PROPOSITION DE STAGE EN COURS D'ETUDES

Référence : **DTIS-2025-63** *(à rappeler dans toute correspondance)*	Lieu :	Toulouse
Département/Dir./Serv. : DTIS	Tél. :	05 62 25 28 21
Responsable(s) du stage : Kevin Delmas, Anthony FAURE GIGNOUX	Email. :	kevin.delmas@onera.fr anthony.faure-gignoux@onera.fr

DESCRIPTION DU STAGE

Thématique(s) : Sûreté et sécurité des systèmes cyber-physiques

Type de stage : ☒ Fin d'études bac+5 ☒ Master 2 □ Bac+2 à bac+4 □ Autres

Intitulé : Formal Verification of Machine Learning Algorithms on Advanced Avionics Hardware

Sujet : Machine Learning (ML) plays a pivotal role in the development of autonomous systems, including future generations of aircraft that will integrate advanced algorithms for enhanced capabilities, such as vision-based autonomous landing for drones and commercial aircraft. While these algorithms perform efficiently in cloud or data center environments, deploying them on autonomous vehicles presents significant challenges—especially in ensuring safety. In the field of aeronautics, every function, whether ML-based or not, must meet rigorous safety standards, even in the event of hardware failures.

Vision-based perception systems, which are critical for autonomous operations, demand immense computational power and high-bandwidth communications (e.g., from cameras). However, current avionics processors lack the necessary capacity to handle such workloads. As a result, new processing architectures, such as Commercial-off-the-shelf (COTS) GPUs and many-core processors, will be essential. Before these can be deployed, it's crucial to study their hardware failure modes, understand how these failures could affect the ML algorithms they support, and develop safeguards to ensure safe execution.

Several existing works, such as [1], [2], and [3], have addressed these issues by formally modeling platform behavior in the presence of faults, along with the mitigation strategies designed to reduce the impact of these faults. These models can be analyzed using solvers to determine if the mitigations are sufficient to guarantee safe hardware operation under specified conditions.

Preliminary research has identified the Versatile Tensor Accelerator (VTA [4]) as a suitable candidate for further exploration of this problem. VTA is open hardware, meaning its hardware description is fully accessible and customizable. It is described using Chisel [5], an advanced high-level hardware description language built on Scala [6].

The primary goal of this internship is to evaluate the effectiveness of a set of pre-selected formal verification methods on the VTA. The key steps include:

- Conducting a literature review to identify the most promising formal verification methods from the pre-selected set.

- Gaining proficiency with the toolset required for functional and cycle-accurate simulation of VTA executions.

- Developing a framework to run small portions of deep neural networks (DNNs) on both functional and cycle-accurate simulators.

- Extending the framework to verify formal properties using the selected methods.

- Assessing the expressiveness and scalability of the approach, initially focusing on specific parts of the VTA, and, if feasible, expanding to the full accelerator.

- Based on the experiments, formulating recommendations for future theoretical and practical developments required for full-scale safety validation of VTA-like accelerators

[1] Guinebert, I., Barrilado, A., Delmas, K., Galtié, F., & Pagetti, C. (2022, June). Quality of Fault Injection Strategies on Hardware Accelerator. In International Conference on Computer Safety, Reliability, and Security (pp. 222-236). Cham: Springer International Publishing.

[2]Faure-Gignoux, A, Delmas, K, Gauffriau, A, Pagetti, C. (2024) Methodology for formal verification of hardware.safety strategies using SMT. International conference on embedded software (EMSOFT)

[3] Dobis, A., Laeufer, K., Damsgaard, H. J., Petersen, T., Rasmussen, K. J. H., Tolotto, E., ... & Schoeberl, M. (2023). Verification of chisel hardware designs with chiselverify. Microprocessors and Microsystems, 96, 104737.

[4] https://github.com/apache/tvm-vta

[5] https://www.chisel-lang.org/

[6] https://www.scala-lang.org/

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

Méthodes à mettre en oeuvre :

☒ Recherche théorique

☒ Recherche appliquée

☐ Recherche expérimentale

☒ Travail de synthèse

☐ Travail de documentation

☐ Participation à une réalisation

Possibilité de prolongation en thèse : **Non**

Durée du stage : Minimum : 5 Maximum : 6

Période souhaitée : Mars-Septembre 2025

PROFIL DU STAGIAIRE

Connaissances et niveau requis :

Hardware description languages (advanced)

Compilation, Computing architectures (intermediate)

Formal verification (notions)

Programming (advanced)

Ecoles ou établissements souhaités :

Master 2 ou ecole d'ingénieur avec cursus mathématiques appliquées ou sûreté de fonctionnement