VALMEM – Fiche B – Description du projet

Résumé en Français

Validation fonctionnelle et temporelle de mémoires embarquées, décrites au niveau transistor, par des méthodes formelles – VALMEM

– Acronyme : VALMEM
– Thème de l'appel du projet principal : Architectures du Futur
– Sous-thème : Environnements de conception et environnements d'exécution
– Type : Projet de Recherche Industrielle ou Exploratoire – 3 ans

Le projet VALMEM s'intéresse à la vérification fonctionnelle et temporelle de circuits mémoires.

Les circuits mémoires ont la particularité d'intégrer des fonctionnalités toujours plus complexes tout en devant répondre à des objectifs de performances accrues. Pour ces raisons, ces circuits sont conçus directement au niveau transistor, ce qui rend très difficile leur validation.

VALMEM regroupe des partenaires universitaires (LSV, LIP6) et industriel (STMicroelectronics) aux compétences complémentaires qui abordent ce problème de vérification avec une approche formelle spécialisée pour les circuits mémoires, en partant de leur description en transistors. L'objectif est de fournir une plate-forme logicielle prototype, basée sur des abstractions originale du modèle en transistors, et des méthodes de vérification spécifiques, dans le but de vérifier un jeu d'exemples de circuits mémoires commercialisés.

Résumé en Anglais

Functional and Timed Validation of Embedded Memories Described at Transistor Level Using Formal Methods – VALMEM

– Acronym : VALMEM
– Subject of main call for proposition : Architectures du Futur
– Subtopic : Environnements de conception et environnements d'exécution
– Type : Industrial or Exploratory Research Project – 3 years

The VALMEM project focuses on the functional and timed verification of embedded memory circuits.

Memory circuits are specific in the sense that they embody more and more functionalities and have to meet more and more performance requirements. For these reasons, these circuits are designed at the transistor level (without appealing to standard cells libraries). This is why their verification is a major challenge.

In the VALMEM project, academic partners (LSV, LIP6) and industrial company (STMicroelectronics) will share their complementary knowledges to tackle this verification problem using a specialized formal approach dedicated to "custom" circuit memories.

The aim of this project is to deliver a prototype platform, based on an original abstraction of the transistor-level description, and on customized verification methods. Real commercialized products will be formally analysed.

I - Description courte du projet

Validation fonctionnelle et temporelle de circuits mémoires décrits au niveau transistor par des méthodes formelles - VALMEM

- Acronyme : VALMEM
- Champs thématiques : Environnements de conception et environnements d'exécution
- Type : projet de recherche – 3 ans

I-1 Contexte et motivation du projet

De nos jours, les mémoires dans les circuits électroniques prennent une importance prépondérante : elles représentent actuellement jusqu'à 70% de la surface des circuits numériques embarqués (SOC) ; pour certaines applications complexes, jusqu'à 400 bloc-mémoires peuvent être intégrés sur un même circuit ; la performance globale d'un circuit dépend essentiellement du temps d'accès à ces mémoires. Par ailleurs, la complexité de ces mémoires provient non seulement de l'accroissement du nombre de point-mémoires contenus, mais surtout des nouvelles fonctionnalités offertes répondant aux exigences accrues des nouvelles applications (modes veille, changement de tension d'alimentation, mémoires associatives haute densité,...).

Pour répondre à ces exigences de performance, *les mémoires embarquées sont directement conçues au niveau transistor* (par opposition à l'utilisation de bibliothèques de portes logiques standard).

Actuellement, ces mémoires sont validées dans un processus de vérification basé essentiellement sur de la simulation électrique (e.g., voir [HSIM]). Ces simulations sont très coûteuses en temps, et ne permettent qu'une vérification parcellaire. A l'issue de cette simulation, peuvent subsister des dysfonctionnements qui ne seront détectés qu'après la fabrication. De telles erreurs nécessitent des mois d'efforts humains et matériels pour être localisées, puis corrigées. Ce retard compromet alors gravement le succès commercial du produit.

Pour ces raisons, d'autres voies que la simulation méritent d'être explorées afin d'accroitre la qualité du processus de validation, et détecter les erreurs de conception au plus tôt. L'analyse statique est une approche alternative qui cherche à déterminer les caractéristiques temporelles des transistors isolément, en ignorant la fonctionnalité des composants [Dioury et al. 00]. Elle aboutit ainsi malheureusement à une approximation trop grossière des délais globaux de propagation dans notre cadre de composants dessinés directement au niveau transistor.

Dans le cadre du projet MEDEA+ Blueberries (jan. 2004–déc. 2006), auquel participent deux des partenaires de la présente proposition (LSV et STMicroelectronics), l'utilisation de méthodes à base d'automates temporisés [Alur-Dill 94] a été exploitée pour valider certaines caractéristiques fonctionnelles et temporelles de petites mémoires simples [Blueberries 06a,06b]. Ces méthodes paraissent prometteuses et ont permis d'identifier plusieurs verrous technologiques :

- nécessité d'une méthode d'abstraction d'un circuit conçu au niveau transistor, combinant des informations fonctionnelles et temporelles.
- nécessité d'un interfaçage automatique reliant la sortie de l'abstraction à un moteur de parcours de graphe (model checker) dédié.
- nécessité d'adapter les méthodes générales de vérification temporisée aux spécificités des circuits mémoires.

Le présent projet propose d'étudier ces différents points. Aux deux partenaires de Blueberries (STMicroelectronics et LSV), s'associe naturellement le LIP6, reconnu pour son expertise dans le domaine de l'abstraction fonctionnelle et de l'analyse temporelle de circuits.

L'objectif est de proposer une solution logicielle prototype mettant en évidence l'intérêt de cette approche formelle par rapport aux processus existants à base de simulation. Nous visons le traitement automatique de plusieurs circuits mémoires commerciaux offrant des fonctionnalités complexes.

A cette fin, nous exploiterons les compétences complémentaires des partenaires :

- STM : expertise en conception et développement de circuits mémoires commercialisés à grande échelle.
- LIP6 : expertise en analyse des systèmes décrits au niveau transistor (abstraction et caractérisation temporelle).
- LSV : expertise en méthodes et outils de vérification formelle des systèmes temporisés (automates temporisés et model-checking).

I-2 Retombées scientifiques et techniques attendues

Nous attendons les principales retombées scientifiques et techniques suivantes :

- Conception d'un nouveau modèle abstrait rendant compte de la fonctionnalité et des caractéristiques temporelles du circuit mémoire (associé au type de vérification ciblée)
- Méthode d'abstraction fonctionnelle et extraction des caractéristiques temporelles à partir d'un modèle en transistors selon le nouveau modèle.
- Vérification exhaustive par model checking (parcours du graphe abstrait) de l'adéquation du modèle abstrait avec sa spécification fonctionnelle et temporelle.
- Exploration de nouvelles représentations symboliques de contraintes temporelles, et des algorithmes de manipulation associés.

I-3 Retombées industrielles et économiques escomptées

Nous comptons identifier, pour la vérification des circuits mémoires, les gains en termes de qualité, coût et temps des méthodes et outils développés au cours de ce projet par rapport au processus de developpement industriel actuellement en production.

I-4 Principaux "délivrables"

Nous fournirons les principaux délivrables suivants :

- Revue de l'état de l'art des méthodes de simulation, abstraction et vérification des circuits mémoire.
- Discussion du modèle de délai "bi-bounded" [Brzozowski-Seger 94], et proposition d'un modèle mieux adapté au problème traité.
- Identification d'un ensemble de cas d'études comprenant la description de mémoires et de leurs fonctionnements attendus (ainsi que, le cas échéant, des dysfonctionnements observés)
- Définition d'une nouvelle méthode d'abstraction automatisable incluant des informations temporelles, adaptée à la conception de circuits-mémoires et développement d'un prototype associé.

– Recherche de nouveaux algorithmes de model-checking à base de représentation symbolique de contraintes spécialisées (e.g., SAT + théorie des intervalles sur réels) ; développement d'un prototype associé.
– Application des prototypes aux cas d'études ; comparaison avec analyse au moyen d'outils existants.

II - Description scientifique et technique détaillée du projet

VALMEM

II-1 Objectifs scientifiques

II-1.1 But du projet

Notre objectif est de vérifier formellement des propriétés temporelles quantitatives sur plusieurs exemples de mémoires embarquées décrites au niveau transistor, qui sont conçues et commercialisées par le partenaire industriel du projet (STM). Nous visons à répondre à une carence des méthodes de vérification formelles et des méthodes de validation industrielles:

- Les méthodes formelles actuelles partent en effet d'un niveau de spécification de la mémoire beaucoup plus abstrait que le niveau transistor.
- Les méthodes industrielles de validation actuelles travaillent dans un cadre très parcellaire, tant au niveau de la représentation du circuit que du test par simulation.

Pour atteindre cet objectif, nous proposons une nouvelle chaîne de validation, synthétisant une abstraction de la description du circuit au niveau transistor, et assurant une analyse exhaustive du modèle abstrait ("model checking" de systèmes temporisés).

II-1.2 Positionnement de la proposition par rapport à l'AAP

Notre projet s'inscrit dans la thématique exposée dans le thème 4 du programme "Architecture du futur": Environnements de conception et environnements d'exécution. En effet, notre but est de proposer une méthode de validation des caractéristiques temporelles de circuit-mémoires. Nous répondons ainsi aux objectifs du thème 4, visant à assurer la conformité aux spécifications, notamment temporelles, en nous spécialisant sur les composants mémoire. Nous répondons également aux objectifs "méthodologie de conception, de garanties de sûreté de fonctionnement et de fiabilité", décrits dans ce thème 4.

II-2 Contexte

Cette proposition de projet fait suite au projet MEDEA+ Blueberries dans lequel le LSV et STMicroelectronics (en coopération avec TRANSEDA) ont collaboré pour vérifier des propriétés temporelles quantitatives de circuits mémoires décrits au niveau transistor. Il s'agit de déterminer et d'optimiser des temps de traversée de bout en bout de tels circuits au moyen de méthodes formelles basées sur des automates temporisés. En pratique, la détermination de ces temps de traversée de bout en bout sur le modèle en transistors se fait soit par simulation électrique (e.g., voir [HSIM]), soit par analyse statique [Dioury et al. 00].

La simulation électrique approxime le comportement des transistors en résolvant des équations différentielles résultant des caractérisations électriques des transistors. Ce genre de simulation est très coûteuse et ne peut être conduite de façon exhaustive. En pratique, on se concentre donc sur des portions présumées critiques, qui sont déterminées manuellement par le concepteur. Une telle approche est incomplète et source d'erreurs potentielles, qui seront très difficiles à détecter, localiser et corriger dans la suite du flot de conception.

L'analyse statique, quant à elle, détermine les caractéristiques temporelles des transistors isolément, en ignorant la fonctionnalité des composants. Elle aboutit ainsi souvent à une approximation trop grossière des délais globaux de propagation, et ne permet pas de montrer que la spécification du circuit est effectivement réalisée par le composant.

Il existe des approches alternatives aux méthodes à base de simulation ou d'analyse statique: le *model checking* de systèmes temporisés ou l'*analyse min-max* par évaluation symbolique [CDY 99]. L'approche de model checking temporisé pour des circuits digitaux a été proposée dès 1995 par Maler et Pnueli, et a fait l'objet de nombreuses développements [Maler-Pnueli 95], [BBM 03], [Clariso-Cortadella 04], utilisant des outils de vérification dédiés à l'analyse de sytèmes temporisés (par exemple, [KRONOS], [UPPAAL], [HYTECH]). En fait, ni cette approche par model checking temporisé , ni l'approche min-max ne répondent pas complètement à certaines exigences particulières de notre problématique, du fait qu'elles partent d'un niveau de représentation déjà trop élevée (réseau de portes logiques au lieu de réseau de transistors); en outre, elles considèrent un modèle de délai de type "bi-bounded", ce qui induit une approximation trop grossière pour les circuits que nous considérons ici.

Dans le cadre du projet Blueberries, nous avons ébauché une approche formelle reposant aussi sur la preuve, mais partant du niveau de représentation en transistors [Blueberries 06a,06b]. Une telle approche a permis la vérification formelle et l'optimisation de caractéristiques temporelles d'une mémoire simple (SPSMALL). Cette approche nécessite une étape préliminaire de modélisation combinant la fonctionnalité et le temps (passage de la représentation en transistors à un "graphe abstrait temporisé"), qui permet ensuite de recourir à des méthodes de model checking classiques.

Cette expérience a mis en évidence certaines difficultés inhérentes à l'inadaptation du modèle temporel standard des circuit ("bi-bounded delay") ainsi que le manque d'adaptabilité des méthodes formelles générales aux spécificités des circuits mémoires. Nous souhaitons repousser les limites imposées par le phénomène d'explosion combinatoire en améliorant la définition du modèle de circuits mémoire, et en spécialisant les techniques de vérification par automates temporisés.

Les eléments de solution envisagés incluent les points suivants:

- Réduction spatiale: exploitation des symétries, régularités, ... (en particulier, en exploitant des spécificités de l'architecture des circuit-mémoires, comme la régularité du

graphe des chemins véhiculant les données à travers les point-mémoires)

- Enrichissement de l'analyse statique par une approche combinant l'abstraction fonctionnelle et la caractérisation temporelle d'un réseau de transistors
- Développement de méthodes algorithmiques pour les automates temporisés adaptés aux circuits-mémoires (représentation et algorithmes de résolution de contraintes spécialisées).

Description des partenaires

LSV Le Laboratoire Spécification et Vérification (LSV) est le laboratoire de recherche en informatique de l'ENS Cachan (Ecole Normale Supérieure de Cachan), associé au CNRS. Les activités de recherche de l'équipe impliquée dans le projet portent sur la vérification de propriétés temporelles quantitatives de systèmes et logiciels critiques. Les compétences principales de l'équipe concernent la modélisation des systèmes sous forme d'automates temporisés paramétrés ainsi que le développement et l'utilisation d'outils de vérification associés (model checking).

Le LSV collabore avec STMicroelectronics dans le domaine de la vérification à base d'automates temporisés des circuits mémoires dans le cadre du projet MEDEA+ Blueberries (janvier 2004-décembre 2006), et souhaite spécialiser dans cette proposition les modèles et les méthodes généraux employés dans Blueberries pour accroitre la portée de ces méthodes de vérification.

LIP6 Le Laboratoire d'Informatique de Paris 6 (LIP6) appartient à l'Université Pierre et Marie Curie (UPMC). Il regroupe plus de 400 chercheurs. Le département SOC, dirigé par le professeur Alain Greiner, est un des 5 départements du LIP6. Il regroupe une soixantaine de chercheurs dont 35 doctorants.

Le département SOC a développé la chaîne de CAO-VLSI ALLIANCE. Cet ensemble d'outils permet la conception des circuits numériques CMOS, depuis la spécification jusqu'au dessin des masques de fabrication. Cette chaîne comporte des outils d'aide à la conception (modélisation et simulation VHDL, synthèse logique, placement, routage, ...) et des outils de vérification (analyse temporelle statique, analyse de bruit de diaphonie, analyse de la consommation et simulation niveau switch, ...). Cette chaîne d'outils est diffusée internationalement sous licence GPL et utilisée dans plus de 200 universités dans le monde.

L'ensemble des outils de vérification est basé sur la technique d'abstraction fonctionnelle. Le LIP6 possède une expertise dans ce domaine et dans la modélisation temporelle. Ces deux thèmes ont fait l'objet de plusieurs thèses. [1]

[1] 1994: M. Laurentin - Thèse de l'Université Pierre et Marie Curie, "Abstraction et vérification fonctionnelle pour VLSI"

1998: K. Dioury - Thèse de l'Université Pierre et Marie Curie, "Analyse temporelle hiérarchique des circuits VLSI à très haute densité d'intégration"

1998: N. Abdallah - Thèse de l'Université Pierre et Marie Curie, "Méthode de simulation logico-temporelle de circuits numériques complexes prenant en compte le front des signaux et les collisions dans le cadre de la simulation mixte analogique-numérique"

1999: A. Lester - Thèse de l'Université Pierre et Marie Curie, "Abstraction fonctionnelle des circuits numériques VLSI avec une methode formelle basée sur une extraction de réseau de portes"

2003: G. Avot - Thèse de l'Université Pierre et Marie Curie, "Analyse temporelle des circuits intégrés digitaux CMOS, pour les technologies profondément submicroniques"

La technique d'abstraction fonctionnelle, ainsi que l'outil d'analyse temporelle, initialement développés dans le cadre de la chaîne ALLIANCE sont aujourd'hui commercialisés par une start-up issue du LIP6 (Avertec).

Dans ce projet, le LIP6 souhaite explorer les techniques d'abstraction et de représentation des circuits-mémoire et les méthodes de modélisation temporelle incluant une analyse fonctionnelle des chemins.

STMicroelectronics STMicroelectronics (STM) est le 6ème fabricant de circuits intégrés mondial avec plus de 50 000 collaborateurs dans le monde et un chiffre d'affaire de 8,8 milliards de dollars en 2005. Il conçoit et commercialise des dispositifs sur puces qui s'intègrent dans différents types d'applications: automobile, électronique grand public, électronique embarquée. Dans bon nombre de ces applications, des SoC (Systemes sur Puces) qui intègrent différentes fonctionnalités indépendantes, sont utilisées. Ces applications nécessitent des zones de stockage très rapides, très compactes et de capacité très variable: des mémoires embarquées SRAM. Pour répondre à tous les types d'applications (haute densité, grande vitesse, faible consommation), des mémoires SRAM très variées sont dessinées au niveau transistor. Dans cette proposition, qui fait suite à la coopération entretenue avec le LSV dans le projet MEDEA+ Blueberries, nous nous appuierons sur ce portefeuille très complet pour choisir les architectures de mémoire les plus représentatives pour évaluer les solutions de vérification à base de méthodes formelles.

Coopérations existantes. Le LSV et STMicroelectronics coopèrent actuellement au sein du projet MEDEA+ Blueberries (qui s'achève en décembre 2006). Par ailleurs, toutes les équipes impliquées dans VALMEM participent également à plusieurs projets (inter)nationaux, dont une liste complète figure en Section III-2.

II-3 Organisation du projet – description des sous-projets

Le projet s'organise en 4 tâches:

1. Identification des problèmes spécifiques aux mémoires et élaboration d'un ensemble d'études de cas issus de problèmes industriels
2. Passage de la représentation en transistors au modèle abstrait; méthodes d'abstraction
3. Méthodologie de validation
4. Application aux études de cas et développements de prototypes

II-3.1 Tâche 1: Identification des problèmes spécifiques à la validation des mémoires et définition d'une ensemble d'études de cas

Cette tâche recense les problèmes spécifiques à la validation des mémoires décrites au niveau transistor, et détermine un ensemble de cas qui feront l'objet d'une analyse comparée du processus de validation standard avec le nouveau processus proposé.

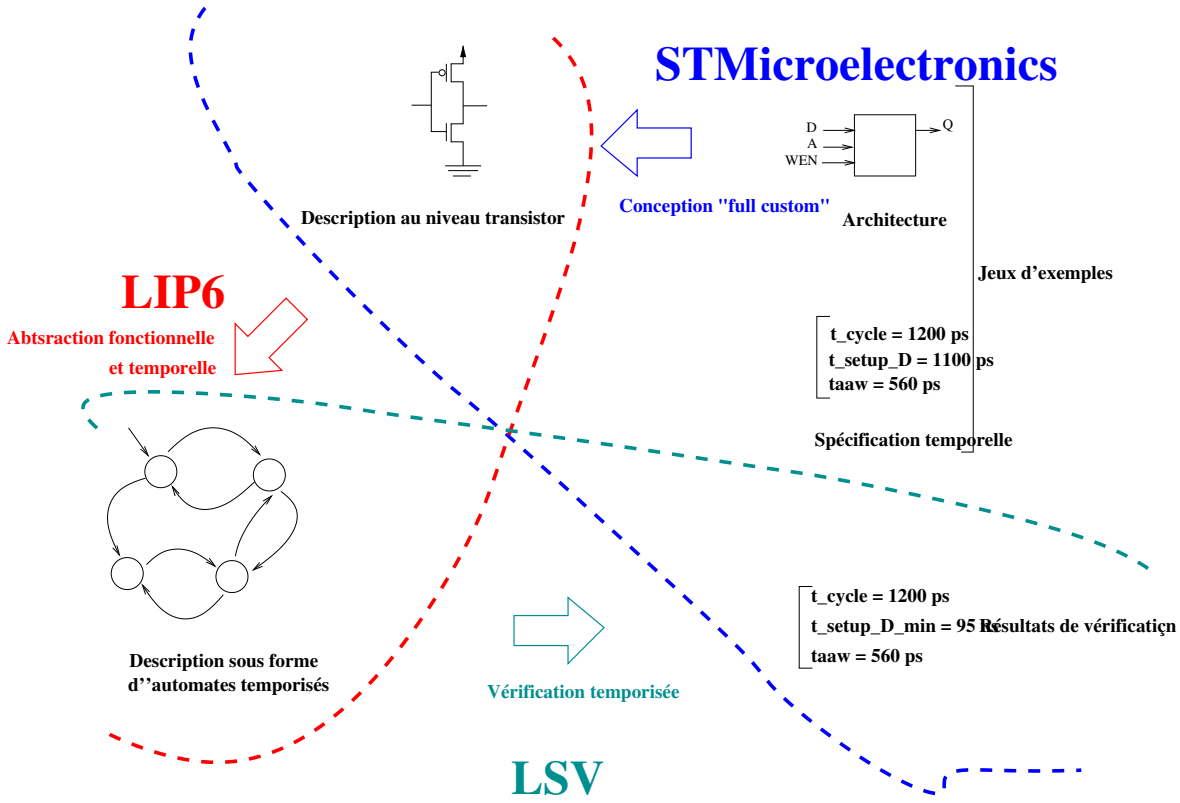

Figure 1: Vue schématique du projet VALMEM

Sous-tâche 1.1: Identification des problèmes spécifiques aux mémoires

Une étude précise des méthodes actuelles de développement des mémoires embarquées sera effectuée. L'étude portera en particulier sur les mémoires embarquées SRAM pour Systèmes sur Puce (SoC) développées par STMicroelectronics. Il fera notamment l'inventaire des principales limitations des méthodes de validation actuellement utilisées en production.

Responsable : STM
Participants : LIP6, LSV, STM
Durée: t_0 à $t_0 + 6$
Délivrable: Rapport D1.1. "Etat de l'art sur la conception et la validation des mémoires embarqués"

Sous-tâche 1.2: Elaboration d'un ensemble d'étude de cas issus de problèmes industriels

Il s'agit de sélectionner trois études de cas parmi l'ensemble des mémoires SRAM commercialisés par STMicroelectronics. Ces mémoires seront choisies en se focalisant sur des fonctionnalités de plus en plus complexes (en ignorant les caractéristiques liées à la taille de la mémoire). Suite au projet MEDEA+ "Blueberries", certaines mémoires apparaissent comme des études de cas intéressantes. Il s'agit notamment de:

- la mémoire SPSMALL, déjà étudiée dans "Blueberries", (avec une forte interaction humaine); nous souhaitons reprendre cet exemple pour comparer les résultats obtenus dans Blueberries avec ceux qui seront obtenus avec la chaîne de validation, développée dans ce projet.
- une mémoire embarquée avec "self-timing". Cette mémoire présente un contrôle plus complexe que celui de la mémoire SPSMALL. Elle est disponible en 90nm/65nm/45nm, ce qui correspond à une architecture unique avec différents jeux de paramètres temporels.
- La mémoire TERCAM, intégrant un mode de comparaison (nécessaire pour la réalisation de mémoires associatives), disponible en différentes technologies (90nm/65nm).

Responsable : STM
Participants : STM
Durée: t_0 à $t_0 + 6$
Délivrable: Rapport D1.2. "Définition des études de cas"

Sous-tâche 1.3: Application du flot de conception standard sur une étude de cas

La mémoire la plus simple, issue de D1.2, sera analysée selon le flot de validation couramment employée par STMicroelectronics. Un document décrira les performances et les limitations de ce processus de validation sur ce cas concret.

Responsable : STM
Participants : STM
Durée: $t_0 + 6$ à $t_0 + 12$

Délivrable Rapport D1.3. “Analyse du flot de conception et vérification d’une étude de cas avec la chaîne d’outils existante”

II-3.2 Tâche 2: Passage de la représentation en transistors au modèle abstrait; méthodes d’abstraction

Les circuits-mémoire “custom” sont des composants numériques. Cependant, les schémas utilisés pour la conception des ces circuits sont très particuliers. Ils incluent des circuits spécifiques qui permettent de concilier de temps d’accès très faibles et un encombrement minimal. Par ailleurs, certaines des ces mémoires comportent des fonctions complexes telles que des modes de veille ou des dispositifs de changement de tension pour réduire la consommation.

De ce fait, l’analyse fonctionnelle de ces circuits nécessite le développement d’une technique d’abstraction adéquate. De plus, la modélisation temporelle de ces circuits est très dépendante de leur topologie et de l’organisation spatiale des points-mémoire. De même, la prise en compte des chemins non-fonctionnels dans la modélisation temporelle de ces circuits est un élément clef.

Notre objectif est, dans un premier temps, de définir un modèle abstrait fonctionnel et temporel pour les circuits-mémoire custom. Ce modèle doit être défini de manière à pouvoir être intégré à un outil de vérification formelle. Dans un deuxième temps, un prototype logiciel sera développé permettant d’obtenir ce modèle abstrait à partir d’un schéma en transistors et des spécifications de la technologie de fabrication.

Pour ce faire, nous proposons de procéder en 4 étapes.

Sous-tâche 2.1: Etat de l’art des méthodes de validation temporelle

Nous procéderons à l’analyse manuelle des schémas des circuits-mémoire, puis nous établirons un état de l’art des méthodes d’abstraction et de modélisation temporelle (en considérant tout particulièment le modèle de délai “bi-bounded” généralement utilisé dans la vérification formelle).

Responsable : LIP6
Participants : LIP6, LSV
Durée: t_0 à $t_0 + 6$
Délivrable : Rapport D2.1.“Etat de l’art des méthodes de validation des mémoires”

Sous-tâche 2.2: Proposition d’un modèle fonctionnel et temporel d’un circuit-mémoire

Nous identifierons des points faibles des modèles existants et proposerons un modèle abstrait fonctionnel et temporel adapté à la vérification formelle. Ce modèle prendra en compte les spécificités des circuits-mémoire décrits au niveau transistor. La pertinence de ce modèle est un facteur essentiel pour la précision de la vérification visée.

Responsable : LIP6
Participants : LIP6, LSV
Durée: t_0 à $t_0 + 6$
Délivrable : Rapport D2.2 “Definition d’un nouveau modèle fonctionnel et temporel pour la vérification formelle de circuits mémoires”

Sous-tâche 2.3: Méthodes d'abstraction

Nous proposerons une méthode d'abstraction adaptée aux circuits-mémoire. Cette méthode intègrera les aspects fonctionnels et temporels de la description en transistors. Elle doit permettre d'analyser un circuit dans un temps raisonnable.

Responsable : LIP6
Participants : LIP6, LSV
Durée: $t_0 + 6$ à $t_0 + 12$
Délivrable : Rapport D2.3 "Combinaison de méthodes d'abstraction fonctionnelle et de méthodes de caractérisation temporelle d'un réseau de transistors"

Sous-tâche 2.4: Implémentation d'un prototype d'abstracteur

Nous développerons un outil logiciel prototype permettant de générer le modèle abstrait fonctionnel et temporel d'un circuit-mémoire. Cet outil prendra en entrée le schéma en transistors d'un circuit (extrait à partir du dessin des masques de fabrication) et les caractéristiques de la technologie de fabrication. Le modèle abstrait généré sera utilisé par l'outil de vérification formelle.

Responsable : LIP6
Participants : LIP6
Durée: $t_0 + 12$ à $t_0 + 24$
Délivrable : Prototype D2.4

II-3.3 Tâche 3: Méthodologies de validation temporelle

Dans le projet Blueberries, des outils généraux d'analyse des systèmes à base d'automates temporisés ont été utilisés. La tâche 3 vise à spécialiser ces méthodes dans le cadre de la vérification des circuits mémoires.

Sous-tâche 3.1: Spécialisation du modèle des automates temporisés

La représentation en automates temporisés de la mémoire présente les caractéristiques suivantes: grand nombre d'automates, petite taille individuelle, forte localisation du couplage entre automates. Une restriction appropriée du modèle d'automates temporisés et de leur produit sera proposée pour tenir compte de ces particularités.

Responsable : LSV
Participants : LSV, LIP6
Durée: $t_0 + 6$ à $t_0 + 12$
Délivrable: Rapport D3.1. "Modèle d'automates temporisés adaptés aux mémoires"

Sous-tâche 3.2: Algorithmes de vérification spécialisés

Dans la continuation de D3.1., nous développerons des méthodes de parcours de graphe (model checking) adaptés au nouveau modèle. Nous nous attacherons à conserver la potentialité de paramétrage, déjà exploitée avec succès dans le projet Blueberries.

Responsable: LSV (de $t_0 + 12$ à $t_0 + 18$).
Partenaires: LSV, LIP6
Durée: $t_0 + 12$ à $t_0 + 18$
Délivrable: Rapport D3.2. “Model checking d’automates temporisés spécialisés”

Sous-tâche 3.3: Implémentation d’un prototype de vérificateur

Ces modèles et algorithmes seront implémentés dans un outil-prototype. Cet outil prendra en entrée les descriptions abstraites de la mémoire (issues de la tâche 2) et permettra la vérification de propriétés fonctionnelles et temporisées.

Responsable: LSV
Partenaires: LSV
Durée: $t_0 + 12$ à $t_0 + 24$
Délivrable: Prototype D3.3. “Prototype de vérificateur”

II-3.4 Tâche 4: Application aux études de cas

Les prototypes développés dans les sous-tâches 2.3 et 3.3 seront expérimentés ici sur les jeux d’études élaborés dans la tâche 1. Les résultats obtenus seront comparés aux résultats avec le processus standard.

Sous-tâche 4.1: Analyse de l’application du flot de conception et de vérification standard aux (autres) études de cas

A la suite du rapport D1.3., les autres mémoires retenues seront analysées selon la chaîne de validation standard, pour servir de point de comparaison avec notre nouvelle démarche.

Responsable: STM
Partenaires: LSV, STM, LIP6
Durée: $t_0 + 12$ à $t_0 + 18$
Délivrable: Rapport D4.1. “Analyse du flot de conception et de vérification standard des (autres) études de cas avec la chaîne d’outils existante”

Sous-tâche 4.2: Expérimentation des prototypes sur les études de cas

Une interaction forte sera mise en place entre les 3 partenaires pour appliquer les nouveaux développements et prototypes aux mémoires retenues pour l’étude. Cette comparaison se fera en milieu industriel, ce qui nous permettra d’évaluer directement les nouvelles solutions proposées.

Responsable: STM
Partenaires: LSV, STM, LIP6
Durée: $t_0 + 18$ à $t_0 + 36$
Délivrable: Rapport D4.2. avec Démonstration “Expérimentation des prototypes sur les études de cas”

Sous-tâche 4.3: Comparaison des résultats obtenus et conclusions

Nous ferons une synthèse des résultats obtenus en D1.3., D4.1. et D4.2., afin de définir l'intérêt de la démarche proposée par rapport au flot de conception existant sur des exemples réels.

Responsable: STM
Partenaires: LSV, STM, LIP6
Durée: $t_0 + 30$ à $t_0 + 36$
Délivrable: Rapport D4.3. "Comparaison des résultats obtenus et conclusions"

II-3.5 Gestion du projet

Coordination. Laurent Fribourg (LSV) est le coordinateur global du projet.
En outre, chaque partenaire a un coordinateur:

- LSV: Laurent Fribourg
- LIP6: Pirouz Bazargan-Sabet
- STMicroelectronics: Remy Chevallier

Par ailleurs, il y a un responsable par tâche, chargés de la coordination et du suivi d'avancement des travaux et fournitures associés.

- Tâche 1: Remy Chevallier
- Tâche 2: Pirouz Bazargan-Sabet
- Tâche 3: Laurent Fribourg
- Tâche 4: Remy Chevallier

II-4 Délivrables

Notation: R = rapport; P = prototype; D = démonstration (application d'un prototype sur une étude de cas)

No	Titre	Nature	Resp.	Participants	début en $t_0 + \ldots$	fin en $t_0 + \ldots$
D1.1	Etat de l'art sur la conception des mémoires embarqués	R	STM	tous	0	6
D1.2	Définition des études de cas	R	STM	-	0	6
D1.3	Analyse du flot de conception et vérification d'une étude de cas avec la chaîne d'outils existante	R	STM	-	6	12
D2.1	Etat de l'art des méthodes de validation des mémoires	R	LIP6	LSV	0	6
D2.2	Définition d'un nouveau modèle fonctionnel et temporel	R	LIP6	LSV	0	6
D2.3	Combinaison des méthodes d'abstraction fonctionnelle et de caractérisation temporelle	R	LIP6	LSV	6	12
D2.4	Prototype d'abstracteur	P	LIP6	-	12	24
D3.1	Modèle d'automates temporisés adaptés aux mémoires	R	LSV	LIP6	6	12
D3.2	Model checking d'automates temporisés spécialisés	R	LSV	LIP6	12	18
D3.3	Prototype de vérificateur	P	LSV	-	12	24
D4.1	Analyse du flot de conception et vérification des (autres) études de cas avec la chaîne d'outils existante	R	STM	tous	12	18
D4.2	Expérimentation des prototypes sur les études de cas	R& D	STM	tous	18	36
D4.3	Comparaison des résultats obtenus et conclusions	R	STM	tous	30	36

II-5 Résultats escomptés

A l'issue du projet, les partenaires disposeront d'une solution logicielle prototype permettant la validation de mémoire au niveau transistor ainsi que d'une analyse permettant que comparer la méthode proposée avec les méthodes existantes à base de simulation.

La solution logicielle sera composée de deux outils prototypes. D'une part, un outil permettra d'abstraire la fonctionalité du circuit mémoire tout en y ajoutant des informations temporelles. D'autre part, à partir du modèle fonctionnel temporisé, un outil de vérification dédié permettra de valider les circuits mémoire. Ces deux outils prototypes étant novateurs, ils feront l'objet de publications dans des conférences et/ou revues internationales.

L'analyse comparative permettra de mettre en évidence les avantages et inconvénients de la méthode proposée par rapport aux méthodes actuellement utilisées sur des exemples commerciaux ciblés, aussi bien de façon quantitative que de façon qualitative.

II-6 Propriété intellectuelle

Au démarrage du projet, les partenaires signeront un protocole d'accord relatif aux questions de propriété intellectuelle et commerciale. Ce protocole d'accord comprendra également des clauses relatives à la confidentialité et aux publications. Dans son principe, ce protocole d'accord stipulera :

1. que chaque partie reste propriétaire de ses connaissances antérieures et que la participation au projet n'apporte pas de transfert des droits relatifs auxdites connaissances au profit des autres partenaires ou de tiers ;

2. qu'en ce qui concerne les résultats du projet, il ne sera créé aucune situation de copropriété. Chaque partenaire reste propriétaire des résultats relatifs aux sous-tâches auxquelles il a participé.

3. que les partenaires sont soumis à une obligation de confidentialité vis-a-vis des tiers sur les informations qu'ils recoivent au cours du projet.

En ce qui concerne les impératifs de publication, les partenaires adopteront les principes suivants :

1. Tout projet de publication ou communication émanant d'un partenaire et relatif aux travaux menés dans le cadre du projet sera soumis, préalablement à sa divulgation, à l'accord des autres partenaires.

2. Le projet de publication peut, soit être accepté "en l'état", soit faire l'objet d'une demande de modifications motivée par le souci de ne pas porter atteinte aux conditions d'une bonne exploitation industrielle et commerciale des résultats présentés dans le projet et particulièrement de respecter les intérêts des partenaires. En outre, une telle demande doit être présentée dans les meilleurs délais afin de ne pas entraver le projet. La réponse des partenaires devra intervenir dans les 15 jours ouvrés à compter de la date d'envoi de la demande par mail ou par courrier. Sans réponse de leur part, leur accord sera considéré comme acquis. Toutefois, de telles demandes de modification doivent s'efforcer de ne pas porter atteinte à la valeur scientifique du contenu du projet.

II-7 Eléments de Bibliographie

[Alur-Dill 94] R. Alur and D.L. Dill, "A Theory of Timed Automata" *Theoretical Computer Science 126*, North-Holland, pp. 183-235, 1994.

[BBM 03] R. Ben Salah and M. Bozga and O. Maler, "On timing analysis of combinational circuits", FORMATS'03, LNCS 2791, Springer, pp.204-219, 2003.

[Blueberries 06a] R. Chevallier, E. Encrenaz-Tiphène, L. Fribourg and W. Xu, "Timing Analysis of an Embedded Memory: SPSMALL", WSEAS Transactions on Circuits and Systems 5(7), pages 973-978, 2006.

[Blueberries 06b] R. Chevallier, E. Encrenaz-Tiphène, L. Fribourg and W. Xu. "Verification of the Generic Architecture of a Memory Circuit Using Parametric Timed Automata". In Proceedings of the 4th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'06), Paris, France, September 2006, LNCS 4202, pages 113-127. Springer.

[Brzozowski-Seger 94] J.A. Brzozowski and C-J.H. Seger, *Asynchronous Circuits*, Springer, 1994.

[CDY 99] S. Chakraborty, D.L. Dill and K.Y. Yun. "Min-Max Timing Analysis and An Application to Asynchronous Circuits". Proc. of the IEEE 87(2): 332-346, 1999.

[Clariso-Cortadella 04] R. Clariso and J. Cortadella, "Verification of timed circuits with symbolic delays", Proc. Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 628-633, 2004.

[Dioury et al. 00] K. Dioury, A. Lester, A. Debreil, G. Avot, A. Greiner and M.-M. Rosset-Louërat. "Hierarchical Static Timing Analysis at Bull with HiTas", Design Automation and Test in Europe Conference User Forum (DATE'2000), Paris, France, Mars 2000, pp. 55-60.

[HSIM] HSIM Simulator Description, `http://www.synopsys.com/products/`.

[HYTECH] T.A. Henzinger, P.-H Ho and H. Wong-Toi. "A User's guide to HYTECH", TACAS'95, LNCS 1019, Springer, pp. 41–71, 1995.

[KRONOS] S. Yovine. "KRONOS: A verification tool for real-time systems", *International Journal on Software tools for Technology Transfer 1*, pp. 123-133, 1997.

[Maler-Pnueli 95] O. Maler and A. Pnueli, "Timing analysis of asynchronous circuits using timed automata", CHARME'95, LNCS 987, Springer, pp.189-205, 1995.

[UPPAAL] K. Larsen, P. Pettersson and W. Yi, "UPPAAL in a Nutshell", *International Journal on Software tools for Technology Transfer 1*, pp. 134-152, 1997.

III - Justifications scientifiques des moyens demandés

III-1 Moyens financiers demandés à l'ANR dans le cadre du présent AAP

La majeure partie de notre budget est consacrée aux allocations de doctorat et postdoctorat. Notre projet de recherche est un projet sur trois ans, il nous permettra ainsi d'encadrer des thésards durant la totalité de leur thèse.

Nous insistons sur le fait que ces recrutements auront une dimension multi-site : les thésards recrutés auront à travailler en étroite collaboration avec l'ensemble des chercheurs impliqués dans les tâches correspondantes, cela impliquera des séjours longs dans les différents sites et pourra aussi se traduire par des coencadrements de thèse.

Le budget "fonctionnement" sera réparti au prorata des investissements des différentes équipes académiques impliquées. Il servira à l'organisation des réunions internes du projet (réunions plénières et réunions des sous-projets), aux visites entre sites (par exemple pour de longs séjours), ainsi qu'à des missions à l'étranger pour assister à des conférences internationales du domaines etc.

Le tableau 1 présente la répartition du personnel pour lequels une aide financière est demandée. Il s'agit du personnel non permanent recruté par les laboratoires pour le projet et du personnel permanent mis à disposition par le partenaire industriel pour la réalisation du projet.

	Nb total (en hommes.an)	LSV	LIP6	ST
Doctorants	3	3		
Postdoctorants	5	2	3	
Ingénieurs	2,4			2,4

Tab. 1 – Répartition du personnel pour lequel une aide financière est demandée

Le tableau 2 présente la répartition de l'aide demandée par partenaire. (Les 102,275 keuros demandés pour STM correspondent aux 35% du coût total dépensé par ce partenaire dans le projet.) Ce qui donne la répartition suivante de l'aide demandée par partenaire :

	LSV	LIP6	STM
Alloc. doctorants	90 k€		
Alloc. postdoc	90 k€	195 k€	
Salaire ing.			102,275 k€
Equipement pour les (post)doctorants	10 k€	10 k€	
Budget fonctionnement	40 k€	35 k€	
Total	**230 k€**	**240 k€**	**102,275 k€**

Tab. 2 – Aide demandée par partenaire

NB : Concernant le partenaire industriel STMicroelectronics, les frais d'équipement et de fonctionnement n'apparaissent pas, car ils sont inclus dans les coûts indirects liés aux salaires.

Nous donnons ci-dessous la liste et l'implication du personnel permanent impliqué dans le projet.

Partenaire	Prénom Nom	EC/C	Tps rech. (‡)
LSV	Emmanuelle Encrenaz	EC	40%
	Laurent Fribourg	C	40%
	Claudine Picaronny	EC	40%
LIP6	Pirouz Bazargan-Sabet	EC	40%
	Marie-Minerve Louerat	C	40%
	Patricia Renault	EC	40%
STMicroelectronics	Remy Chevallier	C	80%

TAB. 3 – Liste des participants

(‡) Le sigle 'EC' désigne un enseignant-chercheur, et le sigle 'C' un chercheur. La participation est donnée en pourcentage du temps de recherche (avec la convention habituelle selon laquelle 100% du temps de recherche d'un enseignant-chercheur équivaut à 50% de son temps total de travail).

Les "mini-CV" des permanents sont joints ci-après.

III-2 Autres actions contractuelles dans lesquelles les partenaires sont engagés

Nous présentons ici les projets institutionnels dans lesquels des personnes participant au projet sont investies.

STMicroelectronics Coopération au projet MEDEA+ "Blueberries" (*Building Up Embedded Memories*). Durée : 2004-2006.
Leader du Workpackage 3 : Design Verification (Partenaires : TRANSEDA, LSV)
Tâche WP3.1 : Formal techniques for fast/exhaustive eSRAM verification
Tâche WP3.2 : Fault injection and validation flows for eDRAMs and eSRAMs

LIP6

- Coopération avec l'ASU (Ain Shams Université). Durée : 2003-2008.
  Sujet : "Conception de circuits analogiques intégrés réutilisables. Environnement de conception CAIRO+"
- Projet CAPES-COFECUB avec l'Université Federal de Campina Grande, Brésil.
  Durée : 2005-2008.
  Sujet : "Réseaux de capteurs sans fil basse consommation"

LSV :

- European Network of Excellence ARTIST2 – Conception de systèmes embarqués. Durée : 2004-2008.
  Partenaires (du cluster "Testing and Verification") : Univ. d'Aalborg (DK), VERIMAG, Univ. de Twente (PB), Centre Fédéré en Vérification (B), INRIA. IRISA
- Projet Medea+ Blueberries (Workpackage 3 : Design Verification). Durée : 2004-2006.
  Partenaires : STM, TRANSEDA.
- Projet ANR "ESCAPADE" (Evaluation de l'impact des systèmes informatisés sur la sûreté de fonctionnement des installations industrielles)
  Partenaires : EDF, CEA, Université de Troyes. Soumis.

III-3 Suggestion d'Experts

Oded MALER, Oded.Maler@imag.fr, VERIMAG.
Domaines d'expertise : Vérification formelle de circuits, Automates temporisés.

Etienne SICARD, etienne.sicard@insa-toulouse.fr, INSA-Toulouse.
Domaines d'expertise : cross-talk, compatibilité électromagnétique.

Christian Piguet, christian.piguet@csem.ch, CSEM.
Domaines d'expertise : conception basse consommation.

Michel Robert, Michel.Robert@lirmm.fr, LIRMM.
Domaines d'expertise : modélisation temporelle.

PARTICIPANTS

Pirouz BAZARGAN SABET

Né le 2 Avril 1962, Maître de Conférences à l'Université Paris 6.

Domaine d'expertise:
Méthodes et outils de vérification post-layout de circuits numériques CMOS (simulation logique et temporelle, analyse temporelle, évaluation de la consommation, analyse de bruit de diaphonie).

Publications

1. N. Abdallah, P. Bazargan Sabet . "Modeling the Effects of Input Slew Rate and Temporal Proximity of Input Transitions in Event-Driven Simulation", 38th IEEE Southeastern Symposium on System Theory, Cookeville, Tennessee, USA, 2006.

2. P. Bazargan Sabet, P. Renault. "Using Symbolic Simulation to Exhibit Worst Case Crosstalk Noise Configuration", 4th IEEE Latin-American Test Workshop, Natal, Rio Grande de Norte, Brasil, pp. 264-268, 2003.

3. P. Bazargan Sabet, F. Ilponse. "Modeling Crosstalk Noise for Deep Submicron Verification Tools", Design Automation and Test in Europe, IEEE & ACM, pp. 530-534, 2001.

Remy CHEVALLIER

29 ans, Ingénieur méthodes et vérification à STMicroelectronics.

Domaine d'expertise:
Amélioration de la qualité des circuits avant fabrication par l'étude et le déploiement de méthodes innovantes de vérification formelle.

Publications:

1. R. Chevallier, E. Encrenaz-Tiphène, L. Fribourg and W. Xu. "Timing analysis of an embedded memory: SPSMALL". WSEAS Transactions on Circuits and Systems 5(7), pages 973-978, 2006.

2. M. Baclet and R. Chevallier. "Timed Verification of the SPSMALL Memory". In Proceedings of the 1st International Conference on Memory Technology and Design (ICMTD'05), Giens, France, May 2005, pages 89-92.

3. Ghiath Al Sammane, Dominique Borrione, Remy Chevallier, "Verification of behavioral descriptions by combining symbolic simulation and automatic reasoning". ACM Great Lakes Symposium on VLSI 2005: 260-263.

Emmanuelle ENCRENAZ

Née le 24 Septembre 1969, Maître de Conférences à l'Université Paris 6, actuellement en délégation CNRS au LSV (sept. 2005 - août 2007).

Domaine d'expertise:
Méthodes formelles pour la conception et la vérification de systèmes matériels.

Publications

1. S. Taktak, E. Encrenaz, J.-L. Desbarbieux. "An Automatic Tool for the Deadlock Detection in Whormhole Networks on Chip", 11th IEEE international workshop on High-Level Design Verification and Test (HLDVT'2006), nov 2006, California.

2. C. Braunstein, E. Encrenaz. "Formalizing the incremental design and verification process of a pipelined protocol converter", IEEE 17th international workshop on Rapid System Prototyping (RSP'2006) june 2006, Crete.

3. C. Roux, E. Encrenaz. "CTL may be ambigous when model-checking Moore Machines", IFIP WG 10.5 12th international advanced research working conference on correct harware design and verification methods (CHARME 2003), nov 2003, Italy. Lecture Notes in Computer Science vol 2860.

Laurent FRIBOURG

Né le 26 novembre 1957, Directeur de Recherche au CNRS, au LSV.

Domaine d'expertise:
Méthodes formelles à base d'automates temporisés (model checking).

Publications

1. R. Chevallier, E. Encrenaz-Tiphène, L. Fribourg and W. Xu. "Verification of the Generic Architecture of a Memory Circuit Using Parametric Timed Automata". In Proceedings of the 4th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'06), Paris, France, September 2006, LNCS 4202, pages 113-127. Springer.

2. R. Chevallier, E. Encrenaz-Tiphène, L. Fribourg and W. Xu. "Timing analysis of an embedded memory: SPSMALL". WSEAS Transactions on Circuits and Systems 5(7), pages 973-978, 2006.

3. B. Bérard, L. Fribourg, F. Klay and J.-F. Monin. "A Compared Study of Two Correctness Proofs for the Standardized Algorithm of ABR Conformance". Formal Methods in System Design 22(1), pages 59-86, 2003.

Marie-Minerve LOUERAT

Née le 29 avril 1959, Actuellement Chargée de recherche au CNRS au LIP6.

Domaine d'expertise:
Outils et méthodes de conception de circuits intégrés analogiques et mixtes. Impact des nouvelles technologies sur les outils de vérification VLSI. Analyse statique temporelle.

Publications

1. R. Iskander, M.-M. Louërat, A. Kaiser. "Hierarchical Graph-Based Sizing for Analog Cells Through Reference Transistors", Microelectronics and Electronics (PRIME'06),Otranto, Italy, June 2006, pp. 321-324, Winner of the Bronze Leaf Certificate.

2. H. Aboushady, L. de Lamarre, N. Beilleau, M.-M. Rosset-Louërat. "Automatic Synthesis and Simulation of Continuous-Time Sigma Delta Modulators", Design Automation and Test in Europe (DATE'04), Paris, February 2004, pp. 674-675, Winner of the Best Interactive Presentation.

3. K. Dioury, A. Lester, A. Debreil, G. Avot, A. Greiner, M.-M. Rosset-Louërat. "Hierarchical Static Timing Analysis at Bull with HiTas", Design Automation and Test in Europe Conference User Forum (DATE'2000), Paris, France, Mars 2000, pp. 55-60, Winner of the User Forum.

Claudine PICARONNY

45 ans. Actuellement: Maître de Conférences au LSV.

Domaine d'expertise:
Vérification formelle des systèmes distribués, en particulier des protocoles de télécommunication.

Publications

1. M. Duflot, M. Kwiatkowska, G. Norman, D. Parker, S. Peyronnet, C. Picaronny and J. Sproston. "Practical Applications of Probabilistic Model Checking to Communication Protocols". In FMICS Handbook on Industrial Critical Systems. Springer, 2006.

2. M. Duflot, L. Fribourg, Th. Hérault, R. Lassaigne, F. Magniette, S. Messika, S. Peyronnet and C. Picaronny. "Probabilistic Model Checking of the CSMA/CD Protocol Using PRISM and APMC". In Proceedings of the 4th International Workshop on Automated Verification of Critical Systems (AVoCS'04), London, UK, August-September 2004, ENTCS 128(6), pages 195-214. Elsevier Science Publishers, 2005.

3. B. Bérard and C. Picaronny. "Accepting Zeno Words without Making Time Stand Still". In Proceedings of the 22nd International Symposium on Mathematical Fundations of Computer Science (MFCS'97), Bratislava, Slovakia, August 1997, LNCS 1295, pages 149-158. Springer.

Patricia RENAULT

Née le 21 Avril 1976. Actuellement : Maître de conférences à l'université Pierre et Marie Curie - Laboratoire d'Informatique de Paris 6.

Domaine d'expertise:
Méthodes et outils de vérification de circuit au niveau transistor.

Publications

1. P. Renault and P. Bazargan Sabet. "Splitting of RC-Network for Accurate Model Reduction", 16th International Conference on Microelectronics (ICM'04), Tunis, Tunisia, décembre 2004, pp. 734-737

2. P. Renault and P. Bazargan Sabet. "Determining The Analytic Waveform of an RC-Circuit Output", 11th International Conference Mixed Design of Integrated Circuits and Systems (MIXDES 2004), Szczecin, Poland, June 2004, pp. 363-368

3. P. Renault and P. Bazargan Sabet. "A Simplified Circuit to Model RC Interconnect", 4th WSEAS International Conference on Instrumentation, Measurement, Control, Circuits and Systems (IMCCAS'04), Miami, USA, avril 2004