Méthodologie pour l'intégration d'IP de réseaux de neurones dans une puce avec une assurance de sureté

Soutenance de thèse – GUINEBERT Iban

2 décembre 2024 à 10h00

Salle des thèses ISAE-SUPAERO, 10 Avenue Marc Pelegrin, Toulouse

Devant le jury composé de :

- Katell Morin-Allory, Maîtresse de conférences, Grenoble INP, Rapporteuse
- Guy Gogniat, Professeur, Université Bretagne Sud, Rapporteur
- Angeliki Kritikakou, Maîtresse de conférences, Université de Rennes, Rennes, Examinatrice
- Sébastien Pillement, Professeur, Université de Nantes, Nantes, Examinateur
- Daniela Dragomirescu, Professeure, INSA Toulouse, Toulouse, Examinatrice
- Kévin Delmas, Ingénieur de recherche, ONERA, Toulouse, Invité
- Andres Barrilado, Ingénieur, NXP Semiconductors, Toulouse, Invité
- Claire Pagetti, Directrice de recherche, ONERA, Toulouse, Directrice de thèse

Résumé

Ce travail a été financé par l'institut d'intelligence artificielle et naturelle de Toulouse (ANITI) et a bénéficié d'une bourse de la région Occitanie.

L'intelligence artificielle basée sur les réseaux de neurones profonds (DNN) est de plus en plus importante dans de multiples domaines d'application, en particulier dans les systèmes critiques où ces algorithmes pourraient être utilisés pour la prise de décision dans des systèmes automatisés voire autonomes. Cependant, pour envisager cette intégration, les réseaux neuronaux ainsi que les composants matériels qui les exécutent doivent répondre à un haut niveau de garanties pour assurer la sécurité des utilisateurs et de l'environnement. L'injection de fautes est une technique largement utilisée pour vérifier et valider un composant qui doit fournir des garanties de sécurité (selon des normes telles que l'ISO 26262).

Ce travail se place dans le contexte de l'injection de fautes pour les accélérateurs matériels dédiés à l'exécution de réseaux neuronaux. L'objectif est de fournir un formalisme 1) pour raisonner sur la propagation des données dans un accélérateur matériel, et finalement 2) pour proposer des campagnes d'injection de fautes précises avec un ensemble limité d'expériences. Nous avons défini une méthodologie basée sur la modélisation formelle de l'architecture matérielle qui identifie les instants et les données vulnérables aux corruptions pendant l'inférence d'un DNN. Cette modélisation permet de tracer dans l'architecture la propagation des corruptions silencieuses des données (SDC) causées par des fautes permanentes de type stuck-at ou des fautes transitoires de type bit-flip. Elle permet également d'identifier les fautes ayant le même effet sur le système, ce qui aide à construire une relation d'équivalence. Les classes d'équivalence de fautes associées sont utilisées pour calculer une métrique de couverture par rapport à une stratégie d'injection de fautes exhaustive. Le modèle proposé permet d'évaluer les stratégies d'injection de fautes en fonction de leur couverture, afin de déterminer si ces stratégies sont capables de tester toutes les défaillances du système qui pourraient entraîner des pannes dangereuses. Un outil appelé FIXME (Flows Inspector X Modelling hardware Errors) a été développé en SCALA pour calculer efficacement des ensembles de fautes ayant un effet équivalent pour une architecture, ainsi que le taux de couverture des stratégies d'injection.

Cette méthode est évaluée sur un type d'accélérateurs de réseaux neuronaux appelés streaming qui implémente chaque couche d'une topologie de réseau donnée en tant que composant matériel. Les résultats illustrent l'efficacité de la méthode pour identifier précisément les fautes matérielles qui peuvent avoir un effet sur le calcul, et pour calculer efficacement la couverture de n'importe quelle stratégie d'injection de fautes. Cela ouvre la voie à une méthodologie plus avancée pour identifier les composants matériels qui sont cruciaux pour l'exécution d'un réseau de neurones.

Mots clés

Réseaux de neurones, Sûreté de fonctionnement, micro-électronique numérique

Vous êtes invité à rejoindre la web-conférence JITSI via le lien ci-dessous :

https://isae-supaero-fr.zoom.us/j/91605885779?pwd=a8kiNtQGXaJFqpd2pkolDFEMimsykR.1