

Université de technologie de Compiègne - Proposition de thèse

1^{re} partie : Fiche scientifique	
Intitulé de la thèse	ARS²TA Analyse des Risques Security et Safety pour le Train Autonome
Type de financement	Contrat doctoral sur allocation Ministère
Laboratoire d'accueil	Heudiasyc, UMR CNRS 7253, équipe de recherche SCOP https://www.hds.utc.fr/recherche/equipes-de-recherche/scop-surete-communication-optimisation.html
Directeur(s) de thèse	Ahmed Lounis (ECC) et Mohamed Sallak (MCF HDR)
Domaines de compétence	Informatique, électronique
Description du sujet de thèse	<p>Le secteur du transport ferroviaire est de plus en plus impacté par le développement du numérique. L'utilisation de l'Internet des objets pour la connexion, le contrôle à distance et la supervision des systèmes ferroviaires expose ce type de systèmes aux risques numériques et aux cyber-attaques. En particulier, des nouvelles menaces liées aux cyber-attaques peuvent affecter la <i>safety</i> de ces systèmes. Traditionnellement, l'analyse <i>safety</i> des systèmes ferroviaires ne prend pas en compte la cybersécurité ce qui peut entraîner des accidents majeurs. En effet, les systèmes ferroviaires sont conçus pour être fiables et sûrs, plutôt que cyber-sécurisés et il n'existe pas de méthodes reconnues et acceptées par la communauté de la <i>safety</i> pour l'analyse des risques de cybersécurité. Par ailleurs, l'utilisation d'une même échelle pour la quantification des probabilités d'occurrence des événements dangereux pour la <i>safety</i> et la <i>security</i> semble problématique car en cybersécurité ces échelles sont souvent qualitatives. L'objectif de cette thèse est de proposer pour la première fois une étude quantitative approfondie de l'impact de la <i>security</i> sur la <i>safety</i> pour les trains autonomes. Cette étude comprendra une première tentative de quantification des risques cybersécurité en présence d'incertitudes. Par la suite, nous proposerons une méthodologie permettant de minimiser cet impact ou du moins de prendre en compte cet aspect dès la phase de vérification des exigences de <i>safety</i>. Enfin, nous pourrions généraliser la méthodologie proposée à tout système critique embarqué.</p>
Mots clés	Cyber-sécurité, incertitude, <i>safety</i> , cyber-attaques, analyses des risques, évaluation des risques,
Profil et compétences du candidat	<p>Bac+5 en Informatique, Réseaux ou Système embarqué</p> <p>Qualités attendues : travail en équipe, une grande capacité d'adaptation, autonomie et rigueur.</p> <p>Des compétences en cybersécurité, <i>safety</i>, sûreté de fonctionnement et/ou analyse des données seront appréciées.</p>
Date de début de la thèse	Octobre 2021
Lieu de travail de thèse	Université de technologie de Compiègne, laboratoire Heudiasyc

2^e partie : Fiche de poste

Durée	36 mois
Possibilité missions complémentaires	Enseignement possible dans le cycle ingénieur à l'UTC
Laboratoire d'accueil	<p>Heudiasyc (UMR 7253) est une unité mixte de recherche associant l'UTC et le CNRS. Elle mène une recherche pluridisciplinaire centrée sur les sciences et technologies de l'information, incluant l'apprentissage, le raisonnement incertain, la recherche opérationnelle, les réseaux, la robotique, l'automatique et l'ingénierie des connaissances.</p> <p>Les activités d'Heudiasyc sont fondées sur la synergie entre recherche amont et recherche technologique, pour répondre aux grands enjeux de la société dans le domaine des sciences de l'information et ceci en étroite collaboration avec des partenaires métiers, notamment industriels.</p>
Moyens matériels	Bureau collectif (4 doctorants), ordinateur fixe ou portable; moyens de calcul GPU du laboratoire et du CNRS, plateforme ferroviaire
Moyens humains	42 EC, 14 BIATSS/ITA, 47 doctorants, 1 post-doc
Moyens financiers	Le projet bénéficiera des budgets de fonctionnement de projets en cours et aussi d'une participation de l'équipe pour les frais de fonctionnement (conférences, missions, etc.)
Modalités de travail	Réunions régulières avec les encadrants dont la fréquence variera selon le besoin, la phase de la thèse et l'avancement.
Projet de recherche lié à cette thèse	Non
Collaboration(s) nationale(s)	Des collaborations avec l'IRT Railenium peuvent être envisagées en fonction des résultats obtenus
Collaboration(s) internationale(s)	Non
Thèse en cotutelle internationale	Non
Coordonnées de la personne à contacter	Tel : 33 (0)3 44 23 79 51 Mail : ahmed.lounis@hds.utc.fr

Contactez d'abord le directeur de thèse avant de renseigner un dossier de candidature en ligne sur <https://webapplis.utc.fr/admissions/doctorants/accueil.jsf>

Université de technologie de Compiègne – Thesis proposal

Part 1: Scientific sheet	
Thesis proposal title	Security and Safety Risk Analysis for Autonomous Train
PhD grant	Doctoral work contract based on a Ministry of Research Grant
Research laboratory	Research unity : Heudiasyc research team: SCOP web site: https://www.hds.utc.fr/
Thesis supervisor(s)	Ahmed Lounis et Mohamed Sallak (HDR)
Scientific domain(s)	Computer science and information technologies Science and technology
Description of the thesis proposal	The rail transport sector is continuously impacted by new technologies development. Using the Internet of Things to connect, remotely control and monitor rail systems exposes these systems to security risks like cyber-attacks. In particular, new security threats can affect the safety of these systems. Traditionally, safety analysis of railway systems does not take cybersecurity in consideration, which can lead to major accidents. Indeed, railway systems are designed to be reliable and safe, rather than cyber-secure, and there are no recognized and accepted methods by the safety community for analyzing cybersecurity risks. Furthermore, using the same scale to quantify the dangerous events occurrence probabilities of to safety and security seems problematic because in cybersecurity these scales are often qualitative. The objective of this thesis is to propose for the first time a deep quantitative study of the impact of cyber-security on safety for autonomous trains. This study will include a first attempt to quantify cybersecurity risks in the presence of uncertainties. We then propose a methodology to minimize this impact or at least take this aspect in consideration from the safety requirements verification phase. Finally, we will be able to generalize the methodology proposed to any critical embedded system.
Keywords	Cyber-security, uncertainty, safety, cyber-attacks, risk analyzes, risk assessment,
Requirements	Bac+5 in computer science, Networks and/or embedded systems Required qualities: teamwork, adaptation capabilities, autonomy and rigor Skills in cybersecurity, safety, operational safety and / or data analysis will be appreciated.
Starting date	1 October 2021
Location	Heusiasyc Lab, Compiègne, France

Part 2: Job description	
Duration	36 months
Additional missions available	teaching
Research laboratory	<p>Heudiasyc (UMR 7253) is a joint research unit which associates the UTC and the CNRS. Members conduct research focused on information sciences and technologies, including machine learning, reasoning under uncertainty, operational research, networks, robotics, automatic control, and knowledge engineering.</p> <p>These activities are grounded in the synergy between upstream and applied research, in order to respond to the major challenges facing society in the field of information sciences, in close collaboration with business partners, particularly industry.</p>
Material resources	Shared office (4 PhD students), PC or laptop ; lab and CNRS computational resources
Human resources	(academics : 42, staff : 14, PhD students : 47, postdoctoral fellows : 1)
Financial resources	The thesis proposal will benefit from the fundings of the SCOP team for operating expenses (conferences, missions, etc)
Working conditions	scientific support and regular follow-up during meetings with the thesis supervisors,
Research project	no
National collaborations	Collaborations with IRT Railenium may be considered according to obtained results
International collaborations	no
International cosupervision (cotutelle)	no
Contact	<p>Tel : 33 (0)3 44 23 79 51 Mail : ahmed.lounis@hds.utc.fr Adress : Laboratoire Heudiasyc UMR CNRS 7253 CS 60319, 57 avenue de Landshut 60203 Compiègne Cedex, France</p>

Please contact first the thesis supervisor before applying online on <https://webapplis.utc.fr/admissions/doctorants/accueil.jsf>