

## Proposition d'action spécifique

# Composants et architectures temps réel

**Coordinateur : Anne-Marie Deplanche**

IRCCyN- UMR 6597 - Ecole Centrale de Nantes  
BP 92101 - 1, rue de la Noe - 44321 - Nantes cedex 3

[Anne-Marie.Deplanche@irccyn.ec-nantes.fr](mailto:Anne-Marie.Deplanche@irccyn.ec-nantes.fr)

Tel. : 02 40 37 69 77 - Fax. : 02 40 37 69 30

Juin 2003

## 1. Contexte et problématique

Cette proposition d'action spécifique s'intègre dans le contexte du développement formel d'applications temps réel distribuées et sûres par composition de composants. Ce type d'application relève de deux critères antagonistes :

- Le premier est d'ordre économique. Les approches « composants » apportent une grande flexibilité dans la réutilisation de parties d'application et ont pour objectif final une productivité accrue.
- Le second est lié aux propriétés de sûreté, et pour ce projet en particulier, aux propriétés temps réel pour lesquelles une garantie doit être formellement prouvée.

La plupart des approches étudiées à ce jour portent sur la notion de composant logiciel. Néanmoins, les modèles et techniques associées ne peuvent suffire dans le cadre du temps réel où il est indispensable de prendre en compte l'impact des performances du support exécutif (puissance des processeurs, stratégies d'ordonnancement, débit des réseaux, protocoles, ...) sur les caractéristiques des composants ou de leurs architectures. Si on s'attache à la notion de composition, les premières études ont été menées par la communauté du génie logiciel et ont développé le concept de langage de description d'architectures (ADL – Architecture Description Language) (Medvidovic and Taylor, 2000). En particulier, certains de ces langages ont été proposés pour le développement d'applications temps réel ; on peut citer, en particulier MetaH (Vestal S., 1995.). L'approche architecturale constitue un point clé pour la validation d'une composition de composants en particulier, la description formelle d'architecture doit, entre autres, permettre de dériver automatiquement les modèles analysables par des techniques de validation / vérification formelle. Les travaux réalisés à ce jour pour résoudre ce problème dans le contexte du temps réel, portent essentiellement sur les analyses d'ordonnancabilité (Binns and Vestal, 2001) ou sur l'évaluation de performances par des techniques de simulation (Castel Pietra *et al.*, 2002).

## 2. Travaux à mener

Le problème de la conception d'applications temps réel distribuées par une approche « composants/architecture » sera abordé par des actions coordonnées et complémentaires afin :

- d'une part, d'identifier ce qui, dans le domaine des applications temps réel distribuées, peut constituer un « composant » (Kopetz, 2002) et ainsi d'en proposer une définition formelle (un composant est-il un logiciel résidant sur une entité de calcul, un ensemble <logiciel(s)-calculateur(s) support(s)>, un ensemble de logiciels distribués, les services de communication d'une architecture complexe distribuée, un intergiciel, ...)
- et, d'autre part, de faire émerger des modèles et / ou méthodes qui permettent de représenter un composant et d'exploiter ces modèles pour des activités de validation / vérification tant au niveau propre du composant qu'au niveau de sa composition au sein d'une architecture ; nous focaliserons les études sur les modèles et / ou méthodes qui permettront de prendre en considération les aspects « temps réel » et qui supporteront les activités de validation / vérification tant *a priori* qu'*a posteriori* (test).

En particulier, nous nous proposons d'étudier la notion d'architecture « type » (framework), particulièrement présente dans le domaine des systèmes temps réel (« Design Pattern », « ADL temps réel »). dans le but de proposer une approche pour leur description (et leur comparaison). Cela permettrait à terme de s'affranchir du reproche que l'on peut faire aux ADL temps réel, d'être dédié à un domaine d'application très particulier comme les systèmes embarqués dans l'automobile (Elloy and Simonot-Lion, 2002 ; Hansson et al., 1996), dans l'avionique (Binns and Vestal, 2001), multimédia (Duran-Limon and Blair, 2000), etc.

Les domaines d'application privilégiés seront d'une part :

- les systèmes critiques embarqués,
- les systèmes de télé opération ou télésurveillance mettant en œuvre des infrastructures de télécommunication et / ou de l'Internet.

## 3. Equipes impliquées

### 3.1. Partenaires académiques

#### ▪ AOSTE (avant projet commun I3S - INRIA)

Marie-Agnes Péraldi-Frati ([map@unice.fr](mailto:map@unice.fr))

Le savoir faire des membres de l'avant-projet AOSTE<sup>1</sup> porte sur :

- la spécification de « Profils UML » pour systèmes embarqués (André *et al.*, 2002)
- La spécification du comportement des composants (aspects réactifs) et la sémantique et l'analyse des modèles utilisés pour décrire ces comportements (modèles synchrones) (André, 2003 ; André and Rigault, 2002)

---

<sup>1</sup> Les membres de l'avant-projet AOSTE, du projet TRIO de l'INRIA, de l'équipe « Systeme Temps Réel » de l'IRCCyN ont participé aux projets nationaux COVADIS, Architecture Electronique Embarquée (Elloy and Simonot-Lion, 2002) et au projet européen ITEA EAST-EEA.

- Les modèles exécutables d'architectures mixtes matérielles/logicielles (Mallet *et al.*, 2001)

- **CITI (INSA – Lyon)**

*Jean-Philippe Babau* ([Jean-Philippe.Babau@if.insa-lyon.fr](mailto:Jean-Philippe.Babau@if.insa-lyon.fr))

Le Centre d'Innovations en Télécommunications et Intégration de services développe une activité de recherche fondamentale et appliquée dans les domaines des réseaux et des télécommunications. L'objectif majeur est de concevoir, modéliser, et valider les éléments matériels et logiciels permettant la mise en œuvre de services et protocoles dans les réseaux ainsi que dans les systèmes embarqués (Babau, 2000).

Dans le cadre de cette proposition, le CITI apportera ses compétences sur les modèles de systèmes exécutifs à base de composants (thèse en cours en collaboration avec France Télécom R&D).

- **Féria – groupe SVF (Spécification, Vérification Formelles)**

Féria (Fédération de Recherche en Informatique et Automatique) est une fédération CNRS regroupant les trois laboratoires d'informatique toulousains ONERA/DTIM IRIT/CNRS et LAAS/CNRS.

*François Vernadat* ([francois@laas.fr](mailto:francois@laas.fr))

Le groupe SVF a pour domaine de compétences l'étude et la mise en œuvre des techniques formelles pour le développement - de la spécification à la vérification - des systèmes informatiques. Les domaines d'application visés concernent les systèmes concurrents et réactifs. Dans le cadre de l'action spécifique, l'effort portera sur les ADLs, particulièrement sur le plan de leur sémantique, afin de permettre leur couplage avec des techniques formelles de spécification (du comportement et des propriétés attendues) et de vérification. La réalisation d'un tel couplage permettra de vérifier les propriétés qualitatives et quantitatives des systèmes considérés (Berthomieu, 2003).

Féria/SVF participe notamment au projet RNTL COTRE (Composants Temps Réel) dont l'objectif est de définir une démarche outillée de modélisation et de validation d'architecture de logiciels temps réel permettant de combiner les approches formelles et semi-formelles dans un processus industriel. Dans le cadre de ce projet, le groupe SVF a acquis une compétence dans le domaine des ADL utilisés dans l'avionique (Farinas *et al.*, 2002 ; Berthomieu *et al.*, 2002).

- **INRIA – Projets TRIO (LORIA-UMR 7503) et TRISKELL (IRISA- UMR 6074)**

*Françoise Simonot-Lion* ([simonot@loria.fr](mailto:simonot@loria.fr))

Le projet TRIO<sup>1</sup> du LORIA développe des méthodes, modèles et outils pour la conception d'architecture distribuées temps réel. Dans le cadre de cette action spécifique, TRIO apportera ses compétences sur trois points :

- Modélisation d'architectures opérationnelles distribuées et soumises à des contraintes temps réel et définition de « Profil UML » afin de dériver d'un modèle architectural, un / des modèles reposant sur les automates temporisés ou des réseaux de files d'attente afin de vérification de propriétés de performances d'une implémentation (Cavaliere *et al.*, 2001 ; Castelpietra *et al.*, 2002)

- Spécification de « design pattern » dans le domaine de la conception d'applications temps réel (thèse en cours de Ricardo Santos Marques)
- Techniques de placement / ordonnancement et d'analyse d'ordonnançabilité dans le contexte des applications distribuées à contraintes de temps strictes ou faibles et à garanties déterministes et / ou stochastiques (Santos Marques, 2003 ; Navet and Song, 2003 ; Gaujal *et al.*, 2003 ; Poggi *et al.*, 2003).

Le projet TRISKELL de l'IRISA a pour objectif général la construction fiable et économiquement efficace d'applications par assemblage de composants logiciels, en particulier dans le domaine des systèmes répartis et réactifs ayant des temps de réponse statistiquement contraints (« temps réel mou »). Il apportera ses compétences dans la construction des modèles, des outils et des bibliothèques de composants spécifiques pour l'assemblage de composants pouvant provenir de sources tierces et ce, sous une garantie de fiabilité. Il s'agit notamment d'étudier des modèles permettant la spécification de propriétés à la fois fonctionnelles et non-fonctionnelles de composants devant être déployés sur des systèmes répartis, et de bâtir un continuum d'outils tirant partie de ces éléments de spécification, allant de vérificateurs hors-ligne à des moniteurs supervisant en ligne le comportement des composants d'une application répartie (Cariou *et al.*, 2002 ; Nebut *et al.*, 2002, Manjarrés *et al.*, 2002, Jézéquel, 2003).

▪ **IRCCyN (UMR CNRS 6597) – Equipe « Système Temps Réel »**  
*Anne-Marie Deplanche, ([Anne-Marie.Deplanche@irccyn.ec-nantes.fr](mailto:Anne-Marie.Deplanche@irccyn.ec-nantes.fr))*

De par ses travaux antérieurs, l'équipe « Système Temps Réel »<sup>1</sup> a acquis des compétences dans les domaines suivants :

- ADL temps réel, description d'architectures logicielles : ce domaine a été abordé aussi bien dans le cadre académique que dans le cadre contractuel. Dans le cadre académique, le projet REACT et l'ADL CLARA ont fait l'objet de deux thèses, l'une portant sur la définition du langage et la vérification des architectures opérationnelles sous l'hypothèse d'architecture matérielle à ressources infinies (Durand, 1998), l'autre sur la définition et la réalisation d'un support d'exécution distribuée pour CLARA et la construction de simulateur pour les architectures opérationnelles résultantes (Faucou, 2002).
- Validation d'architecture opérationnelle (AO) de systèmes temps réel distribués : il s'agit ici principalement de travaux réalisés dans le cadre académiques. Les techniques abordées sont principalement : la simulation de haut niveau d'AO (Faucou, 2002), la simulation fine d'AO (Briday, 2003), le calcul de placement (Beauvais, 2006) et l'analyse d'ordonnançabilité (Hladik, 2002).

▪ **LAMSADE (UMR CNRS 7024) – LERI/RESYCOM**  
*Patrice Moreaux ([patrice.moreaux@univ-reims.fr](mailto:patrice.moreaux@univ-reims.fr))*

La contribution des laboratoires LAMSADE et LERI/RESYCOM se situe à deux niveaux :

- D'une part, ces laboratoires travaillent sur la synthèse de composants capables d'interagir avec des services en supposant seulement connue leur spécification externe. Cette interaction suppose à la fois le respect des contraintes temporelles imposées par le service et aussi la prise en compte de l'indéterminisme du service dû à son activité

interne. Des algorithmes de synthèse ont déjà été élaborés (basés sur le modèle des automates temporisés) et une plate-forme d'exécution de services Web est en cours de réalisation (Donatelli *et al.*, 2003 ; Haddad and Melliti, 2003).

- D'autre part sur des composants à contraintes temporelles, ils développent des algorithmes de génération et d'exécution de tests. Les modèles utilisés sont SDL et RT-LOTOS d'une part et les automates temporisés et les graphes des régions d'autre part. Ces algorithmes sont implantés dans un outil expérimental. Le test des systèmes embarqués est également en cours (Fouchal, 2003 ; Rollet and Fouchal, 2003).

## 3.2. Autres partenaires

### ▪ CEA – Laboratoire LSP

Sébastien Gérard ([GERARD@ortolan.cea.fr](mailto:GERARD@ortolan.cea.fr))

Le Laboratoire Logiciels pour la Sécurité des Procédés (L-LSP) réalise ses travaux dans le cadre du programme « Systèmes embarqués » du CEA-LIST. Il a ainsi élaboré de nouvelles méthodes et outils de développement des systèmes embarqués via des projets de recherche comme AIT-WOODDES (projet européen, IST du 5<sup>ème</sup> PCRD), ACOTRIS (projet RNTL'2000) et CLIPS (projet RNTL'2002 sur les composants). Ces projets ont, notamment permis le développement et l'évaluation d'une offre méthodologique UML et orienté composant pour le domaine du temps réel (environnement ACCORD/UML du CEA étendant l'AGL généraliste Objecteering) (Guelfi *et al.*, 2003 ; Tessier *et al.*, 2003 ; Gérard *et al.*, 2002a ; Gérard *et al.*, 2002b)). Deux thèses sont d'ailleurs en cours pour enrichir la dimension composant de ACCORD/UML d'une part vis-à-vis du domaine embarqué, et d'autre part par rapport à la problématique des familles de produits. Le L-LSP est également partenaire du projet européen démarré en avril 2002 : ARTIST (Advanced Real Time in IST) (Brinksma *et al.*, 2003). Ce projet de type « mesure d'accompagnement » regroupe en réseau des laboratoires européens de pointe sur les problématiques des « composants », du « temps réel dur » et des « infrastructures de mise en oeuvre » dans le but d'identifier les concepts clés pour les systèmes temps réel à venir.

## 4. Références

- Binns P. and S. Vestal., (2001), Formalizing software architecture for embedded systems, Proceedings of EMSOFT'01, volume 2211 de LNCS, Springer.
- Duran-Limon H. and G. Blair, (2000), Specifying Real-Time Behaviour in Distributed Software Architecture, in Proceedings of 3th Australasian Workshop on Software and Systems Architectures, 2000.
- Kopetz. H., (2002), On the Specification of Linking Interfaces in Distributed Real-Time Systems., Rapport de recherche n° 8/2002, Université Technique de Vienne.
- Medvidovic N. and R. Taylor, (2000), A Classification and Comparison Framework for Software Architecture Description Languages, IEEE Transactions on Software Engineering, 26(1).
- Vestal S., (1995), MetaH Reference Manual, Technical Report, Honeywell Technology Center.

### *Références des équipes partenaires*

- André C and Rigault J-P., (2002), *Variations on the Semantics of Graphical Models for Reactive Systems*, System Man and Cybernetics (SMC'02), October, 2002, Hammamet (TN), in Proceedings (CD-ROM), IEEE Press, ISBN: 2-9512309-4-x, Index TA2L2.

- André C, (2003), *Computing SyncCharts Reactions*, SLAP'03 (Synchronous Languages, Applications and Programming), July 1st, 2003, Porto (P)
- André C, Péraldi-Frati M-A, Rigault J-P.,(2002), *Integrating the Synchronous Paradigm into UML: Application to Control-Dominated Systems*, UML 2002,October, 2002, Dresden (D), in Proceedings, Springer-Verlag, pp 438-444.
- Babau J-P., (2000), *Object Oriented Design for Real-Time Systems-Response to C. E. Pereira's Contribution*. Real-Time System (1): 95-99 (2000)
- Beauvais. J.-P., (1996), *Etude d'algorithmes de placement de tâches temps réel périodiques complexes dans un système réparti* ». Thèse de doctorat de l'Ecole Centrale de Nantes et de l'Université de Nantes.
- Berthomieu B., Ribet P.O, Vernadat F., Bernartt JL, Farines J.M, Bodeveix J.P., Filali M., Padiou G., Farail P., Gauffillet P., Dissaux P., Lambert J.L., (2002), *Towards the verification of real-time systems in avionics: the Cotre approach*, 8th International Workshop on Formal Methods for Industrial Critical Systems
- Berthomieu B., Vernadat F., (2003) *State class constructions for branching analysis of Time Petri nets 9th International Conference on Tools and Algorithms for the Construction and Analysis of Systems TACAS'2003*, Varsovie (Pologne), 7-11 Avril 2003
- Briday M., Bechenec J.-L., Trinquet Y., (2003),. *Modelisation of a distributed hardware system for accurate simulation of real-time applications*, *Proceedings of 5th IFAC International Conference on Fieldbus Systems and their Applications (FeT'03)*.
- Brinksma E., G. Coulson, I. Crnkovic, A. Evans, S. Gérard, S. Graf, H. Hermanns, B. Jonsson, A. Ravn, P. Schnoebelen, F. Terrier, A. Votintseva, and J.-M. Jézéquel, (2003), *ARTIST Roadmap: Component-based Design and Integration Platforms*, ARTiST (Project IST-2001-34820): Roadmap. 2003. p. 78, <http://www.artist-embedded.org/Roadmaps/A2-roadmap.pdf>
- Cariou E., Beugnard A., and Jézéquel J-M., (2002), *An architecture and a process for implementing distributed collaborations*, In *Proceedings of EDOC 2002*, Lausanne, Switzerland, September 2002.
- Castel Pietra, P., Y.-Q. Song,, F. Simonot-Lion, and M Attia., (2002), *Analysis and simulation methods for performance evaluation of a multiple networked embedded architecture*, IEEE Transactions on Industrial Electronics, 49-6, pp. 1251-1264.
- Cavaliere D., Simonot-Lion F., Song Y.-Q., and Hembert O., (2001), *A Component Model Approach for Modelling and Validation of an Automated Manufacturing System*, in Actes de 8th IEEE International Conference on Emerging Technologies and Factory Automation, Antibes - Juan les Pins.
- Donatelli S., S. Haddad, P. Moreaux, M. Sene, (1999), *Bounds for rewards of systems with client/server interaction*, 3rd International Meeting on the Numerical Solution of Markov Chain. Zaragoza, Spain September 1999.
- Durand. E., (1998), *Description et vérification d'architecture d'application temps réel : CLARA et les réseaux de Petri temporel*, Thèse de doctorat de l'Ecole Centrale de Nantes et de l'Université de Nantes.
- Elloy J.-P. and Simonot-Lion F., (2002), *An Architecture description language for in-vehicule embedded system development*, in Proceedings of IFAC 15th World Congress B'02.
- Farinas J.M., Berthomieu B., Bodeveix J.P., Farail P., Filali M., Gauffillet P., Hafidi H., Lambert J.L., Michel P., Vernadat F., (2002), *The COTRE project: rigorous software development for real time systems in avionics*, 27th IFAC/IFIP/IEEE Workshop on Real Time programming
- Faucou S, (2003), *Description et Construction d'Architectures Opérationnelles Validées Temporellement*, Thèse de doctorat de l'Université de Nantes.
- Fouchal H., (2003), *Conformance Testing Techniques for Timed Systems (invited talk)*, 29th International Software SEMinar (SOFTSEM'02), (Praha, Tcheck Republic),November 24-29, 2002, LNCS 2450, pp. : 1-18.
- Gaujál B. and Navet, N. and Migge, J. (2001), *Dual-Priority versus Background Scheduling: a Path-wise Comparison*, in Real-Time Systems, Kluwer Academic Publishers, vol. 25, n°1, pp39-66, 2003.
- Gérard S., E. Pelachi, P. Petterson, and B. Josko, "Methodology for developing real time embedded systems", CEE: Pub, D3/CEA/WP1.3/V1.0. 2002. p. 158.
- Gérard S., F. Terrier, and Y. Tanguy, (2002), *Using the Model Paradigm for Real-Time Systems Development: ACCORD/UML*, in OOIS'02-MDSD. 2002. Montpellier: Springer.
- Guelfi N., A. Schoos, S. Gérard, and F. Terrier, (2003), *EUDEMES:Component-Based Development Methods for Small-Size Embedded Systems*, ERCIM NEWS, 2003. vol. 52 (Embedded Systems): p. 64.
- Haddad S., T. Melliti, (2003), *Synthesis of agent for web services interaction*, en phase de soumission

- Hladik P.-E. and Déplanche A.-M., (2003), *An extension of holistic schedulability analysis for precedence relations in multiprocessor systems*, *Proceedings of 15<sup>th</sup> Euromicro Conference on Real-Time Systems – Work In Progress (ECRTS'03)*.
- Jézéquel J.-M., (2003), *Model-driven engineering with contracts, patterns, and aspects*, In Tutorial Program of AOSD 2003: 2nd International Conference on Aspect-Oriented Software Development. ACM-IEEE, March 2003.
- Mallet F., Boeri F., (2001), *Architectures validation in an object-oriented framework*, 15 th European Simulation MultiConference, République Tchèque, pp. 139-145.
- Manjarrés A., S. Pickin, G. Sunyé, D. Pollet, and J.-M. Jézéquel, (2002), *Oo analysis patterns as UML metalevel collaborations*, In proc. of ES2002. The 22nd SGAI International Conference on Knowledge Based Systems and Applied Artificial Intelligence: Research and Development in Intelligent Systems XIX, BCS Conference Series. Springer-Verlag, decembre 2002.
- Navet N. and Song Y.-Q., (1999), *Reliability Improvement of the Dual-Priority Protocol under Unreliable Transmission*, Control Engineering Practice, Pergamon Press, vol. 7, n°8, .
- Nebut C., Pickin S., Le Traon Y., and J.-M. Jézéquel, (2002), *Reusable test requirements for UML-modeled product lines*. In *Proceedings of REPL'02 (workshop on Requirements Engineering for Product Lines)*, Essen, Germany, September 2002.
- Poggi, E. and Song, Y.-Q. and Koubaa, A. and Wang, Z., (2003), *Matrix-DBP For (m, k)-firm Real-Time Guarantee*, in Real Time and Embedded System, Paris.
- Rollet A. and H. Fouchal, (2003), *Robustness Protocol Testing*, Innovative Internet Computing Systems (I2CS'02),(Leipzig, Germany),June 18-21, 2003,
- Santos Marques R., Navet N., Simonot-Lion F., (2003), *Frame Packing under Real-Time Constraints*, Proceedings of 4th IFAC Conference FET03, (réd. Teknéa), Paris.
- Tessier P., S. Gérard, C. Mraidha, F. Terrier, and J.-M. Geib., (2003), *A Component-Based Methodology for Embedded System Prototyping*, in 14th IEEE International Workshop on Rapid System Prototyping (RSP'03). 2003. San Diego, USA: IEEE.