**L'université Savoie Mont Blanc recrute un**
**Ingénieur de recherche en Intelligence Artificielle F/H**

**Contrat à Durée Déterminée de 18 mois**

**Quotité : 100%**
**Site : Annecy**

**Au sein du LISTIC**
**Poste à pourvoir : au plus tôt**

## Contexte

Avec plus de 15 000 étudiants, une offre de formation pluridisciplinaire riche d'une centaine de diplômes nationaux et des laboratoires de qualité qui la font apparaître dans le classement de Shanghai, l'université Savoie Mont Blanc, membre de l'alliance européenne UNITA, est un établissement à taille humaine qui conjugue la recherche et la professionnalisation, la proximité avec ses territoires et une large ouverture sur le monde.
Sur ses trois campus d'Annecy, du Bourget-du-Lac et de Jacob-Bellecombette, elle propose différents cursus courts et longs (Diplômes d'université, Bachelors universitaires de technologie, Licences, Masters, Doctorats, Diplômes d'ingénieurs) que ce soit en formation initiale ou continue, en alternance ou via diverses validations, en présentiel ou à distance.
Entre Genève, Turin, Lyon et Grenoble, aux frontières de la Suisse et de l'Italie, avec le concours des collectivités qui l'ont vu naître et des entreprises qui l'accompagnent, elle est un acteur majeur du dynamique écosystème national et transfrontalier, fortement impliqué dans son développement économique, social et culturel.

Les travaux se dérouleront dans le cadre du projet CYBERSIM, financé par le Programme de Transfert au Campus Cyber (PTCC), en partenariat avec le laboratoire de recherche De Vinci Research Center (DVRC), le laboratoire LISTIC et l'entreprise Airbus Protect.

**Profil recherché** : Le candidat doit avoir une solide expérience dans le domaine de l'intelligence artificielle (IA), des connaissances en analyse de données et en IA explicable (XAI) seront également appréciées. Une expérience de la recherche académique et/ou un doctorat serait souhaitable.

**Affectation :** Vous serez affecté au Laboratoire d'Informatique, Systèmes, Traitement de l'Information et de la Connaissance (LISTIC) à Annecy dont les orientations scientifiques s'inscrivent dans les priorités données en France à la recherche en Intelligence Artificielle (IA) et au développement du numérique.

## 1. Description

Les systèmes cyber-physiques (CPS) sont des infrastructures structurantes de notre société qui sont déployées dans des secteurs économiques critiques comme l'énergie, le transport ou le médical. La particularité de ces systèmes est qu'ils comprennent à la fois une dimension physique pour manipuler un procédé et créer un bien ou un service, et une dimension informatique pour traiter l'information du système

afin d'en augmenter sa flexibilité, son autonomie ou encore sa performance. Cependant, cette hybridation entre le physique et l'informatique fait des CPS des systèmes critiques assujettis au risque de cyberattaque. En effet, dû à leur interaction avec le monde physique, nous devons garantir la sûreté des CPS face aux défaillances mais aussi face aux cyberattaques.

Dans le cadre du projet CYBERSIM, en collaboration avec Airbus Protect, nous développons un cadre formel innovant permettant d'automatiser l'appréciation du risque de cybersécurité pour la sûreté des CPS. Ce cadre, basé sur les modèles, permet de générer un ensemble de scénarios de cyberattaque réalistes qui impactent la sûreté du système. Cependant, dû à la complexité des CPS, nous nous confrontons à un problème d'explosion combinatoire avec un nombre important de scénarios. Pour pallier ce problème, nous souhaitons définir un framework (ensemble d'outils) permettant d'évaluer la pertinence d'un scénario d'attaque. Une première contribution a été de définir un critère de coupure vu comme une « empreinte » [Serru2023] qui prend en compte les dépendances entre les actions d'une attaque. Des résultats préliminaires obtenus avec un cas d'étude d'une architecture automobile extraite du projet [EVITA2011] ont permis de passer de plus de 400 000 séquences de longueur 10 à une soixantaine de séquences ayant une empreinte inférieure ou égale à 2. Une deuxième contribution a été de développer un cadre robuste pour la quantification d'un scénario d'attaque nommé « fonction de coût multi-métriques » [DaSilva2025]. À partir des données fournies par le framework MITRE EMB3D, nous avons créé un modèle de coût permettant d'évaluer et de classer les scénarios d'attaque générés selon leur pertinence.

Les prochaines étapes du projet consistent à enrichir notre cadre formel et à assurer le transfert de ces résultats académiques au partenaire industriel Airbus Protect. Des analyses de cybersécurité nouvellement développées seront implémentées dans SimfiaNeo, un logiciel développé par Airbus Protect pour l'analyse des risques de sûreté de fonctionnement dans des secteurs tels que l'aérospatiale, la défense, l'énergie et les transports. Ces développements devraient permettre d'automatiser les tâches des analystes de risque et d'optimiser leur temps de travail en fournissant des indicateurs pour évaluer les scénarios les plus probables, identifier les faiblesses de l'architecture du système étudié et mettre en œuvre des contre-mesures, tout cela dès la conception même du système, en combinant à la fois analyses de sûreté et de sécurité dans le même outil. Les résultats du projet devront être validés par des cas d'usage industriels.

**Objectifs** : Le futur ingénieur de recherche travaillera sur des modèles d'intelligence artificielle (IA) pour optimiser la fonction de coût à partir des données historiques existantes. Plus précisément, la personne recrutée :

- Réalisera un modèle d'intelligence artificielle capable de générer des scénarios d'attaques réalistes ciblant les infrastructures cyber-physiques.
- Proposera des outils permettant d'expliquer (XAI) les choix du modèle d'IA pour améliorer la fonction de coût que nous avons développée.
- Si le temps le permet, le futur ingénieur de recherche proposera un modèle d'IA capable de proposer un ensemble de remédiations qui minimisent la fonction de coût (criticité d'un scénario d'attaque) globale du système. Ce modèle pourra intégrer des métriques complémentaires comme le coût financier, la difficulté de mise en œuvre, etc. pour choisir la solution de remédiation la plus adaptée aux contraintes de l'organisation.

Les résultats de ces travaux seront appliqués à un cas d'usage réaliste afin de permettre leur implémentation et leur valorisation au travers du logiciel SimfiaNeo commercialisé par Airbus Protect.

**Références**

[Serru2023] Théo Serru, Nga Nguyen, Michel Batteux, et Antoine Rauzy. Minimal Critical Sequences in Model-Based Safety and Security Analyses: Commonalities and Differences. ACM Transactions on Cyber-Physical Systems, May 2023,
[EVITA2011] EVITA Project. 2011. EVITA: E-safety vehicle intrusion protected applications. https://www.evita-project.org/
[DaSilva2025] Mike Da Silva, Nga Nguyen. Quantitative Security Metrics: Assessment of Cyberattack Scenarios for Embedded Systems, IEEE/IFIP International Conference on Dependable Systems and Networks, Industry Track, Naples, Italy, June 2025

**CONDITIONS D'EMPLOI**

- Traitement brut mensuel : à partir de 2490€ et jusqu'à 2926€ (INM 491 (échelon 2) à INM 577 (échelon 5)) classe A Ingénieur de recherche - fourchette de rémunération proposée pour tenir compte des diplômes et de l'expérience professionnelle (A adapter selon les recrutements)
- Droit annuel à congés : 3,75 jours par mois (45 jours par an + RTT selon organisation du travail)
- Temps de travail : plusieurs modalités d'organisation
- Télétravail possible
- Possibilités de subventions : restauration, transports publics, activités périscolaires…
- Accès à la formation, aux activités sportives proposées par l'université

**Procédure de recrutement :**

**Pour candidater, envoyer un CV et une LETTRE DE MOTIVATION par voie électronique à l'adresse mike.da-silva@univ-smb.fr avec pour objet « IGR IA - CYBERSIM »**