

Titre de la thèse : Évaluation de la fiabilité des systèmes embarqués dès la phase de conception par réseaux de Petri temporels étendus.

Résumé :

Le travail de cette thèse porte sur l'évaluation des performances en termes FMDS des systèmes dynamiques. Nous nous intéressons plus particulièrement à l'évaluation de la fiabilité des systèmes embarqués temps réel à cause de leur criticité qui nécessite de garantir un niveau de fiabilité convenable. Une étude de sûreté de fonctionnement doit donc être menée au plus tôt dans le cycle de développement de ces systèmes avant que les choix de conception ne soient figés. Au plus tôt nous détectons une erreur de conception, au plus tôt elle sera corrigée et moins coûteuse sera cette correction. Par conséquent, cette étude doit être effectuée à partir de l'analyse des modèles des systèmes embarqués en cours de conception afin de diminuer le nombre de prototypes nécessaires à la validation des systèmes conçus.

Un moyen d'évaluer la sûreté de fonctionnement des systèmes embarqués est la recherche des scénarios redoutés menant à un état dangereux afin de comprendre les raisons de la dérive qui peut avoir des conséquences dramatiques pour le système et l'utilisateur. L'approche que nous proposons est basée tout d'abord sur une analyse qualitative permettant la mise en évidence des comportements en présence de défaillances pour obtenir un modèle dysfonctionnel du système, vient, ensuite, l'analyse quantitative pour l'évaluation des performances en termes de fiabilité. Ces performances, permettent aux concepteurs d'évaluer, d'optimiser et de garantir son maintien en bon fonctionnement tout au long de son cycle de vie.

La méthode proposée est une solution au problème de la fiabilité dynamique des systèmes embarqués interruptibles, pour une prise en compte de manière efficace et réaliste des contraintes de fonctionnement en temps réel auxquelles ces systèmes sont soumis, les scénarios sont générés à partir d'une modélisation orientée-objets du système en réseaux de Petri à chronomètres qui permettent de modéliser la suspension et la reprise des tâches et offrent une configuration plus détaillée du système conçu et de nouvelles interactions entre les différents composants du système qui décrivent d'autres comportements dangereux. En évitant l'exploration du système complet, une simulation hybride des dynamiques discrète et continue est effectuée sur l'ensemble des événements menant vers l'état critique ; La dynamique continue du système est couplée à la dynamique discrète représentée par un algorithme de génération de scénarios à partir des réseaux de Petri à chronomètres orientés objets.

Mots clés :

Systèmes embarqués, Fiabilité, Scénarios redoutés, Contraintes temporelles, Réseaux de Petri à chronomètres.