NOM – Prénom : HAUR IMANE

TITRE DE LA THESE

AUTOSAR compliant multi-core RTOS formal modeling and verification

Résumé

De graves incidents peuvent se produire si des erreurs sont présentes dans un système logiciel temps réel. Il est donc impératif de développer un système informatique exempt d'erreurs. Les tests sont une méthode standard pour identifier les erreurs dans les programmes logiciels. Ils sont largement utilisés dans la pratique, bien qu'il soit clairement impossible de les utiliser dans des systèmes hautement critiques où les résultats des tests pourraient causer des dommages si des erreurs sont connues avant le déploiement réel. Une autre solution consiste à simuler le comportement du système sur un ordinateur. La simulation ne fonctionne pas sur le système temps réel, mais sur son modèle. Le modèle est une représentation abstraite du système, généralement conçue en utilisant les mathématiques ou la logique. Les tests et la simulation sont tous les deux largement utilisés dans les applications industrielles et leur utilisation s'est avérée très utile. Cependant, comme il s'agit de méthodes non exhaustives, elles ne garantissent pas l'élimination de toutes les erreurs. Il n'est donc généralement pas possible de simuler ou de tester tous les scénarios ou comportements possibles d'un système donné. La vérification formelle est une solution pour augmenter la fiabilité de l'implémentation du système. Elle représente le terme général pour un ensemble de techniques qui utilisent l'analyse statique basée sur des modèles mathématiques pour vérifier l'exactitude du comportement du matériel ou du logiciel. C'est une technique qui a été recommandée comme méthode de vérification de la sûreté dans plusieurs normes industrielles, telles que la norme ISO-26262 pour l'industrie automobile.

Dans notre travail de thèse, nous nous intéressons à l'utilisation des méthodes formelles dans le processus de vérification de la sûreté opérationnelle et de la conformité aux standards des systèmes d'exploitation multicœurs temps réel (RTOS). Nous proposons une approche de *model-checking*, que nous conduisons sur le système d'exploitation temps réel Trampoline, conforme aux standards OSEK/VDX et AUTOSAR. Pour cela, nous utilisons le modèle de réseau de Petri temporel à états finis. Puisque le contrôle des systèmes temps réel multicœurs nécessite souvent un accès simultané en vrai parallélisme aux ressources partagées et que les réseaux de Petri temporels ne capturent pas directement ces caractéristiques, nous proposons d'étendre le formalisme avec des transitions colorées et des fonctionnalités de haut niveau, c'est-à-dire une syntaxe prédéfinie manipulant différents types d'expressions composées de variables. Nous utilisons ce formalisme étendu pour modéliser le RTOS multicœur qui reproduit le flux de contrôle et utilise les mêmes variables que l'implémentation. Cette approche a permis de vérifier la conformité du RTOS multicœur avec le standard Autosar, l'ordonnançabilité d'un système temps réel ainsi que les mécanismes de synchronisation : accès concurrents aux structures de données du système d'exploitation, ordonnancement multicœur et traitement des interruptions inter-cœur. Cela a permis l'identification automatique de deux erreurs possibles dans l'exécution concurrente, montrant une protection insuffisante des données et une synchronisation défectueuse. Les deux erreurs ont été corrigées et la conformité du modèle mis à jour a été vérifiée.

Mots-clés : Formal verification, Model-checking, High-level Colored Time Petri Nets, Real-time operating systems, Multi-core execution, AUTOSAR OS verification