Laboratoire VERIMAG

Directeur: Nicolas Halbwachs

Vague A : Campagne d'évaluation 2014–2015

Unité de recherche

Dossier d'évaluation

Unité Mixte de Recherche 5104 CNRS - Grenoble INP - UJF

Centre Équation
2, avenue de VIGNATE
F-38610 GIERES
tel : +33 456 52 03 40
fax : +33 456 52 03 50
http://www-verimag.imag.fr

Contents

Avant-Propos

Ce document constitue le rapport d'activité du laboratoire Verimag pour la période allant du 1er janvier 2009 au 30 juin 2014, ainsi que les perspectives pour la prochaîne période. Nous avons choisi de rédiger ce rapport en français pour les parties factuelles et administratives, et en anglais pour les parties scientifiques, de nombreux membres du laboratoires n'étant pas francophones.

Note sur les références bibliographiques : La liste complète des publications de la période est donnée dans l'Annexe D, par équipe et par catégorie. Dans le texte, les clés de référence sont constituées d'une lettre pour l'équipe (S=Synchrone, D=DCS, T=Tempo), d'une lettre pour la catégorie (J=Journal, C=Conference, B=Books and Edited Proceedings, P=PhD Thesis, O=Other visible publication) et d'un numéro d'ordre. Les références externes ou hors période sont données en annexe I.

Foreword

This document is the activity report of Verimag laboratory for the period comprised between January 1st, 2009 and June 30, 2014, together with the perspectives for the next period. It has been decided to write this report in French for the factual and administrative parts, and in English for the scientific chapters, since many members of the laboratory don't read French.

Note on bibliographic references : The complete list of publications for the period is given in Appendix D, sorted by team and category. In the text, publications are references by keys, made of a letter for the team (S=Synchrone, D=DCS, T=Tempo), a letter for the category (J=Journal, C=Conference, B=Books and Edited Proceedings, P=PhD Thesis, O=Other visible publication) and a number. External and previous references are given in Appendix I.

Chapter 1

General Report
Présentation de l'unité

1.1 Introduction

Verimag a été créé en 1993, d'abord comme unité mixte industrielle avec la société Vérilog, puis, à partir de 1997, comme UMR commune au CNRS, à l'Université Joseph Fourier (Grenoble 1), et à Grenoble INP. Verimag a été dirigé par Joseph Sifakis jusqu'en 2006, et par Nicolas Halbwachs depuis lors.

Le domaine général des recherches menées au laboratoire concerne la conception et la validation des systèmes informatiques embarqués, en privilégiant une approche formelle.

A ce jour, les effectifs sont de 41 permanents (23 enseignants-chercheurs, 8 chercheurs, 6 ingénieurs et 4 administratifs), auxquels il faut ajouter une douzaine de post-doctorants et contractuels, et une trentaine de doctorants. Verimag est hébergé dans des locaux de l'Université Joseph Fourier, situés dans deux bâtiments en lisière du domaine universitaire de Saint-Martin d'Hères et Gières.

1.2 Politique scientifique

Initialement focalisés sur la programmation synchrone et la vérification par model-checking, les thèmes de recherche du laboratoire se sont largement diversifiés, notamment vers la modélisation et l'analyse des systèmes temporisés et hybrides (discrets-continus), la sécurité informatique, la modélisation des systèmes à la frontière du logiciel et du matériel (systèmes sur puces, réseaux de capteurs), les méthodes d'analyse par interprétation abstraite, la prise en compte de "propriétés non fonctionnelles"[1], la conception par composants, l'algorithmique distribuée.

Durant toute la période 2009-2014, le laboratoire a été structuré en 3 équipes, dont on trouvera plus loin les rapports détaillés :

- Synchrone : définition et implantation de langages de programmation temps-réel, approches d'implantation dirigées par les modèles, conception par composants, analyse de pire temps d'exécution ; modélisation fidèle et simulation efficace de systèmes numériques (systèmes sur puce, réseaux de capteurs) incluant des propriétés non-fonctionnelles ; applications du model-checking, fondements et applications de l'interprétation abstraite, méthode SMT ; test automatisé ; algorithmique distribuée.
- Distributed Complex Systems (DCS) : Conception de systèmes embarqués basée sur des modèles à composants, en particulier le langage et la chaîne d'outils BIP qui permet un flot de conception rigoureux, de la vérification passant à l'échelle et des méthodes d'implémentation "correctes par construction" — Sécurité : preuve de protocoles de sécurité, formalisation et vérification de propriétés de sécurité, analyse de vulnérabilité de code, test de propriétés de sécurité — Vérification de logiciel en particulier basé sur

[1] faute d'une meilleure expression : il s'agit de propriétés quantitatives concernant le temps d'exécution, l'occupation mémoire, la consommation énergétique, ...

de l'analyse statique et des procédures de décision, outils de preuve — vérification basée sur des modèles, en particulier modèles d'architecture et modèles non-fonctionnels.

- Tempo : Méthodes et outils pour la validation, la vérification et l'instrumentation de systèmes continus et hybrides, application aux systèmes de contrôle embarqués, aux circuits analogiques, et aux systèmes biologiques ; techniques d'optimisation multi-critères appliquées au déploiement d'applications sur plates-formes multi-coeurs.

Cependant, le domaine de recherche général — les systèmes embarqués — et l'approche générale consistant à s'appuyer sur des méthodes formelles, sont largement communs aux 3 équipes. Un autre trait commun est la mise en œuvre d'une synergie entre la recherche fondamentale et les applications : les thèmes de recherche sont largement inspirés des applications — coopérations et études de cas industrielles —, et les solutions proposées sont confrontées aux applications. Enfin, ces solutions sont très souvent implémentées dans des outils logiciels pérennes. Les frontières des équipes sont perméables, et les collaborations inter-équipes sont nombreuses, avec des projets communs et des publications cosignées.

Le laboratoire bénéficie d'un contexte local très favorable, auquel il prend toute sa part.

- Les thématiques de Verimag occupent une position centrale dans celles du LabEx PERSYVAL, créé en 2012, et dédié à la maîtrise de la convergence des mondes physique et numérique. Nous avons largement participé au montage de ce LabEx et à son animation.
- Verimag a pris une part importante à la création du CRI, Centre de Recherche Intégrative, hébergeant des projets collaboratifs. Joseph Sifakis en assure la direction scientifique, et le groupe "BIP" de l'équipe DCS fait partie du CRI depuis sa création en 2010.
- Verimag participe activement à l'Institut Carnot LSI et au pôle de compétitivité Minalogic.
- Nous avons étroitement participé à la préparation du projet de bâtiment PILSI, qui devrait être disponible en 2016 et héberger 3 laboratoires : le LIG, le LJK, et Verimag, ainsi que l'UMS MI^{2}S.

Le laboratoire entretient des collaborations formalisées avec la plupart des laboratoires grenoblois du pôle MSTIC (TIMA, TIMC, LIG, LJK, GIPSA, Institut Fourier), notamment dans le cadre du LabEx PERSYVAL.

Les réseaux Artist, Artist2 et Artist-Design, dont Joseph Sifakis était le principal instigateur, ont assuré au laboratoire une excellente visibilité européenne et internationale. Maintenant terminés, ces réseaux se prolongent par l'action EMSIG (Embedded Systems Special Interest Group[2]), à laquelle nous participons (Joseph Sifakis et Nicolas Halbwachs appartiennent au comité de pilotage). La collaboration de longue date de l'équipe Synchrone avec STMicroelectronics permet au laboratoire d'être visible sur des projets liés à la conception de systèmes sur puce, au niveau européen (projet OpenES dans le cadre CATRENE, projet de projet dans le cadre ECSEL).

Au niveau national, nous participons au GDR GPL[3], et notamment à son groupe "compilation" que nous avons contribué à créer. Nous sommes très présents dans les projets des investissements d'avenir liés aux systèmes embarqués (d'abord "Briques Génériques du Logiciel Embarqué" - BGLE, puis "Logiciel Embarqué et Objets Communicants" - LEOC) avec 2 projets BGLE en cours, un projet "sécurité numérique" et un projet LEOC en cours de négociation. Nous sommes également très impliqués dans des projets ANR, en collaboration avec des partenaires académiques ou industriels.

1.3 Profil d'activités

Unité/Equipe	Recherche académique	Interaction avec l'environnement	Appui à la recherche	Formation par la recherche	Total
Ensemble	57%	5%	15%	23%	100%
dont équipe Synchrone	51%	6%	16%	27%	100%
dont équipe DCS	57%	3%	18%	22%	100%
dont équipe Tempo	63%	10%	5%	22%	100%

On trouvera en annexe D les éléments factuels justifiant ce profil, tant au niveau global du laboratoire qu'à celui de chaque équipe .

[2] www.emsig.net/
[3] gdr-gpl.cnrs.fr

	UJF	INP	CNRS	Total
Chercheurs et enseignants-chercheurs	10 MC, 4 Pr	6 MC, 2 Pr	3 CR, 4 DR, 1 DREm	30
Administratifs	3		1	4
Ingénieurs	1 IE		1 AI, 4 IR	6
Contractuels et postdoctorants	12			12
Doctorants	31			31

Table 1.1: Effectifs au 30 juin 2014

	Synchrone	DCS	Tempo
Chercheurs	1CR, 2DR	1CR, 1DR, 1DREm	1CR, 1DR
Enseignants-chercheurs	6MC, 1PR	6MC, 5PR	1MC
Ingénieurs	1IR	2IR	1IR
Contractuels et postdoctorants	5	4	1
Doctorants	5	16	9

Table 1.2: Effectifs des équipes

	UJF	INP	CNRS
2009			+1 CR
2010		+1 MC	+1 IR −1 IE
2011	−1 Pr		
2012	−1 IE		−2 CR −1 DR + 1DR +1 AI
2013	−1 MC		
2014	+1 IE		
Bilan	−2	+1	0

Table 1.3: Mouvements de personnels permanents

1.4 Organisation et vie de l'unité

1.4.1 Personnel

Les effectifs au 30 juin 2014 sont donnés par la table 1.1, et la répartition par équipe par la table 1.2. La table 1.3 donne les évolutions des effectifs en personnel permanent au cours de la période. Les enseignants-chercheurs relèvent tous de la 27e section du CNU. Par contre, après la division de la section 7 du CoNRS, si la plupart des membres du laboratoire ont opté pour la section 6, certains se sont mieux reconnus dans la section 7. Cette répartition reflète bien la position du domaine de recherche du laboratoire, à la frontière du logiciel, du matériel et du contrôle.

Dans la période considérée, le laboratoire a bénéficié du recrutement d'une chargée de recherche (Barbara Jobstmann) et d'un assistant-ingénieur (Philippe Genin) CNRS et d'une maître de conférence Grenoble INP (Claire Maïza), de l'arrivée en mutation d'un ingénieur de recherche CNRS (Olivier Lebeltel) et d'un ingénieur d'étude UJF (Patrick Fulconis), et de la promotion d'un CR en DR (David Monniaux). La même période a vu le départ en retraite d'un professeur UJF (Pierre-Claude Scholl) et le passage en éméritat d'un directeur de recherche (Joseph Sifakis), le départ en mutation de 2 ingénieurs d'étude (Claude Dutreilly, CNRS, et Jean-Noël Bouvier, UJF), ainsi que le départ en détachement d'une CR CNRS (Barbara Jobstmann) et d'un maître de conférence UJF (Pascal Lafourcade). En conséquence, actuellement, 3 chercheurs[4] CNRS et un enseignant-chercheur sont en détachement.

La figure 1.1 donne l'évolution des effectifs non-permanents au cours de la période.

[4]En plus de B. Jobstmann, Sergio Yovine (DR) et Stavros Tripakis (CR)

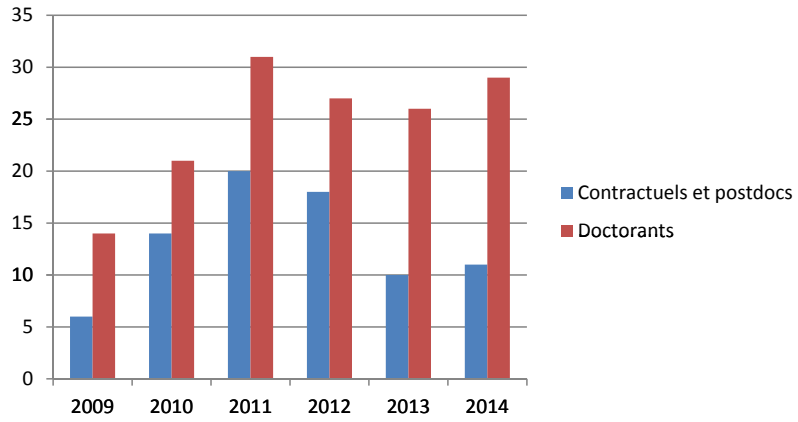


Figure 1.1: Évolution des effectifs non permanents

1.4.2 Gouvernance

L'organigramme fonctionnel est donné en annexe B. Le bureau est constitué de la direction (directeur et directeur adjoint) et des responsables d'équipe. Le bureau est réuni chaque fois que des décisions ponctuelles doivent être prises rapidement. Le conseil de laboratoire est réuni tous les 2 mois. Sa composition formelle est donnée en annexe H, mais les séances sont ouvertes à tous les permanents. Les séances du conseil donnent lieu à un compte-rendu. Enfin, une assemblée générale du laboratoire est organisée une fois par an.

1.4.3 Services

Les services sont centralisés.

L'administration est assurée par 4 personnes : une gestionnaire en charge des affaires générales, de la gestion des personnels et du budget, une personne en charge du suivi des contrats, et deux personnes chargées des missions et des commandes. Avec, chaque année, une douzaine d'embauches de contractuels, de l'ordre de 300 missions et 250 commandes, et une vingtaine de contrats en cours, ce service assure des fonctions vitales pour le laboratoire.

Le service informatique est constitué de 2 ingénieurs, en temps normal. Cependant, au cours de la période, ce service a souvent du fonctionner en sous-effectif ou avec des contractuels, du fait du départ d'un ingénieur en 2010 qui n'a été remplacé qu'en 2012, puis d'un autre départ en 2012, qui n'a été remplacé qu'en 2014. Le service gère un parc informatique conséquent (13 serveurs, 246 stations fixes ou mobiles). Certaines fonctionnalités (réseau, messagerie) sont confiées à l'unité mixte de service MI^{2}S.

Les ingénieurs de recherche sont affectés aux équipes, dans lesquelles ils participent aux projets, dont ils assurent souvent la gestion, et développent et maintiennent les logiciels issus de la recherche. Ils sont aussi chargés de certaines tâches d'intérêt général, concernant notamment les outils communs.

1.4.4 Outils communs

Au fil des années, nous avons développé un certain nombre d'outils pour faciliter la gestion du laboratoire, outils accessibles par l'intranet. Ces développements constituent des tâches d'intérêt général confiées aux ingénieurs de recherche. Nous disposons d'une base de données financières, permettant de gérer et de suivre les contrats quelle que soit la tutelle gestionnaire [5], d'une base de gestion des effectifs, des locaux et de l'annuaire, d'un outil de demande de mission et de gestion des absences, et d'un outil d'annonce et de suivi des différents séminaires. Au cours de la période, le site Web du laboratoire a été refait, et une base de données des publications a été développée.

[5] Quoique le laboratoire soit en délégation globale de gestion financière depuis 2012, il reste quelques projets au CNRS.

1.4.5 Budget, gestion

On trouvera le détail des budgets du laboratoire pour 2012 et 2013 dans les tableaux joints au dossier. Pour donner une idée générale, la figure 1.2 donne les montants des ressources 2013 (y compris les salaires des personnels permanents) et leur utilisation. La figure 1.3 donne le détail des ressources propres (89% du budget non consolidé) selon leurs origines.

Le laboratoire prend en charge les dépenses communes : frais d'infrastructure, salaire d'une gestionnaire contractuelle, l'essentiel des dépenses d'équipement et de maintenance, achat de fournitures et de licences de logiciels, missions du directeur et frais de réception. Les ressources propres sont utilisées au niveau des équipes. Selon les années, le laboratoire peut reverser une partie de la dotation aux équipes, ou, au contraire, doit demander aux équipes une participation aux dépenses communes.

Le laboratoire est en délégation globale de gestion financière (DGGF) à l'UJF depuis 2012. A l'époque, il était prévu que tous les laboratoires grenoblois passent en DGGF à l'une de leurs tutelles à brève échéance, et nous avons accepté d'être un laboratoire pilote de ce processus. Cependant, l'expérience n'a pas été poursuivie, et la promesse qui nous avait été faite d'aligner les pratiques de la tutelle gestionnaire sur les meilleures pratiques n'a pas été tenue. Notre demande de revenir en gestion mixte UJF/CNRS, n'a pas eu d'effet jusqu'ici.

1.4.6 Locaux

Le laboratoire occupe des locaux de 1440 m^2 appartenant à l'UJF. Au début de la période, ces locaux se composaient du bâtiment Equation-3 et de 2 plates-formes du bâtiment CTL. En 2011, à l'installation du CRI au CTL, le bâtiment Equation-4 a été réhabilité, et les occupants d'une plate-forme du CTL ont déménagé dans la moitié d'Equation-4 (l'autre moitié étant occupée par une équipe du LIG).

1.4.7 Animation interne

Le séminaire du laboratoire a lieu assez régulièrement, en moyenne une ou deux fois par mois. On trouvera en annexe I la liste des intervenants pour la période. En plus de ce séminaire général et des réunions des équipes, un séminaire régulier de cryptologie est organisé en collaboration avec d'autres laboratoires concernés (Institut Fourier, LJK, CEA), et un séminaire sur l'analyse de logiciel, commun aux équipes Synchrone et DCS, a vu le jour récemment.

Enfin, depuis 2013, nous organisons annuellement une série de séminaires des doctorants de 2e année (voir §3.1.2).

1.5 Faits marquants

En 2012, nous avons eu à déplorer la disparition de Paul Caspi, chercheur d'exception et grande figure du laboratoire. En son honneur, l'ACM SIGBED[6] a créé le "prix de thèse Paul Caspi" qui a été décerné pour la première fois cette année.

NOE Artist design : Verimag a été l'instigateur du réseau d'excellence Artist-Design[7], faisant suite aux réseaux Artist et Artist2. Ces réseaux ont fédéré une vaste communauté de recherche sur la conception des systèmes embarqués en Europe, et ont donné au laboratoire une visibilité européenne et internationale exceptionnelle.

Start-up Argosim : Les méthodes de test de logiciels synchrones développées au laboratoire depuis 1998, et expérimentées avec succès dans plusieurs projets (notamment le projet Minalogic COMON, voir page 131), ont conduit à la création d'une start-up en 2013, Argosim[8]. Voir §2.1.2.3

[6] SIGBED est le groupe d'intérêt consacré aux systèmes embarqués de l'*Association for Computing Machinery*.
[7] ww.artist-embedded.org
[8] www.argosim.com

	Total	Fonctionnement	Salaires
Total établissements	3 508 155	149 180	3 358 975
CNRS	1 246 044	65 000	1 181 044
UJF	1 886 776	64 180	1 822 596
Grenoble INP	375 335	20 000	355 335
Contrats et programmes	1 424 936	679 748	745 187
Total	**4 912 861**	**808 699**	**4 104 162**

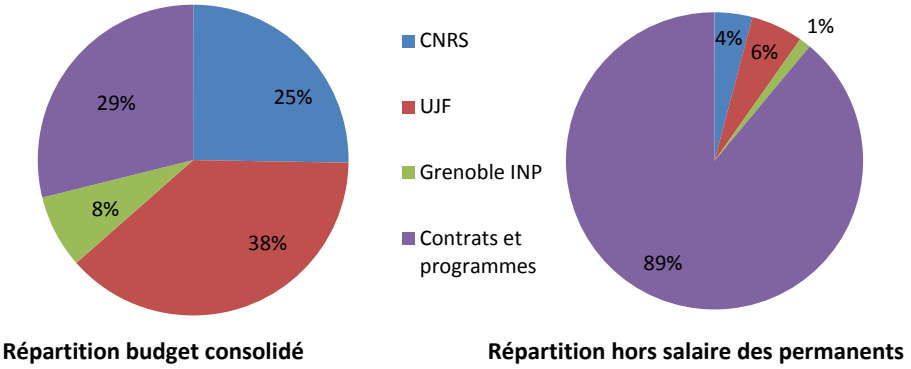


Figure 1.2: Budget consolidé 2013

	Total	Fonctionnement	Salaires
Europe hors ERC	614 207	349 508	264 699
ERC	121 192	66 019	55 173
ANR	265 183	88 655	176 528
Projets hors MESR	44 285	34 783	9 502
Invest. d'avenir	259 979	41 518	218 461
C. industriels	72 802	61 215	11 587
Autres	27 289	18 052	9 237
Dotations spécifiques	19 999	19 999	0
Total	1 424 936	679 748	745 187

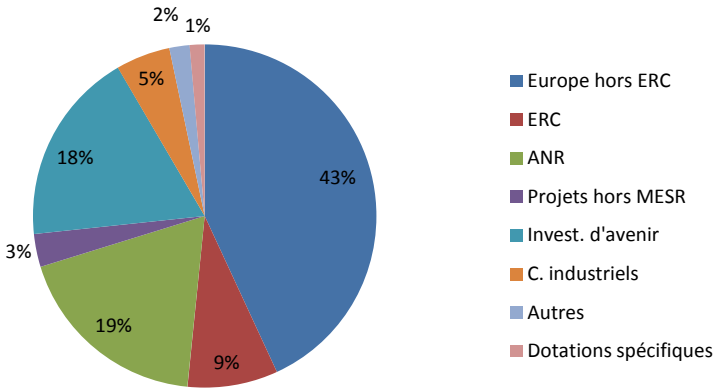


Figure 1.3: Détail des ressources propres 2013

Projet ERC STATOR : David Monniaux, DR CNRS de l'équipe Synchrone, a obtenu un projet ERC "Starting investigator" sur l'analyse statique des programmes (voir §2.1.2.2). Ce projet, doté d'un budget de 1472 k€, se déroule de 2013 à 2017.

Organisation de grandes conférences : Verimag a organisé plusieurs événements importants, en particulier la conférence CAV 2009 (Computer Aided Verificationi[9]) — principale conférence internationale sur la vérification automatisée — et surtout ETAPS 2014, (European Joint Conferences on Theory and Practice of Software[10]), qui est un des principaux événements scientifiques concernant les méthodes de développement du logiciel : regroupant 6 conférences internationales et plus de 20 workshops, ETAPS 2014 a attiré près de 800 participants.

Pour célébrer les 20 ans de Verimag nous avons organisé trois journées scientifiques, les 26, 27 et 28 septembre 2012, où nous avons invité un pannel d'orateurs prestigieux :

Gilles Barthe (IMDEA)	Ahmed Bouajjani (LIAFA, Paris)
Luca Benini (Università di Bologna)	Tom Henzinger (IST Austria)
Albert Benveniste (Inria, Rennes)	Joseph Sifakis (EPFL et Verimag)
Gérard Berry (Collège de France)	Parvin Varaiya (Berkeley)

Reinhard Wilhelm (Saarland University)

Ces journées ont attiré une soixantaine de participants.

"Best papers" : Meilleur article pour Jannik Dreier à la Third IEEE International Conference on Information Privacy, Security, Risk and Trust [D-C111] ; Meilleur article pour Stéphane Devismes, Karel Heurtefeux et Yvan Rivierre à ICNC'2011 [S-C47] ; Meilleur article pour Radu Iosif à CADE 2013 [D-C19] ; Meilleur article d'étudiant pour Yvan Rivierre à SSS'2013 [S-C13].

Distinctions Joseph Sifakis a été élu à l'Académie des Sciences en 2011, et nommé Commandeur de la Légion d'Honneur en 2012. Nicolas Halbwachs a été élu à l'Academia Europaea en 2010. En 2010, le projet MARAE a été distingué par la Fondation de Recherche pour l'Aéronautique et l'Espace (FRAE), et, à cette occasion, Saddek Bensalem a reçu un des trois prix de la meilleure publication scientifique des programmes de recherche.

1.6 Auto-évaluation

1.6.1 Forces

La principale force de Verimag est la qualité de sa production scientifique et sa visibilité internationale. La qualité des publications est attestée par de nombreuses références : par exemple, plus de 40% des articles publiés dans la conférence EMSOFT'2013 citent au moins une publication de Verimag, et les publications citées datent presque toutes de moins de 10 ans. Le rayonnement du laboratoire apparaît en particulier dans notre forte présence dans les comités de programme des conférences et workshops (123 comités pour la période, dont 4 co-présidences de comités de conférences majeures); nous avons aussi organisé de très nombreux événements et écoles (voir §D.1.2).

La cohérence scientifique du laboratoire est un atout : Verimag réunit des compétences complémentaires sur des sujets variés, mais tous reliés à un domaine bien délimité. Les coopérations entre les différents groupes sont réelles et fructueuses. Les thématiques se sont diversifiées, mais sans dispersion.

La synergie entre les recherches fondamentales et les applications est une réalité. Les collaborations industrielles directes sont généralement limitées à des contrats CIFRE, mais souvent poursuivies sur le long terme. Par ailleurs, nous avons de nombreuses collaborations industrielles dans le cadre de projets (Europe, ANR, pôles de compétitivité).

[9] www-cav2009.imag.fr/
[10] www.etaps.org

L'encadrement des doctorants est de bonne qualité : il y a eu, certes, 5 abandons sur la période, mais 3 d'entre-eux ont eu lieu en fin de 1ère année, les deux autres correspondant à des embauches avant la fin de la thèse. Par ailleurs, nos docteurs se placent bien; sur 36 doctorants diplômés pendant la période, aucun n'est en recherche d'emploi : 11 ont obtenu des situations académiques, 16 sont dans l'industrie, 8 sont en postdoctorat, 1 est en sabbatique.

Enfin, un changement de génération est en cours, de manière satisfaisante. De jeunes chercheurs et enseignants-chercheurs prennent des responsabilités (encadrement, coordination de projets, passage de HDR), et le remplacement de la direction (directeur, responsables d'équipe) est prêt.

1.6.2 Faiblesses

Le nombre de thèses encadrées est assez variable, et peut être jugé faible, au regard des capacités d'encadrement. La difficulté de recruter des doctorants — qu'il faut souvent attirer par des stages des années à l'avance — et un certain élitisme en sont la cause. La durée des thèses est longue, mais dans la moyenne de l'Ecole doctorale, et les doctorants sont financés sur cette durée.

L'évolution des thématiques rend quelque peu caduques le périmètre et la cohésion des équipes, c'est pourquoi une restructuration du laboratoire sera proposée dans le projet.

Il reste des enseignants peu impliqués dans la recherche, mais certains de ceux qui étaient dans ce cas en début de période se sont ré-investis dans des projets et se sont remis à publier.

Nous continuons d'avoir de grandes difficultés à recruter au CNRS. En 2012, un candidat du laboratoire a été bien classé, mais a préféré une grande université américaine; en 2014, une excellente candidate n'a pas été classée en section 06, avant d'être recrutée 1ère sur un poste Inria !

1.6.3 Opportunités

Le nouveau bâtiment PILSI, en construction dans le cadre du plan "Campus", devrait accueillir, en 2016, les 3 laboratoires LIG, LJK et Verimag, ainsi que l'unité de service MI^{2}S. Non seulement, nous espérons que ces nouveaux locaux seront plus propices à notre activité, mais la proximité immédiate d'autres équipes de recherche en informatique et en mathématiques appliquées ouvre aussi des perspectives de coopération scientifique ainsi que de synergie entre les services. Sur ce dernier point, la réflexion est déja bien avancée entre les 3 laboratoires.

Nous espérons que la construction d'une grande université Grenoble-Alpes donnera une meilleure visibilité internationale au site, et ouvrira une ère de relations apaisées entre nos tutelles. La structuration en pôles thématiques est tout-à-fait adéquate, et Verimag trouve naturellement sa place au sein du pôle MSTIC.

1.6.4 Menaces

Le détachement de 3 chercheurs CNRS et d'un enseignant-chercheur représente une vraie perte de potentiel. En particulier, le thème de l'analyse de protocoles cryptographiques est affaibli, d'autant que Yassine Lakhnech est moins présent du fait de ses fonctions de vice-président recherche de l'UJF. Cette perte de potentiel risque fort de perdurer, avec la réduction drastique des créations de postes universitaires, et nos difficultés à recruter au CNRS.

Le déménagement au campus ouest du groupe BIP avec le CRI est évidemment un risque pour la cohésion du laboratoire.

Le passage en DGGF est un handicap pour le laboratoire. Il serait temps que les tutelles reconnaîssent que cette démarche est un échec.

Chapter 2

Detailed scientific report
Présentation détaillée

2.1 Synchrone team

2.1.1 Synchrone team: Scientific production

The main scientific topics of the team during the period are:

1. **Modeling and simulation** for systems-on-a-chip and networks of embedded systems; trade-off between efficiency and precision/faithfulness in models and simulation tools;
2. **Distributed algorithms**, in particular self-stabilizing ones, applications to security in sensor networks
3. Foundations of, tools for, and applications of **abstract interpretation**, **decision procedures**
4. Languages and methods for the **automatic testing** of embedded reactive systems
5. **Implementation and analysis** methods for critical embedded systems, in particular worst-case-execution-time analysis (WCET) and real-time calculus; energy-aware implementations for embedded systems; recent focus on manycore hardware platforms.

The work on simulation and modeling for sensor networks, and the work on distributed algorithms applied to security in sensor networks, have been done in the context of the two ANR projects ARESA and ARESA2 (see pages 140 and 126), together with L. Mounier and P. Lafourcade of the DCS team, and in collaboration with Orange Labs. The work on modeling and simulation for systems-on-a-chip is done in the context of a long-lasting collaboration with STMicroelectronics. The work on manycore architectures is done in collaboration with S. Mancini from the TIMA laboratory, and Kalray. We also started quite recently (November, 2013) a collaboration with Orange Labs in Grenoble, and Didier Donsez from the LIG laboratory, about smart cities. A CIFRE PhD student (L. Lemke, see page 160) works on the formal models that are needed for the deployment of software onto the devices of the smart city, in the context of shared and open infrastructures.

In the last five years, the team has fully integrated the work on distributed algorithms and systems, and the work on worst-case-execution-time analysis (we lead the ANR project W-SEPT, page 114). The work on hardware architectures has converged with the work on programming languages for critical systems, allowing us to participate in the national project CAPACITES led by Kalray, where we propose to study the implementation of dataflow synchronous formalisms on the manycore platform proposed by the company, in close collaboration with end users like Airbus, Eurocopter, Dassault Aviation, etc. The work on abstract interpretation has evolved into a well identified activity, including fundamental work on the core of abstract interpreters (ANR ASOPT project, page 132) and new directions like the certification of tools (ANR VERASCO project, page 115, together with members of the DCS team), and the application to WCET. D. Monniaux has obtained an ERC grant on research of new approaches in combinations of abstract interpretation and satisfiability testing (STATOR, page 109).

2.1.1.1 Modeling and simulation

The development of complex hardware/software embedded systems, and networks of embedded systems, faces several problems: the cost of the final object to be developed, either a system-on-a-chip (SoC), or a deployment in the field for, e.g., sensor networks; the lack of observability means for this final object; and its late availability. This is the reason why the properties of the hardware/software systems are most of the time assessed by simulations, using a system-level model, also called *virtual prototype* (VP). The VP is an executable model, and simulations are performed with discrete-event simulation engines, typically. Hardware companies have adopted SystemC and Transaction-Level Modeling (TLM) for SoCs. As in any context where modeling and simulation are used, a trade-off has to be found between the precision of the model, and the speed of the simulation. We worked on several aspects related to this trade-off. We also extended previous work to include non-functional properties: energy consumption and temperature in SoCs, security in sensor networks.

In the openTLM project (see page 141), we worked on compilation techniques and formal verification of SystemC. A new tool called PinaVM includes a compiler front-end [**S-C77**] [**S-C76**] and a back-end [**S-C58**] able to generate code for the model-checker SPIN. PinaVM is internally based on the "static single assignment representation" (SSA), which we showed allows an efficient encoding [**S-C84**]. PinaVM is also used for purposes other than verification like optimized compilation.

In the ANR project HELP (see page 125), we proposed a general instrumentation method that adds energy consumption information to a functional TLM model (in the form of *power-state* or *traffic* models); we defined an efficient co-simulation method, with a temperature simulator [**S-C27**] [**S-C9**] [**S-C10**] (either ATMI, or the tool ACEplorer developed by the partner DOCEA Power). The libraries developed in the project are available as free software; the principles of the instrumentation and the cosimulation have been implemented by the industrial partners, in their design flow. We worked on the coupling between modeling principles and implementations of the simulation engine, in order to get significant improvements of the simulation speed. We proposed to augment TLM models with a notion of *task with duration*, first in Java with jTLM [**S-C53**] [**S-C52**], and then as a conservative extension of SystemC that allows parallel executions [**S-C20**], without changing the behavior of the existing models that do not use the extension. This is a very promising approach, compatible with existing TLM models (contrary to approaches like TLM-DT that require an entire rewrite of the models) and offering more potential for parallelization than other approaches targetting the simulation engine only; the topic continues in the openES project (page 109). We also worked on temporal decoupling to improve simulation speed even in the sequential case [**S-C17**].

We developed the component model 42 (PhD of T. Bouhadiba, page 158, [**S-P7**]), inpired by Ptolemy, as a means to study models of communication and computation (MoCCs). The "42ization" of SystemC [**S-C80**] was a first step towards system-level models of SoCs, in which some components may be known only by very abstract but formalized specifications (given by *contracts* for instance); these formal contracts, together with the semantics of an assemblage of components, allows to "execute" a system at a very early stage of development. We continue this topic in the openES project (page 109), in the wider context of functional and extra-functional properties (like energy-consumption and temperature, studied in the project HELP).

In the context of a CIFRE PhD with STMicroelectronics (G. Funchal, page 158), we studied memory models [**S-C51**], and how to include them in the TLM models that serve for the development of low-level software in SoCs. We proposed to abstract the detailed behavior of the memory hierarchy by non-deterministic models, able to show the memory bugs of the low-level software.

In the context of the ANR projects ARESA and ARESA2 (pages 140 and 126), we proposed simulation models for energy consumption in sensor networks; the simplest models are based on the "joule-per-bit" abstraction, relating the energy consumption to the number of bits transmitted; this is implementable in any simulator. Since this abstraction hides the cost of *idle listening*, it is sometimes necessary to augment the model with some information on the state of the hardware, especially the radio component. This requires a significant change in the simulation models, and the definition of manageable abstractions, for a reasonable simulation speed. We defined such models, first using tools of the synchronous community, and then using tools of the sensor network community; the comparison between models and real measurements will be finally possible in collaboration with Orange labs, in the context of a CIFRE PhD starting in 2014. In ARESA2, our main topic was the trade-off between energy consumption and security (see also section 2.1.1.2); as far as modeling is concerned, we studied and implemented the attacker models.

2.1.1.2 Distributed algorithms

This topic aims at providing new solutions for modern networks, such as Wireless Sensor Networks (WSNs). These networks are resource-constrained, large-scale, and fault-prone. The work consists in designing distributed algoritms, in particular probabilistic ones. We validate our solutions using formal analysis and simulations.

During the last four years, we followed several directions, including the design and analysis of self-stabilizing, probabilistic, and/or secure algorithms.

Concerning the self-stabilizing topic, most of our work has been done as part of the PhD thesis of Yvan Rivierre [**S-J12**, **S-C28**, **S-J3**, **S-C13**, **S-J4**], this latter dealing with distributed spanning structures. The remainder of the work deals with properties related to self-stabilization [**S-C94**, **S-C83**, **S-C91**, **S-J16**, **S-J17**, **S-C65**, **S-C70**, **S-J15**, **S-C71**, **S-C42**, **S-C32**]. Especially, we proposed new fault-tolerant properties and solutions [**S-C2**]. Concerning the probabilistic topic, we analytically study random walk protocols [**D-C42**, **D-J3**]. We have evaluated the performances of various types of random walk, in particular self-avoiding and biased random walks.

Finally, we designed in [**D-C17**] resilient versions of the tabu random walks to solve secure convergecast routing in WSNs prone to insider attacks. Our solution uses some classical lightweight cryptographic mechanisms to ensure data confidentiality, integrity, and authenticity. Then, we introduce an original self-adaptive reputation mechanism to maintain an interesting delivery rate. This work has been done as part of the ANR project ARESA2 (page 126). The point of view of fault-tolerance allowed us to answer the question of attackers in sensor networks. This is a problem in itself, because the Dolev-Yao hypothesis of an attacker that can do anything but decrypt messages without the key, is far too strong for sensor networks. We have to limit the power of attackers, and decide beforehand what type of attacks a sensor network can resist.

2.1.1.3 Decision procedures and abstract interpretation

The semantics of finite unfoldings of program executions can be expressed as first-order formulas over arithmetic or extensions thereof. Many verification approaches therefore use *decision procedures* to check whether such formulas hold, or *satisfiability testing* to get solutions (models). Such solutions often express *counterexamples* to purported properties or inductive invariants: in many approaches, solutions directly map to counterexample traces that can be reported back to the user (in case of a trace from an initial state to an error state) or fed back to a refinement procedure. It is therefore of paramount importance that decision procedures are efficient in practice, even in cases known to have high worst-case complexity (e.g. quantifier alternation), despite the progresses made in *satisfiability modulo theory* (SMT) since 2000.

We have researched efficient procedures for decision [**S-C26**] and *quantifier elimination* in linear arithmetic [**S-C75**, **S-C38**]. With respect to quantifier-free formulas generated from program semantics, we have researched partial abstractions, which dramatically improve the performance of SMT-solver in the case of formulas arising from worst-case execution time analysis (WCET) [**S-C1**].

Outside of certain very restricted classes of programs, reachability after an unbounded number of program steps is a undecidable problem. Abstract interpretation is an approach to static analysis where sets of reachable states, too difficult to represent exactly, are over-approximated by symbolic sets on which it is possible to compute; the final result of an analysis by abstract interpretation is generally an *inductive invariant* chosen within a specific *abstract domain* (e.g. products of intervals or convex polyhedra, for numerical properties).

Traditionally, abstract interpretation computes inductive invariants as the limit of an ascending *Kleene iteration* sequence, accelerated using *widening* operators. Widenings are a known cause of imprecision (leading to false positives) and of non-monotonicity (better knowledge of the system may lead to more false positives); we have researched methods for computing the exact limit, based on quantifier elimination [**S-J18**] and policy iteration [**S-C54**, **S-J8**]. We proposed also a method to improve fixpoints obtained by widening-narrowing [**S-C33**]. Another source of imprecision is the enforced approximation into the abstract domain at every program location; we bypass it using implicit path enumeration by SMT-solving [**S-J8**, **S-C35**, **S-C34**, **S-C54**, **S-C61**, **S-J18**].

One criticism of formal methods is that the tools (e.g. static analyzers) may themselves contain bug: how much can we trust their results? We have therefore investigated the construction of static analysis tool fully proved correct within the Coq proof assistant, relying on a constraint-only representation of convex polyhedra [**S-C11**, **D-C34**].

2.1.1.4 Automatic testing

During the last decade, the team worked on stochastic extensions of synchronous languages. The motivation is to simulate the (physical) environment of a reactive system. Reactive systems and programs are particular, in that they usually function in a closed loop with their environment. Simulating the environment is compulsory to be able to test reactive programs with realistic inputs.

During the last five years, the industrial partners of the Minalogic project COMON (see page 131) have experimented with the tools developed at Verimag [S-C5]. A major result of the project is that our tools and methodology are useful, not only for automated testing, but also for requirement engineering. This has led to the creation of the startup company Argosim (see below, section 2.1.2.3).

2.1.1.5 Implementation and analysis

We worked on the implementation of critical systems, starting from high level models of control systems, and targeting various embedded execution platforms. We proposed the notion of *Loosely Time-Triggered Architectures*, which are more common and less costly than purely time-triggered architectures like TTA, and yet allow implementations that guarantee important properties of critical systems [S-C74]. We worked on an extension of the Lustre language that allows to describe extra-functional and implementation-specific information such as tasks, execution rates, and buffers [S-C81]. The interest of the method is twofold: automatic code generation for a (particular) real-time OS, and automatic functional model extraction for analysis and verification. Note that the language is based on a very abstract view of hard real-time OSes, which makes the support of a particular OS relatively easy (we made experiments with Xenomai and OSEK).

During the Synchronics project (see page 133), we worked on specific topics related to data-flow languages in general, and Lustre in particular. The main results are an object-oriented extension of Lustre [S-C102], and a general method for performing separate compilation of data-flow languages [S-C98].

In the context of the PhD of N. Berthier (see page 157), we used synchronous models and discrete control, to propose a coordination layer between the hardware of small embedded systems like the nodes of a sensor network, and the upper layer application software. This is similar to paravirtualization techniques, and allows to avoid bugs due to the concurrent use of the devices, like the ones due to peaks in power consumption.

We lead the ANR project W-SEPT (page 114) in which we propose to benefit from the information of a high-level synchronous program (typically Lustre or SCADE) to improve the precision of a worst-case-execution-time (WCET) analysis. The first results are promising [S-C22, S-C1].

We work on the integration of worst-case execution time and delays in scheduling analyses. Based on the improvement of cache analysis for cache-related preemption delays [S-J9], we investigate how to better integrate WCET and delays in a set of scheduling analyses. Our main results largely improve previous analyses in the context of preemptive systems with cache memory [S-C4].

In our quest for the appropriate level of details in the models of embedded systems, we started a study of real time calculus (RTC) which abstracts concrete behaviors into *arrival curves*, in the context of the ANR FoToVP project (see page 139). Analytical models like RTC cannot handle a notion of *state*, which leads to very rough abstractions if the system under study has several functioning modes characterized by very different values of the quantitative property to be modeled (energy consumption, throughput, latency, ...). There were proposals for introducing states in the methods for RTC, based on timed automata. We extended the existing schemes with a granularity-based abstraction [S-C78]. We studied the fundamental problem of *causality* [S-C66] [S-C41] for the formalism of arrival curves, which becomes a real problem when those curves are produced from timed automata. We also designed a tool based on abstract interpretation tools and SMT-solving, to get the best provable RTC output using a state-based model [S-C64].

2.1.2 Synchrone team: Scientific influence

2.1.2.1 Participation in the spread of the synchronous technology

During the last ten years, synchronous languages and synchronous methods for the implementation of (critical) embedded systems have gained a lot of visibility in the major conferences of the domain (DAC, DATE, ACM EMSOFT and ACM LCTES). Moreover, we established a connection between the community working on

critical systems with the synchronous technology, and the community working on scheduling methods or worst-case execution time analysis; members of the team were involved in the program committees of several real-time scheduling conferences like ECRTS (2012, 13, 14), RTAS (2014), RTNS (2013, 14). We defined and lead the ANR project W-SEPT (see page 114) which gathers the main actors of WCET analysis in France. See section 2.1.1.5 for the results obtained so far.

Recognizing the pioneering work of our colleague Paul Caspi, ACM SIGBED created in 2014 the "Paul Caspi" PhD thesis award; for this first edition we received 11 nominations. F. Maraninchi is a member of the selection committee. Between 2009 and 2014, we have chaired the ACM conference EMSOFT twice, and been part of the programme committee six times. We also participated in the PCs of ACM LCTES five times, DAC Embedded Software and Systems, the track "E2: Compilation and Code Generation for Embedded Software" at DATE three times. F. Maraninchi and N. Halbwachs are members of the steering committee of EMSOFT. F. Maraninchi is an associate editor of the newly created open-access journal *Leibniz Transactions on Embedded Systems (LITES)*.

We participate in the definition of the project CAPACITES[1] led by the company Kalray. This is a big national project to study the use of manycore architectures in the domain of critical systems. We propose to extend the synchronous compilers to these architectures. This is a unique opportunity to understand the needs of the major actors of critical systems in France (Airbus, Eurocopter, Dassault Aviation, ...) and to design usable solutions.

2.1.2.2 ERC Grant for D. Monniaux

In the 2000s, two approaches to the sound static analysis of software were industrially successful: 1. abstract interpretation, in particular for safety-critical embedded systems (e.g. Astrée and PolySpace commercial tools) 2. predicate abstraction (e.g. Microsoft Device Driver verifier), with the development of powerful *satisfiability modulo theory* (SMT) solvers. Furthermore, in abstract interpretation, alternatives to Kleene iterations (downward and upward policy iteration, reduction to mathematical programming...) have been proposed.

The purpose of the STATOR project (see page 109), a starting investigator grant from the European research council (ERC), is to investigate combined approaches, mixing abstraction, SMT-solving and alternate iteration schemes, and the relationship between numerical and discrete (enumerated types, pointer information) data, in order to improve both precision and efficiency.

The first concrete application is an approach based on abstraction of partial programs so as to scale SMT-solving up to worst-case execution time [**S-C1**].

2.1.2.3 Creation of a startup company: Argosim

The success of our methods and tools for automatic testing, assessed by their use in the COMON project (see page 131), has led to the creation of the Argosim[2] startup company in 2013, which aims at industrializing the concepts (random-based simulations of environments, automated testing, and requirements engineering) and the associated technology (stochastic data-flow synchronous languages, constraint solving based on BDDs and polyhedra).

2.1.2.4 Long-lasting Collaborations, Industrial Transfer, and Impact on Standards

The team maintains close collaborations with STMicroelectronics (since 2002) and Orange Labs (since 2004). This allows us to transfer results progressively. In particular, the relationship with STMicroelectronics is a unique opportunity to have an impact on the norms for the transaction-level-modeling of systems-on-a-chip. Some of the results of the HELP ANR project (page 125) have been first developed at Verimag and published as open-source software, then adapted to the design flow at ST and DOCEA Power, and are currently being promoted in the normalisation committees. The collaboration with Orange allows to benefit from a physically deployed sensor network, for the evaluation of our algorithms and modeling techniques.

[1] Call LEOC "Logiciel Embarqué et Objects Connectés", investissements d'avenir
[2] www.argosim.com

2.1.3 Synchrone team: Interaction with the economic, social and cultural environment

Since 2007, F. Maraninchi is one of the two academic members of the organisation and evaluation committees of the software cluster of the competitiveness pole Minalogic[3]. This role includes the participation in the monthly meeting of the organisation committee, and in two evaluation committees per year.

The team has a lot of interactions with the local and national economic environment related to embedded systems: 10 collaborative projects with indutrial partners (STATOR, OpenES, W-SEPT, VERASCO, HELP, ARESA2, COMON, ASOPT, ARESA, OpenTLM, see details in section E); 3 ongoing CIFRE contracts (with ST and Orange Labs), and 3 more under negociation for 2014-2017. One of the projects (COMON) was sufficiently close to transferrable results, and led to the creation of a startup company (see above, section 2.1.2.3). Other projects give us an access to normalization committees, see above, section 2.1.2.4. The long-lasting cooperation with STMicroelectronics gives us an access to the new ECSEL European program[4].

The definition and management of the master curriculum in embedded software and systems at Grenoble INP (see below) gives a lot of opportunities for informal collaborations and discussions with people from industry. A recent study on embedded systems in France, by OPIEEC[5], entitled "Evolution of jobs and training needs for embedded systems", mentions that some master curricula are directly linked to research laboratories which are very active in the domain, and the example given is Verimag.

Among the PhD students who defended their PhD recently, one is working with Mathworks/Polyspace, 2 with Synopsys R&D. They have been hired for the competences acquired during their PhD.

D. Monniaux gave talks at Ensimag (LIESSE series[6]) on program verification, computability, complexity for undergraduate teaching staff ("classes préparatoires") in 2011 and 2012, published an introduction to computability in a magazine of popular mathematics [**S-O7**] and wrote opinion pieces in the national daily newspaper *Libération* regarding open data (2009), scientific publishing and open access (2011) and the use of English in teaching and research (2013).

M. Moy participated in the definition of the training offered by Ensimag to the teachers of "classes préparatoires", on Python and databases, introduced recently in the programme.

M. Moy, together with Laurent-Maillet Contoz from STMicroelectronics, presented the work done in the STMicroelectronics/Verimag collaboration at College de France in January 2014[7].

2.1.4 Synchrone team: Internal organization and life of the team

The team is organized along several research directions (see above), with non-empty intersections. The persons in charge of the projects organize small subgroups. In addition, despite the diversity of topics (from abstract interpretation to hardware modeling), we manage to organize a biweekly team seminar, in English, in which all members participate. This allows us to maintain a high level of collaboration between projects, and a wide use of the members' competencies. For instance, links have been established between: (i) abstract interpretation and WCET analysis; (ii) distributed algorithms and models of sensor networks; (iii) models of systems-on-a-chip and implementation of Lustre; etc. We also have projects involving members of DCS (L. Mounier, P. Lafourcade), allowing interesting connections, e.g., between security and fault-tolerance. All the members of the team are involved in at least one collaborative project; the teachers are very active in attracting students for research internships.

2.1.5 Synchrone team: Training through Research

The team is one of the two pillars of the "Embedded Software and Systems"[8] master curriculum, which belongs to the Ensimag (applied maths, computer science and telecommunications) and Phelma (physics, electronics, material science) departments of Grenoble INP (30 to 45 students per year). F. Maraninchi is one of the two

[3] www.minalogic.org
[4] ec.europa.eu/digital-agenda/en/time-ecsel
[5] www.fafiec.fr/81-l-observatoire-opiiec/etudes/metiers-de-l-ingenierie/211-evolution-metiers-besoins-systemes-embarques.html
[6] liesse.it-sudparis.eu/liesse.htm
[7] http://www.college-de-france.fr/site/gerard-berry/seminar-2014-01-29-17h30.htm
[8] Embedded Software and System (SLE) master curriculum at Ensimag

persons in charge of this master, since its creation in 2008. She and M. Moy, P. Raymond and C. Maïza teach several courses in this master. In particular, two of the research directions of the group for the period considered have been transferred into courses: (i) transaction-level-modeling of systems-on-a-chip, and (ii) correct-by-construction implementation of control systems, from Simulink to embedded code via Lustre. The students of this master programme, when hired in companies (Airbus, Thalès, Mathworks/Polyspace, Elsys Design, STMicroelectronics, Synopsys, Mentor Graphics, ..., to name a few) contribute to the dissemination of the results developed in the team.

P. Raymond and F. Maraninchi also teach the course entitled "Embedded Systems" (36h) of the master of science in informatics at Grenoble[9].

F. Maraninchi created the "introduction to research" module at Ensimag, in 2007. The idea is to have students at master 1 level spend time in a lab, for a short research project. Since the creation of the module, the team has hosted a dozen of students. The team also promotes short-term internships of various kinds (first contact with research for Ensimag first year students (Bachelor 3) or UJF bachelor students, research projects for UJF Master 1 or Master 2 students, ...).

Since 2012, F. Maraninchi is a member of the board of the Doctoral School MSTII (mathematics, information sciences and technologies, informatics) which gathers 400 PhD students. Since 2013, D. Monniaux is a member of the board for habilitations in applied mathematics and informatics.

2.2 DCS team

2.2.1 DCS team: Scientific production

The main scientific domains covered by the DCS team during the period are

1. **System Design**: Building a design chain from high-level specifications to implementation on a distributed software/hardware platform including formal verification support and correct-by-construction implementation techniques
2. **Security**: Proofs of security protocols, security properties and information flow, code analysis and vulnerability detection
3. **Software Verification and certification**: Software verification, static analysis, certificate generation
4. **Model-based Verification**: architecture verification, non-functional verification, contract-based design and verification

2.2.1.1 System Design

System design is the process leading to a mixed software/hardware system meeting given specifications. It involves the development of application software taking into account features of an execution platform. The latter is defined by its architecture involving a set of processors equipped with hardware-dependent software such as operating systems as well as primitives for coordination of the computation and interaction with the external environment.

Our research focuses on rigorous system design as a coherent and accountable process aimed at building cost-effectively systems of guaranteed quality. The aim is to provide the theoretical underpinnings, methods and tools for moving from empirical approaches to a well-founded discipline. The pursued research directions are the following:

1. Study notions of embedding of domain specific languages into BIP. Embeddings are structure-preserving transformations based on the operational semantics of the source languages. They can be formally defined and automated. Using embeddings ensures the semantic coherency of the design flow by taking BIP as the common semantic model of all system representations.

2. Study of scalable verification techniques. These include compositional verification techniques for specific essential properties such as deadlock-freedom and invariants. The obtained results, implemented in the D-Finder tool, avoid state explosion by computing symbolically global system invariants as the composition

[9] mosig.imag.fr

of component invariants and interaction invariants. The latter characterize the way the global state space of a composite component is restriction by its interactions. Another interesting work direction is statistical model checking applied for performance analysis to very complex BIP system models. This technique allows in particular, estimation with some degree of confidence, of parameters such as latency and throughput.

3. Study of correct-by-construction implementation techniques. These techniques combine a set of transformations and principles for building correct implementations of abstract system models. Transformations are based on action refinement consisting in replacing actions of the abstract model by sequences of primitives used for their implementation. They are provably correct, that is they preserve essential properties of the source model and additionally they meet new properties enforced by construction. Correctness-by-construction is achieved by using architectures. These are formalized in BIP as generic component transformers enforcing characteristic properties by using compositionality and composability rules.

2.2.1.1.1 The BIP Design Flow. We study rigorous system design as a formal systematic process supported by a methodology based on divide-and-conquer strategies consisting of a set of steps leading from requirements to an implementation. At each step, a particular humanly-tractable problem must be solved by addressing specific classes of requirements. The abstract principles of component-based design and correctness-by-construction are two main ingredients of our approach.

The BIP design flow [**D-J30**, **D-C94**, **D-C92**] uses the BIP language to ensure consistency between the different design steps. This is mainly achieved by applying source-to-source transformations between refined system models. These transformations are proven correct-by-construction, that means, they preserve observational equivalence and consequently essential safety properties. Functional verification is applied only to high level models for checking safety properties such as invariants and deadlock-freedom. To avoid inherent complexity limitations, the verification method applies compositionality techniques implemented in the D-Finder tool [**D-J33**, **D-C152**]. The BIP design flow involves 4 major distinct steps:

1. The translation of the application software into a BIP model. We study and implement translations of several programming models into BIP including synchronous [**D-C167**, **D-C135**, **D-P13**], data-flow [**D-C94**] and event driven models [**D-P17**]. More recently, we considered also domain specific languages and models used for sensor networks and field bus protocols [**D-C14**, **D-C5**].

2. The generation of an abstract system model from the BIP model representing the application software, a model of the target execution platform as well as a mapping of the atomic components of the application software model into processing elements of the platform [**D-C96**, **D-C92**, **D-P3**]. The obtained model takes into account hardware architecture constraints and execution times of atomic actions.

3. The generation of a concrete system model obtained from the abstract model by expressing high level coordination mechanisms e.g., multiparty interactions and priorities by using primitives of the execution platform [**D-J13**, **D-P16**, **D-P2**]. This transformation involves the replacement of atomic multiparty interactions by protocols using asynchronous message passing and arbiters ensuring overall coherency (more details are presented in the 'Distributed Implementation' subsection below).

4. The generation of executable, monolithic or distributed C/C++ code from sets of interacting components executed by the same processor [**D-C159**, **D-P16**]. This allows efficient implementation by avoiding overhead due to coordination between components.

2.2.1.1.2 The BIP Framework. BIP [BBS06] (Behavior, Interaction, Priority) is a general framework encompassing rigorous design. It uses the BIP language and an associated toolset supporting the design flow. The BIP language is a notation which allows building complex systems by coordinating the behaviour of a set of atomic components. Behavior is described as a Petri net extended with data and functions described in C. The transitions of the Petri net are labeled with guards (conditions on the state of a component and its environment) as well as functions that describe computations on local data. The description of coordination between components is layered. The first layer describes the interactions between components. The second layer describes dynamic priorities between the interactions and is used to express scheduling policies.

The BIP framework has been extended in several directions. Specific extensions for modeling real-time and mixed-criticality aspects are described below. In addition, we mention the development of Dy-BIP [D-C60], a dynamic extension of the BIP component framework rooted in rigorous operational semantics and supporting a powerful and high-level set of primitives for describing dynamic interactions.

2.2.1.1.3 The Real-Time BIP. To allow direct expression of timing constraints in real-time systems, we extended the BIP framework so that each atomic component is represented as a timed automaton. Our approach relies on two design steps: (1) we build an *abstract model* of the application including only timing constraints representing user requirements, and (2) we automatically generate from this model a *physical model* representing the application running on a platform, by taking into account execution times [D-C129, D-J8, D-C91] . The method is based on a set of tools including a compiler and a real-time execution engine that enforces the real-time constraints of the system at run-time. The real-time execution engine has been later extended by adding a parallel (thread-based) execution mode for multi-core platforms [D-C21]. We are currently improving this work by considering fully distributed architectures.

2.2.1.1.4 Mixed Criticality. So far we have focused on mixed-critical real-time systems with finite execution (which may repeat periodically). For such systems, in [D-C15] we have proposed a formal modeling methodology for multiprocessors executing a predictable scheduling policy assuming no bus/cache interference. We use real-time BIP language, representing a network of timed automata with a possibility of strong "as soon as possible" (eager) synchronization. For non-preemptive scheduling policies we developed multi-core code generation tools. In [D-C20] and [D-C16] we proposed preemptive scheduling algorithms restricted to uni-processor dual-critical systems without task dependencies. The algorithm in [D-C20] is based on extension of best-known algorithm for this problem, significantly improving the computation time and the percentage of accepted highly-loaded job sets. On top of these results, the algorithm in [D-C16] introduces a general way of producing compact time-triggered tables, which is favorable for certification. In future we will work on explicit support of multiprocessors, task graphs, and bus/cache interferences.

2.2.1.1.5 Distributed Implementation. The goal of this work is to automatically produce a distributed and decentralized implementation from a high-level model of a component-based system expressed in BIP. The main concerns are the correctness, that is, preservation of the functional properties, and efficiency, the runtime performance of the implementation. In a distributed context, one cannot generally assume atomic execution of multiparty interactions. The only communication primitive available is usually point-to-point asynchronous message passing. Therefore, the first transformation of the design flow consists in breaking atomicity of interactions [BBBS08] and inserting a two-phase offer-notification protocol. First, the component sends an offer indicating the interactions it can execute from its current state. Then it waits for a notification indicating which action has been executed. A centralized engine gathers the offers, execute interactions, and sends the notifications, ensuring correct execution of the model. The decision to execute an interaction is taken by the engine, using either an oracle [BBBS08], distributed knowledge [D-C56] or ensuring that a predicate holds [D-C46].

The second transformation consists in decentralizing the engine, by having several engines, each responsible for a subset of the interactions. If two interactions involve a common component, they are potentially conflicting and they cannot execute in parallel. This requires a mechanism to resolve conflicts between engines. A first solution avoids conflicts by grouping together conflicting interactions [D-C134]. A more decentralized solution [D-C130, D-J13] relies on existing distributed protocols for conflict resolution. However, these protocols do not encompass priorities. Priorities can be supported by transforming models with priorities into equivalent models with interactions and e.g., priority managers [D-C90, D-J19], detection of false conflicts [D-C56] or restrictions [D-C46]. We propose an optimization for multiparty interaction protocols that reduces the number of messages by using knowledge obtained from the high-level model [D-C49].

2.2.1.1.6 Performance evaluation. Extra-functional aspects are becoming of paramount importance in modern systems. These are subject to a lot of uncertainties since evolving in arbitrary environments. Therefore, one first needs a stochastic modeling formalism to capture their underlying probabilistic behaviour and second,

a rigorous approach to evaluate their performance at system level. In this context, the BIP framework was recently extended with a stochastic semantic and a Statistical Model Checking (SMC) engine [**D-C59**, **D-J2**]. A tool that combines theses feature was built, namely SBIP [**D-C13**]. This has been used to model and to evaluate several real-life case studies [**D-C124**, **D-C125**, **D-C27**]. In these works, an abstraction method was also proposed to deal with very large systems where SMC may face scalability issues.

2.2.1.2 Security

During this period, the DCS team extended and diversified its research activities in the domain of security analysis. The aim is to use formal approaches to state, verify or validate security properties. Domains that are targeted are cryptographic protocols, embedded secure applications and secure architectures. Security research developed in DCS constitutes a significant part of the SCCyPhy (Security and Cryptology for CyberPhysical systems) action team of the Persyval lab. Pascal Lafourcade is a co-supervisor of the thesis funded by SCCyPhy and Marie-Laure Potet is in charge (with Roland Groz) of the Code analysis and Protection axis of SCCyPhy. SCCyPhy constitutes a good opportunity for the local security researchers to reply to project calls or company requests, as made through the Shiva project (page 129) or other pending calls.

2.2.1.2.1 Proofs of security protocols. In the ANR projects SCALP (page 133), and PROSE (page 119), we develop automatic formalisms based on Hoare Logic and CIL (Computational Indistinguishability Logic) to automatically establish the security of several cryptographic primitives [**D-C168**, **D-C143**, **D-J29**, **D-C33**, **D-C176**, **D-C175**]. In particular, Pierre Corbineau is the co-supervisor of the thesis by Mathilde Duclos who used CIL to produce a formalized security proof for an intrusion-resilient protocol, using the Coq proof assistant.

In the FUI project SHIVA (page 129), we propose an Hoare logic to prove the security of MAC (Message Authentication Code). In the ANR project SFINCS (page 136), we create a type system to analyze the security of symmetric encryption. We also provide an Hoare Logic to prove automatically the security of encryption modes like CBC, OFB.

In the ANR project AVOTE (page 136), we propose several methods to analyze several security properties of e-voting [**D-C54**, **D-C57**, **D-C102**], e-auction [**D-C31**, **D-C32**] and other systems [**D-C111**, **D-C132**]. These works also lead us to identify some flaws in cryptographic schemes [**D-C29**, **D-C72**]. We use several tools to perform these studies [**D-C178**, **D-C160**, **D-C161**] and also prove a fundamental result in the applied pi-calculus [**D-C30**].

In the ANR Project ARESA2 (page 126), we study the security of Wireless Sensor Networks. We develop some formal methods to consider a more realistic intruder. We also provide a secure resilient randomized routing algorithm called SR3 in collaboration with Synchrone Team and we analyze the reinforced random walks [**D-C44**, **D-C68**, **D-C42**, **D-J3**, **D-C17**, **D-C71**, **D-C18**]

2.2.1.2.2 Analysis of Security properties In the domain of security, one of the main difficulty is to be able to state properties and verify them. In the Lise project (page 128) we propose a framework dedicated to digital evidences production in order to establish liability in a B2B contract context [**D-C109**, **D-J25**]. Lise project was a multi-disciplinary project involving lawyers. Starting from the specification of involved liabilities and a set of well-identified claims we proposed log architectures, and their expected properties [**D-C146**, **D-C147**], allowing us to establish expected liabilities. This approach constitutes the Eduardo Mazza's thesis.

More recently, in the context of the D-MILS project (page 117), the DCS team started a research activity on modelling, analysis and implementation of *secure* component-based systems. The Secure-BIP framework introduced in [**D-C6**] extends BIP with annotations for tracking information flow for data and interactions. Two kinds of non-interference properties (for event resp. data flows) have been formally introduced and for both of them, sufficient conditions that ensure and simplify their automated verification have been proposed. This work is currently being extended towards the construction of a complete design flow for component-based systems which deals with security aspects [**D-O2**].

2.2.1.2.3 Code analysis and vulnerability detection We develop binary level analysis techniques to identify vulnerabilities in low level code. Proposed approaches combine static and dynamic techniques [**D-C113**, **D-C70**]. Vulnerability analysis research started in DCS with the Vulcain MSTIC project [**D-C144**] and are

now developed in the context of the Binsec project (page 107) and the thesis of Josselin Feist. We develop tools [D-J6] to detect complex vulnerabilities such as Uses-After-Free which require to identify sophisticated patterns (a memory allocation which is used after being freed). Behind vulnerabilities we also aim to define exploitability conditions in order to classify bugs corresponding to false alarms (from a vulnerability point of view). In the CIFRE thesis of Sofia Bekrar we also proposed a vulnerability detection tool based on a smart fuzzing technique by combination of dynamic taint analysis and evolutionary test-based generation [D-C45, D-C93].

In the domain of embedded applications with a high level of security requirements (smart-cards, secure tokens) we propose some analysis techniques dedicated to fault injections provoking code mutations. Due to the increase of attack potential (multi-fault) one main difficulty is to establish and implement criteria allowing to define and evaluate the robustness of applications. We developed Lazart, a tool based on concolic execution, dedicated to the robustness evaluation of C code against control flow attacks [D-C4]. We are currently establishing collaborations with some actors of the domain in order to compare and combine high and low level code analysis and define a global process of evaluation.

2.2.1.3 Software verification and certification

The domain of *software analysis* has seen important progress during the last four decades. To face the complexity that arises in reasoning about modern software systems, we developed automatic program verification methods. Therefore, we investigated the generation of *certificates* establishing the correctness of the verification verdict. The certificates are machine-checkable proofs which are submitted to the Coq proof-checker.

2.2.1.3.1 Modular techniques for scalar programs. We considered programs handling scalar variables ranging over infinite data types, essentially mathematical integers. For these kinds of programs, we developed new inter-procedural summarization techniques for programs with (possibly recursive) function calls. The program properties considered in these works where safety (assertion violations) and termination. At the heart of our method lies a technique for computing transitive closures of loops labeled by conjunctive transition relations [D-J42, D-C170, D-C128]. known decidable fragments of arithmetic. To this end, it is important to know for which classes of transition relations it is possible to compute the transitive closure precisely and fast – the relations falling outside these classes being dealt with using suitable abstractions. The three main classes of integer relations for which transitive closures can be computed precisely in finite time are: (1) *difference bounds constraints* [D-J42], (2) *octagons* [D-C170], and (3) *finite monoid affine transformations* [D-C128]. Based on these results we study the complexity of the reachability and termination problems for flat programs with octagonal loops, and found that reachability is NP-complete [D-C3], while termination is in PTIME [D-O4]. Recently, we extended the NP-completeness result for the safety problem to certain classes of recursive programs [D-O1] with unbounded stack usage.

The transitive closure computation technique from [D-C128] has been extended to deal with unrestricted programs, described in the Numerical Transition System format (NTS) [D-C55], and more recently, to deal with inter-procedural (possibly recursive) programs, in [D-C28, D-O6]. We also integrated precise computation of transitive closures with interpolation-based abstraction refinement in [D-C50]. Another application of this technique was decidability of the termination problem for certain types of programs [D-C47, D-O4].

2.2.1.3.2 Verification of programs with higher-order data structures. We equally considered programs handling arrays and dynamically linked recursive data structures (lists, trees, and beyond) and objects. When reasoning on such data-structures, one issue is to relate an abstract description of the data-structure (for instance a partial function from keys to values) to its implementation (for instance as a hash-table). Moreover this relation needs to be verified in a modular way. Hence, in ARC-INRIA CeProMi (page 143), we have studied how to adapt the usual notions of data-invariant and data-refinement from the B method in presence of pointers [D-C83]. To do that, we need a dynamic notion of data-encapsulation, called *ownership*: the read/write-access to a data-structure need to be expressed inside the assertions about programs. We have encoded this notion of ownership through ghost variables: this allows to use a standard SMT-solver to discharge verification conditions. This also leads us to propose some extensions of the B method in order to allow more flexible software architectures (even without pointers) [D-B10].

Verification of programs with arrays relies on previous work on decidability of array logics [HIV08b, HIV08a]. The idea of reducing the verification of partial correctness properties to the reachability of counter automata was used in [**D-C164**] to describe a method that can handle certain classes of programs that traverse and modify integer arrays. During the period 2009-2014, we studied safety and termination problems for programs with lists [**D-J38**], and trees [**D-C172**, **D-J7**, **D-J34**], by reduction to similar problems for counter automata, or tree automata (enlarged with different types of data constraints).

Recently, a main point of interest is the study of decidability properties of Separation Logic [Rey02]. To this end, we have defined a very general fragment of the logic (in which most popular recursive data structures can be expressed, for which satisfiability and validity of entailments are decidable problems [**D-C19**]. (best paper award). We recently developed and implemented an algorithm for deciding entailment, based on a direct translation to tree automata [**D-O3**]. This method is proved to be complete for a well-defined subset of the logic, for which the entailment problem is EXPTIME-complete.

2.2.1.3.3 Certification of validation tools. Validation tools are meant to verify critical software and these tools are themselves programs, often complex ones, with bugs inside. Then, how can we trust the verdict of a validation tools?

In his PhD [**D-P14**], Manuel Garnacho addresses the challenge of instrumenting an existing static analyzer to make it produce certificates of its results. The instrumented analyzer in question discovers invariants of array-processing programs (Mathias Péron's PhD [**S-P6**]). The instrumented version automatically produces certificates in the form of Hoare style proof of program invariants in the Coq syntax [**D-O17**]. Although the analyzer reasons on values in an abstract domain, the proof is only concerned with concrete invariants, using a concretization of abstract values in first-order logic formulae. The instrumented analyzer has been used to generate the correctness proof of a buffering protocol written in C [**D-J44**].

Research on *a posteriori* certification of results is continuing in ANR VERASCO (page 115). In this project, Verimag is in charge of the certification of the abstract domain of linear relations between variables called polyhedra, a core library of the analyzer. Pierre Corbineau and David Monniaux have designed a specific verification technique for linear filters (IIR) that is instrumented for the generation of Coq-verifiable certificates. As a part of his PhD, A. Fouilhé developed a *polyhedra abstract domain* which produces formal certificates of correctness. An untrusted OCaml oracle performs most of the computations and outputs proof hints which are used by a certified checker, developed in Coq, to establish the correctness of the results [**D-C8**, **D-C9**]. Experiments showed that the overhead of result certification is sufficiently low for our abstract domain to remain competitive with well-established, non-certifying, implementations [**D-C34**]. We recently focused on three linear approximations techniques that are mandatory in our polyhedral library to deal with *multivariate polynomial expressions* in statements, such as $z := x * y$: a fast one, implemented and certified in Coq, that consists in intervalizing variables, and two others, more costly but more precise, based upon Bernstein and Handelman representations of polynomials [**D-O16**]. The plan is to have them integrated in our certifying polyhedra library.

2.2.1.3.4 Work in collaboration with LIAMA Beijing J-F. Monin has been on leave at LIAMA (Beijing) from September 2009 to August 2013. With contributors of this lab, he developed a Coq-based framework for proving data-centric distributed algorithms written in Netlog [**D-C106**, **D-C62**] and a certified instruction set simulator for **SimSoC**[**D-C112**, **D-C74**, **D-C26**]. Our proposal has been to certify a central module in **SimSoC**, namely the ARM CPU simulator, which somehow encodes the 1138 pages of the ARM reference manual in C. In order to get the required flexibility and accuracy, we experimented a direct approach based on the operational semantics formalized in Coq of the C language, available from the Compcert project. Up to our knowledge, this is the first development of formal correctness proofs based on operational semantics, at least at this scale.

2.2.1.4 Model-based Verification and Synthesis

Advancing not only verification technology but also its integration in the design process is a challenge that has been addressed by the DCS group and the lab since it inception as evidenced by the work around the IF toolbox [BFG+99, BGO+04] that lead to the more recent development of BIP (see section 2.2.1.1). In the period of the

report, we have worked on model-based technologies and providing tools for them by focusing on architecture models and non-functional aspects, we have have developed a general notion of contract framework and more generally on compositional verification techniques, we have worked on knowledge-based technologies for control and distribution of global specifications, and we have worked on analysis and synthesis methods for quantitative properties.

2.2.1.4.1 Model-based technologies Modeling languages such as UML, AADL or more specialized frameworks, such as Autosar[10] are increasingly accepted and used in industry. We have continued our effort of providing tools and methodologies for these standards. We have extended our IF-based UML toolbox in [**D-J46**, **D-C153**, **D-C67**] (project OpenEmbeDD and industrial collaborations OMEGA-4-Rhapsody and FullMDE described on pages 144, 141 and 135). In particular, in the project OpenEmBeDD, we have also adapted our tools IF and BIP for handling AADL specifications [**D-C149**, **D-C177**] and we have defined a formally-based transformation chain allowing the use of a professional performance analysis tool for design specifications at different levels of abstraction [**D-J45**]. We have also worked on such translation-based approaches in the SPEEDS project, but HRC, the common format that we have developed in that project, was far too low-level to obtain models usable in practice.

2.2.1.4.2 Contract-based and compositional verification One of the main objectives of the SPEEDS project (see page 140) was to introduce *contracts* and a methodology for dealing with them in different model-based design approaches. As the HRC model defined in that project was based on the existence of several computation models we have defined a notion of contract framework taking a component framework as well as notions of refinement as parameters and we have defined a formal reasoning framework for them [**D-O8**] and shown its usefulness in the multi-tool and multi-model context imagined in the SPEEDS project [**D-C104**, **D-B1**]. We have also proposed some concrete instances of such a contract-framework targeted for particular property classes [**D-C118**, **D-J24**]. We are currently applying this work to multi-viewpoint contracts so as to allow the integration of analysis results obtained by completely unconnected tools, such as performance analysis, schedulability analysis, safety analysis ... without requiring independence.

Compositional verification has been equally studied for checking safety properties on component-based systems described in BIP. A new compositional method relying on automatic generation of invariants has been introduced in [BBSN08], [**D-J33**] and implemented in the D-Finder tool [**D-C152**]. This method has been extended in several directions. Several incremental variants, where invariants and properties are established along the model construction, have been studied in [**D-C115**, **D-C76**, **D-C24**, **D-J4**]. More recently, the method has been extended to timed models and timed properties [**D-C2**].

2.2.1.4.3 Knowledge-based control and distribution Obtaining distributed implementations from global specifications is a relevant and challenging topic. First, we have considered the problem of transforming a Petri net with priorities into a Petri net as a controller synthesis problem [**D-C163**] which we have then generalized to consider knowledge-based controller synthesis for safety properties [**D-C139**, **D-C105**, **D-J23**, **D-J22**].

Concrete applications to the problem of generating truly distributed implementations from BIP specifications is reported in section 2.2.1.1. In [**D-C117**, **D-C73**, **D-C75**], we have directly generalized existing protocol solutions for distributing Petri nets and extended them for handling global properties. And finally, in [**D-C36**, **D-J1**] we have proposed to use this knowledge-based approach for optimizing distribution algorithms and for proving their correctness. In particular, we have given a knowledge-based definition of several implementation relations.

2.2.1.4.4 Quantitative Verification and Synthesis Classical specifications are in many cases not expressive enough for synthesis. We develop theory and tools that allow designers to use quantitative specifications to state soft constraints to guide the synthesis process. Given a set of hard constraints and a set of soft constraints, our approach automatically derives implementations that satisfy the hard constraints and optimize the soft constraints with respect to the worst-case environment [**D-C179**, **D-C122**] or with respect to an average-case environment [**D-C123**, **D-C79**]. Furthermore, our framework allows us to construct robust systems, which

[10] A tool supported modeling standard proposed in the automotive domain

behave reasonably even in case of unanticipated behavior of the environment [D-C155, D-C116, D-C98]. Finally, we have developed a specification framework and an underlying semi-symbolic algorithm to automatically construct efficient systems [D-C114, D-C64]. Our most recent implementation can generate (in a matter of seconds) efficient controllers for systems with several millions of states.

Many large systems are constructed in a component-based manner. We developed a theory and a tool to synthesize priorities between actions in a component-based model to ensure safety properties or avoid deadlocks in the system [D-C78, D-C85, D-C82].

We have also developed synthesis techniques for unbounded data domains [D-C140], analyzed population models in systems biology [D-C180, D-J28] and business process models [D-C181], summarized our work on synthesis techniques for Reactive(1) designs [D-J14], as well as our work on finding and fixing faults based on game theory [D-J15].

2.2.2 DCS team: Scientific influence

2.2.2.1 Embedded System Design

Several memebrs of the DCS group are recognized by the community for their foundational work on rigorous component-based design (J. Sifakis, S. Bensalem). In this domain, the group has promoted research directions on modeling real-time component-based systems (J. Combaz, M. Bozga), incremental and compositional verification (S. Bensalem), correct-by-construction model transformation and implementation. The BIP framework is a unique platform for studying and implementing new research ideas and is nowadays used in many projects, altogether with industrial and academic partners.

2.2.2.2 Security

Several members of the DCS group are recognized by their community for their works on cryptography computational verification, voting protocol verification, methodology for high-level Common Criteria verification and low-level code exploitability analysis. They are (or have been) implied in the main ANR projects in these fields (Prose, AVOTE, SCALP, SFINCS, LISE, BinSec, Shiva,Diamonds) and in several program committees (FPS 2009, FPS 2010, SIS 2010, SETOP 2011, AFRICACRYPT 2012, FPS 2012, FPS 2013, GreHack 2012, GreHack2013, Maroc 2013, Hotspot2014, CSS 1014).

2.2.2.3 Verification technology

Several members of the DCS group are recognized among the founders of nowadays commonplace techniques in this field, such as: predicate abstraction (S. Graf), counterexample-based abstraction refinement (Y. Lakhnech and S. Bensalem) and regular model checking (Y. Lakhnech). Other members of this group, R. Iosif and M. Bozga are recognized by the community for their works on verification of programs with pointers, acceleration, termination, etc. DCS members participate in the program committees of several flagship conferences in the field (CAV,TACAS,VMCAI,ATVA,etc.)

2.2.3 DCS team: Interaction with the economic, social and cultural environment

The DCS team has tight interactions with a number of industrial partners. In particular,

- direct industrial collaborations implementing technology transfer and consulting for companies of the Grenoble region: Actoll (2011), Cyberio (2011-2012), and Kalray (2013). In particular, the collaboration with Actoll lead to the development, implementation and deployment of a real-time BIP controller for the payment at motorways tolls (in France).
- direct industrial collaborations with the European Space Agency ESA in 2010 and 2011 which lead to a new version of the IFx toolset handling UML 2 and Rhapsody models.
- tight collaborations with Orange-Labs and the regional company Vupen on sensor networks.

- strong interactions with CEA LETI, in particular in the context of CRI and also CEA LIST in a number of projects
- collaborations in the context of national and european projects (for a more exhaustive list see section D.3)

Marie-Laure Potet, Laurent Mounier and Josselin Feist wrote an article in the special issue of MISC (june 2014) on vulnerabilities detection.

Pascal Lafourcade gave several lectures in several high schools (Moirans, Stendhal, La Mure ...), the goal of these lectures is to explain cryptography by images to the young students. Moreover, he has participated to the DEVORE project at Collège Fantin Latour, where he explained basics of cryptographic primitives and security to the selected best students that are involved in this program.

Susanne Graf has been an expert (jointly with Hubert Garavel from INRIA Montbonnot) for BSI (Bundesamt f. Sicherheit in Informationssystemen) in 2011-12, an expertise leading to a study on *Formal Methods for Safe and Secure Systems* (350 pages) published by BSI [D-B2].

2.2.4 DCS team: Internal organization and life of the team

The team is organized in several, partly overlapping sub-groups according to the topics detailed above. Each of these sub-groups has its internal organization, its group seminar and coordination meetings. The leaders of the subgroups coordinate for achieving the team coherence. Long term software development (outside PhD theses) is done by the group's research engineers M. Bozga and J. Combaz. In addition to the more or less regular subgroup seminars, there are ad-hoc meetings around research problems at the occasion of the venue of visitors, involving the relevant persons of the entire team.

Nevertheless, the team has become very large on one hand and has on the other hand lost several important members over the years. J. Sifakis is emeritus and only little present in the lab, Y. Lakhnech is vice-president of UJF. B. Jobstmann is on leave since 2012 and P. Lafourcade since september 2013. Therefore the team will be totally reorganized by splitting up. There will be a new team composed by the group working on BIP, the members working on formal verification and certification (for general software or security properties) join a new team on formal verification, and some will join the refocused Synchrone team.

The fact that both engineers of the DCS team should be (mostly) affected to the group working on BIP may be a problem.

2.2.5 DCS team: Training through Research

The DCS team is strongly involved in the SCCI (Sécurité, Cryptographie et codage de l'information) and Safe (Sécurité, Audit, Informatique légale) master curricula. Members of DCS are in charge of courses dedicated to cryptographic protocol verification, code analysis for security and smart card secure applet development project. A large part of the content of these courses stem from research directions of the team. Marie-Laure Potet is responsible of the UE SCLAM of Safe and has been responsible of the "Information Systems Engineering" (from its creation until January 2013) which belongs to the Ensimag department of Grenoble INP. She also participates to the "Ecole des Jeunes Chercheurs en Programmation" programme until June 2011 (an event associated to the GDR GPL). Pascal Lafourcade is involved in Master SAFE and SCCI by teaching the security models lecture. He also gave a lecture on homomorphic encryption.

Jean-François Monin gave lectures in all editions of Asian-Pacific Summer School on Formal Methods from 2009 to 2013, and was a co-organizer of the 2013 edition. He delivered a doctoral course on "Interactive Proofs with Coq" at the Doctoral School of Grenoble in June 2014.

We receive a large number of student internships (UJF bachelor students, research projects for UJF and Ensimag Master 1 or Master 2 students, ...).

Pascal Lafourcade was implied in the organization of the "Journées Codes et Cryptographie" in March 2014.

Pascal Lafourcade was the co-organizer of "Séminaire de Cryptologie, Codage et Infrastructures Sécurisées de Grenoble" Each month we received two invited speakers about security and cryptography [11] The aim of this seminar is to structure the Grenoble community.

[11] http://www-verimag.imag.fr/~async/CCIS/index.php

2.3 Tempo team

2.3.1 Tempo team: Scientific production

The group is working mostly in the domain of hybrid systems, which mix discrete/logical transition dynamics with continuous dynamics defined by differential equations. For this class of dynamical systems we provide support for computer-aided engineering at various degrees of formality (and hence scalability). The scientific activities of the team during the period can be classified into the following list of major topics.

1. **Hybrid verification by reachability**: set-based simulation methods that export the ideas of algorithmic formal verification (model checking) toward continuous and hybrid systems;
2. **Hybrid verification by simulation**: complementary methods that try to systematize the generation of inputs (static and dynamic) to an open system so as to detect bugs and provide a good coverage of its reachable states;
3. **Monitoring temporal properties**: developing formalisms to define properties and performance measures for hybrid (mixed) signals together with monitors that can automatically detect violations of such properties;
4. **Conformance testing of hybrid systems**: using a notion of hybrid space coverage measure to develop algorithms and tools for generating test cases for hybrid systems. The developed results can be applied to validation of analog and mixed signal circuits.
5. **Optimization and evaluation of multi-core deployment**: using SMT solvers to pose and solve multi-criteria optimization problems concerning optimal deployment (mapping, scheduling, buffer allocation, etc.). Developing a tool for design-space exploration for abstract data-flow models of applications, experimental validation on multi-core platforms.
6. **Other Work**: theoretical and computational results not directly related to the above.

Much of the work on *reachability* is based on a significant improvement in the algorithmics of computing reachable states for *linear systems* that took place mostly in the preceding period. As a joint effort of the team, the tool **SpaceEx** has been developed, consolidating these achievements and providing many features that make a difference between a prototype tool developed during a thesis and a tool which is one step closer to real-life usability. **SpaceEx** has become the academic de facto standard for reachability computation with 164 citations in the last three years and a vibrant user community (247 users coming from 140 institutions, 10% of which are from industry).

Verification by *simulation* is an alternative method which explores the reachable state-space by sampling the uncertainty space (initial states, parameters, input signals) and conducting simulations. The applicability of this technique to systems not admitting nice mathematical models (e.g. program code) makes it very attractive for industrial users who see it a a sophisticated bug hunting technology. This technique has also been used extensively for parameter synthesis for biological models.

Unlike the above two approaches, *monitoring* is not concerned with coverage of the space of possible behaviors but in checking whether *individual* simulation traces satisfy temporal properties expressed in *signal temporal logic* (STL), an extension of standard LTL with dense time and predicates over real-valued variables. During the period we made various extensions to STL (frequency-domain properties, parametric identification, quantitative semantics), improved the algorithms and collaborated with industrial partners interested in integrating a similar technology in their tools.

While the applicability of formal methods is limited by the complexity of exhautive analysis, *testing* can be used for much larger systems. In order to measure testing quality, a notion of coverage is needed. Therefore, in the context of the PhD of Tarik Nahhal, we focused on *testing*, which was also motivated by the fact that testing is the main technique used in practice for *circuit validation*. Although testing has been well studied in the context of finite state machines and then extended to timed systems, it was not much investigated for continuous and hybrid systems. Our results have high impact that led to two industrial grants from Toyota Motor Engineering & Manufacturing North America, Inc. (TEMA) and United Technologies Corp. (Ireland). The goal of these

grants is to investigate the possibilities of a transfer of our testing technology to these companies to improve the reliability of designs.

Much of the work on *optimal deployment* on *multi-cores* was done in the framework of the Minalogic Project ATHOLE (with ST and CEA as partners) which was a major source of financing of the team during the period, including the 4 theses (Legriel, Saidi, Kempf, Tendulkar). The project led to investigation of the proper ways to model applications (task graphs, split-join graphs) architectures (processors, interconnects, DMAs) and external event generators. A variety of methods have been used for optimization and evaluation including exhaustive timed verification, Monte-Carlo simulation, and most notably SMT solvers which have been used to explore feasible solutions in the design space. After the end of the project and the decision of ST to not to share the P2012 platform with the outside, work has been continued using the platform of Tilera and later of Kalray. A byproduct of the project was the introduction of a new research theme, namely multi-criteria optimization and approximation of Pareto fronts.

2.3.1.1 Hybrid Verification by Reachability

Computing the states reachable by all trajectories of an open, continuous or hybrid, dynamical system is the natural extension of symbolic model-checking to the continuous domain [**T-C47**, **T-C39**, **T-C13**]. The work can be classified according to the type of dynamics considered.

For the so called linear hybrid automata (LHA), where the derivative of the continuous variables in each discrete state is constant, the tool PHAVer (currently implemented as a scenario on **SpaceEx**) represents the state-of-the art in the domain. It has been recently applied [CJL+09, BMP10] and extended for synthesis [BFM13] and probabilistic systems [ZSR+10]. The techniques to efficiently compute with sets that have been developed for PHAVer can also be applied in other domains; promising preliminary results have been obtained in program verification [**T-C52**].

Most of the work was focused on *linear* and *piecewise-linear* systems where new computational results using support functions [**T-C51**] and polytopes [**T-C35**] allowed us to increase the dimensionality of analyzed systems by more than an order of magnitude. The approach based on support functions has been implemented in the **SpaceEx** tool [**T-C25**] with a lot of efforts in algorithmics, design and implementation to make the tool robust. Further gains in both precision and speed have been achieved by improvements on computing the intersection operation [**T-C20**] and led to a thesis [**T-P3**]. As progress in the scalability of reachability algorithms has allowed us to work on systems with hundreds of variables, it became apparent that the number of convex sets computed can exhibit an explosive growth. This is inherent to all classic approaches to reachability for piecewise-linear systems, since a non convex set is covered by convex sets. A way to quantify this convexification error was developed and a sub-optimal algorithm for computing a minimal cover was published in [**T-C11**] and integrated in **SpaceEx**. High-level improvements to guide the search of the reachability algorithms have been developed in collaboration with the chair of Software Engineering of A. Podelski at the University of Freiburg [**T-C16**, **T-B3**].

An important research frontier in reachability computation is the treatment of nonlinear systems. We developed a method for dynamic hybridization (piecewise-linearization) which improves upon previous versions of the idea by avoiding the need for intersection. This has been applied to models of biochemical reactions [**T-J7**] and later improved in [**T-C34**, **T-C55**] by taking into account the curvature of the vector field while choosing size and shape of linearization domains. Another class of methods used domain-specific techniques specialized for polynomial systems, such as using box splines [**T-C56**], the Bernstein expansion [**T-C57**, **T-J3**, **T-C58**] and they were successfully applied to the analysis of biological models [**T-C18**]. The results have been implemented in the library **NLTOOLBOX** [**T-C6**] and have been the subject of the thesis [**T-P2**]. Another application of nonlinear systems reachability algorithms is parameter synthesis for biological models [**T-C2**].

In order to efficiently perform unbounded time verification, we also applied the *abstract interpretation* framework (developed in program analysis) to the computation of *invariants* and *abstract semantics* for affine hybrid automata w.r.t. a given set of linear templates [**T-C23**]. This can then be used to yield an over-approximation of the unbounded time reachable set. We also make use of a *max-strategy improvement algorithm* that allows us to precisely compute these abstract semantics. In addition, we extended this result by adding uncertainty to the model [**T-C24**]. The invariant computation was also combined with the Bernstein technique for polynomial systems and applied to verification of embedded control programs [**T-C59**].

2.3.1.2 Hybrid Verification by Simulation

The alternative approach to verification is based on simulation/testing based while sampling of the uncertainty space of the system [T-C32]. There are two major classes of techniques depending on the type of uncertainty. For static uncertainty (values of parameters or initial states) to tool Breach [T-C33] implements a technique for parameter-space exploration using local sensitivity information provided by the numerical simulator. This information is used for an intelligent search in the space of parameters which can trace or approximate the boundaries between regions of the parameter-space that lead to satisfaction or violation of an STL property. The tool and the technique have been used in a variety of applications ranging from analog circuits [T-J9] via embedded control systems [T-C48] to systems biology [T-J10, T-J8, T-J2]. It is fair to say that the whole methodology based on Breach and STL served as our major entry point into fruitful collaborations with researchers from the life sciences.

2.3.1.3 Monitoring Temporal Properties

Signal temporal logic (STL) and its associated monitoring tool AMT [T-J6], developed during the thesis of D. Nickovic (2008), has generated industrial interest since its publication, as is manifested by the ongoing CIFRE thesis with Mentor Graphics. The intended application domain was assertion-based verification of analog circuits [T-C38], but the expressivity of the language turned out to be useful also for control systems [T-C48] and biological models [T-C49, T-J8, T-J2].

In [T-C37] the logic has been endowed with a quantitative semantics which allows to quantify the robustness of satisfaction or violation. This measure can serve in guiding the search for bugs in a simulation-based exploration. In [T-C10] an efficient algorithm for computing the robustness degree, linear in the size of the input signal was proposed. In [T-C28] we partially solved the following inverse problem: given a parameterized STL formula and a set of traces, find the range of parameters that render the formula satisfied. In [T-C19] we extended STL with frequency-domain properties using a shifting window Fourier transform that produces spectral signals whose temporal evolution can be referred to using the usual STL operator. This combination of time and frequency allowed us to express and check music-related properties of signals.

On the implementation side, the robust semantics has been implemented in the tool Breach [T-C33], and a new version of AMT has been rewritten by O. Lebeltel using Java. Further developments are the subject of a joint project with the Austrian Institute of Technology.

2.3.1.4 Conformance Testing of Hybrid Systems

Test coverage is a way to characterize the relation between the number and the type of tests to execute and the portion of the system's behavior effectively tested. The classical notions of coverage for software testing (such as statement and path coverages) are unsuitable for the behaviors of a hybrid system. We thus proposed a *novel coverage measure*, which on one hand reflects the testing objectives and, on the other hand, can be efficiently computed to guide the test generation process. It is based on the *star discrepancy notion* from statistics that measures the equidistribution degree of a set of states over the state space.

Based on the RRT algorithm (Rapidly exploring Random Trees) for robotic motion planning, we developed the **gRRT** algorithm, one of the first *coveraged-guided test generation* algorithms for hybrid systems [T-J11, T-C54, T-C53]. While the coverage-guided algorithm tends to produce test suites with a "uniform" coverage over the whole state space, in order to bias the exploration towards some critical paths we proposed a new *property-guided sampling method*, which uses a random walk on a discrete abstraction (reflecting the exploration objective) of the original system.

In addition, to address practical settings with *partial observability*, it is necessary to reconstruct the trajectory of the system under test in order to produce a verdict. To this end, we proposed to use a *hybrid Newton observer* that can provide an estimate for the current location and the continuous state based on the information on the input and the output of the system under test [T-C17]. These results have been implemented in the tool **HTG** for hybrid systems test generation which can handle, in addition to hybrid automata, electrical circuits specified in SPICE [T-C53]. The approach was also applied to the property falsification problem [T-C7].

2.3.1.5 Optimization for Multi-Core Deployment

The team has been involved in the past in numerous attempts to fight the clock explosion in reachability-based verification of timed automata [T-C44] and make timing verification, evaluation and optimization feasible. During the ATHOLE project we tried other types of techniques. In [T-C30] we used an SMT solver to find optimal schedules for task-graphs on multi-cores while treating the number of processors used as a constraint. We then realized that a more useful approach is to move to *multi-criteria optimization* (MCO) where trade-offs between latency, cost and other features are presented to the decision maker. We developed two methods for approximating the Pareto front of such problems, the first one based on conducting a generalized multi-dimensional binary search with an SMT solver used as a query oracle [T-C40, T-C31], and one based on stochastic local search [T-C29]. The results are summarized in the thesis [T-P5] and further research on MCO is now conducted in a new thesis.

The applications investigated in the ATHOLE project exhibited a lot of data parallelism (video encoding/decoding) and we studied the problem of partitioning a data array into chunks of optimal size and shape for efficient utilization of the DMA machinery between main memory and the cores. The results were published in [T-J4, T-J1] and are the object of the thesis [T-P4]. An abstract model of scheduling under uncertainty where different jobs arrive dynamically has been investigated in [DM08]. Within the ATHOLE project a prototype tool **DespEx** (the design-space explorer) has been developed which, based on a high-level system description (architecture, application, environment and deployment), evaluates system performance using mostly simulation. This high-level approach [T-C1] which provides much more efficient simulation than what is common in many hardware and software circles, is described in the thesis [T-P1]. Some reflections on the the lessons learned from the ATHOLE experience and on the importance and usability of timed models in general appear in [T-B1].

More recently we started a collaboration with Kalray and acquired their new platform. We studied the efficient deployment of split-joint graphs on this platform. These graphs which are a subclass of SDF (synchronous data-flow) provide a compact way to encode data-parallelism and consequently lead to very large task-graphs that need special symmetry breaking predicates [T-C5] to handle by a solver. An extensive infra-structure development and experimental evaluation work has been conducted on the Kalray platform and is reported in the forthcoming thesis of P. Tendulkar.

2.3.1.6 Other Results

Moving from set-theoretic to probabilistic non-determinism in verification and synthesis is a current trend as demonstrated in the recent popularity of *statistical model checking* to which A. Donze, a non-permanent member and alumni of the team, made a significant contribution [T-J9]. We developed timed automata models, *duration probabilistic automata* (DPA) where timing is not given by an interval but by a *uniform* distribution over this interval. Continuous-time models have been used extensively elsewhere but they rarely use distributions other than the easy case of exponential where no clocks are needed. In [T-C41] we presented en extension to zone-based reachability to DPA using density transformers. In [T-C27] we developed a clock-free method for computing probabilities over qualitative paths of the DPA. This allows us to compute and compare the expected performance of different schedulers. In [T-C12] we showed how the problem of synthesizing expected-time optimal schedulers on this model can be solved using an adaptation of dynamic programming.

In [T-C43, T-O1] new concepts and results concerning the entropy of timed languages were established. These results underly a large part of the ANR project Eqinocs in which we currently participate. The paper [T-C42] investigates games with mean-payoff and characterizes their expressive power. In [T-C3] we extend Angluin's algorithm for learning regular languages to deal with large alphabets. In [T-C36] we presented a modern exposition of the classical Krhon-Rhodes theorem about the cascaded decomposition of automata. In [T-B2] together with biologists we summarized the insights from our collaboration on modeling the specialization of blood cells. In [T-C14] we investigate models of mass action systems and in particular their sensitivity to initial spatial distribution of the various species.

2.3.2 Tempo team: Scientific influence

2.3.2.1 Hybrid Systems

The group is one of the leading groups worldwide in the domain of hybrid systems. O. Maler is among the founders and members of the steering committee of the conference series HSCC (today part of CPSWeek). In this domain the group has promoted research directions (continuous reachability, controller synthesis, systematic simulation, monitoring temporal properties) that proved useful and popular. Other members of the group, T. Dang and G. Frehse are well recognized by the hybrid community due to their work on reachability, test generation and development of robust tools. T. Dang was the PC chair of HSCC in 2013.

2.3.2.2 Timed Systems

In the past, previous incarnations the group were instrumental in the study of timed automata, providing pioneering results and tools for verification and controller synthesis with applications to scheduling. The conference series FORMATS, initiated by O. Maler who currently chairs the steering committee is an established venue for presenting results in the domain.

2.3.2.3 Analog Verification

Members of the team were among the first to identify verification of analog and mixed-signal circuits as an application domain for hybrid technology. The workshop FAC (formal verification of analog circuits) was initiated by O. Maler and has been recently extended in scope and renamed *frontiers in analog CAD* and draws academic and industrial participants from both sides of the Atlantic. T. Dang was a PC chair in 2013, and G. Frehse is the organization chair for the 2014 workshop in Grenoble.

2.3.2.4 Systems Biology

The inter-disciplinary difficulties associated while interacting with people from control, scheduling and circuit design, pale compared to those encountered while trying to communicate with life scientists. The group organized two inter-disciplinary meetings in Grenoble under the title *Towards System Biology*, the second in 2011, which gathered biologists, physicists mathematicians and computer scientist. The group was involved in the new conference series HSB, *hybrid systems biology* for which T. Dang was a PC chair in 2013 and O. Maler in 2014.

2.3.2.5 Verification in General

O. Maler was a PC co-chair of CAV 2009, the major venue for formal verification. Members of the team participated in program committees of conferences outside the specific timed and hybrid context, including CAV, FMCAD, CMSB, RV, ICALP, PODC and ATVA.

2.3.3 Tempo team: Interaction with the economic, social and cultural environment

In recent years, with the maturation of the computational techniques developed in the group, there is an increase in collaborations with industrial partners, detailed below.

1. **STMicroelectronics**: During the ATHOLE project on multi-cores, ST granted two CIFRE contracts to the group. Today we have strong ties with ST Crolles on analog CAD, culminating in 2 joint Nano2017 projects waiting for final approval;

2. **Mentor Graphics**: There is currently a CIFRE contract on the integration of AMS assertions in Mentor's simulation tools;

3. **Atrenta**: Two alumni of the group, S. Cotton and J. Legriel, work in Atrenta and there is an ongoing CIFRE contract on switching and power reduction in digital circuits.

4. **Kalray**: We had two contracts for testing our deployment optimization tools on their MPPA platform;
5. **Toyota USA**: We have an ongoing contract about simulation-based verification of engine models;
6. **United Technology Research Center**: We are finalizing a contract on simulation-based verification of HVAC (heating, ventilation, air-conditioning) systems;
7. **Bosch**: The SpaceEx verification tool has been used to verify an electro-mechanical breaking system. The timing effects of a software controller were studied in combination with a model of the physical plant, and the results have been published at RTSS 2014.
8. **Mathworks**: One of the group alumni, J-F. Kempf, works there and O. Maler participated in their annual faculty summit in, June 2014.
9. **Easii-IC**: We have a joint project (together with the Austrian Institute of Technology) and pending joint submissions to H2020 and Nano2017.

2.3.4 Tempo team: Internal organization and life of the team

The group is rather small and does not necessitate a strict hierarchical structure. A group seminar is held more or less regularly, in which researchers, students and visitors present their results. Seminars are held in English, partly due to presence of non-natives and partly to train French students to feel more comfortable in English. Long-term software development (outside PhD theses) is done either by the group's research engineer O. Lebeltel or by the current post-doc S. Minopoli. There are many ad-hoc meetings around research problems, preparation of proposals and visitors, involving the relevant subsets of the team.

2.3.5 Tempo team: Training through Research

During the period, members of the team gave the following courses: Implementation of Control Systems and Realistic modelling and Multi-task implementation of control systems (by Thao Dang at ENSIMAG, Grenoble University of Technology INPG)

In addition the following, advanced mini-courses where given in international schools and events: PhD School on Quantitative Model Checking (Copenhagen, 2010), Spring school of the French Society for Theoretical Biology (St Flour, 2012), International school on formal methods (Bertinoro, 2013), Advanced course on cyber-physical systems (Technical university of Vienna, 2013), Nano-Terra summer school (Aix-les-Bains, 2013).

Chapter 3

Training through Research
Implication dans la Formation par la Recherche

3.1 Thèses et Habilitations

3.1.1 Doctorants

Durant la période, 69 doctorants ont été accueillis au laboratoire (voir listes §G.6 et §G.7). Les origines sont très diverses (30 de France, 13 d'Europe hors France, 8 d'Afrique du nord, 15 d'Asie, 3 d'Amérique nord et sud, et 1 australien).

La table 3.1 liste les 37 thèses soutenues. 5 étudiants ont abandonné en cours de thèse — 3 en fin de 1ère année, et 2 qui ont été embauchés avant d'avoir rédigé leur thèse. La durée moyenne des thèses est de 45 mois. Sur les 37 docteurs diplômés, 7 sont en post-doctorat, 19 sont dans l'industrie, et 10 ont obtenu une position académique; un seul n'est pas en activité à ce jour, parce qu'il a choisi de prendre une année sabbatique.

3.1.2 Séminaires doctorants

Depuis 2013, nous organisons annuellement une série de séminaires des doctorants de 2e année : chaque étudiant présente pendant 30 minutes son sujet et l'état de ses travaux, l'exposé étant suivi de 30 minutes de questions. Ces séminaires de doctorants se révèlent très positifs, d'une part parce qu'ils permettent aux étudiants de faire une première présentation de leur travail, en confrontation avec les chercheurs, et d'autre part parce qu'ils assurent une bonne divulgation des sujets en cours à l'intérieur du laboratoire.

3.1.3 Habilitations

La table 3.2 liste les 6 HDR soutenues durant la période, avec la situation des personnes au moment de la soutenance. Notons qu'il y a eu une HDR externe : John Plaice, ancien doctorant du laboratoire et professeur à Sidney.

3.1.4 Stages de recherche

Nous accueillons chaque année de nombreux stagiaires, d'origines et de niveaux variés : stages de M2R, de fin d'étude d'ingénieurs, de magistère; TER ("travaux d'étude et de recherche", niveau M1) et IRL ("initiation à la recherche en laboratoire", 2e année Ensimag), "stages d'excellence" (niveaux L1 à L3).

Nom	Prénom	1e Insc.	Date sout.	Etablissement	Encadrant	Equipe
COTTON	Scott	2005	25/06/2009	UJF	O. Maler	TEMPO
CHKOURI	Yassin	2005	07/04/2010	UJF	J. Sifakis	DCS
DEGORRE	Aldric	2005	21/10/2009	UJF	O. Maler	TEMPO
LE GUERNIC	Colas	2005	28/10/2009	UJF	O. Maler	TEMPO
PERON	Mathias	2005	22/09/2010	UJF	N. Halbwachs	SYNC
POULHIES	Marc	2005	05/03/2010	INPG	J. Sifakis	DCS
BOUHADIBA	Tayeb	2006	15/09/2010	INPG	F. Maraninchi	SYNC
FALCONE	Ylies	2006	09/11/2009	UJF	J.C. Fernandez	DCS
GARNACHO	Manuel	2006	27/08/2010	UJF	M. Perin	DCS
NGUYEN	Than	2006	27/05/2010	UJF	J. Sifakis	DCS
QUINTON	Sophie	2006	21/01/2011	UJF	S. Graf	DCS
BEN HAFAIEDH	Imen	2007	03/02/2011	UJF	S.Graf	DCS
FUNCHAL	Giovanni	2007	18/11/2011	INPG	F.Maraninchi et M. Moy	SYNC
JABER	Mohamad	2007	28/10/2010	UJF	J.Sifakis	DCS
SFYRLA	Vassiliki	2007	21/06/2011	UJF	J.Sifakis	DCS
LEGRIEL	Julien	2007	04/10/2011	UJF	O. Maler	TEMPO
SAIDI	Selma	mars-08	24/10/2012	UJF	O. Maler	TEMPO
KEMPF	Jean-François	avr-08	29/10/2012	UJF	O.Maler	TEMPO
DAUBIGNARD	Marion	2008	12/01/2012	UJF	Y. Lakhnech	DCS
PERRELLE	Valentin	2008	21/02/2013	UJF	N.Halbwachs	SYNC
RAY	Rajarshi	2008	29/05/2012	UJF	G.Frehse	TEMPO
BERTHIER	Nicolas	2008	12/03/2012	INPG	F.Maraninchi, L. Mounier	SYNC/DCS
ABDELLATIF	Tesnim	2008	05/06/2012	INPG	J.Sifakis	DCS
SAMPAIO	Eduardo	2008	26/06/2012	INPG	ML Potet	DCS
SFAXI	Lilia	2008	05/05/2012	UJF	Y. Lakhnech	DCS
KONECNY	Filip	fev.2009	29/10/2012	UJF	R.Iosif	DCS
SIMACEK	Jiri	fev.2009	29/10/2012	UJF	R.Iosif	DCS
PIETREK	Artur	fev.2009	02/10/2012	UJF	J.C. Fernandez	DCS
SHI	Xiaomu	2009	10/07/2013	UJF	JF Monin	DCS
TESTYLIER	Romain	2009	07/12/2012	U. Grenoble	T.Dang	TEMPO
BOURGOS	Paraskevas	2009	09/04/2013	U. Grenoble	S.Bensalem	DCS
QUILBEUF	Jean	2009	16/09/2013	U. Grenoble	M.Bozga	DCS
SIFAKIS	Emmanuel	2009	06/05/2013	U. Grenoble	S.Bensalem	DCS
BEKRAR	Sofia	jan.2010	10/10/2013	U. Grenoble	L. Mounier	DCS
RIVIERRE	Yvan	2010	12/12/2013	U. Grenoble	F.Maraninchi	SYNC
DREIER	Jannik	2010	25/11/2013	U. Grenoble	P.Lafourcade	DCS
VON ESSEN	Christian	2010	28/04/2014	U. Grenoble	S.Bensalem, B. Jobstmann	DCS

Table 3.1: Thèses soutenues 01/2009 - 06/2014

MONNIAUX	David	CR CNRS	06/2009	SYNC
DANG	Thao	CR CNRS	01/2010	TEMPO
BOZGA	Marius	IR CNRS	02/2010	DCS
PLAICE	John	Prof.	12/2010	Ext.
LAFOURCADE	Pascal	MCF UJF	11/2012	DCS
MOY	Matthieu	MCF INP	03/2014	SYNC

Table 3.2: HDR soutenues 01/2009 - 06/2014

3.2 Participation aux formations doctorales et masters recherche

3.2.1 Responsabilités à l'Ecole doctorale

Florence Maraninchi est co-responsable de la spécialité "Informatique" de l'Ecole Doctorale MSTII[1] (Mathématiques, Sciences et Technologies de l'Information, Informatique), et à ce titre, membre de son bureau et du conseil de l'ED. Nicolas Halbwachs est membre du conseil de l'ED. David Monniaux est membre de la commission des habilitations à diriger les recherche en informatique et mathématiques appliquées.

3.2.2 Interventions et responsabilités en M2R

Des membres du laboratoire participent à l'organisation et à la formation de la filière "Systèmes et logiciels embarqués[2] commune aux écoles Ensimag et Phelma de Grenoble INP.

Ils interviennent également au master MOSIG[3], qui est le master recherche international en informatique de Grenoble.

Le laboratoire est aussi fortement impliqué dans les masters SCCI (Sécurité, Cryptographie et codage de l'information) et SAFE (Sécurité, audit, informatique légale).

3.3 Organisation d'écoles pour doctorants

Comme coordonateur des réseaux Artist2 et Artist-design, le laboratoire a pris une part importante à l'organisation et l'enseignement de plusieurs écoles d'été Artist. En 2013 nous avons également organisé une école dans le cadre du LabEx Persyval :

- ARTIST School in South America: Embedded Systems Design[4], Buenos Aires, 3-7 août 2009
- ARTIST Summer School in China[5], Tsinghua, 19-24 juillet 2009
- ARTIST Summer School in Europe[6], Autrans, 7-11 septembre 2009
- ARTIST Summer School in Europe[7], Aix-les-Bains, 4-9 septembre 2011
- PERSYVAL-Lab Summer School on Cyber-Physical Systems[8], Grenoble, 8-12 juillet 2013

[1] edmstii.ujf-grenoble.fr
[2] Filière SLE
[3] mosig.imag.fr
[4] www.artist-embedded.org/artist/Overview,1736.html
[5] www.artist-embedded.org/artist/Overview,1630.html
[6] www.artist-embedded.org/artist/Overview,1633.html
[7] www.artist-embedded.org/artist/Overview,2278.html
[8] persyval-lab.org/en/summer-school/cps

Chapter 4

Perspectives

4.1 Summary of the competences

Verimag is a relatively small laboratory, with a well defined and shared scientific approach. We master the theoretical principles and tools of computer science that can be used for the development of safe and efficient computer systems. The joined competences of the teams and members of the lab allow us to see the *big picture*: the variety of applications domains and case-studies from industrial partners give us the *horizontal* view, and we developed several approaches for building complete *vertical* solutions, from mathematical models to implementations.

Moreover, both theoretical and practical results are placed in a long-term perspective, together with the development of tools. During the last five years, a startup company was created, based on a set of results and tools developed during more than 20 years, and successfully used by the industrial partners of several collaborative projects.

The scientific topics of the lab are the following:

- Formal validation (based on model-checking, abstract interpretation or theorem-proving; symbolic execution, runtime verification, automatic testing, etc.)
- Design, implementation, programming languages (component-based, model-driven and correct-by-construction approaches; definition and implementation of programming languages for critical systems; optimisation and certified tools)
- Faithful modeling and efficient simulation (modeling for hybrid systems and hardware/software digital systems at various levels of abstraction, efficient exploration of state spaces, parallelized simulation engines)

plus a transverse topic:

- Security, safety and Quality-of-Service properties of digital systems, trade-offs between all these properties; in the recent years, we contributed to the inclusion of timing and energy-consumption properties in this picture.

The natural scientific connections with other domains are: applied and pure mathematics, hardware and systems, networks, control theory and control engineering, optimisation, etc. In Grenoble, we have fruitful collaborations with all the institutes and labs that offer these competences: TIMA, TIMC, LJK, IF, LIG, INRIA, CEA, GIPSA. We are involved in the *project-team* of the Persyval-lab Labex dedicated to security (from mathematical foundations to hardware implementations); we also lead two Persyval *exploratory projects*, one on the implementation of critical systems on manycore architectures (with TIMA), and the other on distributed algorithmitics applied to sensor networks protocols (with LIG).

The application domains we studied in details are:

- Embedded control systems
- Communication protocols, distributed algorithms and systems

- Modern hardware architectures (systems-on-a-chip, manycore processors)
- Analog circuits
- Biological systems
- Security protocols, smart cards, security in general-purpose software
- Sensor networks

4.2 A vision of the domain for the next five years

Within the next five years, we will experience the consequences of several convergences that have already started:

- **Security and safety**, which were originally defined and studied in disjoint domains (e.g., smart cards and protocols for security, critical embedded control systems for safety) will have to be taken into account together. For instance, planes are now communicating systems, no longer isolated from potential security attacks. In the industry, the norms and institutions that are traditionally in charge of security or safety will have to be confronted to each other, if not merged. This will take time, but interesting scientific problems have to be studied and solved before, for which the combined competences of the Verimag members can be very useful. In the avionics domain, for instance, safety is ensured by carefully crafted architecture principles that are validated once and for all (like the integrated-modular-avionics, or IMA, principles). These architectures made for safety are being extended to allow for the implementation of mixed-criticality systems; but on some aspects they appear vulnerable to attacks, and will have to be redefined with security principles in mind, for the very beginning. Our combined competences in safety (including mixed-criticality) and security of complex systems will be very useful for that purpose. In particular, the combined experience in the quite different certification processes (for security, or for safety), will be needed.
- The **theoretical principles and tools used in formal validation** of computer systems (both hardware and software) range from model-checking to abstract interpretation and theorem-provers; in practice, none of these methods works totally in isolation; in theory, the underlying mathematical notions can be shared. A conjoint use and development of the full range of available methods and tools will be the key.
- Several domains will require the conjoint use of the methods and tools originally developed in isolation for **resource-constrained embedded systems** on one side, and **distributed communicating systems** on the other side. This is already the case for sensor networks and it will become the rule for the internet-of-things. It will also be true for the structure of the hardware/software systems themselves: a modern manycore processor uses a network-on-chip, and it becomes possible to think of compilation for this type of hardware as a distributed system problem.
- The domain named **cyber-physical systems** will reach full maturity, with a now clear understanding of the necessary relations between physical environments, digital control systems, and networks, in holistic system development methods.

In a lot of domains, **modeling, virtual prototyping and efficient simulation or monitoring** are becoming unavoidable. For instance, software development for wireless sensor networks (WSNs) has been recognized as a very difficult process, especially when security and energy-consumption have to be taken into account. Validating the essential properties of the software on effective deployments of WSNs faces several problems, among which: the cost of real deployments, the lack of observability means, the late availability. This is the reason why the properties of the software are most of the time assessed by simulations. Another example is the way *energy consumption*, originally thought of as an extra-functional property, now interacts fully with functional and timing aspects, since most embedded systems include power-managers. More generally, the design of complex cyber-physical systems requires the modeling of the physical world, and efficient simulation of the interactions between the physical and digital worlds.

The problem of designing and validating a faithful model that allows either efficient simulations, or efficient formal exhaustive analysis, is a key point for the development of correct and efficient complex systems. This will become even more true for next generation cyber-physical systems, taking into account at the same time safety, security and QoS properties, and dealing with faults in the hardware execution platforms, or hazards in

the physical environment.

Verimag proposes to advance the state-of-the-art in methods and tools for the development of safe, secure and efficient systems of systems. The aim is to provide the theoretical underpinnings, methods and tools for moving from empirical approaches to a well-founded discipline.

4.3 Organisation of the laboratory

For the next period, the laboratory will be organized into four teams. The convergence we observe between all the methods and tools of formal verification leads to the creation of a dedicated team, led by D. Monniaux, who received an ERC grant. The Tempo team is unchanged. The Synchrone team refocuses on programming languages, distributed systems, modeling and simulation, and the use of formal verification tools; the two persons working on the development of new formal verification methods and tools join the new team. The DCS team is also split following this principle: the people working on formal verification and certification (for general software or security properties) join the new team; moreover, the group working on BIP becomes a team.

4.4 Detailed projects of the new teams

4.4.1 PACSS: Preuves et Analyses de Code pour la Sûreté et la Sécurité / Proofs and Code Analysis for Safety and Security (David Monniaux)

Formal methods, and, in particular, software analysis, have made great inroads in the domain of verification of safety-critical systems, that is, systems whose failure may result in loss of life and limb. The certification authorities encourage the use of formal methods for avionics (DO-178C standard) and even mandate their use for certain medical devices. Yet, they are currently little-used outside the niche market of safety-critical embedded systems. Outside of this niche, there exists a much larger number of programs whose failure is less catastrophic in human terms, but may result in heavy economic losses: a software bug may cripple entire industrial, transportation, retail or telecommunication infrastructures.

Thus, from the user's point of view, software analysis methods can be classified as (1) methods that allow to *establish correctness* of systems, which are useful to certify the software before its release, and (2) methods for efficient *bug detection*, which are very useful to programmers at early stages of software development. The methods in the first class are based on techniques of *over-approximation* of sets of reachable states and execution traces (i.e., abstract interpretation), while the methods in the second class use *under-approximation* (i.e., precise acceleration) techniques. Both classes of software analyzers benefit from advances in automated reasoning and proof theory, such as *proof-based certification* (i.e., using human guided proof assistants such as Coq or Isabelle) for (1) and *Craig interpolation* (i.e., generalization of unfeasible traces) for (2).

Another emerging domain of software analysis is (3) finding security breaches in low-level code. Although related to the more traditional domains (1) and (2), software analysis for security breaches brings its own problems. For instance, safety proofs almost always assume that the execution environment (e.g., processor) behaves as expected; in contrast, hostile intruders cannot be assumed to "play by the book" and may trigger behaviours that would normally be considered impossible; low-level analyses are thus necessary.

According to the above distinction, the PACSS team will be organized among three, possibly overlapping, research directions.

4.4.1.1 Safety-critical systems code

We wish to pursue collaborations with industrial partners (e.g., Airbus, Rolls-Royce, Continental) on the verification of safety-critical software. Mature industrial tools (e.g., Polyspace Verifier, Astrée) have focused on proving the absence of runtime errors (e.g., null pointer exceptions). Yet, it is also desirable to prove functional properties (even if full functional correctness is out of reach), such as expected behaviors of the system, as well as non-functional properties such as worst-case execution time. At the same time, high standards of soundness must be maintained: the user should be able to reasonably trust negative results (absence of violations).

This research direction will aim both at enlarging the scope of applications of sound methods, at to reinforce the trust in analyzer, for instance by developing formally proved tools.

4.4.1.2 Non safety-critical industrial applications

This research direction aims at developing scalable analysis methods for large industrial-size applications such as mobile phone applications, web servers, databases, etc. One of the main challenges for this class of applications is the handling of the dynamic memory, via imperative low-level mechanisms such as pointers, dynamic allocation, garbage collection, etc. Such primitives are usually not allowed in safety-critical systems, due to the programming standards: for instance, dynamic allocation and recursive calls are forbidden in the A level of the DO-178C standard.

Most existing industrial-scale tools for software analysis (e.g., Coverity, Frama-C, Astrée) currently make very rough abstractions of the program's behavior with respect to the manipulation of dynamic data structures, which manifest themselves as an increase in the number of false alarms reported by the tool. The key to this problem is the definition of logic-based symbolic representations for memory structures. These formalisms must be investigated from the point of view of expressive power, decidability, and complexity, by considering several key problems that constitute the basic ingredients of any automated verification approach, such as pre/post-image computation, satisfiability, interpolation and entailment checking.

Another equally important ingredient of an automated and scalable verification technique is *modularity*, i.e., the capability of performing local analyses on small, tractable, parts of the program, and combining the results of these analyses in a verification condition for the entire program. Modularity is currently recognized as being the key to scalability of analyses to programs of several millions lines of source code.

4.4.1.3 Security code analysis

We are currently developing a platform (as part of the BINSEC project) offering several analyses for detecting security holes in low level code. Techniques that proved to be useful in vulnerability analysis consist in mixing static and dynamic analyses. Security code analysis implies two levels of analysis : vulnerability detection that exhibit some holes and exploitability analysis that decides if these holes are really dangerous ones. Vulnerability detection encompasses classical bug detection but can also require to take into account hostile environments. Then analyses are based both on the semantics of the code but also on the model of environment and its influence on the code execution. Exploitability analysis, moreover, relies on several other analyses including taint, traces generalization and non-conform semantics as undefined behaviours.

We plan to develop a second axis, dedicated to the verification of less classical security properties, such as isolation or non-interference. More generally, flow analysis is a very important ingredient in security requirements (Common Criteria, Trusted Execuction Environment, MILS). The first difficulty is how to state such properties and to propose verification techniques to ensure such properties. We are in particular interested by isolation requirements that are recurrent in a lot of security targets.

The Security code analysis axis will reuse verifications techniques developed in this team and will supply new applications and problems for verification techniques. Application domains that are targeted are embedded devices (mobile, smart cards, secure tokens), industrial control systems (scada) or large public applications.

4.4.2 Synchrone (Matthieu Moy)

The Synchrone team's research interests are evolving: after the reorganization of teams, the research on formal verification tools will be performed in the new team PACSS. The "automatic testing" topic has reached maturity and has been transferred to a start up company in the previous period. The team will continue to maintain the academic tools and work on applications.

On the other hand, new trends are emerging. Multi and manycore architectures are already the norm on many non-critical systems, but the growing need for performance is forcing designers to consider them even for critical hard-real time systems. The traditional tools to implement hard-real time, including the ones developed in the Synchrone team around the Lustre language have to be completely re-thought for this new generation of hardware.

4.4.2.1 Virtual prototyping and Simulation

In application domains like System-on-a-Chip and Wireless Sensor Networks, the need for fast and abstract simulation via virtual prototypes is no longer questioned. Simulation techniques are well established (e.g. SystemC/TLM has been massively deployed in production within STMicroelectronics for almost 10 years), but are already reaching some limits. We also worked with Orange Labs for more than 10 years, on the modeling of functional and non-functional properties of sensors networks. These two domains will be necessary for the virtual prototyping methods and tools required for the internet of things, and other systems of (cyber-physical) systems.

The complexity of systems to be simulated grows faster than the speed of individual processors of the machines hosting the simulation. As the systems to simulate are usually communicating systems, it becomes necessary to model and simulate *systems of systems*, and not only individual systems. This raises the need for more abstract models and even faster simulation. This can be achieved in several ways:

- Use the physical parallelism of the host machines, or even perform a distributed simulation. This is different from typical high-performance computing where a computation is parallelized or distributed, because the program to parallelize represents a system with its own time and parallelism. Simulated time have to be modeled carefully to avoid making it a performance bottleneck. We already proposed a new model of time with the sc-during library [**S-C20**], which is being improved in the OpenES project (see page 109). A CIFRE PhD will start with STMicroelectronics on the subject in fall 2014, and we are working on a European project proposal on fast and parallel simulation for SoCs, in which we will work on the connection or merge of models of time (our notion of duration [**S-C20**], distributed-time [MMGP10], ...). This will hopefully lead to a standardized set of new constructs and guidelines in the next version of SystemC.

- Raise the abstraction level by removing details. Too many details slow down the simulation, but also compromise the understandability of the observations. An interesting direction is to mix abstraction levels within a simulation: simulate precisely a component or subsystem, and abstract its environment as much as possible. Removing completely the environment is usually not possible or not realistic. Yet, an abstract description of the environment or of a part of the system is possible in the form of a *contract*. More generally, contracts can be compared to their implementation (conformance testing) or used as replacement for concrete components when the precise model is not available or too slow. Another direction will be explored in the context of sensor networks, in a CIFRE PhD starting with Orange Labs in fall 2014: the observation of a deployed sensor network has to be done using the same radio channel used for the normal operation of the network. It's therefore intrusive functionally, and involves an increased energy consumption. It should be kept to the minimum compatible with the nature of the decisions that have to be taken thanks to this observations. We will explore, in particular, the idea of having variable-step observations, similar to variable-step integration in tools like Simulink.

Virtual prototypes are not limited to functional properties. Some systems behave differently depending on physical values like temperature, and all embedded systems are meant to interact with their physical environment. A holistic simulation needs to take into account the impact of computations on physics and vice versa. We already worked on models for power consumption for SoCs (in the HELP project, see page 125) and wireless sensor networks (in ARESA and ARESA2, pages 140, 126), and plan to work on generalizations of this: not only allow concrete simulations, but also provide formalisms to express the properties in a component-based manner and at a high-level of abstraction. This is not trivial since various extra-functional properties (time, energy, temperature) are linked to each others and do not compose trivially (e.g. the fact that one component consumes a lot of energy has an obvious impact on the temperature of its neighbors). We already started working on the subject within the OpenES project.

4.4.2.2 Distributed Algorithms

Two permanents are mainly involved in this topic: Karine Altisen and Stéphane Devismes. Moreover, a PhD will start in this field in October 2014. Finally, two related new projects are just starting: DACRAW and DIAMS.

The major goal of the above thesis is to develop new fault-tolerant solutions dedicated to WSN. In particular, it should answer the most usually encountered problems, such as resource allocation, routing, and clustering. The proposed solutions should meet desirable properties to be suitable for WSN.

We will also continue a local collaboration with Pierre Corbineau and Michaël Périn on the *certification of existing self-stabilizing algorithms using Coq*. Beyond such certifications, our long term goal is to propose a *framework, based on Coq, to (semi-) automatically construct certified proofs of self-stabilization* and its variants, *e.g.*, fault-containment, superstabilization.

The expected outcome of the DIAMS project is the design of efficient monitoring algorithms for widely distributed architecture that can be applied to cyber-physical systems. The solutions should be generic to serve as a basis for future algorithms that will be specialized for some application-domains.

DACRAW deals with the IEEE 802.15.4e standard, which defines TSCH, a new MAC protocol which focuses on ultra low-power and high reliability, targeting industrial applications. The main objective is the design of fully distributed routing protocols compatible with TSCH.

4.4.2.3 Implementation and Timing Analysis of Real-Time Embedded Systems

A precise timing analysis, providing safe upper bounds to the Worst Case Execution Time (WCET) is necessary to guarantee that embedded systems fulfill their real-time requirements. Imprecision in timing analysis has two main sources: the increasing complexity and unpredictability of the hardware, and the difficulty to identify the feasible executions paths of the software. The team has recently started to focus on this second source of imprecision, by undertaking and leading the ANR project W-SEPT (page 114). To tackle the problem, the team relies, on one hand, on its experience in compilation, from high-level dedicated language (such as Lustre/Scade) to C code and then binary, and in the other hand on the expertise in program analysis for checking the feasibility of execution paths. The promising results of the W-SEPT project have lead to consider possible extension: a more complete WCET aware compilation flow, that handles the traceability of infeasible paths, but also considers the hardware, and tries to limit the use of unpredictable features. The team is currently gathering a consortium to create a European Project around these ideas, by extending its collaboration with tool providers (compilers and program analysis) and users (embedded systems developers).

Timing analysis will also face new problems due to the increasing use of non-sequential execution platforms, even in critical domains. Indeed, the hardware industry is progressively moving to multicore and manycore architectures. In general purpose systems, the challenge is usually to get the best average-case performance on these systems. For hard real-time systems, on the other hand, many modern architecture optimizations are counter-productive as they sacrifice predictability in favor of performance. Still, the market of critical hard real-time systems is not large enough to allow the creation of dedicated processors or systems on chips. Some compromises have to be found to let the same architecture be usable in critical contexts and for other embedded systems. One attempt in this direction is the MPPA architecture from Kalray, which took into account the worst-case performances in its design, and also targets non-critical multimedia applications. We started studying the MPPA architecture and the way to adapt synchronous programming to it in a semantics-preserving manner, and plan to continue working on it in a collaborative project currently under negotiation (the LEOC project "CAPACITES", and a point-to-point CIFRE collaboration with Eurocopter).

This new research direction is very promising for the team. The Synchrone team has all the required scientific background to tackle the issue: the team pioneered the use of synchronous languages to implement real-time systems. We studied the hardware/software interfaces in various contexts. Recently, the team also developed some expertise in WCET analysis for sequential software. We believe the knowledge on sequential WCET can be combined and extended with previous works on formal verification of parallel systems (via model-checking and abstract interpretation). The research topic correspond to a strong need of industry sectors like avionics that should be solved within the next few years.

4.4.3 RSD: Rigorous System Design (Saddek Bensalem)

Today one of the main visions for embedded systems — as initially formulated in the Strategic Research Agenda of the Joint Technology Initiative ARTEMIS — is to overcome the fragmentation between different application sectors and to facilitate cross-sectorial sharing of tools and technologies that are quite separate. A

major evolution in our society is taken place whereby our world is widely supported by intelligent embedded systems, a world where all systems, machines and objects become smart, have a presence in cyber space, exploit the digital information and services around them, communicate with each other, with the environment and with people, and manage their resources autonomously. The ubiquitous presence of the Internet, provides the communication infrastructure for smart objects to be connected. Life in our society, along with security and safety, will increasingly depend on embedded systems technologies.

It is hard to imagine what Computer Science will be in two decades. More than any other discipline, it is driven by applications and exponential progress in technology. The broadening of its perimeter is accompanied by a shift in focus from algorithms and programs to systems.

The dominant vision for the development of strongly integrated "systems of systems" is currently hitting a wall. Several incarnations of this vision for building global trustworthy services through increasing integration may not become a reality. The most general one is the Internet of Things, which is intended to develop global services by interconnecting everyday objects. One instance of this vision is Smart Grids for efficient and reliable energy management. Another instance is intelligent transport systems to improve safety and reduce vehicle wear, transportation times, and fuel consumption.

Mixed criticality systems naturally emerge through the integration of large networked systems via the Internet. They find numerous applications in building automation, smart metering, medical monitoring, traffic control and large scale infrastructure monitoring and control, e.g. asset monitoring and smart grid. Embedded networked systems are seen as a key enabling technology for this. These systems must be highly available and utilize a mixture of pre-existing and new infrastructure to provide new functionality. The applications are also likely to use shared components and services for implementing safety-critical features. The requirements on components, but more importantly, on the design process and platform properties should be enforced by the need to meet safety standards requiring independence of concurrent functions. Many emerging embedded applications now share networks and components in configurations whose conceptual structure no longer readily maps to their physical structure. In parallel, open networks of embedded systems couple applications from multiple domains: everything can, in principle, be connected to everything else. Networked systems are becoming the neural system of our cyber-society.

The main and well-identified scientific and technical obstacle is mastering interaction between systems of mixed criticality. How to prevent failures of non-critical systems from affecting the behavior of critical systems raises difficult problems, which lack theory to be tackled with. The objective is to bridge the gap between critical and best-effort systems engineering by addressing on a foot of equality trustworthiness and resource optimization through the combined use of existing and novel techniques.

Management of criticality is key point and it is important that critical parts of a system do not interfere with non-critical parts such as maintenance functions, or added value services provided to users such as navigation or weather information. Note that preventing failures of non-critical components from affecting the behavior of critical components raises difficult problems. However, the theory with which to tackle them is lacking.

Why we need new concepts?

With the use of networking, which may be fixed or wireless, there is also the need to consider self-organizing and adaptive systems. The predictability of the network in terms of Quality of Service is highly important. Dependability and security become key issues particularly considering applications such as health care where patient data may be collected remotely by sensors. In addition to the need to provide data in a timely and guaranteed manner this introduces privacy issues. There are also implications on the provenance of data that may well be used in critical diagnostics. The wider scale connection of systems to produce systems-of-systems requires the need for design methodologies, models and tools support for mixed criticality. However, the methodologies and tools to support the implementation of mixed criticality systems are still in their infancy. A major research effort is required to cover a number of key challenges with respect to the rigorous design of mixed criticality systems:

- A theoretical framework that supports scalable smooth system integration and reuse of independently developed components is needed in order to increase the level of abstraction in the design process and to reduce complexity.

- The provision of a generic framework that supports mixed criticality, safe, secure, maintainable, reliable and timely system services despite the accidental failure of system components and the activity of malicious intruders is essential.
- Design tools that can be integrated into the core design process workflow that address heterogeneous structures, particularly power efficient mapping on heterogeneous multiprocessing devices and complex memory hierarchies.
- Integration of applications with different safety requirements merged on the same system components and communication channels require new approaches to integration, qualification and incremental certification.
- Radical design and verification methodologies that will enable correct-by-construction design with automatic co-verification so as to achieve an order of magnitude advance in productivity and allow privacy and content protection in dynamic and distributed environments.

The research directions that we plan to investigate will be based on the above challenges. Mainly, we want to develop theory methods and tools for the rigorous correct-by-construction design of integrated mixed criticality systems.

4.4.4 Tempo (Oded Maler)

In the domain of hybrid verification and validation we intend, after having made significant progress in scalability, to get closer to application domains. For the Cyber-Physical systems this will be be realized by intensifying our interaction with partners in the automotive (Toyota, Bosch) and HVAC (United Technologies) domains as well as trying to establish stronger relations with tool providers such as Mathworks and ANSYS. Technically this will involve further maturation and extension of the tools such as making them more robust and connecting them with industry standard tools such as Simulink. This work will involve integration as well as development of new research results concerning efficient treatment of differential-algebraic systems, improved techniques for nonlinear dynamics and controller synthesis.

In the domain of monitoring we intend, in tight collaboration with the Austrian Institute of technology, to develop a new industrial-strength version of the AMT tool. While the monitoring technology is applicable to any domain that uses simulations, its primary application domain will be analog circuits. Through our network of collaborations in the domain (Mentor, ST, Easii-ic) we hope to influence the industrial reality of analog and mixed-signal verification. We intend to tackle theoretical and conceptual challenges in the monitoring domain such as extension to regular expressions, giving explanation/diagnostics in case of violation, different quantitative semantics, solving inverse problems, and more.

We intend to continue our excursion into Systems Biology, in tight collaboration with local partners TIMC and LBFA in the context of the Beesy center for Systems Biology where we have fruitful interactions with actors from the biochemical, medical and computational domains. Another ambition is to try to regroup various workshops and sub-communities into a common "dynamic systems biology" community. Technically we intend to improve our technique for parameter-space exploration and work on methodological aspects of integrating verification-inspired techniques in the biologist's workflow.

In the domain of optimization, and in particular multi-criteria optimization, we intend to explore new techniques based on local search for approximating the Pareto front as we believe the topic is of primary importance in any complex domain where decisions are to be made. We hope to have the human resources to continue with our extensive work on using these techniques to study efficient deployment of programs on multi-core architectures.

Appendices

Appendix A

Executive summary
Présentation synthétique

Titre de l'entité

Intitulé de l'unité : VERIMAG
Nom du directeur pour le contrat en cours : Nicolas Halbwachs
Nom du directeur pour le contrat à venir : Florence Maraninchi

---

Effectifs de l'entité

- **au 1/1/2009 :** 23 enseignants-chercheurs ; 8 chercheurs ; 10,5 techniciens, ingénieurs et autres personnels ; 35 post-docs et doctorants ; 2 chercheurs en détachement.
- **au 30/06/2014 :** 22 enseignants-chercheurs ; 7 chercheurs ; 10 techniciens, ingénieurs et autres personnels ; 43 post-docs et doctorants ; 3 chercheurs et 1 enseignant-chercheur en détachement ; 1 chercheur émérite.

Bilan quantitatif des publications de l'entité.

	Articles de revues	Conférences	Thèses	HDR
2009	12	79	4	1
2010	16	65	7	3
2011	17	75	5	0
2012	19	48	12	1
2013	12	54	8	0
2014	6	19	1	1
Total	82	340	37	6

Quelques publications majeures :

- Pierre Ganty, Radu Iosif, and Filip Konecný. Underapproximation of procedure summaries for integer programs. In TACAS, pages 245–259, 2013.
- Tayeb Bouhadiba, Matthieu Moy, and Florence Maraninchi. System-level modeling of energy in TLM for early validation of power and thermal management. In Design Automation and Test Europe (DATE), Grenoble, France, March 2013.
- Judicaël Courant, Marion Daubignard, Cristian Ene, Pascal Lafourcade, and Yassine Lakhnech. Automated proofs for asymmetric encryption. J. Autom. Reasoning, 46(3):261–291, 2011.
- Thao Dang, Colas Le Guernic, and Oded Maler. Computing reachable states for nonlinear biological

models. Theoretical Computer Science, April 2011.
- Ananda Basu, Saddek Bensalem, Doron Peled, and Joseph Sifakis. Priority scheduling of distributed systems based on model checking. Formal Methods in System Design, 39(3):229–245, 2011.
- David Monniaux. Quantifier elimination by lazy model enumeration. In Computer-aided verification (CAV). Springer, July 2010.

Logiciels importants:
- PinaVM A SystemC front-end based on the LLVM compiler infrastructure
- PAGAI Path Analysis for invariant Generation by Abstract Interpretation
- BIP Compiler, generation of C++ code from BIP models.
- D-Finder, verification of safety properties for component-based systems described in BIP.
- SpaceEx: The State Space Explorer platform for verification, monitoring, and simulation of hybrid systems

---

Faits illustrant le rayonnement ou l'attractivité académiques de l'entité
- Coordination du réseau d'excellence européen Artist Design
- Projet ERC STATOR (D. Monniaux)
- Organisation de grandes conférences: CAV 2009, ETAPS 2014
- Joseph Sifakis a été élu à l'Académie des Sciences en 2011, et nommé Commandeur de la Légion d'honneur en 2012.

Faits illustrant les interactions de l'entité avec son environnement socio-économique
- Création de la start-up Argosim
- 7 contrats CIFRE

Principales contributions de l'entité à des actions de formation
- Organisation de 5 écoles internationales pour doctorants
- Interventions dans plusieurs M2R, responsabilités à l'Ecole Doctorale MSTII

Executive summary

Title of the entity

Name of the laboratory : VERIMAG
Director for the current period: Nicolas Halbwachs
Director for the next period: Florence Maraninchi

Staff of the laboratory

- **at 1/1/2009:** 23 teaching researchers; 8 researchers; 10,5 administrative and technical staff; 35 post-docs and PhD-students; 2 detached researchers chercheurs.
- **at 30/06/2014:** 22 teaching researchers; 7 researchers; 10 administrative and technical staff; 43 post-docs and PhD-students; 3 detached researchers and 1 detached teaching researcher; 1 emeritus researcher.

Number of publications (1/1/2009–30/06/2014)

	Journal articles	Conferences	Theses	HDR
2009	12	79	4	1
2010	16	65	7	3
2011	17	75	5	0
2012	19	48	12	1
2013	12	54	8	0
2014	6	19	1	1
Total	82	340	37	6

Some major publications:

- Pierre Ganty, Radu Iosif, and Filip Konecný. Underapproximation of procedure summaries for integer programs. In TACAS, pages 245–259, 2013.
- Tayeb Bouhadiba, Matthieu Moy, and Florence Maraninchi. System-level modeling of energy in TLM for early validation of power and thermal management. In Design Automation and Test Europe (DATE), Grenoble, France, March 2013.
- Judicaël Courant, Marion Daubignard, Cristian Ene, Pascal Lafourcade, and Yassine Lakhnech. Automated proofs for asymmetric encryption. J. Autom. Reasoning, 46(3):261–291, 2011.
- Thao Dang, Colas Le Guernic, and Oded Maler. Computing reachable states for nonlinear biological models. Theoretical Computer Science, April 2011.
- Ananda Basu, Saddek Bensalem, Doron Peled, and Joseph Sifakis. Priority scheduling of distributed systems based on model checking. Formal Methods in System Design, 39(3):229–245, 2011.
- David Monniaux. Quantifier elimination by lazy model enumeration. In Computer-aided verification (CAV). Springer, July 2010.

Main softwares:

- PinaVM A SystemC front-end based on the LLVM compiler infrastructure
- PAGAI Path Analysis for invariant Generation by Abstract Interpretation
- BIP Compiler, generation of C++ code from BIP models.
- D-Finder, verification of safety properties for component-based systems described in BIP.
- SpaceEx: The State Space Explorer platform for verification, monitoring, and simulation of hybrid systems

Facts illustrating the academic influence and attractivity of the laboratory

- Coordination of the European network of excellence Artist Design
- ERC project STATOR (D. Monniaux)
- Organisation of major conferences: CAV 2009, ETAPS 2014
- Joseph Sifakis was elected at the Académy of Sciences en 2011, et nominated “Commandeur de la Légion d’honneur” in 2012.

Facts illustrating the interactions of the laboratory with its socio-economic environment

- Creation of the start-up Argosim
- 7 CIFRE contracts

Main contribution to training actions

- Organisation of 5 international schools
- Participation to several Masters, participation to the administration of the Doctoral School MSTII

Appendix B

Organisation chart
Organigramme fonctionnel

Direction
N. Halbwachs, S. Graf

Administration
- Affaires générales : Ch. Saunier
- Personnels: Ch. Saunier
- Budget : Ch. Saunier
- Contrats : V. Roux-Marchand
- Missions, commandes : R. Carbonero, S. Magnin

Service Informatique
P. Fulconis, Ph. Genin

Commission Moyens Informatiques
P. Fulconis, Ph. Genin, S. Graf, M. Moy, L. Mounier, C. Parent, P. Raymond

Commission Communication
K. Altisen, G. Frehse, S. Graf, E. Jahier

Responsables
- Hygiène et sécurité : Ch. Saunier
- Formation : V. Roux-Marchand
- Org. séminaires : S. Devismes
- Bibliothèque : D. Monniaux
- Site Web : E. Jahier
- Intranet : M. Bozga

Bureau
S. Graf, N. Halbwachs, Y. Lakhnech, O. Maler, F. Maraninchi

Conseil du Laboratoire

Equipes

Synchrone
Resp. F. Maraninchi (Prof.)
- 3 chercheurs CNRS
- 7 enseignants-chercheurs
- 4 ingénieurs et postdoc (1 IR: E. Jahier)
- 6 doctorants

DCS
Resp. Y. Lakhnech (Prof.)
- 2 chercheurs CNRS
- 11 enseignants-chercheurs
- 9 ingénieurs et postdoc (2 IR: M. Bozga, J. Combaz)
- 16 doctorants

Tempo
Resp. O. Maler (DR)
- 2 chercheurs CNRS
- 1 enseignant-chercheur
- 3 ingénieurs et postdoc (1 IR: O. Lebeltel)
- 8 doctorants

Appendix C

Internal rules
Règlement intérieur

- UNITE 5104 – VERIMAG

Règlement intérieur

I Règles de fonctionnement des instances du laboratoire

Le directeur : Le directeur de l'UNITE est nommé par le directeur général du CNRS, après avis des instances compétentes et du conseil de laboratoire, pour un mandat de 4 ans renouvelable deux fois.
Il est responsable de l'élaboration et de la mise en œuvre du projet scientifique de l'UNITE. Il doit, en s'appuyant sur le directeur adjoint et les responsables d'équipes :

- ✓ conduire et organiser l'UNITE
- ✓ motiver et évaluer le personnel ITA
- ✓ communiquer et informer à l'intérieur comme à l'extérieur du laboratoire
- ✓ situer son UNITE dans l'environnement scientifique.

Il est chargé par le directeur général du CNRS du bon fonctionnement et du respect des règles professionnelles dans le laboratoire. Il doit veiller à la sécurité des agents placés sous son autorité. Sa responsabilité pénale peut être recherchée en cas de manquement aux règles de sécurité.

L'assemblée générale : L'assemblée générale comprend tous les personnels titulaires et les personnels participant à l'activité de l'UNITE sous réserve d'une ancienneté minimale d'un an.
Elle se réunit au moins une fois par an. Elle est convoquée par le directeur du laboratoire.

Le conseil de laboratoire :
Le conseil de laboratoire de l'UNITE, présidé par le directeur du laboratoire, se réunit au moins 3 fois par an. Le conseil est créé par décision de la direction générale du CNRS pour un mandat de 4 ans. Il comprend 15 membres (le directeur, le directeur adjoint, 6 membres nommés, 7 membres élus). Il a un rôle consultatif sur :

- ✓ la coordination des recherches, la composition des équipes
- ✓ les moyens budgétaires à demander par l'UNITE et la répartition de ceux qui lui sont alloués,
- ✓ la politique des contrats de recherche concernant l'UNITE
- ✓ la politique de transfert de technologie et la diffusion de l'information scientifique de l'UNITE
- ✓ les demandes de moyens humains
- ✓ la politique de formation par la recherche
- ✓ les conséquences à tirer de l'avis formulé par les sections du Comité national de la recherche scientifique dont relève l'UNITE
- ✓ le plan de formation en cours et pour l'année à venir
- ✓ toutes mesures relatives à l'organisation et au fonctionnement de l'UNITE et susceptibles d'avoir une incidence sur la situation et les conditions de travail du personnel.

L'avis du conseil de laboratoire est pris avant l'établissement du rapport de stage des personnels recrutés dans le corps des ITA.
L'avis du conseil de laboratoire est recueilli par le directeur général du CNRS en vue de la nomination du directeur et du directeur adjoint de l'UNITE.

Appartenance au laboratoire
Les membres du laboratoire se répartissent entre **:**

- ✓ membre titulaire : est membre titulaire tout personnel relevant du statut de fonctionnaire affecté à l'UNITE ou l'ayant pour appartenance principale.
- ✓ membre non titulaire : personnel travaillant temporairement dans l'UNITE dans le cadre d'une rémunération CDD, d'une bourse, de vacations…
- ✓ membre associé : tout personnel statutaire ayant choisi l'UNITE en rattachement secondaire
- ✓ personnels en CDI
- ✓ invités : tous personnels invités dans l'UNITE
- ✓ stagiaire : tout personnel accueilli dans l'UNITE dans le cadre d'une convention de stage.
  Les stagiaires accompagnés de leur directeur de stage devront se présenter au secrétariat qui leur fournira les informations utiles et les règles à respecter pendant leur séjour au laboratoire.
  Tout stagiaire reste sous l'entière responsabilité de son directeur de stage, qui doit veiller au respect des règles du laboratoire.

II Règles de fonctionnement général

1 Nouvel entrant : tout nouvel entrant est invité à se présenter au secrétariat et à fournir tous les renseignements nécessaires à la gestion de son dossier. Il lui sera remis la charte informatique, le code de bonne conduite (annexe C), les consignes d'alarme, le règlement intérieur de l'unité.

2 Horaires de travail :

Durée annuelle du travail (concerne tous les personnels ITA et les chercheurs CNRS)
A compter du **1er janvier 2004**, la durée annuelle du **travail effectif** est fixée à **1607 heures**.
La durée quotidienne du travail effectif ne peut excéder 10 heures.
Le temps de travail effectif se définit comme le temps pendant lequel l'agent est à la disposition de son employeur et doit se conformer à ses directives sans pouvoir vaquer librement à des occupations personnelles.

Cette définition intègre dans le temps de travail effectif, l'exercice du droit à la formation, des droits syndicaux et sociaux.

En revanche, ne constituent pas du temps de travail effectif :

♦ Le temps de pause méridienne, ainsi que toute autre pause durant laquelle la personne n'est pas à la disposition de son employeur (n'a pas à se conformer à ses directives, et peut vaquer librement à des occupations personnelles)

♦ Le temps de trajet entre le domicile et le lieu de travail habituel. Est du temps de travail effectif, le temps de trajet entre le lieu habituel de travail et un autre lieu de travail désigné par l'employeur, notamment pour les personnels ayant deux lieux de travail habituel.

Durée hebdomadaire du travail

La durée hebdomadaire du travail effectif est égale à **38h30** pour les personnels CNRS, au moins **36h40** pour les personnels universitaires (pause de 20 minutes comprise) titulaires et non titulaires en fonction dans l'établissement, au plus **38h20** pour l'UJF.
L'horaire journalier de travail pour les agents CNRS est : 8h30 - 12h & 13h -17h12.
Le travailleur isolé doit être occasionnel et consacré à des tâches ne présentant aucun risque.Dans le cas où des travaux dangereux doivent nécessairement être exécutés en dehors des horaires normaux et/ou sur des lieux isolés ou locaux éloignés, il est strictement obligatoire d'être accompagné.

Cycle de travail

Le travail est organisé collectivement selon un cycle hebdomadaire de **5 jours**.
Toutefois, le travail des agents autorisés à accomplir un service à temps partiel d'une **durée inférieure ou égale à 80%** de la durée hebdomadaire, peut se dérouler selon un **cycle inférieur à 5 jours.**

Le nombre de jours de congés annuels et de jours « RTT » des agents autorisés à travailler à temps partiel est calculé en fonction de la quotité du temps travaillé.

Congés annuels

Le nombre de jours de congés annuels est fixé par **chaque tutelle** pour une année civile ou universitaire.
Il est de 32 jours ouvrés pour le CNRS et de 45 jours ouvrés pour l' INPG et l' UJF .
Les agents CNRS bénéficient des deux jours de fractionnement des congés annuels conformément à l'article 1er décret du 26 octobre 1984 susvisé.

La détermination des jours RTT

Le nombre de jours « RTT » est fonction de la durée hebdomadaire de travail, retenu par chaque établissement. Il est de 13 jours pour les agents CNRS.

L'utilisation des jours de congés et de RTT

Les jours RTT et les jours de congés sont utilisés dans les mêmes conditions.
Les jours RTT et les jours de congés dont disposent les agents au delà des jours de fermeture sont utilisés dans des conditions identiques à savoir celles relatives aux congés annuels : ils sont accordés par

le Directeur de laboratoire, sous réserve des nécessités de service (décret n° 84-972 du 26 octobre 1984 relatif aux congés annuels des fonctionnaires de l'Etat, qui précise : « le calendrier des congés est fixé par le chef du service, après consultation des fonctionnaires intéressés, compte tenu des fractionnements et échelonnements de congés que l'intérêt du service peut rendre nécessaires. Les fonctionnaires chargés de famille bénéficient d'une priorité pour le choix des périodes de congés annuels »).

Un délai de prévenance de 2 jours est fixé pour les congés isolés. Les congés « d'été » doivent être demandés en Mai afin que l'organisation du travail puisse être adaptée en conséquence (personnels UJF et CNRS). Pour les personnels INPG, un planning annuel concernant les congés de 5 jours au moins sera établi avant la fin janvier. Pour les congés inférieurs à 5 jours la demande sera déposée deux semaines à l'avance.

Les jours de congés et les jours RTT non utilisés pendant l'année civile pour les personnels CNRS et universitaire pour les personnels INPG et UJF sont reportables jusqu'au 28 février de l'année suivante pour le CNRS, au 31 décembre pour l'INPG et L'UJF.
Les jours qui n'auront pas été utilisés à cette date seront définitivement perdus, sauf si ces jours ont été déclarés dans un Compte épargne temps.

Durée des absences de service

L'absence de service ne peut excéder 31 jours consécutifs (la durée de l'absence est calculée du premier au dernier jour sans déduction des samedis, dimanches et jours fériés) pour les agents CNRS, 30 jours ouvrés consécutifs pendant la période juillet et août pour les agents UJF (sauf cas spécifiques liés aux activités pédagogiques).

Contrôle des congés

Les jours de congés annuels et les jours « RTT » seront comptabilisés au niveau de l'UNITE.

3 - Absence :

Toute indisponibilité consécutive à la maladie doit, sauf cas de force majeure dûment justifiée, être signalée au secrétariat du personnel de l'UNITE dans les 24 heures. Sous les 48 heures qui suivent l'arrêt de travail, le salarié produira un certificat médical indiquant la durée prévisible de l'indisponibilité.
En cas d'accident ou de maladie professionnelle, le salarié fournira, dans les 48 heures, au secrétariat de l'UNITE, une déclaration d'accident et un certificat initial. La production de ce certificat est indispensable pour l'ouverture du dossier.
Tout accident corporel survenant à l'UNITE, quel qu'en soit le caractère de gravité, sera immédiatement signalé au secrétariat de l'UNITE. Dans un but de prévention, les circonstances de l'accident seront consignées sur la « fiche d'accident » fournie par le secrétariat.

4 Confidentialité :

Chacun est tenu de respecter la confidentialité des travaux qui lui sont confiés ainsi que ceux de ses collègues. En particulier, en cas de présentation à l'extérieur, l'autorisation du responsable scientifique est obligatoire.

5 Publications :

Un exemplaire de toutes les publications (articles, revues, thèses…) dont tout ou partie du travail a été effectué à l'unité doit être remis dès parution sur le site Web du laboratoire et dans l'application HAL.
Les publications des membres de l'Unité doivent faire apparaître l'appartenance à l'Unité et le rattachement aux tutelles sous la forme :
Nom
CNRS
Intitulé tutelle
Intitulé Unité

6 Hygiène et sécurité :

Chacun doit se préoccuper de sa propre sécurité et de celle des autres. Il incombe au Directeur de veiller à la sécurité et à la protection des agents et d'assurer la sauvegarde des biens de l'UNITE.
L'ACMO (agent chargé de la mise en œuvre des règles d'hygiène et de sécurité, voir liste en annexe A) est nommé par le directeur du laboratoire après avis du conseil de l'unité. Il assiste et conseille le directeur, sensibilise les agents aux consignes, participe à la formation des agents, aux visites de

contrôle de l'inspecteur de l'hygiène et de la sécurité, assure la bonne tenue du registre et tire les enseignements des accidents intervenus dans l'UNITE.
L'interdiction de fumer s'applique dans les locaux. Cette décision st conforme à la législation en vigueur (décret N°2006-1386 du 15 novembre 2006.

Accidents :
En cas d'accident ou de blessures, s'adresser au : **15**, prévenir l'ACMO.
Incendie :
En cas d'incendie, donner l'alerte au **18**, fermer les portes et les fenêtres, appeler à l'aide et contacter l'équipe d'intervention incendie dont la liste est affichée dans les laboratoires.
Des extincteurs sont à votre disposition dans le laboratoire, mais les lances à incendie ne peuvent être utilisées que par les personnes habilitées.
Après utilisation d'extincteurs, prévenir l'ACMO pour remplacement.
Alerte incendie :
En cas de déclenchement des sirènes d'alarmes, tout le personnel doit EVACUER rapidement le bâtiment et dans l'ordre, assisté par les équipes de première intervention.

7 Informatique

L'utilisation des moyens informatiques est soumise à des règles explicitées dans la charte informatique du CNRS dont les nouveaux utilisateurs prendront connaissance. Cette charte est avant tout un code de bonne conduite (voir annexe B). Elle a pour objet de préciser la responsabilité des utilisateurs, en accord avec la législation, afin d'instaurer un usage correct des ressources informatiques et des services Internet, avec des règles minimales de courtoisie et de respect d'autrui.

8 Informations

- ✓ sur panneau d'affichage pour les informations administratives, syndicales et sociales.
- ✓ sur le site de l'UNITE (serveur Web) pour la diffusion et la promotion de ses activités scientifiques et de ses compétences techniques.

Selon les dispositions légales en vigueur, un tel site web constitue une publication de l'UNITE dont le directeur de publication, responsable légal, est le directeur du laboratoire.
Un comité de rédaction, dirigé par le « Webmaster », gère le contenu du serveur. Ce comité de rédaction comprend outre le « Webmaster » des représentants de chaque équipe de recherche.
Les pages personnelles sont sous la seule responsabilité des personnes qui devront respecter la charte informatique.

9 Formation

Les agents de l'UNITE sont invités à discuter de leur souhait de formation avec leur Directeur et le correspondant de formation. Les demandes retenues seront adressées aux bureaux de formation concernés.
Tous les nouveaux arrivants devront suivre une sensibilisation hygiène et sécurité dispensée par l'ACMO.

10 Missions

Tout agent se déplaçant pour l'exercice de ses fonctions doit être en possession d'un ordre de mission (ou d'une convocation valant ordre de mission) établi **préalablement** au déroulement de la mission. Ce document est **obligatoire** du point de vue administratif et juridique (seul l'agent muni d'un ordre de mission régulièrement établi est couvert au regard de la réglementation sur les accidents de service) et financier. L'ordre de mission peut être **avec frais** ou **sans frais**.

11 Locaux

Le Bâtiment est ouvert de 6h à 23h45 du lundi au vendredi. Après 18h, l'agent accède au bâtiment sous sa seule responsabilité.
Avant de quitter le laboratoire chaque agent doit s'assurer que les fenêtres, les portes sont fermées. Les stores baissés et les lumières éteintes.
En dehors des horaires d'ouverture, les personnes présentes doivent respecter les consignes concernant la mise sous alarme du bâtiment.

Les Réservations de salles doivent être faites sur le site Intranet prévu à cet effet.

12 Départ du laboratoire

Chaque personnel quittant le laboratoire doit passer au secrétariat rendre la carte d'accès aux locaux et la clé de son bureau.

III Annexes

- A : liste ACMO
- B : Charte informatique
- C : Code de bonne conduite

Ce règlement intérieur a été présenté et adopté en conseil de laboratoire le 15 octobre 2007. Toute modification fera l'objet d'un avenant signé des tutelles.

Farid OUABDESSELAM	Paul JACQUET	Younis HERMES
Président	Président	Délégué Régional
UJF	INP Grenoble	CNRS site Alpes

Appendix D

Research production
Réalisations et produits de la recherche

D.1 Production globale

La production du laboratoire est évidemment le fait des équipes, les détails en seront donnés dans les sections D.2, D.3 et D.4 qui leur sont consacrées. Nous donnons ici un résumé de la production globale, et les éléments qui relèvent du laboratoire dans son ensemble.

D.1.1 Production scientifique globale

D.1.1.1 Publications

	Journaux	Conférences	HDR	Thèses
2009	12	79	1	4
2010	16	65	3	7
2011	17	75		5
2012	19	48	1	12
2013	12	54		8
2014	6	19	1	1
Total	82	340	6	37

D.1.1.2 Logiciels

17 outils logiciels sont maintenus et distribués.

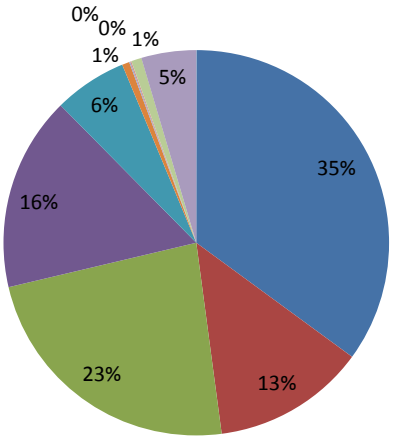
D.1.2 Rayonnement et administration de la recherche

D.1.2.1 Projets

La Figure D.1 donne le nombre et le montant (en K€) des projets et contrats de la période, selon leur provenance.

D.1.2.2 Activités éditoriales

- **(Co-)Présidence des comités de programme** de CAV09, EMSOFT09, EMSOFT12, FMCAD13, RV09, RV13, FORMATS14.



	nb.	K€
Europe hors ERC	14	4017
Europe ERC	1	1472
ANR	20	2682
Poles de compétitivité	6	1868
PIA	2	702
AGIR/MSTIC	2	70
PERSYVAL	2	10
Inria	1	12
Carnot	2	100
Industriel	11	527

Figure D.1: Projets de la période

Participation à 123 **comités de programme** de conférences et workshops internationaux.
Appartenance aux **comités de pilotage** des conférences EMSOFT, HSCC, "Frontiers in Analog Circuits", ETAPS, Runtime Verification, SPIN Symposium.

- Membres des **comités de rédactions** des journaux "Formal Methods in System Design" (Springer), "Software Tools for Technology Transfer" (Springer), "Leibniz Transactions on Embedded Systems" (Dagstuhl).

D.1.2.3 Organisation d'événements et d'écoles

2009 ARTIST School in South America : Embedded Systems Design, Buenos Aires
ARTIST Summer School in China, Tsinghua
ARTIST Summer School in Europe, Autrans
International Conference CAV'09, Grenoble
3rd International Workshop on Security and Electronic Voting, Grenoble
2nd Canada-France Workshop on Foundations & Practice of Security
Ecole Temps Réél. ETR 2009, Telecom Paris-Tech (day on real time applications)
Dagstuhl Seminar on Specification and Validation of Concurrent Software
2010 International Conference MEMOCODE'10, Grenoble
Int. Workshop on Model-Based Architecting and Construction of Embedded Systems (ACES^{MB}), Oslo
2011 B 2011, Limerick
MEMOCODE 2011, Cambridge
VERIDYC Verification and Synthesis, Grenoble
Workshop on Foundations & Practice of Security, Paris
ARTIST Summer School in Europe 2011, Aix-les-Bains
Second Workshop : Toward Systems Biology, Grenoble
Workshop ACCA, Chamonix
International Conference SSS'11, Grenoble
2012 Workshop Computed Aided Security, Grenoble
HSCC'12, Beijing
20 years of Verimag, Grenoble
ICDCN, Hong Kong
2013 IWHSB, Florence
PERSYVAL-Lab Summer School on Cyber-Physical Systems

Workshop WCET 2013, Paris
Workshop FIMCP 2013, Marrakech

2014 European Joint Conferences ETAPS'2014, Grenoble
Journée Code et Cryptographie 2014, Grenoble,
École de printemps C2 2014, Grenoble
International Conference FORMATS'14, Florence
International Workshop Hybrid Systems and Biology, Vienna
Int. Workshop on Formal Methods for Timing Analysis (FMTA), Singapore
Int. Workshop on Model-Based Architecting and Construction of Embedded Systems (ACES^{MB}), Barcelona
Workshop on Synthesis of Continuous Parameters (SynCoP), ETAPS, Grenoble
Workshop on Applied Verification of Continuous and Hybrid Systems (ARCH), CPSWeek, Berlin

D.1.2.4 Conférences invitées

2009 CAV 09 (Joseph Sifakis), DATE 09 (Joseph Sifakis)
2010 CPSWeek 2010 (Oded Maler), Ecole d'été de Marktoberdorf 2010 (Susanne Graf), FDL 2010 (Barbara Jobstmann)
2011 VLSI-Soc'11 (J. Sifakis), China National Computer Conference 2011 (J. Sifakis), 4th Science Conclave 2011 (J. Sifakis), FORMATS'11 (O. Maler), EMSOFT'11 (O. Maler), MEMICS 2011 (S. Bensalem), SIES 2011 (B. Jobstmann), Intel&Technion Symposium, Haifa, Israël, september 2011 (F. Maraninchi)
2012 LCTES 2012 (N. Halbwachs), CSS 2012 (P. Lafourcade)
2013 Embedded China 2013 (J-F. Monin), MACIS 2013 (D. Monniaux), iFM 2013 (Susanne Graf)
2014 ISPDC 2014 (Susanne Graf), Journées Nationales des Communications Terrestres (P. Lafourcade) ; Cours du collège de France (M. Moy), FSFMA 2014 (S. Graf)

D.1.2.5 Administration de la recherche

- 2010-12 : Coordonateur du réseau d'excellence ARTIST2 et ARTIST/Design
- 2013-14 : Strategic Management Board of EMSIG (Embedded Systems Special Interest Group)
- 2010-12 : Co-animation du GT2 d'Allistene "Conception et réalisation de systèmes matériels et logiciels"
- 2010-11 : Co-animation du groupe de travail SNRI "sécurité des technologies de l'information et de la communication dans un contexte de sécurité globale"
- 2009-14 : Comité Opérationnel et Comité d'Evaluation du cluster Logiciel (ex EMSOC) du pôle de compétitivité Minalogic
- 2012-14 : Co-responsable du comité scientifique du thème "Pervasive Computing Systems" du labex Persyval-Lab
- 2010-14 : Direction du CRI PILSI
- 2013-14 : Comité scientifique du GDR GPL
- 2012 : Présidence du comité d'évaluation du LIAMA
- 2011 : Comités de selection de projets d'excellence DFG (Allemagne)
- 2013-14 : Swedish Research Council subcommittee for Computer Science
- 2014 : Portuguese Research Council FCT selection of PhD schools

ANR
2010 Comité scientifique SIMI3 des projets "Blanc" "Jeunes chercheurs" et "Blanc international"
2011-13 Comité scientifique SIMI2 des projets "Blanc" "Jeunes chercheurs" et "Blanc international" (vice-présidence en 2013)
2010-12 Comité Scientifique Sectoriel STIC
2013-14 Comité de Pilotage Scientifique du défi 7 "Société de l'information et de la communication"

Comités AERES : IRIT 2009, IRISA 2010, Inria Sophia-Antipolis 2010, INRIA-Bretagne 2011, I3S 2011, LIPN 2012, CRISTAL (LIFL+LAGIS, pres.) 2013, IRCICA 2014 (pres.)

Comités de sélection locaux et nationaux

2009 UJF/LIG (chaire INRIA), INP/LIG (chaire CEA)
2010 UPS/IRIT MCF (chaire CNRS), Concours DR2 INRIA, INP/LIG PR (pres.)
2011 INP MCF (pres.), UJF MCF (pres.), UJF PR (pres.), UPS/IRIT PR , Ecole Polytechnique MCF (chaire CNRS), UPJV Amiens MCF, MCF 27 Lille 1, CNAM PR 27, UPEC PR 27
2012 UJF PR 27, UJF PR 26-27 (pres.), CNAM PR 27, INSA Lyon MCF 27, U. Bordeaux MCF 27
2013 UJF MCF 27, UPEC MCF 27, MCF 27 Limoges
2014 INSA Bourges PR 27, ENS Lyon MCF 27, UPS/IRIT MCF 27, ENS Lyon MCF 27

Comités de sélection internationaux

2009 Assistant PR Uppsala university
2011 PR University of Lugano
2012 PR Chalmers Goeteborg, PR KTH 2012
2013 PR Chalmers Goeteborg

D.1.2.6 Responsabilités universitaires

- 2009-2011 : Direction de l'UFR IM2AG
- 2009-2011 : Direction adjointe DLST
- 2011-2013 : Présidence du CEVU de l'UJF
- 2011-2014 : Présidence du CS de l'UJF
- 2009-2014 : Responsabilité des relations internationales de l'Ensimag
- CEVU et Commission des finances de Grenoble INP
- Conseil de l'Ensimag
- Conseil Scientifique de l'INP
- Conseil Scientifique de l'UFR IM^{2}AG
- Commission HDR de Grenoble INP
- Bureau de l'Ecole doctorale MSTII

D.1.2.7 Visites de longue durée

- 2009 : Doron Peled, 7 semaines - Bruce Krogh 3 mois
- 2010 : Ian Mitchell, 1 mois - Doron Peled, 3 mois
- 2011 : Doron Peled 2011, 2 mois - Viktor Kuncak, 1 mois - Laura Kovacs, 1 mois
- 2012 : Doron Peled 2012, 2 mois

D.1.2.8 Distinctions

- N. Halbwachs, Academia Europaea (2010)
- J. Sifakis, Académie des Sciences (2011)
- J. Sifakis, Commandeur de la Légion d'honneur (2012)

D.1.3 Interactions avec l'environnement économique, social et culturel

- Durant la période, le laboratoire a bénéficié de 7 contrats CIFRE.
- Une start-up a éte créé en 2013 (cf. §2.1.2.3, page 19).
- Depuis 2007, F. Maraninchi est l'un des deux membres académiques du comité opérationnel et d'évaluation du Pôle de compétitivité Minalogic.
- O. Maler est membre du conseil technique de la société ATRENTA.
- En 2012, J. Sifakis et N. Halbwachs ont été appelés pour 2 jours de consultance auprès de la société Astrium.

- En 2010, S. Bensalem, responsable du projet MARAE, a reçu un des trois prix de la meilleure publication scientifique des programmes de recherche de la Fondation de Recherche pour l'Aéronautique et l'Espace, qui ont été remis par les dirigeants des groupes EADS, Safran et Thalès.

D.2 Synchrone team: production

D.2.1 Synchrone team: Publications, by Categories

D.2.1.1 International Journals

[S-J1] Thomas Braibant, Jacques-Henri Jourdan, and David Monniaux. Implementing and reasoning about hash-consed data structures in Coq. *Journal of Automated Reasoning*, pages 1–34, June 2014.

[S-J2] Karine Altisen, Stéphane Devismes, Antoine Gerbaud, and Pascal Lafourcade. Comparison of mean hitting times for a degree-biased random walk. *Discrete Applied Mathematics*, 170:104–109, 2014.

[S-J3] Ajoy Kumar Datta, Lawrence L. Larmore, Stéphane Devismes, Karel Heurtefeux, and Yvan Rivierre. Self-stabilizing small k-dominating sets. *IJNC, International Journal of Networking and Computing*, 3(1):116–136, 2013.

[S-J4] Ajoy Kumar Datta, Lawrence L. Larmore, Stéphane Devismes, and Yvan Rivierre. Self-stabilizing labeling and ranking in ordered trees. *Theoretical Computer Science (Special Issue SSS 2011)*, 512:49–66, 2013.

[S-J5] Stéphane Devismes, Franck Petit, and Sébastien Tixeuil. Optimal probabilistic ring exploration by semi-synchronous oblivious robots. *Theoretical Computer Science (TCS)*, 498:10–27, 2013.

[S-J6] Florence Maraninchi, Nicolas Halbwachs, Pascal Raymond, Catherine Parent, and R. K. Shyamasundar. Specification and validation of embedded systems: A case study of a fault-tolerant data acquisition system with Lustre programming environment. *CSI Journal of Computing*, 1(4), September 2013.

[S-J7] Ajoy Kumar Datta, Stéphane Devismes, Karel Heurtefeux, Lawrence L. Larmore, and Yvan Rivierre. Algorithme autostabilisant construisant un petit ensemble k-dominant. *Technique et Science Informatiques*, 31(8):1273–1299, 2012.

[S-J8] Thomas Gawlitza and David Monniaux. Invariant generation through strategy iteration in succinctly represented control flow graphs. *Logical Methods in Computer Science*, 2012.

[S-J9] Sebastian Altmeyer, Robert I. Davis, and Claire Maiza. Improved cache related pre-emption delay aware response time analysis for fixed priority pre-emptive systems. *Real-Time Systems*, 48(5):499–526, 2012.

[S-J10] Nicolas Berthier, Florence Maraninchi, and Laurent Mounier. Synchronous programming of device drivers for global resource control in embedded operating systems. *ACM Transactions on Embedded Computing Systems (TECS)*, 12, 2013. Selected papers from LCTES'11.

[S-J11] Fabienne Carrier, Stéphane Devismes, Franck Petit, and Yvan Rivierre. Asymptotically optimal deterministic rendezvous. *International Journal of Foundations of Computer Science (IJFCS)*, 22:1143–1159, 2011.

[S-J12] Ajoy Kumar Datta, Stéphane Devismes, Florian Horn, and Lawrence L. Larmore. Self-stabilizing k-out-of-l exclusion on tree networks. *International Journal of Foundations of Computer Science*, 22(3):657–677, 2011.

[S-J13] Stéphane Devismes, Franck Petit, and Vincent Villain. Autour de l'auto-stabilisation. partie i : Techniques généralisant l'approche. *Technique et science informatiques (TSI)*, 30/7:883–894, octobre 2011. numéro spécial algorithmique distribuée.

[S-J14] Stéphane Devismes, Franck Petit, and Vincent Villain. Autour de l'auto-stabilisation. partie ii : Techniques spécialisant l'approche. *Technique et science informatiques (TSI)*, 30/7:895–922, octobre 2011. numéro spécial algorithmique distribuée.

[S-J15] Carole Delporte-Gallet, Stéphane Devismes, and Hugues Fauconnier. Stabilizing leader election in partial synchronous systems with crash failures. *J. Parallel Distrib. Comput.*, 70(1):45–58, 2010.

[S-J16] Sylvie Delaët, Stéphane Devismes, Mikhail Nesterenko, and Sébastien Tixeuil. Snap-stabilization in message-passing systems. *Journal of Parallel and Distributed Computing (JPDC)*, 70(12):1220–1230, 2010.

[S-J17] Stéphane Devismes, Hirotsugu Kakugawa, Sayaka Kamei, and Sébastien Tixeuil. A self-stabilizing 3-approximation for the maximum leaf spanning tree problem in arbitrary networks. *Journal of Combinatorial Optimization (Special Issue)*, 25(3):430–459, 2013.

[S-J18] David Monniaux. Automatic modular abstractions for template numerical constraints. *Logical Methods in Computer Science*, June 2010.

[S-J19] Claude Helmstetter, Florence Maraninchi, and Laurent Maillet-Contoz. Full simulation coverage for systemC transaction-level models of systems-on-a-chip. *Formal Methods in System Design*, 35(2):152–189, October 2009.

[S-J20] Jan Mikác and Paul Caspi. Flush: an example of development by refinements in SCADE/Lustre. *International Journal on Software Tools for Technology Transfer (STTT)*, 11(5), 2009.

[S-J21] David Monniaux. A minimalistic look at widening operators. *Higher order and symbolic computation*, 22(2):145–154, December 2009.

D.2.1.2 International Conferences

[S-C1] Julien Henry, Mihail Asavoae, David Monniaux, and Claire Maïza. How to compute worst-case execution time by optimization modulo theory and a clever encoding of program semantics. In *ACM SIGPLAN 2014 Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES 2014)*, 2014.

[S-C2] Karine Altisen and Stéphane Devismes. On probabilistic snap-stabilization. In *ICDCN'2014, 15th International Conference on Distributed Computing and Networking*, pages 272–286, Coimbatore, India, January 4-7 2014. LNCS.

[S-C3] Karine Altisen and Stéphane Devismes. Stabilisation instantanée probabiliste. In *16èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (AlgoTel)*, Le-Bois-Plage-en-Ré, France, 2014.

[S-C4] Jan Reineke, Sebastian Altmeyer, Daniel Grund, Sebastian Hahn, and Claire Maiza. Selfish-lru: Preemption-aware caching for predictability and performance. In *Proceedings of the 20th Real-Time and Embedded Technology and Applications Symposium (RTAS'14)*, April 2014.

[S-C5] Erwan Jahier, Simplice Djoko-Djoko, Chaouki Maiza, and Eric Lafont. Environment-model based testing of control systems: Case studies. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2014), Held as Part of ETAPS 2014*, Grenoble, France, April 2014. LNCS.

[S-C6] Karine Altisen, Stéphane Devismes, Raphaël Jamet, and Pascal Lafourcade. SR3: Secure resilient reputation-based routing. In *The annual IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS 2013)*, pages 258–265, Cambridge, Massachusetts, USA, May 2013. IEEE.

[S-C7] Karine Altisen, Stéphane Devismes, Raphaël Jamet, and Pascal Lafourcade. Routage sécurisé et résilient pour réseaux de capteurs sans fil. In Nicolas Nisse, Franck Rousseau, and Yann Busnel, editors, *15èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (AlgoTel)*, pages 1–4, Pornic, France, 2013.

[S-C8] Mihail Asavoae, Claire Maiza, and Pascal Raymond. Program semantics in model-based WCET analysis: A state of the art perspective. In Claire Maiza, editor, *13th International Workshop on Worst-Case Execution Time Analysis, WCET 2013, July 9, 2013, Paris, France*, volume 30 of *OASICS*, pages 32–41. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2013.

[S-C9] Tayeb Bouhadiba, Matthieu Moy, and Florence Maraninchi. System-level modeling of energy in TLM for early validation of power and thermal management. In *Design Automation and Test Europe (DATE)*, Grenoble, France, March 2013.

[S-C10] Tayeb Bouhadiba, Matthieu Moy, Florence Maraninchi, Jérôme Cornet, Laurent Maillet-Contoz, and Ilija Materic. Co-Simulation of Functional SystemC TLM Models with Power/Thermal Solvers. In *Virtual Prototyping of Parallel and Embedded Systems (VIPES)*, Boston, États-Unis, May 2013.

[S-C11] Thomas Braibant, Jacques-Henri Jourdan, and David Monniaux. Implementing hash-consed data structures in Coq. In *Interactive theorem proving (ITP)*, volume 7998, 2013.

[S-C12] Fabienne Carrier, Ajoy Kumar Datta, Stéphane Devismes, Lawrence L. Larmore, and Yvan Rivierre. Algorithme autostabilisant avec convergence sûre construisant une (f, g)-alliance. In Nicolas Nisse, Franck Rousseau, and Yann Busnel, editors, *Algotel : 15èmes Rencontres Francophones pour les Aspects Algorithmiques des Télécommunications*, Pornic, France, May 2013.

[S-C13] Fabienne Carrier, Ajoy Kumar Datta, Stéphane Devismes, Lawrence L. Larmore, and Yvan Rivierre. Self-stabilizing (f,g)-alliances with safe convergence. In *SSS'2013, 15th International Symposium on Stabilization, Safety, and Security of Distributed Systems*, Lecture Notes in Computer Science, pages 61–73, Osaka, Japan, November 13-16 2013. Springer.

[S-C14] Ajoy Kumar Datta, Stéphane Devismes, and Lawrence L. Larmore. Self-stabilizing silent disjunction in an anonymous network. In *ICDCN: 14th International Conference on Distributed Computing and Networking*, Lecture Notes in Computer Science, pages 148–160, Tata Institute of Fundamental Research, Mumbai, India, January 3-6 2013. Springer.

[S-C15] Ajoy Kumar Datta, Stéphane Devismes, Lawrence L. Larmore, and Sébastien Tixeuil. Fast leader (full) recovery despite dynamic faults. In *ICDCN: 14th International Conference on Distributed Computing and Networking*, Lecture Notes in Computer Science, pages 428–433, Tata Institute of Fundamental Research, Mumbai, India, January 3-6 2013. Springer.

[S-C16] Alexis Fouilhé, David Monniaux, and Michael Périn. Efficient generation of correctness certificates for the abstract domain of polyhedra. In *Static analysis (SAS 2013)*, volume 7935 of *LNCS*. Springer, 2013.

[S-C17] Claude Helmstetter, Jérôme Cornet, Bruno Galilée, Matthieu Moy, and Pascal Vivet. Fast and Accurate TLM Simulations using Temporal Decoupling for FIFO-based Communications. In *Design, Automation and Test in Europe (DATE)*, page 1185, Grenoble, France, March 2013.

[S-C18] Rob Davis, Luca Santinelli, Sebastian Altmeyer, Claire Maiza, and Liliana Cucu-Grosjean. Analysis of Probabilistic Cache Related Pre-emption Delays. In *25th Euromicro Conference on Real-Time Systems (ECRTS 2013)*, pages 168–179, July 2013.

[S-C19] Will Lunniss, Sebastian Altmeyer, Claire Maiza, and Robert I. Davis. Integrating cache related pre-emption delay analysis into EDF scheduling. In *19th IEEE Real-Time and Embedded Technology and Applications Symposium, RTAS 2013, Philadelphia, PA, USA, April 9-11, 2013*, pages 75–84. IEEE Computer Society, 2013.

[S-C20] Matthieu Moy. Parallel Programming with SystemC for Loosely Timed Models: A Non-Intrusive Approach. In *The Design, Automation, and Test in Europe (DATE)*, Grenoble, France, Mar 2013.

[S-C21] Franck Petit, Anissa Lamani, Stéphane Devismes, Sébastien Tixeuil, and Pascal Raymond. Explorer une grille avec un minimum de robots amnésiques. In Nicolas Nisse, Franck Rousseau, and Yann Busnel, editors, *15èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (AlgoTel)*, pages 1–4, Pornic, France, May 2013.

[S-C22] Pascal Raymond, Claire Maiza, Catherine Parent-Vigouroux, and Fabienne Carrier. Timing analysis enhancement for synchronous program. In *RTNS*, pages 141–150, 2013.

[S-C23] Erwan Jahier, Nicolas Halbwachs, and Pascal Raymond. Engineering functional requirements of reactive systems using synchronous languages. In *International Symposium on Industrial Embedded Systems, 2013. SIES'13.*, Porto, Portugal, 06 2013.

[S-C24] Karine Altisen, Stéphane Devismes, Antoine Gerbaud, and Pascal Lafourcade. Analysis of random walks using tabu lists. In Magnus M. Halldorsson and Guy Even, editors, *19th International Colloquium on Structural Information and Communication Complexity (SIROCCO'2012)*, LNCS, pages 254–266, Reykjavík, Iceland, June 30 - July 2 2012. Springer.

[S-C25] Julien Douady, Christian Hoffmann, Fabienne Carrier, Benoit Chabaud, Arnaud Mantoux, Yves Markowicz, Michael Périn, Virginie Stoppin-Mellet, Gabrielle Tichtinsky, Bernard Ycart, and Hubert Borderiou. Un dispositif pour alerter les étudiants sur leur maîtrise des pré-requis nécessaires pour réussir leur entrée à l'université. In *Congrès de l'Association Internationale de Pédagogie Universitaire*, May 2012.

[S-C26] Diego Caminha Barbosa de Oliveira and David Monniaux. Experiments on the feasibility of using a floating-point simplex in an SMT solver. In *Workshop on Practical Aspects of Automated Reasoning (PAAR)*. CEUR Workshop Proceedings, 2012.

[S-C27] Jérôme Cornet, Laurent Maillet-Contoz, Ilija Materic, Sylvian Kaiser, Hela Boussetta, Tayeb Bouhadiba, Matthieu Moy, and Florence Maraninchi. Co-Simulation of a SystemC TLM Virtual Platform with a Power Simulator at the Architectural Level: Case of a Set-Top Box. In *Design Automation Conference, Session 10U: User Track*, San Francisco, États-Unis, June 2012.

[S-C28] Ajoy Kumar Datta, Stéphane Devismes, Karel Heurtefeux, Lawrence L. Larmore, and Yvan Rivierre. Competitive self-stabilizing k-clustering. In Xavier Defago and Wang-Chien Lee, editors, *ICDCS*, pages 476–485, Macau, China, June 2012. IEEE.

[S-C29] Kumar Ajoy Datta, Stéphane Devismes, Karel Heurtefeux, Lawrence L. Larmore, and Yvan Rivierre. Algorithme de k-partitionnement auto-stabilisant et compétitif. In *14èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (AlgoTel)*, pages 135–138, La Grande Motte, France, 2012.

[S-C30] Ajoy Kumar Datta, Stéphane Devismes, and Lawrence L. Larmore. Brief announcement: Self-stabilizing silent disjunction in an anonymous network. In Andréa W. Richa and Christian Scheideler, editors, *Stabilization, Safety, and Security of Distributed Systems - 14th International Symposium, SSS 2012, Toronto, Canada, October 1-4, 2012. Proceedings*, volume 7596 of *Lecture Notes in Computer Science*, pages 46–48. Springer, 2012.

[S-C31] Stéphane Devismes, Anissa Lamani, Franck Petit, Pascal Raymond, and Sébastien Tixeuil. Optimal grid exploration by asynchronous oblivious robots. In Andrea Richa Sukumar Ghosh, editor, *14th International Symposium on Stabilization, Safety, and Security of Distributed Systems, SSS*, pages 64–76, Toronto, Canada, October 2012. LNCS.

[S-C32] Stéphane Devismes and Franck Petit. On efficiency of unison. In Lélia Blin and Yann Busnel, editors, *4th Workshop on Theoretical Aspects of Dynamic Distributed Systems, TADDS*, pages 20–25, Roma, Italy, December 17 2012. ACM.

[S-C33] Nicolas Halbwachs and Julien Henry. When the decreasing sequence fails. In Antoine Miné, editor, *19th International Static Analysis Symposium, SAS'12*, pages 198–213, Deauville, France, September 2012. LNCS 7460, Springer Verlag.

[S-C34] Julien Henry, David Monniaux, and Matthieu Moy. Succinct representations for abstract interpretation. In *Static analysis (SAS)*, 2012.

[S-C35] Julien Henry, David Monniaux, and Matthieu Moy. PAGAI: a path sensitive static analyzer. In Bertrand Jeannet, editor, *Tools for Automatic Program Analysis (TAPAS)*, 2012.

[S-C36] Karel Heurtefeux and Fabrice Valois. Is RSSI a good choice for localization in wireless sensor network? In *IEEE International Conference on Advanced Information Networking and Applications*, Fukuoka, Japan, March 2012.

[S-C37] Jack Whitham, Robert I. Davis, Neil C. Audsley, Sebastian Altmeyer, and Claire Maiza. Investigation of Scratchpad Memory for Preemptive Multitasking. In *RTSS*, 2012.

[S-C38] Anh-Dung Phan, Nikolaj Bjørner, and David Monniaux. Anatomy of alternating quantifier satisfiability (work in progress). In *10th International Workshop on Satisfiability Modulo Theories (SMT)*, 2012.

[S-C39] Karine Altisen, Stéphane Devismes, Pascal Lafourcade, and Clément Ponsonnet. Routage par marche aléatoire à listes tabous. In *Algotel*, pages 21–24, 2011.

[S-C40] Karel Heurtefeux, Florence Maraninchi, and Fabrice Valois. Areacast : une communication par zone dans les réseaux de capteurs sans fil. In *13 èmes Rencontres Francophones sur les Aspects Algorithmiques de Télécommunications (AlgoTel)*, May 2011.

[S-C41] Karine Altisen and Matthieu Moy. Causality closure for a new class of curves in real-time calculus. In *Proceedings of the 1st International Workshop on Worst-Case Traversal Time*, pages 3–10, Vienna, Autriche, 2011. ACM.

[S-C42] Borzoo Bonakdarpour, Stéphane Devismes, and Franck Petit. Snap-stabilizing committee coordination. In *IPDPS'2011, 25th IEEE International Parallel and Distributed Processing Symposium*, pages 231–242, Anchorage, USA, May 16-20 2011. IEEE.

[S-C43] Borzoo Bonakdarpour, Stéphane Devismes, and Franck Petit. Coordination de comités instantanément stabilisante. In *Algotel*, pages 87–90, 2011.

[S-C44] Nicolas Berthier, Florence Maraninchi, and Laurent Mounier. Synchronous programming of device drivers for global resource control in embedded operating systems. In *ACM SIGPLAN/SIGBED Conference on Languages, Compilers, Tools and Theory for Embedded Systems (LCTES)*, Chicago, IL, USA, April 2011.

[S-C45] Ajoy Kumar Datta, Stéphane Devismes, Maria Gradinariu Potop-Butucaru, François Kawala, and Lawrence L. Larmore. Multi-resource allocation with unknown participants. In Toshimitsu Masuzawa, editor, *PDAA'2011, 3rd International Workshop on Parallel and Distributed Algorithms and Applications*, pages 200–206, Osaka, Japan, December 2011. Conference Publishing Service. Workshop in conjunction with ICNC'2011.

[S-C46] Ajoy Kumar Datta, Stéphane Devismes, Karel Heurtefeux, Lawrence L. Larmore, and Yvan Rivierre. Algorithme auto-stabilisant construisant un ensemble k-dominant minimal borné. In *20èmes Rencontres francophones du Parallélisme*, Saint-Malo, May 2011.

[S-C47] Ajoy Kumar Datta, Stéphane Devismes, Karel Heurtefeux, Lawrence L. Larmore, and Yvan Rivierre. Self-stabilizing small k-dominating sets. In Toshimitsu Masuzawa, editor, *The Second International Conference on Networking and Computing (ICNC'11)*, pages 30–39, Osaka, Japan, December 2011. Conference Publishing Service. Best Paper Award.

[S-C48] Ajoy Kumar Datta, Stéphane Devismes, and Lawrence L. Larmore. Brief announcement: Sorting on skip chains. In Franck Petit and Vincent Villain, editors, *SSS'2011, 13th International Symposium on Stabilization, Safety, and Security of Distributed Systems*, pages 443–444, Grenoble, october 2011. LNCS.

[S-C49] Ajoy Kumar Datta, Stéphane Devismes, and Lawrence L. Larmore. Sorting on skip chains. In Toshimitsu Masuzawa, editor, *Proceedings of PDAA'2011, 3rd International Workshop on Parallel and Distributed Algorithms and Applications*, pages 193–199, Osaka, Japan, December 2011. Conference Publishing Service. Workshop in conjunction with ICNC'2011.

[S-C50] Ajoy Kumar Datta, Stéphane Devismes, Lawrence L. Larmore, and Yvan Rivierre. Self-stabilizing labeling and ranking in ordered trees. In Franck Petit and Vincent Villain, editors, *SSS'2011, 13th International Symposium on Stabilization, Safety, and Security of Distributed Systems*, pages 148–162, Grenoble, october 2011. LNCS.

[S-C51] Giovanni Funchal, Matthieu Moy, Laurent Maillet-Contoz, and Florence Maraninchi. Faithfulness considerations for virtual prototyping of systems-on-chip. In *3rd Workshop on: Rapid Simulation and Performance Evaluation: Methods and Tools (RAPIDO)*, Heraklion, Crete, Greece, January 2011.

[S-C52] Giovanni Funchal and Matthieu Moy. Modeling of time in discrete-event simulation of systems-on-chip. In *ACM/IEEE Ninth International Conference on Formal Methods and Models for Codesign MEMOCODE*, Cambridge Royaume-Uni, 07 2011.

[S-C53] Giovanni Funchal and Matthieu Moy. jTLM: an experimentation framework for the simulation of transaction-level models of systems-on-chip. In *Design, Automation and Test in Europe (DATE)*, 2011.

[S-C54] Thomas Gawlitza and David Monniaux. Improving strategies via SMT solving. In *ESOP*, 2011.

[S-C55] Karel Heurtefeux, Florence Maraninchi, and Fabrice Valois. Areacast: a cross-layer approach for a communication by area in wireless sensor networks. In *17th IEEE International Conference on networks*. IEEE, December 2011.

[S-C56] Claire Maiza and Christine Rochange. A framework for the timing analysis of dynamic branch predictors. In *Proceedings of the 19th International Conference on Real-Time and Network Systems (RTNS2011)*, 2011.

[S-C57] Sebastian Altmeyer, Robert I. Davis, and Claire Maiza. Cache related pre-emption delay aware response time analysis for fixed priority pre-emptive systems. In *Proceedings of the 32nd IEEE Real-Time Systems Symposium (RTSS)*, 2011.

[S-C58] Kevin Marquet, Matthieu Moy, and Bertrand Jeannet. Efficient Encoding of SystemC/TLM in Promela. In *DATICS-IMECS*, Hong-Kong, 03 2011.

[S-C59] David Monniaux and Martin Bodin. Modular abstractions of reactive nodes using disjunctive invariants. In *Programming Languages and Systems (APLAS)*, 2011.

[S-C60] David Monniaux and Pierre Corbineau. On the generation of Positivstellensatz witnesses in degenerate cases. In Marko Van Eekelen, Herman Geuvers, Julien Schmaltz, and Freek Wiedijk, editors, *Interactive Theorem Proving (ITP)*, volume 6898, pages 249–264, August 2011.

[S-C61] David Monniaux and Laure Gonnord. Using bounded model checking to focus fixpoint iterations. In *Static analysis (SAS)*, 2011.

[S-C62] David Monniaux and Julien Le Guen. Stratified static analysis based on variable dependencies. In *Third International Workshop on Numerical and Symbolic Abstract Domains*, 2011.

[S-C63] Matthieu Moy. Efficient and Playful Tools to Teach Unix to New Students. In *16th Annual Conference on Innovation and Technology in Computer Science Education ITiCSE*, Darmstadt Allemagne, 06 2011.

[S-C64] Karine Altisen and Matthieu Moy. ac2lus: Bringing SMT-solving and abstract interpretation techniques to real-time calculus through the synchronous language Lustre. In *22nd Euromicro Conference on Real-Time Systems (ECRTS)*, Brussels, Belgium, Jully 2010.

[S-C65] Samuel Bernard, Stéphane Devismes, Maria Gradinariu Potop-Butucaru, Katy Paroux, and Sébastien Tixeuil. Probabilistic self-stabilizing vertex coloring in unidirectional anonymous networks. In *ICDCN'2010, 11th International Conference on Distributed Computing and Networking*, pages 167–177, Kolkata, India, January 2010.

[S-C66] Karine Altisen and Matthieu Moy. Arrival curves for real-time calculus: the causality problem and its solutions. In Javier Esparza and R. Majumdar, editors, *TACAS*, pages 358–372, March 2010.

[S-C67] Fabienne Carrier, Stéphane Devismes, Franck Petit, and Yvan Rivierre. Rendez-vous d'agents amnésiques. In *12èmes Rencontres Francophones sur les Aspects Algorithmiques de Télécommunications (Algotel 2010)*, pages 35–38, 2010.

[S-C68] Valentin Perrelle and Nicolas Halbwachs. An analysis of permutations in arrays. In Gilles Barthe and Manuel Hermenegildo, editors, *11th International Conference on Verification, Model-checking, and Abstract Interpretation, VMCAI 2010*, pages 279–294, Madrid, Spain, January 2010. Springer.

[S-C69] Stéphane Devismes. Optimal exploration of small rings. In Franck Petit, editor, *WRAS'2010, Third International ACM SIGOPS/SIGACT Workshop on Reliability, Availability, and Security*, pages 9:1–9:6, Zurich, Switzerland, July 2010. ACM.

[S-C70] Carole Delporte-Gallet, Stéphane Devismes, and Hugues Fauconnier. Approximation of δ-timeliness. In Shlomi Dolev, editor, *12th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2010)*, pages 435–451, New York City, USA, September 2010. LNCS.

[S-C71] Stéphane Devismes, Carole Delporte-Gallet, Hugues Fauconnier, and Mikel Larrea. Algorithms for extracting timeliness graphs. In Boaz Patt-Shamir and Tinaz Ekim, editors, *17th International Colloquium on Structural Information and Communication Complexity (SIROCCO 2010)*, pages 127–141, Sirince, Turkey, june 7-11 2010. Springer.

[S-C72] Stéphane Devismes, Hirotsugu Kakugawa, Sayaka Kamei, and Sébastien Tixeuil. A self-stabilizing 3-approximation for the maximum leaf spanning tree problem in arbitrary networks. In My T. Thai and Sartaj Sahni, editors, *COCOON 2010, The 16th Annual International Computing and Combinatorics Conference*, volume 6196 of *Lecture Notes in Computer Science*, pages 80–89, Nha Trang, Vietnam, July 2010. Springer.

[S-C73] Stéphane Devismes, Toshimitsu Masuzawa, and Sébastien Tixeuil. Communications efficaces et auto-stabilisation. In *12èmes Rencontres Francophones sur les Aspects Algorithmiques de Télécommunications (Algotel 2010)*, 2010.

[S-C74] Albert Benveniste, Anne Bouillard, and Paul Caspi. A unifying view of loosely time-triggered architectures. In *International Conference on Embedded Software International Conference on Embedded Software*, Scottsdale, USA, Oct 2010.

[S-C75] David Monniaux. Quantifier elimination by lazy model enumeration. In Byron Cook, Paul Jackson, and Tayssir Touili, editors, *Computer-aided verification (CAV)*. Springer, July 2010.

[S-C76] Kevin Marquet and Matthieu Moy. PinaVM: a SystemC front-end based on an executable intermediate representation. In *International Conference on Embedded Software*, page 79, Scottsdale, USA, 10 2010. SD B.4.4, I.6.4, D.2.4 OpenTLM (projet Minalogic).

[S-C77] Kevin Marquet, Matthieu Moy, and Bageshri Karkare. A theoretical and experimental review of SystemC front-ends. In *Forum for Design Languages (FDL)*, 2010. B.1.4, C.3 OpenTLM (Projet Minalogic).

[S-C78] Karine Altisen, Yanhong Liu, and Matthieu Moy. Performance evaluation of components using a granularity-based interface between real-time calculus and timed automata. In *Eighth Workshop on Quantitative Aspects of Programming Languages (QAPL)*, Paphos, Cyprus, March 2010.

[S-C79] Tayeb Bouhadiba and Florence Maraninchi. Contract-based coordination of hardware components for the development of embedded software. In *COORDINATION'09, the 11th international conference on Coordination Models and Languages*, Lisbon, Portugal, June 2009.

[S-C80] Tayeb Bouhadiba, Florence Maraninchi, and Giovanni Funchal. Formal and executable contracts for transaction-level modeling in systemc. In *ACM International Conference on Embedded Sofware (EMSOFT 09)*, Grenoble, France, October 2009.

[S-C81] Mouaiad Alras, Paul Caspi, Alain Girault, and Pascal Raymond. Model-based design of embeded control systems with a synchronous intermediate model. In *6th IEEE International Conference on Embedded Systems and Software (ICESS-09)*, Hangzhou, China, May 2009.

[S-C82] Samuel Bernard, Stéphane Devismes, Katy Paroux, Maria Gradinariu Potop-Butucaru, and Sébastien Tixeuil. Sur le coloriage auto-stabilisant dans les réseaux unidirectionnels anonymes. In Augustin Chaintreau and Clemence Magnien, editors, *AlgoTel'09*, Carry-Le-Rouet France, 2009.

[S-C83] Samuel Bernard, Stéphane Devismes, Maria Gradinariu Potop-Butucaru, and Sébastien Tixeuil. Optimal deterministic self-stabilizing vertex coloring in unidirectional anonymous networks. In *IPDPS '09: Proceedings of the 2009 IEEE International Symposium on Parallel&Distributed Processing*, pages 1–8, Roma, Italia, 2009. IEEE Computer Society.

[S-C84] Loïc Besnard, Thierry Gautier, Matthieu Moy, Jean-Pierre Talpin, Kenneth Johnson, and Florence Maraninchi. Automatic translation of C/C++ parallel code into synchronous formalism using an SSA intermediate form. In *Ninth International Workshop on Automated Verification of Critical Systems (AVOCS'09)*. Electronic Communications of the EASST, September 2009.

[S-C85] Unmesh D. Bordoloi, Huynh Phung Huynh, Samarjit Chakraborty, and Tulika Mitra. Evaluating design trade-offs in customizable processors. In *46th Annual ACM IEEE Design Automation Conference*, San Francisco, U.S.A, 07 2009.

[S-C86] Michael Glaß, Martin Lukasiewycz, Jürgen Teich, Unmesh D. Bordoloi, and Samarjit Chakraborty. Designing heterogeneous ecu networks via compact architecture encoding and hybrid timing analysis. In *46th Annual ACM IEEE Design Automation Conference*, San Francisco, U.S.A, 07 2009.

[S-C87] Dip Goswami, Pradeep Seshadri, Unmesh D. Bordoloi, and Samarjit Chakraborty. A decomsys based tool-chain for analyzing flexray based automotive control applications. In *IEEE Conference on Automation Science and Engineering -(CASE)*, Bangalore , India, 2009. IEEE.

[S-C88] Fabienne Carrier, Stéphane Devismes, Franck Petit, and Yvan Rivierre. Space-optimal deterministic rendezvous. In *WRAS'09, Second International Workshop on Reliability, Availability, and Security (associated with PDCAT'09)*, pages 342–347, Hiroshima, Japan, December 2009. IEEE Computer Society.

[S-C89] Carole Delporte-Gallet, Stéphane Devismes, Hugues Fauconnier, Franck Petit, and Sam Toueg. Quand le consensus est plus simple que la diffusion fiable. In Augustin Chaintreau and Clemence Magnien, editors, *AlgoTel'09*, pages 101–104, Carry-Le-Rouet France, 2009.

[S-C90] Ajoy Kumar Datta, Stéphane Devismes, Florian Horn, and Lawrence L. Larmore. Self-stabilizing k-out-of-l exclusion on tree networks. In *IPDPS'09, International Conference on Parallel and Distributed Processing Symposium*, pages 1–8, Roma, Italia, 2009. IEEE Computer Society.

[S-C91] Ajoy Kumar Datta, Stéphane Devismes, and Lawrence L. Larmore. A self-stabilizing o(n)-round k-clustering algorithm. In *SRDS'09, 28th International Symposium on Reliable Distributed Systems*, pages 147–155, Niagara Falls, New York, U.S.A., September 2009. IEEE Computer Society.

[S-C92] Sylvie Delaët, Stéphane Devismes, Mikhail Nesterenko, and Sébastien Tixeuil. Snap-stabilization in message-passing systems. In *ICDCN, 10th International Conference on Distributed Computing and Networking*, volume 5408 of *Lecture Notes in Computer Science*, pages 281–286, Hyderabad, India, january 2009. Springer.

[S-C93] Sylvie Delaët, Stéphane Devismes, Mikhail Nesterenko, and Sébastien Tixeuil. Stabilisation instantanée dans les systèmes à passage de messages. In Augustin Chaintreau and Clemence Magnien, editors, *AlgoTel'09*, pages 81–84, Carry-Le-Rouet France, 2009.

[S-C94] Stéphane Devismes, Toshimitsu Masuzawa, and Sébastien Tixeuil. Communication efficiency in self-stabilizing silent protocols. In *ICDCS'09, International Conference on Distributed Computing Systems*, pages 474–481, Montréal, Canada, June 2009. IEEE Computer Society.

[S-C95] Stéphane Devismes, Franck Petit, and Sébastien Tixeuil. Optimal probabilistic ring exploration by semi-synchronous oblivious robots. In Shay Kutten and Janez Zerovnik, editors, *Structural Information and Communication Complexity, 16th International Colloquium, SIROCCO 2009*, volume 5869 of *Lecture Notes in Computer Science*, pages 195–208, Piran, Slovenia, May 25-27 2009. Springer. Revised Selected Papers.

[S-C96] Stéphane Devismes, Franck Petit, and Sébastien Tixeuil. Exploration optimale probabiliste d'un anneau par des robots semi-synchrones et amnésiques. In Augustin Chaintreau and Clemence Magnien, editors, *AlgoTel'09*, pages 109–112, Carry-Le-Rouet France, 2009.

[S-C97] Erwan Jahier, Nicolas Halbwachs, and Pascal Raymond. Synchronous modeling and validation of priority inheritance schedulers. In *Fundamental Approaches to Software Engineering, FASE'09*, York, U.K., March 2009.

[S-C98] Marc Pouzet and Pascal Raymond. Modular static scheduling of synchronous data-flow networks – an efficient symbolic representation. In *International Conference on Embedded Software (EMSOFT'09)*, Grenoble, France, October 2009.

[S-C99] Paul Caspi, Albert Benveniste, Roberto Lublinerman, and Stavros Tripakis. Actors without directors: A Kahnian view of heterogeneous systems. In *Hybrid Systems Computation and Control, HSCC09*, volume 5469 of *Lecture Notes in Computer Science*, 2009.

[S-C100] David Monniaux. On using floating-point computations to help an exact linear arithmetic decision procedure. In *Computer-aided verification (CAV)*, volume 5643 of *Lecture Notes in Computer Science*, pages 570–583. Springer Verlag, 2009.

[S-C101] David Monniaux. Automatic modular abstractions for linear constraints. In *POPL (Principles of programming languages)*. ACM, 2009.

[S-C102] Paul Caspi, Jean-louis Colaço, Léonard Gérard, Marc Pouzet, and Pascal Raymond. Synchronous objects with scheduling policies, introducing safe shared memory in Lustre. In *ACM SIGPLAN/SIGBED 2009 Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES 2009)*, Dublin, Ireland, june 2009.

D.2.1.3 Books, Book Chapters and edited proceedings

[S-B1] Luciano Bononi, Ajoy Kumar Datta, Stéphane Devismes, and Archan Misra, editors. *Distributed Computing and Networking - 13th International Conference, ICDCN 2012, Hong Kong, China, January 3-6, 2012. Proceedings*, volume 7129 of *Lecture Notes in Computer Science*. Springer, 2012.

[S-B2] Stéphane Devismes, Pascal Lafourcade, and Michel Levy. *Informatique théorique : Logique et démonstration automatique, Introduction à la logique propositionnelle et à la logique du premier ordre*. Ellipses, Technosup, 2012.

[S-B3] Florence Maraninchi and John Regehr, editors. *Embedded Software, EMSOFT'12*. ACM, 2012.

[S-B4] Stéphane Devismes. *Quelques Contributions à la Stabilisation Instantanée*. Editions universitaires européennes, 2010.

[S-B5] Samarjit Chakraborty and Nicolas Halbwachs, editors. *Embedded Software, EMSOFT'09*. ACM, 2009.

D.2.1.4 PhD Theses and habilitations

[S-P1] Matthieu Moy. *High-level Models for Embedded Systems*. Habilitation à diriger des recherches (HDR), Univ. Grenoble Alpes, VERIMAG, F-38000 Grenoble, France, Verimag, 2014.

[S-P2] Valentin Perrelle. *Analyse statique de programmes manipulant des tableaux*. Thesis, Grenoble University, march 2013.

[S-P3] Yvan Rivierre. *Self-Stabilizing Algorithms for Constructing Distributed Spanning Structures*. PhD thesis, Université de Grenoble, december 2013.

[S-P4] Nicolas Berthier. *Programmation synchrone de pilotes de périphériques pour un contrôle global de ressources dans les systèmes embarqués*. PhD thesis, Université de Grenoble, March 2012.

[S-P5] Giovanni Funchal. *Contributions to the Transaction-Level Modeling of Systems-on-a-Chip*. PhD thesis, Grenoble Institute of Technology, France, May 2011.

[S-P6] Mathias Péron. *Contributions à l'analyse statique de programmes manipulant des tableaux*. PhD thesis, Université de Grenoble, septembre 2010.

[S-P7] Tayeb Bouhadiba. *42, A Component-Based Approach to Virtual Prototyping of Heterogeneous Embedded Systems*. PhD thesis, University of Grenoble, September 2010.

[S-P8] David Monniaux. *Analyse statique : de la théorie à la pratique*. Habilitation to direct research, Université Joseph Fourier, Grenoble, France, June 2009.

D.2.1.5 Other visible publications

[S-O1] Ajoy Kumar Datta and Stéphane Devismes. Special issue of theoretical computer science, 2013.

[S-O2] Claire Maiza and Christine Rochange. A framework for the timing analysis of dynamic branch predictors. Technical report, IRIT, 2011.

[S-O3] Sebastian Altmeyer, Robert I. Davis, and Claire Maiza. Pre-emption cost aware response time analysis for fixed priority pre-emptive systems. Technical report, University of York, Department of Computer Science, May 2011.

[S-O4] Giovanni Funchal, Matthieu Moy, Florence Maraninchi, and Laurent Maillet-Contoz. Faithfulness considerations for virtual prototyping of systems-on-chip. Technical report, VERIMAG, 2010.

[S-O5] Florence Maraninchi and Tayeb Bouhadiba. 42: Programmable models of computation for the component-based virtual prototyping of heterogeneous embedded systems. Technical report, Verimag, January 2009.

[S-O6] Tayeb Bouhadiba, Florence Maraninchi, and Giovanni Funchal. Formal and executable contracts for transaction-level modeling in systemc - full version. Technical report, Verimag, May 2009.

[S-O7] David Monniaux. Introduction à la calculabilité. *Quadrature*, 86:17–28, 2012.

D.2.2 Synchrone team: Software

PinaVM A SystemC front-end based on the LLVM compiler infrastructure
Authors: Kevin Marquet, Matthieu Moy, Si-Mohamed Lamraoui, Guillaume Sergent
Home page: https://forge.imag.fr/plugins/mediawiki/wiki/pinavm/index.php/Main_Page
License: Free Software (GNU LGPL)
Not distributed outside Verimag.

Unix-training A set of tools to teach Unix efficiently
Authors: Matthieu Moy
Home page: http://www-verimag.imag.fr/~moy/?Unix-training-a-set-of-tools-to
License: Free Software (GNU LGPL)

sc-during Tasks with duration for parallel programming with SystemC
Authors: Matthieu Moy and Swadhin Mangaraj
Home page: http://www-verimag.imag.fr/~moy/?sc-during-Parallel-Programming-on
License: Free Software (GNU LGPL)

PAGAI Path Analysis for invariant Generation by Abstract Interpretation
Authors: Julien Henry, David Monniaux and Matthieu Moy
Home page: http://pagai.forge.imag.fr/

ac2lus A bridge between Real Time Calculus (RTC) and Abstract Interpretation and Model-Checking using the Lustre language
Authors: Matthieu Moy and Karine Altisen
Not distributed outside Verimag.

LIBTLMPWT Fast and Modular Transaction-Level-Modeling and Simulation of Power and Temperature
Authors: Claude Helmstetter and Matthieu Moy
Home page: http://www-verimag.imag.fr/~moy/?LIBTLMPWT-Model-Power-Consumption

jTLM TLM Simulator for Systems-on-a-Chip written in Java (alternative to SystemC)
Authors: Giovanni Funchal and Matthieu Moy
Not distributed outside Verimag.

Lutin Lutin is a language to program stochastic reactive systems.
Authors: Erwan Jahier, Pascal Raymond
Home page: http://www-verimag.imag.fr/Lutin.html

Lustre V6 .
Authors: Erwan Jahier, Pascal Raymond
Home page: http://www-verimag.imag.fr/Lustre-V6.html

Lurette Lurette is an Automatic Test Generator for Reactive Programs.
Authors: Erwan Jahier, Pascal Raymond
Home page: http://www-verimag.imag.fr/lurette.html

RDBG A Reactive programs DeBuGger
Authors: Erwan Jahier
Home page: http://rdbg.forge.imag.fr/
License: Licence of software, e.g. Free Software (GNU LGPL)

Mjollnir A tool for quantifier elimination in the linear theory of the reals, with several approaches
Authors: David Monniaux
Home page: http://www-verimag.imag.fr/~monniaux/download/
License: CeCILL

D.2.3 Synchrone team: Scientific influence

- Grants (see details in Annex E): STATOR, OpenES, CIFRE Orange (Lemke), DACRAW, CESYMPA, WSEPT, VERASCO, HELP, ARESA2, TERRA, COMON, ASOPT, SYNCHRONICS, CIFREs ST (LeGuen, Funchal), ARESA, FOTOVP, OpenTLM.
- Academic collaborations: Apart from the collaborations with the academic partners of the projects, we maintain collaborations, and publish papers, with the following persons:

  - On WCET, caches, and scheduling: Rob Davis (University of York, UK), Sebastian Altmeyer (University of Amsterdam), Jan Reineke (Saarland University, Germany)
  - On synchronous languages: Marc Pouzet (ENS Paris), A. Benveniste (IRISA, Rennes)
  - On distributed algorithms: Ajoy K. Datta and Lawrence L. Larmore (Univ. Nevada Las Vegas), Franck Petit and Sébastien Tixeuil (LIP6, Paris VI)
- Events organisation
  - Local Organizer of the COST action TACLe working group meeting in Paris, July 8th, 2013
  - Local Organizer of SSS'2011 (13th International Symposium on Stabilization, Safety, and Security of Distributed Systems). Grenoble, France. October 10-12, 2011
  - Local Organizer of the 2010 French meeting on compilation (Aussois)
- Awards
  - N. Halbwachs is a member of the Academia Europaea since 2010
  - Best Student Paper Award for Yvan Rivierre at SSS'2013 [**S-C13**]
  - Best Paper Award at ICNC'2011 [**S-C47**]
- Invited conferences
  - C. Maïza was Distinguished International Speaker at the University of York (Feb. 12, 2014) for a talk at the Comp. Sci. Department
  - C. Maïza was invited for a talk at the University of Poitiers, LIAS, Jan 9, 2014
  - D. Monniaux was invited speaker at the 2010 International Mini-Conference on Information Electronics Systems, Sendai, Japan[1]
  - D. Monniaux was invited speaker at MACIS 2013, Nanning China;[2]
  - D. Monniaux was invited tutorial speaker at CAV 2014, Vienna;
  - D. Monniaux taught at the 2011 First summer school on Formal Techniques, Atherton, California,[3]
  - D. Monniaux taught at the 2012 VTSA summer school, Saarbrücken[4]
  - M. Moy, together with Laurent-Maillet Contoz from STMicroelectronics, presented the work done in the STMicroelectronics/Verimag collaboration at College de France in January 2014[5].
  - N. Halbwachs was keynote speaker at the international conference LCTES 2012, Beijing, China, June 2012 [6]
  - F. Maraninchi was invited speaker at the Intel&Technion Symposium, Haifa, Israël, september 2011 [7]
  - F. Maraninchi was invited speaker at the "Grand séminaire" of the LINA Laboratory, Nantes, april 2011 [8]
  - N. Halbwachs was invited speaker at the workshop MSR 2011, Lille, November 2011 [9]
  - F. Maraninchi was invited speaker at the Dagstuhl seminar "Design and Validation of Concurrent Systems", september 2009[10]
  - F. Maraninchi was invited speaker at the Workshop "Simulation Based Development of Certified Embedded Systems", organized by the franco-chinese INRIA-FORMES group, Japan, october 2009
  - F. Maraninchi was invited speaker at the FETCH (Ecole d'hiver Francophone sur les Technologies de Conception des systèmes embarqués Hétérogènes) doctoral school, Chexbres, Switzerland, January, 2009
- Editorial activities
  - F. Maraninchi is a member of the editorial board, Leibniz Transactions on Embedded Systems [11].
  - N. Halbwachs and F. Maraninchi have been co-chairs of the ACM EMSOFT conference [**S-B5**, **S-B3**],

[1] http://www.ecei.tohoku.ac.jp/gcoe/en/confe/2010.html
[2] http://www.mpi-inf.mpg.de/conference/macis2013/
[3] http://fm.csl.sri.com/SSFT11/
[4] http://www.mpi-inf.mpg.de/VTSA12/
[5] http://www.college-de-france.fr/site/gerard-berry/seminar-2014-01-29-17h30.htm
[6] http://lctes12.cs.purdue.edu/
[7] http://workshop.ee.technion.ac.il/index.php?EVT_SysID=158
[8] http://www.lina.univ-nantes.fr/spip.php?page=seminaires&id_rubrique=40&annee=2011
[9] http://www.lifl.fr/msr11/
[10] http://www.college-de-france.fr/site/gerard-berry/seminar-2014-01-29-17h30.htm
[11] http://ojs.dagstuhl.de/index.php/lites

respectively in 2009 and 2012.
- F. Maraninchi has been co-chair of the topic E2 in track E ("Compilers and Software Synthesis for Embedded Systems") of DATE'14
- Cl. Maïza has been co-chair of RTNS'14 (22nd International Conference on Real-Time Networks and Systems), and chair of WCET 2013 (13th International Workshop on Worst-Case Execution Time Analysis)
- N. Halbwachs is editor of the journal FMSD (Formal Methods in System Design, Springer).
- Stéphane Devismes has been guest editor for a special issue of Theoretical Computer Science [**S-O1**]
- Stéphane Devismes has been vice-program chair of the distributed computing track of ICDCN 2012 (13th International Conference on Distributed Computing and Networking).

- Evaluation activities
  - The members of the team participate in the PCs of the following conferences: WMCIS workshop, WCET'14, RTAS'14, RETIMICS workshop'13, RTNS'13, ECRTS'14-13-12, CC'14 (23rd International Conference on Compiler Construction), ... EMSOFT'14, LCTES'14, LCTES'13, DATE'13, DAC'12, DATE'12, LCTES'12, LCTES'11, EMSOFT'09, LCTES'09 WCTT'11-12, DATICS-NESEA'11, DATICS-IMECS'12 TACAS 2009, EMSOFT 2010-11-13-14, ESOP 2010-11, SAS 2013 SSS'14-13-11-10-09, CANDAR'14-13, APDCM'14-13, ICNC'12, ICDCN'12, LAFT'11, Algotel'13-12-11-10, EDCC'10, WRAS'09 CAV 2010, PEPM 2010, ESOP 2012, SAS 2012, VSTTE 2013, VMCAI 2014
  - The members of the team are members of the steering committees of the following conferences: ACM EMSOFT, the 1st International Workshop on Mixed Criticality Systems, ...
  - The members of the team have been reviewers of PhD thesis 16 times, reviewers of HDR 3 times, and participants in PhD or HDR committees 22 times.
- Administrative activities
  - F. Maraninchi is co-responsible of the scientific committee for the "Pervasive Computing Systems" topic of the labex Persyval-Lab[12], since 2012.
  - Fabienne Carrier has been assistant director of the Department of Science and Technology Licence from 2007 to 2011. She participated in the definition of tests on required knowledge, for students entering the first year of university programs. The experience began in 2008 and is continuing. The goal is to help students be aware of their future difficulties; after the tests, remedial teaching is proposed. Results and future evolutions have been published in [**D-C43**].
  - N. Halbwachs belongs to the Steering Committee of EMSIG (Embedded Systems Special Interest Group[13]) since 2013
  - F. Maraninchi was a member of the national committee for the PES (prime d'excellence scientifique), june 2013
  - F. Maraninchi is a member of the board of the doctoral school MSTII (mathematics, information sciences and technologies, informatics) which gathers 400 PhD students, since 2012
  - F. Maraninchi is the director of international relations at Ensimag, since 2008
  - F. Maraninchi has been an elected member of the Grenoble INP CEVU (Conseil des Etudes et de la Vie Universitaire) from 2007 to 2011
  - F. Maraninchi is an elected member of the "conseil de l'Ensimag" since 2012
  - M. Moy was a member of the "CPVE" (pedagogy and students life commission) at Ensimag from 2009 to 2012.
  - The members of the team have been presidents of selection committees 4 times, and participated in selection committees 18 times; N. Halbwachs has been a member of the INRIA Rocquencourt recruiting committee for junior researchers (2013); M. Moy has been a member of the recruting committee for a CNRS engineer.
  - F. Maraninchi was a member of the Grenoble INP HDR committee from 2001 to 2013; D. Monniaux is now a member of the joint UJF and Grenoble INP HDR Committee since 2013.
  - AERES and Labs evaluations: N. Halbwachs took part in the AERES evaluation commiittees of IRISA (2010), Inria-Bretagne (2011), LIPN (2012), and was the president of the AERES committees

[12] persyval-lab.org/research/action/pcs
[13] http://www.emsig.net/

of CRISTAL (=LIFL+LAGIS, 2013) and IRCICA (2014), and of the visiting committee of LIAMA (Beijing, 2012). F. Maraninchi participated in the AERES evaluation committee of the I3S laboratory, Nice, January 2011
  - ANR: N. Halbwachs participated in the scientific committee of "Blanc" and "Jeunes chercheurs" and "Blanc international" (2010-2013); he was member of the "Comité Scientifique Sectoriel STIC" (2010-12) and is presently in the Scientific Steering Committee of the "défi 7, Société de l'information et de la communication" (2013-14).

D.2.4 Synchrone team: Interaction with the economic, social and cultural environment

- Competitiveness poles: Since 2007, F. Maraninchi is one of the two academic members of the organisation and evaluation committees of the software cluster of the competitiveness pole Minalogic[14].
- Industrial contracts
  - CIFRE contracts: (i) 2007-2010, PhD G. Funchal, with STMicroelectronics Grenoble (page 158); (ii) 2013-2016, PhD L. Lemke, with Orange Labs (page 160).
  - Collaborative projects including industrial partners (see details in Annex E): STATOR, OpenES, W-SEPT, VERASCO, HELP, ARESA2, COMON, ASOPT, ARESA, OpenTLM
- Startup creation: Argosim, see section 2.1.2.3.
- Consulting : In 2012, N. Halbwachs participated in two expertises for the company Astrium.

D.3 DCS team: production

D.3.1 DCS team: Publications, by Categories

D.3.1.1 International Journals

[D-J1] Susanne Graf and Sophie Quinton. Distributed implementation of constrained systems based on knowledge. *Journal on Software and Systems Modeling, SoSym*, 2014.

[D-J2] Ayoub Nouri, Saddek Bensalem, Marius Bozga, Benoît Delahaye, Cyril Jegourel, and Axel Legay. Statistical model-checking QoS properties of systems with SBIP. *STTT*, 2014.

[D-J3] Karine Altisen, Stéphane Devismes, Antoine Gerbaud, and Pascal Lafourcade. Comparison of mean hitting times for a degree-biased random walk. *Discrete Applied Mathematics*, 170:104–109, 2014.

[D-J4] Saddek Bensalem, Marius Bozga, Axel Legay, Thanh-Hung Nguyen, Joseph Sifakis, and Rongjie Yan. Component-based verification using incremental design and invariants. *Software and Systems Modeling, SoSyM*, April 2014.

[D-J5] Roderick Bloem, Krishnendu Chatterjee, Karin Greimel, Thomas A. Henzinger, Georg Hofferek, Barbara Jobstmann, Bettina Könighofer, and Robert Könighofer. Synthesizing robust systems. *Acta Inf.*, 51(3):193–220, 2014.

[D-J6] Josselin Feist, Laurent Mounier, and Marie-Laure Potet. Statically detecting use-after-free on binary code. *Journal of Computer Virology and Hacking Techniques*, online article, January 2014.

[D-J7] Radu Iosif and Adam Rogalewicz. Automata-based termination proofs. *Computing and Informatics*, 32(4):739–775, 2013.

[D-J8] Tesnim Abdellatif, Jacques Combaz, and Joseph Sifakis. Rigorous implementation of real-time systems - from theory to application. *Mathematical Structures in Computer Science*, 23(4):882–914, 2013.

[D-J9] Saddek Bensalem, Axel Legay, and Marius Bozga. Rigorous embedded design: challenges and perspectives. *STTT*, 15(3):149–154, 2013.

[D-J10] Ylies Falcone, Mohamad Jaber, Thanh-Hung Nguyen, Marius Bozga, and Saddek Bensalem. Runtime verification of component-based systems in the BIP framework with formally-proved sound and complete instrumentation. *Software and Systems Modeling, SoSyM*, April 2013.

[14] www.minalogic.org

[D-J11] Nicolas Berthier, Florence Maraninchi, and Laurent Mounier. Synchronous programming of device drivers for global resource control in embedded operating systems. *ACM Transactions on Embedded Computing Systems (TECS)*, 12, 2013. Selected papers from LCTES'11.

[D-J12] Jan-Olaf Blech and Michael Périn. Generating invariant-based certificates for embedded systems. *ACM Transactions on Embedded Computing Systems (TECS)*, 11(2):34, 2012.

[D-J13] Borzoo Bonakdarpour, Marius Bozga, Mohamad Jaber, Jean Quilbeuf, and Joseph Sifakis. A framework for automated distributed implementation of component-based models. *Distributed Computing*, 25(5):383–409, 2012.

[D-J14] Roderick Bloem, Barbara Jobstmann, Nir Piterman, Amir Pnueli, and Yaniv Sa'ar. Synthesis of reactive(1) designs. *J. Comput. Syst. Sci.*, 78(3):911–938, 2012.

[D-J15] Barbara Jobstmann, Stefan Staber, Andreas Griesmayer, and Roderick Bloem. Finding and fixing faults. *J. Comput. Syst. Sci.*, 78(2):441–460, 2012.

[D-J16] Tesnim Abdellatif, Saddek Bensalem, Jacques Combaz, Lavindra de Silva, and Felix Ingrand. Rigorous design of robot software: A formal component-based approach. *Robotics and Autonomous Systems*, 60(12):1563–1578, 2012.

[D-J17] Ananda Basu, Saddek Bensalem, Marius Bozga, Benoît Delahaye, and Axel Legay. Statistical abstraction and model-checking of large heterogeneous systems. *STTT*, 14(1):53–72, 2012.

[D-J18] Lilia Sfaxi, Takoua Abdellatif, Yassine Lakhnech, and Riadh Robbana. Sécuriser les systèmes distribués à base de composants par contrôle de flux d'information. *Technique et Science Informatiques*, 31(2):245–279, 2012.

[D-J19] Borzoo Bonakdarpour, Marius Bozga, and Jean Quilbeuf. Model-based implementation of distributed systems with priorities. *Design Automation for Embedded Systems*, July 2012.

[D-J20] Sifakis Emmanuel and Mounier Laurent. Politiques de gestion de protections pour l'implémentation de sections critiques. *Techniques et Sciences Informatiques*, 31(8):1153–1181, 2012.

[D-J21] Ylies Falcone, Jean-Claude Fernandez, Thierry Jéron, Hervé Marchand, and Laurent Mounier. More testable properties. *STTT*, 14(4):407–437, 2012.

[D-J22] Susanne Graf, Doron Peled, and Sophie Quinton. Achieving distributed control through model checking. *Formal Methods in System Design*, 40(2):263–281, 2012.

[D-J23] Ananda Basu, Saddek Bensalem, Doron Peled, and Joseph Sifakis. Priority scheduling of distributed systems based on model checking. *Formal Methods in System Design*, 39(3):229–245, 2011.

[D-J24] Imene Ben Hafaiedh, Susanne Graf, and Sophie Quinton. Building distributed controllers for systems with priorities. *J. Log. Algebr. Program.*, 80(3):194–218, 2011.

[D-J25] Daniel Le Métayer, Manuel Maarek, Eduardo Mazza, Marie-Laure Potet, Stéphane Frénot, Valérie Viet Triem Tong, Nicolas Craipeau, and Ronan Hardouin. Liability issues in software engineering: the use of formal methods to reduce legal uncertainties. *Commun. ACM*, 54(4):99–106, 2011.

[D-J26] Joseph Sifakis. A vision for computer science - the system perspective. *Central Europ. J. Computer Science*, 1(1):108–116, 2011.

[D-J27] Ahmed Bouajjani, Marius Bozga, Peter Habermehl, Radu Iosif, Pierre Moro, and Tomás Vojnar. Programs with lists are counter automata. *Formal Methods in System Design*, 38(2):158–192, 2011.

[D-J28] Thomas A. Henzinger, Barbara Jobstmann, and Verena Wolf. Formalisms for specifying markovian population models. *Int. J. Found. Comput. Sci.*, 22(4):823–841, 2011.

[D-J29] Judicaël Courant, Marion Daubignard, Cristian Ene, Pascal Lafourcade, and Yassine Lakhnech. Automated proofs for asymmetric encryption. *J. Autom. Reasoning*, 46(3):261–291, 2011.

[D-J30] Ananda Basu, Saddek Bensalem, Marius Bozga, Jacques Combaz, Mohamad Jaber, Thanh-Hung Nguyen, and Joseph Sifakis. Rigorous component-based system design using the BIP framework. *IEEE Software*, 28(3):41–48, 2011.

[D-J31] Ylies Falcone, Jean-Claude Fernandez, and Laurent Mounier. What can you verify and enforce at runtime ? *Software Tool in Tecnology Transfer (STTT)*, 14(3), 2012.

[D-J32] Ylies Falcone, Jean-Claude Fernandez, Laurent Mounier, and Jean-Luc Richier. Runtime enforcement monitors: composition, synthesis, and enforcement abilities. *Formal Methods in System Design*, 2011.

[D-J33] Saddek Bensalem, Marius Bozga, Thanh-Hung Nguyen, and Joseph Sifakis. Compositional verification for component-based systems and application. *IET Software*, 4(3):181–193, June 2010.

[D-J34] Peter Habermehl, Radu Iosif, and Tomás Vojnar. Automata-based verification of programs with tree updates. *Acta Inf.*, 47(1):1–31, 2010.

[D-J35] Simon Bliudze and Joseph Sifakis. Causal semantics for the algebra of connectors. *Formal Methods in System Design*, 36(2):167–194, 2010.

[D-J36] Randal E. Bryant, Orna Grumberg, Joseph Sifakis, and Moshe Y. Vardi. 2009 CAV award announcement. *Formal Methods in System Design*, 36(3):195–197, 2010.

[D-J37] Rahul Agarwal, Saddek Bensalem, Eitan Farchi, Klaus Havelund, Yarden Nir-Buchbinder, Scott D. Stoller, Shmuel Ur, and Liqiang Wang. Detection of deadlock potentials in multithreaded programs. *IBM Journal of Research and Development*, 54(5):3, 2010.

[D-J38] Marius Bozga, Radu Iosif, and Swann Perarnau. Quantitative separation logic and programs with lists. *J. Autom. Reasoning*, 45(2):131–156, 2010.

[D-J39] Marius Bozga, Mohamad Jaber, and Joseph Sifakis. Source-to-source architecture transformation for performance optimization in BIP. *IEEE Trans. Industrial Informatics*, 6(4):708–718, 2010.

[D-J40] Takoua Abdellatif, Lilia Sfaxi, and Yassine Lakhnech. Contrôle de flux d'information des systèmes distribués à base de composants. *NOTERE IEEE*, 2010.

[D-J41] Saddek Bensalem, Matthieu Gallien, Felix Ingrand, Imen Kahloul, and Thanh-Hung Nguyen. Toward a more dependable software architecture for autonomous robots. *Special issue on Software Engineering for Robotics of the IEEE Robotics and Automation Magazine*, 16(1):67–77, March 2009.

[D-J42] Marius Bozga, Radu Iosif, and Yassine Lakhnech. Flat parametric counter automata. *Fundam. Inform.*, 91(2):275–303, 2009.

[D-J43] Edmund M. Clarke, Allen Emerson, and Joseph Sifakis. Model checking: algorithmic verification and debugging. *Commun. ACM*, 52(11):74–84, 2009.

[D-J44] Manuel Garnacho and Michael Périn. Convincing proofs for program certification. *Electronic Notes in Theoretical Computer Science*, 238(4):41–56, 2009.

[D-J45] Charles André, Mariano Belaunde, Bernard Berthomieu, Christian Brunette, Agusti Canals, Hubert Garavel, Susanne Graf, Frédéric Lang, Vincent Mahe, Michel Nakhle, et al. Les résultats du projet OpenEmbeDD. *Génie logiciel*, (89), 2009.

[D-J46] Roberto Passerone, Imene Ben-Hafaiedh, Susanne Graf, Albert Benveniste, Daniela Cancila, Arnaud Cuccuru, Sébastien Gérard, François Terrier, Werner Damm, Alberto Ferrari, Leonardo Mangeruca, Bernhard Josko, Thomas Peikenkamp, and Alberto L. Sangiovanni-Vincentelli. Meta-models in Europe: Languages, tools and applications. *IEEE Design & Test of Computers*, 26(3):38–53, 2009.

D.3.1.2 International Conferences

[D-C1] Susanne Graf. Distributed implementation of constrained systems based on knowledge. In Traian Muntean, editor, *IEEE 13th International Symposium on Parallel and Distributed Computing, ISPDC 2013, Porquerolles Golden Island, France, June 24-27, 2014*. IEEE, 2014. Two page abstract.

[D-C2] Lacramioara Astefanoaei, Souha Ben Rayana, Saddek Bensalem, Marius Bozga, and Jacques Combaz. Compositional invariant generation for timed systems. In Erika Abraham and Klaus Havelund, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 20th International Conference, TACAS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS*, volume 8413 of *Lecture Notes in Computer Science*, pages 263–278. Springer, 2014.

[D-C3] Marius Bozga, Radu Iosif, and Filip Konecný. Safety problems are NP-complete for flat integer programs with octagonal loops. In Xavier Rival Kenneth L. McMillan, editor, *Verification, Model Checking, and Abstract Interpretation - 15th International Conference, VMCAI 2014, San Diego, CA, USA, January 19-21, 2014, Proceedings*, volume 8318 of *Lecture Notes in Computer Science*, pages 242–261. Springer, 2014.

[D-C4] Marie-Laure Potet, Laurent Mounier, Maxime Puys, and Louis Dureuil. Lazart: a symbolic approach for evaluation the robustness of secured codes against control flow fault injection. In *ICST*, 2014.

[D-C5] Alexios Lekidis, Marius Bozga, and Saddek Bensalem. Model-based validation of canopen systems. In *Proceedings of WFCS'14 - 10th IEEE International Workshop on Factory Communication Systems, Toulouse, France*. IEEE, May 2014.

[D-C6] Najah Ben Said, Takoua Abdellatif, Saddek Bensalem, and Marius Bozga. Model-driven information flow security for component-based systems. In Yassine Lakhnech Saddek Bensalem, Axel Legay, editor, *Proceedings of FPS'14 - From Programs to Systems - The Systems Perspective in Computing, ETAPS Workshop, FPS 2014, in Honor of Joseph Sifakis*, volume 8415 of *Lecture Notes in Computer Science*. Springer, April 2014.

[D-C7] Simon Bliudze, Marius Bozga, Mohamad Jaber, and Joseph Sifakis. Architecture internalisation in BIP. In *Proceedings of CBSE'14 - The 7th International ACM Sigsoft Symposium on Component-Based Software Engineering - Lille, France*. ACM, June 2014.

[D-C8] Alexis Fouilhe and Sylvain Boulmé. A certifying frontend for (sub)polyhedral abstract domains. In *Verified Software: Theories, Tools and Experiments (VSTTE 2014)*, LNCS. Springer, 2014.

[D-C9] Alexis Fouilhe, Sylvain Boulmé, and Michael Périn. Modular and lightweight certification of polyhedral abstract domains. In *Types for Proofs and Programs (TYPES 2014) – Book of Abstracts*, May 2014.

[D-C10] Christian von Essen and Dimitra Giannakopoulou. Analyzing the next generation airborne collision avoidance system. In *TACAS*, pages 620–635, 2014.

[D-C11] Ylies Falcone Hüseyin Tirli, Abdurrahman Pekts and Nadi Erdogan. Virmon: A virtualization-based automated dynamic malware analysis system. In *6th International Conference Information Security and Cryptology (ISCTURKEY)*, 2013.

[D-C12] Abdurrahman Pektas and Tankut Acarman. A dynamic malware analyzer against virtual machine aware malicious software. In *Security and Communication Networks, doi: 10.1002/sec.931*, 2013.

[D-C13] Ayoub Nouri, Axel Legay, Saddek Bensalem, and Marius Bozga. SBIP: A statistical model checking extension for the BIP framework. In *Statistical Model Checking Workshop, SMC*, 2013.

[D-C14] Alexios Lekidis, Marius Bozga, Didier Mauuary, and Saddek Bensalem. A model-based design flow for can-based systems. In *Proceedings of the iCC CAN in Automation Conference, Paris, France*, November 2013.

[D-C15] Dario Socci, Petro Poplavko, Saddek Bensalem, and Marius Bozga. Modeling mixed critical systems in real-time BIP. In *Proc. ReTiMiCs-2013, Workshop on Real-Time Mixed Criticality Systems*, 2013.

[D-C16] Dario Socci, Petro Poplavko, Saddek Bensalem, and Marius Bozga. Time-triggered mixed-critical scheduler. In *1st International Workshop on Mixed Criticality Systems (WMC)*, 2013.

[D-C17] Karine Altisen, Stéphane Devismes, Raphaël Jamet, and Pascal Lafourcade. SR3: Secure resilient reputation-based routing. In *The annual IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS 2013)*, pages 258–265, Cambridge, Massachusetts, USA, May 2013. IEEE.

[D-C18] Karine Altisen, Stéphane Devismes, Raphaël Jamet, and Pascal Lafourcade. Routage sécurisé et résilient pour réseaux de capteurs sans fil. In Nicolas Nisse, Franck Rousseau, and Yann Busnel, editors, *15èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (AlgoTel)*, pages 1–4, Pornic, France, 2013.

[D-C19] Radu Iosif, Adam Rogalewicz, and Jirí Simácek. The tree width of separation logic with recursive definitions. In Maria Paola Bonacina, editor, *Automated Deduction - CADE-24 - 24th International Conference on Automated Deduction, Lake Placid, NY, USA, June 9-14, 2013. Proceedings*, volume 7898 of *Lecture Notes in Computer Science*, pages 21–38. Springer, 2013.

[D-C20] Dario Socci, Peter Poplavko, Saddek Bensalem, and Marius Bozga. Mixed critical earliest deadline first. In *25th Euromicro Conference on Real-Time Systems, ECRTS 2013, Paris, France, July 9-12, 2013*, pages 93–102. IEEE, 2013.

[D-C21] Ahlem Triki, Jacques Combaz, Saddek Bensalem, and Joseph Sifakis. Model-based implementation of parallel real-time systems. In Vittorio Cortellessa and Dániel Varró, editors, *Fundamental Approaches to Software Engineering - 16th International Conference, FASE 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, M*, volume 7793 of *Lecture Notes in Computer Science*, pages 235–249. Springer, 2013.

[D-C22] Paul C. Attie, Saddek Bensalem, Marius Bozga, Mohamad Jaber, Joseph Sifakis, and Fadi A. Zaraket. An abstract framework for deadlock prevention in BIP. In Dirk Beyer and Michele Boreale, editors, *Formal Techniques for Distributed Systems - Joint IFIP WG 6.1 International Conference, FMOODS/FORTE 2013, Held as Part of the 8th International Federated Conference on Distributed Computing Technique*, volume 7892 of *Lecture Notes in Computer Science*, pages 161–177. Springer, 2013.

[D-C23] Saddek Bensalem, Borzoo Bonakdarpour, Marius Bozga, Doron Peled, and Jean Quilbeuf. Performance evaluation of process partitioning using probabilistic model checking. In Valeria Bertacco and Axel Legay, editors, *Hardware and Software: Verification and Testing - 9th International Haifa Verification Conference, HVC 2013, Haifa, Israel, November 5-7, 2013, Proceedings*, volume 8244 of *Lecture Notes in Computer Science*, pages 344–358. Springer, 2013.

[D-C24] Saddek Bensalem, Marius Bozga, Benoît Boyer, and Axel Legay. Incremental generation of linear invariants for component-based systems. In *13th International Conference on Application of Concurrency to System Design, ACSD 2013, Barcelona, Spain, 8-10 July, 2013*, pages 80–89. IEEE, 2013.

[D-C25] Cristian Ene, Clémentine Gritti, and Yassine Lakhnech. Cil security proof for a password-based key exchange. In Willy Susilo and Reza Reyhanitabar, editors, *Provable Security - 7th International Conference, ProvSec 2013, Melaka, Malaysia, October 23-25, 2013. Proceedings*, volume 8209 of *Lecture Notes in Computer Science*, pages 59–85. Springer, 2013.

[D-C26] Jean-François Monin and Xiaomu Shi. Handcrafted Inversions Made Operational on Operational Semantics. In S. Blazy, C. Paulin, and D. Pichardie, editors, *ITP 2013*, volume 7998 of *LNCS*, pages 338–353, Rennes, France, July 2013. Springer.

[D-C27] Balaji Raman, Ayoub Nouri, Deepak Gangadharan, Marius Bozga, Ananda Basu, Mayur Maheshwari, Axel Legay, Saddek Bensalem, and Samarjit Chakraborty. Stochastic modeling and performance analysis of multimedia socs. In *2013 International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation, SAMOS 2013, Agios Konstantinos, Samos Island, Greece, July 15-18, 2013*, pages 145–154. IEEE, 2013.

[D-C28] Pierre Ganty, Radu Iosif, and Filip Konečný. Underapproximation of procedure summaries for integer programs. In *TACAS*, pages 245–259, 2013.

[D-C29] Jannik Dreier, Jean-Guillaume Dumas, and Pascal Lafourcade. Brandt's fully private auction protocol revisited. In Amr Youssef, Abderrahmane Nitaj, and Aboul Ella Hassanien, editors, *Progress in Cryptology - AFRICACRYPT 2013, 6th International Conference on Cryptology in Africa, Cairo, Egypt, June 22-24, 2013. Proceedings*, volume 7918 of *Lecture Notes in Computer Science*, pages 88–106. Springer, 2013.

[D-C30] Jannik Dreier, Cristian Ene, Pascal Lafourcade, and Yassine Lakhnech. On unique decomposition of processes in the applied -calculus. In Frank Pfenning, editor, *Foundations of Software Science and Computation Structures - 16th International Conference, FOSSACS 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013,*, volume 7794 of *Lecture Notes in Computer Science*, pages 50–64. Springer, 2013.

[D-C31] Jannik Dreier, Hugo Jonker, and Pascal Lafourcade. Verifiability in e-auction protocols. In *1st Workshop on Hot Issues in Security Principles and Trust (HotSpot 2013)*, Hangzhou, China, 2013.

[D-C32] Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech. Formal verification of e-auction protocols. In David Basin and John Mitchell, editors, *Principles of Security and Trust - Second International Conference, POST 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24,*, volume 7796 of *Lecture Notes in Computer Science*, pages 247–266. Springer, 2013.

[D-C33] Martin Gagne, Pascal Lafourcade, and Yassine Lakhnech. Automated security proofs for almost-universal hash for mac verification. In *Computer Security - ESORICS 2013 - 18th European Symposium on Research in Computer Security, London, UK, September 2012. Proceedings*, Lecture Notes in Computer Science. Springer, 2013.

[D-C34] Alexis Fouilhé, David Monniaux, and Michael Périn. Efficient generation of correctness certificates for the abstract domain of polyhedra. In *Static analysis (SAS 2013)*, volume 7935 of *LNCS*. Springer, 2013.

[D-C35] Gustavo Grieco, Laurent Mounier, Marie-Laure Potet, and Sanjay Rawat. A stack model for symbolic buffer overflow exploitability analysis (extended abstract). In *5th Workshop on the Constraints in Software Testing, Verification and Analysis CSTVA 2013 (in association with ICST 2013)*. IEEE, 2013.

[D-C36] Susanne Graf and Sophie Quinton. Knowledge for the distributed implementation of constrained systems. In Einar Broch Johnson Luigia Petre, editor, *10th International Conference on integrated Formal Methods, iFM 2013, Turku, June 10-14. Proceedings*, volume 7940 of *Lecture Notes in Computer Science*, pages 77–93. Springer, 2013.

[D-C37] Ali Kassem, Pascal Lafourcade, Yassine Lakhnech, and Sebastian M ödersheim. Multiple independent lazy intruders. In *1st Workshop on Hot Issues in Security Principles and Trust (HotSpot 2013)*, 2013.

[D-C38] Jean-Francois Kempf, Marius Bozga, and Oded Maler. As soon as probable: Optimal scheduling under stochastic uncertainty. In *TACAS*, 2013.

[D-C39] Emmanuel Sifakis and Laurent Mounier. Predictive taint analysis for extended testing of parallel executions. In Valeria Bertacco and Axel Legay, editors, *Hardware and Software: Verification and Testing - 9th International Haifa Verification Conference*, volume 8244 of *Lecture Notes in Computer Science*, pages 129–144, Haifa (Israel), 2013. Springer.

[D-C40] Christian von Essen and Barbara Jobstmann. Program repair without regret. In Springer, editor, *Computer Aided Verification (CAV)*, 2013.

[D-C41] F. Pietrek, A. Bouchez and De Dinechin B. A tirex-based ssa interpreter. In *DCE '12: International Workshop on Dynamic Compilation Everywhere Paris, France*, 2012.

[D-C42] Karine Altisen, Stéphane Devismes, Antoine Gerbaud, and Pascal Lafourcade. Analysis of random walks using tabu lists. In Magnus M. Halldorsson and Guy Even, editors, *19th International Colloquium on Structural Information and Communication Complexity (SIROCCO'2012)*, LNCS, pages 254–266, Reykjavík, Iceland, June 30 - July 2 2012. Springer.

[D-C43] Julien Douady, Christian Hoffmann, Fabienne Carrier, Benoit Chabaud, Arnaud Mantoux, Yves Markowicz, Michael Périn, Virginie Stoppin-Mellet, Gabrielle Tichtinsky, Bernard Ycart, and Hubert Borderiou. Un dispositif pour alerter les étudiants sur leur maîtrise des pré-requis nécessaires pour réussir leur entrée à l'université. In *Congrès de l'Association Internationale de Pédagogie Universitaire*, May 2012.

[D-C44] Raphël Jamet and Pascal Lafourcade. Formal model for (k)-neighborhood discovery protocols. Springer, 2012.

[D-C45] Sofia Bekrar, Chaouki Bekrar, Roland Groz, and Laurent Mounier. A taint based approach for smart fuzzing. In Giuliano Antoniol, Antonia Bertolino, and Yvan Labiche, editors, *Proceedings of SecTest*, pages 818–825, 2012.

[D-C46] Saddek Bensalem, Marius Bozga, Jean Quilbeuf, and Joseph Sifakis. Optimized distributed implementation of multiparty interactions with observation. In *Proceedings of the 2nd edition on Programming systems, languages and applications based on actors, agents, and decentralized control abstractions*, AGERE! '12, pages 71–82, New York, NY, USA, 2012. ACM.

[D-C47] Marius Bozga, Radu Iosif, and Filip Konečný. Deciding conditional termination. In Cormac Flanagan and Barbara König, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 18th International Conference, TACAS 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS*, volume 7214 of *Lecture Notes in Computer Science*, pages 252–266. Springer, 2012.

[D-C48] Eric Conquet, François-Xavier Dormoy, Iulia Dragomir, Susanne Graf, David Lesens, Piotr Nienaltowski, and Iulian Ober. Formal model driven engineering for space onboard software. In *International Congress on Embedded Real Time Software and Systems (ERTS2), Toulouse, February 2012*. French Society for Electricity, Electronics, and Information and Communication Technologies, 2012.

[D-C49] Saddek Bensalem, Marius Bozga, Doron Peled, and Jean Quilbeuf. Knowledge based transactional behavior. In Tanja Vos Armin Biere, Amir Nahir, editor, *Hardware and Software: Verification and Testing - 8th International Haifa Verification Conference, HVC 2012, Haifa, Israel, November 6-8, 2012. Revised Selected Papers*, volume 7857 of *Lecture Notes in Computer Science*, pages 40–55. Springer, 2012.

[D-C50] Hossein Hojjat, Radu Iosif, Filip Konečný, Viktor Kuncak, and Philipp Rümmer. Accelerating interpolants. In *ATVA*, pages 187–202, 2012.

[D-C51] Gilles Barthe, Benjamin Grégoire, César Kunz, Yassine Lakhnech, and Santiago Zanella Béguelin. Automation in computer-aided cryptography: Proofs, attacks and designs. In *CPP*, volume 7679 of *Lecture Notes in Computer Science*, pages 7–8. Springer, 2012.

[D-C52] Marion Daubignard, Pierre-Alain Fouque, and Yassine Lakhnech. Generic indifferentiability proofs of hash designs. In *CSF - 25th IEEE Computer Security Foundations Symposium, CSF 2012, Cambridge, MA, USA, June 25-27, 2012*, pages 340–353. IEEE, 2012.

[D-C53] Marius Bozga, Alexandre David, Arnd Hartmanns, Holger Hermanns, Kim Guldstrand Larsen, Axel Legay, and Jan Tretmans. State-of-the-art tools and techniques for quantitative modeling and analysis of embedded systems. In Wolfgang Rosenstiel and Lothar Thiele, editors, *2012 Design, Automation & Test in Europe Conference & Exhibition, DATE 2012, Dresden, Germany, March 12-16, 2012*, pages 370–375. IEEE, 2012.

[D-C54] Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech. Defining privacy for weighted votes, single and multi-voter coercion. In *ESORICS - Computer Security - ESORICS 2012 - 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings*, volume 7459 of *Lecture Notes in Computer Science*, pages 451–468. Springer, 2012.

[D-C55] Hossein Hojjat, Filip Konečný, Florent Garnier, Radu Iosif, Viktor Kuncak, and Philipp Rümmer. A verification toolkit for numerical transition systems - tool paper. In *FM*, pages 247–251, 2012.

[D-C56] Saddek Bensalem, Marius Bozga, Jean Quilbeuf, and Joseph Sifakis. Knowledge-based distributed conflict resolution for multiparty interactions and priorities. In Holger Giese and Grigore Rosu, editors, *Formal Techniques for Distributed Systems - Joint 14th IFIP WG 6.1 International Conference, FMOODS 2012 and 32nd IFIP WG 6.1 International Conference, FORTE 2012, Stockholm, Sweden, June 13-16, 2012.*, volume 7273 of *Lecture Notes in Computer Science*, pages 118–134. Springer, 2012.

[D-C57] Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech. A formal taxonomy of privacy in voting protocols. In *Proceedings of IEEE International Conference on Communications, ICC 2012, Ottawa, ON, Canada, June 10-15, 2012*, pages 6710–6715. IEEE, 2012.

[D-C58] Alena Simalatsar, Liangpeng Guo, Marius Bozga, and Roberto Passerone. Integration of correct-by-construction BIP models into the metroii design space exploration flow. In *30th International IEEE Conference on Computer Design, ICCD 2012, Montreal, QC, Canada, September 30 - Oct. 3, 2012*, pages 490–491. IEEE Computer Society, 2012.

[D-C59] Saddek Bensalem, Marius Bozga, Benoît Delahaye, Cyrille Jégourel, Axel Legay, and Ayoub Nouri. Statistical model checking QoS properties of systems with SBIP. In Tiziana Margaria and Bernhard Steffen, editors, *Leveraging Applications of Formal Methods, Verification and Validation. Technologies for Mastering Change - 5th International Symposium, ISoLA 2012, Heraklion, Crete, Greece, October 15-18, 2012, Proc*, volume 7609 of *Lecture Notes in Computer Science*, pages 327–341. Springer, 2012.

[D-C60] Marius Bozga, Mohamad Jaber, Nikolaos Maris, and Joseph Sifakis. Modeling dynamic architectures using dy-bip. In Thomas Gschwind, Flavio De Paoli, Volker Gruhn, and Matthias Book, editors, *Software Composition - 11th International Conference, SC 2012, Prague, Czech Republic, May 31 - June 1, 2012. Proceedings*, volume 7306 of *Lecture Notes in Computer Science*, pages 1–16. Springer, 2012.

[D-C61] Borzoo Bonakdarpour, Marius Bozga, and Gregor Gößler. A theory of fault recovery for component-based models. In Andréa W. Richa and Christian Scheideler, editors, *Stabilization, Safety, and Security of Distributed Systems - 14th International Symposium, SSS 2012, Toronto, Canada, October 1-4, 2012. Proceedings*, volume 7596 of *Lecture Notes in Computer Science*, pages 314–328. Springer, 2012.

[D-C62] Meixian Chen and Jean-François Monin. Formal Verification of Netlog Protocols. In Tiziana Margaria, Zongyan Qiu, and Hongli Yang, editors, *Sixth International Symposium on Theoretical Aspects of Software Engineering, TASE 2012, 4-6 July 2012, Beijing, China*, pages 43–50. IEEE, 2012.

[D-C63] Rui Wang, Min Zhou, Liangze Yin, Lianyi Zhang, Jiaguang Sun, Gu Ming, and Marius Bozga. Modeling and validation of plc-controlled systems: A case study. In Tiziana Margaria, Zongyan Qiu, and Hongli Yang, editors, *Sixth International Symposium on Theoretical Aspects of Software Engineering, TASE 2012, 4-6 July 2012, Beijing, China*, pages 161–166. IEEE, 2012.

[D-C64] Christian von Essen and Barbara Jobstmann. Synthesizing efficient controllers. In Viktor Kuncak and Andrey Rybalchenko, editors, *Verification, Model Checking, and Abstract Interpretation - 13th International Conference, VMCAI 2012, Philadelphia, PA, USA, January 22-24, 2012. Proceedings*, volume 7148 of *Lecture Notes in Computer Science*, pages 428–444. Springer, 2012.

[D-C65] Ananda Basu, Saddek Bensalem, Marius Bozga, and Joseph Sifakis. Rigorous component-based system design - (invited paper). In Franciso Durán, editor, *Rewriting Logic and Its Applications - 9th International Workshop, WRLA 2012, Held as a Satellite Event of ETAPS, Tallinn, Estonia, March 24-25, 2012, Revised Selected Papers*, volume 7571 of *Lecture Notes in Computer Science*, pages 1–9. Springer, 2012.

[D-C66] Aannda Basu, Saddek Bensalem, Marius Bozga, Julien Mottin, Francois Pacull, Athanasios Poulakidas, and Aggelis Aggelis. System level modeling, analysis and code generation: Object recognition case study. In *Proceedings of Embedded World'12 Conference, Nurnberg, Germany*, February 2012.

[D-C67] Eric Conquet, François-Xavier Dormoy, Iulia Dragomir, Susanne Graf, David Lesens, Piotr Nienaltowski, and Iulian Ober. Formal model driven engineering for space onboard software. In *Embedded Real Time Software and Systems (ERTS2 2012), Toulouse*, 2012.

[D-C68] Nacira Ghoualmi, Noudjoud Kahya, and Pascal Lafourcade. Key management protocol in wimax revisited. In *The Third International Conference on Communications Security and Information Assurance (CSIA 2012)*, Delhi, India, May 2012. Springer.

[D-C69] Laurent Mounier and Emmanuel Sifakis. Dynamic information-flow analysis for multi-threaded applications. In Tiziana Margaria and Bernhard Steffen, editors, *Proceedings of ISoLA*, volume 7609 of *Lecture Notes in Computer Science*, pages 358–371, Heraklion, Greece, 2012. Springer.

[D-C70] Sanjay Rawat and Laurent Mounier. Finding buffer overflow inducing loops in binary executables. In *Proceedings of Sixth International Conference on Software Security and Reliability (SERE)*, pages 177–186, Gaithersburg, Maryland, USA, 2012. IEEE.

[D-C71] Karine Altisen, Stéphane Devismes, Pascal Lafourcade, and Clément Ponsonnet. Routage par marche aléatoire à listes tabous. In *Algotel*, pages 21–24, 2011.

[D-C72] Laurent Fousse, Pascal Lafourcade, and Mohamed Alnuaimi. Benaloh's dense probabilistic encryption revisited. In Abderrahmane Nitaj and David Pointcheval, editors, *Progress in Cryptology - AFRICACRYPT 2011 - 4th International Conference on Cryptology in Africa, Dakar, Senegal, July 5-7, 2011. Proceedings*, volume 6737 of *Lecture Notes in Computer Science*, pages 348–362. Springer, 2011.

[D-C73] Imene Ben Hafaiedh, Susanne Graf, and Mohamad Jaber. Model-based design and distributed implementation of bus arbiter for multiprocessors. In *18th IEEE International Conference on Electronics, Circuits and Systems, ICECS 2011, Beirut, Lebanon, December 11-14, 2011*, pages 65–68. IEEE, 2011.

[D-C74] Xiaomu Shi, Jean-François Monin, Frédéric Tuong, and Frédéric Blanqui. First Steps towards the Certification of an ARM Simulator Using Compcert. In Jean-Pierre Jouannaud and Zhong Shao, editors, *Certified Proofs and Programs - First International Conference*, volume 7086 of *LNCS*, pages 346–361, Kenting, Taiwan, December 7-9 2011. Springer.

[D-C75] Imene Ben Hafaiedh, Susanne Graf, and Nejla Mazouz. Distributed implementation of systems with multiparty interactions and priorities. In Gilles Barthe, Alberto Pardo, and Gerardo Schneider, editors, *Software Engineering and Formal Methods - 9th International Conference, SEFM 2011, Montevideo, Uruguay, November 14-18, 2011. Proceedings*, volume 7041 of *Lecture Notes in Computer Science*, pages 38–57. Springer, 2011.

[D-C76] Saddek Bensalem, Andreas Griesmayer, Axel Legay, Thanh-Hung Nguyen, Joseph Sifakis, and Rongjie Yan. D-finder 2: Towards efficient correctness of incremental design. In Mihaela Gheorghiu Bobaru, Klaus Havelund, Gerard J. Holzmann, and Rajeev Joshi, editors, *NASA Formal Methods - Third International Symposium, NFM 2011, Pasadena, CA, USA, April 18-20, 2011. Proceedings*, volume 6617 of *Lecture Notes in Computer Science*, pages 453–458. Springer, 2011.

[D-C77] A. Pietrek, F. Bouchez, and B. Dupont De Dinechin. Tirex : A textual target-level intermediate representation for compiler exchange. In *WIR'11 Workshop on Intermediate Representation*, 2011.

[D-C78] Chih-Hong Cheng, Saddek Bensalem, Barbara Jobstmann, Rongjie Yan, Alois Knoll, and Harald Ruess. Model construction and priority synthesis for simple interaction systems. In Mihaela Gheorghiu Bobaru, Klaus Havelund, Gerard J. Holzmann, and Rajeev Joshi, editors, *NASA Formal Methods - Third International Symposium, NFM 2011, Pasadena, CA, USA, April 18-20, 2011. Proceedings*, volume 6617 of *Lecture Notes in Computer Science*, pages 466–471. Springer, 2011.

[D-C79] Krishnendu Chatterjee, Thomas A. Henzinger, Barbara Jobstmann, and Rohit Singh. Quasy: Quantitative synthesis tool. In Parosh Aziz Abdulla and Rustan Leino, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 17th International Conference, TACAS 2011, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS*, volume 6605 of *Lecture Notes in Computer Science*, pages 267–271. Springer, 2011.

[D-C80] Gilles Barthe, Mathilde Duclos, and Yassine Lakhnech. A computational indistinguishability logic for the bounded storage model. In *Foundations and Practice of Security*, volume 6888 of *Lecture Notes in Computer Science*. Springer, 2011.

[D-C81] Pierre Corbineau, Mathilde Duclos, and Yassine Lakhnech. Certified security proofs of cryptographic protocols in the computational model: An application to intrusion resilience. In Jean-Pierre Jouannaud and Zhong Shao, editors, *Certified Programs and Proofs - First International Conference, CPP 2011, Kenting, Taiwan, December 7-9, 2011. Proceedings*, volume 7086 of *Lecture Notes in Computer Science*, pages 378–393. Springer, 2011.

[D-C82] Chih-Hong Cheng, Barbara Jobstmann, Christian Buckl, and Alois Knoll. On the hardness of priority synthesis. In Béatrice Bouchou-Markhoff, Pascal Caron, Jean-Marc Champarnaud, and Denis Maurel, editors, *Implementation and Application of Automata - 16th International Conference, CIAA 2011, Blois, France, July 13-16, 2011. Proceedings*, volume 6807 of *Lecture Notes in Computer Science*, pages 110–117. Springer, 2011.

[D-C83] Asma Tafat, Sylvain Boulmé, and Claude Marché. A refinement methodology for object-oriented programs. In *Formal Verification of Object-Oriented Software*, volume 6528 of *Lecture Notes in Computer Science*, 2011.

[D-C84] Nicolas Berthier, Florence Maraninchi, and Laurent Mounier. Synchronous programming of device drivers for global resource control in embedded operating systems. In *ACM SIGPLAN/SIGBED Conference on Languages, Compilers, Tools and Theory for Embedded Systems (LCTES)*, Chicago, IL, USA, April 2011.

[D-C85] Chih-Hong Cheng, Saddek Bensalem, Yu-Fang Chen, Rongjie Yan, Barbara Jobstmann, Harald Ruess, Christian Buckl, and Alois Knoll. Algorithms for synthesizing priorities in component-based systems. In Tevfik Bultan and Pao-Ann Hsiung, editors, *Automated Technology for Verification and Analysis, 9th International Symposium, ATVA 2011, Taipei, Taiwan, October 11-14, 2011. Proceedings*, volume 6996 of *Lecture Notes in Computer Science*, pages 150–167. Springer, 2011.

[D-C86] Takoua Abdellatif, Lilia Sfaxi, Riadh Robbana, and Yassine Lakhnech. Automating information flow control in component-based distributed systems. In Ivica Crnkovic, Judith A. Stafford, Antonia Bertolino, and Kendra M. L. Cooper, editors, *Proceedings of the 14th International ACM Sigsoft Symposium on Component Based Software Engineering, CBSE 2011, part of Comparch '11 Federated Events on Component-Based Software Engineering and Softwa*, pages 73–82. ACM, 2011.

[D-C87] Gilles Barthe, Benjamin Grégoire, Yassine Lakhnech, and Santiago Zanella Béguelin. Beyond provable security verifiable IND-CCA security of OAEP. In Aggelos Kiayias, editor, *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, volume 6558 of *Lecture Notes in Computer Science*, pages 180–196. Springer, 2011.

[D-C88] Joseph Sifakis. Methods and tools for component-based system design. In *Design, Automation and Test in Europe, DATE 2011, Grenoble, France, March 14-18, 2011*, page 1022. IEEE, 2011.

[D-C89] Saddek Bensalem, Kees Goossens, Christoph Kirsch, Roman Obermaisser, Edward A. Lee, and Joseph Sifakis. Time-predictable and composable architectures for dependable embedded systems. In Samarjit Chakraborty, Ahmed Jerraya, Sanjoy K. Baruah, and Sebastian Fischmeister, editors, *Proceedings of the 11th International Conference on Embedded Software, EMSOFT 2011, part of the Seventh Embedded Systems Week, ESWeek 2011, Taipei, Taiwan, October 9-14, 2011*, pages 351–352. ACM, 2011.

[D-C90] Borzoo Bonakdarpour, Marius Bozga, and Jean Quilbeuf. Automated distributed implementation of component-based models with priorities. In Samarjit Chakraborty, Ahmed Jerraya, Sanjoy K. Baruah, and Sebastian Fischmeister, editors, *Proceedings of the 11th International Conference on Embedded Software, EMSOFT 2011, part of the Seventh Embedded Systems Week, ESWeek 2011, Taipei, Taiwan, October 9-14, 2011*, pages 59–68. ACM, 2011.

[D-C91] Tesnim Abdellatif, Jacques Combaz, and Marc Poulhiès. Correct implementation of open real-time systems. In *37th EUROMICRO Conference on Software Engineering and Advanced Applications, SEAA 2011, Oulu, Finland, August 30 - September 2, 2011*, pages 57–64. IEEE, 2011.

[D-C92] Ananda Basu, Saddek Bensalem, Marius Bozga, Paraskevas Bourgos, Mayur Maheshwari, and Joseph Sifakis. Component assemblies in the context of manycore. In Bernhard Beckert, Ferruccio Damiani, Frank S. de Boer, and Marcello Bonsangue, editors, *Formal Methods for Components and Objects, 10th International Symposium, FMCO 2011, Turin, Italy, October 3-5, 2011, Revised Selected Papers*, pages 314–333. Springer, 2011.

[D-C93] Sofia Bekrar, Chaouki Bekrar, Roland Groz, and Laurent Mounier. Finding software vulnerabilities by smart fuzzing. In *IEEE Fourth International Conference on Software Testing, Verification and Validation, ICST 2011, Berlin, Germany, 21-25 March 2011*, pages 427–430. IEEE Computer Society, 2011.

[D-C94] Ananda Basu, Saddek Bensalem, Marius Bozga, Paraskevas Bourgos, and Joseph Sifakis. Rigorous system design: The BIP approach. In Zdenek Kotásek, Jan Bouda, Ivana Cerná, Lukás Sekanina, Tomás Vojnar, and David Antos, editors, *Mathematical and Engineering Methods in Computer Science - 7th International Doctoral Workshop, MEMICS 2011, Lednice, Czech Republic, October 14-16, 2011, Revised Selected Papers*, volume 7119 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2011.

[D-C95] Saddek Bensalem, Andreas Griesmayer, Axel Legay, Thanh-Hung Nguyen, and Doron Peled. Efficient deadlock detection for concurrent systems. In Satnam Singh, Barbara Jobstmann, Michael Kishinevsky, and Jens Brandt, editors, *9th IEEE/ACM International Conference on Formal Methods and Models for Codesign, MEMOCODE 2011, Cambridge, UK, 11-13 July, 2011*, pages 119–129. IEEE, 2011.

[D-C96] Paraskevas Bourgos, Ananda Basu, Marius Bozga, Saddek Bensalem, Joseph Sifakis, and Kai Huang. Rigorous system level modeling and analysis of mixed hw/sw systems. In Satnam Singh, Barbara Jobstmann, Michael Kishinevsky, and Jens Brandt, editors, *9th IEEE/ACM International Conference on Formal Methods and Models for Codesign, MEMOCODE 2011, Cambridge, UK, 11-13 July, 2011*, pages 11–20. IEEE, 2011.

[D-C97] Ylies Falcone, Mohamad Jaber, Thanh-Hung Nguyen, Marius Bozga, and Saddek Bensalem. Runtime verification of component-based systems. In Gilles Barthe, Alberto Pardo, and Gerardo Schneider, editors, *Software Engineering and Formal Methods - 9th International Conference, SEFM 2011, Montevideo, Uruguay, November 14-18, 2011. Proceedings*, volume 7041 of *Lecture Notes in Computer Science*, pages 204–220. Springer, 2011.

[D-C98] Roderick Bloem, Krishnendu Chatterjee, Karin Greimel, Thomas A. Henzinger, and Barbara Jobstmann. Specification-centered robustness. In *Industrial Embedded Systems (SIES), 2011 6th IEEE International Symposium on, Vasteras, Sweden, 15-17 June, 2011*, pages 176–185. IEEE, 2011.

[D-C99] Saddek Bensalem, Lavindra de Silva, Andreas Griesmayer, Felix Ingrand, Axel Legay, and Rongjie Yan. A formal approach for incremental construction with an application to autonomous robotic systems. In Sven Apel and Ethan Jackson, editors, *Software Composition - 10th International Conference, SC 2011, Zurich, Switzerland, June 30 - July 1, 2011. Proceedings*, volume 6708 of *Lecture Notes in Computer Science*, pages 116–132. Springer, 2011.

[D-C100] Simon Bliudze and Joseph Sifakis. Synthesizing glue operators from glue constraints for the construction of component-based systems. In Sven Apel and Ethan Jackson, editors, *Software Composition - 10th International Conference, SC 2011, Zurich, Switzerland, June 30 - July 1, 2011. Proceedings*, volume 6708 of *Lecture Notes in Computer Science*, pages 51–67. Springer, 2011.

[D-C101] Borzoo Bonakdarpour, Marius Bozga, and Gregor Göessler. A theory of fault recovery for component-based models. In *30th IEEE Symposium on Reliable Distributed Systems (SRDS 2011), Madrid, Spain, October 4-7, 2011*, pages 265–270. IEEE, 2011.

[D-C102] Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech. Vote-independence: A powerful privacy notion for voting protocols. In Joaquín García-Alfaro and Pascal Lafourcade, editors, *Foundations and Practice of Security - 4th Canada-France MITACS Workshop, FPS 2011, Paris, France, May 12-13, 2011, Revised Selected Papers*, volume 6888 of *Lecture Notes in Computer Science*, pages 164–180. Springer, 2011.

[D-C103] Sifakis Emmanuel and Mounier Laurent. Politiques de gestion de protections pour l'implémentation de sections critiques. In *Actes des Rencontres du Parallélisme (RenPar)*, Saint Malo, France, 2011.

[D-C104] Susanne Graf, Roberto Passerone, and Sophie Quinton. Contract-based reasoning for component systems with complex interactions. In *TIMOBD'11*, 2011.

[D-C105] Susanne Graf, Doron Peled, and Sophie Quinton. Monitoring distributed systems using knowledge. In Roberto Bruni and Jürgen Dingel, editors, *Formal Techniques for Distributed Systems - Joint 13th IFIP WG 6.1 International Conference, FMOODS 2011, and 31st IFIP WG 6.1 International Conference, FORTE 2011, Reykjavik, Iceland, June 6-9, 2011.*, volume 6722 of *Lecture Notes in Computer Science*, pages 183–197. Springer, 2011.

[D-C106] Yuxin Deng, Stéphane Grumbach, and Jean-François Monin. A Framework for Verifying Data-Centric Protocols. In R. Bruni and J. Dingel, editors, *FMOODS/FORTE 2011*, volume 6722 of *LNCS*, pages 106–120, Reykjavik, Iceland, June 6-9 2011. Springer.

[D-C107] Jean-Francois Kempf, Marius Bozga, and Oded Maler. Performance evaluation of schedulers in a probabilistic setting. In *FORMATS*, September 2011.

[D-C108] Takoua Abdellatif, Lilia Sfaxi, Riadh Robbana, and Yassine Lakhnech. Information flow control of component-based distributed systems. In *Concurrency and Computation, Practice and Experience*. Wiley, 2011.

[D-C109] Sylvain Steer, Nicolas Craipeau, Daniel Le Métayer, Manuel Maareck, Marie-Laure Potet, and Valérie Viet Triem Tong. Définition des responsabilités pour les dysfonctionnements de logiciels : cadre contractuel et outils de mise en oeuvre. In *Droit, sciences et techniques : quelles responsabilités ? colloque international du Réseau Droit, sciences et techniques.* Edition LexisNexis, 2011.

[D-C110] David Monniaux and Pierre Corbineau. On the generation of Positivstellensatz witnesses in degenerate cases. In Marko Van Eekelen, Herman Geuvers, Julien Schmaltz, and Freek Wiedijk, editors, *Interactive Theorem Proving (ITP)*, volume 6898, pages 249–264, August 2011.

[D-C111] Jannik Dreier and Florian Kerschbaum. Practical privacy-preserving multiparty linear programming based on problem transformation. In *Proceedings of the Third IEEE International Conference on Information Privacy, Security, Risk and Trust and Third IEEE International Conference on Social Computing (PASSAT/SocialCom'11)*, pages 916–924. IEEE, October 2011.

[D-C112] Frédéric Blanqui, Claude Helmstetter, Vania Joloboff, Jean-François Monin, and Xiaomu Shi. Designing a CPU model: from a pseudo-formal document to fast code. In *Proceedings of the 3rd Workshop on Rapid Simulation and Performance Evaluation: Methods and Tools*, Heraklion, Greece, 01 2011. Best Paper Award.

[D-C113] Sanjay Rawat and Laurent Mounier. Offset-aware mutation based fuzzing for buffer overflow vulnerabilities: Few preliminary results. In *Proc. of The Second International Workshop on Security Testing (SECTEST)*. IEEE, 2011.

[D-C114] Christian von Essen and Barbara Jobstmann. Synthesizing systems with optimal average-case behavior for ratio objectives. In Johannes Reich and Bernd Finkbeiner, editors, *International Workshop on Interactions, Games and Protocols*. Electronic Proceedings in Theoretical Computer Science, 2011.

[D-C115] Saddek Bensalem, Marius Bozga, Axel Legay, Thanh-Hung Nguyen, Joseph Sifakis, and Rongjie Yan. Incremental component-based construction and verification using invariants. In Roderick Bloem and Natasha Sharygina, editors, *Proceedings of 10th International Conference on Formal Methods in Computer-Aided Design, FMCAD 2010, Lugano, Switzerland, October 20-23*, pages 257–256. IEEE, 2010.

[D-C116] Roderick Bloem, Krishnendu Chatterjee, Karin Greimel, Thomas A. Henzinger, and Barbara Jobstmann. Robustness in the presence of liveness. In *Computer Aided Verification, 22nd International Conference, CAV 2010, Edinburgh, UK, July 15-19, 2010*, pages 410–424, 2010.

[D-C117] Imene Ben-Hafaiedh, Susanne Graf, and Hammadi Khairallah. Implementing distributed controllers for systems with priorities. In *Proceedings Ninth International Workshop on the Foundations of Coordination Languages and Software Architectures, FOCLASA*, volume 30 of *EPTCS*, pages 31–46, 2010.

[D-C118] Imene Ben-Hafaiedh, Susanne Graf, and Sophie Quinton. Reasoning about safety and progress using contracts. In Jin Song Dong and Huibiao Zhu, editors, *Formal Methods and Software Engineering - 12th International Conference on Formal Engineering Methods, ICFEM 2010, Shanghai, China, November 17-19, 2010. Proceedings*, volume 6447 of *Lecture Notes in Computer Science*, pages 436–451. Springer, 2010.

[D-C119] Imene Ben-Hafaiedh, Susanne Graf, and Sophie Quinton. Contract-based reasoning about progress: Application to resource sharing in a network. In *Proc. of FLACOS'10*, 2010.

[D-C120] Judicaël Courant, Marion Daubignard, Cristian Ene, Pascal Lafourcade, and Yassine Lakhnech. Automated proofs for asymmetric encryption. In Dennis Dams, Ulrich Hannemann, and Martin Steffen, editors, *Concurrency, Compositionality, and Correctness, Essays in Honor of Willem-Paul de Roever*, volume 5930 of *Lecture Notes in Computer Science*, pages 300–321. Springer, 2010.

[D-C121] Saddek Bensalem, Axel Legay, Thanh-Hung Nguyen, Joseph Sifakis, and Rongjie Yan. Incremental invariant generation for compositional design. In Jing Liu, Doron Peled, Bow-Yaw Wang, and Farn Wang, editors, *4th IEEE International Symposium on Theoretical Aspects of Software Engineering, TASE 2010, Taipei, Taiwan, 25-27 August 2010*, pages 157–167. IEEE Computer Society, 2010.

[D-C122] Krishnendu Chatterjee, Thomas A. Henzinger, Barbara Jobstmann, and Arjun Radhakrishna. Gist: A solver for probabilistic games. In *Computer Aided Verification, 22nd International Conference, CAV 2010, Edinburgh, UK, July 15-19, 2010*, pages 665–669, 2010.

[D-C123] Krishnendu Chatterjee, Thomas A. Henzinger, Barbara Jobstmann, and Rohit Singh. Measuring and synthesizing systems in probabilistic environments. In *Computer Aided Verification, 22nd International Conference, CAV 2010, Edinburgh, UK, July 15-19, 2010*, pages 380–395, 2010.

[D-C124] Ananda Basu, Saddek Bensalem, Marius Bozga, Benoît Caillaud, Benoît Delahaye, and Axel Legay. Statistical abstraction and model-checking of large heterogeneous systems. In Elena Zucca John Hatcliff, editor, *Formal Techniques for Distributed Systems, Joint 12th IFIP WG 6.1 International Conference, FMOODS 2010 and 30th IFIP WG 6.1 International Conference, FORTE 2010, Amsterdam, The Netherlands, June 7-9,*, volume 6117 of *Lecture Notes in Computer Science*, pages 32–46. Springer, 2010.

[D-C125] Ananda Basu, Saddek Bensalem, Marius Bozga, Benoît Delahaye, Axel Legay, and Emmanuel Sifakis. Verification of an afdx infrastructure using simulations and probabilities. In *Runtime Verification - First International Conference, RV 2010, St. Julians, Malta, November 1-4, 2010. Proceedings*, volume 6418 of *Lecture Notes in Computer Science*, pages 330–344. Springer, 2010.

[D-C126] Saddek Bensalem, Doron Peled, and Joseph Sifakis. Knowledge based scheduling of distributed systems. In Zohar Manna and Doron Peled, editors, *Time for Verification, Essays in Memory of Amir Pnueli*, volume 6200 of *Lecture Notes in Computer Science*, pages 26–41. Springer, 2010.

[D-C127] Joseph Sifakis. Component-based construction of heterogeneous real-time systems in BIP. In Sebastian Nanz, editor, *The Future of Software Engineering*, page 150. Springer, 2010.

[D-C128] Marius Bozga, Radu Iosif, and Filip Konečný. Fast acceleration of ultimately periodic relations. In Tayssir Touili, Byron Cook, and Paul Jackson, editors, *Computer Aided Verification, 22nd International Conference, CAV 2010, Edinburgh, UK, July 15-19, 2010. Proceedings*, volume 6174 of *Lecture Notes in Computer Science*, pages 227–242. Springer, 2010.

[D-C129] Tesnim Abdellatif, Jacques Combaz, and Joseph Sifakis. Model-based implementation of real-time applications. In Luca P. Carloni and Stavros Tripakis, editors, *Proceedings of the 10th International conference on Embedded software, EMSOFT 2010, Scottsdale, Arizona, USA, October 24-29, 2010*, pages 229–238. ACM, 2010.

[D-C130] Borzoo Bonakdarpour, Marius Bozga, Mohamad Jaber, Jean Quilbeuf, and Joseph Sifakis. From high-level component-based models to distributed implementations. In Luca P. Carloni and Stavros Tripakis, editors, *Proceedings of the 10th International conference on Embedded software, EMSOFT 2010, Scottsdale, Arizona, USA, October 24-29, 2010*, pages 209–218. ACM, 2010.

[D-C131] Joseph Sifakis. Embedded systems design - scientific challenges and work directions. In Roderick Bloem and Natasha Sharygina, editors, *Proceedings of 10th International Conference on Formal Methods in Computer-Aided Design, FMCAD 2010, Lugano, Switzerland, October 20-23*, page 11. IEEE, 2010.

[D-C132] Jérémie Tharaud, Sven Wohlgemuth, Isao Echizen, Noboru Sonehara, Günter Müller, and Pascal Lafourcade. Privacy by data provenance with digital watermarking - a proof-of-concept implementation for medical services with electronic health records. In Isao Echizen, Jeng-Shyang Pan, Dieter W. Fellner, Alexander Nouak, Arjan Kuijper, and Lakhmi C. Jain, editors, *Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2010), Darmstadt, Germany, 15-17 October, 2010, Proceedings*, pages 510–513. IEEE Computer Society, 2010.

[D-C133] Axel Legay, Benoît Delahaye, and Saddek Bensalem. Statistical model checking: An overview. In Howard Barringer, Ylies Falcone, Bernd Finkbeiner, Klaus Havelund, Insup Lee, Gordon Pace, Grigore Rosu, Oleg Sokolsky, and Nikolai Tillmann, editors, *Runtime Verification - First International Conference, RV 2010, St. Julians, Malta, November 1-4, 2010. Proceedings*, volume 6418 of *Lecture Notes in Computer Science*, pages 122–135. Springer, 2010.

[D-C134] Borzoo Bonakdarpour, Marius Bozga, Mohamad Jaber, Jean Quilbeuf, and Joseph Sifakis. Automated conflict-free distributed implementation of component-based models. In *IEEE Fifth International Symposium on Industrial Embedded Systems - SIES 2010, University of Trento, Italy, July 7-9, 2010*, pages 108–117. IEEE, 2010.

[D-C135] Vassiliki Sfyrla, Georgios Tsiligiannis, Iris Safaka, Marius Bozga, and Joseph Sifakis. Compositional translation of simulink models into synchronous BIP. In *IEEE Fifth International Symposium on Industrial Embedded Systems - SIES 2010, University of Trento, Italy, July 7-9, 2010*, pages 217–220. IEEE, 2010.

[D-C136] Ananda Basu, Borzoo Bonakdarpour, Marius Bozga, and Joseph Sifakis. Systematic correct construction of self-stabilizing systems: A case study. In Shlomi Dolev, Jorge Arturo Cobb, Michael J. Fischer, and Moti Yung, editors, *Stabilization, Safety, and Security of Distributed Systems - 12th International Symposium, SSS 2010, New York, NY, USA, September 20-22, 2010. Proceedings*, volume 6366 of *Lecture Notes in Computer Science*, pages 4–18. Springer, 2010.

[D-C137] Joseph Sifakis. Embedded systems design - scientific challenges and work directions. In Javier Esparza and Rupak Majumdar, editors, *Tools and Algorithms for the Construction and Analysis of Systems, 16th International Conference, TACAS 2010, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2*, volume 6015 of *Lecture Notes in Computer Science*, page 1. Springer, 2010.

[D-C138] Ylies Falcone, Jean-Claude Fernandez, Thierry Jéron, Hervé Marchand, and Laurent Mounier. More testable properties. In Alexandre Petrenko, Adenilso da Silva Simão, and José Carlos Maldonado, editors, *Proceedings of ICTSS - 22nd IFIP WG 6.1 International Conference*, volume 6435 of *Lecture Notes in Computer Science*, pages 30–46, Natal, Brazil, November 2010. Springer. (best paper award).

[D-C139] Susanne Graf, Doron Peled, and Sophie Quinton. Achieving distributed control through model checking. In Tayssir Touili, Byron Cook, and Paul Jackson, editors, *Computer Aided Verification, 22nd International Conference, CAV 2010, Edinburgh, UK, July 15-19, 2010. Proceedings*, volume 6174 of *Lecture Notes in Computer Science*, pages 396–409. Springer, 2010.

[D-C140] Jad Hamza, Barbara Jobstmann, and Viktor Kuncak. Synthesis for regular specifications over unbounded domains. In *Conference on Formal Methods in Computer Aided Design, FMCAD 2010, Lugano, CH*, 2010.

[D-C141] Daniel Le Métayer, Manuel Maarek, Eduardo Mazza, Marie-Laure Potet, Stéphane Frénot, Valérie Viet Triem Tong, Nicolas Craipeau, and Ronan Hardouin. Liability in software engineering. In Jef Kramer and Judith Bishop, editors, *ICSE 2010, International Conference on Software Engineering*. IEEE, 2010.

[D-C142] Gilles Barthe, Marion Daubignard, Bruce M. Kapron, and Yassine Lakhnech. Computational indistinguishability logic. In *ACM Conference on Computer and Communications Security*, pages 375–386, 2010.

[D-C143] Gilles Barthe, Marion Daubignard, Bruce M. Kapron, Yassine Lakhnech, and Vincent Laporte. On the equality of probabilistic terms. In Edmund M. Clarke and Andrei Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning - 16th International Conference, LPAR-16, Dakar, Senegal, April 25-May 1, 2010, Revised Selected Papers*, volume 6355 of *Lecture Notes in Computer Science*, pages 46–63. Springer, 2010.

[D-C144] Dumitru Ceara, Laurent Mounier, and Marie-Laure Potet. Taint dependency sequences: A characterization of insecure execution paths based on input-sensitive cause sequences. In *ICSTW '10: Proceedings of the 2010 Third International Conference on Software Testing, Verification, and Validation Workshops*, pages 371–380, Washington, DC, USA, 2010. IEEE Computer Society.

[D-C145] Sanjay Rawat and Laurent Mounier. An evolutionary computing approach for hunting buffer overflow vulnerabilities: A case of aiming in dim light. In *Proceedings of 6th EC2ND (European Conference on Computer Network Defense*, Berlin, Germany, 2010. IEEE Computer Society.

[D-C146] Eduardo Mazza, Marie-Laure Potet, and Daniel Le Métayer. A formal framework for specifying and analyzing logs as electronic evidence. In *13th Brazilian Symposium of Formal Methods (SBMF)*. LNCS, 2010.

[D-C147] Daniel Le Métayer, Eduardo Mazza, and Marie-Laure Potet. Designing log architecture for legal evidence. In *Software Engineering And Formal Methods (SEFM)*, 2010.

[D-C148] Jean-François Monin. Proof trick: Small inversions. In Yves Bertot, editor, *Second Coq Workshop*, Royaume-Uni Edinburgh, July 2010. Yves Bertot.

[D-C149] Mohamed Yassin Chkouri and Marius Bozga. Prototyping of distributed embedded systems using aadl. In *Model Based Architecting and Construction of Embedded Systems ACES-MB*, pages 65–79, Denver, USA, October 2009. http://sunsite.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-507/paper06.pdf.

[D-C150] Matthieu Anne, Ruan He, Tahar Jarboui, Marc Lacoste, Olivier Lobry, Guirec Lorant, Maxime Louvel, Juan Navas, Vincent Olive, Juraj Polakovic, Marc Poulhiès, Jacques Pulou, Stéphane Seyvoz, Julien Tous, and Thomas Watteyne. Think: View-based support of non-functional properties in embedded systems. In *ICESS '09: Proceedings of the 2009 International Conference on Embedded Software and Systems*, pages 147–156, Washington, DC, USA, 2009. IEEE Computer Society.

[D-C151] Ramzi Ben Salah, Marius Bozga, and Oded Maler. Compositional timing analysis. In *EMSOFT*, 2009.

[D-C152] Saddek Bensalem, Marius Bozga, Thanh-Hung Nguyen, and Joseph Sifakis. D-finder: A tool for compositional deadlock detection and verification. In Ahmed Bouajjani and Oded Maler, editors, *Computer Aided Verification, 21st International Conference, CAV 2009, Grenoble, France, June 26 - July 2, 2009. Proceedings*, volume 5643 of *Lecture Notes in Computer Science*, pages 614–619. Springer, 2009.

[D-C153] Imene Ben-Hafaiedh, Olivier Constant, Susanne Graf, and Riadh Robbana. A model-based design and validation approach with the OMEGA-UML profile and the IF toolset. In *2nd Mediterranean Conference on Intelligent Systems and Automation, CISA 2009, March 23-25, Zarzis, Tunesia*, volume 1107 of *AIP Conference Proceedings*. American Institut of Physics, 2009.

[D-C154] Sophie Quinton, Imene Ben-Hafaiedh, and Susanne Graf. From orchestration to choreography: Memoryless and distributed orchestrators. In *Proc. of FLACOS'09*, 2009.

[D-C155] Roderick Bloem, Karin Greimel, Thomas A. Henzinger, and Barbara Jobstmann. Synthesizing robust systems. In *Proceedings of 9th International Conference on Formal Methods in Computer-Aided Design, FMCAD 2009, 15-18 November 2009, Austin, Texas, USA*, pages 85–92, 2009.

[D-C156] Jan Olaf Blech and Benjamin Grégoire. Using checker predicates in certifying code generation. In *Workshop on Compiler Optimization meets Compiler Verification (COCV)*, 2009.

[D-C157] Jan Olaf Blech, Thanh-Hung Nguyen, and Michael Périn. Invariants and robustness of BIP models. In *Workshop on Invariant Generation (WING)*, 2009.

[D-C158] Jan Olaf Blech and Michael Périn. Certifying deadlock-freedom for BIP models. In *Software and Compilers for Embedded Systems (SCOPES)*, 2009.

[D-C159] Marius Bozga, Mohamad Jaber, and Joseph Sifakis. Source-to-source architecture transformation for performance optimization in BIP. In *IEEE Fourth International Symposium on Industrial Embedded Systems - SIES 2009, Ecole Polytechnique Federale de Lausanne, Switzerland, July 8 - 10, 2009*, pages 152–160. IEEE, 2009.

[D-C160] Cas J. F. Cremers, Pascal Lafourcade, and Philippe Nadeau. Comparing state spaces in automatic protocol analysis. In *Formal to Practical Security*, volume 5458/2009 of *Lecture Notes in Computer Science*, pages 70–94. Springer Berlin / Heidelberg, 2009.

[D-C161] Cas J. F. Cremers, Pascal Lafourcade, and Philippe Nadeau. Comparing state spaces in automatic security protocol analysis. In Véronique Cortier, Claude Kirchner, Mitsuhiro Okada, and Hideki Sakurada, editors, *Formal to Practical Security - Papers Issued from the 2005-2008 French-Japanese Collaboration*, volume 5458 of *Lecture Notes in Computer Science*, pages 70–94. Springer, 2009.

[D-C162] Joseph Sifakis. Component-based construction of heterogeneous real-time systems in bip. In Giuliana Franceschinis and Karsten Wolf, editors, *Applications and Theory of Petri Nets, 30th International Conference, PETRI NETS 2009, Paris, France, June 22-26, 2009. Proceedings*, volume 5606 of *Lecture Notes in Computer Science*, page 1. Springer, 2009.

[D-C163] Ananda Basu, Saddek Bensalem, Doron Peled, and Joseph Sifakis. Priority scheduling of distributed systems based on model checking. In Ahmed Bouajjani and Oded Maler, editors, *Computer Aided Verification, 21st International Conference, CAV 2009, Grenoble, France, June 26 - July 2, 2009. Proceedings*, volume 5643 of *Lecture Notes in Computer Science*, pages 79–93. Springer, 2009.

[D-C164] Marius Bozga, Peter Habermehl, Radu Iosif, Filip Konečný, and Tomás Vojnar. Automatic verification of integer array programs. In Oded Maler Ahmed Bouajjani, editor, *Computer Aided Verification, 21st International Conference, CAV 2009, Grenoble, France, June 26 - July 2, 2009. Proceedings*, volume 5643 of *Lecture Notes in Computer Science*, pages 157–172. Springer, 2009.

[D-C165] Joseph Sifakis. Component-based construction of real-time systems in BIP. In Ahmed Bouajjani and Oded Maler, editors, *Computer Aided Verification, 21st International Conference, CAV 2009, Grenoble, France, June 26 - July 2, 2009. Proceedings*, volume 5643 of *Lecture Notes in Computer Science*, pages 33–34. Springer, 2009.

[D-C166] Joseph Sifakis. Embedded systems design - scientific challenges and work directions. In *Design, Automation and Test in Europe, DATE 2009, Nice, France, April 20-24, 2009*, page 2. IEEE, 2009.

[D-C167] Marius Bozga, Vassiliki Sfyrla, and Joseph Sifakis. Modeling synchronous systems in BIP. In Nicolas Halbwachs Samarjit Chakraborty, editor, *Proceedings of the 9th ACM & IEEE International conference on Embedded software, EMSOFT 2009, Grenoble, France, October 12-16, 2009*, pages 77–86. ACM, 2009.

[D-C168] Cristian Ene, Yassine Lakhnech, and Van Chan Ngo. Formal indistinguishability extended to the random oracle model. In Michael Backes and Peng Ning, editors, *Computer Security - ESORICS 2009, 14th European Symposium on Research in Computer Security, Saint-Malo, France, September 21-23, 2009. Proceedings*, volume 5789 of *Lecture Notes in Computer Science*, pages 555–570. Springer, 2009.

[D-C169] Joseph Sifakis. The quest for correctness-beyond a posteriori verification. In Corina S. Pasareanu, editor, *Model Checking Software, 16th International SPIN Workshop, Grenoble, France, June 26-28, 2009. Proceedings*, volume 5578 of *Lecture Notes in Computer Science*, page 4. Springer, 2009.

[D-C170] Marius Bozga, Codruta Gîrlea, and Radu Iosif. Iterating octagons. In Stefan Kowalewski and Anna Philippou, editors, *Tools and Algorithms for the Construction and Analysis of Systems, 15th International Conference, TACAS 2009, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2*, volume 5505 of *Lecture Notes in Computer Science*, pages 337–351. Springer, 2009.

[D-C171] Ananda Basu, Borzoo Bonakdarpour, Marius Bozga, and Joseph Sifakis. Brief announcement: Incremental component-based modeling, verification, and performance evaluation of distributed reset. In Idit Keidar, editor, *Distributed Computing, 23rd International Symposium, DISC 2009, Elche, Spain, September 23-25, 2009. Proceedings*, volume 5805 of *Lecture Notes in Computer Science*, pages 174–175. Springer, 2009.

[D-C172] Radu Iosif and Adam Rogalewicz. Automata-based termination proofs. In Sebastian Maneth, editor, *Implementation and Application of Automata, 14th International Conference, CIAA 2009, Sydney, Australia, July 14-17, 2009. Proceedings*, volume 5642 of *Lecture Notes in Computer Science*, pages 165–177. Springer, 2009.

[D-C173] Ylies Falcone, Jean-Claude Fernandez, and Laurent Mounier. Runtime verification of safety progress properties. In *Runtime Verification 2009*, Lecture Notes in Computer Science, Grenoble, France, June 2009.

[D-C174] Ylies Falcone, Jean-Claude Fernandez, and Laurent Mounier. Enforcement monitoring wrt. the safety-progress classification of properties. In *Proceedings of the 24th Annual ACM Symposium on Applied Computing - Software Verification and Testing Track*, 2009.

[D-C175] Martin Gagne, Pascal Lafourcade, Yassine Lakhnech, and Reihaneh Safavi. Automated proofs for encryption modes. In Ralf Kuesters, editor, *Workshop on Formal and Computational Cryptography, (FCC'09)*, Port Jefferson NY, USA, July 2009.

[D-C176] Martin Gagne, Pascal Lafourcade, Yassine Lakhnech, and Safavi Reihaneh. Automated proofs for encryption modes. In *13th Annual Asian Computing Science Conference Focusing on Information Security and Privacy: Theory and Practice (ASIAN0'9)*, Urumqi, China, October 2009.

[D-C177] Mohamed Yassin Chkouri and Marius Bozga. Deterministic data flow communication in aadl. In *ICESS '09: Proceedings of the 2009 International Conference on Embedded Software and Systems*, pages 93–100, Hangzhou, Zhejiang P.R. CHINA, May 2009. IEEE Computer Society.

[D-C178] Pascal Lafourcade, Vanessa Terrade, and Sylvain Vigier. Comparison of cryptographic verification tools dealing with algebraic properties. In Joshua Guttman and Pierpaolo Degano, editors, *sixth International Workshop on Formal Aspects in Security and Trust, (FAST'09)*, Eindhoven, Netherlands, November 2009.

[D-C179] Roderick Bloem, Krishnendu Chatterjee, Thomas A. Henzinger, and Barbara Jobstmann. Better quality in synthesis through quantitative objectives. In Ahmed Bouajjani and Oded Maler, editors, *Computer Aided Verification, 21st International Conference, CAV 2009, Grenoble, France, June 26 - July 2, 2009. Proceedings*, volume 5643 of *Lecture Notes in Computer Science*, pages 140–156. Springer, 2009.

[D-C180] Thomas A. Henzinger, Barbara Jobstmann, and Verena Wolf. Formalisms for specifying markovian population models. In Olivier Bournez and Igor Potapov, editors, *Reachability Problems, 3rd International Workshop, RP 2009, Palaiseau, France, September 23-25, 2009. Proceedings*, volume 5797 of *Lecture Notes in Computer Science*, pages 3–23. Springer, 2009.

[D-C181] Dirk Fahland, Cédric Favre, Barbara Jobstmann, Jana Koehler, Niels Lohmann, Hagen Völzer, and Karsten Wolf. Instantaneous soundness checking of industrial business process models. In Umeshwar Dayal, Johann Eder, Jana Koehler, and Hajo A. Reijers, editors, *Business Process Management, 7th International Conference, BPM 2009, Ulm, Germany, September 8-10, 2009. Proceedings*, volume 5701 of *Lecture Notes in Computer Science*, pages 278–293. Springer, 2009.

[D-C182] Sreekanth Malladi and Pascal Lafourcade. Prudent engineering practices to prevent type-flaw attacks under algebraic properties. In Hubert Comon-Lundh and Catherine Meadows, editors, *Workshop on Security and Rewriting Techniques, (SecReT'09)*, Port Jefferson NY, USA, July 2009.

[D-C183] Iman Narasamdya and Michael Périn. "certfication of smart-card applications in common criteria: Proving representation correspondences". In *Fundamental Approaches to Software Engineering*, volume 5503 of *LNCS*, pages 309–324. Springer-Verlag, 2009. (FASE'09).

[D-C184] Iman Narasamdya and Michael Périn. "certfication of smart-card applications in common criteria". In *ACM Symposium on Applied Computing*, pages 601–608. ACM Press, 2009. (SAC'09).

[D-C185] Iulian Ober, Stefan Van Baelen, Susanne Graf, Mamoun Filali, Thomas Weigert, and Sébastien Gérard. Model based architecting and construction of embedded systems. In Michel Chaudron, editor, *Models in Software Engineering, Workshops and Symposia at MODELS 2008, Toulouse, France, September 28 - October 3, 2008. Reports and Revised Selected Papers*, volume 5421 of *Lecture Notes in Computer Science*, pages 1–4. Springer, 2009.

D.3.1.3 Books, Book Chapters and edited proceedings

[D-B1] Susanne Graf, Roberto Passerone, and Sophie Quinton. Contract-based reasoning for component systems with rich interactions. In *Embedded Systems Development*, pages 139–154. Springer New York, 2014.

[D-B2] Hubert Garavel and Susanne Graf. *Formal Methods for Safe and Secure Computers Systems - BSI Study 875*. BSI German Federal Office for Information Security, 2013.

[D-B3] Iulian Ober, Florian Noyrit, Susanne Graf, and Gabor Karsai, editors. *Proceedings of the 6th International Workshop on Model Based Architecting and Construction of Embedded Systems co-located with ACM/IEEE 16th International Conference on Model Driven Engineering Languages and Systems (MoDELS 2013), Miami, Florida, USA, September 29th, 2013*, volume 1084 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2013.

[D-B4] Marius Bozga, Georgios Chasapis, Vassilios Dimakopoulos, and Aggelis Aggelis. *Smart Multicore Embedded Systems*, chapter Image processing: Object Recognition. Springer, 2013.

[D-B5] Stéphane Devismes, Pascal Lafourcade, and Michel Levy. *Informatique théorique : Logique et démonstration automatique, Introduction à la logique propositionnelle et à la logique du premier ordre*. Ellipses, Technosup, 2012.

[D-B6] Marieke Huisman, Barbara Jobstmann, Ina Schaefer, and Mariëlle Stoelinga. Divide and conquer: the quest for compositional design and analysis (dagstuhl seminar 12511). Technical Report 12, Dagstuhl Reports, 2012.

[D-B7] Joaquín García-Alfaro and Pascal Lafourcade, editors. *Foundations and Practice of Security - 4th Canada-France MITACS Workshop, FPS 2011, Paris, France, May 12-13, 2011, Revised Selected Papers*, volume 6888 of *Lecture Notes in Computer Science*. Springer, 2012.

[D-B8] Satnam Singh, Barbara Jobstmann, Michael Kishinevsky, and Jens Brandt, editors. *9th IEEE/ACM International Conference on Formal Methods and Models for Codesign, MEMOCODE 2011, Cambridge, UK, 11-13 July, 2011*. IEEE, 2011.

[D-B9] Klaus Schneider, Barbara Jobstmann, Luca P. Carloni, and Jens Brandt. Message from the chairs. In *8th ACM/IEEE International Conference on Formal Methods and Models for Codesign (MEMOCODE 2010), Grenoble, France, 26-28 July 2010*, pages 1–3. IEEE Computer Society, 2010.

[D-B10] Sylvain Boulmé and Marie-Laure Potet. Relaxing restrictions on invariant composition in the B method by ownership control à la Spec#. In *Rigorous Methods for Software Construction and Analysis*. Springer Berlin / Heidelberg, 2009.

[D-B11] Cormac Flanagan, Susanne Graf, Madhusan Parthasarathy, and Shaz Quadeer, editors. *Dagstuhl Seminar on Design and Validation of Concurrent Systems*, volume 09361 of *Dagstuhl Seminar Series – Abstract collection*, September 2009.

[D-B12] Stefano Berardi, Ferruccio Damiani, and Ugo de'Liguoro, editors. *Types for Proofs and Programs (International Conference TYPES 2008, Revised Selected Papers)*, volume 5497 of *LNCS*. Springer, 2009.

D.3.1.4 PhD Theses and habilitations

[D-P1] Christian von Essen. *Vérification et synthèse quantitative.* PhD thesis, Université de Grenoble, France, 2014.

[D-P2] Jean Quilbeuf. *Implantations distribuées de modèles à base de composants communicants par interactions multiparties avec priorités : application au langage BIP.* PhD thesis, Université de Grenoble, France, 2013.

[D-P3] Paraskevas Bourgos. *Rigorous Design Flow for Programming Manycore Platforms.* PhD thesis, Université de Grenoble, April 2013.

[D-P4] Emmanuel Sifakis. *Towards efficient and secure shared memory applications.* PhD thesis, Université de Grenoble, May 2013.

[D-P5] Tesnim Abdellatif. *Rigorous Implementation of Real-Time Systems.* PhD thesis, Universié de Grenoble, France, 2012.

[D-P6] Marion Daubignard. *Formal Methods For Concrete Security Proofs.* PhD thesis, Grenoble University, Jan 2012.

[D-P7] Pascal Lafourcade. *Computer-Aider Security for: Cryptographic Primitives, Voting Protocols and Wireless Sensor Networks.* Habilitation à diriger des recherches, Verimag, Grenoble, France, 11 2012. 192 pages.

[D-P8] Eduardo Sampaio Elesbao Mazza. *A Formal Framework for Specifying and Analyzing Liabilities Using Log as Digital Evidence.* PhD thesis, Université de Grenoble, Laboratoire Verimag,hal.inria.fr/hal-00789668/, 2012.

[D-P9] Artur Pietrek. *Tirex : a textual target-level intermediate representation.* PhD thesis, Université de Grenoble, October 2012.

[D-P10] Jirí Simácek. *Harnessing Forest Automata for Verification of Heap Manipulating Programs.* PhD thesis, 2012.

[D-P11] Imene Ben-Hafaiedh. *Component-based Systems: from Design to Implementation.* PhD thesis, Grenoble University, 2011.

[D-P12] Sophie Quinton. *Design, Verification and Implementation of Systems of Components.* PhD thesis, Université Joseph Fourier, VERIMAG, January 2011.

[D-P13] Vassiliki Sfyrla. *Modélisation des systèmes synchrones en BIP.* PhD thesis, Université de Grenoble, June 2011.

[D-P14] Manuel Garnacho. *Automatisation de la Certification Formelle de Systèmes Critiques par Instrumentation d'Interpréteurs Abstraits.* PhD thesis, Université de Grenoble, aout 2010.

[D-P15] Thanh-Hung Nguyen. *Constructive Verification for Component-based Systems.* PhD thesis, Universite de Grenoble, May 2010.

[D-P16] Mohamad Jaber. *Implémentations Centralisée et Répartie de Systèmes Corrects par construction á base des Composants par Transformations Source-á-source dans BIP.* PhD thesis, Université Joseph-Fourier - Grenoble I, 2010.

[D-P17] Yassin Chkouri. *Modélisation des systèmes temps-réel embarqués en utilisant AADL pour la génération automatique d'applications formellement vérifiées.* PhD thesis, Université Joseph-Fourier - Grenoble I, 2010.

[D-P18] Marius Bozga. *Component-Based Design of Real-Time Systems.* Hdr, Université Joseph-Fourier - Grenoble I, 2010.

[D-P19] Ylies Falcone. *Study and Implementation of Runtime Validation Techniques.* PhD thesis, Grenoble University, November 2009.

D.3.1.5 Other visible publications

[D-O1] Pierre Ganty and Radu Iosif. Generating bounded languages using bounded control sets. Technical report, 2014.

[D-O2] Najah Ben Said, Takoua Abdellatif, Saddek Bensalem, and Marius Bozga. Building secure-by-construction distributed component-based systems. Technical Report TR-2014-6, Verimag Research Report, 2014.

[D-O3] Radu Iosif, Adam Rogalewicz, and Jirí Simácek. The tree width of separation logic with recursive definitions. Technical report, 2013.

[D-O4] Marius Bozga, Radu Iosif, and Filip Konečný. Deciding conditional termination. Technical report, 2013.

[D-O5] Gregor Göessler, Daniel Le Métayer, Eduardo Mazza, Marie-Laure Potet, Lacramioara Astefanoaei, and Valérie Viet Triem Tong. Apport des méthodes formelles dans l'exploitation de logs informatiques dans un contexte contractuel. Actes des journées AFADL, Grenoble, 2012.

[D-O6] Pierre Ganty, Radu Iosif, and Filip Konečný. Underapproximation of procedure summaries for integer programs. Technical report, 2012.

[D-O7] Jannik Dreier, Jean-Guillaume Dumas, and Pascal Lafourcade. Attacking privacy in a fully private auction protocol, 2012.

[D-O8] Sophie Quinton and Susanne Graf. Contract-based verification of hierarchical systems of components. Technical Report TR-2009-6, Verimag Research Report, 2011. latest update in 2011.

[D-O9] Chih-Hong Cheng, Saddek Bensalem, Yu-Fang Chen, Rongjie Yan, Barbara Jobstmann, Harald Ruess, Christian Buckl, and Alois Knoll. Algorithms for synthesizing priorities in component-based systems. Technical report, CoRR, 2011.

[D-O10] Chih-Hong Cheng, Saddek Bensalem, Rongjie Yan, and Harald Ruess. Distributed priority synthesis and its applications, 2011.

[D-O11] Yuxin Deng, Stéphane Grumbach, and Jean-François Monin. Towards Verifying Declarative Netlog Protocols with Coq. Draft, 2010.

[D-O12] Sreekanth Malladi and Pascal Lafourcade. How to prevent type-flaw attacks on security protocols under algebraic properties. Technical report, VERIMAG, 2010.

[D-O13] Frédéric Blanqui, Claude Helmstetter, Vania Joloboff, Jean-François Monin, and Xiaomu Shi. Designing a CPU simulator: from a pseudo-formal document to fast code. APLAS'10, Poster session, november 2010.

[D-O14] Frédéric Blanqui, Claude Helmstetter, Vania Joloboff, Jean-François Monin, and Xiaomu Shi. SimSoC-Cert: a Certified Simulator for Systems on Chip. Draft, 09 2010.

[D-O15] Mohamad Jaber, Ananda Basu, and Simon Bliudze. Symbolic implementation of connectors in BIP. Technical report, Verimag, 2009.

[D-O16] Alexandre Maréchal and Michaël Périn. Three linearization techniques for multivariate polynomials in static analysis using convex polyhedra. Technical Report TR-2014-7, Verimag Research Report, july 2014.

[D-O17] Manuel Garnacho and Michael Périn. Automatic coq proofs generation from static analyzers by lightweight instrumentation. Technical Report TR-2011-18, Verimag Research Report, 2011.

D.3.2 DCS team: Software

IF IF is a compiler / simulator model-checker, ... for the *IF intermediate representation* extending communicating timed automata. It offers a number of front-ends for different high-level user languages (such a s SDL or UML), thus equipping these high-level languages with simulation and verification facilities.
Authors: Marius Bozga, Susanne Graf, Laurent Mounier, Jean-Claude Fernandez, Iulian Ober, Yassine Lakhnech, Joseph Sifakis
Home page: http://www-if.imag.fr/
License: Free Software for non commercial use. There exists a commercial licence agrement with Pragmadev who has adapted IF as a backend for the Pragmadev version of SDL

IFx-Omega IFx-OMEGA is a compiler / simulator / model-checker for a rich subset of UML 2.2 / SysML 1.1, based on the IF model checker. IFx-OMEGA originated in the European project IST OMEGA, and was further developed with support from other projects including IST ASSERT, ESA Activity 3-12639

and ESA FullMDE.
Authors: Susanne Graf, Iulian Ober
Home page: http://www.irit.fr/ifx/
License: Free Software for non commercial use

BIP Compiler The BIP compiler allows the generation of C++ code from BIP models. The common part of the generated code is the BIP execution engine, which implements the semantics of interactions and priorities of the BIP language. The BIP compiler is provided along with various execution engines (reference, optimized, multi-thread).
Authors: Jacques Combaz, Marc Poulhiès, Ananda Basu, Marius Bozga, Anakreontas Mentis
Home page: http://www-verimag.imag.fr/New-BIP-tools.html
License: Free Software for non commercial use.

SBIP SBIP is a Statistical Model Checking engine for the BIP framework. It allows for verification of quantitative properties - expressed as Probabilistic Bounded LTL (PBLTL) formulas - on stochastic BIP models. The tool implements two important statistical methods, namely, hypothesis testing and parameter estimation as its core parts. Moreover, it provides a front-end for PBLTL formula syntactic validation and a monitoring module for the input formulas. The tool runs currently in command line mode. It takes as input a BPLTL formula, a confidence level for the statistical tests, and a stochastic BIP model binary.
Authors: Ayoub Nouri
Home page: http://www-verimag.imag.fr/Statistical-Model-Checking.html
License: Free Software for non commercial use.

D-Finder D-Finder allows for verification of safety properties and deadlock-freedom for component-based systems described in BIP. D-Finder implements several, compositional and/or incremental, invariant generation methods. Invariants provides symbolic over-approximations of the set of reachable states. Whenever the properties cannot be proved, D-Finder provides strategies for spurious counter example elimination based on symbolic state space exploration.
Authors: Saddek Bensalem, Marius Bozga, Thanh-Hung Nguyen, Andreas Griesmayer, Ouri Maler, Lacramioara Astefanoaiei, Souha Ben-Rayana
Home page: http://www-verimag.imag.fr/dfinder
License: Free Software for non commercial use.

STAC STAC is a Frama-C plugin implementing a static taint analysis calculus for C programs. From set of input functions, it extracts from the program Control Flow Graph a set of *taint dependency sequences* (TDS), expliciting control and data dependencies between user inputs and a given set of vulnerable statements. These TDS can be used as security test objectives.
Authors: Dumitru Ceara, Marie-Laure Potet, Laurent Mounier
Home page: https://code.google.com/p/tanalysis
License: Free Software for non commercial use.

LiSTT Like STAC, LiSTT also implements an inter-procedural static taint analysis calculus, but operating directly on disassembled binary code. Given a set of input functions and vulnerable statements it extracts a "program chop" as the set of functions able to transmit data flows from input sources to vulnerable functions.
Authors: Sanjay Rawat, Marie-Laure Potet, Laurent Mounier
Not distributed outside Verimag.

Lazart Lazart is a test-oriented evaluation tool for the robustness of software against fault injection attacks. Starting from an LLVM software description and an attack objective, it produces a complete set of symbolic test cases on a mutated version of the LLVM code, with respect to a given fault model. Executing these test cases indicates where fault injections are required to fulfill the attack objective.
Authors: Marie-Laure Potet, Laurent Mounier, Louis Dureuil, Maxime Puys
Not distributed outside Verimag.

Flata FLATA is a toolset for the manipulation and the analysis of non-deterministic integer programs (also known as counter automata). The main functionalities of FLATA are: (i) reachability analysis of non-recursive programs - checking if an error control state is reachable, (ii) termination analysis of non-recursive programs - computation of termination preconditions, (iii) computation of summaries of recursive programs
Authors: Filip Konecny, Radu Iosif, Marius Bozga
Home page: http://nts.imag.fr/index.php/Flata
License: Free Software for non commercial use.

Slide SLIDE is a prototype tool for checking entailment in Separation Logic with user-provided inductive definitions of recursive data structures (lists, trees, and beyond).
Authors: Adam Rogalewicz, Radu Iosif, Tomas Vojnar
Home page: http://www.fit.vutbr.cz/research/groups/verifit/tools/slide/
License: Free Software for non commercial use.

D.3.3 DCS team: Scientific influence

1. Grants (for details see in Annex E): ANR BINSEC, FP7 CYPHERS, FP7 DMILS, BGLE MANY-CORELABS, ANR PROSE, ANR VERIDYC, FP7 ASCENS, FP7 CERTAINTY, BGLE ACOSE, FUI CHAPI, ANR EQINOCS, Industrial Cyberio, ARTEMIS ACROSS, Industrial Kalray, ANR LISE, Minalogic SHIVA, ANR SCALP, FP7 PRO3D, ARTEMIS SMECY, Industrial FullMDE, ANR AVOTE, ANR SFINCS, Minalogic MINDS, CIFRE Pietrek, IP SPEEDS, Industrial OMEGA-4-Rhapsody, FP7 Combest, Industrial Sympaa, ARC Inria CeProMi, ANR OpenEmbeDD, ANR EDEN2, FP7 GENESYS.

2. Academic collaborations. We maintain regular collaborations and publish papers with the following academic partners:
   - on BIP and component-based design: Axel Legay (INRIA, Rennes), Borzoo Bonakdarpour (Waterloo Univ.), Simon Bliudze, David Atienza (EPFL, Lausanne), Lothar Thiele (ETH, Zurich), Harald Ruess, Chih-Hong Cheng (Fortiss, Munich), Martin Wirsing (LMU, Munich), Klaus Havelund (NASA JPL), Ylies Falcone (LIG, Grenoble), Rongjie Yan (CAS, Beijing), Paul Attie, Mohamad Jaber (AUB, Lebanon), Kim G. Larsen (Univ. Aalborg), Alberto-Sangiovanni Vincentelli, Ed Lee, Stavros Tripakis (Berkeley), Roberto Passerone (Trento Univ.), Doron Peled (Bar-Ilan Univ.), Rocco De Nicola (IMT Lucca), Sanjoy Baruah (Univ. North Carolina), Panagiotis Katsaros (Thessaloniki Univ.)
   - on security: Bruce Kapron (University of Victoria), Rei Safavi-Naini (University of Calgary), Rance DeLong (The Open Group), Takoua Abdellatif (Sousse Univ.), Gilles Barthe (IMDEA, Madrid), Lilia Sfaxi (Tunis), Roland Groz (LIG, Grenoble), ...
   - on software verification: Pierre Ganty (IMDEA, Madrid), Filip Konecny (EPFL, Lausanne), Adam Rogalewicz (Brno), Ahmed Bouajjani and Peter Habermehl (LIAFA, Paris), Thomas Vojnar (Brno), Hossein Hojjat (Cornell), Frédéric Blanqui and Vania Joloboff (INRIA LIAMA, Beijing) ...
   - on model-based verification, contracts, distribution and synthesis: Doron Peled (Bar Ilan University), Tom Henzinger, Krishnendu Chatterjee (IST, Austria), Andread Griesmayer (Imperial College London), Axel Legay (Irisa Rennes), Roberto Passerone (Trento, Italie), Sophie Quinton et Hubert Garavel (INRIA Montbonnot), Iulian Ober (IRIT, Toulouse), Dimitra Giannakopoulou (NASA Ames), Bertrand Meyer (ETH Zurich)

3. Events organisation
   - S. Bensalem was General chair of the European joint conference on Theory and Practice of Software (ETAPS 2014), that took place in Grenoble from 5 to 13 April 2014.
   - S. Bensalem was co-organizer of the workshop CPS20: Cyber-Physical Systems 20 years from now - visions and challenges, affiliated to CPSWeek 2014, Berlin, Germany, April 14 2014.
   - S. Bensalem and Y. Lakhnech co-organized (with Axel Legay) of the workshop From Programs to Systems - The Systems Perspective in Computing, in honor of Joseph Sifakis, Grenoble April 6 2014 ("http ://www.etaps.org/index.php/2014/workshops").
   - R. Iosif organized the Alpine Verification Meeting, Frejus May 12-14, 2014.

- S. Graf co-organized the Int. Workshop on Model Based Architecting and Construction of Embedded Systems ACES^{MB} that is affiliated with the MODELS conference in 2013, 2010 and 2008
- J-F. Monin was Co-organizer of the 5th Asian-Pacific Summer School on Formal Methods (APSSFM 2013), August 5-10, 2013, Tsinghua University, Beijing.
- S. Bensalem was scientific supervisor of the summer school Cyber-Physical Systems. This school is affiliated to EIT ICT Lab "Action Line Cyber-Physical Systems 2013". the first edition in Grenoble, July 8 to 13, 2013.
- S. Bensalem was Tutorial chair at Embedded System Week in 2012 (ESWEEK 2012).
- B. Jobstmann organised (jointly with Marieke Huisman, Ina Schaefer and Marielle Stoelinga) the Dagstuhl Seminar on *Divide and Conquer: the Quest for Compositional Design and Analysis* in 2011
- S. Bensalem was Organizer and Co-PC chair (with Axel Legay) of the Int. workshop on Rigorous Embedded Design RED with EuroSys 2011 in Salzburg
- R. Iosif organized VERIDYC Verification and Synthesis in 2011 in Grenoble
- DCS co-organized the Workshop on Foundations & Practice of Security in 2011 in Paris
- S. Bensalem was organisation chair of the international conference CAV ("Computer Aided Ve rification"), Grenoble from June 26 to July 2nd 2009.
- S. Graf co-organized (jointly with Shaz Qadeer, Madhusudan Parthasarathy, and Cormac Flanagan) the Dagstuhl Seminar on *Design and Validation of Concurrent Systems* in September 2009
- DCS co-organized the 3rd International Workshop on Security and Electronic Voting, Grenoble in 2009
- DCS co-organized the 2nd Canada-France Workshop on Foundations & Practice of Security in 2009

4. Awards

- S. Sifakis was nominated *Commandeur de la Légion d'honneur* in 2012
- S. Sifakis became member of the French Academie of Science in 2011
- Most Influential Paper Award of the first 10 years of SEFM for [BBS06] at SEFM 2013.
- Best Student Paper Award for [**D-C60**] at SC 2012.
- Best Paper Award for [**D-C112**] at Rapido 2011.
- Best Paper Award for [**D-C111**] at IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT'11).
- Best Paper Award for [**D-C138**] at ICTSS 2010.
- Best Paper Award for [**D-C134**] at SIES 2010.
- Best Paper Award for [**D-C19**] at CADE 2013.

5. Invited conferences

- J. Sifakis has given invited talks at VLSI-Soc in 2011, in China National Computer Conference 2011, 4th Science Conclave 2011, CAV 2009, DATE 2009 and many more
- S. Graf gave invited talks at the following conferences and Summer schools: ISPDC conference in 2014 [**D-C1**], FSFMA workshop in 2014, iFM conference in 2013 [**D-C36**, **D-J1**], Marktoberdorf summerschool 2010
- B. Jobstmann has given invited talks at SIES 2011 and FDL 2010
- P. Lafourcade was invited speaker to the conference Cryptography and Security System 2012 and *Journée Nationale des Communications Terrestres*
- S. Bensalem was invited speaker at WLA 2010, MEMICS 2011, WRLA 2012
- J-F. Monin was invited speaker at *Embedded China* in 2013
- M. Bozga was invited for a talk at SEFM 2013

6. Editorial activities

- J. Sifakis is on the editorial board of FMSD
- S. Graf is on the editorial board of STTT
- S. Bensalem is member of the Steering Committee of ETAPS, since 2012, and also of the International Conference Runtime Verification (RV), since 2012.

- S. Graf is member of the Steering Committee of SPIN since 2003 and of ACES^{MB} since its first edition in 2008.
- B. Jobstmann co-chaired the PC of MEMOCODE in 2010 [D-B9] and in 2011,
- M. Bozga was Co-PC chair of FORMATS (with Axel Legay) in 2014
- S.Bensalem was Co-PC chair of the topic E3 : Model-based Design and Verification for Embedded Systems of the international conferences DATE 2011, 2012, 2013 and 2014.
- S. Bensalem was Co-PC chair of RV'13 (with Axel Legay) and of RV'09 (with Doron Peled), and of the Int. workshop on Validation and Verification for Planning and Scheduling VVPS'XX and VVPS 2011
- S. Bensalem was guest co-editor of a special issue of STTT on "Verification and validation meet planning and scheduling" 2013 (http://link.springer.com/article/10.1007/s10009-013-0294-x). and on on "Rigorous Embedded Design" June 2013 (http://link.springer.com/article/10.1007/s10009-013-0271-4)
- S. Bensalem and Y. Lakhnech co-edited a special issue in honor of Joseph Sifakis, LNCS book, April 2014.

7. Evaluation activities

- The members of DCS participated in the following Program Committees:
  2014: TACAS, DATE, FORTE, iFM, RV, RP, Hotspot, CSS
  2013: TACAS, DATE, FORTE, RV, VECoS, ATVA, CBSE, GreHack, Maroc
  2012: TACAS, DATE, FORTE, RV, VECoS, ATVA, TOOLS, ICTAC, TCS, FM, FORMATS, M2A2, MEMOCODE, LPAR, SIES, FPS, AFRICACRYPT, GreHack
  2011: CAV, FORMATS, DATE, RV, FASE, VECoS, ATVA, SPIN, FORTE, TASE, SDL-Forum, MEMOCODE, FMCAD, IWIGP, SETOP
  2010: TACAS, SAS, VMCAI, EMSOFT, DATE, ABZ, FORTE, RV, VECoS, ATVA, VSTTE, TASE, MEMOCODE, FMICS, FMCAD, FPS, SIS
  2009: CAV, VMCAI, ATVA, FORTE, ACSD, RV, MODELS, SPIN, ICTAC, CIAA, VECoS, MEMOCODE, FPS, VOTE
- S. Graf has been member of the evaluation panel of several national and international research agencies: The German Research Agency DFG for an Excellence intiative in 2011, the Swedish Research Council VR for projects calls in 2013-14, the Portuguese Research Ageny FCT for call for PhD schools in 2014 and the IDEX Sorbonne-Paris-Nord for a project call.
- S. Bensalem was expert for the AERES in 2013, the Netherlands Organisation for Scientific Research in 2012, the Israel Science Fondation in 2010, and the Austrian Science Fund in 2010.
- S. Graf has been the reviewer of the European STREP project CONNECT for the overall duration of the project (2010-2013)
- S. Graf has been an expert for evaluating grant proposals or promotions or for participating in hiring committees for the Belgian API (2010), the Netherlands NWO (2011, 2012), the Swiss SNF (2012), the Austrian FWF (2012), DFG (1 or 2 grants per year), University of Uppsala (2009), University of Lugano (2011), KTH (2012) and Chalmers Goeteborg (2012, 2013). And also for AERES.
- Several members of DCS are regularly and frequently involved in the local and hiring committees (UJF, Grenoble INP) and at national level.

8. Administrative activities

- Y. Lakhnech is a research vice director of UJF
- J-C Fernandez has been the dean of the CS department (director of IM2AG) in 2009-11 and a vice director of UJF (CEVU) from 2011 to 2013
- S. Graf is member of the scientific committee of IM2AG
- J. Sifakis was the coordinator of the NoE ARTIST, ARTIST and ARTIST DEsign from 2006 to 2012 and S. Graf was the coordinator of the Modelling activities in this NoE
- J. Sifakis has been the director of CRI PILSI

D.3.4 DCS team: Interaction with the economic, social and cultural environment

- Industrial contracts: During the period 2009-2014, the members of the DCS group engaged in collaborations with several industrial partners.
  - **EdF R&D**: During the VERIDYC project, EDF R&D conducted the assessment of the tools produced by the other project members (VERIMAG, LIAFA, LSV, CEA)
  - **MathWorks**: A former post-doc of the group, Florent Garnier, was hired for his experience developed during the VERIDYC project
  - **Vupen**: expertise contract, CIFRE of Sofia Bekrar, Binsec Project
  - **orange-Labs**: ARESA2 project (in collaboration with Synchrone)
  - **Cesti-LETI**: expertise contracts, thesis of Louis Dureuil
  - **ESA**: direct research grants and participation in ESA launched collaborative projects (FullMDE, Rhapsody-4-Omega) (for details see in Annex E)
  - **Actoll**: industrial project, modeling, analysis and implementation of an embedded controller for payment with credit cards at motorways tolls, using BIP. A former post-doc of the group, Matthieu Gallien, was hired by ACTOLL.
  - **Cyberio**: industrial project, realisation of a computer-aided design tool for distributed sensor systems.
  - **CEA-LETI**: joint participation in several EU, Artemis and BGLE[15] national projects on design flows for embedded many-core platforms
  - **Thales**: joint participation in several EU and Artemis projects. Today, we have strong ties with Thales Telecommunications on managing information flow security and performance aspects for embedded applications.
  - **Kalray**: joint EU and BGLE national research projects on code generation and deployment of BIP applications on the MPPA platform. A former post-doc of the group, Marc Poulhies, was hired by Kalray.
  - **Magillem**: joint participation to BGLE projects. A former PhD student of the group, Tesnim Abdellatif, was hired by Magillem.
  - **GMV**: industrial project on development of sofware architectures for autonomous systems (in cooperation with LAAS laboratory, Toulouse)
- Consulting
  - S. Graf has been an expert (with H. Garavel) for BSI (Bundesamt f. Sicherheit in Informationssystemen) in 2011-12 [D-B2]

D.4 Tempo team: production

D.4.1 Tempo team: Publications, by Categories

D.4.1.1 International Journals

[T-J1] Selma Saidi, Pranav Tendulkar, Thierry Lepley, and Oded Maler. Optimizing two-dimensional dma transfers for scratchpad based mpsocs platforms. *Microprocessors and Microsystems - Embedded Hardware Design*, 37(8):848–857, 2013.

[T-J2] Szymon Stoma, Alexandre Donzé, Francois Bertaux, Oded Maler, and Grégory Batt. Stl-based analysis of trail-induced apoptosis challenges the notion of type i/type ii cell line classification. *PLoS Computational Biology*, 9(5), 2013.

[T-J3] Thao Dang and Romain Testylier. Reachability analysis for polynomial dynamical systems using the Bernstein expansion. *Reliable Computing Journal, Special issue: Bernstein Polynomials in Reliable Computing*, 2012.

[T-J4] Selma Saidi, Pranav Tendulkar, Thierry Lepley, and Oded Maler. Optimizing explicit data transfers for data parallel applications on the cell architecture. *ACM Transactions on Architecture and Code Optimization, Vol. V,*, January 2012. Published in Hipeac 2012 Conference.

[15] Briques Génériques Logiciels Embarqués

[T-J5] Thao Dang and Romain Testylier. Reachability analysis for polynomial dynamical systems using the Bernstein expansion. *Reliable Computing Journal*, December 2012.

[T-J6] Oded Maler and Dejan Nickovic. Monitoring properties of analog and mixed-signal designs,. *Software Tools for Technology Transfer*, 2012.

[T-J7] Thao Dang, Colas Le Guernic, and Oded Maler. Computing reachable states for nonlinear biological models. *Theoretical Computer Science*, April 2011.

[T-J8] Alexandre Donzé, Eric Fanchon, Lucie Martine Gattepaille, Oded Maler, and Philippe Tracqui. Robustness analysis and behavior discrimination in enzymatic reaction networks. *PLOS One*, 2011.

[T-J9] Edmund M. Clarke, Alexandre Donzé, and Axel Legay. On simulation-based probabilistic model-checking of mixed-analog circuits. *Formal Methods in System Design*, 36(2):97–113, 2010.

[T-J10] Alexandre Donzé, Gilles Clermont, and Christopher James Langmead. Parameter synthesis in nonlinear dynamical systems: Application to systems biology. *Journal of Computational Biology*, 17(3):325–336, 2010.

[T-J11] Thao Dang and Tarik Nahhal. Coverage-guided test generation for continuous and hybrid systems. *Formal Methods in System Design*, 34(2):183–213, 2009.

[T-J12] Thao Dang and Tarik Nahhal. Coverage-guided test generation for continuous and hybrid systems. *Formal Methods in System Design*, 2009.

D.4.1.2 International Conferences

[T-C1] Jean-Francois Kempf, Olivier Lebeltel, and Oded Maler. Formal and informal methods for multi-core design space exploration. In *QAPL*, 2014.

[T-C2] Tommaso Dreossi and Thao Dang. Parameter synthesis for polynomial biological models. In *HSCC*, pages 233–242, 2014.

[T-C3] Oded Maler and Irini Eleftheria Mens. Learning regular languages over large alphabets. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2014)*, Grenoble, France, April 2014. LNCS.

[T-C4] Thao Dang, Bertrand Jeannet, and Romain Testylier. Verification of embedded control programs. In *Proceedings of European Control Conference ECC*, 2013.

[T-C5] Pranav Tendulkar, Peter Poplavko, and Oded Maler. Symmetry breaking for multi-criteria mapping and scheduling on multicores. In *FORMATS*, pages 228–242, 2013.

[T-C6] Romain Testylier and Thao Dang. Nltoolbox: A library for reachability computation of nonlinear dynamical systems. In Dang Van Hung and Mizuhito Ogawa, editors, *Automated Technology for Verification and Analysis - 11th International Symposium, ATVA 2013, Hanoi, Vietnam, October 15-18, 2013. Proceedings*, volume 8172 of *Lecture Notes in Computer Science*, pages 469–473. Springer, 2013.

[T-C7] Thao Dang and Tommaso Dreossi. Falsifying oscillation properties of parametric biological models. In Thao Dang and Carla Piazza, editors, *Proceedings Second International Workshop on Hybrid Systems and Biology, HSB 2013, Taormina, Italy, 2nd September 2013*, volume 125 of *EPTCS*, pages 53–67, 2013.

[T-C8] Sergiy Bogomolov, Alexandre Donzé, Goran Frehse, Radu Grosu, Taylor T Johnson, Hamed Ladan, Andreas Podelski, and Martin Wehrle. Abstraction-based guided search for hybrid systems. In *Model Checking Software*, pages 117–134. Springer Berlin Heidelberg, 2013.

[T-C9] Alexandre Donzé and Goran Frehse. Modular, hierarchical models of control systems in spaceex. In *Control Conference (ECC), 2013 European*, pages 4244–4251. IEEE, 2013.

[T-C10] Alexandre Donzé, Thomas Ferrére, and Oded Maler. Efficient robust monitoring for STL. In *CAV*, 2013.

[T-C11] Goran Frehse, Colas Le Guernic, and Rajat Kateja. Flowpipe approximation and clustering in space-time. In *HSCC*, LNCS. Springer, 2013.

[T-C12] Jean-Francois Kempf, Marius Bozga, and Oded Maler. As soon as probable: Optimal scheduling under stochastic uncertainty. In *TACAS*, 2013.

[T-C13] Oded Maler. Algorithmic analysis of continuous and hybrid systems. In *Infinity*, EPTCS, 2013.

[T-C14] Oded Maler, Adam M. Halasz, Olivier Lebeltel, and Ouri Maler. Exploring the dynamics of mass action systems. In *Hybrid Systems Biology*, volume 125 of *EPTCS*, pages 84–91, 2013.

[T-C15] Mohamed Amin Ben Sassi, Romain Testylier, Thao Dang, and Antoine Girard. Reachability analysis of polynomial systems using linear programming relaxations. In *ATVA*, pages 137–151, 2012.

[T-C16] Sergiy Bogomolov, Goran Frehse, Radu Grosu, Hamed Ladan, Andreas Podelski, and Martin Wehrle. A box-based distance between regions for guiding the reachability analysis of spaceex. In P. Madhusudan and Sanjit A. Seshia, editors, *Computer Aided Verification - 24th International Conference, CAV 2012, Berkeley, CA, USA, July 7-13, 2012 Proceedings*, volume 7358 of *Lecture Notes in Computer Science*, pages 479–494. Springer, 2012.

[T-C17] Thao Dang and Noa Shalev. State estimation and property-guided exploration for hybrid systems testing. In Brian Nielsen and Carsten Weise, editors, *Testing Software and Systems - 24th IFIP WG 6.1 International Conference, ICTSS 2012*, volume 7641 of *Lecture Notes in Computer Science*, pages 152–167. Springer, 2012.

[T-C18] Romain Testylier and Thao Dang. Analysis of parametric biological models with non-linear dynamics. In Ezio Bartocci and Luca Bortolussi, editors, *Hybrid Systems and Biology, HSB 2012*, volume 92 of *EPTCS*, pages 16–29, 2012.

[T-C19] Alexandre Donzé, Oded Maler, Ezio Bartocci, Dejan Nickovic, Radu Grosu, and Scott Smolka. On temporal logic and signal processing. In *ATVA*, 2012.

[T-C20] Goran Frehse and Rajarshi Ray. Flowpipe-guard intersection for reachability computations with support functions. In *IFAC Conf. Analysis and Design of Hybrid Systems (ADHS)*, pages 94–101, 2012.

[T-C21] Selma Saidi, Pranav Tendulkar, Thierry Lepley, and Oded Maler. Optimal 2d data partitioning for dma transfers on mpsocs. In *Proceedings of the 15th EUROMICRO Conference on Digital System Design*, 2012.

[T-C22] Thao Dang and Romain Testylier. Hybridization domain construction using curvature estimation. In *Proceedings HSCC 2011*, 2011.

[T-C23] Thao Dang and Thomas Martin Gawlitza. Template-based unbounded time verification of affine hybrid automata. In Hongseok Yang, editor, *Programming Languages and Systems - 9th Asian Symposium, APLAS 2011*, volume 7078 of *Lecture Notes in Computer Science*, pages 34–49. Springer, 2011.

[T-C24] Thao Dang and Thomas Martin Gawlitza. Discretizing affine hybrid automata with uncertainty. In Tevfik Bultan and Pao-Ann Hsiung, editors, *Automated Technology for Verification and Analysis, 9th International Symposium, ATVA 2011*, volume 6996 of *Lecture Notes in Computer Science*, pages 473–481. Springer, 2011.

[T-C25] Goran Frehse, Colas Le Guernic, Alexandre Donzé, Scott Cotton, Rajarshi Ray, Olivier Lebeltel, Rodolfo Ripado, Antoine Girard, Thao Dang, and Oded Maler. Spaceex: Scalable verification of hybrid systems. In Ganesh Gopalakrishnan and Shaz Qadeer, editors, *Proc. 23rd International Conference on Computer Aided Verification (CAV)*, LNCS. Springer, 2011.

[T-C26] Goran Frehse, Kim Guldstrand Larsen, Marius Mikucionis, and Brian Nielsen. Monitoring dynamical signals while testing timed aspects of a system. In *ICTSS*, pages 115–130, 2011.

[T-C27] Jean-Francois Kempf, Marius Bozga, and Oded Maler. Performance evaluation of schedulers in a probabilistic setting. In *FORMATS*, September 2011.

[T-C28] Eugene Asarin, Alexandre Donzé, Oded Maler, and Dejan Nickovic. Parametric identification of temporal properties. In *RV*, pages 147–160, 2011.

[T-C29] Julien Legriel, Scott Cotton, and Oded Maler. On universal search strategies for multi-criteria optimization using weighted sums. In *CEC*, Mai 2011.

[T-C30] Julien Legriel and Oded Maler. Meeting deadlines cheaply. In *ECRTS*, Mai 2011.

[T-C31] Scott Cotton, Oded Maler, Julien Legriel, and Selma Saidi. Multi-criteria optimization for mapping programs to multi-processors. In *SIES*, pages 9–17, 2011.

[T-C32] Oded Maler. On under-determined dynamical systems. In *EMSOFT*, 2011.

[T-C33] Alexandre Donzé. Breach, a toolbox for verification and parameter synthesis of hybrid systems. In *CAV*, pages 167–170, 2010.

[T-C34] Thao Dang, Oded Maler, and Romain Testylier. Accurate hybridization of nonlinear systems. In *Proceedings of HSCC 2010*, pages 11–20. ACM, 2010.

[T-C35] Eugène Asarin, Thao Dang, Oded Maler, and Romain Testylier. Using redundant constraints for refinement. In Ahmed Bouajjani and Wei-Ngan Chin, editors, *Automated Technology for Verification and Analysis - 8th International Symposium, ATVA 2010, Singapore, September 21-24, 2010. Proceedings*, volume 6252 of *Lecture Notes in Computer Science*, pages 37–51. Springer, 2010.

[T-C36] Oded Maler. On the Krohn-Rhodes cascaded decomposition theorem. In Zohar Manna and Doron Peled, editors, *Time for Verification, Essays in Memory of Amir Pnueli*, volume 6200 of *Lecture Notes in Computer Science*, pages 260–278. Springer, 2010.

[T-C37] Alexandre Donzé and Oded Maler. Robust satisfaction of temporal logic over real-valued signals. In Krishnendu Chatterjee and Thomas A. Henzinger, editors, *Formal Modeling and Analysis of Timed Systems - 8th International Conference, FORMATS 2010, Klosterneuburg, Austria, September 8-10, 2010. Proceedings*, volume 6246 of *Lecture Notes in Computer Science*, pages 92–106. Springer, 2010.

[T-C38] John Havlicek, Scott Little, Oded Maler, and Dejan Nickovic. Property-based monitoring of analog and mixed-signal systems. In Krishnendu Chatterjee and Thomas A. Henzinger, editors, *Formal Modeling and Analysis of Timed Systems - 8th International Conference, FORMATS 2010, Klosterneuburg, Austria, September 8-10, 2010. Proceedings*, volume 6246 of *Lecture Notes in Computer Science*, pages 23–24. Springer, 2010.

[T-C39] Oded Maler. Amir Pnueli and the dawn of hybrid systems. In Karl Henrik Johansson and Wang Yi, editors, *Proceedings of the 13th ACM International Conference on Hybrid Systems: Computation and Control, HSCC 2010, Stockholm, Sweden, April 12-15, 2010*, pages 293–295. ACM ACM, 2010.

[T-C40] Julien Legriel, Colas Le Guernic, Scott Cotton, and Oded Maler. Approximating the Pareto front of multi-criteria optimization problems. In Javier Esparza and Rupak Majumdar, editors, *Tools and Algorithms for the Construction and Analysis of Systems, 16th International Conference, TACAS 2010, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2*, volume 6015 of *Lecture Notes in Computer Science*, pages 69–83. Springer, 2010.

[T-C41] Oded Maler, Kim Guldstrand Larsen, and Bruce H. Krogh. On zone-based analysis of duration probabilistic automata. In Yu-Fang Chen and Ahmed Rezine, editors, *Proceedings 12th International Workshop on Verification of Infinite-State Systems*, volume 39 of *EPTCS*, pages 33–46, 2010.

[T-C42] Rajeev Alur, Aldric Degorre, Oded Maler, and Gera Weiss. On omega-languages defined by mean-payoff conditions. In *FOSSACS*, pages 333–347, 2009.

[T-C43] Eugène Asarin and Aldric Degorre. Volume and entropy of regular timed languages: Discretization approach. In *CONCUR*, 2009.

[T-C44] Ramzi Ben Salah, Marius Bozga, and Oded Maler. Compositional timing analysis. In *EMSOFT*, 2009.

[T-C45] Thao Dang and David Salinas. Image computation for polynomial dynamical systems using the bernstein expansion. In Ahmed Bouajjani and Oded Maler, editors, *Computer Aided Verification CAV'09*, LNCS, pages 277–287. Springer, 2009.

[T-C46] Thao Dang, Colas Le Guernic, and Oded Maler. Computing reachable states for nonlinear biological models. In Pierpaolo Degano and Roberto Gorrieri, editors, *Computational Methods in Systems Biology, 7th International Conference, CMSB 2009, Bologna, Italy, August 31-September 1, 2009. Proceedings*, volume 5688 of *Lecture Notes in Computer Science*, pages 126–141. Springer, 2009.

[T-C47] Oded Maler. Reachability for continuous and hybrid systems. In Olivier Bournez and Igor Potapov, editors, *Reachability Problems, 3rd International Workshop, RP 2009, Palaiseau, France, September 23-25, 2009. Proceedings*, volume 5797 of *Lecture Notes in Computer Science*, pages 24–25. Springer, 2009.

[T-C48] Alexandre Donzé, Bruce H. Krogh, and Akshay Rajhans. Parameter synthesis for hybrid systems with an application to simulink models. In *Proceedings of the 12th International Conference on Hybrid Systems: Computation and Control (HSCC'09)*, LNCS. Springer-Verlag, April 2009.

[T-C49] Alexandre Donzé, Gilles Clermont, Christopher James Langmead, and Axel Legay. Parameter synthesis in nonlinear dynamical systems: Application to systems biology. In *Proceedings of the 13th Annual International Conference on Research in Computational Molecular Biology RECOMB'09*, LNBI. Springer-Verlag, May 2009.

[T-C50] Goran Frehse and Rajarshi Ray. Design principles for an extendable verification tool for hybrid systems. In A. Giua, C. Mahulea, M. Silva, and J. Zaytoon, editors, *Proceedings of the 3rd IFAC Conference on Analysis and Design of Hybrid Systems (ADHS 2009)*. IFAC, 2009.

[T-C51] Colas Le Guernic and Antoine Girard. Reachability analysis of hybrid systems using support functions. In *CAV*, 2009.

[T-C52] Hitashyam Maka, Goran Frehse, and Bruce H. Krogh. Polyhedral domains and widening for verification of numerical programs. In *NSV-II: Second International Workshop on Numerical Software Verification*, 2009.

[T-C53] Thao Dang. *Model-Based Testing for Embedded Systems*, chapter Model-based Testing of Hybrid Systems. CRC Press, 2011.

[T-C54] Stavros Tripakis and Thao Dang. *Model-based Design of Embedded Systems*, chapter Modeling, Verification and Testing using Timed and Hybrid Automata. CRC Press, 2009.

[T-C55] Thao Dang and Romain Testylier. Hybridization domain construction using curvature estimation. In Marco Caccamo, Emilio Frazzoli, and Radu Grosu, editors, *Proceedings of the 14th ACM International Conference on Hybrid Systems: Computation and Control, HSCC 2011*, pages 123–132. ACM, 2011.

[T-C56] T. Dang. Using box splines to approximate reachable sets of polynomial systems. In *NSV-II: Second International Workshop on Numerical Software Verification, Verification of Cyber-Physical Software Systems*, 2009.

[T-C57] Thao Dang and David Salinas. Image computation for polynomial dynamical systems using the bernstein expansion. In Ahmed Bouajjani and Oded Maler, editors, *Computer Aided Verification CAV*, volume 5643 of *Lecture Notes in Computer Science*, pages 219–232. Springer, 2009.

[T-C58] Mohamed Amin Ben Sassi, Romain Testylier, Thao Dang, and Antoine Girard. Reachability analysis of polynomial systems using linear programming relaxations. In Supratik Chakraborty and Madhavan Mukund, editors, *Automated Technology for Verification and Analysis - 10th International Symposium, ATVA 2012*, volume 7561 of *Lecture Notes in Computer Science*, pages 137–151. Springer, 2012.

[T-C59] Thao Dang, Bertrand Jeannet, and Romain Testylier. Verification of embedded control programs. In *Proceedings of European Conrol Conference ECC 2013*, 2013.

[T-C60] Rajarshi Ray. *Reachability Analysis of Hybrid Systems using Support Functions*. PhD thesis, Grenoble University, May 2012.

D.4.1.3 Books, Book Chapters and edited proceedings

[T-B1] Oded Maler. The unmet challenge of timed systems. In *From Programs to Systems*. Springer, 2014.

[T-B2] Emmanuel Pourcelot, Nicolas Mobilia, Alexandre Donzé, Oded Maler, Pascal Mossuz, and Eric Fanchon. Cellular iron regulation in animals: need and use of suitable models. In *Nutzen-Risiko-Bewertung von Mineralstoffen und Spurenelementen: Biochemische, physiologische und toxikologische Aspekte*, page 73. KIT Scientific Publishing, 2014.

[T-B3] Sergiy Bogomolov, Alexandre Donzé, Goran Frehse, Radu Grosu, Taylor T Johnson, Hamed Ladan, Andreas Podelski, and Martin Wehrle. Abstraction-based guided search for hybrid systems. In *Model Checking Software*, pages 117–134. Springer Berlin Heidelberg, 2013.

[T-B4] Thao Dang and Carla Piazza, editors. *Proceedings Second International Workshop on Hybrid Systems and Biology, HSB 2013, Taormina, Italy, 2nd September 2013*, volume 125 of *EPTCS*, 2013.

[T-B5] Thao Dang and Ian M. Mitchell, editors. *Hybrid Systems: Computation and Control (part of CPS Week 2012), HSCC'12, Beijing, China, April 17-19, 2012*. ACM, 2012.

[T-B6] Thao Dang. *Model-Based Testing for Embedded Systems*, chapter Model-based Testing of Hybrid Systems. CRC Press, 2011.

[T-B7] Xin Chen, Erika Abraham, and Goran Frehse. Efficient bounded reachability computation for rectangular automata. In Igor Potapov and Giorgio Delzanno, editors, *Reachability Problems*, volume 6945 of *LNCS*, pages 139–152. Springer, 2011.

[T-B8] Stavros Tripakis and Thao Dang. *Model-based Design of Heterogeneous Systems*, chapter Modeling, Verification and Testing using Timed and Hybrid Automata. CRC Press, 2009.

[T-B9] Ahmed Bouajjani and Oded Maler, editors. *CAV 2009, Proceedings of the 21st Conference on Computer-aided Verification*, volume 5643 of *LNCS*. Springer, 2009.

[T-B10] Goran Frehse. Tools for the verification of linear hybrid automata models. In Jan Lunze and Françoise Lamnabhi-Lagarrigue, editors, *Handbook of Hybrid Systems Control, Theory – Tools – Applications*. Cambridge University Press, 2009.

D.4.1.4 PhD Theses and habilitations

[T-P1] Jean-Francois Kempf. *On Computer-Aided Design-Space Exploration for Multi-Cores*. PhD thesis, University of Grenoble, October 2012.

[T-P2] Romain Testylier. *Reachability Analysis of Nonlinear Systems*. PhD thesis, Université de Grenoble, France, 2012.

[T-P3] Rajarshi Ray. *Reachability Analysis of Hybrid Systems using Support Functions*. PhD thesis, Grenoble University, May 2012.

[T-P4] Selma Saidi. *Optimizing DMA Data Transfers for Embedded Multi-Cores.* PhD thesis, University of Grenoble, October 2012.

[T-P5] Julien Legriel. *Multi-Criteria Optimization and its Application to Multi-Processor Embedded Systems.* PhD thesis, University of Grenoble, October 2011.

[T-P6] Thao Dang. *Methods and Tools for Computer-Aided Design of Embedded Systems.* HDR, Université de Grenoble, France, 2010.

[T-P7] Scott Cotton. *On Some Problems in Satisfiability Solving.* PhD thesis, University Joseph Fourier, 2009.

D.4.1.5 Other visible publications

[T-O1] Eugène Asarin and Aldric Degorre. Volume and entropy of regular timed languages: Analytical approach. submitted to FORMATS 2009, 2009.

D.4.2 Tempo team: Software

SpaceEx: The State Space Explorer Software platform for verification, monitoring, and simulation of hybrid systems
Authors: Goran Frehse, Colas Le Guernic, Alexandre Donzé, Scott Cotton, Rajarshi Ray, Olivier Lebeltel, Rodolfo Ripado, Antoine Girard, Thao Dang, Oded Maler
Home page: http://spaceex.imag.fr/
License: GPLv3

AMT: Analog Monitoring Tool Monitoring temporal properties of continuous and hybrid signals
Authors: Dejan Nickovic, Olivier Lebeltel, Oded Maler
Home page: http://www-verimag.imag.fr/DIST-TOOLS/TEMPO/AMT/content.html
License: None

D.4.3 Tempo team: Scientific influence

- Events organisation
  - O. Maler was a co-organizer of the the workshop *Towards Systems Biology*, Grenoble, 2011.
  - O. Maler organized the workshop *Formal and Informal Methods for Correctness and Performance*, Marrakech, 2013.
  - G. Frehse was a co-organizer of the workshop *Formal Verification of Analog Circuits* (satellite of CAV), Grenoble, 2009.
  - G. Frehse was a co-organizer of the workshop *Synthesis of Continuous Parameters* (satellite of ETAPS), Grenoble, 2014.
  - G. Frehse was a co-organizer of the workshop *Applied Verification of Continuous and Hybrid Systems* (satellite of CPSWeek), Berlin, 2014.
  - G. Frehse, T. Dang and O. Maler organized the workshop *Frontiers in Analog CAD*, Grenoble, 2014.
- Invited conferences
  - O. Maler gave an invited talk at the workshop *The Reachability Problem*, Paris, 2009.
  - O. Maler gave an invited talk at the *Cyber-Physical Week*, Stockholm, 2010.
  - O. Maler gave an invited talk at the *Amir Pnueli Memorial Symposium*, New York, 2010.
  - O. Maler gave an invited talk at the 4^{th} *Workshop on Theorem Proving*, Belgrade, 2011.
  - O. Maler gave an invited talk at the *Workshop on Formal Methods in Robotics*, Salt Lake City, 2011.
  - G. Frehse gave an invited talk at the *Numerical Software Verification* workshop, Salt Lake City, 2011.
  - O. Maler gave an invited talk at the *FORMATS: Formal Methods for Real-time Systems*, Aalborg, 2011.

  - O. Maler gave an invited talk at the *EMSOFT: Embedded Software*, Taipei, 2011.
  - O. Maler gave an invited talk at the *Infinity* workshop, Hanoi, 2013.
  - O. Maler gave an invited talk at the *QAPL* workshop, Grenoble, 2014.
- Evaluation activities
  - O. Maler participated in the evaluation of projects researchers and research teams for the following institutions: *Technion, Haifa, Israel*, *Dutch Science Foundation*, *Austrian Science Fund*, *Swiss National Science Foundation*, *Indian Institute of Technology Bangalore*, *Israel-India Science Foundation*, *US National Science Foundation (NSF)*, *Singapore Education Ministry*, *INRIA* and the *ANR*.
  - G. Frehse participated in the evaluation of projects researchers and research teams for the following institutions: *German Research Society*, *Dutch Technology Foundation*, *Netherlands Organization for Scientific Research*.

D.4.4 Tempo team: Interaction with the economic, social and cultural environment

- Industrial contracts
  - **STMicroelectronics**: We had two CIFRE contracts to the group on multi-core. Today we have strong ties with ST Crolles on analog CAD, culminating in 2 joint Nano2017 projects waiting for final approval.
  - **Mentor Graphics**: There is currently a CIFRE contract on the integration of AMS assertions in Mentor's simulation tools;
  - **Atrenta**: Two alumni of the group, S. Cotton and J. Legriel, work in Atrenta and there is an ongoing CIFRE contract on switching and power reduction in digital circuits.
  - **Kalray**: We had two contracts for testing our deployment optimization tools on their MPPA platform;
  - **Toyota USA**: We have an ongoing contract about simulation-based verification of engine models;
  - **United Technology Research Center**: We are finalizing a contract on simulation-based verification of HVAC (heating, ventilation, air-conditioning) systems;
  - **Bosch**: We have submitted a joint publication and are working on several case studies.
  - **Mathworks**: One of the group alumni, JF. Kempf, works there and O. Maler participated in their annual faculty summit in, June 2014.
  - **Easii-IC**: We have a joint project (together with the Austrian Institute of Technology) and pending joint submissions to H2020 and Nano2017.
- Consulting
  - O. Maler is a member of the technical advisory board of ATRENTA.

Appendix E

List of grants
Liste des contrats

BINSEC - january 2013 – december 2017

ANR, Total Budget: 967 k€, Verimag budget: 139 k€
Partners:
CEA-LIST (leader), EADS IW, INRIA Rennes, LORIA, UJF-Verimag, VUPEN Security
Verimag people involved:
L. Mounier, M-L. Potet, J-C Fernandez, J. Feist

General Objectives:
The global aim of the BINSEC project is to fill part of the gap between formal methods over executable code on one side, and binary-level security analyses currently used in the security industry. We target two main applicative domains: vulnerability analysis and virus detection. Two other closely related applications will also be investigated: crash analysis and program deobfuscation. For malware detection, we want to design signature methods robust to mutations and able to overcome obfuscation, especially self-modifying code. For vulnerability analysis, we want to develop techniques able to locate potential vulnerabilities in an executable file, and able to distinguish between simple crash bugs and exploitable bugs (exploitability). While a priori distinct, we claim that the different fields addressed in BINSEC share common basic problems and could benefit from similar advances in automated binary code analysis, such as precise recovery of control-flow or data-flow information, or low-level type inference. Finally, we will develop a common (lightweight) open-source infrastructure to ease the development of binary-level analysers and to allow communication between prototypes through a common formal model.

Verimag work in the project:
Our objective is to propose analyses and tools assisting the process of vulnerability detection in the whole: detecting potential bugs, that can be activated by users with dangerous effects. We target complex vulnerabilities, such as Use after Free, that can not be easely detected by classical fuzzing technics. We address several theoretical challenges: static analysis for low-level code, exploitability conditions, and proposing memory model and analysis adapted for exploitability, but remaining tractable for static analysis. From a practical point of view, we plan to combine several analyses, in order to be able to successfully treat real-world binary executables. Developed tools will be compatible with the BinSec platform.

Cadmidia - 2013-2017

ANR, Verimag budget: 85 k€
Partners:
TIMC, LBFA, VERIMAG
Verimag people involved:
O. Maler

General Objectives:
Metabolism of Cadmium

Verimag work in the project:
Improve tools for evaluating and debugging biological models.

COMPACS - 2014-2017

ANR, Total Budget: 309 k€, Verimag budget: 16 k€
Partners:
LJK (Grenoble), CRAN (Nancy), VERIMAG
Verimag people involved:
T. Dang

General Objectives:
Computation-Aware Control Design and Implementation

Verimag work in the project:
Develop new techniques for the synthesis of control strategies that are able not only to determine the correct control decisions, but also schedule the control tasks based on the availability of computing units and the state of the physical plant.

MALTHY - 2014-2017

ANR, Total Budget: 919 k€, Verimag budget: 111 k€
Partners:
Inria Rennes, CEA LIST (Saclay), Inria Saclay, Object Direct (Grenoble), VERIMAG
Verimag people involved:
T. Dang, G. Frehse

General Objectives:
Using algebraic methods to advance the state of the art of real-time and hybrid model checking

Verimag work in the project:
Develop model checking methods and tools based on linear algebra, mathematical programming (convex and semi-algebraic optimization) and tropical geometry

STATOR - January 2013 – December 2017

ERC starting investigator grant, Total Budget: 1472 k€, Verimag budget: 1472 k€
Partners:
Université Joseph Fourier - VERIMAG
Verimag people involved:
D. Monniaux, I. Asavoae, P. Dhadich, J. Henry, G. Karpenkov

General Objectives:
STATOR focuses on developing new methods for static analysis of software — that is, mathematically and automatically proving that software behaves in the desired way. Directions of investigations include new fixpoint iteration techniques (based e.g. on policy iteration), combinations of abstraction and satisfiability testing and the relationship between numeric and discrete (e.g. Booleans or data structures) data. The results are to be implemented in publicly available research prototypes.

Verimag work in the project:
Improvements to the PAGAI static analyzer, and applications to worst case execution time analysis by optimization within the solution set of a satisfiability problem with abstracted constraints. Development of a LLVM-to-Horn clause converter. Development of a certified BDD library. Development of policy iteration on succinctly represented large discrete state spaces.

OpenES - April 2013 – October 2016

European (CATRENE), Verimag budget: 233 k€
Partners:
CISC (Austria), Thales (France), NXP (Netherlands), ST (France) DoceaPower (France), Magillem Design Services (France), Vector Fabrics (Netherlands) Synopsys (Netherlands) CEA-LIST (France), UJF-Verimag (France), Technical University of Eindhoven (Netherlands), ECSI (France)
Verimag people involved:
F. Maraninchi, M. Moy, Y. Romenska, S. Mangaraj

General Objectives:
In order to improve European electronics system design productivity (faster time-to-market), design quality (less design errors and less re-designs) to stay competitive, the OpenES consortium joins forces to provide missing links in system-level design and to develop common open solutions based on four pillars: (i) Fill gaps in design flows with new interoperable tools and/or improve existing tools/flows ensuring the semantic continuity of the design flow. (ii) Specifically focus on integral support of both functional and extra-functional requirements from specification to verification, jointly with the use cases defined at system level. (iii) Raise reuse capabilities from IP to HW/SW subsystem in order to eliminate integration effort by supporting reuse of pre-integrated and pre-verified subsystems. (iv) Enhance interoperability of models and tools by upgrading and extending existing young open standards (SystemC TLM, SystemC-AMS, IP-XACT)

Verimag work in the project:
Verimag will contribute to a well-defined structure for high-level models of individual components, subsystems, or full systems. The structure will include both the functional behavior and extra-functional properties like timing and energy consumption. Verimag will work in two complementary directions: (i) A formal definition, independent of any particular modeling language/simulation engine, and including a notion of functional- and extra-functional contracts for hierarchic HW/SW component-based systems; (ii) An efficient execution engine based on SystemC, and able to run the simulation in parallel on multi-core host machines.

DIAMS - 2014 – 2016

Projet AGIR, Verimag budget: 20 k€
Partners:
LIG
Verimag people involved:
S. Devismes

General Objectives:
The DIAMS project aims at tackling the drawbacks observed in preliminary works on distributed monitoring by proposing realistic monitoring and monitor-synthesis algorithms for realistic cyber-physical systems.
The expected outcome will be efficient monitoring algorithms for widely distributed architecture that can be applied to cyber-physical systems. The algorithms will outperforms existing algorithms along the important monitoring metrics: the number of messages, the size of the messages, the delay induced by distributed monitoring (due to the fact monitors need to exchanged messages to recompute the global state), the memory consumed by monitors and the overhead imposed to the program. The algorithm should be general and generic to serve as a basis for future algorithms that will be specialized for some application-domains.

Verimag work in the project:
First, we will propose distributed monitoring algorithms that withstand more and more adversarial (and consequently realistic) environments. Moreover, in practical settings, components and devices may have to face faults, in particular the intermittent loss of messages in communication links. Hence, fault-tolerance should be addressed when dealing with distributed monitoring. For this purpose, we will propose solutions that handle unreliable links and component crashes. Another weakness of the previous approaches is that all components communicate through a single bus that is all-to-all (*i.e.*, any component can send a message to any other component) and full-duplex (*i.e.*, the bus can contain several messages at the same time in either direction). We plan to first relax this assumption by considering the half-duplex case, where each component can still access to the bus to communicate with each other, but only one message can transit at a time. The use of half-duplex communications entail the problem of ensuring fair access of components to the bus, *i.e.*, the bus has to be seen as a shared resource in mutual exclusion. Then, we will consider even more generalized and scalable approaches, where components are organized as a connected communication graph in which direct communications are possible only between pairs of neighboring components.
The first part of our proposal deals with issues related to decentralized control. In the meantime, we will address the problem of continuous growth to the size of local formulae over time. To solve this issue, we propose to adapt data aggregation techniques, which are widely used in user-centric routing and distributed data fusion. These techniques will require to model the monitored system as a hierarchical structure rather than a flat one. First, we will assume structured communication networks, *e.g.*, tree-shaped networks. Then, we will abstract the hierarchy into the logical distributed data structure using, *e.g.*, spanning trees and clustering constructions (such spanning structures being widely used in networking).

CIFRE-Lemke - 2013-2016

Industry, Total Budget: 30 k€, Verimag budget: 15 k€
Partners:
Orange Labs, VERIMAG/Synchrone, LIG/Drakkar.
Verimag people involved:
F. Maraninchi, L. Lemke

General Objectives:
Accompanying contract to the CIFRE thesis of Laurent Lemke

Verimag work in the project:
Shared self-configuring models and software infrastructures for Smart City monitoring and control.

CIFRE Mentor - 2013-2016

Industrial, Verimag budget: 50 k€
Partners:
Mentor, VERIMAG
Verimag people involved:
O. Maler, T. Ferrere

General Objectives:
CIFRE support

Verimag work in the project:
Studying the integration of assertions and measures in analog circuit simulators.

CIFRE Atrenta - 2013-2016

Industrial, Verimag budget: 30 k€
Partners:
Atrenta, VERIMAG
Verimag people involved:
O. Maler, J. Lanik

General Objectives:
CIFRE support

Verimag work in the project:
Developing techniques for power reduction for systems on a chip.

DACRAW - 2014 – 2015

Exploratory Project of the LABEX persyval-Lab, Total Budget: 9.5 k€, Verimag budget: 5 k€
Partners:
LIG Drakkar
Verimag people involved:
K. Altisen, S. Devismes

General Objectives:
The main objective is to provide the means to operate a WSN with the protocol TSCH in a fully distributed manner, namely without using any centralized entities. To reach this goal, our work needs to focus on MAC and routing. It will address three distinct but combined objectives:

- Compute and allocate, in a distributed way, **global schedules** of cells that will guarantee required properties — *e.g.* short delay.
- Compute suitable paths with a **distributed routing algorithm** on which to build the aforementioned schedules.
- Perform **neighbor maintenance** to discover new nodes and maintain connectivity with nodes of interest, on which we can rely to provide efficient routing.

Verimag work in the project:
At the MAC level, we want to propose a self-adaptive protocol that is both a MAC and a stable neighborhood protocol. In other words, this protocol will manage the 1-hop communications and aim at selecting a set of neighbors sufficiently stable and which fulfills desirable criteria, such as a good delivery rate, guarantees on the delivery time, *etc.* This protocol should be self-adaptive in the sense that its behavior should take the variations of the environment into account.
Then, we will propose a cluster-based approach for routing. More precisely, the network will be self-organized using a self-stabilizing clustering algorithm. Then, the two-level hierarchy of the clustering will be used to create efficient routes in the network.
Finally we will focus on the aforementioned problem of schedule computation and allocation, for which we need to provide distributed cell allocation, in order to load-balance the traffic, prevent collisions and eliminate idle listening. In TSCH terminology, such schedules set-up *tracks* that are defined as sequences of cells along a multi-hop path obtained from the routing.

CESyMPA - 2013 – 2014

Exploratory Project of the LABEX persyval-Lab, Total Budget: 10 k€, Verimag budget: 5 k€
Partners:
TIMA SLS
Verimag people involved:
F. Maraninchi, M. Moy, P. Raymond, C. Maïza

General Objectives:
The increase of hardware performances is now led by multicore or manycore architectures, which promise computing power, and low energy consumption; this is no longer possible by increasing the frequency of processors. Modern architectures are thus made of several computing cores, communicating via shared memories or even networks-on-a-chip. The gap between the potential power and what we can do with traditional programming methods is growing.
On the other hand, the main use of such powerful hardware is for applications, like games, that require average performance. This is the reason why they include several levels of automatic optimizations, like memory controllers, caches, dynamic load balancing, operating systems supporting migration, etc. At the same time, critical systems like the ones found in cars, trains, planes and other embedded systems have started requiring more computing power, but the main constraint is the predictability of behavior and timing; in this domain, the focus is on worst-case scenarios, not average performance.
CESyMPA aims at advancing state-of-the-art implementation methods for critical systems, to include manycore architectures. One of the industry standards of the domain is SCADE/Lustre, which provides high level dataflow specifications of the critical applications.

Verimag work in the project:
Following previous work on hardware design, and critical software design and implementation, we study several approaches for the use of modern hardware architectures in critical contexts requiring predictability. Some challenges are: (i) Towards more intrinsically predictable hardware elements; (ii) A holistic view of hardware and software for a correct-by-construction compilation chain guaranteeing determinism and predictability; (iii) Memory hierarchy for critical real-time systems.
Approach and First Results: (i) An ongoing master project is dedicated to providing deterministic implementations of Lustre on the MPPA manycore architecture developed by Kalray; (ii) A complementary approach is to exploit high level information available in a Lustre specification to improve the precision of the worst-case-execution-time computation.

W-SEPT - October 2012 – April 2016

ANR, Total Budget: 620 k€, Verimag budget: 220 k€
Partners:
UJF-Verimag (leader), UPS-IRIT, INRIA-IRISA, Continental SAS Automotive
Verimag people involved:
P. Raymond, C. Maiza, C. Vigouroux, N. Halbwachs, F. Carrier, E. Jahier, M. Asavoae

General Objectives:
Critical embedded systems are generally composed of repetitive tasks that must meet drastic timing constraints, such as termination deadlines. Providing an upper bound of the worst-case execution time (WCET) of such tasks at design time is thus necessary to prove the correctness of the system. The key position of this proposal is to bring semantics back to the heart of timing analysis. The final goal is a gain in precision of the WCET estimate. It will be reached by introducing new strategies at different levels in the whole analysis process. First of all, the semantic properties that are relevant and useful for enhancing timing analysis will be characterized. Semantic information can be discovered from high-level design (when it exists, e.g. Scade, Simulink), from the C code, and/or from the binary code. Solutions to ensure the traceability of the information though the compilation process will be proposed. Then, the state-of-the-art WCET computation method (IPET) will be re-visited to investigate to what extent it can exploit the semantic information transferred from previous steps. Alternative methods will be proposed to go beyond its limitations. All the contributions will be implemented in an open-source toolset dedicated to WCET analysis (Otawa) and experimented on several case studies from the spatial and automotive domains.

Verimag work in the project:
We developed a proof-of-concept tool that checks the feasibility of worst-case execution path at the design level (Lustre). This tool is connected to Lesar to model-check the feasibility and to OTAWA to get the WCET. We also developed a tool to compute WCET using SAT solving modulo theory (also connected to OTAWA to get the WCET of basic blocks). These initial steps lead to an important gain in the precision of WCET estimation. It should be further improved by on-going work on the path analysis by abstract interpretation, ILP and on the traceability in the Lustre compiler.

VERASCO - January 2012 – December 2015

ANR INS, Total Budget: 995 k€, Verimag budget: 188 k€
Partners:
INRIA Paris Rocquencourt (Gallium, Abstraction), Airbus avionics and simulation products, IRISA - Université Rennes I, Université Joseph Fourier - VERIMAG, INRIA Saclay (Toccata)
Verimag people involved:
D. Monniaux, S. Boulmé, P. Corbineau, A. Fouilhe, M. Périn

General Objectives:
In its quest for software perfection, the critical software industry (aircraft, railways, nuclear, medical, etc.), especially in France, has been progressively embracing the use of formal verification tools as a complement, or even as an alternative, to traditional software validation techniques based on testing and reviews. Verification tools based on static analysis, deductive program proof or model checking provide additional, independent assurance about a critical software system; they can also render some tests unnecessary, resulting in net gains in validation costs and time. The usefulness of verification tools in the development and certification of critical software is, however, limited by the amount of trust one can have in their results. A first potential issue is unsoundness of a verification tool: if a verification tool fails (by mistake or by design) to account for all possible executions of the program under verification, it can conclude that the program is correct while it actually misbehaves when executed. A second, more insidious, issue is miscompilation: verification tools generally operate at the level of source code or executable model; a bug in the compilers and code generators that produce the executable code that actually runs can lead to a wrong executable being generated from a correct program. Both issues are known, accounted for in regulations such as DO-178 for avionics, and addressed through best practices that are, however, costly in performance (no code optimizations) and additional validation tasks (more reviews, more testing)."
The VERASCO proposal advocates a different, radical, mathematically-grounded solution to these issues: the formal verification of compilers and verification tools themselves. We set out to develop a generic static analyzer based on abstract interpretation for the C language, along with a number of advanced abstract domains and domain combination operators, and prove the soundness of this analyzer using the Coq proof assistant. Likewise, we will continue our work on the CompCert C formally-verified compiler, the first realistic C compiler that has been mechanically proved to be free of miscompilation, and carry it to the point where it could be used in the critical software industry. [Leroy 2011] We will take advantage of the close coupling between compiler and analyzer made possible by the fact that both are proved against the same formal semantics, in particular to propagate and exploit during compilation the properties inferred by static analysis. Finally, we will investigate the tool qualification issues that must be addressed before formally-verified tools can be used in the aircraft industry.

Verimag work in the project:
Development of a certified polyhedra library and of a static analysis for linear recurrent filters.

CYPHERS - July 2013 – February 2015

European Project FP7, Total Budget: 535 k€, Verimag budget: 96 k€
Partners:
Fortiss, KTH, University of York, University of Trento, Siemens
Verimag people involved:
S. Bensalem

General Objectives:
The ongoing integration of software-intensive embedded systems and global communication networks into Cyber-Physical Systems (CPS) is considered to be the next revolution in ICT with a lot of game-changing business potential and novel business models for integrated services and products. CPS will be a core enabling technology for securing economic leadership in embedded systems/ICT, having an enormous social and economic importance, and making decisive contributions to societal challenges. Europe is well positioned to meet this merging of the physical and virtual worlds. However, to effectively address the associated challenges, a strategic agenda is needed to ensure Europe's competitiveness. This Support Action will systematically survey, analyse, and evaluate the economic, technical, scientific, and societal significance of Cyber-Physical Systems for Europe. The project will develop an integrated strategic CPS research agenda for Europe, and derive comprehensive recommendations for action that will cover the identification and prioritization of research areas, support measures for both horizontal and vertical cooperation, and an outline of possible research partnerships, and will address questions of research funding as well as the issues of training, standardization and policies.

Verimag work in the project:
In this project we will build on existing studies, and elicit expert knowledge through dedicated workshops and targeted interviews, to provide a systematic assessment of current technological and social challenges, potential uses of CPS, current research and research still needed, in order to inform future research activities in the EU. We will furthermore consider the associated risks and opportunities, and also assess the sufficiency of the expertise and engineering skills in Europe. This will enable both research and education to be covered in the vision developed by CyPhERS. We will elaborate further on the form of the systematic assessment, but some key dimensions of the assessment can be extracted from the above discussion. The assessment will at least cover:

- Application domains – the needs for automotive, energy management, medical care, rail; if possible CyPhERS will find a way to structure this analysis to identify issues which cross domains, and those which are domain specific;
- Technologies – the needs across communications networks, enterprise architectures, web services; as with domains a unified approach will be adopted, if this proves practicable.

This work will be carried out through reviews of the literature, but also in discussion with industrial partners and associates.

DMILS - October 2010 – October 2014

European Project FP7, Total Budget: 2850 k€, Verimag budget: 272 k€

Partners:
The Open Group, FBK Trento, Fortiss, Frequentis, Lynuxworks, RWTH Aachen, TTTech, University of York

Verimag people involved:
S. Bensalem, M. Bozga, N. Ben Said

General Objectives:
Distributed systems for critical applications are costly and time-consuming to develop and to certify. Since there is little automated support for early assurance that a system faithfully implements its architectural design and satisfies its requirements, qualification testing and certification processes often reveal deficiencies that require costly late changes. MILS provides compositional system construction and assurance, leveraging individually developed and assured components to predict and assure the properties of composite systems. By providing a modular high-assurance platform and a framework for the certification of systems built on that platform, MILS reduces the cost and time for development, certification, and maintenance of dependable systems.
Distributed MILS relies on extensions to a MILS separation kernel and the addition of a MILS network subsystem using a hardware-based, time-triggered Ethernet "backplane". It will be possible, for the first time, for an application architecture to seamlessly span multiple computer systems, with scalable deterministic operation over a set of nodes, opening many new practical application areas for MILS. Automated assistance, as being developed and applied in this project, is indispensable for the development and verification of dependable distributed systems. System architects, developers, integrators, installers, operators, and particularly the organizations and populations that depend on critical systems, will benefit from the resulting assurances that many of the sources of errors that lead to added cost and dangerous failures of critical systems can be eliminated.
Results of the Distributed MILS project will establish a common framework for critical system construction and certification, encouraging innovation among component and service suppliers, and leading to improved dependability while reducing the cost to develop, certify and deploy trustworthy critical systems.

Verimag work in the project:
VERIMAG is contributing to several topics of the project. First of all, VERIMAG is investigating security extensions (e.g., information flow security, non-interference) in the context of component-based models (as represented in the BIP framework). Second, VERIMAG is developing compositional verification methods and tools and their extension in a security context as proposed by D-MILS. Last but not least, VERIMAG is playing a key role in the deployment of the D-MILS technology by actually leading the work on the automatic construction of *system-wide configurations*, that is, the orchestrated configuration of the (multiple) separation kernels together as well as of the Ethernet backplane in order to support the secure realization of the policy architectures expressed in MILS.

MANYCORELABS - January 2012 – March 2015

National project ("BGLE, investissement d'avenir"), Verimag budget: 364 k€
Partners:
Kalray, Asygn, ATEME, CAPS Entreprise, CEA, Digigram, Docea Power, INRIA, IS2T, Krono-Safe, Renault, Scilab Entreprise, Thales Communications, Thales RT
Verimag people involved:
M. Bozga, S. Bensalem, A. Mentis, S. Ben Rayana, A. Nouri

General Objectives:
The objective of the projet is to allow the Kalray enterprise, associated to a consortium of technological and applicative partners, to position as a leading provider on the market of manycore platforms for embedded systems. Kalray is developing MPPA, a manycore platform built using the most advanced silicon technology (CMOS 28nm) and integrating 256 VLIW optimized cores offering 500 GOPS or 200 GFLOPS computing power for a typical power envelope from 5 to 10W. Two key elements are considered in the project:

1. building an effective software environment and an eco-system of associated partners to Kalray
2. demonstration of the added-value of the MPPA technology on a wide variety of applications, significant for the market of emebdded systems.

Verimag work in the project:
VERIMAG play the role of technology provider in the project. Its contribution is twofold:

- deploying the BIP design flow for the modeling and validation of heterogeneous, composite applications developed for MPPA.
- using the real-time extension of BIP as a programming model for real-time applications, that is, providing the code generation and execution support for execution of real-time BIP models on MPPA.

TOYOTA - 2013-2015

Industrial, Verimag budget: 120K k€
Partners:
Toyota USA, VERIMAG
Verimag people involved:
T. Dang, T. Dreossi

General Objectives:
Test generation for automotive models

Verimag work in the project:
Using the HTG tool for testing Simulink models

parameter

PROSE - 2010-2014

ANR, Verimag budget: 131 k€
Partners:
EVEREST-INRIA, Plume-LIP, ProVal-LRI, CPR-Cédric, VERIMAG/DCS.
Verimag people involved:
P. Corbineau, C. Ene, P. Lafourcade, Y. Lakhnech, J. Dreier, M. Daubignard, M. Duclos

General Objectives:
The PROSE project aims at increasing the confidence in security protocols, and in order to reach this goal, provide security proofs at three levels: i) the symbolic level, in which messages are terms, ii) the computational level, in which messages are bitstrings, iii) the implementation level, the program itself.

Verimag work in the project:
Following the development of the computational indistinguishability logic (CIL) by Y. Lakhnech and M. Daubignard, P. Corbineau developed a full Coq formalisation of CIL rules. Mathilde Duclos has used this formalised framework to formally prove the security of an intrusion resilient algorithm [D-C81]. Work in the PROSE project also includes the Ph.D. thesis of J. Dreier who worked on security proofs in the symbolic model for voting and auction protocols, supervised by P. Lafourcade.

ASCENS - October 2010 – October 2014

European Project FP7, Total Budget: 5300 k€, Verimag budget: 501 k€
Partners:
The partners include in particular LMU Munich, IMT Lucca, Volkswagen AG, EPF Lausanne, Zimory GmbH
Verimag people involved:
S. Bensalem, J. Combaz, B. Jobstmann, L. Astefanoaei, J. Sifakis

General Objectives:
The ASCENS approach will focus on service-component ensembles (SCEs), hierarchical ensembles built from service components (SCs), simpler SCEs and knowledge units (K) connected via highly dynamic infrastructure.
Service components are nodes that can cooperate, with different roles, in an open and non-deterministic environment. A service-component ensemble is a set of service components with dedicated knowledge units, to represent shared local and global knowledge basis about levels of awareness, resources, connectivity and networking, interconnected in a dynamic network, featuring goal-oriented, safe and secure execution and efficient resource management.
To realize ensembles of service components, whose properties go far beyond the state of the art in current software engineering and technology, the following domains need to be thoroughly investigated, which become the concrete objectives of the project.

1. Language support for programming SCEs, expressing awareness and exchanging knowledge
2. Formalization and modelling the fundamental SCE network properties like autonomous behaviour and aware-rich networking
3. Knowledge representation and self-awareness of service components
4. Methods and mechanisms for adaptation and dynamic self-expression
5. Techniques and methodology for the design and development of reliable SCs and SCEs and their verification using formal methods
6. Software infrastructure with a set of tools to support programming, deployment and execution of SCE-based applications
7. A set of case studies (from robotics, cloud computing and e-Vehicles) will illustrate both the generic approach and the wide coverage of the ASCENS technology

Verimag work in the project:
In this project we develop new techniques and the underlying theories to support the design and the implementation of correct and reliable service components (SCs) and service component ensembles (SCEs). We are working in several directions. The first one deals with correctness on the level of a service component, considering in particular non-functional properties like resourceawareness. The second deals with correctness of ensembles of service components mainly focusing on constructive techniques. Given the particular importance of security in ensembles, the third address the problem of building secure ensembles. Finally, we work on techniques to check if a SCs implementation complies with a high-level specification.

CERTAINTY - December 2011 – December 2014

European Project FP7, Total Budget: 2850 k€, Verimag budget: 346 k€
Partners:
AbsInt Angewandte Informatik GmbH, ETH Zurich, KALRAY, Technische Universität Braunschweig, Thales, Uppsala University
Verimag people involved:
S. Bensalem, M. Bozga, P. Poplavko, D. Socci

General Objectives:
The key objective of CERTAINTY is to push forward the certification of real-time mixed critical embedded systems, a process currently challenged by the choices made at application design time about reliability and disturbances handling which deals with the management of interferences between different functions of complex control software over the whole system.
More specifically, from a research and technological perspective CERTAINTY will address the a set of four objectives:

1. To extend modelling languages semantics
2. To support heterogeneous criticality handling at application design level
3. To redefine the way that designers interact with criticality requirements and application behavioural monitoring
4. To experiment and validate the new approach, considering examples that are demanding in terms of complexity in design and efficiency in certification

CERTAINTY will advance the state of the art by validating a mixed critical application on multicore architecture about:

- Function decomposition and associated safety levels and examples of non-trivial interactions and dependencies between control functions in a Flight Management System application representative of industrial mixed critical application in avionics;
- Innovative (integrated, multicore) computing architectures, to elicit the schemes of resource sharing and unreliability that, without proper analysis techniques, appear as source of uncertainties at execution time.

Verimag work in the project:
Our work in CERTAINTY project is to provide the necessary formal, component based validation methods that are a prerequisite for certification. Based on automatically generated formal models (to use mathematical proofs as an additional means of verification) that faithfully model mixed-criticality systems, safety properties as well as extra functional properties are investigated. We are also working on component-based methods that allow for an optimized deployment of the application on the various resources of the underlying heterogeneous execution platform.

ACOSE - December 2011 – December 2014

National project ("BGLE, investissement d'avenir"), Verimag budget: 338 k€
Partners:
CEA, Cyberio, TIMA, MAGILLEM Design Services
Verimag people involved:
S. Bensalem, M. Bozga, S. Djoko Djoko, A. Lekidis

General Objectives:
The ACOSE proposal addresses the end-to-end design for large-scale heterogeneous embedded systems. The key motivations are facilitation of the design of advanced heterogeneous embedded systems with distributed software. At the same time it can provide a secure design flow with system engineering management, performance analysis and validation for multiple programming models to target hardware architectures including multiple heterogeneous smart subsystems and components. The project will be driven by key requirements triggered by industry, like support of legacy, correctness and low power. The aim of the project is to provide a design flows with the following key objectives:

1. Efficient handling of heterogeneity in different dimensions (modeling levels, structur-al compositions, functional/extra-functional descriptions, description language usage, etc.), thus reducing cost of complexity handling of future systems designs;

2. Ensure traceability of the developments from requirement down to implementation and provide decision support system facilities;

3. Handling of extra-functional constraints like power, throughout the design flow (from the application level to the platform level) in a uniform way, thus enabling cost-effective design of ultra-low power systems and increasing the overall energy-efficiency of designs (i.e. more MOPS/mW);

4. Inclusion of legacy software and other IP into the design, enabling fast time-to-market through efficient reuse;

5. Fast validation and verification of designs on all levels of abstraction in the flow, reducing development cycles and overall effort.

Verimag work in the project:
In this project, we will develop methodologies and tools that enable design exploration iterations of the application at high levels of abstraction. The challenge is to be able to include the power and performance constraints and to build the correspondence between high level profiling measures and platform measures obtained by platform code execution. We will address several important topics :

- System model optimal distribution: To generate distributed implementations from BIP system models it is necessary to transform these models into implementable system models e.g., Send/Receive (S/R) or Shared-Memory BIP models. Then, from implementable system models and a mapping of atomic components into processing elements of a platform it is possible to generate efficient C/C++ or MPI-code. We are seeking heuristics that can provide (near) optimal implementation with respect to several functional (number of messages) or non-functional (response times, energy consumption) criteria.

- Correctness analyses and performance evaluation: The objective of this task is to simulate and validate the system mapping and implementations derived by the BIP design flow. The challenges are to develop fast simulation tools, specific for the different design flows, as well as to propose novel validation methods, adapted for the system models developed in the project. Another important objective is to develop appropriate methodologies for system debugging supporting all dataflow based design flow.

- Statistical abstraction and statistical model checking: in this work our goal is to overcome the above difficulty by proposing a series of new techniques for the efficient verification of heterogeneous systems by combining Statistical Abstraction and Statistical-Model Checking. There are strong and promising evidences indicating that the concept of statistical abstraction should be formalized, and developed. It is also likely that statistical model checking algorithms can be made more efficient by taking the methodology used to design the system into account.

CHAPI - December 2009 – April 2013

FUI Project, Verimag budget: 174 k€
Partners:
Thales, Kalray, Alstom, CAPS Entreprise, Leadtech Design, UXP, CEA, DIGITEO/SCILAB
Verimag people involved:
J. Combaz, A. Triki, T. Abdellatif

General Objectives:
The collaborative project CHAPI supports the emergence of a new generation of programmable logic devices, which aims to serve the market demand in high performance and flexible integrated circuits for embedded computing.
CHAPI focused mainly on two topics:

- the optimization and validation of a first generation of circuits on use cases from several industrial application domains, and
- the integration of complementary software development tools to facilitate the development of new applications.

Verimag work in the project:
OASIS is a framework proposed by CEA for developing real-time applications, which was ported on the Kalray platform during the project. Our work in CHAPI consisted in using BIP as an intermediate language for verifying OASIS applications. This corresponded to two main working directions.
First, we developed a method and corresponding prototype tool for translating OASIS applications into BIP models. Such models use the real-time extension of BIP introduced before the project. The soundness of the transformation is established thanks to the formal semantics of both OASIS and BIP.
Second, we extended the compositional verification approach of D-Finder for real-time models. This allowed us to verify safety (invariance) properties for OASIS applications, by translating them into BIP models using our prototype tool. We also checked the applicability of the approach on typical examples.

EQINOCS - 2011-2014

ANR, Verimag budget: 70 k€
Partners:
LIAFA, LIGM, LACL, VERIMAG
Verimag people involved:
O. Maler, R. Iosif, IE. Mens, T. Ferrere, J. Lanik

General Objectives:
Study the entropy of timed languages and related concepts.

Verimag work in the project:
Developed new tools for integration (of probabilities) over zones. New algorithms for synthesizing controllers for scheduling problems under uniformly distributed durations, for robust monitoring os temporal properties and for learning over large alphabets.

AMT-SpaceEx - 2013-2014

Carnot, Verimag budget: 100 k€
Partners:
VERIMAG
Verimag people involved:
O. Maler, G. Frehse, O. Lebeltel, S. Minopoli

General Objectives:
Integration of STL Monitoring and Matlab/Simulink Models in SpaceEx

Verimag work in the project:
A new implementation of the AMT tool for monitoring analog signals against STL properties toward iuntegration in **SpaceEx**. In a similar vein, the project also develop and implement model transformations from the industrial standard Matlab/Simulink models to SpaceEx models. This capability significantly reduces the overhead that industrial partners incur when investigating and pursuing research collaborations with Verimag.

Cyberio - 2011-2014

Industrial, Verimag budget: 100 k€
Partners:
CYBERIO, VERIMAG
Verimag people involved:
S. Djoko-Djoko, A. Lekidis, M. Bozga, S. Bensalem

General Objectives:
The objective of the project has been the realisation of a computer-aided design tool for distributed sensor systems targetted by CYBERIO. The challenges for building such systems are managing the complexity of the distributed algorithms, the guarantee of performance while taking into account energy constraints, and the rapid deployment on specific target platforms and/or network infrastructures.
Verimag work in the project:
VERIMAG has extended the BIP design flow to the family of sensor systems considered. The work included elaboration/adaptation of programming models for sensor applications as well as the modeling of specific networks architectures and protocols (e.g., Can/CanOpen, WiFi, etc) in BIP. Moreover, the existing methods for performance evaluation and automatic code generation have been extended and implemented.

VERIDYC - October 2009 – March 2013

ANR, Total Budget: 598 k€, Verimag budget: 115 k€
Partners:
VERIMAG (leader), LIAFA, LSV, CEA Saclay, EDF R&D
Verimag people involved:
R.Iosif,M.Bozga

General Objectives:
The goal of this project is the verification of C programs that are used to control safety-critical systems, such as airplanes, subway lines or power plants.

Verimag work in the project:
A major problem is the scalability of existing verification techniques for programs with dynamic data structures. These techniques are capable nowadays of analyzing and finding bugs in toy programs of about 100 lines of code. In this project we aim, on one hand, at extending the existing verification techniques in order to deal with parallel programs handling singly-linked lists and array data structures. On the other hand, we aim at applying these techniques to real-life test cases with several thousands lines of C code.

HELP - December 2009 – June 2013

ANR Arpège, Total Budget: 700 k€, Verimag budget: 120 k€
Partners:
CNRS-Verimag (leader), CNRS-LEAT, INRIA-Aoste, STMicroelectronics, DOCEA Power
Verimag people involved:
F. Maraninchi, M. Moy, T. Bouhadiba, C. Helmstetter

General Objectives:
Energy consumption of consumer electronics systems (mobile phones, set-top-boxes, etc.) is a key point, even when they are not intended for mobility. For instance, if all the set-top-boxes in France could be put to some idle mode, this would spare one nuclear plant unit. The techniques to reduce energy consumption in circuits do exist, but the design methods for full systems are not adapted yet. Time-to-market constraints, and the growing complexity of systems, require that those design methods be improved, in particular by allowing an early analysis of the consumption by using abstract models, or virtual prototypes, long before the actual system is built. The project aims at: (i) defining high level models for the early expression of energy consumption objectives and implementation, and validating their fidelity w.r.t. real systems; (ii) defining a general method for the development of consumption-aware models, from functional models, integrated into industrial design flows, and validated on case-studies.

Verimag work in the project:
We have identified the relevant information for energy consumption models, and proposed a general instrumentation method that adds these information to a functional TLM model; we have defined a general co-simulation method, with a temperature simulator. The libraries developed in the project, available as free software, allow various levels of abstraction. The case-studies have been designed at several levels of abstraction, which gave interesting insights on the trade-off between simulation speed and precision.

ARESA2 - December 2009 – August 2013

ANR, Verimag budget: 137 k€
Partners:
Orange Labs, Coronis, VERIMAG, INRIA, LIG Grenoble, Telecom Bretagne
Verimag people involved:
F. Maraninchi, L. Mounier, S. Devismes, P. Lafourcade, K. Altisen, K. Heurtefeux

General Objectives:
The ARESA2 project aims at advancing the state of the art in Secure, Internet-Connected, Wireless Sensor and Actuator Networks.

Verimag work in the project:
We studied trade-offs between energy consumption and security in sensor networks. We defined the protocol SR3, a resilient routing algorithm for wireless sensor networks. We also worked on the level of details that are necessary in simulation models in order to get a faithful view of energy consumption. We defined and implemented new attacker models, in order to validate our protocol.

ACROSS - April 2010 - July 2013

European Project ARTEMIS, Total Budget: 4947 k€, Verimag budget: 305 k€
Partners:
The partners include in particular EADS Innovation Works, Germany, SELEX Electronic System S.p.A., Italy, CASSIDIAN, Germany, SYSGO AG, Germany, Thales Communications S.A., France
Verimag people involved:
S. Bensalem, B. Boyer, A. Griesmayer, M. Bozga, J. Sifakis

General Objectives:
The ACROSS project aims at achieving the following objectives:
an ACROSS-MPSoC that implements generic core services (e.g., deterministic communication, global time, diagnosis, fault and error containment) in an FPGA-based hardware for multiprocessor systems-on-a-chip (MPSoC) design and implementation of generic optional services to be used in multiple application domains a general model-based design methodology, supported by appropriate adaptable tools, for the implementation and verification of ACROSS-based applications taking into account existing domain-specific models/tools design and implementation of domain-specific optional services for the realization of embedded applications in the following domains: automotive, aerospace and industrial design and implementation of selected sample applications from the cited domains, which will show the benefits of using the ACROSS approach.

Verimag work in the project:
In this project we worked on the development of a tool-supported development methodology for the ACROSS platform. Its main purpose is bridging the gap between domain-specific processes where application engineers use modeling and programming, APIs, etc. dedicated to their individual problem domains, and the ACROSS hardware/software platform that provides a cross-domain technology for the efficient implementation of mixed-criticality systems. Consequently, the main benefit for application developers and system integrators from the different application domains is that the ACROSS development methodology provides methods and tools to efficiently manage the complexity originating from the architecture of the ACROSS platform. By relying on the knowledge of platform-experts condensed into platform components, models and tools, domain-experts can concentrate on the implementation of the required functionality, considering their particular industry-specific constraints and processes. The tool-support provided by WP3 is based on the model-driven development paradigm. In order to ensure the cross-domain applicability of the approach, and to provide the flexibility to co-operate with existing work flows, different integration levels have been defined for the ACROSS development process.
In the course of the project, we achieved the following results:

- Definition / integration of domain-specific and generic application meta-models, covering both functional and non-functional properties. Definition of platform meta-models providing an abstraction of the core and optional services defined in the ACROSS architecture (e.g., ACROSS MPSoC, operating system...).
- Definition of platform-specific meta-models for the configuration of the ACROSS platform. Algorithms, models and tools for analysis and verification (e.g., scheduler for the time-triggered network-on-chip, system-level design-space exploration, reliability analysis, ESL models, deadlock analysis, simulation.)
- Automatic model-to-model transformations (e.g., from domain-specific to generic application models, synthesis of platform-specific (configuration) models), source code and platform configuration files generators

Kalray - 2013-2014

Industrial, Verimag budget: 40 k€
Partners:
VERIMAG
Verimag people involved:
P. Tendulkar, P.Poplavko, S. Saidi, O. Maler, I. Galanommatis, C. Poorna, J. Maselbas,

General Objectives:
Application deployment on the Kalray platform

Verimag work in the project:
Developing an independent data-flow middle-ware for the platform and evaluating its performance experimentally.

LISE - 2008 – 2012

ANR, Total Budget: 553 k€, Verimag budget: 131 k€
Partners:
INRIA/LICIT(leader), INRIA/AMAZONES,DANTE/UVSQ, Supelec/Rennes, LORIA, UJF-Verimag, PtINT/Caen
Verimag people involved:
M-L. Potet, E. Mazza, S. Boulmé

General Objectives:
The LISE project (Liability Issues in Software Engineering) aimed to address liability issues from the legal and technical points of view. It was a multidisciplinary project involving lawyers and computer scientists. The goal was to cover the whole chain of of liability engineering, from liability specification (at contract negotiation time) to liability determination (at litigation time). Targeted applications are IT applications with critical aspects. Technical results of the LISE project is an effective framework allowing to define and establish liabilities according to the legal status of software and electronic evidences.
Verimag work in the project:
In the LISE project, Vérimag was in charge of the global demarch of liabibility description and resolution. We developed a platform helping the parties both in the drafting phase of the contract, in the definition of the architecture to collect evidence and in the liability establisment. We propose, and implement, some criteria characterizing architectures that are "acceptable", i.e. that permit to resolve conflicts, relatively to a set of potential claims.

Terra - 2011 – 2012

MSTIC UJF, Verimag budget: 50 k€
Partners:
Lig/Inria Mescal
Verimag people involved:
K. Altisen, S. Devismes, A. Gerbaud, P. Lafourcade, J.M. Vincent

General Objectives:
Numerous routing algorithms have been proposed for Wireless Sensors Networks (WSNs). In most cases, those algorithms are compared by performing numerical simulations on specific networks. Nevertheless, a formal analysis is needed to obtain general results. The project aims at proving some efficiency results on probabilistic routing protocols dedicated to large-scale Wireless Sensors Networks. Since these networks are time-evolving, this will imply the proposition of new metrics about the resiliency of the protocols. We aim at characterizing some classes of topologies for which we can theoretically compare algorithms and give upper bounds on their efficiency.

Verimag work in the project:
The project Terra is devoted to the analytic evaluation of distributed protocols dedicated to WSNs. Due to the characteristics of WSNs, those solutions must be resilient to topological changes. New routing protocols have recently been developed at Verimag. Numerical simulations suggest that they are time-efficient, resource-efficient and inherently self-adaptive. Nowadays, those facts must be formally enunciated, then proved. This implies to be able to evaluate analytically the quality of the protocols based on the quantity of resources involved, the average computation time, but also, some new concepts such as the resiliency of the protocols against topological changes.

SHIVA - 2010 – 2012

Minalogic, Verimag budget: 97 k€
Partners:
CS (leader), EASII IC, NETHEOS, UJF(IF-LJK-Vérimag), TIMA
Verimag people involved:
P. Lafourcade, L. Laknech, M-L. Potet

General Objectives:
Le projet SHIVA, Secured Hardware Immune Versatile Architecture, visait de fournir un module matériel programmable et reconfigurable, avec un haut niveau de sécurité évaluable au sens des critères communs à un niveau EAL4/5. Ce module s'intégrera dans des plates-formes d'infrastructure réseau à haut débit pour offrir aux entreprises, aux institutions et aux opérateurs la possibilité de sécuriser leur réseau, par application de leur propre chiffre symétrique, soit choisi ou spécialisé parmi des standards génériques, soit personnalisé. Deux modules sécurisés ont été produits en proof of concept (Module Netheos et Shiva-CS) ainsi que les plate-ofrmes logicielles garantissant la maîtrise des flux entrants/sortants.

Verimag work in the project:
Dans ce projet le rôle de Vérimag était de participer à la spécification des mécanismes de sécurité du module Shiva ey à la modélisation de certains de ces mécanismes. Une modélisation formelle d'un profil de protection EAL4+ pour les crypto-modules a été développé ainsi que la preuve calculatoire de protocoles d'échanges de clé.

MULTIFORM - 2008-2012

European project, Total Budget: 3700 k€, Verimag budget: 250 k€
Partners:
Verimag, Universities of Dortmund, Eindhoven, Aachen, Aalborg; Embedded Systems Institute, VEMAC, KVCA
Verimag people involved:
O. Maler, G. Frehse, O. Lebeltel, R. Ray

General Objectives:
Integrated Multi-formalism Tool Support for the Design of networked Embedded Control Systems

Verimag work in the project:
The main objective of the MULTIFORM project is the integration and the support for interoperability of tools and methods based on different modeling formalisms in order to make a significant step towards integrated coherent tool support for the design of large complex controlled systems from the first concept to the implementation and further on over their entire life cycle.
Verimag contributed the verification tools PHAVer and SpaceEx, and helped develop methods for model translation to and from the Computational Interchange Format (CIF) and for monitoring of control systems.

COMON - September 2009 – April 2012

Minalogic, Total Budget: 3000 k€, Verimag budget: 207 k€
Partners:
Atos Origin (France), Corys TESS (France), Rolls-Royce Civil Nuclear (France), CNRS-Verimag (France)
Verimag people involved:
N. Halbwachs, P. Raymond, E. Jahier, S. Djoko-Djoko, Chaouki Maiza

General Objectives:
COMON is a Minalogic project funded by the FUI (Fonds Unique Interministériel) and local authorities (Metro, ville de Grenoble).
The COMON project gathered Verimag and 3 industrial partners specialized in complementary parts of the design of control systems for nuclear plants. Corys TESS designs plant simulators that are used in particular for training operators. Atos Origin designs computerized control rooms (software and hardware). Rolls-Royce Civil Nuclear designs the software and hardware automatic mechanisms (classified by safety authorities) in charge of securing the plant.
Control systems in nuclear plants are very complex to set up, and involve a lot of providers that generally integrate their sub-systems after several years of work, when the plant is being built. Every problem encountered during this integration phase is very costly. Hence the will to add a little bit of agility in the process, and to integrate sub-systems as soon as possible. The motivation for this consortium was therefore to take advantage of the partners complementary background to set up a development framework based on early simulations, model refinements, and continuous integration. In other words, we wanted to follow a model-based approach principles, and rely on a early executable model that is refined and validated at each step of its elaboration.

Verimag work in the project:
In this project, we have demonstrated the use of our tools and languages, based on the synchronous paradigm, (1) to check the correctness of reactive systems developed incrementally, using heterogeneous industrial engineering workbenches; and (2) to elaborate consistent and accurate functional requirements. We have performed experiments where Lurette is controlling the 3 partners' workbenches on a custom case study designed to be representative of each partner's usual activity.
The interest expressed in Lurette by the three industrial partners of the COMON project is one of the reasons that convinced people to establish in 2013 the Argosim company. Argosim is developing the Stimulus tool based on the Lurette principles.

ASOPT - December 2008 – June 2012

ANR Arpège, Total Budget: 651 k€, Verimag budget: 136 k€
Partners:
INRIA-PopArt (leader), CNRS-VERIMAG, CEA-LMeASI / École polytechnique, INRIA-MaxPlus, EADS Innovation Works
Verimag people involved:
D. Monniaux, N. Halbwachs, V. Perrelle

General Objectives:
ASOPT is a fundamental research project proposal, involving software development for experimental and dissemination purposes.
Static program analysis basically consists in finding program invariants: properties that are known to hold for all executions. These invariants can often be expressed as geometric shapes. For instance, the index variables in nested loops often lie within simple shapes, such as triangles or convex polyhedra. Most abstract interpretation techniques leverage such geometrical properties in order to automatically obtain invariants. Many abstract interpretation techniques attempt to find "good", if not optimal, parameters for a geometric shape verifying certain constraints; this not only applies to purely numerical abstractions (for numerical program variables), but also to abstractions of data structures (arrays and more complex shapes). This problem can often be addressed by optimization techniques, opening the possibility of exploiting a wide range of advanced techniques from mathematical programming.
The purpose of this project is to develop new abstract domains and new resolution techniques to improve the quality of program analysis, especially for embedded control programs, and in the longer run, for numerical simulations programs. To this end, the project will bring together static analysis, optimization, and control/game theory experts around some program verification problems expressed geometrically, in order to invent, develop, and experiment new methods.

Verimag work in the project:
Main results:

- Polyhedra and linear programming in $(\max, +)$ algebra, extending applications of$(\max, +)$ algebra to programs, in particular for timed systems.
- Parametrization of zonotopes by other geometric shapes, accounting better for tests within programs.
- Generalization of solving of equation systems by policy iteration, yielding precise (and often optimal) invariants for a wider class of systems.

SCALP - 2008-2012

ANR, Total Budget: 472 k€, Verimag budget: 160 k€
Partners:
EVEREST-INRIA, Plume-LIP, ProVal-LRI, CPR-Cédric, VERIMAG/DCS.
Verimag people involved:
S. Boulmé, P. Corbineau, C. Ene, P. Lafourcade, Y. Lakhnech, J-F. Monin

General Objectives:
The SCALP project aims at having a Coq-based tool for proving correctness of cryptosystems. We will demonstrate its usefulness by considering three major areas: key-exchange protocols, and data integrity, and watermarking. In contrast to existing Dolev-Yao based verification tools, we will be able to treat group protocols and have complexity-theoretic proofs. More importantly, the tool will be open in the sense that it should be reasonably easy to consider new primitives. This does not seem easily achievable for symbolic tools.

Verimag work in the project:
First we develop an Hoare Logic to automatically prove the computational security of generic asymmetric encryption schemes. Then we proposed a Computational Indistinguishability Logic (CIL). CIL is a logic that supports concise and intuitive proofs across several models of cryptography. Its starting point is the notion of oracle system, an abstract model of interactive games in which adaptive adversaries play against a cryptographic scheme by interacting with oracles. Oracle systems are inspired by probabilistic process algebra, but do not commit to a particular model or syntax. As a result, they provide a unified foundation for cryptographic games, can be formalized neatly in a proof assistant, and capture both the standard model and idealized models such as the random oracle model or ideal ciphertext model. Moreover, oracle systems provide a unifying semantics for the different languages used in practical tools for cryptographic proofs Using this framework we are able to verify several exiting cryptographic schemes, like PSS.

SYNCHRONICS - 2008-2012

Action d'envergure INRIA, Verimag budget: 12 k€
Partners:
LIENS, INRIA PROVAL/ALCHEMY/POP ART, (n.b. This project was mainly internal to INRIA, Verimag-Synchrone appeared as a guest partner of the INRIA-POP ART team)
Verimag people involved:
Pascal Raymond, Erwan Jahier, Mouaid Alras

General Objectives:
The goal of the SYNCHRONICS project was to propose new languages (or extensions of existing ones) for the design and implementation of critical embedded systems. The project relied on the synchronous concurrency model, and on the formal definition of the language, in order to guarantee safety by construction. Synchronous languages (such as Lustre) were already well known and accepted in the domain of critical systems. The project aimed at going further by considering new questions, for instance: how to take into account asynchronous phenomena (jitter, execution time, communication through buffers)? how to mix discrete and continuous descriptions in a model-based design (hybrid language)? how to (efficiently) simulate thousands of concurrent synchronous processes? how to perform separate compilation of data-flow concurrent languages?

Verimag work in the project:
In this project, Verimag mainly worked on the extension of the synchronous paradigm and its compilation. We proposed with LIENS an object-oriented extension in order to improve reusability and versatility of the designs. We also worked on modular compilation of concurrent data-flow languages.

PRO3D - January 2010 – December 2012

European Project FP7, Total Budget: 2617 k€, Verimag budget: 353 k€
Partners:
CEA/LETI, EPF Lausanne, ETH Zurich, STMicroelectronics/Grenoble, University of Bologna
Verimag people involved:
A. Basu, S. Bensalem, M. Bozga, J. Sifakis

General Objectives:
During the last three decades, the performance of microprocessors and microcontrollers has steadily increased at the impressive rate of 100 times per decade. This was fuelled by: (1) The exponential growth in clock speeds; (2) The exponential growth in the number of transistors per die; and (3) The acceleration of instruction flows obtained by various techniques for reducing latency and maximising the amount of computation per clock cycle.
However, this picture was rapidly and radically changing. The shift to parallel architectures was not at all the consequence of a scientific breakthrough. It was primarily a consequence of hitting technology walls that prevented from pushing forward the efficient implementation of traditional uniprocessor designs in silicon. These technologies hitting walls are: (a) Voltage scaling and power reduction techniques, or Power Wall; (b) Instruction-level parallelism, or Complexity Wall; (c) Memory latency hiding techniques, or Memory Wall; (d) Reliable and low-variability silicon technology, or Yield Wall.
As an illustration of the rapidly evolving context of PRO3D, we can mention that the expected industrial solutions to the Memory Wall changed dramatically during the course of the project. At the start of PRO3D the most promising solution was WideIO, where a dedicated memory layer is connected to the computing fabric by vertical interconnects. This solution was expected to outperform the flat, 2D, LPDDR solutions both in speed and energy efficiency. By the time the project completed, the LPDDR roadmap had accelerated to the point of overlapping significantly WideIO whith an incremental evolution of the standard, 2D-based, solution: LPDDR3 and LPDDR4.
The PRO3D project proposed a holistic approach for the development activities ranged from programming to architecture exploration and fabrication technologies, and yield the following outcome: (1) Thermal Modelling and Simulation. (2) Programming, compilation, verification and deployment for 3D manycore architectures, including Statistical Model Checking (SMC) of System Models. (3) Exploiting 3D opportunities into multicore architectures. (4) System-level thermal-aware exploration and analysis of 3D designs. (5) Virtual Prototyping.

Verimag work in the project:
In PRO3D project we developped a rigorous design flow based on the BIP and DOL component framework: The flow is (i) model-based, that is, both application software and mixed hardware/software system descriptions are modeled by using a single, semantic framework; (ii) it is component-based, that is, it provides primitives for building composite components as the composition of simpler components; (iii) it is tool-supported, that is, all steps in the design flow are realized automatically by tools; (iv) It supports Satistical Model Checking of system models (SMC).
The core idea of SMC is to conduct simulations of the system and then use statistical results in order to decide whether the system satisfies the property or not. For instance, SMC can be used to estimate the probability that a system satisfies a given property. In contrast with exhaustive approaches, a simulation-based solution does not guarantee a correct result. However, it is possible to bound the probability of making an error. In PRO3D, SMC has been successfully applied through the BIP framework for evaluation of performance properties of mixed hardware/software system models.

SMECY - February 2010 – February 2012

European Project ARTEMIS, Total Budget: 6513 k€, Verimag budget: 312 k€
Partners:
The partners include in particular CEA, Hellenic Aerospace Industry S.A., ST Microelectonics, Saab AB, Electronic Defense Systems, ACE Associated Compiler Experts b.v. Netherlands
Verimag people involved:
S. Bensalem, M. Bozga, P. Bourgos, A. Nouri, J. Sifakis

General Objectives:
SMECY envisions that recently emerged multi-core technologies will rapidly develop to massively parallel computing environments which, due to improved performance, energy and cost properties, will extensively penetrate the embedded system industry in a few years. This will affect and shape the whole business landscape, e.g. semiconductor vendors need to be capable of offering advanced multicore platforms to diverse application sectors, IP providers need to retarget existing and develop new solutions to be compatible with evolving multicore platforms and the need of embedded system houses, in addition to product architecture adaptations and renewing their system, architecture, software and hardware development processes. The SMECY project aims at achieving the following objectives:

1. develop new programming technologies enabling the exploitation of many (100s) core architectures.
2. launch an ambitious European initiative to match initiatives in Asia (e.g. teams funded by JST/CREST programmes) and USA (e.g. PARLAB in Berkeley, Parallel@illinois and Pervasive Parallelism Laboratory in Stanford) and to enable Europe to become the leader.

Verimag work in the project:
In the SMECY project we developed a new programmable architectural solutions based on multicore technology, and associated supporting tools in order to master complete system design of future smart multicore embedded systems. All of this is strongly driven by the requirements and constraints from different application areas as well as the target platform.
The hardware platforms and the development tools developed has been demonstrated and evaluated for a certain set of representative applications provided by industrial partners of SMECY, such as radar systems, video/audio treatments and energy efficient wireless communication systems.

FullMDE - 2011 - 2012

Industrial Collaboration, Verimag budget: 20 k€
Partners:
EADS (coordinator), Esterel, Praxis, IRIT, ESA (funding provider)
Verimag people involved:
Susanne Graf, Imen Ben Hafaiedh (doc)

General Objectives:
FullMDE is a follow-up project of the ASSERT IP which was mainly concerned with non functional requirements and code generation taking these into account. The objective of FullMDE "Full Model Driven Development for On-Board Software" is to complete the ASSERT project by a functional approach.

Verimag work in the project:
The objective of Verimag was to help IRIT to extend the OMEGA-IF tool to deal with AADL specifications and to experiment with a contract-based approach.

AVOTE - 2007-2011

ANR, Total Budget: 529 k€, Verimag budget: 139 k€
Partners:
LSV, LORIA, VERIMAG.
Verimag people involved:
C. Ene, P. Lafourcade, Y. Lakhnech, J-F Monin

General Objectives:
The AVOTE project aims at using formal methods to analyze electronic voting protocols.

Verimag work in the project:
We studied electronic voting protocols. We proposed a complete hierachy of security properties. This allows us to compare some protocols that were uncomparable using previous frameworks. We also show that for verification privacy properties of voting protocols, considering one coerced intruder is enough.

SFINCS - 2008-2011

ANR, Total Budget: 445 k€, Verimag budget: 131 k€
Partners:
LIFL/POPS, LIF/MOVE, Norsys, TRUSTED LOGIC, VERIMAG/DCS.
Verimag people involved:
P. Lafourcade, Y. Lakhnech, L. Mounier, M. Périn

General Objectives:
The SFINCS project aims at studying applications of this theory on practical use-cases to identify bottlenecks that prevent wider industrial adoption of information flow control techniques.

Verimag work in the project:
We studied non interference for deterministic encryption. We developed a type system for secure information flow to prevent a program from leaking information from variables that hold secret data to variables that hold public data. The intuition that encrypting a secret yields a public value, that can be stored in a public variable, is faithful for probabilistic encryption but erroneous for deterministic encryption. We prove the computational soundness of our type system in the concrete security framework. We also develop an Hoare Logic to automatically prove the computational security of generic asymmetric encryption schemes.

MIND - August 2008 – April 2011

Minalogic Project, Verimag budget: 114 k€
Partners:
STMicroelectronics, France Telecom R&D, LOGICA, Schneider Electric, Sogeti High Tech, INERIS, ST Ericsson, Itris Automation Square, INRIA, IST, ISTIA
Verimag people involved:
J. Combaz, M. Poulhiès

General Objectives:
MIND is a Minalogic project that aimed at developing an industrial technology for component-based construction of software for embedded systems. This includes the development of programming languages (extended C, ADL, IDL), a chain for compiling architectures and generating code, and a graphical IDE integrated into Eclipse. These developments are extendable and adaptable to constraints specific to partners.

Verimag work in the project:
During the project, we considered a specialization of the MIND language for data-flow applications, namely MIND-DF. The expression of a MIND-DF application relies on the mechanism of annotations offered by the MIND framework.
Our goal in the project was to provide automated means for verifying MIND-DF applications. Properties to verify are of two types: *(i)* functional properties, i.e., the application runs without deadlock meaning that there is no problem with communication FIFOs sizes, initial elements in the FIFOs (e.g. for feedback loops), and produce/consume rates, and *(ii)* temporal properties such as latency or throughput.
To this end, we developed a prototype tool for translating MIND-DF programs into BIP models from which we can use existing verification tools such as D-Finder. The applicability of the approach was demonstrated for functional properties by applying the tool chain on several input examples written in MIND-DF. For non functional properties, we specified how to include temporal properties in the generated BIP models.

VEDECY - 2009-2011

ANR, Total Budget: 419 k€, Verimag budget: 175 k€
Partners:
POP-ART Inria Grenoble, Laboratory Jean Kuntzmann Grenoble, VERIMAG
Verimag people involved:
T. Dang, T. Dreossi

General Objectives:
Verification of Cyber-Physical Systems

Verimag work in the project:
Specific approaches for reachability analysis of nonlinear systems that are significantly more scalable than those currently available

ATHOLE - 2007-2011

Minalogic, Total Budget: 2500 k€, Verimag budget: 850 k€
Partners:
ST, CEA-LETI, Thales, CWS, VERIMAG
Verimag people involved:
O. Maler, S. Saidi, J. Legriel, JF. Kempf, P. Tendulkar, O. Lebeltel, G. Frehse, A. Degorre

General Objectives:
Develop and deploy applications on the P2012 platform of ST

Verimag work in the project:
We developed methods for multi-criteria optimization for solving optimal deployment problems for data-flow applications on multi-cores. We developed a tool for high-level design-space exploration. We investigated question related to the efficient utilization of DMAs for data-parallel applications.

CIFRE-Leguen - 2009-2011

Industry, Total Budget: 45 k€, Verimag budget: 45 k€
Partners:
STMicroelectronics, VERIMAG/Synchrone.
Verimag people involved:
D. Monniaux, N. Halbwachs, J. Leguen

General Objectives:
Accompanying contract to the CIFRE thesis of Julien Leguen

Verimag work in the project:
Static analysis of SSA code using abstract interpretation.

CIFRE-Pietrek - 2009-2011

Industry, Total Budget: 45 k€, Verimag budget: 45 k€
Partners:
Kalray, VERIMAG/DCS.
Verimag people involved:
J.-C. Fernandez, A. Pietrek

General Objectives:
Accompanying contract to the CIFRE thesis of Artur Pietrek

Verimag work in the project:
CLI-JIT Compilation for Embedded Media Processing

CIFRE-Funchal - 2008-2011

Industry, Verimag budget: 37.5 k€
Partners:
STMicroelectronics, VERIMAG/Synchrone.
Verimag people involved:
F. Maraninchi, M. Moy, G. Funchal

General Objectives:
Accompanying contract to the CIFRE thesis of Giovanni Funchal

Verimag work in the project:
Definition of components with multiple levels of abstraction, for the transactional modeling of systems-on-a-chip.

FoToVP - 2007-2010

ANR, Total Budget: 148 k€, Verimag budget: 99 k€
Partners:
VERIMAG, IRISA Rennes
Verimag people involved:
F. Maraninchi, M. Moy, K. Altisen, Y. Liu, U. Bordoloi

General Objectives:
In the context of past or current projects involving industrial partners from various application domains, the participants of FoToVP have observed several approaches for the design of complex and/or critical embedded systems, based on the notion of virtual prototyping. This allowed us to identify clearly where there is a need for formal tools. We started studying the benefits of formal methods and tools in the other projects, with the constraints of particular application domains, and with practical objectives in mind. Some recurring problems appeared, that need to be investigated further, independently of these application domains, and with less constraining short-term practical objectives. In this project called FoToVP, standing for "Formal Tools for Virtual Prototyping of Embedded Systems", we would like to study these recurring problems, in order to develop more fundamental and generic results. The motivations are clearly related to industrial applications, and the applicability of the project results will be evaluated with respect to these industrial practises and applications.

Verimag work in the project:
We have established a link between two types of models: (1) abstract models manageable with analytic calculus, but hardly faithful to real systems; (2) Computational models that improve faithfulness but are usable for simulation only.
We have shown how to exploit the SSA form of compilers for a direct automatic translation of a model written in a language like SystemC or Java, into a mathematical model that can be analyzed by formal verification tools. This has been exploited by Verimag for SystemC.

ARESA - 2006-2010

ANR, Verimag budget: 150 k€
Partners:
VERIMAG, CITI Lyon, LIG Grenoble
Verimag people involved:
F. Maraninchi, L. Mounier, O. Bezet

General Objectives:

Verimag work in the project:

SPEEDS - May 2006 - May 2010

European IP, Total Budget: 9050 k€, Verimag budget: 770 k€
Partners:
The academic partners were INRIA, OFFIS and PARADES, and the main industrial partners Airbus (coordinator), Bosch, EADS, Esterel Tech, IBM, SAAB.
Verimag people involved:
Susanne Graf (local coordinator), M. Bozga, J. Sifakis, S. Quinton (doc), I. Ben-Hafaiedh (doc), S. Prochnow (postdoc), H. Ruiz-Bareda (postdoc)

General Objectives:
The SPEEDS project aimed at significant improvements of productivity and competitiveness of the European industry in the fields of embedded system- and component design, design-quality, testing and integration and certification of avionics / electronics applications. It builds on existing standards like SysML. It defines modeling concepts, methodologies and analysis methods while incorporating them in an environment of commercial development tools.

Verimag work in the project:
Our main objectives in SPEEDS were

1. to participate in the definition of the HRC (Heterogeneous Rich Components) metamodel, an open model constructed to seamlessly extend the capabilities of existing industry-specific system engineering meta-models like AUTOSAR and AADL. HRC forms the foundations for a component based construction of complete virtual system models. SPEEDS supports a concept of coarse grained integration of COTS tools via the meta-model.

2. to provide a generic contract meta-theory allowing to extend almost any component framework to a hierarchical contract framework equipped with powerful reasoning rules for checking contract satisfaction and dominance

3. to implement prototype tools for handling the case studies provided by the industrial partners.

OMEGA-4-Rhapsody - 2009-2010

Direct Industrial Collaboration, Total Budget: 50 k€, Verimag budget: 50 k€
Partners:
A direct collaboration with ESA, the European Research Agency
Verimag people involved:
Susanne Graf and Iulian Ober (IRIT)

General Objectives:
This is a follow-up project of the European projects OMEGA (2002-2005) and ASSERT (2004-2008) were we had extended the IF toolset to an analysis and verification tool for rich operational UML models. In this project, the aim was to extend the OMEGA-IF tool to allow the analysis of models produced with Ilogix' Rhapsody

Verimag work in the project:
We have extended the subset of UML accepted to a large subset of the operational part of UML 2.0 as accepted by the Rhapsody modeller; in particular we have integrated architecture models and parallel state charts.

OpenTLM - 2006 — 2010

Minalogic (FUI), Total Budget: 5000 k€, Verimag budget: 426 k€
Partners:
STMicroelectronics/Grenoble, Orange IT&L@bs, Safetronix, INRIA/pop-art, CEA/LETI, TIMA, UJF-Verimag
Verimag people involved:
F. Maraninchi, M. Moy, K. Marquet, T. Bouhadiba

General Objectives:
The objective of the OpenTLM project is to offer to embedded software developers a tool kit, available under open source license, and based on the SystemC/TLM standard. It enables them to develop and test the embedded software ahead of availability of hardware platforms (silicon, but also hardware emulators). It gives the opportunity to promote a broader use of the TLM methodology, already adopted by hardware teams, as well as a better concurrent development of hardware and software parts of the system. Indeed, if software is mature enough when silicon is available, the overall period for system integration is reduced, which accelerates the availability of the product and optimizes time-to-market.
Software included in the openTLM toolkit include software execution and debugging tools, verification tools, and basic software building blocks.

Verimag work in the project:
Verimag contributed verification tools. A runtime-verification tool called SCRV allows improving the coverage of existing testsuites. The tool PinaVM includes a compiler front-end able to extract semantic information from a SystemC/TLM program, and a back-end allowing the use of the SPIN model-checker to formally verify properties on the input program.

Combest - December 2008 – December 2010

European Project FP7, Total Budget: 2750 k€, Verimag budget: 530 k€
Partners:
EADS/Innovation Works (Germany), ETH Zurich, Israeli Aircraft Industry, INRIA, OFFIS, TU Braunschweig, Università degli Studi di Trento
Verimag people involved:
S. Bensalem, M. Bozga, B. Jobstmann, B. Bonakdarpour, J. Sifakis

General Objectives:
The project pursues a dual approach, combining fundamental work with methods and tools for rigorous embedded systems design.
The fundamental work in COMBEST studies component-based design, by tackling two main problems:

1. Developing frameworks for the composition of heterogeneous components.
2. For such frameworks, develop theory allowing constructivity: inferring global properties of a system from the properties of its components. The methods and tools developed use results of the theoretical work, to ensure a rigorous design for heterogeneous systems. The tools cover modelling, verification, and performance analysis. Their use is supported by a global design methodology. In addition, we use two case studies, provided by industrial partners, to evaluate applicability of the tools.

Verimag work in the project:
For embedded systems, component-based design techniques should address both hardware and software components in a unified way. They should be able to handle hard constraints on performance and dependability as well as dissimilarities between levels of abstraction and communication primitives. The two main difficulties to handle are:

- The presence of heterogeneous components. In software engineering, components are mainly used for structuring functions and associated data. In contrast, hardware components are inherently parallel, and synchronous.
- Predictability of basic properties of the designed system. We argue in favour of constructivity, which is reasoning about global system properties based on properties of its individual components. Constructivity should allow satisfaction of essential properties by construction, to avoid costly a posteriori global system validation. In this project, we provided a formal frameworks which overcome these difficulties. The theoretical results has been integrated in coherent component-based design flows and validated through comparison with existing industrial practice. Furthermore, these theoretical results has been implemented in scalable supporting methods and tools.

Sympaa - 2010

Industrial, Verimag budget: 20 k€
Partners:
ACTOLL, CEA, VERIMAG
Verimag people involved:
M. Bozga, J. Sifakis

General Objectives:
The ACTOLL company is leader on information systems and electronic banking for motorway transportations systems. The aim of this project was the modeling, analysis and implementation of an embedded controller for payment with credit cards at motorways tolls, using BIP

Verimag work in the project:
In a first phase, a complete BIP model of the controller has been developed by VERIMAG in collaboration with CEA. The model has been functionally validated using BIP tools. In a second phase, the BIP model has been used to produce a multi-threaded implementation. This implementation runs on top of the BIP engine. It has been deployed on the target platform, validated and nowadays, effectively used at tolls of a motorway in the north of France.

CeProMi - January 2008 – December 2009

Action de Recherche Coopérative INRIA, Total Budget: 29 k€, Verimag budget: 0 k€
Partners:
INRIA-Proval (Saclay), Verimag-DCS (Grenoble), INRIA-Gallium (Rocquencourt) et INRIA-Cassis (Besançon/Nancy).
Verimag people involved:
S. Boulmé, M-L. Potet

General Objectives:
The CeProMi project studied how to achieve *modular* reasoning about sequential and imperative programs that involve memory sharing between components: typically, programs written in C, Java or ML. Hence, its issue was to find *sound* reasonings from *local* properties of components (objects or modules), such that for each component, its local properties are proved independently of its clients.

Verimag work in the project:
Sylvain Boulmé and Marie-Laure Potet of Verimag-DCS have proposed a conservative extension of the B method that supports more state sharing between components. This proposal is inspired by the Spec# approach of Leino. They also help to supervise two PhD students of INRIA-Proval. First, Wendi Urribarí has proposed mechanisms of composition and refinement from B in order to design a module system à la Leroy for the Why language (a subset of ML extended with Hoare assertions). Second, Asma Tafat extended the Spec# approach with a notion of refinement inspired from B in the context of the Krakatoa language (a subset of Java extended with Hoare assertions). Her work led to a publication with Claude Marché (INRIA-Proval) and Sylvain Boulmé (Verimag-DCS).

OpenEmbeDD - May 2006 - May 2009

ANR, Verimag budget: 170 k€
Partners:
In this platform project, CEA, LAAS and INRIA (several teams) were the academic partners, and Airbus, CS, France Telecom and Thales the main industrial partners
Verimag people involved:
S. Graf, M. Bozga, J. Sifakis, O. Constant (postdoc), Y. Chkoury (doctorant)

General Objectives:
OpenEmbeDD is an Eclipse-based "Model Driven Engineering" platform dedicated to Embedded and Real-Time systems (E/RT). Its aim is to offer engineers who design and develop E/RT software the means to express, simulate, validate and test the targeted system before any component has been solded on a circuit board. The OpenEmBeDD project has been continued in the Artemis CESAR project, see OpenEmBeDD Website

Verimag work in the project:
Our objective in this project was to integrate our model-based technology into the platform and to run the tools in two case studies. We have defined and implemented a AADL-to-BIP transformation which allowed to simulate and verify the AADL case study provided by CS, and we have extended the UML-based perfomance analysis framework developed in the PerSiForm project to allow Thales to conduct the performance analysis on their case study.

EDEN2 - March 2006 - August 2009

ANR, Total Budget: 1205 k€, Verimag budget: 182 k€
Partners:
Axalto Cards and Terminals division, CEA Grenoble (LETI), CEA Saclay (LIST), Trusted Labs Versailles, Université Joseph Fourier/VERIMAG
Verimag people involved:
M. Périn, I. Narasamdya, M. Garnacho, J.O. Blech

General Objectives:
The ANR Eden2 project (2006-2009) aimed at defining methodology and tools for the certification of security applications at the highest level of the Common Criteria. The Common Criteria (CC) is an international standard for the evaluation of security related systems. It guarantees that a target of evaluation enforces security policies by tracking the security requirements along the development process. The Common Criteria Methodology requires to describe and relate the security concerns at several levels of details: the security policy model (SPM), the functional specification of security functions (FSP) and the low-level design of the target system (TDS). The evaluation toward a certification consists in checking that two adjacent levels in the development chain satisfy a conformance relation that ensures the preservation of security properties. At the highest level of the CC certification, which is called evaluation assurance level 7 (or EAL7), the specification of each level must be formal and the conformance relation between adjacent levels must be formally proved. The Eden2 methodology was applied to applications for smart-cards. Trusted Labs and Axalto patented part of the methodology and transfered results of the projet in their industrial developments.

Verimag work in the project:
In the Eden2 project, we proposed a precise and formal definition of security conformance relation. Conformance between two levels of specification is formulated in a general framework of inclusion of behavioral trace and the conformance proofs are conducted in the theory of inter-program properties. These results were presented at SAS'09 [D-C184]. The accompanying verification techniques has been presented at FASE'09 [D-C183]. They are based on Floyd-Hoare's principle for proving that a program enforces a property, extended to two programs (which correspond to two adjacent levels) and considering a property that relates the security variables of the two programs.
The certification authorities (eg. DCSSI) did not trust the result of the validation tools used to establish conformance properties. So, with M.Garnacho (Phd 2006-2010) and J.O Blech (post-doc 2008-2009) we started certifying verdict of our validation tools by generation of certificates in a form that can be submitted to a trustable certificate checkers (the Coq proof checker). The results were published [D-J44, D-C156, D-C157, D-P14, D-J12].

GENESYS - June 2006 – June 2009

European Project FP7, Total Budget: 1850 k€, Verimag budget: 48 k€
Partners:
The partners include in particular STMicroelectronics, NXP Semiconductors Netherlands B.V.
Verimag people involved:
S. Bensalem, S. Bliudze, J. Sifakis

General Objectives:
It was the objective of the GENESYS project to develop a cross-domain reference architecturefor embedded systems that meets the requirements and constraints documented in the ARTEMIS SRA. These ARTEMIS requirements are composability, networking and security, robustness, diagnosis and maintenance, integrated resource management, evolvability and self-organization. The reference architecture will be domain-independent and serve as a template that can be instantiated to concrete platforms for individual application domains (i.e., automotive, avionic, industrial control, mobile, consumer electronics). In more detail, the objectives are as follows:

- The first technical objective is the definition of a cross-domain architectural style, which encompasses fundamental architectural principles for an as large as possible common set of platform services. A principle is an accepted statement about some fundamental insight in a domain of discourse. Principles form the basis for the formulation of operational rules. In GENESYS these principles are operationalized in the templates of the architectural service specification. The architectural principles guide the architecture designer in such a way that the cross-domain reference architecture meets the ARTEMIS challenges.

- Based on the cross-domain architectural style, a reference architecture template will provide a concise description of platform services. It will be possible to instantiate the template for individual domains in order to meet the specific requirements of an application domain. The sets of platform services at the different integration levels will represent generic component libraries. Any particular instantiation of the template will incorporate a selected subset of the platform services at the respective level of integration (i.e., chip-level, device-level, open or closed system-level).

- Another objective is the development of a model- and quality-driven development methodology for the reference architecture template. We will define a methodology framework for real-time embedded systems by extending the existing model-and quality-driven architecture development approaches by measurable quality characteristics (e.g., performance, reliability, maintainability).

- The fourth objective is the prototypical evaluation of the reference architecture template. Four exploratory prototypes for the industrial and consumer domains will demonstrate and help to evaluate the feasibility of selected central architectural concepts and services in the targeted application domains. The prototypes will concentrate on exemplary integration levels, namely the chip- and device-levels. Suitable programming languages (e.g., C) and hardware description languages (e.g., VHDL) will be used for developing the software (e.g., tools, software implementations of platform services) and hardware (e.g., hardware implementation of platform services) for the prototype implementations.

Verimag work in the project:

Appendix F

Risk evaluation document
Document unique d'évaluation des risques

Document des résultats de l'évaluation des risques

Université Joseph Fourier - Niveau Unité de travail

.

Unité : laboratoire, pool TP, services techniques	*Nom de l'unité / Bâtiments concernés (situation géographique)* *Laboratoire VERIMAG – UMR 5104* *Centre Equation, 2 avenue de Vignate – 30610 Gières* *Cette unité est elle une unité mixte ? Oui* *Si oui INSERM /CEA/CNRS/INRA/ autres : CNRS*
Principales activités	Recherche en informatique
Directeur / Responsable / Chef de service	Nicolas HALBWACHS, directeur du laboratoire
Lieux de travail	Désignation des lieux de travail VERIMAG, bâtiment centre équation 3 et centre équation 4, Centre des technologies du logiciel Surface des locaux 1440 m2
Animateur de l'évaluation des risques	Nom : SAUNIER CAILLY Christine Fonction : Responsable administrative
Personnes associées à l'évaluation *(nombre et fonction)*	Phase d'évaluation Tous les personnels permanents du laboratoire Phase de planification Animateur et Directeur
Signature du Directeur / Responsable/ chef de service	Date 01/01/2014 Signature

La signature de ce document vaut validation de l'ensemble du document unique : inventaire et évaluation des risques, mais aussi plan d'actions

©Réalisation ABCYS Consulting - City Parc 38 rue de la Tuilerie- 38170 SEYSSINET- Tel : 04-38-70-11-00 www.abcys-consulting.com

Fiche d'identification et évaluation des Risques

UNITE DE TRAVAIL **Laboratoire VERIMAG**

Lieu de travail	Dangers communs ou équipement ou matériel ou produit	Risques associés	Description des risques	F	Caractéristique d'exposition	G	Moyens de prévention existants	Moyens de prévention inexistants ou dysfonctionnements	Correct	A améliorer	A redéfinir ou à mettre en place	M	NRR	Améliorations possibles
couloir	**cheminement**	**collision, chute**	**armoire dans couloir**	**4**	**encombrement**	**1**	TOH	TOH		x		0,10		
							TOH	TOH						
							TOH	TOH						
							TOH	TOH						
							TOH	TOH						
							TOH	TOH						
							TOH	TOH						
							TOH	TOH						

Appendix G

List of staff
Liste des personnels

G.1 Signed List of Permanent Staff

aeres
agence d'évaluation de la recherche et de l'enseignement supérieur

liste des personnels(chercheurs, enseignants-chercheurs et assimilés) de l'unité présents au 30 juin 2014 et qui seront toujours au 1er janvier 2016

Nom	Prénom	grade	Etablissement ou organisme employeur	N° de l'équipe interne de rattachement, le cas échéant	Date d'arrivée dans l'unité	Emargement
ALTISEN	Karine	MCF	GRENOBLE INP	E1	09/2002	
BENSALEM	Saddek	PR1	U GRENOBLE 1	E2	01/1999	
BIDINGER	Philippe	MCF	U GRENOBLE 1	E2	09/2006	
BOULME	Sylvain	MCF	GRENOBLE INP	E2	01/2008	
CARRIER	Fabienne	MCF	U GRENOBLE 1	E1	01/1999	
CORBINEAU	Pierre	MCF	U GRENOBLE 1	E2	09/2008	
DANG	Thao	CR1	CNRS	E3	01/2008	
DEVISMES	Stéphane	MCF	U GRENOBLE 1	E1	09/2008	
ENE	Cristian	MCF	U GRENOBLE 1	E2	01/2004	
FERNANDEZ	Jean-Claude	PR Ex1	U GRENOBLE 1	E2	07/2002	
FREHSE	Goran	MCF	U GRENOBLE 1	E3	09/2006	
GRAF	Susanne	DR2	CNRS	E2	01/1999	
HALBWACHS	Nicolas	DR1	CNRS	E1	01/1999	
IOSIF	Radu	CR1	CNRS	E2	10/2002	

Nom	Prénom	grade	Etablissement ou organisme employeur	N° de l'équipe interne de rattachement, le cas échéant	Date d'arrivée dans l'unité	Emargement
LAKHNECH	Yassine	PR2 Ex 1	U GRENOBLE 1	E2	09/1999	
MAIZA	Claire	MCF	GRENOBLE INP	E1	09/2010	
MALER	Oded	DR1	CNRS	E3	01/1999	
MARANINCHI	Florence	PR2 Ex1	GRENOBLE INP	E1	09/2000	
MONIN	Jean-françois	PR2	U GRENOBLE 1	E2	09/2003	
MONNIAUX	David	DR2	CNRS	E1	09/2007	
MOUNIER	Laurent	MCF	U GRENOBLE 1	E2	01/1999	
MOY	Matthieu	MCF	GRENOBLE INP	E1	12/2006	
NICOLLIN	Xavier	MCF	GRENOBLE INP		01/1999	
PARENT-VIGOUROUX	Catherine	MCF	U GRENOBLE 1	E1	01/1999	
PERIN	Michaël	MCF	U GRENOBLE 1	E2	06/2001	
POTET	Marie-Laure	PR2	GRENOBLE INP	E2	01/2008	
RASSE	Anne	MCF	U GRENOBLE 1		01/1999	
RAYMOND	Pascal	CR1	CNRS	E1	01/1999	
RIPPERT	Christophe	MCF	GRENOBLE INP		03/2005	
WACK	Benjamin	PRAG	U GRENOBLE 1		06/2012	

G.2 Teachers-Researchers

Karine Altisen, MCF Grenoble INP, Synchrone team, in Verimag since 09/2002.

Saddek Bensalem, PR1 UJF, DCS team, in Verimag since 01/1999.

Philippe Bidinger, MCF UJF, DCS team, in Verimag since 09/2006.

Sylvain Boulme, MCF Grenoble INP, DCS team, in Verimag since 01/2008.

Fabienne Carrier, MCF UJF, Synchrone team, in Verimag since 01/1999.

Pierre Corbineau, MCF UJF, DCS team, in Verimag since 09/2008.

Stéphane Devismes, MCF UJF, Synchrone team, in Verimag since 09/2008.

Cristian Ene, MCF UJF, DCS team, in Verimag since 01/2004.

Jean-Claude Fernandez, PRCE1 UJF, DCS team, in Verimag since 07/2002.

Goran Frehse, MCF UJF, Tempo team, in Verimag since 09/2006.

Yassine Lakhnech, PRCE1 UJF, DCS team, in Verimag since 09/1999.

Claire Maiza, MCF Grenoble INP, Synchrone team, in Verimag since 09/2010.

Florence Maraninchi, PRCE1 Grenoble INP, Synchrone team, in Verimag since 09/2000.

Jean-François Monin, PR2 UJF, DCS team, in Verimag since 09/2003.

Laurent Mounier, MCF UJF, DCS team, in Verimag since 01/1999.

Matthieu Moy, MCF Grenoble INP, Synchrone team, in Verimag since 12/2006.

Xavier Nicollin, MCF Grenoble INP, in Verimag since 01/1999.

Catherine Parent-Vigouroux, MCF UJF, Synchrone team, in Verimag since 01/1999.

Michaël Perin, MCF UJF, DCS team, in Verimag since 06/2001.

Marie-Laure Potet, PR1 Grenoble INP, DCS team, in Verimag since 01/2008.

Anne Rasse, MCF UJF, in Verimag since 01/1999.

Christophe Rippert, MCF Grenoble INP, in Verimag since 03/2005.

Benjamin Wack, PRAG UJF, in Verimag since 06/2012.

G.3 Researchers

Thao Dang, CR1 CNRS, Tempo team, in Verimag since 01/2008.

Susanne Graf, DR2 CNRS, DCS team, in Verimag since 01/1999.

Nicolas Halbwachs, DR1 CNRS, Synchrone team, in Verimag since 01/1999.

Radu Iosif, CR1 CNRS, DCS team, in Verimag since 10/2002.

Oded Maler, DR1 CNRS, Tempo team, in Verimag since 01/1999.

David Monniaux, DR2 CNRS, Synchrone team, in Verimag since 09/2007.

Pascal Raymond, CR1 CNRS, Synchrone team, in Verimag since 01/1999.

G.4 Engineers, Administrative staff

Marius-Dorel Bozga, IR CNRS, DCS team, in Verimag since 01/2001.

Rosen Carbonero, Technicienne de recherche et formation UJF, in Verimag since 09/2006.

Jacques Combaz, IR CNRS, DCS team, in Verimag since 12/2008.

Patrick Fulconis, IE UJF, in Verimag since 01/2014.

Philippe Genin, AI CNRS, in Verimag since 02/2012.

Erwan Jahier, IR CNRS, Synchrone team, in Verimag since 09/2002.

Olivier Lebeltel, IR CNRS, Tempo team, in Verimag since 05/2010.

Sandrine Magnin, Adjointe technique recherche et formation UJF, in Verimag since 04/2007.

Valérie Roux-Marchand, Technicienne en gestion administrative CNRS, in Verimag since 02/2002.

Christine Saunier-Cailly, Technicienne de recherche et formation UJF, in Verimag since 09/2002.

G.5 Temporary engineers, Postdocs

Irina Asavoae, Postdoc, Synchrone team, in Verimag since 01/2013.

Mihail Asavoae, Postdoc, Synchrone team, in Verimag since 01/2013.

Lacramioara Astefanoaei, Engineer, DCS team, in Verimag since 11/2012.

Paraskevas Bourgos, Engineer, DCS team, in Verimag since 06/2013.

Prasoon Dadhich, Engineer, Synchrone team, in Verimag since 09/2013.

Khalil El Harake, Engineer, DCS team, in Verimag since 03/2014.

Karim Hossen, Engineer, DCS team, in Verimag since 03/2014.

Anakreontas Mentis, Engineer, DCS team, in Verimag since 07/2012.

Petro Poplavko, Postdoc, DCS team, in Verimag since 11/2010.

Wei-Tsun Sun, Engineer, Synchrone team, in Verimag since 06/2014.

Stefano Minopoli, Engineer, Tempo team in Verimag since 05/2013.

G.6 PhD Students (PhD defended)

Christian von Essen (DCS) [Started October 2010-defended in April 2014],
Supervisor(s): S. Bensalem, B. Jobstmann,
Quantitative Verification and Synthesis,
Funding: French Ministery of Research scholarship, Master diploma from Aachen, nationality: German,
Christian is now R&D engineer, Google, Zurich

Jannik Dreier (DCS) [Started November 2010-defended in November 2013],
Supervisor(s): Y. Lakhnech and P. Lafourcade ,
Formal Verification of Voting and Auction Protocols, From Privacy to Fairness and Verifiability,
Funding: Project Contract, Master diploma from Master in Grenoble INPG, nationality: German,
He is currently at ETHZ doing a post-doct at David Basin Group

Yvan Rivierre (synchrone) [Started October 2010-defended in November 2013],
Supervisor(s): F. Maraninchi, S. Devismes, F. Carrier,
Self-Stabilizing Algorithms for Constructing Distributed Spanning Structures,
Funding: French Ministery of Research scholarship, Master diploma from Grenoble, nationality: French,
Yvan decided to take a sabbatical year

Sofia Bekrar (DCS and LIG Vasco) [Started January 2010-defended in october 2013],
Supervisor(s): R. Groz and L. Mounier,
Recherche de vulnérabilités logicielles par combinaison d'analyses de code binaire et de frelatage,
Funding: Cifre Contract with Vupen Security, Master diploma from Constantine (Algeria), nationality: French,
Sofia is currently R&D engineer, Vupen Security, Montpellier

Jean Quilbeuf (DCS) [Started October 2009-defended in September 2013],
Supervisor(s): M. Bozga, J. Sifakis,
Distributed Implementations of Component-based Systems with Prioritized Multiparty Interactions. Application to the BIP Framework.,
Funding: French Ministery of Research scholarship, Master diploma from Grenoble, nationality: French,
Jean is now postdoc student at Fortiss, Munich

Xiaomu Shi (DCS) [Started October 2009-defended in July 2013],
Supervisor(s): J-F. Monin, V. Joloboff,
Certification of an Instruction Set Simulator,
Funding: LIAMA, Master diploma from LAAS, Toulouse, nationality: Chinese,
Xiaomu is now Post Doc, Tsinghua, China

Paraskevas Bourgos (DCS) [Started October 2009-defended in April 2013],
Supervisor(s): S. Bensalem,
Rigorous Design Flow for Programming Manycore Platforms,
Funding: French Ministery of Research scholarship, Master diploma from Grenoble, nationality: Greek,
Paraskevas is now R&D engineer, Floralis, Grenoble

Valentin Perrelle (synchrone) [Started October 2009-defended in March 2013],
Supervisor(s): N. Halbwachs,
Static Analysis of Array-Manipulating Programs,
Funding: French Ministery of Research scholarship, Master diploma from Paris, nationality: French,
Valentin is now a postdoc student at IRT SystemX, Paris

Emmanuel Sifakis (DCS) [Started October 2009-defended in March 2013],
Supervisor(s): S. Bensalem, L. Mounier,
Towards efficient and secure shared memory applications,
Funding: SCALP Project, Master diploma from Grenoble, nationality: French,
Emmanuel is now R&D engineer, Diginext, Aix-en-Provence

Filip Konecny (DCS) [Started February 2009-defended in October 2012],
Supervisor(s): R. Iosif,
Relational Verification of Programs with Integer Data,
Funding: Czech Government scholarship and VERIDYC Project, Master diploma from Brno University of Technology, nationality: Czech,
Software Engineer, NetSuite, Brno, CZ

Jiri Simacek (DCS) [Started February 2009-defended in October 2012],
Supervisor(s): R. Iosif,
Harnessing Forest Automata for Verification of Heap Manipulating Programs,

Funding: Czech Government scholarship and VERIDYC Project, Master diploma from Brno University of Technology, nationality: Czech,
Software Engineer, NetSuite, Brno, CZ

Romain Testylier (tempo) [Started Sept 2009-defended in December 2012],
Supervisor(s): T, Dang,
Reachability Analysis of Non-linear Dynamical Systems,
Funding: Projects VEDECY, Master diploma from University of Grenoble, nationality: French,
He is currently working as a research engineer in INRIA Grenoble

Jean-Francois Kempf (tempo) [Started April 2008-defended in October 2012],
Supervisor(s): O. Maler,
On Computer-Aided Design-Space Exploration for Multi-Cores,
Funding: ATHOLE project, Master diploma from ULP Strasbourg, nationality: French,
He is currently working at the Mathworks, Grenoble

Artur Pietrek (DCS) [Started October 2009-defended in October 2012],
Supervisor(s): B. Dupont De Dinechin, J.-Cl. Fernandez,
Tirex : a textual target-level intermediate representation,
Funding: CIFRE Kalray, Master diploma from Pologne, nationality: Polonaise,
Currently engineer at MathWorks, Grenoble

Selma Saidi (tempo) [Started Mars 2008-defended in October 2012],
Supervisor(s): O. Maler,
Optimizing DMA Data Transfers for Embedded Multi-Cores,
Funding: CIFRE with ST, Master diploma from Paris Diderot, nationality: Algerian,
Selma is now a post-doc at Braunschweig University, Germany

Eduardo Mazza Sampaio (DCS) [Started May 2008-defended in June 2012],
Supervisor(s): M-L. Potet and D. Le Metayer,
A Formal Framework for specifying and Analyzing Liabilities Using Log as Digital Evidence,
Funding: ANR LISE grant, Master diploma from Brazil, nationality: Brazilian,
Eduardo is now R&D engineer, Canada

Tesnim Abdellatif (DCS) [Started October 2008-defended in June 2012],
Supervisor(s): J. Sifakis, J. Combaz,
Rigorous Implementation of Real-time Applications,
Funding: French Ministery of Research scholarship, Master diploma from Grenoble, nationality: French,
Tesnim is now R&D engineer, Magillem, Paris

Lilia Sfaxi (DCS) [Started October 2008-defended in May 2012],
Supervisor(s): Y. Lakhnech,
Construction des systèmes répartis à base de composants sécurisés,
Funding: Tunisian scholarship, Master diploma from Grenoble, nationality: Tunisian,
Lilia is now assistant-professor at INSAT, Tunis

Rajarshy Ray (tempo) [Started November 2008-defended in May 2012],
Supervisor(s): G. Frehse,
Reachability Analysis of Hybrid Systems using Support Functions,
Funding: Projects, Master diploma from Chennai Mathematical Institute, India, nationality: Indian,
He is currently Assistant professor at Shillong, India

Nicolas Berthier (synchrone,DCS) [Started October 2008-defended in March 2012],

Supervisor(s): F. Maraninchi, L. Mounier,
Synchronous Programming of Device Drivers for Global Resource Control in Embedded Operating Systems,
Funding: French Ministery of Research scholarship, Master diploma from Grenoble, nationality: French,
Nicolas is now a postdoc student at IRISA, Rennes

Marion Daubignard (DCS) [Started October 2009-defended in January 2012],
Supervisor(s): Y. Lakhnech and P. Lafourcade ,
Formal Methods for Concrete Security Proofs,
Funding: French scholarship, Master diploma from Master in Grenoble, nationality: French,
She is currently working at DGA

Giovanni Funchal (synchrone) [Started May 2007-defended in November 2011],
Supervisor(s): F. Maraninchi, M. Moy,
Contributions to the Transaction-Level Modeling of Systems-on-a-Chip,
Funding: CIFRE STMicroelectronics, Master diploma from Grenoble and U. Federal do Rio Grande do Sul, Brazil, nationality: Brazilian,
Giovanni is now R&D engineer, Synopsys, Dublin

Julien Legriel (tempo) [Started December 2007-defended in October 2011],
Supervisor(s): O. Maler,
Multi-Criteria Optimization and its Application to Multi-Processor Embedded Systems,
Funding: CIFRE with ST, Master diploma from Grenoble INP, nationality: French,
He is currently working in Atrenta, Grenoble

Vassiliki Sfyrla (DCS) [Started September 2007-defended in June 2011],
Supervisor(s): M. Bozga, J. Sifakis,
Modélisation des systèmes synchrones en BIP,
Funding: French Ministery of Research scholarship, Master diploma from Greece, nationality: Greek,
Vassiliky is currently R&D engineer, VISEO, Grenoble

Imene Ben Hafaiedh (DCS) [Started October 2007-defended in February 2011],
Supervisor(s): S. Graf,
Component-based Systems: from Design to Implementation,
Funding: French scholarship, Master diploma from Grenoble, nationality: Tunisian,
Imen is currently Maître Assistant at ISI-El Manar University, Tunisia

Sophie Quinton (DCS) [Started October 2006-defended in January 2011],
Supervisor(s): S. Graf,
Design, Verification and Implementation of Systems of Components ,
Funding: ENS scholarship, Master diploma from ENS Cachan in Rennes, nationality: French,
Sophie is currently Chargé de Recherche at INRIA Rhône-Alpes

Mohamad Jaber (DCS) [Started October 2007-defended in October 2010],
Supervisor(s): J. Sifakis,
Centralized and Distributed Implementations of Correct-by-construction Component-based Systems by using Source-to-source Transformations in BIP,
Funding: French Ministery of Research scholarship, Master diploma from Grenoble, nationality: Lebanese,
Mohamad is now Assistant Professor at the American University of Beirut

Tayeb Bouhadiba (synchrone) [Started October 2006-defended in September 2010],
Supervisor(s): F. Maraninchi,
Component-Based Virtual Prototyping of Heterogeneous Embedded Systems,

Funding: French Ministery of Research scholarship, Master diploma from Grenoble, nationality: Algerian,
Tayeb is now R&D engineer at Synopsys, Grenoble

Mathias Péron (synchrone) [Started October 2005-defended in September 2010],
Supervisor(s): N. Halbwachs,
Contributions à l'analyse statique de programmes manipulant des tableaux,
Funding: French Ministery of Research scholarship, Master diploma from Lyon, nationality: French,
Mathias is now R&D engineer, The Mathworks/Polyspace, Grenoble

Manuel Garnacho (DCS) [Started October 2006-defended in August 2010],
Supervisor(s): Y. Lakhnech, M. Périn,
Formal certification of critical systems by instrumentation of a static analyzer,
Funding: ANR EDEN2, Master diploma from Grenoble, nationality: French,
M.Garnacho is currently in post-doc at IRIT, Toulouse

Than-Hung Nguyen (DCS) [Started October 2007-defended in May 2010],
Supervisor(s): S. Bensalem, J. Sifakis,
Constructive Verification of Component-Based Systems,
Funding: FP7 Combest project, Master diploma from Grenoble, nationality: Vietnamese,
Than-Hung is now Assistant professor at Hanoi University of Science and Technology, Vietnam

Yassin Chkouri (DCS) [Started October 2006-defended April 2010],
Supervisor(s): J. Sifakis,
Modélisation des systèmes temps-réel embarqués en utilisant AADL pour la génération automatique d'applications formellement vérifiées,
Funding: Rhônes-Alpes Region Scholarship, Master diploma from Lyon, nationality: Moroccan,
Yassin is now Assistant professor at the National School of Applied Sciences (ENSA) of Tetouan, Maroc

Marc Poulhies (DCS) [Started October 2005-defended March 2010],
Supervisor(s): J. Sifakis,
Conception et implantation de système fondé sur les composants, vers une unification des paradigmes génie logiciel et système,
Funding: Allocation France-Telecom, Master diploma from Lausanne, nationality: French,
currently engineer at Synopsys

Ylies Falcone (DCS) [Started October 2006-defended in Nov 2019],
Supervisor(s): J.-Cl. Fernandez, L. Mounier, J.L. Richer,
Etude et mise en oeuvre de techniques de validation à l'exécution,
Funding: French Ministery of Research scholarship, Master diploma from Grenoble, nationality: Française,
now MCF UJF

Colas Le Guernic (tempo) [Started October 2005-defended in October 2009],
Supervisor(s): O. Maler,
Reachability Analysis of Hybrid Systems with Linear Continuous Dynamics,
Funding: Allocation RPI, Master diploma from ENS Paris, nationality: French,
he is currently working at the DGA, Rennes

Aldric Degorre (tempo) [Started Sept 2005-defended in October 2009],
Supervisor(s): O. Maler,
On some Quantitative Aspects of Formal Languages,
Funding: Allocation RBS, Master diploma from ENS Bretagne, nationality: French,
he is currently an assistant professor (MdC) in Univeristy Paris Diderot

Scott Cotton (tempo) [Started Sept 2005-defended in June 2009],
Supervisor(s): O. Maler,
On some Problems in Satisfiability Solving,
Funding: Project DECIDE!, Master diploma from Saarland University, nationality: American,
he is currently working in Atrenta, Grenoble

G.7 PhD Students (ongoing)

Vikas Jaiman (tempo) [Started April 2014-April 2017],
Supervisor(s): T. Dang,
Contract-Based Design of Cyber-Physical Systems,
Funding: AGIR 2013, Master diploma from Central University of Rajasthan, India, nationality: Indian

Abdurrahman Pektas (DCS) [Started April 2013-April 2016],
Supervisor(s): T. Acarman, Y. Falcone and J.Cl. Fernandez,
Personal Financing,
Funding: Behavior based malicious software detection and classification, Master diploma from Galatasaray University Istanbul, Turkey, nationality: Indian

Amrit Kumar (DCS) [Started November 2013-November 2016],
Supervisor(s): P. Lafourcade and C. Lauradoux,
Sécurité et protection de la vie privée pour le calcul déporté,
Funding: Labex Persival Grant, Master diploma from Grenoble, nationality: French

Hosein Nazarpour (DCS) [Started October 2013-October 2016],
Supervisor(s): S. Bensalem, Y. Falcone,
Development of the technique for monitoring of distributed system expressed in the BIP platform,
Funding: Artemis project, Master diploma from University Joseph Fourier, Grenoble, France, nationality: Iranian

Yuliia Romenska (synchrone) [Started November 2013-October 2016],
Supervisor(s): F. Maraninchi,
Component-based design and modeling, for functional and performance properties of hardware/software systems,
Funding: OpenES CATRENE Project, Master diploma from Univ. Nice and Univ. Kharkiv, Ukraine, nationality: Ukrainian

Laurent Lemke (synchrone) [Started November 2013-October 2016],
Supervisor(s): F. Maraninchi, D. Donsez,
Shared self-configuring models and software infrastructures for Smart City monitoring and control,
Funding: CIFRE Orange Labs, Grenoble, Master diploma from Grenoble, nationality: French

Egor "George" Karpenkov (synchrone) [Started November 2013-November 2016],
Supervisor(s): D. Monniaux,
Static Analysis of programs, Applications of SMT-Solving and policy iteration,
Funding: ERC research grant "STATOR", Master diploma from University of Sydney, nationality: Australian

Louis Dureuil (DCS) [Started November 2013-October 2016],
Supervisor(s): M-L. Potet,

Code Analysis technics to evaluate robustness of critical embedded applications against fault injection,
Funding: CEA grant, Master diploma from Grenoble, nationality: French

Josselin Feist (DCS) [Started October 2013-September 2016],
Supervisor(s): M-L. Potet and L. Mounier,
Binary Code Analysis and exploitable vulnerability detection,
Funding: French Ministery of Research scholarship, Master diploma from Strasbourg, nationality: French

Dogan Ulus (tempo) [Started October 2013-November 2016],
Supervisor(s): O. Maler,
Timed Pattern Matching,
Funding: Allocation avancée, Master diploma from Bogazici University Istanbul, nationality: Turkish

Hela Guesmi (DCS) [Started September 2013-September 2016],
Supervisor(s): S. Bensalem, Belgacem Heida,
"Validation des spécifications des applications temps-réel",
Funding: CEA Research scholarship, Master diploma from Tunis, Tunisia, nationality: Tunisian

Tommaso Dreossi (tempo) [Started April 2013-June 2016],
Supervisor(s): T. Dang,
Topic: Parameter Synthesis for Biological Models,
Funding: Co-tutelle, University of Udine, Master diploma from Univeristy of Udine, Italy, nationality: Italian

Thomas Ferrere (tempo) [Started Mars 2013-June 2016],
Supervisor(s): O. Maler,
Monitoring AMS assertions,
Funding: CIFRE with Mentor Graphics, Master diploma from University of Paris 7, nationality: French

Abhinav Srivastav (tempo) [Started February 2013-June 2016],
Supervisor(s): O. Maler,
Local Search for Multi-Criteria Optimization,
Funding: Allocation Labex Persyval, Master diploma from Birla Institute of Technology, India, nationality: Indian

Souha Ben Rayana (DCS) [Started October 2012-October 2015],
Supervisor(s): S. Bensalem, M. Bozga,
Compositional verification of component-based real-time systems and applications,
Funding: Artemis project, Master diploma from Ecole Supérieure de Communications de Tunis (SUP'COM), Tunisia, nationality: Tunisian

Najah Ben Said (DCS) [Started October 2012-October 2015],
Supervisor(s): S. Bensalem, M. Bozga, T. Abdellatif,
Information flow security in component based systems,
Funding: FP7 project D-MILS, Master diploma from Ecole Nationale d'ingénieurs de Sousse (ENISo), Tunisia, nationality: Tunisian

Alexios Lekidis (DCS) [Started October 2012-October 2015],
Supervisor(s): S. Bensalem, M. Bozga,
Tools for the development of systems based on distributed multimedia sensor networks,
Funding: BGLE Acose grant, Master diploma from Aristotle University of Thessaloniki, ECE Department, Greece, nationality: Greek

Jan Lanik (tempo) [Started October 2012-October 2015],
Supervisor(s): O. Maler,
Activity Reduction in Digital Circuits,
Funding: CIFRE with Atrenta, Master diploma from Masaryk University, Brno, Chech Republic, nationality: Indian

Irini-Eleftheria Mens (tempo) [Started October 2012-October 2015],
Supervisor(s): O. Maler,
Learnign Regual Languages over Large Alphabets,
Funding: Allocation ecole doctoral, Master diploma from Oniversity of Thessaloniiki, Greece, nationality: Greek

Alexis Fouilhe (synchrone,DCS) [Started October 2012-October 2015],
Supervisor(s): D. Monniaux, M. Périn,
Certified static analysis,
Funding: ANR research grant "VERASCO", Master diploma from Lyon, nationality: French

Ozgün Pinarer (DCS,synchrone) [Started October 2012-September 2015],
Supervisor(s): F. Maraninchi, L. Mounier,
Methods and tools for the evaluation of energy consumption in sensor networks,
Funding: French Ministery of Research scholarship, Master diploma from Univ. Galatasaray, Istanbul, Turkey, nationality: Turkish

Ali Kassem (DCS) [Started 2012-November 2015],
Supervisor(s): P. Lafourcade and Y. Lakhnech,
Formal analysis of cryptographic protocols,
Funding: French Ministery of Research scholarship, Master diploma from Grenoble, nationality: French

Ahlem Triki (DCS) [Started October 2011-October 2014],
Supervisor(s): S. Bensalem, J. Combaz,
Rigorous implementation of distributed real-time systems,
Funding: Artemis project, Master diploma from Ecole Polytechnique de Tunis, Tunis, nationality: Tunisian

Ayoub Nouri (DCS) [Started October 2011-October 2014],
Supervisor(s): S. Bensalem, M. Bozga, A. Legay,
Performance evaluation of embedded systems using statistical model checking and abstraction,
Funding: Artemis project, Master diploma from Institut Supérieur d'Informatique, Tunis, nationality: Tunisian

Dario Socci (DCS) [Started October 2011-October 2014],
Supervisor(s): S. Bensalem,
Design Flow for Mixed-Critical Applications on Multi-core Systems,
Funding: FP7 project Certainty, Master diploma from Università degli Studi di Napoli Federico II, Italy, nationality: Italian

Julien Henry (synchrone) [Started October 2011-September 2014],
Supervisor(s): D. Monniaux, M. Moy,
Static Analysis by Abstract Interpretation and Decision Procedures,
Funding: French Ministery of Research scholarship, Master diploma from Grenoble, nationality: French

Molka Becher (DCS) [Started October 2011-September 2014],
Supervisor(s): S. Bensalem, Jean-Francois Pacull,
"Placement d'applications parallèles sur une infrastructure matérielle de type MPSoC reconfigurable",
Funding: CEA Research scholarship, Master diploma from Tunis, Tunisia, nationality: Tunisian

Raphël Jamet (DCS) [Started September 2011-October 2014],
Supervisor(s): P. Lafourcade,
Security of WANET,
Funding: French Ministery of Research scholarship, Master diploma from Grenoble, nationality: French

Kim Quyen Ly (DCS) [Started October 2010-October 2014],
Supervisor(s): J.-F. Monin,
Automated Verification of Termination Certificates,
Funding: LIAMA, Master diploma from Université de Bordeaux 1, nationality: Vietnamese

Mathilde Duclos (DCS) [Started October 2010-September 2014],
Supervisor(s): Y. Lakhnech and P. Corbineau,
Certification d'un Protocole Cryptographique en Coq,
Funding: French Ministery of Research scholarship, Master diploma from Grenoble, nationality: French

Pranav Tendulkar (tempo) [Started October 2010-October 2014],
Supervisor(s): O. Maler,
Multi-criteria Optimization for Multi-core Deployment,
Funding: Contract, Master diploma from University of Lugano, nationality: Indian

Appendix H

Laboratory council
Conseil de laboratoire

Membres élus

Elus collège 1

Titulaires	Suppléants
Karine Altisen	Fabienne Carrier
Pascal Lafourcade	Thao Dang
Marie-Laure Potet	Goran Frehse
Catherine Vigouroux	Stéphane Devismes
Matthieu Moy	Anne Rasse
Yvan Riviere	Mathilde Duclos

Elus collège 2

Titulaire	Suppléant
Jacques Combaz	Olivier Lebeltel

Membres nommés

Yassine Lakhnech
Oded Maler
Florence Maraninchi
Saddek Bensalem
Patrick Fulconis
Christine Saunier Cailly

Membres de droit

Susanne Graf
Nicolas Halbwachs

Appendix I

List of seminars
Liste des séminaires

- 2009/03/05 : Thomas Gawlitza (Technische Universität München), Precise Relational Invariants Through Strategy Iteration.
- 2009/04/02 : Domagoj Babic (Fujitsu Labs America), Scalable and Precise Extended Static Checking.
- 2009/04/09 : Alexandre Donzé (Verimag), Calcul numérique d'ensembles atteignables pour les systèmes hybrides et applications.
- 2009/04/16 : Christophe Guillon (STMicroelectronics), Les représentations SSA et Psi-SSA.
- 2009/05/07 : Villard Jules (LSV, Cachan), Proving Copyless Message Passing.
- 2009/05/14 : Florian Kammueller (Technische Universitat Berlin), ASPfun: un calcul pour des objets distribués.
- 2009/06/25 : Zvonimir Rakamaric (University of British Columbia), Static and Precise Detection of Concurrency Errors in Systems Code Using SMT Solvers.
- 2009/09/15 : Dino Distefano (Queen Mary University, London), Compositional Shape Analysis by means of Bi-Abduction.
- 2009/09/24 : Bageshri Karkare (Verimag), Efficiency, Precision, Simplicity, and Generality in Interprocedural Data Flow Analysis..
- 2009/10/29 : Stephane Demri (ENS Cachan), The covering and boundedness problems for branching vector addition systems.
- 2009/11/12 : Florent Garnier (Verimag- Team DCS), A classification of randomized fair strategies for studying termination of term rewriting.
- 2009/11/19 : Matthias Althoff (Technische Universität München), Reachability Analysis of Nonlinear and Hybrid Systems with Zonotopes.
- 2009/11/19 : Bruce Krogh (Dept. of Electrical and Computer Engineering, Carn), Research Directions in Cyber-Physical Systems.
- 2009/12/02 : Constantin Enea (Paris 7), A Logic-based Framework for Reasoning about Composite Data Structures.
- 2010/01/14 : Arnaud Sangnier (Universite de Turin), Reversal-bounded counter machines revisited.
- 2010/02/16 : Bahareh Badban (University of Konstanz), Automated Invariant Generation for the Verification of Real-Time Systems.
- 2010/03/04 : Ondrej Sery (Charles University Prague), Code analysis with Blast.
- 2010/03/09 : Thomas Gawlitza (Verimag), Combining Strategy Iteration with Semidefinite Programming for Abstract Interpretation.
- 2010/03/19 : Nicolas Blanc (ETH Zurich), Analyse statique de SystemC avec Scoot : de la Verification à la Simulation.
- 2010/04/01 : Claire Maiza (Compiler Design Lab, Saarland University), Static analysis of interferences in the cache memory in preemptive real-time systems.
- 2010/04/22 : Nikolay Kosmatov (CEA - LISI), All-Paths Test Generation for Programs with Internal

Aliases in PathCrawler.

- 2010/05/07 : Alexandre Donze (Verimag), Model-based design and analysis of hybrid systems:simulation-based techniques, applications and perspectives.
- 2010/05/07 : Kevin Marquet (Verimag), Vérification automatique de modèles de systèmes sur puce.
- 2010/05/10 : Nadia El Mrabet (GREYC algo team - Université de Caen), Arithmétique des couplages, performance et résistance aux attaques par canaux cachés.
- 2010/05/10 : Regis Gascon (Inria Sophia-Antipolis), Verification of quantitative properties on constraint automata.
- 2010/05/10 : Christophe Joubert (Technical University of Valencia, Spain), Datalog-based Program Analysis with BES and RWL.
- 2010/05/10 : Arnaud Sangnier (DISI, Università di Genova), Weak Time Petri Nets Strike back!.
- 2010/06/17 : Karel Heurtefeux (Synchrone), Qualitative localization applied to routing and MAC layer in Wireless Sensor Networks.
- 2010/06/18 : Arshia Cont (IRCAM), Antescofo : A performance-synchronous language for computer music.
- 2010/07/01 : Jocelyne Troccaz (CNRS/TIMC), TBA.
- 2010/07/08 : Sophie Quinton (Verimag), Achieving distributed control through model checking.
- 2010/08/26 : Sébastien Bourdeauducq (Sharism at Work), Milkymist : un System-on-Chip libre et orienté video temps réel.
- 2010/11/05 : Moshe Vardi (Rice University), From Philosophical to Industrial Logics.
- 2010/11/18 : Antoine Gerbaud (Synchrone/Asynchrone), Walker model for complex networks.
- 2011/03/02 : Christian von Essen (DCS), Synthesizing Systems with Optimal Average-Case Behavior for Ratio Objective.
- 2011/03/03 : Hubert Garavel (INRIA), CADP 2010: A Toolbox for the Construction and Analysis of Distributed Processe.
- 2011/03/16 : Fabio Somenzi (University of Colorado in Boulder), Clause Manipulation for Faster Satisfiability.
- 2011/05/18 : Jinyun Xue (Institute of Software, Chinese Academy of Science,), PAR Method and PAR Platform for Developing Reliable Software and Its New Development.
- 2011/05/19 : Viktor Kuncak (EPFL), Towards Implicit Programming.
- 2011/05/26 : Jannik Dreier (Verimag), Privacy Properties for Voting Protocols: The completed picture.
- 2011/06/28 : Francesco Logozzo (Microsoft Research), Practical program verification for the working programmer with CodeContracts and Abstract Interpretation.
- 2011/06/30 : Nathalie Bertrand (IRISA), Determinizing timed automata..
- 2011/07/21 : Pierre Ganty (IMDEA), Pattern-based Verification for Multithreaded Programs.
- 2011/09/15 : Balaji Raman (DCS, Verimag), On Buffering with Stochastic Guarantees in Resource-Constrained Media Players.
- 2011/11/14 : Philippe Suter (EPFL), Sets with Cardinality Constraints in Satisfiability Modulo Theories.
- 2012/01/19 : Christian von Essen (Verimag), Synthesizing Efficient Controllers.
- 2012/01/26 : Tom Henzinger (IST-Austria), Quantitative Reactive Modeling.
- 2012/02/09 : Jan Olaf Blech (Fortiss), Proof Assistant Based Certification for Modeling Languages and its Application to PLC Development.
- 2012/02/10 : Laurent George (INRIA Rocquencourt / AOSTE Team INRIA), Robustesse temporelle dans les systèmes embarqués mono et multiprocesseur.
- 2012/02/16 : Goran Frehse (Verimag), Safety Analysis of Hybrid Systems with SpaceEx.
- 2012/02/23 : Franck Petit (LIP6), Strength of Stabilization vs. Amount of Resources.
- 2012/03/01 : Jerôme Leroux (LABRI), Vector Addition System Reachability Problem.
- 2012/03/05 : Sriram Rajamani (Microsoft Research), Program Analysis and Machine Learning: A Win-Win Deal.
- 2012/03/08 : Goran Frehse (Verimag), Safety Analysis of Hybrid Systems with SpaceEx.
- 2012/03/12 : Gilles Muller (LIP6 / INRIA), Remote Core Locking: Migrating Critical-Section Execution to Improve the Performance of Multithreaded Applications.
- 2012/03/22 : Oded Maler (Verimag), Performance Evaluation of Schedulers in a Probabilistic Setting.

- 2012/04/05 : Laura Kovacs (Technical University of Vienna), Playing in the Grey Area of Proofs.
- 2012/05/09 : Pierre Ganty (IMDEA (Madrid)), A Perfect Model for Bounded Verification.
- 2012/05/11 : Xavier Urbain (ENSIIE), Démonstration automatique : techniques, outils et certification..
- 2012/05/24 : Saddek Bensalem (Verimag), Rigorous Component-based System Design Using the BIP Framework.
- 2012/05/25 : Johannes Reich (SPA), A System Perspective on Processes and Their Interactions..
- 2012/05/31 : Pavol Cerny (IST Austria), Quantitative Abstraction Refinement.
- 2012/06/01 : Ian Mitchell (Verimag), Scalable approximation of the viability kernel and safe control synthesis for LTI systems using maximal reachability.
- 2012/06/07 : Gilles Muller (LIP6), Remote Core Locking: Migrating Critical-Section Execution to Improve the Performance of Multithreaded Applications.
- 2012/06/21 : Jean-Christophe Filliâtre (CNRS / LRI), Combining Interactive and Automated Theorem Proving in Why3.
- 2012/06/26 : Gerardo Schneider (Chalmers — University of Gothenburg), Towards a Framework for Conflict Analysis of Normative Texts Written in Controlled Natural Language.
- 2012/07/05 : Pascal Cuoq (CEA), Collaboration dánalyses dans Frama-C.
- 2012/07/12 : Roberto Bruttomesso (ATRENTA), Automated Analysis of Parametric Timing-Based Mutual Exclusion Algorithms.
- 2012/09/13 : Corneliu Popeea (Technical University of Munich), Synthesizing Software Verifiers from Proof Rules.
- 2012/09/14 : Rance Delong (SRI International), MILS and DMILS project.
- 2012/10/16 : Guillaume Brat (NASA Ames), An overview of formal methods for Aeronautics at NASA.
- 2012/11/09 : Damien Massé (Université de Bretagne Occidentale (Brest)), Inférences de propriétés de terminaison par itération de stratégies.
- 2012/12/06 : Irina Asavoae (University Alexandru Ioan Cuza, Iasi, Romania), Bounded Model Checking of Recursive Programs with Pointers in K Abstract.
- 2012/12/06 : Mihail Asavoae (University Alexandru Ioan Cuza, Iasi, Romania), Semantics-Based WCET Analysis.
- 2013/01/16 : Prabhakar Pavithra (IMDEA, Spain), Approximation based Verification of Hybrid Systems.
- 2013/03/06 : Marc Pouzet (UPMC / ENS), Zélus: A Synchronous Language with ODEs.
- 2013/03/18 : Rolf Ernst (TU Braunschweig), Mixed critical system design and analysis.
- 2013/03/18 : Wang Yi (Uppsala University), Scheduling and Analysis of Cyclic Mode-Switches.
- 2013/03/19 : Sanjit Seshia (University of California, Berkeley), Integrating Induction and Deduction for Verification and Synthesis.
- 2013/03/22 : Karem Sakalla (University of Michigan Ann Arbor), Saucy3: Fast Symmetry Discovery in Graphs.
- 2013/04/12 : Florent Garnier (Verimag), Verifying C-Programs memory faults freedom by mean of Abstract Interpretation and a-posteriori model verification.
- 2013/04/25 : Deshmukh Jyotirmoy (Toyota), Mining Temporal Requirements of an Industrial-Scale Control System.
- 2013/04/26 : Zhoulai Fu (IMDEA Madrid), Picking up your targets — aggressive strong update beyond common sense.
- 2013/05/23 : Adam Halasz (West Virginia University), Challenges and possible strategies in the modeling of signal initiation by membrane bound receptors.
- 2013/05/30 : Chantal Keller (Laboratoire d'informatique de l'X), A Modular Integration of SAT/SMT Solvers to Coq through Proof Witnesses.
- 2013/06/11 : Christian von Essen (Verimag), Of Markov Decision Processes and Airborne Collisions.
- 2013/06/27 : Klaus Draeger (University of Oxford), Synchronization Invariants.
- 2013/07/11 : Sriram Sankaranarayanan (University of Colorado at Boulder), Invariance and Termination for Probabilistic Programs using Martingales..
- 2013/07/18 : Gaël Thomas (Paris VI / LIP6), A Study of the Scalability of Stop-the-world Garbage Collectors on Multicores.
- 2013/09/26 : Garnacho Manuel (IRIT), A Mechanized Semantic Framework for Real-Time Systems.

- 2013/10/31 : Mirko Fiacchini (GIPSA-lab, Grenoble), Set-theory and invariance for complex systems.
- 2013/11/07 : Ocan Sankur (Université Libre de Bruxelles), Robust Strategies in Timed Automata.
- 2013/11/25 : Mahfuza Farooque (École polytechnique), A Bisimulation between DPLL(T) and a Proof-Search Strategy for the Focused Sequent Calculus.
- 2013/12/09 : Giuseppe Lipari (LSV et Scuola Superiore Sant'Anna, Pisa), Hierarchical scheduling and component-based analysis of real-time systems.
- 2014/01/07 : Corneliu Popeea (Technische Universitaet Muenchen), Automated verification of multi-threaded programs.
- 2014/02/07 : Victor Magron (LAAS), Formal Certificates for Nonlinear Inequalities.
- 2014/02/14 : Franck Cassez (NICTA, Sydney, Australie), A compositional approach to inter-procedural analysis.
- 2014/02/27 : Eugene Asarin (LIAFA), Toward a Timed Theory of Channel Coding.
- 2014/04/03 : Florian Brandner (ENSTA-ParisTech), Refinement of Worst-Case Execution Time Bounds by Graph Pruning.
- 2014/04/03 : Jan Reineke (Universität des Saarlandes), PRET DRAM controller: bank privatization for predictability and temporal isolation.
- 2014/04/14 : Kees Goossens (TUE), CompSOC: A Mixed-Criticality Platform, Formalism, and Design Flow.
- 2014/05/28 : Dejan Nickovic (Austrian Institute of Technology), Require, Test and Trace It.

Appendix J

External Bibliography

[BBBS08] Ananda Basu, Philippe Bidinger, Marius Bozga, and Joseph Sifakis. Distributed semantics and implementation for systems with interaction and priority. In Kenji Suzuki, Teruo Higashino, Keiichi Yasumoto, and Khaled El-Fakih, editors, *Formal Techniques for Networked and Distributed Systems - FORTE 2008, 28th IFIP WG 6.1 International Conference, Tokyo, Japan, June 10-13, 2008, Proceedings*, volume 5048 of *Lecture Notes in Computer Science*, pages 116–133. Springer, 2008.

[BBS06] Ananda Basu, Marius Bozga, and Joseph Sifakis. Modeling heterogeneous real-time components in bip. In *Fourth IEEE International Conference on Software Engineering and Formal Methods (SEFM 2006), 11-15 September 2006, Pune, India*, pages 3–12. IEEE Computer Society, 2006.

[BBSN08] Saddek Bensalem, Marius Bozga, Joseph Sifakis, and Thanh-Hung Nguyen. Compositional verification for component-based systems and application. In Sung Deok Cha, Jin-Young Choi, Moonzoo Kim, Insup Lee, and Mahesh Viswanathan, editors, *Automated Technology for Verification and Analysis, 6th International Symposium, ATVA 2008, Seoul, Korea, October 20-23, 2008. Proceedings*, volume 5311 of *Lecture Notes in Computer Science*, pages 64–79. Springer, 2008.

[BFG+99] Marius Bozga, Jean-Claude Fernandez, Lucian Ghirvu, Susanne Graf, Jean-Pierre Krimm, and Laurent Mounier. IF: An intermediate representation and validation environment for timed asynchronous systems. In *Proceedings of Symposium on Formal Methods 99, Toulouse*, volume 1708 of *LNCS*. Springer Verlag, September 1999.

[BFM13] Massimo Benerecetti, Marco Faella, and Stefano Minopoli. Automatic synthesis of switching controllers for linear hybrid systems: Safety control. *Theor. Comput. Sci.*, 493:116–138, 2013.

[BGO+04] Marius Bozga, Susanne Graf, Iulian Ober, Ileana Ober, and Joseph Sifakis. The IF toolset. In *4th International School on Formal Methods for the Design of Computer, Communication and Software Systems: Real Time, SFM-04:RT, Bologna, Sept. 2004*, volume 3185 of *LNCS Tutorials*. Springer Verlag, 2004.

[BMP10] Sergiy Bogomolov, Corina Mitrohin, and Andreas Podelski. Composing reachability analyses of hybrid systems for safety and stability. In Ahmed Bouajjani and Wei-Ngan Chin, editors, *ATVA*, volume 6252 of *Lecture Notes in Computer Science*, pages 67–81. Springer, 2010.

[CJL+09] Franck Cassez, Jan J Jessen, Kim G Larsen, Jean-François Raskin, and Pierre-Alain Reynier. Automatic synthesis of robust and optimal controllers–an industrial case study. In *Hybrid Systems: Computation and Control*, pages 90–104. Springer, 2009.

[DM08] Aldric Degorre and Oded Maler. On scheduling policies for streams of structured jobs. In *FORMATS*, pages 141–154, 2008.

[HIV08a] Peter Habermehl, Radu Iosif, and Tomás Vojnar. A logic of singly indexed arrays. In Andrei Voronkov Iliano Cervesato, Helmut Veith, editor, *Logic for Programming, Artificial Intelligence, and Reasoning, 15th International Conference, LPAR 2008, Doha, Qatar, November 22-27, 2008. Proceedings*, volume 5330 of *Lecture Notes in Computer Science*, pages 558–573. Springer, 2008.

[HIV08b] Peter Habermehl, Radu Iosif, and Tomás Vojnar. What else is decidable about integer arrays? In Roberto M. Amadio, editor, *Foundations of Software Science and Computational Structures, 11th International Conference, FOSSACS 2008, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2008*, volume 4962 of *Lecture Notes in Computer Science*, pages 474–489. Springer, 2008.

[MMGP10] Aline Mello, Isaac Maia, Alain Greiner, and Francois Pecheux. Parallel simulation of SystemC TLM 2.0 compliant MPSoC on SMP workstations. In *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2010*, pages 606–609. IEEE, 2010.

[Rey02] J.C. Reynolds. Separation Logic: A Logic for Shared Mutable Data Structures. In *Proc. of LICS'02*. IEEE CS Press, 2002.

[ZSR+10] Lijun Zhang, Zhikun She, Stefan Ratschan, Holger Hermanns, and Ernst Moritz Hahn. Safety verification for probabilistic hybrid systems. In *CAV*, volume 6174 of *LNCS*, pages 196–211. Springer, 2010.