviaires constituent les secteurs de plus forte criticité. Ceci explique que la validation de la commande d'un tel système nécessite une attention toute particulière.
Du point de vue normatif et réglementaire, la norme CEI 61506 «Mesure et commande dans les processus industriels – Documentation des logiciels d'application» définit la validation comme le moyen de confirmer que les fonctions et les performances du produit sont conformes aux exigences. Cette norme prévoit de plus les quatre étapes suivantes pour la validation :

- La validation par le fournisseur du système de mesure et commande intégré dans un environnement de test simulant celui de l'utilisateur final ;
- La recette par le client avant livraison à l'utilisateur (factory acceptance test – FAT: test de recette en usine) ;
- Les tests sur le système installé et mis en service ;
- La recette par le client avant mise en exploitation du système (site acceptance test – SAT: test de recette sur site).

Ces quatre étapes sont bien entendu essentielles. Cependant, la lecture de leurs définitions amène les remarques suivantes :

- ces étapes de validation se situent à la fin du processus de développement c'est-à-dire bien trop tard ;
- la validation par le fournisseur est basée sur un modèle de simulation mais rien n'est dit sur la construction de ce modèle (degré de finesse, complétude, …), ni sur son utilisation à des fins de validation ;
- enfin, les méthodes d'analyse formelles, telles que les techniques de vérification/validation formelle et de test de conformité ne sont pas même mentionnées ; il est vrai que, malgré les nombreux et importants résultats de recherche obtenus dans ces domaines et l'intérêt de ces méthodes qui permettent des analyses exhaustives, elles restent (très) difficiles à utiliser dans un contexte industriel (problèmes de passage à l'échelle, difficultés d'intégration dans les environnements de conception), en particulier pour ce qui concerne l'analyse de propriétés quantitatives (durées, coûts, grandeurs physiques).

Il importe donc de développer des environnements d'ingénierie numérique de la commande des systèmes critiques permettant un **continuum de validation** durant le cycle de vie. Ces environnements devront être basés sur les outils existants, qui correspondent à certains besoins, savoir-faire et pratiques, notamment en termes de langages normalisés, de visualisation, de capacité à simuler des modèles de grande taille,… Ils devront comporter de plus des outils facilitant la construction et l'utilisation de modèles de simulation ainsi que des possibilités de validation à l'aide de méthodes d'analyse formelles.

2.2. POSITIONNEMENT DU PROJET / POSITION OF THE PROJECT

Le projet VACSIM vise à contribuer à la réalisation d'un tel environnement en partant des outils d'ingénierie existants ControlBuild et Dymola de la société Dassault Systèmes ; cette caractéristique est garante d'une bonne diffusion et valorisation des résultats du projet. La présence d'un industriel concepteur et exploitant de systèmes de commande critiques dans le consortium est un autre facteur garantissant l'impact des travaux.

Ce projet se situe dans la suite du projet ANR TESTEC (TEst des Systèmes Temps réel Embarqués Critiques – 07 TLOG 022), les partenaires des deux projets étant les mêmes. Le projet TESTEC a fourni les résultats suivants :

- plus d'une vingtaine de communications et publications dans des conférences et revues sélectives du domaine ;
- la réalisation de deux maquettes de laboratoire permettant le test de contrôleurs spécifiés en grafcet et la vérification de systèmes temporisés ; ces deux maquettes ont été utilisées pour le traitement de cas industriels et leur intégration dans un environnement de conception industriel est envisagée ;

- la réalisation d'un module logiciel, intégré dans l'outil ControlBuild, permettant le test de conformité de systèmes de commande logiques spécifiés par diagrammes logiques.

Malgré l'intérêt de ces résultats, les travaux du projet TESTEC nous ont montré que les seules approches formelles de test et de vérification n'étaient pas suffisantes pour la validation de commandes de systèmes critiques, mais qu'il convenait de s'intéresser à leur couplage avec des approches de simulation, les caractéristiques de ces approches, notamment en termes de capacité à passer à l'échelle et d'exhaustivité de l'analyse, étant duales.

En réponse à l'AAP INS, le projet VACSIM se positionne dans les axes 2 (axe principal) et 4 (axe secondaire). L'une des caractéristiques essentielles de ce projet est en effet la prise en compte du système physique à piloter, dénommée également partie opérative par la suite, terme usuel chez les concepteurs considérés ; les approches de simulation et d'identification qui seront mises en œuvre lors du projet se focalisent en effet sur le système bouclé constitué de ce système connecté à sa commande. De plus, étant donné les cibles applicatives qui seront retenues dans ce projet, les exigences de sûreté, déterminisme et temps réel sont au cœur des préoccupations.
En ce qui concerne les problématiques de l'axe 4, le projet VACSIM vise clairement à la cohérence entre différents niveaux d'ingénierie en prenant en compte les besoins des utilisateurs des différents outils (de spécification, simulation, vérification, test).

En dernier lieu, nous estimons que les préoccupations du projet VACSIM sont tout à fait d'actualité et complémentaires de celles de plusieurs projets tels que ITEA2 EuroSysLib (http://www.itea2.org/public/project_leaflets/EUROSYSLIB_profile_oct-07.pdf), qui s'intéresse exclusivement à l'aspect simulation, et MULTIFORM (ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/necs/fp7-fact-sheet-multiform_en.pdf), qui s'intéresse à l'intégration de plusieurs formalismes pour la conception de la commande de systèmes embarqués, mais qui ne considère pas les modalités d'utilisation de ces formalismes.

2.3. ÉTAT DE L'ART / STATE OF THE ART

Cette section comporte plusieurs parties qui correspondent aux domaines considérés dans le projet VACSIM.

2.3.1 ETAT DE L'ART SUR LA SIMULATION DE PARTIE OPERATIVE

Pour la validation des systèmes de commande, une pratique industrielle courante consiste à utiliser un simulateur de la partie opérative connecté aux spécifications, puis à la réalisation du système de commande. L'offre en outils de simulation de partie opérative comprend, par exemple :

- Les outils MATLAB, pour le calcul, et Simulink, pour la représentation des fonctions mathématiques et des systèmes par diagramme en blocs, de la société Mathworks, qui peuvent être utilisés pour modéliser la partie commande, les instruments et la partie commandée (partie opérative) afin de valider un fonctionnement d'ensemble.
- Pour des modélisations plus complexes, qui obligent à intégrer des équations explicites (équations différentielles, polynômes), des environnements de simulation, libres comme Modelica ou commerciaux comme Dymola de la société Dassault Systèmes, permettent une simulation multi-domaine temps réel de systèmes complexes.
- En plus de ces outils généralistes, d'autres outils sont optimisés pour une activité donnée en contrôle industriel ou dans un métier particulier. Par exemple l'outil ControlBuild Validation de Geensoft / Dassault Systèmes, qui peut être utilisé pour simuler le comportement des équipements électromécaniques des instruments, le comportement physique d'une installation et représenter des pupitres de conduite, en offrant la possibilité d'injecter des défauts pour une validation en usine du contrôle et une formation des opérateurs.
- Des simulateurs de formation pleine échelle d'installations de grande taille, telles que des centrales électriques, existent, par exemple les simulateurs de la société CORYS pour le transport et l'énergie.
- Pour le besoin de leurs études lors de programmes critiques, certains industriels comme EDF ont pu développer sur mesure des outils métier qui leur sont propres.
- De grands fournisseurs comme ALSTOM, en particulier dans l'énergie, ont aussi développé une offre d'outils pour simuler l'installation, la partie contrôle et les interfaces de conduite, utilisable pour une validation en usine de systèmes de contrôle.

Si la modélisation du comportement physique des systèmes est de plus en plus utilisée dans l'industrie lors de la conception de nouveaux produits, le fonctionnement de ces systèmes est en général soumis à un certain nombre de conditions, qu'il s'agisse de contraintes physiques, d'exigences ou d'hypothèses, regroupées sous le terme de propriétés. Ces propriétés ont fait l'objet de travaux dans le cadre du projet ITEA2 EuroSysLib, auquel participaient EDF et Dassault Systèmes, qui s'est terminé en 2010 et avait pour objectif de développer le langage Modelica, langage de modélisation physique de plus en plus utilisé dans l'industrie, et de ses bibliothèques couvrant différents domaines. Il est donc possible, lors de l'utilisation de simulateurs couplés à une partie commande critique, de représenter les propriétés attendues d'un système, en particulier de sûreté de fonctionnement et de performance, et de vérifier lors des simulations que ces propriétés sont effectivement satisfaites.
Une approche consistant à associer un modèle de comportement Modelica à un modèle de propriétés exprimé dans un autre langage a aussi été étudiée dans le cadre du projet ITEA2 OpenProd, actuellement en cours d'étude avec le développement du profil UML ModelicaML.

Par contre, les cas connus de ce type de techniques correspondent à des utilisations manuelles du simulateur, sans méthode pour son utilisation, c'est-à-dire sans démarche guidant l'introduction d'états et de défauts sur le modèle de partie simulée pour la sollicitation de la partie contrôle, ni d'objectifs clairs de taux de couverture des tests de l'ensemble. Il n'existe pas de méthode reconnue définissant les utilisations de ces simulateurs pour la validation de la commande des systèmes critiques : choix des défauts sur la partie installation, sur la partie instruments, sur la partie contrôle-commande, critères de couverture de ces différentes parties lors de leur simulation.

2.3.2 ETAT DE L'ART SUR LA VERIFICATION ET LE TEST (POINT DE VUE INDUSTRIEL)

Les concepteurs de systèmes temps réel embarqués critiques sont de plus en plus souvent confrontés à l'obligation de fourniture de résultats de tests dans le cadre de certifications ou de recettes. Ceci explique que de nombreux outils, permettant de générer automatiquement des tests à partir de spécifications données généralement sous la forme de modèles Simulink/Stateflow ou UML, aient été commercialisés ces dernières années, tels que :

- Conformiq Test Generator, de Conformiq, (www.conformiq.com/),
- IBM Rational Test RealTime, d'IBM,
- LTG de LEIRIOS (www.leirios.com),
- MaTeLo d'ALL4TEC (www.all4tec.net),
- Reactis Tester, de Reactive Systems, Inc. (www.reactive-systems.com),
- Safety Test Builder de Geensoft / Dassault Systèmes (www.geensoft.com),
- T-VEC tester, de T-VEC (www.t-vec.com).

Malgré l'intérêt de ces outils, on peut remarquer qu'ils ne prennent pas en compte l'ensemble des langages normalisés utilisés pour les systèmes critiques, tels ceux de la norme IEC 61131-3, et qu'il est très difficile, voire impossible, de les employer pour le traitement de systèmes de grande taille (problèmes de passage à l'échelle).

A coté des outils commercialisés, on trouve des prototypes de recherche possédant une maturité significative. On peut ainsi citer notamment, au niveau national

- les outils du CEA LIST : GATeL [MA 00], qui utilise des modèles Lustre, et Agatha [BFG 03] qui travaille à partir de modèles SDL, Statemate et UML ;
- TGV (Verimag – IRISA Vertecs), outil de génération automatique de séquences de tests de conformité pour les protocoles ;
- Lutess (LSR) et Lurette (Verimag).
- et au niveau international :
- TorX (Universités Twente/Nijmegen) : génération et exécution de tests à la volée pour modèles Lotos :
- T-Uppaal (Université d'Aalborg): génération et exécution de tests à la volée depuis des automates temporisés ;
- PET (University of Warwick) : génération de tests à l'aide de techniques de model-checking et résolution de contraintes.

Chacun de ces prototypes apporte une contribution effective pour la génération automatique de tests, mais aucun d'entre eux ne permet actuellement le passage à l'échelle requis pour une diffusion industrielle.

Enfin on peut constater que la génération automatique de tests à partir de spécifications a fait partie ou fait partie des thématiques de projets à plus large spectre, tels que :

- AVERROES, projet RNTL labellisé en 2002 et auquel participait le LaBRI ;
- CARROLL, programme de recherche commun au CEA List, à l'INRIA et à THALES, dans le cadre du projet MUTATION ;
- ARTIST, réseau d'excellence IST, piloté par Verimag, et auquel participe l'INRIA Rennes / Vertecs et EDF R&D, dans le cadre du Cluster Test et Vérification ;
- Usine Logicielle, projet du pôle de compétitivité Ile-de-France System@tic, en particulier dans le cadre du sous-projet MoDriVal, auquel participe EDF R& D.

Comme pour les prototypes de recherche mentionnés précédemment, les résultats de ces projets constituent des contributions effectives pour la génération automatique de tests à partir de modèles de spécification, mais aucun d'entre eux ne permet actuellement le passage à l'échelle requis pour une diffusion industrielle. D'autre part, la réduction de la taille des tests en utilisant des résultats de vérification des modèles de spécification ou d'implantation ne fait pas partie des objectifs revendiqués par ces projets.

En ce qui concerne la vérification formelle, plusieurs outils ont été commercialisés, en particulier :

- Incisive functional verification, de Cadence (www.cadence.com), pour la vérification de modèles de conception de composants électroniques ;
- SCADE design verifier et Esterel Studio d'Esterel Technologies (www.esterel-technologies.com), basés sur les langages synchrones Lustre et Esterel, et ayant des applications en électronique, avionique et automobile ;
- Safety checker blockset, de Geensoft / Dassault Systèmes (www.geensoft.com), basé sur le langage synchrone Signal, et permettant la vérification de modèles Simulink/Stateflow.

Malgré l'intérêt de ces offres commerciales, on peut remarquer encore une fois qu'aucune d'entre elles ne couvre la totalité des langages d'implantation utilisés pour la commande des systèmes critiques, et en particulier les langages de la norme CEI 61131-3, et qu'elles ne proposent pas l'optimisation de la taille des tests à partir des résultats de vérification.

Le projet ANR TESTEC a, par contre, montré l'intérêt de l'utilisation des techniques de vérification pour réduire cette taille, sur la base de cas-types de logiques industrielles ou de sécurité de machines. Ces travaux ont permis la transformation du prototype TESTMINATOR d'EDF R&D vers un logiciel de la suite ControlBuild de Geensoft / Dassault Systèmes, qui bénéficie de plus d'une possibilité d'animation des spécifications logicielles par les cas de test générés. Actuellement, ces techniques sont utilisables pour des systèmes logiques critiques qui peuvent réaliser plusieurs milliers de fonctions simples, utilisant

typiquement de quelques entrées à une quinzaine d'entrées. Au-delà d'une quinzaine d'entrées, par exemple pour des fonctions logiques complexes qui utiliseraient plus de quarante ou cinquante entrées, les techniques actuellement prototypées ne permettent pas une réduction du nombre de scénarios d'essais à un niveau acceptable. Le projet TESTEC a aussi été l'occasion de formaliser un algorithme de génération de tests et de vérifications minimales qui utilise, en plus des techniques maintenant maîtrisées, l'existence de sorties intermédiaires entre les sorties à tester et leurs entrées, autorisant un test progressif par partie. Le temps imparti au projet TESTEC n'a cependant pas permis de prototyper ces nouveaux algorithmes et de les mettre en œuvre sur des cas industriels.

2.3.3 ETAT DE L'ART SUR LES FONDAMENTAUX DES METHODES DE VALIDATION FORMELLE DE PROPRIETES QUANTITATIVES

Validation de systèmes modélisés par automates temporisés

La plupart des systèmes embarqués incorporent des contraintes temporelles. La complexité croissante et la criticité de tels systèmes (leurs défaillances peuvent avoir un coût humain et/ou économique considérable) font qu'il est nécessaire d'adopter des méthodes formelles et des techniques automatiques pour les concevoir et vérifier leur bon fonctionnement.

Dans ce cadre, les automates temporisés introduits dans les années 90 par Alur et Dill [AD94], sont un modèle courant des systèmes temporisés, qui généralise les automates finis par l'ajout d'horloges (variables réelles évoluant toutes à la même vitesse) qui peuvent être testées et remises à zéro. Malgré un espace infini d'états, de nombreux problèmes de vérification (e.g. accessibilité) sont décidables pour les automates temporisés en exploitant une abstraction finie : l'automate des régions. Une variante de cette abstraction, plus grossière mais plus efficace, l'automate des zones, est utilisée par les outils de vérification de tels modèles, comme UPPAAL [BW04]. La décidabilité de l'accessibilité est également à la base de techniques automatiques de génération de tests de conformité à partir de spécifications d'automates temporisés [KT09,BJSK11].

Récemment, plusieurs variantes du modèle des automates temporisés ont été introduites dans le but de modéliser plus finement les systèmes temps-réels. Ces extensions incorporent par exemple, des probabilités [BBBBG08] ou des coûts [ALP01, BFHLPRV01] et visent à évaluer les performances quantitatives d'un système en permettant d'exprimer, par exemple, un temps moyen ou un coût minimal d'exécution.

La validation à l'exécution a été étudiée sous différents points de vue: le test de conformité, la vérification à l'exécution et l'enforcement à l'exécution. Le test de conformité consiste à s'assurer de la validité d'une implémentation boîte-noire vis à vis de sa spécification, le problème principal étant alors celui de la génération automatique des tests à partir de modèles de spécifications. Des outils académiques comme TGV [JJ05], STG [JJRZ05], TorX [TB03] pour les systèmes de transitions, ou encore T-Uppaal [MLN04] pour les modèles temporisés, permettent notamment la génération automatique de tests de conformité. Le projet ANR TESTEC a aussi proposé des solutions adaptées dans le cadre de systèmes temporisés non-déterministes [BJSK10] et à flots de données [LMR10], mais pas dans le cadre

numérique. La vérification à l'exécution [Fal09, HG08, BLS09, CM05] consiste à s'assurer qu'un système en cours d'exécution vérifie bien certaines propriétés (e.g. logiques), alors que l'enforcement à l'exécution [Sch00, LBW05, Ham06, Fal09] cherche à éviter les violations de propriétés en intervenant sur les actions. C'est le cas des outils j-VETO et j-POST [Fal09], java-MOP [CR07] et RuleR [BHRG09]. A notre connaissance, ce dernier point n'a pas été étudié formellement dans un cadre temporisé.

Pour les systèmes distribués temps-réel, et en particulier les GALS (globalement asynchrone localement synchrone), l'application de techniques de validation formelle est cruciale dès la phase de conception, afin de détecter les comportements erronés imprévus dûs à la concurrence. On dispose à ce jour d'un certain nombre d'outils permettant la vérification automatique par model-checking de tels systèmes. Citons notamment les outils UPPAAL [BW04], RT-SPIN [TC96] et TReX [ABS01], qui reposent sur des modèles d'automates temporisés communicant par variable partagée, rendez-vous, ou canaux FIFO, et les outils ROMEO [GLMR05] et TINA [BV06] qui permettent l'analyse de Réseaux de Petri temporisés.

Model-checking & Programmation par contraintes

Les techniques de model-checking sont utilisées depuis de nombreuses années pour la vérification du matériel [BCC99] et du logiciel [DKW08, JhM09]. Les outils associés à cette approche reposent sur la construction d'un modèle du programme qui représente les états atteignables et sur la recherche dans cet ensemble d'un état qui viole une propriété (ou d'un état garantissant qu'une propriété sera vérifiée).
Du fait des problèmes d'explosion combinatoire, l'ensemble des états atteignable est souvent borné et de nombreux outils de "Bounded Model-Checking" (BMC) ont été développés ces dernières années (e.g. EUREKA[AMP06], F-Soft[IYG08], CBMC[1]). Schématiquement, ces outils fonctionnent de la manière suivante:

1. Le programme est déplié k fois, où k représente la borne
2. Le programme et la propriété sont transformés en une grande formule booléenne ϕ telle que ϕ est satisfiable si et seulement si il existe un contre exemple qui viole la propriété;
3. Un solveur SAT ou SMT(Satisfiability Modulo Theories, e.g. YICES[2], Z3[3], [NiO07]) est utilisé pour déterminer si la formule ϕ est satisfiable.

Dans son tutorial à FMCAD'07[Bry07], R. Bryant posait la question de l'apport possible des solveurs de contraintes pour la vérification de programmes bornés. Les solveurs de contraintes avaient déjà été utilisés pour la génération de jeux de test, en particulier par l'équipe de l'I3S[GBR98], partenaire du projet. Un cadre conceptuel pour leur utilisation dans le Model Checking avait aussi été défini [DeP99]. L'équipe CELTIQUE de L'l'INRIA[4] Rennes

[1] Cf. http://www.cprover.org/cbmc/
[2] http://yices.csl.sri.com/
[3] http://research.microsoft.com/en-us/um/redmond/projects/z3/index.html
[4] http://euclide.gforge.inria.fr/

continue les travaux sur la génération automatique de jeux de test à l'aide d'outils basés sur la programmation par contraintes.
Par ailleurs des techniques de model checking et de test de logiciel ont été utilisées à l'I3S pour la modélisation en biologie. Cet activité a permis de développer des techniques de réduction de modèles guidées par les propriétés à vérifier et ainsi de réduire efficacement la taille des jeux de tests sélectionnés. Plus précisément, la réduction de modèle est guidée sur une notion "d'observables" de sorte que les réductions ne changent pas la véracité des propriétés testées. Ces nouvelles approches, majeures pour limiter le coût des expériences biologiques, devraient s'avérer prometteuses une fois ré-injectées dans le domaine du logiciel
L'équipe de l'I3S a développé un environnent basé sur la programmation par contraintes [CoR06,CRV10] pour la vérification de programmes bornés. L'originalité de cette approche réside dans le fait qu'elle exploite la structure de contrôle du programme pour mieux réduire l'espace de recherche. Plus précisément, au lieu de transformer a priori l'ensemble du programme en un système booléen (ou un système de contraintes), seul le code correspondant à un parcours dans un graphe de flot de contrôle simplifié est transformé en contraintes. La clé du succès de cette approche réside alors dans la stratégie de parcours choisie. Différentes stratégies de recherche ont été implémentées. Dans le cadre d'un projet ANR précédent (TESTEC), une stratégie non séquentielle [CVR11] a donné des résultats très encourageants pour la vérification de propriétés sur un gestionnaire de clignotants, une application non triviale fournie par un des partenaires industriels du projet.

Localisation des erreurs
Lorsque le programme contient des erreurs, les outils de model-checking fournissent des contre-exemples et des traces d'exécution qui sont longues et difficile à comprendre. La localisation des portions de code qui contiennent des erreurs est de ce fait souvent fort couteuse, même pour des programmeurs expérimentés. Différentes approches ont été proposée pour assister le programmeur dans cette tâche. Bal et al [BNR03] ont ainsi proposé d'utiliser plusieurs contre-exemples et de comparer les traces d'exécution avec celles d'exécutions correctes. Les transitions qui n'apparaissent pas dans des traces d'exécution correctes sont considérées comme des possibles causes d'erreur. Cet approche a un coût important et la localisation des erreurs n'est pas toujours très précise. Plus récemment, différentes approches basées sur la dérivation de traces correctes ont été proposées. Ainsi Explain [GKL04] appelle CBMC pour trouver une exécution incorrecte, puis utilise un solver pseudo-booléen pour identifier la solution correcte la plus proche. Il calcule ensuite la différence entre les deux traces. Dans [GBC06, GSB07], les auteurs partent aussi de la trace d'un contre-exemple et recherchent les modifications minimales du programme qui permettent (avec les mêmes données d'entrée) d'obtenir un résultat correct. Cette approche permet d'identifier un sur-ensemble des instructions erronées (ou des prédicats associés). Pour réduire la taille de cet ensemble, le processus est relancé pour différents contre-exemples et les auteurs calculent l'intersection des ensembles de prédicats suspects. Cette approche nécessite toutefois l'exploration d'un espace de recherche très grand et peut conduire à des diagnostic absurdes du fait qu'on peut modifier n'importe quelle expression

(e.g., modification de la dernière affectation d'une fonction pour retourner le résultat attendu). Pour éviter ces défauts, [ZGG06] et [LiL10] ont proposé de modifier uniquement un ou plusieurs prédicats du flot de contrôle. Enfin dernièrement, dans [MaM11] les auteurs ont abordé le problème de manière différente : ils utilisent un solveur MAX-SAT pour calculer le maximum de clauses qui peuvent être satisfaites dans la formule dérivée de la trace incorrecte et de la post-condition.

2.4. OBJECTIFS ET CARACTERE AMBITIEUX/NOVATEUR DU PROJET / OBJECTIVES, ORIGINALITY AND NOVELTY OF THE PROJECT

L'objectif final du projet VACSIM est le développement d'un démonstrateur de l'intérêt du couplage simulation / méthodes d'analyse formelles pour l'ingénierie numérique du contrôle-commande des systèmes critiques. Ce démonstrateur sera basé sur les outils de simulation et validation de la société Dassault Systèmes connectés aux résultats obtenus durant le projet et permettra le traitement de plusieurs cas industriels.

Pour atteindre cet objectif, plusieurs verrous scientifiques sont à lever afin d'améliorer le niveau de maturité des méthodes d'analyse formelle ; ils concernent la décidabilité et la complexité du model-checking de certaines classes d'automates finis temporisés, la résolution de systèmes de contraintes non linéaires sur les flottants, la détermination de taux de couverture par identification de systèmes à événements discrets, et le développement de stratégies permettant le passage à l'échelle de ces méthodes. Les verrous techniques auxquels devra s'attaquer ce projet sont relatifs aux méthodologies d'utilisation des simulateurs de processus et au couplage entre méthodes de simulation, vérification et test, en s'intéressant à la problématique de modélisation multi-échelles.

Il convient de souligner l'aspect novateur de ce projet, les approches de simulation et d'analyse formelle étant bien souvent opposées, alors que nous pensons qu'aucune de ces approches prise isolément ne peut fournir une solution complète pour la validation des systèmes critiques mais qu'il convient de développer des stratégies d'utilisation combinée. On pourra noter enfin que le développement de ces stratégies nécessite un partenariat pluridisciplinaire entre automaticiens et informaticiens afin de tirer le meilleur profit des compétences de ces deux communautés en termes d'outils de modélisation et d'analyse.

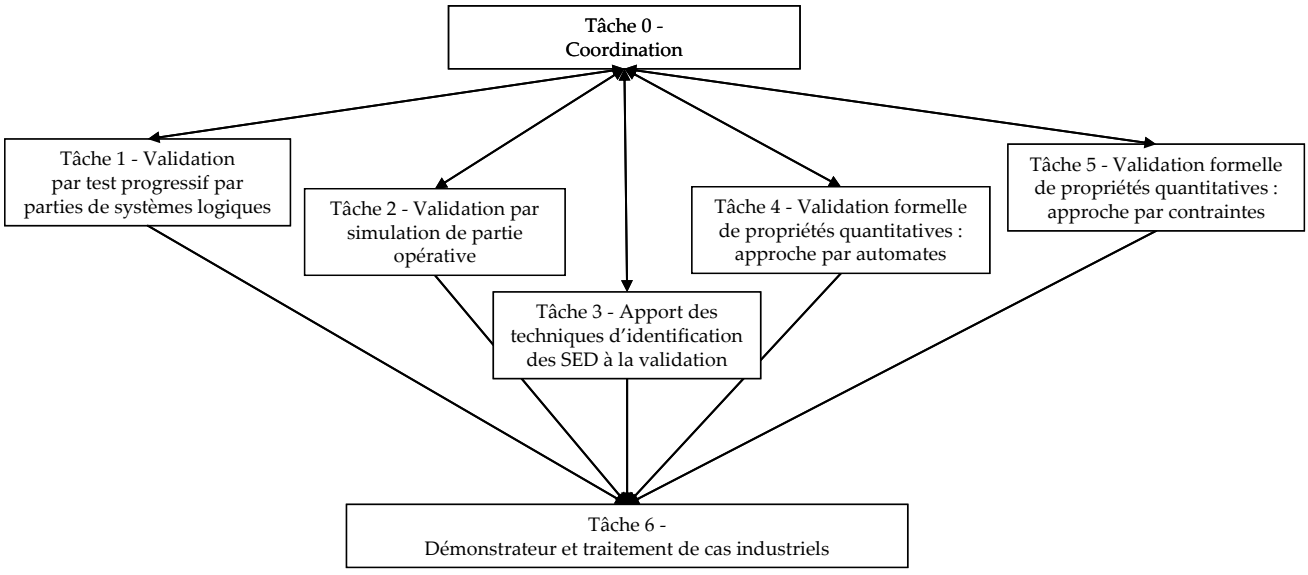
Les résultats du projet pourront être intégrés dans l'outil ControlBuild à sa conclusion. En particulier, les résultats obtenus lors des traitements de cas industriels seront d'une grande utilité pour l'industrialisation.

3. PROGRAMME SCIENTIFIQUE ET TECHNIQUE, ORGANISATION DU PROJET / SCIENTIFIC AND TECHNICAL PROGRAMME, PROJECT ORGANISATION

3.1. PROGRAMME SCIENTIFIQUE ET STRUCTURATION DU PROJET / SCIENTIFIC PROGRAMME, PROJECT STRUCTURE

Le projet VACSIM comporte six tâches techniques (tâches 1 à 6) et une tâche de coordination (tâche 0). Les tâches 1 et 2 visent à proposer des contributions méthodologiques, alors que les résultats des tâches 3 à 5 sont de nature formelle. La tâche 6 a pour objectif d'utiliser les résultats des cinq tâches précédentes dans un démonstrateur permettant de montrer, sur la base de traitements de cas industriels, l'intérêt du couplage simulation / méthodes d'analyse formelles pour l'ingénierie numérique du contrôle-commande des systèmes critiques. La tâche de coordination assure la cohérence entre les travaux des tâches 1 à 5 et en particulier entre les modèles de simulation et ceux utilisés par les méthodes formelles. Les liens entre ces tâches sont schématisés ci-dessous.

On notera enfin que, même si certaines tâches peuvent relever plus de l'automatique (Tâche 3) ou de l'informatique (Tâche 5), la réalisation, de manière cohérente et dans un souci de complémentarité, de l'ensemble de ces tâches nécessite un consortium pluridisciplinaire regroupant des partenaires académiques chercheurs en automatique et en informatique ainsi que des industriels représentant les utilisateurs des outils d'ingénierie de la commande des systèmes critiques et les éditeurs de ces outils.



3.2. MANAGEMENT DU PROJET / PROJECT MANAGEMENT

Un comité de pilotage sera mis en place ; chaque partenaire du projet y sera représenté par un membre. Outre la tâche de coordination définie précédemment, la complémentarité et la cohérence des travaux des différentes tâches seront assurées par la tenue :

- de réunions mensuelles du comité de pilotage du projet, par visio- ou télé-conférence ;
- et de réunions bisannuelles, d'une durée de deux jours chacune et se déroulant à tour de rôle chez chacun des partenaires, réunissant tous les acteurs du projet ; ces réunions permettront des exposés suivis de discussions approfondies ainsi que des échanges formels et informels.

3.3. DESCRIPTION DES TRAVAUX PAR TACHE / DESCRIPTION BY TASK

3.3.1 TACHE 1 / TASK 1 : VALIDATION PAR TEST PROGRESSIF PAR PARTIES DE SYSTEMES LOGIQUES

Objectif : Le projet TESTEC a été l'occasion de formaliser un algorithme de génération de tests et de vérifications minimales qui utilise, en plus des techniques développées dans ce projet, l'existence de sorties intermédiaires entre les sorties à tester et leurs entrées, autorisant un test progressif par parties. Le temps imparti au projet TESTEC n'a cependant pas permis de prototyper ces nouveaux algorithmes et de les mettre en œuvre sur des cas industriels. Le projet VACSIM sera l'occasion de vérifier le caractère réalisable et performant de ces nouvelles possibilités, qui correspondraient à la levée d'un verrou technique important pour le problème de la réduction de la combinatoire du test des fonctions logiques critiques non bouclées. L'objectif final de cette tâche est de développer un prototype, intégré dans l'environnement ControlBuild, réalisant le test progressif par parties de systèmes logiques non-bouclés et de le mettre en œuvre sur des cas industriels.

Durée : 36 mois (de T0 à T0+36)
Responsable : EDF R&D
Partenaires impliqués : Dassault Systèmes, I3S, LURPA

Livrables :
L1.1 : Spécification et validation sur études de cas d'un algorithme de test progressif par parties de systèmes logiques non-bouclés (T0+12) - Document
L1.2 : Développement d'un algorithme de test progressif par parties de systèmes logiques non-bouclés dans l'environnement ControlBuild (T0+24) - Logiciel
L1.3 : Evaluation sur études de cas industriels d'un algorithme de test progressif par parties de systèmes logiques non-bouclés dans l'environnement ControlBuild (T0+36) - Document

3.3.2 TACHE 2 / TASK 2 : VALIDATION PAR SIMULATION DE PARTIE OPERATIVE

Objectif : Cette tâche a pour objectif de proposer une méthode d'utilisation automatisée d'un simulateur de partie opérative, afin d'augmenter l'efficacité de ce type de technique de validation.
Pour les systèmes de commande complexes en effet, une pratique industrielle courante consiste à utiliser un simulateur de la partie contrôlée, aussi dénommée partie opérative, bouclé aux spécifications, puis à la réalisation, du système de contrôle-commande. Malheureusement, les cas connus de ce type de techniques correspondent à des utilisations manuelles du simulateur, sans méthode pour son utilisation, c'est à dire sans démarche guidant l'introduction d'états et de défauts sur le modèle de partie simulée pour la sollicitation de la partie commande, ni d'objectifs clairs de taux de couverture des tests de l'ensemble. Cette difficulté scientifique et technique conduit concrètement à l'impossibilité d'automatiser ce type de test, du fait de l'absence de formalisation d'une démarche d'utilisation. Ceci peut aboutir à un coût prohibitif et à des efforts démesurés quand une exigence d'un grand nombre de cas de tests est posée, typiquement pour le test statistique d'un système critique. Le nouveau projet VACSIM sera l'occasion d'examiner les possibilités de résoudre cette difficulté. L'objectif est ici de développer un environnement de simulation de systèmes critiques, intégrant l'analyse de propriétés de sûreté de fonctionnement, qui puisse automatiser une utilisation méthodique du simulateur qui aura été définie dans le projet, sur la base d'objectifs et de taux de couverture de test rationnellement définis.

Durée : 36 mois (de T0 à T0+36)
Responsable : EDF R&D
Partenaires impliqués : Dassault Systèmes, LaBRI, LURPA

Livrables :
L2.1 : Spécification et validation, sur études de cas, d'une méthode d'utilisation des simulateurs de parties opératives : objectifs, propriétés de sûreté de fonctionnement, taux de couverture et limitations de la simulation (T0+12) - Document
L2.2 : Développement d'une utilisation automatisée du simulateur ControlBuild Validation de Dassault Systèmes (T0+24) - Logiciel
L2.3 : Evaluation sur études de cas industriels d'une utilisation automatisée du simulateur ControlBuild Validation de Dassault Systèmes (T0+36) - Document

3.3.3 TACHE 3 / TASK 3 : APPORT DES TECHNIQUES D'IDENTIFICATION DES SED A LA VALIDATION DES SYSTEMES CRITIQUES

Objectif : L'objectif de cette tâche est de montrer que les techniques d'identification des systèmes à événements discrets (SED), qui ont été jusqu'à présent développées à des fins de diagnostic à base de modèle, peuvent contribuer à la validation des systèmes critiques lors de leur ingénierie. Pour ce faire, trois sous-tâches complémentaires ont été définies.
Durée : 30 mois (de T0 à T0+30)

Responsable : LURPA
Partenaires impliqués : EDF R&D, I3S, INRIA

Sous-tâche 3.1 : Identification d'un système bouclé contrôleur - simulateur de partie opérative (T0 à T0+18)
En Automatique, l'identification d'un système a pour objectif de construire un modèle mathématique du comportement d'un système réel, considéré comme une boîte noire dont les entrées/sorties sont observables, à partir d'observations de ses réponses à des sollicitations. L'approche d'identification est duale de celle de modélisation et est très largement utilisée en automatique des systèmes continus, la complexité des processus à commander rendant bien souvent impossible la construction, à partir des connaissances sur le comportement physique des éléments du processus, d'un modèle exploitable pour la commande.
Pour ce qui concerne les systèmes à événements discrets, cette approche est nettement moins répandue mais plusieurs résultats importants ([MRM98],[CGS06],[CGS07],[DFM08]), auxquels le LURPA a contribué ([KLE 05],[ROT10]), ont été obtenus depuis une dizaine d'années cependant. Ces résultats sont basés sur une modélisation du système bouclé constitué d'un contrôleur et d'une partie opérative réels par une classe d'automates non-déterministes à sorties (non-deterministic autonomous automata with outputs (NDAAO)). Il convient dans un premier temps d'étudier l'applicabilité de ce formalisme à la modélisation du comportement d'un système bouclé où la partie opérative n'est plus qu'une simulation de la réalité ou de proposer un autre formalisme.

Sous-tâche 3.2 : Validation par identification d'un système bouclé contrôleur - simulateur de partie opérative (T0+6 à T0+24)
Sur la base des résultats de la sous-tâche précédente, une méthode de validation par comparaison, par exemple par bi-simulation, du comportement identifié au comportement attendu sera proposée et expérimentée. Pour ce faire, nous comptons utiliser le banc expérimental TeLoCO développé lors du projet ANR TESTEC.

Sous-tâche 3.3 : Validation formelle par couplage identification – test de conformité (T0+12 à T0+30)
Les techniques d'identification sont complémentaires de celles de test de conformité. Ces dernières permettent en effet de s'assurer que le comportement de la spécification est bien inclus dans celui de l'implantation, mais non l'inverse. Partant d'observations sur une implantation, l'identification vise au contraire à construire un modèle formel d'un système réel. Il nous paraît donc essentiel d'étudier les couplages possibles entre ces deux approches, afin d'améliorer la validation des systèmes critiques et, par voie de conséquence, le niveau de confiance des utilisateurs de ces systèmes.
Enfin, nos travaux antérieurs ont permis de relier la longueur des mots acceptés par le modèle formel résultant de l'identification à celle des mots réellement observés. L'utilisation de ces résultats pour une meilleure maîtrise du taux de couverture d'un test de conformité

nous paraît une piste de recherche prometteuse tant du point de vue théorique qu'en termes d'application.

Livrables :
L3.1 : Méthode d'identification d'un système bouclé contrôleur - simulateur de partie opérative (T0+18) - Document
L3.2 : Validation par identification d'un système bouclé contrôleur - simulateur de partie opérative (T0+24) – Logiciel + Document
L3.3 : Validation formelle par couplage identification – test de conformité (T0+30) - Document

3.3.4 TACHE 4 / TASK 4 : VALIDATION FORMELLE DE PROPRIETES QUANTITATIVES : APPROCHE PAR AUTOMATES

Objectif : Cette tâche a pour but de contribuer à l'avancée de techniques de validation de systèmes temporisés. Elle est divisée en trois sous-tâches complémentaires, visant chacune une problématique particulière de validation : l'analyse quantitative des automates temporisés, les techniques de validation à l'exécution (test, monitoring et enforcement), et la vérification d'automates temporisés communicants.
Durée : 30 mois (de T0 à T0+30)
Responsable : INRIA
Partenaires impliqués : EDF R&D, I3S, LaBRI, LURPA

Sous-tâche 4.1 : Analyse quantitative des automates temporisés (T0 à T0+18)
Pour exprimer des consommations d'énergie ou des phénomènes aléatoires, plusieurs extensions du modèle des automates temporisés ont été proposées. Dans cette sous-tâche, nous proposons de développer des techniques de vérification pour ces aspects quantitatifs des automates temporisés, et de les appliquer à la validation de systèmes temps-réel.
Tout d'abord, nous nous intéresserons à quantifier l'ensemble des trajectoires d'un système temps-réel en étudiant une distribution de probabilité naturelle sur l'ensemble de ces traces. Cette extension probabiliste permettra de s'intéresser par exemple au temps moyen d'exécution d'une tâche. Par ailleurs, un tel modèle pourra être utilisé dans la génération automatique de tests. Une autre façon de quantifier l'ensemble des exécutions d'un système est de définir une distance entre ses traces, et de mesurer par exemple le diamètre de l'ensemble des exécutions du système. Une telle distance s'appliquera naturellement à la définition d'un critère de couverture sémantique pertinent pour le test de systèmes temps-réel.
D'autre part, il est naturel d'associer à chaque exécution d'un système une valeur représentant, par exemple son coût, ou toute autre quantité. Dans ce but, nous nous focaliserons sur la quantification des éventuelles défaillances d'un système temps-réel en exprimant pour chacune de ses exécutions la portion de temps passé dans des états critiques. Cette notion de fréquence sera étudiée, dans le but de développer des algorithmes calculant

l'ensemble des fréquences pour un automate temporisé, voire la fréquence moyenne qui exprimera à quel point un système est défaillant.
L'ensemble des méthodes mises en place pourra ensuite être exploité dans d'autres champs de la validation formelle que le test ou la vérification, comme le diagnostic ou le contrôle.

Sous-tâche 4.2 : Validation à l'exécution de systèmes temporisés (T0+6 à T0+24)
Dans les systèmes critiques, il s'avère souvent utile de pouvoir s'assurer à l'exécution que certaines propriétés sont vérifiées (e.g. les actions effectuées par le système sont cohérentes). Par extension, il est parfois possible de "corriger/contraindre" (toujours à l'exécution) les actions du système afin que celui-ci respecte ces propriétés. Nous nous proposons d'étudier ces aspects (vérification et enforcement à l'exécution) dans le cadre de systèmes temporisés manipulant éventuellement des données numériques. Ces techniques sont prometteuses dans la mesure où elles ne nécessitent pas de disposer d'une spécification formelle du modèle permettant ainsi de maîtriser (dans une certaine mesure) l'explosion combinatoire. De plus, dans la continuité des travaux déjà effectués à l'INRIA et au LaBRI, nous étudierons dans quelles mesures les techniques pour la vérification quantitative développées dans la sous-tâche 4.1 pourront s'appliquer à la génération automatique de tests et plus particulièrement au problème de couverture pour le test de systèmes réactifs.

Sous-tâche 4.3 : Vérification d'automates communicants temporisés (T0+12 à T0+30)
Avant d'implanter une application critique, il est nécessaire de vérifier que la spécification vérifie bien les propriétés souhaitées. Cependant, avant de se lancer dans cette phase, il est indispensable de s'assurer que l'approche de vérification choisie est viable.
Les systèmes d'automates finis communiquant par canaux FIFO non bornés (CFSM) sont fréquemment utilisés dans la modélisation de systèmes communicants. Cependant, dans le cadre non-temporisé, la vérification de propriétés comportementales de ce genre de modèles est indécidable ([BZ83]), mais il existe certaines classes décidables ([FM85], [FC87], [AJ96]).
Dans le cadre de systèmes critiques temps-réel, il s'avère souvent nécessaire de se placer dans un contexte distribué asynchrone (pour éviter les simplifications peu réalistes). Dans ce cas, il est naturel de prendre en compte des aspects temps-réels locaux en utilisant des automates temporisés comme composants de base. Les outils RT-SPIN [TC96] et TreX [ABS01] permettent d'analyser de tels modèles, cependant les canaux de communication sont bornés a priori dans RT-SPIN, et ils sont à pertes dans TreX. A notre connaissance, et malgré un intérêt pratique évident, la décidabilité de la vérification des CFSM temporisés (à canaux non-bornés) a été peu étudiée, et se limite en général à des hypothèses trop fortes pour une application réelle ([KY06, ABG07]).
L'objectif de cette sous-tâche consiste à étudier la décidabilité et la complexité du model-checking des CFSM temporisés. Nous chercherons dans quelle mesure il est possible de relâcher les hypothèses habituelles afin de pouvoir appliquer ces travaux sur des cas réalistes de systèmes temps-réel. Les pistes envisagées concernent notamment des restrictions sur les architectures de communication, sur l'asynchronisme, sur le nombre d'horloges ou sur la fiabilité des canaux. D'autre part, les aspects décidabilité et complexité algorithmique de la

vérification de propriétés comportementales seront étudiés.

Livrables :
L4.1 : Etude de techniques d'analyse quantitative des modèles temporisés (T0+18) - Document
L4.2 : Etudes de techniques de validation à l'exécution pour des systèmes réactifs critiques. (T0+24) - Document
L4.3 : Décidabilité et complexité du model-checking des systèmes d'automates finis temporisés communicant par canaux FIFO non bornés (T0+30) - Document

3.3.5 TACHE 5 / TASK 5 : VALIDATION FORMELLE DE PROPRIETES QUANTITATIVES : APPROCHE PAR CONTRAINTES

Objectif : Cette tâche a pour but de contribuer à l'avancée de techniques de validation par résolution de systèmes de contraintes. Elle est divisée en deux sous-tâches complémentaires, visant chacune une problématique particulière.
Durée : 30 mois (de T0 à T0+30)
Responsable : I3S
Partenaires impliqués : Dassault Systèmes, INRIA, LaBRI

Sous-tâche 5.1 : Génération et résolution des systèmes de contraintes (T0 à T0+24)
Les systèmes auxquels nous nous intéressons sont typiquement des systèmes temps réels pour lesquels un modèle à été développé dans un langage comme Simulink et un programme de contrôle en C a été généré automatiquement à parti dudit modèle. Dans ce type de configuration, il est indispensable de vérifier certaines propriétés sur le programme C qui va effectivement piloter le processus. Le schéma général de ce type d'architecture est le suivant: à partir d'un modèle Simulink un programme en langage C est généré automatiquement. Le code obtenu est instrumenté pour ajouter les propriétés, exprimées en langage naturel, que doit vérifier ce code. La vérification de ces propriétés s'effectue à l'aide d'un outil de bounded-model checking (CBMC, CPBPV, DVPS par exemple) qui produit, le cas échéant, un contre exemple.

Dans le cadre du projet TESTEC, nous avons développé des stratégies de recherche adaptées à ce type d'application pour des systèmes de vérification qui utilisent des solveurs de contraintes dans un domaine fini (sous ensemble des entiers) et des solveurs linéaires sur les réels dans un système de "Bounded-Model-Checking". Toutefois, nous n'avons pas pu traiter des problèmes avec des contraintes non linéaires sur les flottants –contraintes qui se rencontrent par exemple dans l'application ABS- du fait de l'absence d'outils disponibles, et surtout nous nous sommes heurtés à des problèmes de passage à l'échelle.

Dans le cadre de ce projet, nous proposons d'essayer de faire sauter ces deux "verrous technologiques". Pour cela nous comptons:

1. Tirer profit des acquis des techniques de "Model-Checking" introduites dans le domaine de la bio-informatique où une des principales caractéristiques des problèmes est leur grande taille. La bio-informatique dans le domaine des systèmes complexes a débuté en important largement des techniques issues de la vérification de logiciel ; elle constitue maintenant une science mature, qui a développé des techniques de gestion des systèmes complexes sophistiquées, que l'informatique pourrait maintenant à son tour "importer" vers l'activité de vérification des logiciels complexes.
2. Utiliser des travaux récents réalisés par des membres de notre équipe (en collaboration avec le CEA) sur la résolution de systèmes de contraintes sur les flottants.

L'intégration de l'ensemble de ces techniques dans un système de vérification dédié aux applications temps réels embarquées, nous conduira naturellement aussi à développer des stratégies de recherche pour les solveurs de contraintes adaptées à la structure de chaque problème.

Sous-tâche 5.2 : Localisation des erreurs (T0+6 à T0+30)
Comme mentionné précédemment la question de la localisation des erreurs à partir d'un contre-exemple où une trace d'exécution est un problème important. Il nous semble donc essentiel d'explorer les aides que nous pouvons apporter à l'utilisateur dans ce domaine. Les approches actuelles sont essentiellement basées sur des solveurs SAT bien adaptées à des model-checker comme CBMC. Dans notre environnent pour la vérification de programmes bornés basée sur la programmation par contraintes, nous avons un modèle plus riche dont nous pouvons essayer d'en tirer parti. Ainsi à partir du système de contrainte dérivé de la trace d'un contre-exemple et de la post-condition, nous pouvons calculer aisément des IIS (Irreducible Infeasibility set)[1] pour les contraintes linéaires et des "minimum conflict sets"[Jun04] pour les contraintes du CSP. Dans le cadre de ce projet, nous allons évaluer l'apport de ces informations sur les exemples fournis par les industriels et développer un système d'aide à la location des erreurs, basée sur ces principes.

Livrables :
L5.1 : Apport de la bio-informatique à la vérification des systèmes complexes (T0+18) - Document
L5.2 : Vérification de propriétés quantitatives par résolution de systèmes de contraintes sur les flottants (T0+24) – Logiciel + Document
L5.3 : Système d'aide à la localisation des erreurs (T0+30) - Document

3.3.6 TACHE 6 / TASK 6 : DEMONSTRATEUR ET TRAITEMENT DE CAS INDUSTRIELS

Objectif : Sur la base des résultats des tâches 1 à 5, cette tâche a pour but de développer un démonstrateur intégré dans l'environnement ControlBuild et permettant de montrer l'intérêt du couplage simulation / méthodes d'analyse formelles pour l'ingénierie numérique du

contrôle-commande des systèmes critiques. Ceci sera effectué par le traitement de plusieurs cas industriels critiques.
Durée : 18 mois (de T0+18 à T0+36)
Responsable : Dassault Systèmes
Partenaires impliqués : Tous
Livrables :
L6.1 : Démonstrateur du couplage simulation / méthodes d'analyse formelles (T0+36) – Logiciel + Document
L6.2 : Traitement de cas industriels (T0+36) - Logiciel + Document

3.3.7 TACHE 0 / TASK 0 : COORDINATION

Objectif : Cette tâche vise à garantir la complémentarité et la cohérence des travaux des tâches 1 à 5. Elle devra en premier lieu permettre de définir le rôle de chacune des techniques retenues (simulation, test, analyse par identification, vérification de propriétés quantitatives) dans le cycle de vie de la commande d'un système critique. Ceci aura pour conséquence de proposer des règles d'usage des modèles sous-tendant ces techniques, par exemple simulation d'un modèle détaillé pour l'ensemble des évolutions prévues et analyse formelle d'une abstraction de ce modèle autour d'un point de fonctionnement particulièrement critique, ainsi que des critères d'équivalence (ou de non-équivalence) entre ces modèles. Outre l'organisation décrite en section 3.2, cette tâche s'appuiera sur un espace de travail collaboratif permettra l'échange des résultats.
Durée : 36 mois (de T0 à T0+36)
Responsable : LURPA
Partenaires impliqués : Tous
Livrables :
L0.1 : Rapport de fin de projet : complémentarité des méthodes de simulation et d'analyse formelle pour la validation de la commande des systèmes critiques (T0+36) - Document

3.4. CALENDRIER DES TACHES, LIVRABLES ET JALONS / TASKS SCHEDULE, DELIVERABLES AND MILESTONES

Voir pages suivantes.

Diagramme de Gantt des tâches

	T0 à T0 + 6 mois	T0 + 6 mois à T0 + 12 mois	T0 + 12 mois à T0 + 18 mois	T0 + 18 mois à T0 + 24 mois	T0 + 24 mois à T0 + 30 mois	T0 + 30 mois à T0 + 36 mois
Tâche 1 : Validation par test progressif de systèmes logiques						
1.1. Spécification et validation d'un algorithme						
1.2. Développement dans l'environnement ControlBuild						
1.3. Etudes de cas						
Tâche 2 : Validation par simulation de partie opérative						
2.1. Spécification et validation d'une méthode d'utilisation						
2.2. Développement d'une utilisation automatisée						
2.3. Etudes de cas						
Tâche 3 : Identification des SED pour la validation						
3.1. Identification d'un système bouclé contrôleur-simulateur						
3.2. Validation par identification						
3.3. Couplage identification-test de conformité						
Tâche 4 : Propriétés quantitatives : approche par automates						
4.1. Analyse quantitative des automates temporisés						
4.2. Validation à l'exécution						
4.3. Vérification d'automates communicants temporisés						
Tâche 5 : Propriétés quantitatives : approche parcontraintess						
5.1. Génération et résolution de systèmes de contraintes						
5.2. Localisation des erreurs						
Tâche 6 : Démonstrateur et études de cas industriels						
Tâche 0 : Coordination						

Tableau des livrables

Date de livraison	Id.	Titre	Tâche	Responsable	Type de fourniture
T0+12	L0.0	Accord de consortium	0	LURPA	Contrat
T0+12	L1.1	Spécification et validation sur études de cas d'un algorithme de test progressif par parties de systèmes logiques non-bouclés	1	EDF	Document
T0+12	L2.1	Méthode d'utilisation des simulateurs de parties opératives	2	EDF	Document
T0+18	L3.1	Identification d'un système bouclé contrôleur - simulateur de partie opérative	3	LURPA	Document
T0+18	L4.1	Analyse quantitative des modèles temporisés	4	LaBRI	Document
T0+18	L5.1	Apport de la bio-informatique à la vérification des systèmes complexes	5	I3S	Document
T0+24	L1.2	Algorithme de test progressif par parties de systèmes logiques non-bouclés dans l'environnement ControlBuild	1	Dassault Systèmes	Logiciel
T0+24	L2.2	Utilisation automatisée du simulateur ControlBuild Validation	2	Dassault Systèmes	Logiciel
T0+24	L3.2	Validation par identification	3	LURPA	Logiciel + Document
T0+24	L4.2	Techniques de validation à l'exécution pour des systèmes réactifs critiques	4	INRIA	Document
T0+24	L5.2	Vérification de propriétés quantitatives par résolution de systèmes de contraintes sur les flottants	5	I3S	Logiciel + Document
T0+30	L3.3	Validation formelle par couplage identification – test de conformité	3	LURPA	Document
T0+30	L4.3	Décidabilité et complexité du model-checking	4	INRIA	Document
T0+30	L5.3	Système d'aide à la localisation des erreurs	5	I3S	Document
T0+36	L1.3	Evaluation sur études de cas industriels d'un algorithme de test progressif par parties	1	EDF	Document
T0+36	L2.3	Evaluation sur études de cas industriels d'une utilisation automatisée du simulateur	1	EDF	Document
T0+36	L6.1	Démonstrateur du couplage simulation / méthodes d'analyse formelles	6	Dassault Systèmes	Logiciel + Document
T0+36	L6.2	Traitement de cas industriels	6	EDF	Document
T0+36	L0.1	Rapport de fin de projet	0	LURPA	Document

Comme indiqué en section 3.2, l'ensemble des participants au projet se réuniront deux fois par an, durant 2 jours, afin de présenter et discuter les résultats contenus dans les livrables. Ces réunions constitueront les jalons du projet.

Les réunions mensuelles du comité de pilotage permettront de préparer efficacement ces jalons.

4. STRATEGIE DE VALORISATION, DE PROTECTION ET D'EXPLOITATION DES RESULTATS / DISSEMINATION AND EXPLOITATION OF RESULTS. INTELLECTUAL PROPERTY

Les résultats scientifiques obtenus lors de ce projet seront soumis aux conférences et revues reconnues des domaines considérés, en particulier aux conférences organisées par l'IEEE, l'IFAC et l'IFIP, aux revues IFAC Automatica ou Control Engineering Practice, IEEE TAC, IEEE TASE, LNCS.

Les résultats techniques obtenus, en particulier les démonstrateurs qui constituent les livrables 1.2, 2.2 et 6.1, ont vocation à être industrialisés et à faire partie de l'offre logicielle de la société Dassault Systèmes à l'issue du projet. Ceci afin de fournir des aides efficaces aux services d'ingénierie ayant en charge le développement de futurs systèmes critiques, que ce soit dans le domaine de la production d'énergie ou dans d'autres domaines (transport ferroviaire ou maritime, secteur automobile, …).

Un accord de consortium sera établi dès le début du projet afin de définir la propriété des résultats. Cet accord constitue un livrable du projet : L0.0 à T0 + 12. Il s'inspirera fortement de l'accord établi entre les mêmes partenaires lors du projet TESTEC, ce dernier ayant donné entière satisfaction.

Les principes suivants seront appliqués pour la définition de cet accord :

- Les partenaires académiques (CNRS, ENS Cachan, ENSEIRB, INRIA) seront propriétaires des maquettes, codes, développements qu'ils réaliseront en propre.
- La société Dassault Systèmes est propriétaire de l'outil ControlBuild. Elle aura la propriété de l'ensemble des développements qu'elle réalisera sur cet outil dans le cadre du projet.
- La société EDF sera propriétaire de ses développements propres dans le cadre du projet, notamment des algorithmes de test par partie de systèmes logiques et d'utilisation automatisée de simulateur de partie opérative.

Les livrables publics du projet seront la propriété commune de l'ensemble des participants. Il est convenu que les méthodologies et développements spécifiques réalisés par les universités, industriels et organismes de recherche pourront faire l'objet d'un transfert de licence ou savoir-faire à la société Dassault Systèmes suivant un accord qui pourra être réalisé durant ou à l'issue du projet.

5. DESCRIPTION DU PARTENARIAT / CONSORTIUM DESCRIPTION

5.1. DESCRIPTION, ADEQUATION ET COMPLEMENTARITE DES PARTENAIRES / PARTNERS DESCRIPTION & RELEVANCE, COMPLEMENTARITY

Dassault Systèmes (DS)

Dassault Systèmes (DS) est un éditeur de logiciel spécialisé dans les outils de conception assistée par ordinateur. La gamme de produits de la société est étendue et comprend 7 marques de produits interconnectés pour former une plateforme technique. La société est le leader de son marché.

La marque la plus connue de l'entreprise est la marque CATIA, CATIA est composée de 200 produits logiciels qui ensemble composent la solution leader pour la création de produit en 3D. La société a développé en interne, et suite à l'acquisition de Geensoft, une suite d'outils pour la conception de l'électronique embarquée qui utilise les principes de Model Based Engineering dans lesquels différents niveaux de modèles sont réalisés pour définir les fonctions, puis les solutions techniques avant d'être utilisés pour réaliser le logiciel, les configurations et enfin les bancs de tests des solutions électroniques embarquées. Un de ces produits est ControlBuild qui est utilisé dans le transport et l'énergie pour modéliser et générer le code d'applications à forte contrainte de sûreté de fonctionnement.

Dans le cadre d'autres projets de R&D, en particulier le projet TESTEC et le projet EDONA, Geensoft a expérimenté des techniques de génération de jeux de test et l'intégration de ces techniques aux outils de conception ; ces expérimentations ont abouti à l'intégration de modules spécialisés dans les outils ControlBuild et AutosarBuilder. Les équipes R&D de DS sur les sujets systèmes sont de 100 personnes environ et en croissance rapide.

EDF R&D

EDF Recherche & Développement a pour mission de préparer ce que sera le monde énergétique de demain. Résoudre les problèmes quotidiens dans l'exercice de nos métiers, imaginer l'avenir du paysage énergétique et contribuer à conforter la position du Groupe EDF sur la place internationale, tels sont les enjeux. Au sein d'EDF R&D, le département Simulation et Traitement de l'information pour les Procédés industriels a pour mission d'améliorer la sûreté, la disponibilité et la productivité des moyens de production du Groupe EDF (centrales nucléaires, hydrauliques, thermiques, renouvelables), de maîtriser leurs coûts de maintenance et d'accroître leur durée de vie. Le département est organisé en cinq groupes d'études dont le groupe Contrôle-Commande qui a pour mission d'être une source de propositions innovantes dans les domaines du contrôle-commande et de l'informatique industrielle utilisée dans les moyens de production. Il contribue à la maîtrise de la durée de vie des systèmes de contrôle-commande et à la compétitivité des moyens de production, en maîtrisant leur sûreté de fonctionnement. Dans le domaine des tests de validation, EDF R&D possède une expertise forte tant au niveau méthodologique que réalisation. Elle la met en œuvre en particulier dans le cadre de nouveaux projets de systèmes de contrôle-commande (nucléaire N4, EPR, Chine) et lors de projets de rénovation des systèmes existants.

EDF R&D a investigué, à des fins exploratoires, la complémentarité des vérifications formelles et des générations de test automatisées, notamment par le développement d'un prototype Testminator pour les systèmes logiques non bouclés. EDF R&D développe par ailleurs des simulateurs de parties opératives pour la validation fonctionnelle du contrôle-commande et maîtrise les techniques d'analyse statique de codes pour la vérification des logiciels critiques. EDF R&D participe aussi au projet Usine Logicielle du Pôle de compétitivité 'System@tic', dans le cadre du sous-projet MODRIVAL pour la validation des systèmes (génération de tests à partir de spécifications en UML) et les outils d'analyse de logiciels.

I3S

L'I3S a une grande expérience dans la programmation par contraintes et applique ces techniques depuis plus de 10 ans à la génération de jeux de test logiciels et la vérification de programmes. Gilles Bernot, qui a rejoint l'I3S récemment, a été un des pionniers dans l'utilisation des méthodes formelles pour le test et la vérification. Dans la continuité de ces travaux, son équipe est devenue moteur dans l'application des méthodes formelles aux systèmes biologiques complexes. L'outil SMBioNet développé dans ce cadre met en œuvre des techniques d'énumération parcimonieuse qu'on se propose d'appliquer au logiciel.

Une partie de travaux de l'I3S dans ce domaine a été menée dans le cadre du projet RNTL DANOCOPS, l'ACI V3F et les projets ANR CAVERN et TESTEC. C'est dans le cadre de ce dernier projet que nous avons commencé à travailler avec les partenaires du projet qui est soumis; c'est à dire appris à dialoguer avec des automaticiens et appris à connaître les problèmes des industriels comme ceux de Geensys et EDF R&D.

Les enseignants-chercheurs de l'I3S impliqués dans ce projet totalisent une vingtaine de publications internationales (dont plus de 10 revues) dans des domaines directement liés à leur contribution dans ce projet.

INRIA VerTeCs

L'équipe-projet INRIA VerTeCs possède une grande expertise dans la conception de techniques et outils pour la vérification, le contrôle et la génération automatique de tests de conformité pour des systèmes réactifs. Ses recherches se fondent sur des modèles formels et des techniques de vérification. Ayant une renommée internationale en génération automatique de tests, l'équipe VerTeCs s'est intéressée depuis plusieurs années à la génération symbolique de tests de conformité pour des modèles de spécifications de type automates étendus, en évitant l'énumération des données a priori non bornées. Plus récemment, elle a étudié la génération automatique de test pour différentes classes d'automates temporisés, avec ou sans données, et notamment dans le cadre du projet ANR TESTEC en considérant un modèles d'automates temporisés à flots de données (en collaboration avec le LaBRI). L'équipe Vertecs possède également des compétences solides en vérification qualitatives et quantitatives sur les modèles temporisés. Elle mène aussi des recherches sur la combinaison méthodologique et technique de la vérification et du test. L'équipe collabore sur ces thèmes avec plusieurs laboratoires en Europe, en particulier dans le cadre du réseau Artist et dans le cadre d'une équipe associée au Brésil. Les membres de l'équipe Vertecs intervenant dans le projet VACSIM sont auteurs d'une bonne vingtaine

de publications dans des conférences internationales et quelques articles de journaux sur les thèmes dans lesquels elle se propose d'intervenir dans le cadre de ce projet.

LaBRI

Au niveau du LaBRI (UMR 5800), les thèmes "modélisation et vérification" et "test de systèmes informatisés" sont concernés par le projet VACSIM. Les membres de ces thèmes ont une longue expérience dans la modélisation et la validation de systèmes. Entre autres, ces travaux s'appliquent dans le cadre de systèmes embarqués, temps-réel ou protocoles de communication. Ils ont étudié la vérification des systèmes infinis (notamment, les systèmes communicants d'une part, et les systèmes temporisés d'autre part) et différents types de test (conformité, interopérabilité, robustesse) dans le cadre de projets nationaux (Calife-RNRT, Platonis-RNRT, Averroes-RNTL, Persee-ACI, SpaCIFY-ANR, Webmov-ANR, Averiss-ANR, Dots-ANR, Testec-ANR) et de contrats de recherche avec des industriels (BULL, EDF, Airbus, RATP, France Telecom R&D, THALES). Les outils McScM et TGSE ont été développés. Le LaBRI a notamment déjà collaboré avec l'ensemble des partenaires du projet VACSIM au travers du projet ANR TESTEC. Cette collaboration a permis la mise au point de modèles et méthodes de test pour systèmes temps-réel à flot de données. En effet, grâce à son expérience dans le domaine des automates temporisés, l'équipe du LaBRI a contribué avec l'INRIA Rennes au développement d'algorithmes de génération de tests pour une classe de systèmes proposés par les partenaires industriels (EDf - Geensoft). La particularité de ces travaux était de proposer une nouvelle modélisation concise et adaptée pour ce genre de systèmes, et de prendre en compte l'aspect symbolique du temps pour limiter l'explosion combinatoire dans la production de tests. Ces travaux ont été publiés dans des conférences internationales. Ce projet a aussi donné lieu à des travaux sur la complémentarité entre le test structurel et le test à base de modèles. Ces derniers sont toujours en cours.

LURPA

La thématique générale des recherches de l'équipe ISA (Ingénierie des Systèmes Automatisés) du LURPA : *Commande sûre des systèmes à événements discrets (Dependable Control of Discrete event Systems),* s'insère bien dans les préoccupations des axes 2 et 4 de l'AAP Ingénierie Numérique & Sécurité. Cette thématique, qui vise 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'accroître la sûreté de fonctionnement, constitue une proposition originale de l'équipe qui a été reconnue par l'IFAC (International Federation of Automatic Control), notamment sous la forme d'une série de workshops *Dependable Control of Discrete event Systems (DCDS).*

Cette équipe a, d'autre part, une longue expérience de la collaboration avec des équipes relevant de l'informatique ou des mathématiques appliquées, dans le cadre de l'Institut Farman (FR 3311), où nous avons été partenaires de plusieurs projets de recherche pluridisciplinaire avec le LSV (UMR 8643) et le CMLA (UMR 8536).

Enfin, un certain nombre des recherches s'effectuent dans le cadre de projets de recherche coopérative avec les centres de R&D de grandes entreprises (Alstom Power, EADS Innovation Works, EDF R&D) qui conçoivent et/ou exploitent des systèmes très critiques.

Complémentarité et valeur ajoutée des coopérations

Les deux industriels participant au projet (EDF et Dassault Systèmes) sont respectivement représentatifs des concepteurs et exploitants de systèmes critiques et de l'offre en outils d'ingénierie numérique de ces systèmes. Ceci garantit que les solutions techniques développées durant le projet VACSIM seront à la fois adaptées aux besoins des premiers, notamment en termes de langages et de pratiques métier, et aux caractéristiques et performances des outils logiciels d'ingénierie. La valorisation industrielle de ces solutions sera donc aisée.

Les laboratoires partenaires dans ce projet relèvent de l'automatique et de l'informatique. Cette particularité nous paraît essentielle pour apporter des solutions scientifiques répondant réellement aux besoins des concepteurs de systèmes de commande, en particulier pour ce qui concerne la modélisation des processus commandés, tout en s'appuyant sur des algorithmiques rigoureuses.

Enfin, les six partenaires ont une expérience de collaboration de trois ans, dans le cadre du projet TESTEC. Ils ont appris à se connaître et à coopérer efficacement durant ce projet. Les propositions scientifiques résultant du projet VACSIM répondront donc à de réels besoins industriels et pourront donner lieu rapidement à des solutions industrialisables.

5.2. QUALIFICATION DU COORDINATEUR DU PROJET / QUALIFICATION OF THE PROJECT COORDINATOR

Jean-Marc Faure est Professeur des Universités, 61ème section. Au niveau national et international, il est respectivement membre du Comité de Direction du GdR MACS et des comités techniques Discrete Event and Hybrid Systems et Manufacturing Plant Control de l'IFAC. Il a été ou est responsable d'une dizaine de projets de recherche coopérative avec de grandes entreprises (DS, EADS IW, EDF R&D, Renault) et du projet ANR TESTEC (07 TLOG 022). Il a d'autre part une longue expérience de collaboration avec des chercheurs relevant de l'informatique (Organisation des Journées Automatique et Informatique 2004, Comité de programme des conférences MSR'03,05,07,09,11, Projets dans le cadre de l'Institut Farman (FR 3311)).

5.3. QUALIFICATION, ROLE ET IMPLICATION DES PARTICIPANTS / QUALIFICATION AND CONTRIBUTION OF EACH PARTNER

- à renseigner par rapport à la durée totale du projet

Partenaire / partner	Nom / Name	Prénom / First name	Emploi actuel / Position	Discipline / Field of research	Personne. mois* / PM	Rôle/Responsabilité dans le projet / Contribution to the project 4 lignes max
DS	Gueguen	Thierry	Architecte	Méthode formelles et procesus	6	Coordination (comité de pilotage)
DS	Mevel	Eric	Directeur technique	Intégration outils	9	Coordination (comité de pilotage)
DS	Esteve	Robin	Ingénieur	Développe	33	Implémentation des algorithmes dans

			développement	ment de ControlBuild		ControlBuild
DS	Lebihan	Pierre	Ingénieur développement	Développement de ControlBuild	9	Implémentation des algorithmes dans ControlBuild
EDF R&D	Chériaux	François	Ingénieur-Chercheur Expert	Contrôle-commande	7,2	Coordination (comité de pilotage) Algorithme de test progressif par parties Utilisation automatisée d'un simulateur de parties opératives
EDF R&D	Chériaux	François	Ingénieur-Chercheur Expert	Contrôle-commande	7,2	Coordination (comité de pilotage) Algorithme de test progressif par parties Utilisation automatisée d'un simulateur de parties opératives
EDF R&D	Salaün	Patrick	Ingénieur-Chercheur Senior	Contrôle-commande	5,4	Algorithme de test progressif par parties Utilisation automatisée d'un simulateur de parties opératives
EDF R&D	Gazet	Thibaut	Ingénieur-Chercheur	Contrôle-commande	7,2	Cf. ci-dessus
EDF R&D	Picci	Laurence	Ingénieur-Chercheur	Contrôle-commande	7,2	Cf. ci-dessus
EDF R&D	Neyret	Maxime	Ingénieur-Chercheur	Contrôle-commande	7,2	Cf ci-dessus
I3S	Rueher	Michel	PR 27	Contraintes	7.2	Coordination (comité de pilotage) Définition de stratégies de recherche (pour la résolution des contraintes)
I3S	Collavizza	Hélène	MCF 27	Contraintes & Preuves	14.4	Définition de stratégies de recherche (pour la résolution des contraintes)
I3S	Comet	Jean-Paul	PR 27	Bioinformatique	14.4	Adaptation des techniques de V&V issues de la modélisation des systèmes biologiques complexes
I3S	Bernot	Gilles	PR 27	Bioinformatique	10.2	Cf ci-dessus
INRIA	Jéron	Thierry	DR INRIA Responsable du projet Vertecs	Vérification, contrôle et test de systèmes réactifs	9	Coordination (comité de pilotage) Vérification et test de systèmes réactifs temporisés
INRIA	Marchand	Hervé	CR INRIA	Contrôle et test de systèmes réactifs	9	Contrôle et test de systèmes réactifs
INRIA	Bertrand	Nathalie	CR INRIA	Vérification qualitative et quantitative	6	Vérification quantitative de systèmes réactifs et temporisés.
INRIA	Stainer	Amélie	Doctorante MENSR à l'Université de Rennes	Vérification quantitative	6	Vérification quantitative de systèmes réactifs et temporisés.
LaBRI	Rollet	Antoine	MCF 27	Test de systèmes informatisé	9	Coordination (comité de pilotage) Test de systèmes temps-réel

				s		
LaBRI	Sutre	Grégoire	CR CNRS	Modélisation et vérification	7,5	Automates communicants
LaBRI	Herbreteau	Frédéric	MCF 27	Modélisation et vérification	7,5	Vérification de systèmes temporisés
LaBRI	Felix	Patrick	MCF 27	Test de systèmes informatisés	6	Test formel, test de protocoles
LaBRI	Castanet	Richard	PR Emerite	Test de systèmes informatisés	3	Test de systèmes embarqués, protocoles
LURPA	Faure	Jean-Marc	PR 61	Analyse formelle des SED	9	Coordination (comité de pilotage) Vérification et test des SED
LURPA	Roussel	Jean-Marc	MCF 61	Analyse formelle des SED	9	Vérification et test des SED
LURPA	Lesage	Jean-Jacques	PR 61	Identification des SED	9	Identification des SED
LURPA	De Smet	Olivier	MCF 60	Identification des SED	6	Identification des SED

6. JUSTIFICATION SCIENTIFIQUE DES MOYENS DEMANDES / SCIENTIFIC JUSTIFICATION OF REQUESTED RESSOURCES

6.1. PARTENAIRE 1 / PARTNER 1 : DASSAULT SYSTEMES

- *Équipement / Equipment*

Néant

- *Personnel / Staff*

Il s'agit uniquement de personnel permanent (directeur technique, chef de projet et ingénieurs de développement). Le nombre d'h.mois prévus est de 57 pour la totalité du projet, soit un budget de frais de personnel de 327 594 euros.
L'aide demandée pour ce poste est de 161 712,29 €.

- *Prestation de service externe / Subcontracting*

Néant

- *Missions / Travel*

Ces frais concernent la tenue de deux réunions plénières et deux réunions techniques par an pour deux personnes.

Le budget total comprenant frais de déplacement, frais de restauration et frais d'hébergement est estimé à 5 000 euros.

- *Dépenses justifiées sur une procédure de facturation interne / Costs justified by internal procedures of invoicing*

Néant.

- *Autres dépenses de fonctionnement / Other expenses*

Néant.

6.2. PARTENAIRE 2 / PARTNER 2 : EDF R&D

- *Équipement / Equipment*

Néant

- *Personnel / Staff*

Il s'agit uniquement de personnel permanent (un Ingénieur-Chercheur Senior, un Ingénieur-Chercheur Expert, trois Ingénieurs-Chercheurs). Le nombre d'h.mois prévus est de 34,2 pour la totalité du projet, soit un budget de frais de personnel de 418 500 euros.
L'aide demandée pour ce poste est de 165 992,5 €.

- *Prestation de service externe / Subcontracting*

Néant.

- *Missions / Travel*

  - 4 000 € pour les missions liées aux travaux d'acquisition sur le terrain (réunions de travail, réunion plénières)
  - 1 000 € pour les missions relevant de colloques et congrès
  - Total 5 000 €

- *Dépenses justifiées sur une procédure de facturation interne / Costs justified by internal procedures of invoicing*

Néant.

- *Autres dépenses de fonctionnement / Other expenses*

Néant.

6.3. PARTENAIRE 3 / PARTNER 3 : I3S

- *Équipement / Equipment*

Néant

- *Personnel / Staff*

2 personnels non permanents seront recrutés :
Ingénieur de recherche :
Connaissance approfondie des techniques de programmation par contraintes et de la problématique des flottants. Compréhension des outils de model-checking et des problèmes de vérification. Expérience significative dans le développement de prototypes de recherche et leur évaluation.
Post Doc :
Connaissance approfondie des outils de model-checking. Solide background théorique et compétences dans l'évaluation expérimentale.
Coût total personnel : 128 510,43 €

- *Prestation de service externe / Subcontracting*

Néant

- *Missions / Travel*

- 5 missions en France pour 2 personnes par an
- 2 missions internationales par an
Coût total missions : 14 500 €

- *Dépenses justifiées sur une procédure de facturation interne / Costs justified by internal procedures of invoicing*

Néant

- *Autres dépenses de fonctionnement / Other expenses*

Achats d'ordinateur portables, livres, consommables, documentation et ouvrages divers, inscriptions aux colloques.
Coût total missions : 8 500 €

6.4. PARTENAIRE 4 / PARTNER 4 : INRIA

- *Équipement / Equipment*

Deux postes de travail seront financés sur le projet, l'un pour le doctorant recruté, l'autre pour le renouvellement de machines de l'équipe. Coût : 5 000 €.

- *Personnel / Staff*

Un doctorant sera recruté à l'INRIA sur la durée du projet (sujet de thèse : Test de propriétés quantitatives à partir de modèle temporisé). Il sera encadré par les personnels permanents participants au projet et sera financé entièrement sur ce projet (Coût : 134 568€).
Deux stagiaires de master seront également recrutés pour une durée totale de 6 mois (Coût : 13 800 €).
Total personnel : 148 368 €

- *Prestation de service externe / Subcontracting*

Néant.

- *Missions / Travel*

Les dépenses liées aux missions couvrent les missions propres à la réalisation du projet (réunions de suivi de projet, réunions entre partenaires) et les missions dans le cadre de conférences internationales où seront publiés les travaux du projet. Coût : 15 000 €

- *Dépenses justifiées sur une procédure de facturation interne / Costs justified by internal procedures of invoicing*

Néant.

- *Autres dépenses de fonctionnement / Other expenses*

Les frais généraux (assistance, encadrement, coût de structure) s'élèvent à 4% du coût total des dépenses, soit 6 734,72€.

Le coût total demandé par l'Inria est de 175 102,72 €.

6.5. PARTENAIRE 5 / PARTNER 5 : LABRI

- *Équipement / Equipment*

Néant

- *Personnel / Staff*

Ce projet permettra de recruter un post-doc sur 24 mois (sujet: validation de systèmes temporisés communicants), ainsi que trois stagiaires de master sur 6 mois chacun. L'objectif de ces stages est de réaliser des études de cas industrielles, i.e. de mettre en pratique sur des cas réels les résultats théoriques obtenus sur la validation des systèmes temporisés communicants.
Coût de personnel non permanent recruté sur le projet:

- 46 000 x 2 pour postdoc sur deux ans = 92 000 euros
- trois stages master/ingénieur: 7 600 euros

Sous-Total pour le personnel non permanent : 99 600 euros

- *Prestation de service externe / Subcontracting*

Aucune

- *Missions / Travel*

Réunions régulières des participants : de l'ordre de 5 réunions par an soit 15 réunions pour 3 personnes. Ces réunions sont prévues sur les différents sites des partenaires. On estime à environ 200 Euros en moyenne la mission : 5 x 3 pers x 3 ans x 200 euros = 9 000 euros.
Participation à des colloques européens ou internationaux pour échanger et présenter des résultats :

- 2 colloques x 3 personnes x 2 500 euros = 15 000 euros
- Frais d'inscription = 2 000 euros

Sous-total correspondant aux missions : 26 000 euros

- *Dépenses justifiées sur une procédure de facturation interne / Costs justified by internal procedures of invoicing*

Aucune

- *Autres dépenses de fonctionnement / Other expenses*

Achat de 3 ordinateurs : 1 600 x 3 = 4 800 euros
Consommables : 800 euros
Documentation et ouvrages divers : 1 000 euros

Sous-total autres dépenses de fonctionnement : 6 600 euros

6.6. PARTENAIRE 6 / PARTNER 6 : LURPA

- *Équipement / Equipment*

Néant.

- *Personnel / Staff*

Recrutement d'un doctorant sur la durée du projet (sujet de thèse : Validation par identification de SED et test).
Coût : 111 600 €.

- *Prestation de service externe / Subcontracting*

Néant.

- *Missions / Travel*

- 2 missions en France pour 3 personnes par an : 9 000 €
- 2 missions internationales par an pour 2 personnes : 15 000 €

- *Dépenses justifiées sur une procédure de facturation interne / Costs justified by internal procedures of invoicing*

Néant.

- *Autres dépenses de fonctionnement / Other expenses*

Mise à niveau du banc de test TeLoCo : 5 000 €

Achats d'ordinateur portables : 5 000 €

Livres, consommables, documentation et ouvrages divers : 2 000 €

Coût total autres dépenses : 12 000 €

7. ANNEXES / ANNEXES

7.1. REFERENCES BIBLIOGRAPHIQUES / REFERENCES

Références concernant l'identification des SED

[CGS06]M.P. Cabasino, A. Giua, C. Seatzu. Identification of deterministic Petri nets. WODES'06: 8th Int. Workshop on Discrete Event Systems (Ann Arbor, MI, USA), Jul 2006.

[CGS07] M.P. Cabasino, A. Giua, C. Seatzu, Identification of Petri nets from knowledge of their language. Discrete Event Dynamic Systems, Vol. 17, No. 4, pp. 447-474, Dec 2007.

[DFM08]M. Dotoli, M.P. Fanti, A.M. Mangini, Real Time Identification of Discrete Event Systems Using Petri Nets, Automatica, 2008, vol. 44, n°5, pp. 1209-1219

[KLE 05] S.Klein. Identification of Discrete Event Systems for Fault Detection Purposes. Doctorat de l'Ecole Normale Supérieure de Cachan, Spécialité : Electronique Electrotechnique et Automatique, juin 2005.

[MRM98]Meda, M.E., Ramirez, A., Malo, A. Identification in discrete event systems. IEEE SMC Conference, 11-14 Oct 1998, pp. 740–745.

[RLL09] M. Roth, J.-J. Lesage, L. Litz. Distributed identification of concurrent discrete event systems for fault detection purposes. European Control Conference 2009, ECC 2009, Budapest (Hungary), August 23-26 2009.

[RLL10a]M. Roth, L. Litz, J.-J. Lesage,. Identification of discrete event systems: Implementation issues and model completeness. 7th Int. Conf. on Informatics in Control Automation and Robotics, ICINCO'10, Funchal (Portugal), Vol. 3 pp. 73-80, June 2010.

[RLL10b]M. Roth, J.-J. Lesage, L. Litz. Black-box identification of discrete event systems with optimal partitioning of concurrent subsystems. American Control Conference, ACC'10, Baltimore (MD-USA), pp. 2601-2606, June 30-July 02, 2010.

[RO 10] M. Roth. Identification and fault diagnosis of industrial closed-loop discrete event systems. PhD thesis, ENS de Cachan, 225 p., October 2010

Références concernant les automates temporisés et l'analyse quantitative

[AD94] Rajeev Alur and David L. Dill. A theory of timed automata. Theoretical Computer Science, 126(2) :183–235, 1994.

[AD09] Eugene Asarin and Aldric Degorre. Volume and entropy of regular timed languages : Analytic approach. In Proceedings of the 7th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS'09), volume 5813 of Lecture Notes in Computer Science, pages 13–27. Springer, 2009.

[AD09b] Eugene Asarin and Aldric Degorre. Volume and entropy of regular timed languages : Discretization approach. In Proceedings of the 20th International

Conference on Concurrency Theory (CONCUR'09), volume 5710 of Lecture Notes in Computer Science, pages 69–83. Springer, 2009.

[ALP01] Rajeev Alur, Salvatore La Torre, George J. Pappas: Optimal Paths in Weighted Timed Automata. HSCC 2001: 49-62

[BBBBG08] Christel Baier, Nathalie Bertrand, Patricia Bouyer, Thomas Brihaye, and Marcus Größer. Almost-sure model checking of infinite paths in one-clock timed automata. In Proceedings of the 23rd Annual Symposium on Logic in Computer Science (LICS'08), pages 217–226. IEEE Computer Society Press, 2008.

[BBBM08] Nathalie Bertrand, Patricia Bouyer, Thomas Brihaye, and Nicolas Markey. Quantitative model-checking of one-clock timed automata under probabilistic semantics. In Proceedings of the 5th International Conference on the Quantitative Evaluation of Systems (QEST 2008), pages 55–64. IEEE Computer Society Press, 2008.

[BFHLPRV01] Gerd Behrmann, Ansgar Fehnker, Thomas Hune, Kim Guldstrand Larsen, Paul Pettersson, Judi Romijn, Frits W. Vaandrager: Minimum-Cost Reachability for Priced Timed Automata. HSCC 2001: 147-161

[BJSK10] N. Bertrand, T. Jéron,A. Stainer and M. Krichen. Off-line Test Selection with Test Purposes for Non-Deterministic Timed Automata. In Proceedings of the International Conference on Tools and Algorithms for the construction and Analysis of Systems (TACAS'11), LNCS, Springer, 2011.

[BW04] Timed Automata: Semantics, Algorithms and Tools, Johan Bengtsson and Wang Yi. In Lecture Notes on Concurrency and Petri Nets. W. Reisig and G. Rozenberg (eds.), LNCS 3098, Springer-Verlag, 2004.

[KT09] M. Krichen and S. Tripakis. Conformance testing for real-time systems. Formal Methods in System Design, 34(3):238{304, 2009.

Références concernant le test

[JJ05] C. Jard and T. Jéron. TGV: theory, principles and algorithms. Software Tools for Technology Transfer, 7(4):297-315, 2005.

[JJRZ05] B. Jeannet, T. Jéron, V. Rusu, E. Zinovieva. Symbolic Test Selection based on Approximate Analysis. In 11th Int. Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'05), LNCS, Volume 3440, Pages 349-364, Edinburgh (Scottland), April 2005.

[LMR10] O. Landry Nguena, H. Marchand, A. Rollet. Automatic Test Generation for Data-Flow Reactive Systems with time constraints (Short paper). In 22nd IFIP International Conference on Testing Software and Systems, Pages 25-30, Natal, Brazil, November 2010.

[MLN04] M. Mikucionis, K.G. Larsen, B. Nielsen. T-UPPAAL: online model-based testing of real-time systems. In Proceedings of the 19th International Conference on Automated Software Engineering (ASE'04), IEEE, 2004.

[TB03] Tretmans, G.J. and Brinksma, H. (2003) TorX: Automated Model-Based Testing. In: First European Conference on Model-Driven Software Engineering, December 11-12, 2003, Nuremberg, Germany.

Références concernant vérification / enforcement

[BHRG09] Howard Barringer, Klaus Havelund, David E. Rydeheard, Alex Groce: Rule Systems for Runtime Verification: A Short Tutorial. RV 2009: 1-24.

[BLS09] Andreas Bauer, Martin Leucker, and Christian Schallhart. Comparing LTL semantics for runtime verification. Journal of Logic and Computation, 2009.

[CM05] Severine Colin and Leonardo Mariani. Run-time verification. In Manfred Broy, Bengt Jonsson, Joost-Pieter Katoen, Martin Leucker, and Alexander Pretschner, editors, Model-based Testing of Reactive Systems, volume 3472 of LNCS, pages 525–556. Springer Verlag, 2005.

[CR07] Chen, F., Rosu, G.: MOP: An Efficient and Generic Runtime Verification Framework. In: OOPSLA 2007: Object-Oriented Programming, Systems, Languages and Applications, pp. 569–588 (2007)

[Fal09] Yliès Falcone. Etude et mise en oeuvre de techniques de validation à l'exécution, Phd Thesis, Université de Grenoble, 2009.

[Ham06] Kevin W. Hamlen. Security Policy Enforcement By Automated Program-Rewriting. PhD thesis, Cornell University, 2006.

[HG08] Klaus Havelund and Allen Goldberg. Verify your runs. In Verified Software : Theories, Tools, Experiments : First IFIP TC 2/WG 2.3 Conference, VSTTE 2005, Zurich, Switzerland, October 10-13, 2005, Revised Selected Papers and Discussions, pages 374–383, Berlin, Heidelberg, 2008. Springer-Verlag.

[LBW05] Jay Ligatti, Lujo Bauer, and David Walker. Enforcing Non-safety Security Policies with Program Monitors. In ESORICS, pages 355–373, 2005.

[Sch00] Fred B. Schneider. Enforceable security policies. ACM Trans. Inf. Syst. Secur., 3(1) :30–50, 2000.

Références pour CFSM

[ABS01] Aurore Annichini, Ahmed Bouajjani and Mihaela Sighireanu. TReX: A Tool for Reachability Analysis of Complex Systems. In Proceedings of the International Conference on Computer Aided Verification (CAV'01), LNCS 2102, 368-372, Springer, 2001.

[BV06] B. Berthomieu, F. Vernadat. Time Petri Nets Analysis with TINA. In Third International Conference on Quantitative Evaluation of Systems (QEST'06), IEEE, 2006.

[BZ03] Daniel Brand, Pitro Zafiropulo. On communicating Finite-State Machines. In Journal of the ACM (JACM), 30 (2), ACM, 1983.

[GLMR05] Guillaume Gardey, Didier Lime, Morgan Magnin and Olivier (H.) Roux. Romeo: A Tool for Analyzing Time Petri Nets. In Proceedings of the International Conference on Computer Aided Verification (CAV'05), LNCS 3576, 418-423, Springer, 2005.

[TC96] Stavros Tripakis and Costas Courcoubetis. Extending Promela and Spin for Real Time. In Proceedings of TACAS '96, LNCS 1055, 1996.

Références pour model-checking et contraintes

[AMP06] Armando, A. and Mantovani, J. and Platania, L. Bounded Model Checking of C Programs using a SMT solver instead of a SAT solver. LNCS: 3925(146-162), 2006.

[BCC99] Armin Biere, Alessandro Cimatti, Edmund Clarke, and Yunshan Zhu. Symbolic Model Checking without BDDs. In TACAS, volume 1579 of LNCS, pages 193-207. Springer,1999.

[Bry07] Randal E. Bryant. Modeling Data in Formal Verification. FMCAD 2007 (Formal Methods in Computer Aided Design).

[CLR11] A Dynamic Constraint-Based BMC Strategy For Generating Counterexamples Hélène Collavizza, Nguyen LeVinh, Michel Rueher, France Samuel Devulder, Thierry Gueguen, Geensys. 26th ACM Symposium On Applied Computing (SVT track), 2011.

[CoR06] Hélène Collavizza, Michel Rueher: Exploration of the Capabilities of Constraint Programming for Software Verification. TACAS 2006: 182-196.

[CRV10] Hélène Collavizza, Michel Rueher, Pascal Van Hentenryck: CPBPV: a constraint-programming framework for bounded program verification. Constraints 15(2): 238-264 (2010).

[DeP99] Delzanno, G., & Podelski, A. (1999). Model checking in CLP. In Proc. of TACAS 1999 (pp. 223–239).

[DKW08] Vijay D'Silva, Daniel Kroening, and Georg Weissenbacher. A survey of automated techniques for formal software verification. IEEE Trans. on CAD of Integrated Circuits and Systems, 27(7):1165-1178, 2008.

[GBR98] Gotlieb, A., Bernard, B., & Rueher, M. (1998). Automatic test data generation using constraint solving techniques. In Proc. of ISSTA 1998 (pp. 53–62).

[IYG08] Ivancic, F., Yang, Z., Ganai, M., Gupta, A., & Ashar, P. (2008). Efficient SAT-based bounded model checking for software verification. Theoretical Computer Science, 404(3), 256–274.

[JhM09] Ranjit Jhala, Rupak Majumdar: Software model checking. ACM Comput. Survey. 41(4): (2009)

[KPV03] Khurshid, S., Pasareanu, C. S., & Visser, W. (2003). Generalized symbolic execution for model checking and testing. In Proc. of TACAS 2003 (pp. 553–568).

[NiO07] Nieuwenhuis, R., Oliveras, A., Rodríguez-Carbonell, E., & Rubio, A. (2007). Challenges in satisfiability modulo theories. In RTA 2007 (pp. 2–18).

Références concernant la localisation des erreurs

[BNR03] Thomas Ball, Mayur Naik, and Sriram K. Rajamani. From Symptom to Cause: Localizing Errors in Counterexample Traces. Proc. POPL 2003. ACM Press, pp. 97-105

[GBC06] Andreas Griesmayer, Roderick Bloem, and Byron Cook. Repair of Boolean Programs with an Application to C. Proc of CAV'06 LNCS 4144, pp. 358-371.

[GSB07] Andreas Griesmayer, Stefan Staber, and Roderick Bloem Automated Fault Localization for C Programs. Electronic Notes in Theoretical Computer Science 174 (2007) 95–111.

[GCK06] Alex Groce, Sagar Chaki, Daniel Kroening , and Ofer Strichman. Error explanation with distance metrics. International Journal on Software Tools for Technology (2006) 8(3): 229–247

[GKL04] Alex Groce, Daniel Kroening, and Flavio Lerda Understanding Counterexamples with explain. Proc. of CAV 2004, LNCS 3114, pp. 453–456, 2004.

[Jun04] Ulrich Junker: QUICKXPLAIN: Preferred Explanations and Relaxations for Over-Constrained Problems. Proc. of AAAI 2004. Pp. 167-172.

[LiL10] Yongmei Liu, Bing Li: Automated Program Debugging Via Multiple Predicate Switching. Proc. AAAI 2010, AAAI Press.

[MaM11] Manu Jose, Rupak Majumdar. Cause Clue Clauses: Error Localization using Maximum Satisfiability. Proc. of PDLI 11 (32nd ACM SIGPLAN conference on Programming Language Design and Implementation).

[ZGG06] Xiangyu Zhang, Neelam Gupta, Rajiv Gupta: Locating faults through automated predicate switching. Proc. ICSE 2006, ACM press, pp. 272-281

Références bibliographiques des membres d'EDF R&D ayant trait au projet

[CPPF10]Conformance test of logic controllers of critical systems from industrial specifications, F. Chériaux, L. Picci, J. Provost (LURPA), J.M. Faure (LURPA). Proceedings of ESREL 2010, Rhodes, Greece, Ale, Papazoglou & Zio (eds), Taylor & Francis, ISBN 978-0-415-60427-7, pp. 1569-1576.

[CST08] F. Chériaux, D. Trognon, P. Salaün. Model-based Testing of Safety Logics. 18th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference and the 51st ISA POWID Division Symposium, Phoenix (USA), June 2008.

[CST09] Functional Test of Control Systems Ensuring a High Coverage Rate. F. Chériaux, P. Salaün, F. Daumas. Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC&HMIT 2009, Knoxville (USA), April 2009.

[SCT07] P. Salaun, F. Chériaux, D. Trognon. Prospects for model-based testing of discrete systems. 1st IFAC Workshop Dependable Control of Discrete Systems (DCDS'07), June 13-15, 2007, Cachan (France).

Références bibliographiques des membres d'I3S ayant trait au projet

J.-P. Comet, G. Bernot, Introducing continuous time in discrete models of gene regulatory networks . Book chapter in Proc. of the Evry Spring school on Modelling and simulation of biological processes in the context of genomics, March 3rd-7th, 9th Edition, Amar, Képès, Norris Ed., EDP Sciences pub., ISBN 978-2-7598-0545-7, p.61-94 , 2010.

A. Richard, J-P. Comet, G. Bernot, Formal Methods for Modeling Biological Regulatory Networks . Book Chapter in Modern Formal Methods and Applications, H.A. Gabbar Ed., Springer, ISBN: 1-4020-4222-1 , 2006.

Z. Khalis, J.-P. Comet, A. Richard, G. Bernot, The SMBioNet Method for Discovering Models of Gene Regulatory Networks . Invited review, Genes Genomes and Genomics, A. Mansour

Ed., Global Science Books, Vol.3, Special Issue 1, p.15-22, ISSN:1749-0383, ISBN 978-4-903313-33-7 , 2009.

G. Bernot, F. Tahi, Behaviour Preservation of a Biological Regulatory Network when Embedded into a Larger Network . Fundamenta Informaticae, IOS Press Amsterdam, Vol.91, Issue.3-4, p.463-485, ISSN:0169-2968 , 2009.

S. Troncale, J.-P. Comet, G. Bernot, Enzymatic Competition: Modeling and Verification with Timed Hybrid Petri Nets . Pattern Recognition, Vol.42, Num.4, p.562-566, April , 2009.

Références bibliographiques des membres de l'INRIA ayant trait au projet

[BBBBG08] Christel Baier, Nathalie Bertrand, Patricia Bouyer, Thomas Brihaye, and Marcus Größer. Almost-sure model checking of infinite paths in one-clock timed automata. In Proceedings of the 23rd Annual Symposium on Logic in Computer Science (LICS'08), pages 217–226. IEEE Computer Society Press, 2008.

[BBBM08] Nathalie Bertrand, Patricia Bouyer, Thomas Brihaye, and Nicolas Markey. Quantitative model-checking of one-clock timed automata under probabilistic semantics. In Proceedings of the 5th International Conference on the Quantitative Evaluation of Systems (QEST 2008), pages 55–64. IEEE Computer Society Press, 2008.

[BJSK11] N. Bertrand, T. Jéron, A. Stainer and M. Krichen. Off-line Test Selection with Test Purposes for Non-Deterministic Timed Automata. In Proceedings of the International Conference on Tools and Algorithms for the construction and Analysis of Systems (TACAS'11), LNCS, Springer, 2011.

[BSJK11] N. Bertrand, A. Stainer, T. Jéron, M. Krichen. A game approach to determinize timed automata. In 14th International Conference on Foundations of Software Science and Computation Structures (FOSSACS), March 2011.

[CJMR07] C. Constant, T. Jéron, H. Marchand, V. Rusu. Integrating formal verification and conformance testing for reactive systems. IEEE Transactions on Software Engineering, 33(8):558-574, August 2007.

[CJMR08] C. Constant, T. Jéron, H. Marchand, V. Rusu. Validation of Reactive Systems. In Modeling and Verification of Real-TIME Systems - Formalisms and software Tools, S. Merz, N. Navet (eds.), Chap. 2, pp. 51-76, Hermès Science, January 2008.

[CJMR06] C. Constant, T. Jéron, H. Marchand, V. Rusu. Combinaison entre vérification et test pour la validation de systèmes réactifs. In Traité I2C. Systèmes Temps Réel: Techniques de Description et de Vérification - Théorie et Outils, Vol. 1, Chap. 2, pp. 59-88, Hermès Science, 2006.

[JJ05] C. Jard and T. Jéron. TGV: theory, principles and algorithms. Software Tools for Technology Transfer, 7(4):297-315, 2005.

[JJRZ05] B. Jeannet, T. Jéron, V. Rusu, E. Zinovieva. Symbolic Test Selection based on Approximate Analysis. In 11th Int. Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'05), LNCS, Volume 3440, Pages 349-364, Edinburgh (Scottland), April 2005.

[JJR07] B. Jeannet, T. Jéron, V. Rusu. Model-based test selection for infinite state reactive systems. In Formal Methods of Components and Objects - FMCO 2006, Amsterdam, Netherlands, Revised Lectures, F.S de Boer, M. M. Bonsangue, S. Graf, W.-P. de Roever (eds.), Lecture Notes in Computer Science, Volume 4709, Pages 47-69, 2007.

[CJJ07] C. Constant, B. Jeannet, T. Jéron. Automatic test generation from interprocedural specifications. In TestCom/Fates07, LNCS, Pages 41-57, Tallinn, Estonia, June 2007.

[LMR10] O. Landry Nguena, H. Marchand, A. Rollet. Automatic Test Generation for Data-Flow Reactive Systems with time constraints (Short paper). In 22nd IFIP International Conference on Testing Software and Systems, Pages 25-30, Natal, Brazil, November 2010.

[FFJMM10] Y. Falcone, Fernandez J.-C, T. Jéron, H. Marchand, L. Mounier. More Testable Properties. In 22nd IFIP International Conference on Testing Software and Systems, Lecture note in Computer Science, Volume 6435, Pages 30-46, Natal, Brazil, November 2010.

Références bibliographiques des membres du LaBRI ayant trait au projet

[NMR10] O. Nguena Timo and H. Marchand and A. Rollet : Automatic Test Generation for Data-Flow Reactive Systems with time constraints. In 22nd IFIP International Conference on Testing Software and Systems (ICTSS10), (ex Testcom/Fates), November 8-12, 2010, Natal, Brazil, 6p. (short paper)

[SBRC10] F. Saad-Khorchef, I. Berrada, A. Rollet, R. Castanet : Automated Robustness Testing for Reactive Systems: Application to Communicating Protocols. In 10th International Conference on Innovative Internet Community Services (I2CS), Jubilee Edition 2010, June 3-5, 2010, Bangkok, Thailand. Lecture Notes in Informatics

[NR10] O. Nguena Timo and A. Rollet : Conformance testing of variable driven automata. In 8th IEEE International Workshop on Factory Communication Systems Communication in Automation (WFCS 2010), May 18-21, 2010, Nancy, France, 8p.

[RS07a] A. Rollet and F. Saad-Khorchef : A Formal Framework for Robustness Testing. In International Journal of Computer and Information Science (IJCIS) Volume 8, Number 2, June 2007, p.290-299

[CFCB09] Cao D., Felix P., Castanet R., Berrada I. : Testing Service Composition Using TGSE tool. In The proceedings of SERVICES 2009 (Part I) - IEEE 3rd International Workshop on Web Services Testing (WS-Testing 2009). In conjunction with 7th IEEE International Conference on Web Services (ICWS 2009), États-Unis d'Amérique (2009)

[CBFS06] Castanet R., Berrada I., Felix P., Sallah A. : Timed diagnostics and test case minimization for real time systems. In TESTCOM/FATES 2006, New York : Etats Unis (2006)

[BCF05] Berrada I., Castanet R., Felix P. : Testing Communicating Systems : a Model, a Methodology and a tool. In TESTCOM05, Montréal : Canada (2005)

[HS10] F. Herbreteau, B. Srivathsan. Efficient On-The-Fly Emptiness Check for Timed Büchi Automata. Proc. of the 8th Int. Symp. on Automated Technology for Verification and Analysis (ATVA'10), 2010.

[HSW10] F. Herbreteau, B. Srivathsan and I. Walukiewicz. Efficient Emptiness Check for Timed Büchi Automata. Proc. of the 22nd Int. Conf. on Computer Aided Verification (CAV'10), 2010.

[HST07] F. Herbreteau, G. Sutre and T.Q. Tran. Unfolding Concurrent Well-Structured Transition Systems. Proc. of the 13th Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'07), LNCS, Springer, Volume 4424, pages 706-720, Braga, Portugal, mar-apr 2007.

[BH06] B. Boigelot and F. Herbreteau. The Power of Hybrid Acceleration. Proc. of the 18th Int. Conf. on Computer Aided Verification (CAV'06), LNCS, Springer, Volume 4144, pages 438-451, Seattle USA, aug 2006.

[HLMS10] A. Heussner, J. Leroux, A. Muscholl, and G. Sutre. Reachability Analysis of Communicating Pushdown Systems. In Proc. 13th Int. Conf. Foundations of Software Science and Computation Structures (FOSSACS'10), Paphos, Cyprus, Mar. 2010, volume 6014 of Lecture Notes in Computer Science, pages 267-281. Springer, 2010.

[HLS09] A. Heussner, T. Le Gall, and G. Sutre. Extrapolation-based Path Invariants for Abstraction Refinement of Fifo Systems. In Proc. 16th Int. SPIN Workshop on Model Checking of Software (SPIN'09), Grenoble, France, Jun. 2009, volume 5578 of Lecture Notes in Computer Science, pages 107-124. Springer, 2009.

[LS07a] J. Leroux and G. Sutre. Acceleration in Convex Data-Flow Analysis. In Proc. 27th Int. Conf. Found. of Software Technology and Theor. Comp. Sci. (FSTTCS'07), New Delhi, India, Dec. 2007, volume 4855 of Lecture Notes in Computer Science, pages 520-531. Springer, 2007.

[LS07b] J. Leroux and G. Sutre. Accelerated Data-flow Analysis. In Proc. 14th Int. Static Analysis Symposium (SAS'07), Kongens Lyngby, Denmark, Aug. 2007, volume 4634 of Lecture Notes in Computer Science, pages 184-199. Springer, 2007.

Références bibliographiques des membres du LURPA ayant trait au projet

J. Provost, J.-M. Roussel, J.-M. Faure. Translating Grafcet specifications into Mealy machines for conformance test purposes. Control Engineering Practice, doi : 10.1016/j.conengprac.2010.10.001.

A. P. Estrada-Vargas, E. Lopez-Mellado, J.-J. Lesage. A comparative analysis of recent identification approaches for discrete-event systems. Mathematical Problems in Engineering, Vol. 2010, Article ID 453254, doi:10.1155/2010/453254.

H. Bel Mokadem, B. Bérard, V. Gourcuff, O. de Smet, J.-M. Roussel. Verification of a timed multitask system with Uppaal. IEEE Transactions on Automation Science and Engineering, 7(4), pp. 921-932.

F. Chériaux (EDF R&D), L. Picci (EDF R&D), J. Provost, J.-M. Faure. Conformance test of logic controllers of critical systems from industrial specifications, Proceedings of ESREL 2010,

Rhodes, Greece, Ale, Papazoglou & Zio (eds), Taylor & Francis, ISBN 978-0-415-60427-7, pp. 1569-1576.

J. Provost, J.-M. Roussel, J.-M. Faure. SIC-testability of sequential logic controllers. WODES 2010, Berlin, Germany, pp. 203-208, August 30 - September 1, 2010

M. Roth, J.-J. Lesage, L. Litz. Black-box identification of discrete event systems with optimal partitioning of concurrent subsystems. American Control Conference, ACC'10, Baltimore (MD-USA), pp. 2601-2606, June 30-July 02, 2010.

M. Roth, J.-J. Lesage, L. Litz. Identification of discrete event systems: Implementation issues and model completeness. 7th Int. Conf. on Informatics in Control Automation and Robotics, ICINCO'10, Funchal (Portugal), Vol. 3 pp. 73-80, June 2010

S. Ruel, O. de Smet, J.-M. Faure. Finding the bounds of response time of networked automation systems by iterative proofs. INCOM'09 : Proceedings of the 13th IFAC Symposium on Information Control Problems in Manufacturing, Moscow, June 2009

V. Gourcuff, O. de Smet, J.-M. Faure. Improving large-sized PLC programs verification using abstractions. 17th IFAC World Congress, Seoul (Korea), July 2008

7.2. BIOGRAPHIES / CV, RESUME

Gilles Bernot, short CV

Gilles Bernot, 51 years old, is "exceptional class" full professor of computer science at the École Polytechnique Universitaire of the university of Nice-Sophia Antipolis since 2007. He was previously full professor at Genopole®-Evry from 1992 to 2007 and assistant professor at the Ecole Normale Supérieur of Paris (ENS Ulm) from 1987 to 1992. PhD at the university of Orsay in 1986 and HDR in 1992. His research area since 1999 is the formal modelling of biological complex systems in the context of genomics.

Main responsabilities :

- founder and head of the research team in formal methods for software engineering at the computer science laboratory of Evry from 1993 to 1999,
- director of the computer science laboratory of Evry from 1998 to 2004 (UMR CNRS),
- founder and head of the research team in bioinformatics from 2000 to 2005,
- founding co-director of the Epigenomics Project of Genopole® from 2003 to 2007 (deputy director since 2007),
- Vice-President of the National Council of Universities (CNU) in computer science from 2003 to 2007 (approx. 3000 teaching-researchers),
- Scientific Delegate at the French Agency for the Evaluation of Research (AERES, Life Sciences Dpt) from 2007 to 2009,
- founder and head of the research axis in bioinformatics of the MDSC pole, I3S laboratory, at Sophia Antipolis since 2007,
- director of the IT doctoral school of Nice since 2009.
- Gilles Bernot is co-author of approximately 100 publications, among them approximately 50 in bioinformatics.

Hélène Collavizza, short CV

Hélène Collavizza a obtenu sa thèse de doctorat à l'Université d'Aix Marseille 1 (France) en 1991. Elle est Maître de Conférences à l'Université de Nice - Sophia Antipolis (France) depuis 1992, au département informatique de Polytech'Sophia. Elle y a passé son ***Habilitation à Diriger des Recherches*** en 2010.

Travaux de recherche

Mes travaux ont porté sur la vérification formelle des processeurs jusqu'en 1996, en utilisant un modèle orienté objet et des méthodes de simplification formelle. J'ai ensuite travaillé sur les problèmes de satisfaction de contraintes sur les domaines continus, en donnant une formalisation théorique des approches existantes et en introduisant une nouvelle approche pour le calcule des boîtes intérieures. Mes travaux actuels concernent la vérification de programmes bornés (par Bounded Model Checking ou BMC) en utilisant la programmation par contraintes (en collaboration avec Pascal Van Hentenryck de Brown University). Les méthodes de BMC classiques construisent une formule qui représente la conjonction de la négation de la spécification et des chemins d'exécution bornés dans le programme. Si cette formule est satisfiable, alors le programme n'est pas conforme à sa spécification. L'originalité de notre approche est de construire un système de contraintes de façon dynamique, grâce auquel nous pouvons éliminer au plus vite les chemins d'exécution impossible. J'ai également abordé cet aspect sous un angle plus théorique en basant le BMC sur la sémantique du langage et en utilisant le démonstrateur de théorèmes HOL (travaux effectués en collaboration avec Mike Gordon de Cambridge University).

Activités d'enseignement

Les points forts de mon activité d'enseignement sont :

- La création puis la responsabilité du cours d'architecture des ordinateurs.
- La mise en place, en collaboration avec mon collègue Jean-Paul Stromboni, de projets de 1ère année du cycle ingénieur associés aux journées DeViNT (Déficients Visuels et Nouvelles Technologies).
- L'encadrement de nombreux projets de 2ème année autour de la déficience visuelle.
- La responsabilité (de 2001 à 2007) du cours d'algorithmique en licence professionnelle LPSIL (IUT d'informatique).
- La création d'un nouveau cours d'introduction à la programmation dans le cadre du CIP (Cycle Initial Préparatoire) avec comme langage support Python.

Activités de diffusion et valorisation

Dans le cadre des projets DeViNT, j'ai développé une synthèse synthèse vocale déstinée à suppléer les informations sonores par des informations visuelles (voir http://vocalyse.polytech.unice.fr/, il y a environ un télé-chargement par semaine depuis janvier 2007). Depuis 2006, un CD-ROM contenant la plupart des projets est diffusé chaque année auprès des participants déficients visuels lors de la journée DeViNT. La synthèse vocale et le CD-Rom ont été présentés dans différents colloques, comme les XXVIème «Journées d'Etudes sur la Parole», le «Challenge Handicap Inter-universitaire de Metz» édition 2007 (nous avons remporté le 1er prix de la Communication autour de l'ordinateur)

ou l'émission ``La tête au carré'' sur France Inter le 12 Juin 2008 (voir http://sites.radiofrance.fr/franceinter/em/lateteaucarre/ index.php?id=68154).

Activités administratives

- Correspondante du département informatique auprès du CIP de Polytech'Sophia
- Membre élu du conseil du département informatique de Polytech'Sophia (2005 à 2007).
- Correspondante de la Bibliothèque Universitaire (2004 à 2007)
- Membre de commissions de spécialistes de 27ème section : assesseur de 1994 à 1998, vice-présidente Maître de Conférences de 1998 à 2001, membre simple de 2004 à 2008.
- Co-présidente de la journée DeViNT'06, organisation logistique des journées DeViNT'04 et 2005.
- Responsable pédagogique de la première année du cycle ingénieur informatique de Polytech'Sophia, (de 2000 à 2004, promotions de 100 à 120 étudiants, une quarantaine d'intervenants).
- Responsable de la communication du département informatique (de 1995 à 2000)
- Représentante de Polytech'Sophia au conseil de la licence professionnelle LPSIL (de 2000 à 2007)
- Membre élu du Conseil d'Administration de l'ESSI (de 1994 à 2000).

Jean-Paul Comet, short CV

Professeur d'Informatique à l'école polytechnique de l'Université de Nice – Sophia Antipolis, depuis le 1er septembre 2007

Extensions et applications de méthodes formelles pour l'aide à la modélisation formelle des réseaux de régulation génétique, utilisation du model-checking, des méthodes de tests, des approches par contraintes, de la transformation de graphes pour la bio-informatique des systèmes biologiques.

Co-encadrement de 6 étudiants en thèse :

A. Richard (2003-2006, modélisation des réseaux génétiques), S. Troncale (2005-2008, model-checking de réseaux de Petri hybride temporisés), M. Poudret (2005-2009, transformation de graphes pour les opérations topologiques de modélisation géométrique), J. Fromentin (2006-2009, modélisation hybride de réseaux génétiques), Z. Khalis (2006-2010, généralisation de la logique de Hoare pour la modélisation en biologie), J. Chanderis (depuis 2009, modélisation de systèmes biologiques par automates cellulaires 3D à coordonnées réelles).

Participation à l'animation de la recherche :

- Membre du comité scientifique d'une école jeunes chercheurs sur modélisation des réseaux biologiques. Juin 2010.
- Referee pour les revues Bioinformatics, IJMMS, TCBB, pour les conf. ISMB, ECAI ;
- Program Committee de ISMB'2005, JOBIM'2007, ICBPE'2009, CSBio'2010.
- Edition d'un livre, modelling and simulation of biological processes, 2004,
- Coordinateur avec M. Kaufman d'un numéro spécial de TSI sur la modélisation et simulation pour la post-génomique , paru en mars 2007,
- Organisation avec S. Vial et F. Quessette de 3 journées thématiques sur les réseaux d'interaction.

Publications :

10 chapitres de livres, 19 revues internationales avec comité de lecture,

1 revue nationale en 2004 et revue de vulgarisation,

Thierry Jéron est directeur de recherche à l'INRIA Rennes – Bretagne Atlantique, habilité à diriger des recherches et responsable scientifique de l'équipe-projet INRIA Vertecs depuis 2001. Il a obtenu sa thèse en 1991 et est chercheur à l'INRIA depuis 1993. Ses travaux de recherche actuels concernent la vérification et la validation de systèmes réactifs, plus particulièrement la génération de tests à base de modèles formels, la vérification et le diagnostic. Il a été impliqué dans de nombreux projets de recherche nationaux (ANR, RNTL, RNRT) et internationaux (IST Agedis, Réseaux d'excellence ARTIST, ARTIST Design) et collaborations internationales (Pays-Bas, Brésil, USA). Il est co-auteur d'une soixantaine d'articles dans des conférences internationales et journaux internationaux. Il est membre du groupe de travail IFIP TC10 (Computer Systems Technology) sur les systèmes embarqués.

Hervé Marchand est chargé de recherche à l'INRIA Rennes - Bretagne Atlantique dans l'équipe VerTeCs. Son domaine de recherches est principalement axé sur la validation des systèmes réactifs. En particulier, il s'intéresse au problème de la synthèse de contrôleurs, à la génération de tests et au diagnostic de pannes et pour de tels systèmes. Il a participé à des projets nationaux ou internationaux tels que Potestat Politess, Testec, Artist Design durant lesquels il s'est intéressé à la génération automatique de tests de conformité pour des systèmes réactifs et au déploiement de politique de sécurité dans les systèmes d'informations. Il est auteur de plus d'une cinquantaine d'articles dans des conférences internationales ou des revues. Depuis 2009, il est éditeur associé de Transactions on Automatic Control.

Principales publications :

1) Y. Falcone, Fernandez J.-C, T. Jéron, H. Marchand, L. Mounier. **More Testable Properties**. In 22nd IFIP International Conference on Testing Software and Systems, Natal, LNCS, Volume 6435, Pages 30-46, Brazil, November 2010. (Best paper award)

2) J. Dubreil, Ph. Darondeau, H. Marchand, **Supervisory Control for Opacity,** *IEEE Transactions on Automatic Control*, Vol 55(5):1089-1100, May 2010.

3) E. Rutten, H. Marchand, **Automatic Generation of Safe Handlers for Multi-Task Systems,** *Journal of Embedded Computing*, 3(4):255-276, 2009.

4) C. Constant, T. Jéron, H. Marchand, V. Rusu, **Integrating formal verification and conformance testing for reactive systems,** *IEEE Transactions on Software Engineering*, 33(8):558-574, August 2007.

5) G. Kalyon, T. Le Gall, H. Marchand, T. Massart, **Symbolic Supervisory Control of Infinite Transition Systems under Partial Observation using Abstract Interpretation**.
to appear in *Discrete Event Dynamical System*, 2011.

Antoine Rollet, short CV

Maître de conférences à l'Institut Polytechnique Bordeaux

Thèmes de recherche :

Test de systèmes temps-réel, Test de systèmes embarqués, Test de robustesse, Test de conformité

Formation :

- *2005- ... :* Maître de conférences à l'ENSEIRB / IPB
- *2004-2005 :* Attaché Temporaire d'Etudes et de Recherche (mi-temps) à l'Université de Reims depuis septembre 2004.
- *2002-2004 :* Thèse de Doctorat d'informatique à l'Université de Reims Champagne Ardenne,
- *1999-2002* : Ecole d'ingénieurs en Informatique de l'Université de Nice Sophia Antipolis.

Activités de recherche et d'enseignement :

- *Année 2007- 2009 :* Responsable de la filière Réseaux et Systèmes Répartis en 3ème année informatique Enseirb

Publications significatives récentes :

- Sébastien Salva and Antoine Rollet. Testabilité des services web. Ingénierie des Systèmes d'Information RSTI série ISI, 13(3) :35–58, 06 2008.
- Antoine Rollet and Fares Saad Khorchef. A Formal Framework for Robustness Testing. International Journal of Computer and Information Science, 8(2) :290–299, 06 2007.
- Omer Nguena Timo and Hervé Marchand and Antoine Rollet Automatic Test Generation for Data-Flow Reactive Systems with time constraints. In 22nd IFIP International Conference on Testing Software and Systems (ICTSS10), (ex Testcom/Fates), November 8-12, 2010, Natal, Brazil, 6p. (short paper).
- Omer Nguena Timo and Antoine Rollet. Conformance testing of variable driven automata. In 8th IEEE International Workshop on Factory Communication Systems Communication in Automation (WFCS 2010), May 18-21, 2010, Nancy, France, 8p., 05 2010.
- Sébastien Salva and Antoine Rollet. Test purpose generation for timed protocol testing. In 2nd International Conference on Communication Theory, Reliability, and Quality of Service (CTRQ 2009), July 20-25, 2009 - Colmar, France, page 7p, France, 07 2009.

Jean-Marc Faure received the Ph.D. degree from the Ecole Centrale de Paris and the "Habilitation à diriger des recherches" from the University of Aix-Marseille in 1991 and 1997 respectively. He is currently Professor of Automatic Control at the Institut Supérieur de Mécanique de Paris and researcher at LURPA (Laboratory of Research in Automated Production) of Ecole Normale Supérieure de Cachan, France. His research fields are modeling, synthesis and analysis of Discrete Event Systems (DES) with special focus on formal verification and test methods to improve dependability of critical systems. J.-M. Faure is member of the IFAC TC 1.3 "Discrete Event and Hybrid Systems" and vice-chair of the TC 5.1 "Manufacturing Plant Control". He is with Jean-Jacques Lesage the initiator of the IFAC Workshops series "Dependable Control of Discrete Systems". He has served in many committees of IFAC and IEEE conferences.
Main recent publications:
Translating Grafcet specifications into Mealy machines for conformance test purposes, J. PROVOST, J.-M. ROUSSEL, J.-M. FAURE, Control Engineering Practice, doi : 10.1016/j.conengprac.2010.10.001
Building meaningful timed plant models for verification purposes, M. PERIN, J.-M. FAURE, 13th IFAC symposium on Information Control Problems in Manufacturing, INCOM'09, Moscou(Russie), 3-5 juin 2009, pp. 970-975
Improving large-sized PLC programs verification using abstractions, V. GOURCUFF, O. DE SMET, J.-M. FAURE, 17th IFAC World Congress, Seoul (Korea), July 2008
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'08, pp. 334-339, Göteborg (Sweden), May 2008
Manufacturing plant control challenges and issues, G. MOREL, P. VALCKENAERS, J.-M. FAURE, C. E. PEREIRA, C. DIEDRICH, Control Engineering Practice, Volume 15, Issue 11, pp. 1321-1331, November 2007

Jean-Marc Roussel received the Ph.D. degree from the Ecole Normale Supérieure de Cachan in 1994. He is currently Associate Professor in Automatic Control at Ecole Normale Supérieure de Cachan. His research fields are algebraic approaches for synthesis, verification and conformance test of Discrete Event Systems (DES). Since 2010, he is responsible of the team Automation Engineering of LURPA.
Main recent publications:
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, February 2011, doi: 10.1016/j.ress.2010.10.001
Verification of a timed multitask system with Uppaal, H. BEL MOKADEM, B. BERARD, V. GOURCUFF, O. DE SMET, J.-M. ROUSSEL, IEEE Transactions on Automation Science and Engineering, 7(4), pp. 921-932
SIC-testability of sequential logic controllers, J. PROVOST, J.-M. ROUSSEL, J.-M. FAURE, WODES 2010, Berlin, Germany, pp. 203-208, August 30 - September 1, 2010

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'08, pp. 187-192, Göteborg (Sweden), May 2008

Designing dependable controllers using algebraic specifications, J.M. ROUSSEL, J.M. FAURE, Control Engineering Practice, Volume 14, Issue 10, pp. 1143-1155, October 2006

7.3. IMPLICATION DES PERSONNES DANS D'AUTRES CONTRATS / STAFF INVOLVEMENT IN OTHER CONTRACTS

Part.	Nom de la personne participant au projet / name	Personne . Mois	Intitulé de l'appel à projets, source de financement, montant attribué / Project name, financing institution, grant allocated	Titre du projet : Project title	Nom du coordinateur / coordinator name	Date début & Date fin / Start and end dates
DS[5]	Thierry Gueguen	9	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11
DS	Eric Mevel	9	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11
EDF	François Chériaux	10	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11
EDF	Patrick Salaün	10	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11
EDF	Laurence Picci	8	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11
EDF	Thibaud Gazet	8	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11
I3S	Gilles Bernot	7	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11
I3S	Gilles Bernot	7	ANR BLANC 2010	BioTempo	A. Siegel	01.03.11 / 28/02/14
I3S	Hélène Collavizza	9	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11

[5] Société ayant racheté la société Geensoft qui participait au projet TESTEC

I3S	Jean Paul Comet	8	ANR BLANC 2010	BioTempo	A. Siegel	01.03.11 / 28/02/14
I3S	Michel Rueher	9	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11
I3S	Michel Rueher	8	Européen (FP7)	Mancoosi	R. Di Cosmo	01.02.07 / 31/05/11
I3S	Michel Rueher	4	ANR-2010-SEGI-013-01	AEOLUS	R. Di Cosmos	01.12.10 / 31.03.14

INRIA	Thierry Jéron	10	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11
INRIA	Hervé Marchand	10	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11
INRIA	Nathalie Bertrand	6	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11

LaBRI	Antoine Rollet	10	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11
LaBRI	Patrick Félix	6	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11
LaBRI	Richard Castanet	6	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11

LURPA	Jean-Marc Faure	10	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11
LURPA	Jean-Marc Roussel	10	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11
LURPA	Olivier de Smet	6	ANR-07 TLOG 022	TESTEC	J.M. Faure	01.12.07 / 31.07.11