REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ EL-HADJ LAKHDAR – BATNA
FACULTÉ DES SCIENCES
DEPARTEMENT D'INFORMATIQUE

THESE

Présentée par

REBAIAIA Mohamed-Larbi

pour obtenir le titre de

DOCTEUR en Sciences

Spécialité

INFORMATIQUE

Sujet de la thèse :

Spécification et Vérification des Systèmes Critiques :

Extension de l'Environnement VALID pour la Prise en Charge du Temps Réel

---

Soutenue publiquement le 16 février 2011 devant le jury composé de :

M. Noureddine BOUGHECHEL	Professeur	Président
M. Mohamed BENMOHAMED	Professeur	Directeur de Thèse
M. Djamel-Eddine SAIDOUNI	Professeur	Examinateur
M. Allaoua CHAOUI	Maître de conférences	Examinateur
M. Azzedine BILAMI	Maître de conférences	Examinateur
M. Brahim BELATAR	Maître de conférences	Examinateur

SOMMAIRE

CHAPITRE 5 : THEORIE DU MODEL-CHECKING

CHAPITRE 6 : LA LOGIQUE DE REECRITURE, MAUDE ET FULL-MAUDE

CHAPITRE 7 : SPECIFICATION DES SYSTEMES TEMPS REEL DANS LE CADRE DE LA LOGIQUE DE REECRITURE

CHAPITRE 8 : PROPOSITION D'UN ENVIRONNEMENT POUR LA MODELISATION DES SYSTEMES REACTIFS

CHAPITRE 9 : IMPLANTATION

Résumé : *La technologie des systèmes mixtes matériels et logiciels connaît de nos jours une révolution sans pareille dans tous les domaines technologiques. Le fait de mélanger matériel et logiciel, ceci a donné naissance à des systèmes très complexes. La conception de tels systèmes, nécessite l'intervention de ressources humaine, financière et technologique très importante. Pour veiller au bon fonctionnement de leurs conceptions, ces systèmes doivent être soumis à des processus de validation très rigoureux. Une telle tâche n'est point évidente vue l'accroissement rapide de la complexité et de l'hétérogénéité des nouvelles architectures (matériel/logiciel). Aussi correcte que possible, la conception doit tenir compte de certaines propriétés dites critiques, qui sans leur présence risque d'engendrer une situation de catastrophe et même de ternir l'image de la compagnie.*

Dans ce travail, nous nous sommes intéressées à la mise en place d'un environnement intégré pour le développement des systèmes réactifs temps-réel. A cet effet, nous avons proposé plusieurs solutions pour la modélisation, la spécification et la vérification de plateformes matériel/logiciel. Dans un premier temps, nous avons utilisé une technique simple et efficace pour implémenter les diagrammes de décision binaire utilisés pour la représentation et la vérification des réseaux booléens symbolisant les systèmes réactifs. Nous avons ensuite, montré que l'axiomatisation des logiques temporelles linéaire LTL et arborescente CTL, permet de cerner de peu le problème de la complexité combinatoire spacio-temporelle. Les automates temporisés et la logique TCTL ont permis de mettre en place un modèle très utile pour la spécification et la vérification des systèmes temps-réels.
En se basant d'un coté sur la logique de réécriture comme modèle de spécification algébrique et philosophie universelle de raisonnement formel, et du système Maude comme outil de programmation et d'exécution de ces spécifications, nous avons intégré le tout en tant que noyau de programmation de l'environnement en question et sur lequel un ensemble de modules intégrés et spécialisés sont venus se greffer. Nous avons d'autant plus compris durant cette recherche, que la description UML et son extension UML/OCL et UML-RT, constituent pour le moment les meilleurs moyens pour la modélisation "semi-formelle" des systèmes réactifs temps-réel. Finalement, nous avons montré l'aisance même de l'utilisation de cet environnement à travers plusieurs exemples et benchmarks connus.

Mots-clés : *Spécification, Vérification, ROBDD, Logique de Réécriture, Maude, UML/OCL, UML-RT, Méthodes Formelles, Systèmes Réactifs Temps-réel.*

Abstract : *With the increasing emergence of hardware/software distributed systems, designers need in some ways efficient methods and tools to improve the safeness of such systems and to reduce drastically their design engineering time. In general, some traditional methods as simulation and testing are used to detect errors and bugs, but they are inadequate to certify the correctness of complex systems. To accelerate the design and to avoid distributed systems malfunctions, new mathematical-based techniques have been used to improve the deficiency of the old methods. During the last two decades, Model-checking and theorems proving have been the major research verification fields intensively used to check the design correctness of some big projects (NASA lance rockets, Pentium chips, etc.) In fact, despite the generalization of formal methods, some problems remain in suspense in producing coherent specification fully integrated semantics and avoiding the size complexity of designs.*

In this Thesis, we present a hierarchical approach and an open environment to describe and to verify distributed and concurrent systems. The system currently uses UML and extension UML/OCL and UML-RT notations and provides rewriting logic, model checking, theorem proving, and simulation techniques. The Model checking algorithm developed in this research work is based on the axiomatization of LTL linear temporal model and tree temporal logic CTL. We have used temporal automata and TCTL to describe formal behavioral description and to verify timed-based properties. Our experience has shown that combining Temporal Logics and a theoretical well based techniques as the Rewriting logic embodied in the core of the fastest formal system (Maude), can improve the verification of the correctness of large circuits and critical software, and can decrease the time-consuming to perform a solution. Such good solutions are obtained due to the strategy rules incorporated in Maude system which are based on the recent theoretic researches by the rewriting community. When one would like to analyze the results depicted in the benchmark experiments results, he will be surprised because due to the execution CPU time which is, in general insignificant comparing with other verification commercial tools.

Keywords : *Specification, Verification, ROBDD, Rewriting Logic, Maude Language, UML/OCL, UML-RT, Formal Methods, Reactive Real-Time Systems.*