

Vérification de flot de contrôle sur un processeur NIOS II

Résumé :

Les technologies récentes devenant de plus en plus sensibles aux fautes transitoires induites par des événements naturels, il est devenu fondamental de prendre en compte la robustesse parmi les contraintes de conception d'un système embarqué, pour de très nombreux domaines d'application. Par ailleurs, les erreurs sont de plus en plus souvent multiples, ce qui augmente l'intérêt pour l'utilisation de méthodes de vérification fonctionnelles comme la vérification du flot de contrôle (CFC) dans le cas d'un système à base de microprocesseur. L'objectif du travail est l'analyse de faisabilité d'une approche de CFC dans le cas d'un processeur configurable propriétaire (soft core NIOS II de Altera), l'adaptation d'un coprocesseur de surveillance existant et le développement d'un démonstrateur sur la base d'une étude de cas définie par Airbus.

Description :

De nombreuses applications imposent des contraintes de sûreté pouvant être assez strictes (par exemple, dans le domaine automobile ou transports en général). Les technologies récentes devenant de plus en plus sensibles aux fautes transitoires induites par des événements naturels, des protections doivent être implantées dans les circuits pour garantir le niveau requis de sûreté. Ces protections peuvent être basées sur du matériel, sur du logiciel ou sur une collaboration entre matériel et logiciel. Les erreurs observées étant de plus en plus souvent des erreurs multiples, les protections classiques à base de codes détecteurs deviennent soit inefficaces, soit trop coûteuses. D'autres approches peuvent être envisagées, cherchant à vérifier des propriétés fonctionnelles du système. L'approche considérée sera une technique de vérification de flot de contrôle (CFC), appliquée à un système intégré à base de microprocesseur. La vérification est réalisée par un coprocesseur de surveillance ("watchdog"), exécutant un logiciel dérivé du logiciel d'application exécuté par le processeur principal. Cette approche est actuellement implantée pour un processeur dont les sources sont disponibles (Sparc v8).

Le travail consistera tout d'abord à analyser les contraintes à prendre en compte pour utiliser une approche similaire avec un système construit autour d'un processeur configurable propriétaire dont les sources ne sont pas disponibles (le soft core NIOS II sur technologie Altera), puis à proposer une implantation de la vérification en tenant compte des caractéristiques architecturales de ce processeur.

Les principales étapes du travail seront :

- étude de la méthode de CFC choisie
- analyse des caractéristiques du processeur NIOS II, dans l'optique de l'implantation de la surveillance (identification des contraintes et limitations)
- adaptation du coprocesseur de surveillance existant pour le processeur Sparc v8
- implantation et validation fonctionnelle d'un démonstrateur, en lien avec une étude de cas définie par Airbus
- évaluation des caractéristiques en termes de coût matériel, performances et robustesse

Rémunération : de l'ordre de 1300 €par mois.

Contact :

Régis LEVEUGLE

TIMA

46 av. Félix Viallet

38031 Grenoble Cedex

e-mail : Regis.Leveugle@imag.fr

Tél : 04.76.57.46.86 Fax : 04.76.57.49.81

Analyse de durées de vie dans des circuits numériques

Résumé :

De nombreuses applications imposent des contraintes de sûreté (par exemple, dans les domaines automobile ou aéronautique) et/ou des contraintes de sécurité (par exemple, dans le domaine des cartes à puces). Par ailleurs, les risques d'erreurs liées à des perturbations transitoires augmentant, il est devenu fondamental de prendre en compte la robustesse parmi les contraintes de conception d'un système embarqué, même pour des applications jugées peu critiques. La durée de vie des informations mémorisées dans les registres d'un circuit influe directement sur la probabilité qu'une perturbation transitoire puisse entraîner une défaillance de l'application. L'objectif du travail est de proposer et de mettre en place une approche permettant d'évaluer ces durées de vie dans un circuit numérique spécifié au niveau RTL.

Description :

Les technologies récentes devenant de plus en plus sensibles aux fautes transitoires induites par des événements naturels, il est devenu fondamental de prendre en compte la robustesse parmi les contraintes de conception d'un système embarqué, même pour des applications jugées peu critiques. Naturellement, cette prise en compte est encore plus importante dans les domaines critiques, que ce soit pour la sûreté (par exemple, dans les domaines automobile ou transport en général) ou la sécurité (par exemple, dans le domaine des cartes à puces).

Le risque de dysfonctionnement en cas de perturbation dépend fortement de l'utilisation des registres internes d'un circuit par l'application considérée. Le risque est d'autant plus fort que la durée pendant laquelle une information peut être réutilisée (ou "durée de vie") est longue.

L'objectif du travail est de proposer et de mettre en place une approche permettant d'évaluer ces durées de vie dans un circuit numérique spécifié au niveau RTL. Cette approche sera en partie fondée sur des simulations du système, complétées par une analyse des instants de lecture et d'écriture des différents registres.

Les principales étapes du travail seront :

- étude du contexte et des approches existant pour l'analyse de durées de vie
- proposition d'une approche permettant de réaliser l'analyse des durées de vie dans les bascules internes d'un circuit numérique
- automatisation de l'approche sur la base de simulations par ModelSim
- expérimentation sur des exemples de circuits (plusieurs versions d'un multiplieur séquentiel, filtre FIR, cryptoprocèsseur AES) et analyse des limitations

Rémunération : de l'ordre de 1300 €par mois.

Contact :

Régis LEVEUGLE

TIMA

46 av. Félix Viallet

38031 Grenoble Cedex

e-mail : Regis.Leveugle@imag.fr

Tél : 04.76.57.46.86 Fax : 04.76.57.49.81

Analyse de criticité des registres dans un microprocesseur Sparc

Résumé :

De nombreuses applications imposent des contraintes de sûreté (par exemple, dans les domaines automobile ou aéronautique) et/ou des contraintes de sécurité (par exemple, dans le domaine des cartes à puces) qui nécessitent d'implanter des protections contre les effets de perturbations transitoires. Pour optimiser ces protections, il est nécessaire d'évaluer précisément les conséquences des erreurs potentielles et d'identifier les éléments les plus critiques. Dans le cas d'un système à base de microprocesseur, il s'agit d'évaluer précisément la criticité des différents registres en fonction des informations qu'ils contiennent pendant l'exécution de l'application. Ceci est compliqué, dans le cas de processeurs récents, par les nombreux registres internes implantés dans les pipelines. L'objectif du travail est de pouvoir modéliser l'effet de telles architectures afin de raffiner les évaluations de criticité des registres.

Description :

De nombreuses applications imposent des contraintes de sûreté pouvant être assez strictes (par exemple, dans les domaines automobile ou aéronautique), qui nécessitent d'implanter des protections contre les effets de fautes transitoires induites par des événements naturels. Dans d'autres applications, par exemple dans le domaine des cartes à puces, les contraintes de sécurité (au sens confidentialité) peuvent nécessiter le même type de protections pour lutter contre des attaques volontaires visant à obtenir un accès non autorisé à des informations ou à des services. Dans les deux cas, les protections implantées doivent être optimisées de façon à réduire les coûts en matériel et en performances. Pour cela, il est nécessaire d'évaluer précisément les conséquences des erreurs potentielles et d'identifier les éléments les plus critiques.

Dans le cas d'une fonction implantée de manière logicielle et exécutée par un microprocesseur, le risque de dysfonctionnement en cas de perturbation dépend fortement de l'utilisation des registres internes par l'application considérée. Les évaluations classiques ne tiennent compte que des registres visibles par l'utilisateur. Toutefois, dans les processeurs récents, de nombreux registres internes existent (registres de pipeline de la micro-architecture). L'objectif de cette étude est d'améliorer l'analyse prédictive de criticité en tenant compte précisément des transferts d'informations dans l'ensemble des registres internes. L'étude de cas portera sur le pipeline de calcul entier du processeur Leon3 (Sparc v8), disponible sous la forme d'un modèle VHDL synthétisable.

Les principales étapes du travail seront :

- analyse de l'architecture du processeur Leon3 et des travaux antérieurs menés sur le sujet, incluant un premier algorithme de modélisation des transferts de données internes tenant compte des chemins d'anticipation dans le pipeline.
- étude des résultats d'injection de fautes existant ; réalisation d'injections complémentaires (par simulation RTL ou émulation) pour identifier les sources d'imprécision de l'analyse.
- proposition de modifications dans l'algorithme de prédiction de criticité, implantation de ces modifications, et validation
- synthèse sur l'efficacité de l'analyse prédictive et comparaison avec les méthodes antérieures.

Rémunération : de l'ordre de 1300 €par mois.

Contact :

Régis LEVEUGLE

TIMA

46 av. Félix Viallet

38031 Grenoble Cedex

e-mail : Regis.Leveugle@imag.fr

Tél : 04.76.57.46.86 Fax : 04.76.57.49.81