Convergence sûreté-sécurité des Systèmes de Contrôle Industriel

Mike Da Silva*[1], Pierre-Henri Thevenon[1], Stéphane Mocanu[2], and Maxime Puys[3]

[1]CEA, LETI – Commissariat à l'Énergie Atomique et aux Énergies Alternatives (CEA) - Grenoble – France

[2]Laboratoire d'Informatique de Grenoble – Centre National de la Recherche Scientifique : UMR5217, Université Grenoble Alpes, Institut polytechnique de Grenoble - Grenoble Institute of Technology, Centre National de la Recherche Scientifique, Institut Polytechnique de Grenoble - Grenoble Institute of Technology – France

[3]Laboratoire d'Informatique, de Modélisation et d'Optimisation des Systèmes – Ecole Nationale Supérieure des Mines de St Etienne, Centre National de la Recherche Scientifique, Université Clermont Auvergne, Institut national polytechnique Clermont Auvergne – France

Résumé

Les systèmes de contrôle industriel (ICS) sont conçus pour fournir un service, tel que la production d'électricité ou le traitement de l'eau, tout en protégeant les personnes, les biens et l'environnement. Aujourd'hui, les ICS évoluent en intégrant de plus en plus les technologies de l'information (IT), exposant ainsi leurs infrastructures aux cyberattaques. Cependant, contrairement aux technologies de l'information, les ICS présentent des risques et des contraintes en matière de sûreté et nécessitent des solutions de cybersécurité spécifiques qui empêchent les cyberattaques d'avoir un impact sur la sûreté du système. Dans cet article, nous présenterons les principaux mécanismes d'une méthode d'analyse de risque sûreté-sécurité que nous avons développé. Cette méthode permet d'identifier les vulnérabilités du système ainsi que leur impact sur la sûreté.

*Intervenant