www.onera.fr

ONERA
THE FRENCH AEROSPACE LAB

PROPOSITION DE STAGE EN COURS D'ETUDES

Référence : **DTIS-2024-59**
(à rappeler dans toute correspondance)

Lieu : Toulouse

Département/Dir./Serv. : DTIS/SEAS

Tél. : 05 62 25 26 81

Responsable(s) du stage : Julien Brunel & Youcef Bouchebaba

Email. : julien.brunel@onera.fr

DESCRIPTION DU STAGE

Thématique(s) : Ingénierie des systèmes et des Logiciels

Type de stage : X Fin d'études bac+5 X Master 2

Intitulé : Analyse de vulnérabilité de plateformes multi-coeurs embarquées

Sujet : Le domaine avionique est caractérisé depuis plusieurs années par plusieurs évolutions de fond, comme : (1) la multiplication des automatismes embarqués, entraînant l'augmentation du nombre et de la taille des logiciels avioniques ; (2) l'abandon progressif des composants spécifiques avioniques et à l'inverse l'utilisation croissante de processeurs COTS pour des raisons de coût, de maturité et d'outillage; et (3) l'ouverture de l'avionique à des flux externes et des fonctions logicielles tierces qui se retrouvent ainsi potentiellement en interaction avec le cœur critique de l'avionique. Si ces évolutions permettent le développement d'avions plus performants, plus « intelligents », plus « verts » et plus compétitifs, elles posent cependant plusieurs problèmes difficiles. En particulier, l'ouverture des architectures aux flux et fonctions tierces, et la cohabitation de ces fonctions avec des logiciels avioniques critiques dans ces processeurs complexes posent la question de la cybersécurité et de sa prise en compte lors de la certification. Lors de la dernière décennie, la préoccupation de la cybersécurité s'est développée dans le monde aéronautique, indépendamment de l'utilisation de processeurs modernes.

En ce qui concerne les plateformes d'exécution, les concepteurs s'interdisent toujours d'héberger plusieurs applications de domaines différents, ou plusieurs fonctions de sécurité différentes, sur un même calculateur. Une des raisons motivant ce choix est liée à la complexité de la démonstration de l'isolation inter-domaines dans le cadre de la certification. Ceci limite certains aspects cruciaux du développement d'un nouveau programme avion tels que le gain de poids potentiel lié à la mutualisation du hardware, ainsi que les opportunités commerciales que pourraient pourrait apporter plus de connectivité.

Un effort international a mené à standardiser le processus de conception des systèmes avioniques vis à vis de la cybersécurité, au sein des documents DO-236A / ED-202A, DO-356A / ED-203A. Ces standards ne proposent pas encore un niveau d'exigence assez raffiné pour considérer les problèmes de sécurité liés à l'isolation de processus sur des plateformes multi-cœurs. En effet, ils demeurent en général au niveau d'abstraction qui concerne l'intégrateur de systèmes, c'est-à-dire l'avionneur. Cependant, dans certaines plateformes multi-coeurs, des mécanismes ont déjà été développés dans le but de garantir des propriétés de cybersécurité. C'est le cas par exemple du *secure boot* et l'*ARM trust zone*.

Au sein du département DTIS de l'ONERA, de nombreux travaux portent sur l'étude des architectures multi-coeurs, en se reposant sur méthodes formelles et sur diverses plateformes expérimentales. Jusqu'à présent, ces travaux se concentrent essentiellement sur le respect de contraintes temps-réel. Par ailleurs, des travaux théoriques sont menés au DTIS sur la cybersécurité de ce type de plateformes (comme l'identification de familles d'attaques pertinentes). L'objectif de ce stage est d'étendre et de valider ces travaux à l'aide de d'expérimentations sur une plateforme multi-coeurs existante. En fonction des premiers résultats et des intérêts du candidats, des techniques de vérification formelle permettant de garantir des propriétés de cybersécurité pourront être développées.

Plus précisément, le travail consistera à :

- Explorer les principales vulnérabilités au sein des architectures multi-coeurs ;
- Étudier les différents mécanismes de sécurité existants dans les architectures multi-coeurs en général, et identifier les vulnérabilités auxquelles ils répondent ;
- Sélectionner et instancier certains de ces mécanismes sur la plateforme UltraScale MPSoC ZCU102 ;
- Identifier comment ces mécanismes peuvent aider à répondre aux objectifs de certification tels qu'ils sont présentés dans les standards ;
- Proposer des modèles formels pour représenter les architectures, et des techniques de vérification associées permettant de répondre à certains objectifs de cybersécurité.

.

Est-il possible d'envisager un travail en binôme ?

Méthodes à mettre en oeuvre :

X Recherche théorique	Travail de synthèse
X Recherche appliquée	Travail de documentation
X Recherche expérimentale	X Participation à une réalisation

Possibilité de prolongation en thèse : Oui

Durée du stage : Minimum : 5 mois Maximum : 6 mois

Période souhaitée : printemps 2024

PROFIL DU STAGIAIRE

Connaissances et niveau requis :	Ecoles ou établissements souhaités :
bases en programmation (C), des compétences en architecture, cybersécurité ou méthodes formelles sont un plus	M2 d'informatique ou école d'ingénieur