Analyse des effets de fautes sur l'exécution de programmes **Projet SESI M1 – 2024-2025**

Descriptif

L'exécution de programmes peut être perturbée par le fait d'injecter des fautes sur la plate-forme d'exécution, par exemple en modifiant temporairement la tension d'alimentation, ou en soumettant le circuit à des perturbations électromagnétiques. Les phénomènes physiques induits par ces perturbations peuvent modifier les états d'éléments de la microarchitecture de la plate-forme d'exécution, et conduire à des comportements divergeant par rapport à une exécution du programme dans un environnement non fauté.

Différentes contre-mesures peuvent être implantées dans le processeur pour pallier aux effets de ces éventuelles fautes : le cœur CV32E40S dispose de différents moyens de remédiation.

L'objectif du projet est de proposer des outils facilitant l'analyse de l'effet des fautes sur des cœurs de processeurs RISC-V : CV32E40P et CV32E40S, en exploitant les traces d'exécution de programmes sur ces plates-formes, le programme assembleur exécuté, et la description de la microarchitecture des cœurs.

Un ensemble d'expérimentations ont été menées sur deux cœurs RISC-V différents : CV3240P et CV3240S. On dispose ainsi, pour différents programmes et cœurs, de traces de référence et de traces fautes associées à chaque référence. Les traces sont produites dans des fichiers .VCD détaillant l'état de tous les signaux RTL à chaque cycle processeur.

On souhaite construire une méthode et des outils d'analyse de ces traces afin de mieux comprendre l'effet des fautes sur l'exécution du programme. Pour ce faire, on mettra en évidence les divergences de comportements entre les traces de références et les traces fautes, et si possible en visualisant, sur la microarchitecture de ces cœurs, le phénomène de propagation des effets des fautes.

Les étapes possibles sont :

- Prise en main de l'environnement d'étude :
 - o Compréhension des architectures CV3240P et CV3240S (blocs fonctionnels, vue macroscopique du code Verilog)
 - o Compréhension des traces de référence et de traces fautes (fournies par le CEA-List), sélection d'un sous-ensemble d'étude
- Analyse de la divergence de traces entre la trace de référence et la trace fautes :
 - o Identification du point de divergence et de la propagation aval des divergences dans la trace fautes
 - o Recherche d'outils libres existants permettant l'analyse de divergence de trace et automatisation sur les exemples fournis ou à défaut, proposition et codage d'une application d'analyse de divergence de 2 traces.
 - o Etude et proposition pour la visualisation de cette divergence sur la microarchitecture du processeur

Le code produit devra être documenté et mis sur un dépôt GIT. Un rapport synthétisera les travaux.

Nombre d'étudiants : 1 ou 2

Remarque

Ce travail fait partie d'une collaboration scientifique entre le LIP6 et le CEA-List.

Contact

Emmanuelle.encrenaz@lip6.fr, mathieu.jan@cea.fr, damien.courousse@cea.fr