Proposition de stage (M1/M2, année 2023)

Vérification formelle de logiciels critiques en instrumentation spatiale

Contexte

Le développement des instruments, permettant l'observation et l'exploration de l'espace, nécessite un cadre très précis, tant les contraintes mécaniques ou électriques, issues de la miniaturisation des satellites, sont déjà fortes. Les logiciels embarqués à bord de ces systèmes doivent concilier ces contraintes avec des ressources (temps et espace) tout aussi restreintes, tout en assurant le bon fonctionnement de la charge utile. Dans le contexte actuel du NewSpace, la demande croissante pour des logiciels embarqués vérifiés et certifiés sûrs devra être satisfaite dans les prochaines années.

Le projet PIONEERS – consortium financé par la Commission Européenne – porte sur la fabrication de nouvelles générations de sismomètres à 6 degrés de liberté en utilisant des technologies optiques. Ces sismomètres ont pour but d'étudier la structure interne de corps célestes (planètes ou astéroïdes) afin de déterminer leur dangerosité ou leur habitabilité pour de futures missions spatiales.

Sujet de stage

Les instruments développés dans ce cadre utilisent des cibles type ARM (cartes SoC FPGA de Xilinx) et nécessitent d'être programmés par des langages bas niveau (C, C++). Plusieurs aspects critiques du logiciel de vol méritent d'être analysés et garantis sûrs avant d'être réellement mis en production. Le but de ce stage est d'étudier la mise en œuvre de techniques formelles permettant de garantir des propriétés de sûreté sur ces systèmes dans le cadre de PIONEERS.

Ce stage se situe entre ingénierie et recherche technologique. Le rôle du stagiaire sera de

- Dresser un état de l'art des technologies d'analyses statiques sur cibles bas niveau.
- Mettre en place une infrastructure d'analyse statique adaptée aux cibles Xilinx.
- Concevoir des spécifications formelles du système.
- Documenter le travail pour assurer la continuité des travaux par les ingénieurs.

Les parties du code source qui seront à étudier concernent :

- La détection des erreurs au runtime (dépassements sur des entiers, déréfencement de pointeurs invalides et allocations insuffisantes)
- La spécification et preuves sur des parties du code et la preuve de correction du code par rapport à ces spécifications :
    - Traitement du signal : Calculs numériques utilisés dans le traitement des données brutes reçues par les capteurs avant leur conversion en données physiques pertinentes.
    - Machine à état principale : Fortes contraintes de temps chronométrique pesant sur l'ordonnancement des tâches (acquisition, traitement, transmission)

Le sujet de stage reste ouvert aux initiatives personnelles du stagiaire permettant de répondre à la problématique.

Profil recherché

Étudiant en M1/M2 ou école d'ingénieurs en informatique. Connaissances en méthodes formelles exigées (vérification déductive, automatique, tests, logiques formelles, calculs de plus faible préconditions, model-checking).

Cadre de travail

Le stage, d'une durée de 6 mois, se déroulera au sein des deux départements DEOS et DISC de l'ISAE-SUPAERO à Toulouse. Le stagiaire bénéficiera de l'expertise du DEOS pour la conception de systèmes embarqués et du DISC pour le développement de méthodes formelles. La durée hebdomadaire de travail est de 35h et donne lieu à une indemnité approximative de 590 €/mois.

Contact

- Hai Nguyen Van hai.nguyen-van@isae-supaero.fr
- Xavier Thirioux xavier.thirioux@isae-supaero.fr

Ressources

1. Crockett et al., *The Zynq Book, Embedded Processing with the ARM Cortex-A9 on the Xilinx Zynq-7000 All Programmable SoC*, University of Strathclyde, 2014.
2. Correnson et al., Frama-C User Manual, CEA, 2022.