Offre de stage : Etat de l'art scientifique sur l'intégration des nouveaux risques de cyberattaque par les entreprises industrielles

Référence	CYBERINSTITUTE-INT-19003
Description	Depuis les années 2000, les systèmes industriels sont au cœur d'une révolution technologique numérique centrée sur l'usage de machines dotées de calculateurs de plus en plus performants. Ceux-ci intègrent des fonctions logicielles toujours plus importantes et sont connectés à des systèmes d'information. Cette évolution des outils industriels s'est accompagnée d'un ensemble de vulnérabilités qui n'ont pas été prises en compte assez tôt. Ainsi, les systèmes industriels intégrant ces nouvelles technologies numériques ont commencé à se voir attaqués par des attaques les ciblant spécifiquement, avec des conséquences parfois catastrophiques. L'un des principaux verrous entravant une meilleure prise en compte de tels risques de cyberattaque par les organisations du secteur industriel réside dans la difficulté des décideurs à allouer une part de leur attention à un nouveau type de risque, encore mal identifié par les professionnels de la sécurité des systèmes industriels (SSI), celui de cyberattaque contre les objets connectés du système de contrôle-commande. Les responsables de la SSI et de l'automation et, plus largement, les managers de l'organisation, évoluent en effet dans un environnement d'une extrême complexité, déjà saturé de risques divers, dans lequel tout input extérieur – par exemple la mise à jour logicielle de n'importe quelle composante d'une ligne de production – menace de faire basculer le système en mode de fonctionnement dégradé. C'est pourquoi il est important d'étudier les facteurs et processus qui font que des acteurs déjà fortement sollicités par d'autres préoccupations en viennent à intégrer préventivement une nouvelle forme de menace. Dans le cadre de ce stage pour le Grenoble Alpes Cybersecurity Institute, la mission du stagiaire consistera à réaliser un travail d'état de l'art – recherches bibliographiques et synthèse de la littérature scientifique repérée – portant sur les dynamiques organisationnelles, professionnelles et institutionnelles de sensibilisation aux risques de cyberattaques contre les composantes connectées d'un système industriel. Cette étude devra mettre en lumière l'ensemble des facteurs facilitateurs et inhibiteurs de l'intégration de dispositifs de protection : technologiques (outils permettant de détecter ou de contrecarrer des attaques), organisationnels et professionnels (réalités de l'entreprise, profil des expertises internes en sécurité, organisation et fonctionnement de la fonction cybersécurité), économiques (contraintes économiques liées aux marchés où évolue l'entreprise), juridiques (évolution des normes légales, techniques et certifications), incitations publiques (par exemple via les lois, la réglementation, l'INPI, les services de sécurité intérieure), évolutions réglementaires (certifications, discussions en cours au niveau de l'ENISA, nouvelles normes 62443) ou liées aux assurances, état objectif des menaces, perception des risques par les ingénieurs et managers. L'étude devra aussi contribuer à recenser les différents types d'attaques menaçant les systèmes industriels ; classifier les différentes solutions de protection contre les attaques ; établir une typologie de ces systèmes en fonction de leurs vulnérabilités et possibilités de protection ; et, enfin, élaborer une typologie des processus de prise de conscience des menaces et des modes d'intégration des solutions de protection dans les différents types de système identifiés.
Prérequis	Le ou la candidat(e) doit avoir un profil de formation Bac+5 et pouvoir justifier de solides connaissances en sociologie (des sciences et techniques, des organisations, du travail…), en science politique (politiques de sécurité, gestion des risques…) ou en science de l'ingénieur avec un fort intérêt pour les sciences sociales, et devra impérativement lire couramment l'anglais scientifique. <u>Bibliographie</u> [1] Boin, A., and Schulman, P. (2008). Assessing NASA's safety culture: The limits and possibilities of high-reliability theory. *Public Administration Review*, 68 (6), 1050-1062. [2] Goldin Ian, Mariathasan Mike, The Butterfly Defect: How Globalization Creates Systemic Risks, and What to Do about It, *Princeton University Press*, 2014. [3] Haavik Torgeir K., New Tools, Old Tasks: Safety Implications of New Technologies and Work Processes for Integrated Operations in the Petroleum Industry, *CRC Press*, 2017. [4] Hopkins Andrew, Managing Major Hazards: The Lessons of the Moura Mine Disaster, *Allen & Unwin*, 2001. [5] Perrow Charles, Normal Accidents – Living with High Risk Technologies, *Princeton University Press*, 1999. [6] Perrow Charles, The Next Catastrophe - Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters, *Princeton University Press*, 2011. [7]Rousseau, D. M. (1989). The price of success? Security-oriented cultures and high reliability organisations. *Industrial Crisis Quarterly*, 3, 285-302. [8] Sicard F., E. Zamaï, and J.-M. Flaus, Filters based Approach with Temporal and Combinational Constraints for Cybersecurity of Industrial Control Systems, *IFAC-Pap., vol. 51, no. 24, pp. 96–103*, Jan. 2018. [9] Vaughan Diane, The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA, *Chicago: University of Chicago Press*, 1996. [10] Weick Karl, Managing the Unexpected: Resilient Performance in an Age of Uncertainty, 2nd Edition, *Jossey-Bass*, 2011. [11] Weick, K.. E., Sutcliffe, K. M., and Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. In

	R. S. Sutton and B. M. Staw (Eds.), Research in Organizational Behavior, Volume 1 (pp. 81-123). Stanford: Jai Press

Encadrant(s)	Thierry Delpeuch (CNRS, PACTE), Eric Zamaï (Grenoble INP, G-SCOP)
Candidature	Envoyer CV, lettre de motivation avec recommandations de 2 référents (dont responsable de la formation), relevés de notes de M1 (obligatoire) et relevé de notes de M2 (si possible) à cyberalps-contact@univ-grenoble-alpes.fr Pour plus d'information sur le stage, contacter eric.zamai@grenoble-inp.fr ou thierry.delpeuch@ummrpacte.fr
Localisation	Laboratoire G-SCOP ou Laboratoire PACTE
Date de début	Février 2019
Durée	5 à 6 mois
Gratification	Selon réglementation en vigueur (env. 560€/mois). Possibilité de prise en charge partielle des frais de transport.

financed by
IDEX Université Grenoble Alpes