Proposition de recherche doctorale

Ingénierie des modèles pour la conception de plates-formes temps-réel critiques avioniques

Mots clés :

- **Directeur de thèse** : LAURENT PAUTET
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire Traitement et Communication de l'Information
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Ingénierie des modèles pour la conception de plates-formes temps-réel critiques avioniques Contexte Au niveau industriel, l'industrie avionique est passé depuis plusieurs années, avec l'avènement du programme A380 d'une architecture avionique dite fédérée c'est à dire une architecture où chaque calculateur est défini pour héberger une fonction dédiée, à une architecture avionique intégrée c'est à dire une architecture où un calculateur est capable d'héberger plusieurs fonctions. De là est né le concept de l'IMA (Integrated Modular Avionique) Ce concept d'IMA nous a permis de rationaliser l'électronique de bord en ramenant de plusieurs dizaines (environ 37) à quelques unités (7), les différents types de calculateurs embarqués nécessaires pour exécuter l'ensemble des applications nécessaires à la gestion du vol. Cette révolution, introduite avec le programme A380 côté AIRBUS ou celui du 787 côté BOEING a donné naissance a l'IMA[1] de première génération ou IMA1G et a continué avec le programme A350 dans lequel ces 7 types de calculateurs différents ont en fait été ramenés à 2, cette évolution étant toujours basé sur le concept d'IMA1G. Cette évolution entre ces deux générations d'avion s'est également faite en ajoutant entre les calculateurs et les senseurs ou actuateurs des interfaces de regroupement appelées RDC pour Remote Data Concentrateur. Cette évolution va continuer pour s'orienter vers une architecture de l'avionique de calcul centrée réseau en passant par une étape intermédiaire appelée IMA2G permettant d'introduire de nouveaux concepts d'architecture avionique. THALES estime que ces évolutions d'architecture ne peuvent se faire que si elles sont accompagnées par un processus outillé permettant à l'utilisateur de disposer des outils nécessaires à la prédiction des performances. Télécom ParisTech consacre plusieurs thèses sur le domaine des systèmes partitionnés s'appuyant sur l'IMA [6]. Notamment, Télécom ParisTech est responsable de la rédaction de l'annexe ARINC653 pour le langage AADL auprès du comité de standardisation. Définir une méthode dirigée par les modèles permettant de produire l'architecture matérielle nécessaire à la bonne exécution d'un système logiciel IMA donné constitue à ses yeux une avancée scientifique tout à fait intéressante. Cette prédiction est critique durant les phases projets car elle va permettre le dimensionnement de l'avionique calculateur qui devra être embarquée afin de répondre aux exigences applicatives. Problématique Il existe actuellement des outils tels que ORCHESTRA ou ADVANCE VITAL permettant, à partir d'exigences client, de réaliser des modélisations fonctionnelles de ces dites exigences. Cette modélisation permet de vérifier que la compréhension d'un sujet, et donc des besoins opéra- tionnels, est bien partagée entre le donneur d'ordre et la ou les personne(s) en charge de la réponse à cet appel d'offre. Il existe également des outils dits « d'early validation » du logiciel permettant de réaliser des pré-validations sur des simulateurs de processeurs (tels que les outils proposés par VIRTUTECH [2]). Ces outils ont comme inconvénients, premièrement de ne pas être temps réel, deuxièmement de ne couvrir que l'aspect calcul et troisièmement de ne pas permettre l'évaluation des performances requises au niveau des calculateurs. Le domaine d'excellence de THALES est la conception de plates-formes de calcul. Ces platesformes sont généralement à concevoir tant sur l'aspect matériel que logiciel. Elles sont interconnectées et doivent répondre à des critères permettant de les « standardiser » afin de réduire leur type de façon très significative. L'évolution proposée à travers la troisième génération de l'IMA consiste à étendre ce concept à des domaines non encore couverts par ce concept tels que les commandes de vol, les commandes moteur, la gestion cabine, etc. Le domaine que doit couvrir l'IMA s'élargit et les applications à embarquer sont de plus en plus consommatrices de ressources tant calcul que mémoires ou réseau, Les délais de mise à disposition des équipements sont raccourcis et les « donneurs d'ordres » demandent à disposer d'une plus grande maturité des équipements dès la phase dite EIS ou entrée en service (Enter Into Service). L'ensemble des ces éléments conduit THALES de façon naturelle à analyser comment couvrir le domaine de « l'early validation » au niveau architecture matérielle. Ce domaine de recherche, non couvert au niveau outil et peu couvert actuellement par la littérature scientifique, doit nous permettre de disposer d'une base de modèles permettant, une fois l'architecture élaborée, d'une part de vérifier la « compliance » de la réponse par rapport aux exigences dès les phases les plus amonts de l'étude et d'autre part de nous engager sur les performances de la plate-forme de calcul dès les phases d'appel d'offre. De plus, nous devons considérer que les exigences clients ne sont pas des données immuables, elles évoluent au cours de la vie d'un programme et parfois de manière très significative. Il nous faut donc pouvoir, par la modélisation réalisée, valider que l'évolution demandée n'a pas d'impact sur l'architecture retenue et sur ses performances ou de savoir les quantifier afin de déterminer les évolutions à apporter à cette architecture et les impacts en terme de coûts et de délais de mise en œuvre. On peut noter que le processus de description pourra s'enrichir de techniques de prototypage et de raffinement afin de suivre au mieux les évolutions des exigences. Ces approches connaissent un essor tout à fait conséquent comme le montrent les publications dans des conférences commes Rapid System Prototyping auxquelles Télécom ParisTech contribue [7]. Sujet de Thèse Comme indiqué précédemment, que cela soit au niveau du contexte ou au niveau de la problématique, THALES doit faire face à l'évolution de plusieurs critères de façon simultanée : • Le domaine couvert par l'IMA s'est accru et continue de s'accroître • Les performances demandées sont de plus en plus contraignantes o Plus de puissance de calcul demandée o Plus de fonctions hébergées o Plus de mémoire consommée o Plus de

bande passante utilisée o Maîtrise plus fine des latences o Maîtrise plus fine des WCET (Worst case Execution Time) L'ensemble de ces contraintes lié au fait que les outils ou langages disponibles ne nous permettent pas à ce jour de disposer de représentation – tant sur l'aspect logiciel que matériel – d'une plate-forme complexe, nous amène à étudier comment modéliser les composants, bases des architectures : processeur, mémoire, bus, transaction et comment créer un simulateur permettant d'associer l'ensemble de ces modèles pour créer une architecture de traitement. Le sujet proposé demande donc : • Pour chaque élément d'une plate-forme (processeur, mémoire, réseau, bus d'intercommunication, composant programmable, Operating Système, Middleware) de déterminer : • Les éléments dimensionnant des composants à simuler qu'il s'agisse d'un composant matériel (micro-processeur, mémoire, bus, FPGA, contrôleur, etc.) et/ou logiciel (Operating system, Driver, Services Plate-forme ou middleware). • Comment décrire, dans un langage restant à définir, l'ensemble de ces éléments de façon à pouvoir créer une base de données o Cette description doit être basée sur les paramètres dimensionnant des composants à modéliser (ex pour une mémoire : taille mémoire, temps d'accès, vitesse, latence, burst, taux d'attente lié au refresh, etc.) • De réaliser le moteur de simulation permettant d'interconnecter l'ensemble des modèles dans le but de prédire l'ensemble des performances intrinsèques de l'architecture ainsi réalisée, performances en termes de puissance de calcul, de consommation mé- moire ainsi que de débit d'entrée-sortie au niveau de l'ensemble des nœuds. Un lien étroit sera à établir avec les applicatifs à héberger afin de pouvoir extraire les paramètres clés de ces fonctions dans le but de générer les stimuli permettant d'exciter le modèle dans le but de prédire sa réponse par rapport aux exigences applicatives. Approche et Innovation L'approche envisagée consiste à s'appuyeréel embarqués afin de mieux appréhender les propriétés du domaine. Certains de ces langages en voie de définition ou de standardisation comme AADL [3] ou MARTE [4] seront considérés en premier lieu. Cette approche intéresse au plus haut point Télécom ParisTech qui dispose d'un environnement de modélisation autour d'AADL nommé ocarina (http://ocarina.enst.fr). Les études qui ont été menées portent presque uniquement sur la modélisation de composants logiciels pour une application donnée, les composants matériels étant supposés fixés lors de l'expression des besoins. Dans ce cadre, certains composants logiciels, notamment ceux liés à la plate-forme logi- cielle d'exécution sont générés automatiquement [5]. Il s'agit également de vérifier que les propriétés exigées sur les composants logiciels seront satisfaites par des techniques de modelchecking [8]. Dans le cadre de cette thèse, il s'agit d'adopter une approche duale, c'est à dire de fixer les composants logiciels. A l'aide d'un langage de description d'architecture, l'architecture matérielle sera déduite, éventuellement générée, et finalement vérifiée afin de s'assurer que les besoins exprimés au niveau des composants logiciels sont bien satisfaits. Une partie de ces vérifications pourront être menées à bien grâce aux technologies de simulation fournies par THALES. Si des recherches sont menées pour optimiser les performances des architectures matérielles (notamment pour des bancs de tests généraux), plus rares sont celles menées pour optimiser les composants matériels de manière dédiée à une application logicielle donnée. Ces approches sont également rarement le résultat d'une approche automatique fondée sur les modèles. Il faut noter que d'autres organismes s'intéressent à cette problématique. A titre d'exemple, CMU/SEI a entamé un certain nombre de travaux afin de consolider le langage AADL sur ces aspects de descriptions plus fines des composants matériels. L'Agence Spatiale Européenne a lancé des projets de recherches internes en vue de générer les composants matériels sous forme de modèles VHDL. Plus généralement, il faut noter que ces activités de recherche sont dans la lignée de projets de premier plan comme IST-ASSERT, TOPCASED, etc. Compte tenu de la forte évolution de l'IMA, décrite précédemment, ces travaux de recherche permettront de contribuer significativement à ces standards. En effet, peu nombreux sont les environnements de modélisation pour les systèmes temps réel embarqués mais encore moins nombreux sont ceux qui traitent précisément de systèmes spécifiques à l'IMA. Par ailleurs, dans une approche traditionnelle fondée sur l'Ingénierie Des Modèles, les composants logiciels sont modélisés et conçus en considérant les composants matériels comme des invariants du problème. Les composants logiciels sont raffinés, configurés et déployés afin de satisfaire les exigences exprimées. Le caractère innovant de ce travail consiste ici à considérer les composants logiciels comme invariants du problème et de raffiner les composants matériels en respectant une approche fondée sur les modèles. Dans ce travail où l'Ingénierie Des Modèles sera utilisée dans le cadre d'une approche duale de l'approche traditionnelle, le langage de modélisation devra naturellement permettre une description fine des composants matériels et de leur interaction. A ce titre de nombreuses contributions sont envisageables. En dehors de la description fine des matériels, il faudra considérer des aspects logiciels comme le noyau ou les pilotes comme part intégrante de l'architecture matérielle. Dans un premier temps, le processus sera défini, mis en œuvre et enrichi sur un certain nombre de cas d'étude industriels. Dans un second temps, il s'agira d'établir une catégorisation des ar- chitectures en fonction des exigences afin de standardiser ces solutions comme incite à le faire l'IMAG3. Cette phase de catégorisation peut également être comprise comme la définition de gabarits de conception pour les composants matériels. [1] Integrated Modular Avionic ARINC653 – ARINC600 – ARINC664 – etc. [2] VIRTUTECH – Outil SIMICS [3] SAE AS-2C Architecture Description Language Subcommittee. Architecture Analysis and Design Language (AADL) v2 - Draft v1. 6, SAE AS5506. SAE Aerospace, January 2008 [4] OMG document number: ptc/07-08-04 [5] J. Hugues, B. Zalila, L. Pautet, and F. Kordon. From the Prototype to the Final Embedded System Using the Ocarina AADL Tool Suite. ACM Transactions in Embedded Computing Systems (TECS), 7(4) :1–25, July 2008. [6] J. Delange, L. Pautet, and F. Kordon. Code Generation Strategies for Partitioned Systems. In 29th IEEE Real-Time Systems Symposium (RTSS'08), page 53_56, Barcelona, Spain, December 2008. [7] J. Hugues, B. Zalila, L. Pautet, and F. Kordon. Rapid Prototyping of Distributed Real-Time Embedded Systems Using the AADL and Ocarina. In 18th IEEE/IFIP International Workshop on Rapid System Prototyping (RSP'07), pages 106–112, Porto Allegre Brésil, May 2007. [8] J. Hugues, F. Kordon, L. Pautet, and T. Vergnaud. A Factory To Design and Build Tailorable and Verifiable Middleware. In Monterey Workshop 2005 on Networked Systems : realization of reliable systems on top of unreliable networked platforms, volume LNCS, pages 123–144, February 2007.

Résumé du projet de recherche (Langue 2)

Il existe actuellement des outils tels que ORCHESTRA ou ADVANCE VITAL permettant, à partir d'exigences client, de réaliser des modélisations fonctionnelles de ces dites exigences. Cette modélisation permet de vérifier que la compréhension d'un sujet, et donc des besoins opéra- tionnels, est bien partagée entre le donneur d'ordre et la ou les personne(s) en charge de la réponse à cet appel d'offre. Il existe également des outils dits « d'early validation » du logiciel permettant de réaliser des pré-validations sur des simulateurs de processeurs (tels que les outils proposés par VIRTUTECH [2]). Ces outils ont comme inconvénients, premièrement de ne pas être temps réel, deuxièmement de ne couvrir que l'aspect calcul et troisièmement de ne pas permettre l'évaluation des performances requises au niveau des calculateurs. Le domaine d'excellence de THALES est la conception de plates-formes de calcul. Ces platesformes sont généralement à concevoir tant sur l'aspect matériel que logiciel. Elles sont interconnectées et doivent répondre à des critères permettant de les « standardiser » afin de réduire leur type de façon très significative. L'évolution proposée à travers la troisième génération de l'IMA consiste à étendre ce concept à des domaines non encore couverts par ce concept tels que les commandes de vol, les commandes moteur, la gestion cabine, etc. Le domaine que doit couvrir l'IMA s'élargit et les applications à embarquer sont de plus en plus consommatrices de ressources tant calcul que mémoires ou réseau, Les délais de mise à disposition des équipements sont raccourcis et les « donneurs d'ordres » demandent à disposer d'une plus grande maturité des équipements dès la phase dite EIS ou entrée en service (Enter Into Service). L'ensemble des ces éléments conduit THALES de façon naturelle à analyser comment couvrir le domaine de « l'early validation » au niveau architecture matérielle. Ce domaine de recherche, non couvert au niveau outil et peu couvert actuellement par la littérature scientifique, doit nous permettre de disposer d'une base de modèles permettant, une fois l'architecture élaborée, d'une part de vérifier la « compliance » de la réponse par rapport aux exigences dès les phases les plus amonts de l'étude et d'autre part de nous engager sur les performances de la plate-forme de calcul dès les phases d'appel d'offre. De plus, nous devons considérer que les exigences clients ne sont pas des données immuables, elles évoluent au cours de la vie d'un programme et parfois de manière très significative. Il nous faut donc pouvoir, par la modélisation réalisée, valider que l'évolution demandée n'a pas d'impact sur l'architecture retenue et sur ses performances ou de savoir les quantifier afin de déterminer les évolutions à apporter à cette architecture et les impacts en terme de coûts et de délais de mise en œuvre. On peut noter que le processus de description pourra s'enrichir de techniques de prototypage et de raffinement afin de suivre au mieux les évolutions des exigences. Ces approches connaissent un essor tout à fait conséquent comme le montrent les publications dans des conférences commes Rapid System Prototyping auxquelles Télécom ParisTech contribue [7].