
Extraction de signaux logiciels et matériels pour la résilience des réseaux d'énergie

Lalie Arnoud*^{†1}, Eric Gaussier^{‡2}, Pierre-Henri Thevenon^{§1}, and Victor Breux^{¶1}

¹Commissariat à l'énergie atomique et aux énergies alternatives - Laboratoire d'Electronique et de Technologie de l'Information – Direction de Recherche Technologique (CEA) – France

²Laboratoire 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

Résumé

Les infrastructures critiques que sont les réseaux d'énergie tendent de plus en plus à faire cohabiter des technologies opérationnelles (OT) dont le rôle est d'assurer la pérennité d'un processus industriel, avec des technologies d'information (IT) qui ont pour objectif de collecter et rendre disponible un grand nombre de données.

Cela les expose à de nouvelles vulnérabilités qui sont aujourd'hui exploitées par des groupes étatiques, mafieux ou politiques avec des objectifs pouvant aller de la rançon au sabotage à des fins de guerre.

La détection d'intrusion au sein des dispositifs des réseaux d'énergie apparaît alors comme une contre-mesure essentielle afin d'identifier une attaque et de la contenir avant que ses effets ne soient critiques.

Nos travaux de recherche proposent de considérer l'ensemble du système cyber-physique dans la détection d'attaques informatiques visant le procédé physique d'une installation énergétique, en analysant l'impact que ces attaques ont sur les signaux logiciels et matériels des dispositifs.

*Intervenant

[†]Auteur correspondant: lalie.arnoud@cea.fr

[‡]Auteur correspondant: Eric.Gaussier@imag.fr

[§]Auteur correspondant: pierre-henri.thevenon@cea.fr

[¶]Auteur correspondant: victor.breux@cea.fr