micro et nanoélectronique
microsystèmes
intelligence ambiante
biologie et santé
chaîne de l'image

Vérification formelle de systèmes et circuits asynchrones

Collaboration IAN - VASY

Yves Durand
Hubert Garavel
Wendelin Serwe
Yvain Thonnart

INRIA RHÔNE-ALPES leti MINATEC INSTITUT CARNOT CEA LETI

cea

Introduction - Motivations

Objectifs

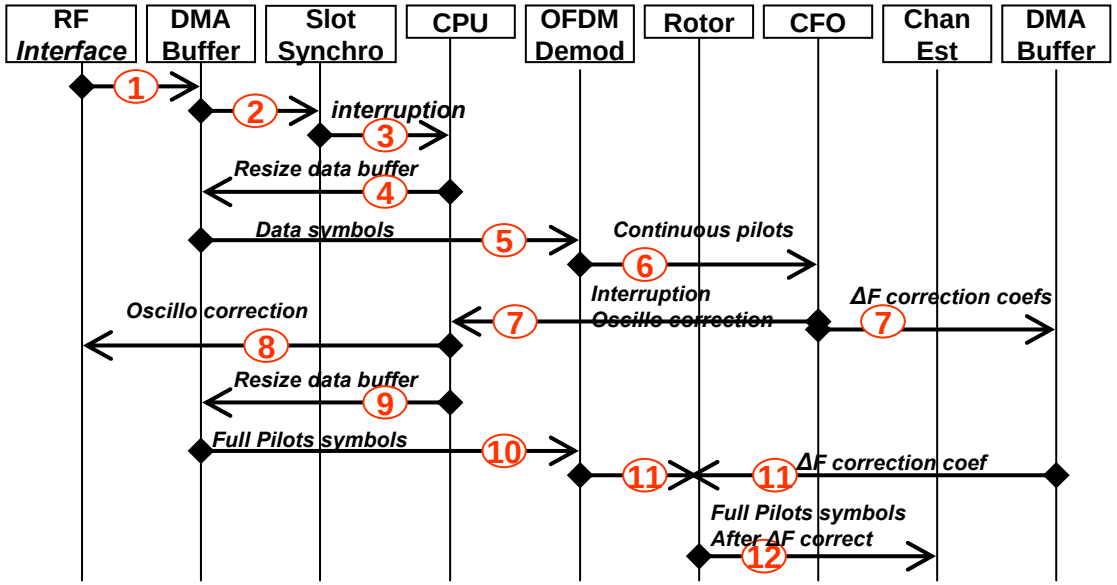
- Le LETI conçoit des circuits et systèmes faisant intervenir de l'asynchronisme
- L'INRIA fournit des outils de vérification formelle (CADP) pour les systèmes asynchrones.
- But : résoudre les problèmes du LETI à l'aide des outils INRIA

Problématique asynchrone dans les SoC

- Nécessité de la distribution du calcul
  - Limites du contrôle centralisé
  - Passage à l'échelle des SoCs complexes
- Multiples formes de l'asynchronisme
  - Systèmes distribués et protocoles associés
    - Networks-on-Chip
  - Circuits en logique asynchrone
    - Processus communicants asynchrones
    - Implémentation matérielle
- 50% des ressources dévolues à la vérification
- Aucune solution commerciale pour vérifier les architectures asynchrones

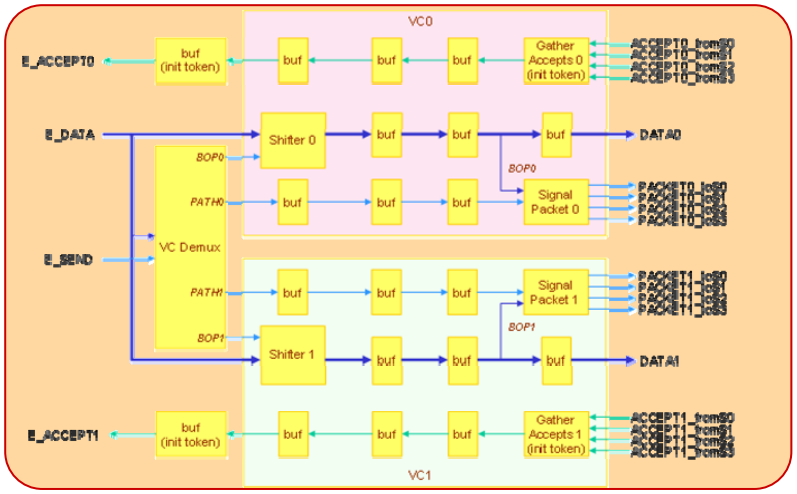
Niveau système

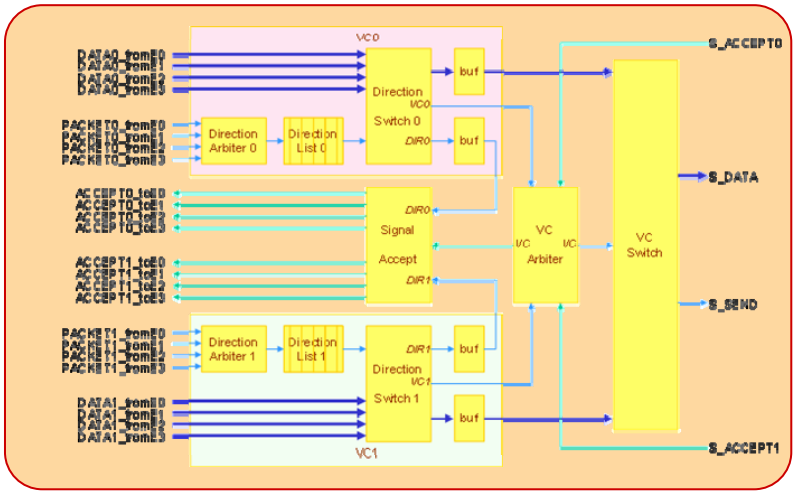
- Processus distribués
- Synchronisation par messages
- Problématiques :
  - Garantir l'absence de blocage
  - Garantir l'intégrité des données dans les FIFOs
  - etc.



Micro-architecture des circuits asynchrones

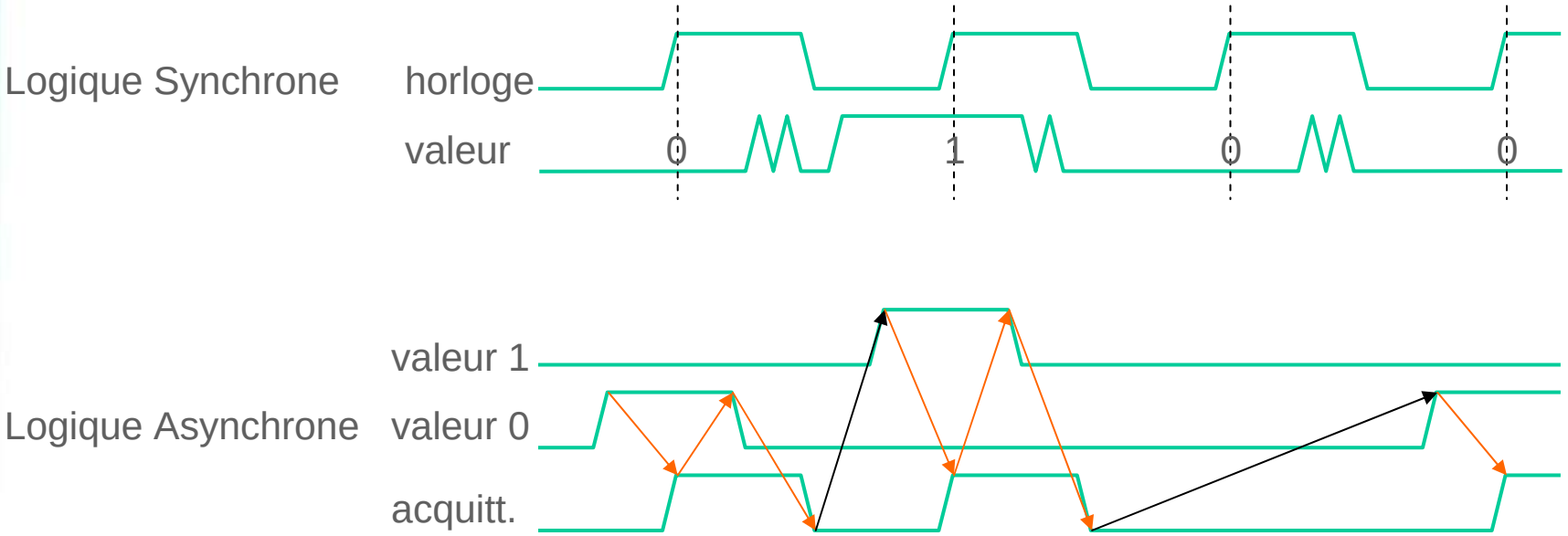
- La fonction globale est réalisée par des processus communicants élémentaires implantables en portes logiques
- Les échanges de données se font par synchronisations locales
- Un jeu d'événements d'entrée d'un processus déclenche un jeu d'événements de sortie
- Problématiques :
  - absence de deadlock
  - la composition des processus élémentaires doit réaliser la fonction globale





Niveau implémentation en portes logiques

- La logique est insensible aux délais
  - Toute transition d'un signal correspond à une communication
- Problématiques :
  - la logique ne doit pas effectuer de transition non significative
  - toute transition entrante doit être acquittée par une transition sortante



Résultats de la collaboration : Méthodes et outils

Les outils CADP de l'INRIA

- Une large palette de fonctions
  http://www.inrialpes.fr/vasy/cadp
- Plusieurs langages de modélisation utilisés au LETI
  - LOTOS : langage directement supporté par CADP
  - CHP : langage indirectement supporté
  - TLM : étude de faisabilité en cours
- Vérification par equivalence checking
- Vérification par model checking
- Evaluation de performance (chaînes de Markov)

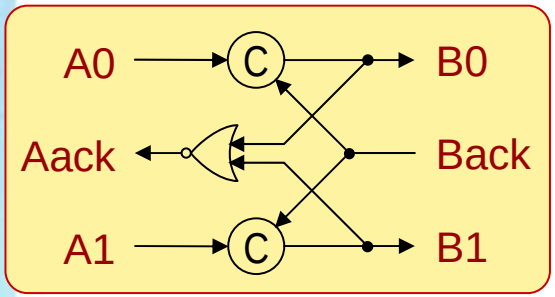
Axe 1 : vérification de modèles CHP

- Pour FAUST, le CEA/Léti utilise le langage CHP en partenariat avec le TIMA (outil de synthèse TAST)
- Objectif : permettre l'utilisation de CADP pour vérifier des descriptions CHP
- Résultat 1 : sémantique formelle de CHP
  - définition complète de la sémantique de CHP en formalisme SOS
  - y compris la notion de "*probe*"
- Résultat 2 : traducteur CHP2LOTOS
  - sep. 2005 : première version ("mono-probe")
  - sep. 2007 : seconde version ("multi-probe")
  - 20 000 lignes de code
- Utilisation sur des spécifications CHP du LETI
  - plusieurs erreurs détectées
- Publications : conf. IFM'05, soumission à une revue

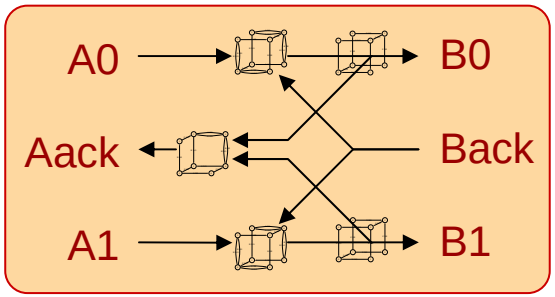
Axe 2 : vérification de modèles TLM

- Idée : faire le lien entre SystemC/TLM (projet OpenTLM de Minalogic) et les outils CADP de l'INRIA
- Etude de la traduction TLM -> LOTOS
  - Problème : TLM est informel alors que LOTOS est formel
- Résultats :
  - sémantique asynchrone (sans *scheduler*) pour TLM
  - compatibilité (par préordre) avec la sémantique synchrone
  - schéma de traduction entre TLM et CADP
  - expérimentation positive sur un modèle TLM (Verimag)
  - travaux en cours sur un gros modèle TLM (*blitter* ST)
- Publication : conf. FM'08

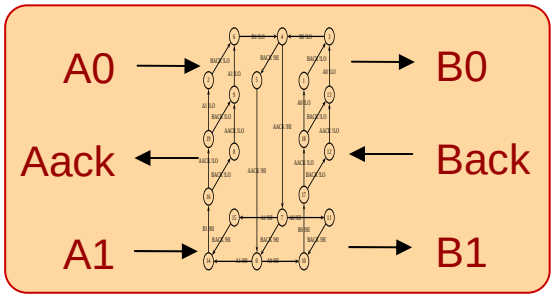
Axe 3 : vérification d'implémentations matérielles



Implémentation quasi-insensible aux délais



Modèle comportemental compositionnel (1600 états)



Modèle comportemental réduit (20 états)

- Besoins :
  - traduction de CHP en RTL (netlists) manuelle ou semi-manuelle
  - il faut vérifier que les assemblages de portes logiques (NAND, NOR, Muller, etc) font ce qui est décrit en CHP
  - plus difficile qu'en synchrone, car on doit vérifier les signaux à tout instant et non pas seulement sur les fronts d'horloge
  - beaucoup de travaux théoriques, mais pas d'outils commerciaux

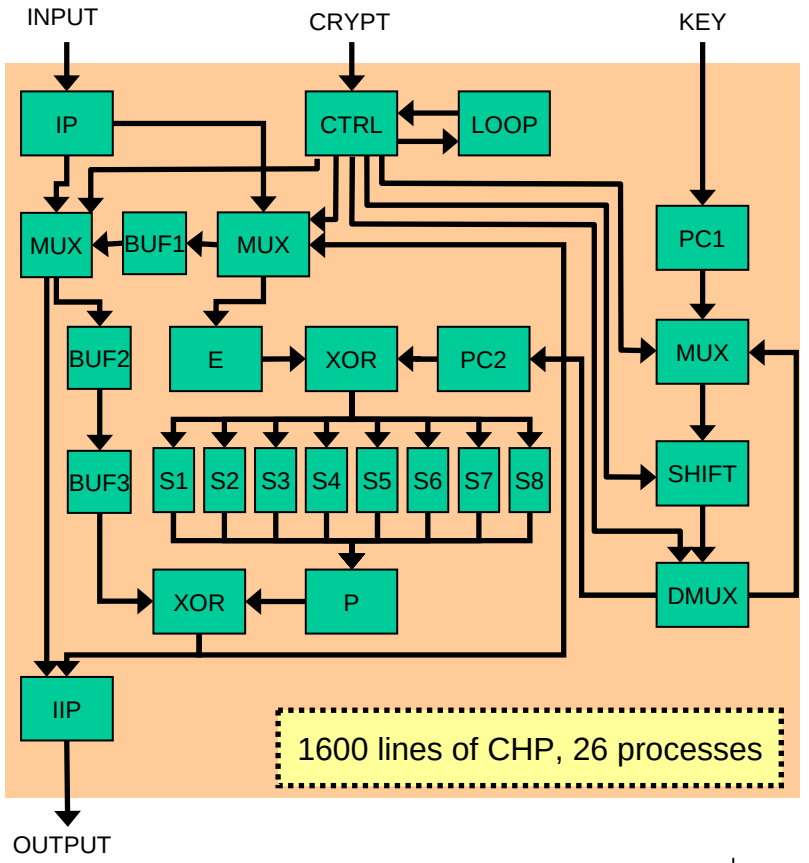
- Résultats [Y. Thonnart] :
  - on peut utiliser LOTOS et CADP pour vérifier une implantation matérielle
  - vérification formelle de la nécessité de l'hypothèse de fourche asynchrone dans la conception de circuits asynchrones quasi-insensibles aux délais

Résultats de la collaboration : Vérification de SoCs du LETI

Étude de cas : DES asynchrone

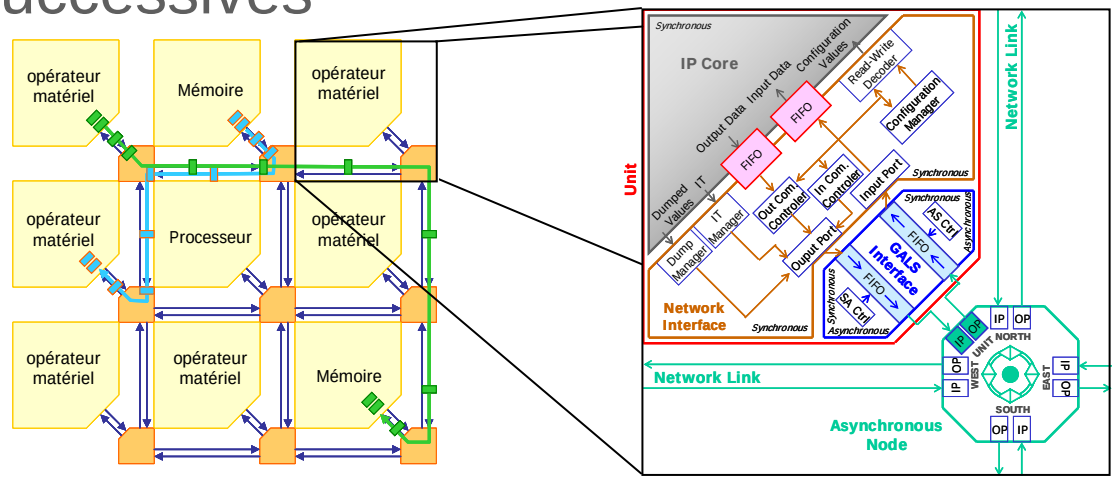
- Étude de faisabilité : DES (*Data Encryption Standard*)
- Modélisation manuelle en LOTOS
- Traduction CHP vers LOTOS
- Grand espace d'états

  (> 108 millions états)
- Avec CADP, génération compositionnelle dans 10 minutes (16.910 états)
- Propriétés vérifiées :
  - Absence de blocage
  - Bon nombre d'itérations



Les concepts de l'architecture FAUST

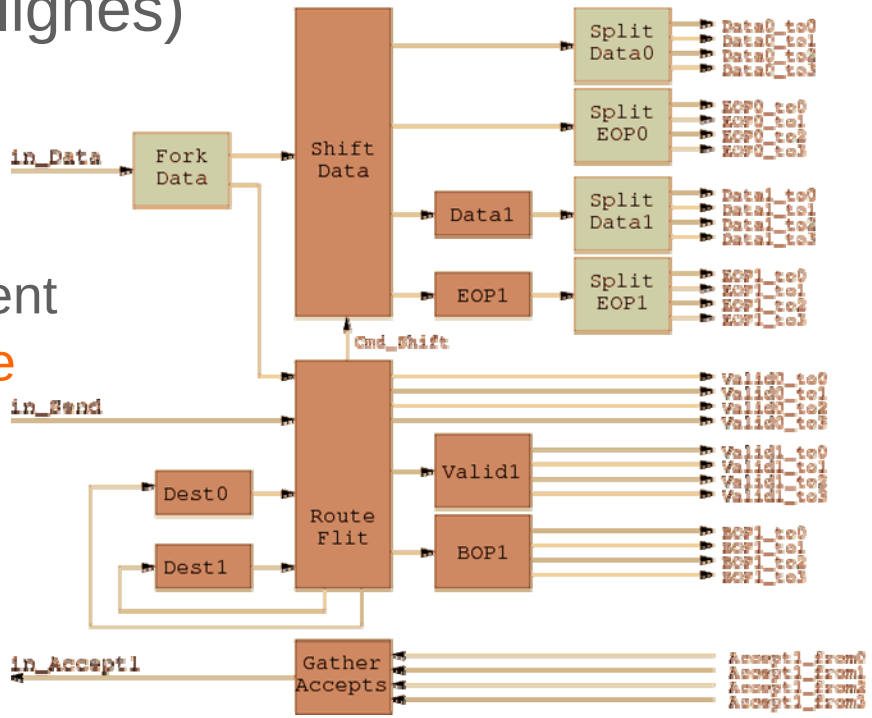
- Architecture distribuée pour flots de données
- Applications : télécommunications sans fil à haut débit
- Une architecture GALS (*Globally Asynchronous, Locally Synchronous*)
- Organisation en NoC (*network on chip*), implémenté en logique asynchrone
- Deux versions successives



FAUST v1 : Micro-architecture du routeur

- Étage d'entrée (14 processus asynchrones)
- Modélisée en CHP (1 200 lignes)
- Traduit en LOTOS (3 600 lignes) avec CHP2LOTOS
- Techniques de réduction
  - Indépendance des données
  - Restriction de l'environnement
  - Génération compositionnelle (40 étapes, 500 lignes)

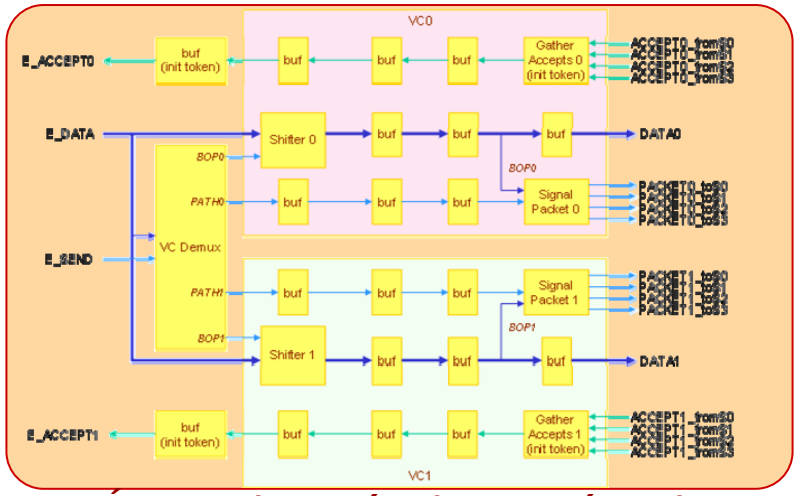
  ➔1 300 états (4 minutes)
- Propriétés vérifiées
  - absence de blocage
  - intégrité des données



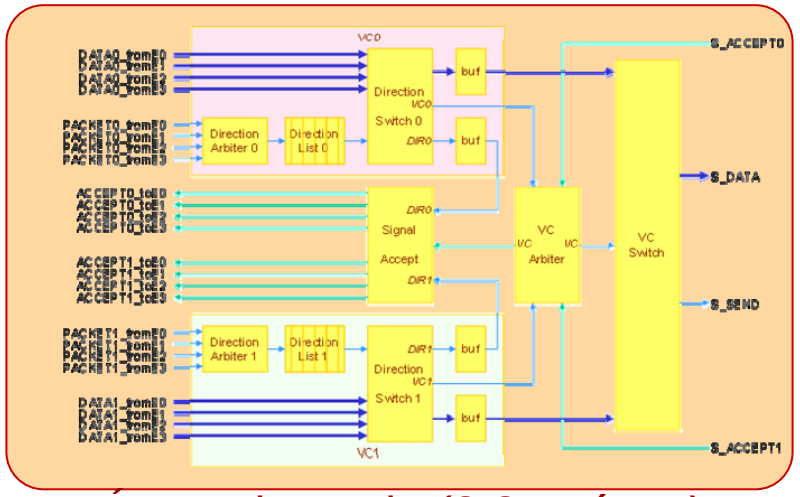
- Découverte d'un **problème de routage** (sous-spécification en CHP, résolu dans l'implantation)
- Publication lors de la conf. internationale ASYNC'07

FAUST v2 : Micro-architecture du routeur

- Modélisé en CHP
  - 27 + 13 processus
  - 900 lignes de CHP
- Traduit en LOTOS
  - utilisation de CHP2LOTOS
  - 2 000 lignes de LOTOS
- Génération compositionnelle pour lutter contre l'explosion combinatoire
- Espaces d'états générés
  - plusieurs millions d'états
  - simulation interactive avec l'outil OCIS
- Travaux en cours …



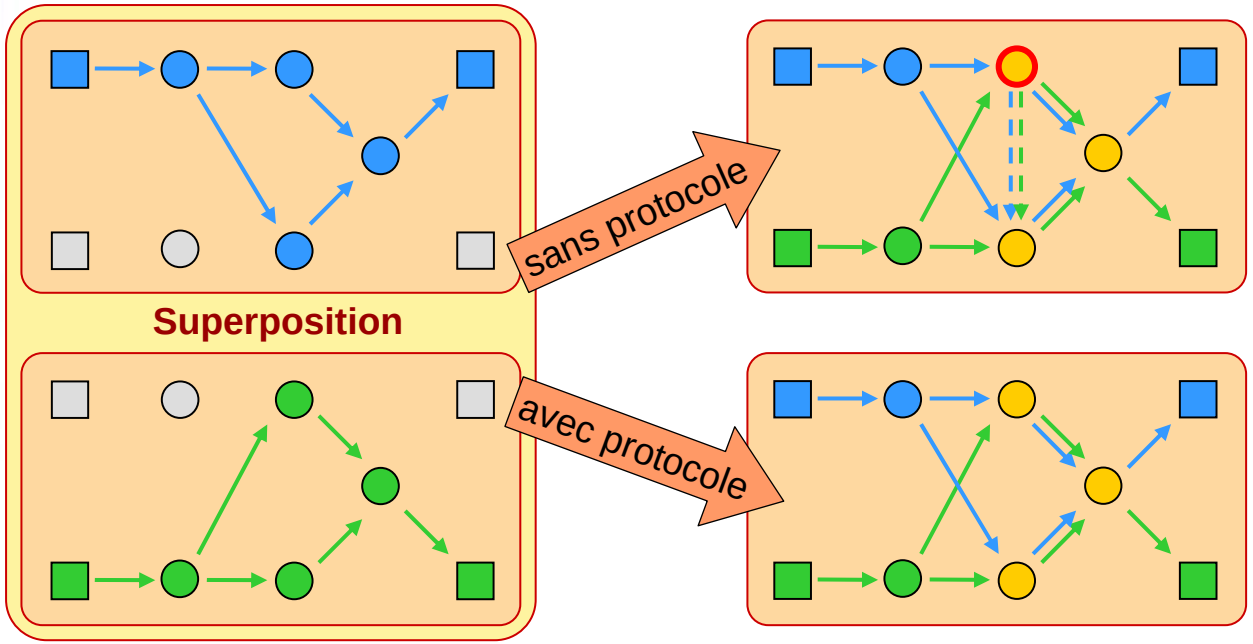
Étage d'entrée (4,2 M états)



Étage de sortie (2,8 M états)

FAUST : Synchronisation multi-tâches

- Superposition de deux tâches réparties simultanées
- Modélisation en LOTOS (500 lignes) : 300000 états
- Validation du protocole de synchronisation entre ressources distribuées dans le cas d'un fonctionnement multi-applicatif jusqu'à 5 ressources



Blocage du système

Exhibé avec CADP

Bon fonctionnement

Vérifié avec CADP (5 ressources)

Conclusion

Une coopération active

- L'INRIA a financé 4 années de post-doctorant (Gwen Salaün, puis Olivier Ponsini)
- 2005 : voyage d'études au Japon
  - Fabien Clermidy (CEA/LETI)
  - Wendelin Serwe (INRIA)
- 2005 : proposition RNTL "VEPADI"
- 2005-2006 : projet de pôle Minalogic "MULTIVAL"
  - Bull, CEA/LETI, INRIA/VASY, ST
  - déc. 2005 : labellisation EMSOC
  - déc. 2006 : démarrage du projet
  - Trois architectures à fort potentiel :
    - FAME2 (Bull)
    - FAUST (CEA/LETI)
    - xSTream (STMicroelectronics)
- Publications : IFM'05, ASYNC'07, FM'08

Retombées et perspectives

- Apport de méthodes et outils pour concevoir des systèmes distribués et des circuits asynchrones
- Face aux besoins du LETI, les outils CADP de l'INRIA ont plutôt bien tenu le choc
- Perspectives
  - Principalement dans le cadre du projet MULTIVAL
  - Côté INRIA : meilleure intégration des outils CADP dans le flot de conception ; passerelles avec CHP et SystemC/TLM
  - Côté LETI : utilisation de CADP à plusieurs niveaux :
    - Système : co-simulation entre implémentation et modèle LOTOS
    - Architecture : vérification du routeur FAUST v2
    - Implantation : développement d'un traducteur VERILOG2LOTOS pour modéliser l'implémentation au niveau portes

Contributeurs

CEA/LETI

- Edith Beigné
- François Bertrand
- Yves Durand
- Sahar Foroutan
- Virang Shah
- Yvain Thonnart
- Pascal Vivet

INRIA

- Hubert Garavel
- Claude Helmstetter
- Frédéric Lang
- Radu Mateescu
- Olivier Ponsini
- Gwen Salaün
- Wendelin Serwe