Ecole Nationale Supérieure de Mécanique et d'Aérotechnique
Téléport 2 - 1 avenue Clément Ader
BP 40109
86961 Futuroscope Chasseneuil Cedex
Tél : +33 (0)5 49 49 80 80

Approche méthodologique pour l'enseignement de la cybersécurité des composants embarqués dans les systèmes critiques

Laboratoire :	LIAS (https://www.lias-lab.fr)
Établissement :	ISAE-ENSMA (https://www.ensma.fr)
Directeur de thèse :	Emmanuel Grolleau
Co-encadrants académiques :	à préciser
Entreprise :	AC6 (https://www.ac6.fr/)
Co-directeurs industriels :	Roy Jamil, Ayoub Bourjilat
Financement :	CIFRE AC6

1 Candidature recherchée

Le ou la candidat(e) doit être titulaire d'un diplôme d'ingénieur ou Master, et avoir de solides compétences en informatique embarquée, programmation, architecture des processeurs. La thèse se déroulera principalement dans les locaux d'AC6 à Courbevoie, avec des séjours au LIAS, ISAE-ENSMA à Chasseneuil du Poitou, site du Futuroscope.

Le dossier de candidature doit être envoyé par courrier électronique **au plus tard le 1/05/2025, minuit**, à grolleau@ensma.fr et est constitué de :

- Lettre de motivation ;
- CV mentionnant explicitement le parcours académique ;
- feuilles de notes des années universitaires mentionnant, si possible, le classement ;
- tout élément jugé utile pour mettre la candidature en valeur.

Nous recherchons en particulier :

- L'envie d'enseigner et de partager des connaissances.
- Connaissances de base en microcontrôleurs ou microprocesseurs (STM32, NXP, Arduino, Microchip-PIC, RPie, etc.),
- Connaissance en systèmes d'exploitation RTOS (Zephyr, FreeRTOS, MBED OS, etc.) et Linux embarqué,
- Connaissance de base en sécurité,
- Maîtrise de la programmation, en particulier C/C++,
- Maîtrise du français et de l'anglais, tant à l'écrit qu'à l'oral,

Version non définitive du sujet, en discussion avec Ac6

2 Contexte et problématique

Le domaine de la cybersécurité, en particulier dans les systèmes embarqués [Alo+21], que ce soit dans le domaine des transports ou de l'IoT, est de plus en plus critique. De nombreux standards industriels abordent la sécurité principalement sous un angle culturel, systémique et lié aux processus, comme par exemple l'ISO/SAE 21434 [ISO21] dans l'automobile, ou encore diverses normes en avionique civile qui y font référence (voir une compilation dans [IAT22]). Ces standards font référence à l'utilisation de composants logiciels ou matériels supposés

résilients aux cyberattaques, notamment à la manipulation externe, à la rétro-ingénierie et aux attaques par canal auxiliaire.

Cette problématique devient d'autant plus pressante avec l'entrée en vigueur prochaine du Cyber Resilience Act (CRA) [Par24], un règlement européen imposant des exigences strictes en matière de cybersécurité pour les produits comportant des éléments numériques. Ce texte oblige les fabricants à garantir un niveau de sécurité dès la conception (« security by design ») et tout au long du cycle de vie du produit, y compris dans les environnements contraints comme les systèmes embarqués. Le CRA introduit également une obligation de conformité, sous peine de sanctions, rendant indispensable une meilleure compréhension et maîtrise des exigences de sécurité à bas niveau, souvent négligées dans la formation actuelle.

Cependant, l'étude menée dans le cadre du projet européen CyberSec4Europe [Cyb20] montre que l'aspect cybersécurité des composants est peu couvert dans les syllabus de cybersécurité des universités européennes.

Une des explications à cette carence est la difficulté de former à la fois à la cybersécurité et à l'embarqué, deux cultures scientifiques initialement distinctes. En effet, les paradigmes de sécurité hérités des architectures centralisées, reposant sur une protection forte des périmètres, ne sont pas directement applicables dans les environnements embarqués, où la distribution des composants et la possibilité d'un accès physique élargissent considérablement la surface d'attaque.

3 Problématiques scientifiques

L'entreprise AC6 propose notamment de la formation professionnelle dans le domaine de l'embarqué, et traite, au moins partiellement, de la sécurité des composants embarqués. Elle s'intéresse en particulier au déploiement sécurisé des systèmes d'exploitation, dans le but de réduire les surfaces d'attaque liées à la manipulation externe et à la rétro-ingénierie. Les profils des apprenants en formation professionnelle sont très variés, avec des parcours académiques allant de l'électronique à l'informatique générale, et une culture système plus ou moins développée.

Dans ce contexte, AC6 envisage de repenser en profondeur les approches pédagogiques liées à la cybersécurité des systèmes embarqués. Ce domaine, encore largement enseigné de manière segmentée et selon des paradigmes traditionnels, souffre d'un manque d'intégration entre les spécificités matérielles, les pratiques industrielles actuelles et les cadres réglementaires émergents tels que le CRA. L'objectif est de concevoir une démarche pédagogique fondée sur une structuration cohérente des savoirs, prenant en compte à la fois la diversité des profils des apprenants et les exigences concrètes du déploiement sécurisé dans des environnements contraints.

L'objectif de la thèse est de tirer parti des dizaines de formations annuelles délivrées par AC6, afin d'identifier précisément et de hiérarchiser les prérequis nécessaires à une bonne compréhension des technologies et des problématiques liées au déploiement sécurisé sur des composants embarqués. Ensuite, elle vise à proposer et tester sur les apprenants diverses méthodes pédagogiques. Les syllabus produits, ainsi que les progressions pédagogiques associées, seront également adaptés et testés en école d'ingénieur, dans le cadre de la formation initiale.

Ecole Nationale Supérieure de Mécanique et d'Aérotechnique
Téléport 2 - 1 avenue Clément Ader
BP 40109
86961 Futuroscope Chasseneuil Cedex
Tél : +33 (0)5 49 49 80 80

4 Travaux de la thèse

Le ou la doctorant(e) suivra les différentes étapes suivantes :
- Réalisation d'un état de l'art sur la cybersécurité dans les systèmes embarqués ;
- Réalisation d'un état de l'art sur l'enseignement de la cybersécurité et des RTOS ;
- Mise en place d'un processus itératif comprenant les étapes suivantes, à réévaluer autant que nécessaire :
  - Choix d'une méthode d'évaluation de l'impact des formations dans le domaine ;
  - Élaboration de syllabus et de prérequis précis pour la cybersécurité dans les composants embarqués, et confrontation avec les profils types des apprenants ;
  - Analyse des résultats observés sur les apprenants.

Références

[Alo+21] Abdulmohsan Aloseel, Hongmei He, Carl Shaw et Muhammad Ali Khan. « Analytical Review of Cybersecurity for Embedded Systems ». In : *IEEE Access* 9 (2021), p. 961-982. DOI : 10.1109/ACCESS.2020.3045972.

[Cyb20] CyberSec4Europe Consortium. *Education and Training Review*. Rapp. tech. D6.2. Version 1.2. Submitted Version. CyberSec4Europe, fév. 2020. URL : https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf.

[IAT22] IATA. *Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation*. 2022. URL : https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation-of-cyber-regs.pdf (visité le 01/04/2025).

[ISO21] ISO. *ISO/SAE 21434 :2021, Road vehicles — Cybersecurity engineering*. 2021. URL : https://www.iso.org/standard/70918.html.

[Par24] European Parliament. *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*. 2024. URL : https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.