Cybersecurity of smart-grid control systems: Intrusion detection in IEC 61850 automation systems
Maëlle Kabir-Querrec, Stéphane Mocanu, Jean-Marc Thiriet, Eric Savary

To cite this version:

HAL Id: hal-01569875
https://hal.science/hal-01569875
Submitted on 27 Jul 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Cybersecurity of smart-grid control systems: Intrusion detection in IEC 61850 automation systems

Maëlle KABIR-QUERREC1,2, Stéphane MOCANU1, JEAN-MARC THIRIET1, ERIC SAVARY2
1 Univ. Grenoble Alpes, GIPSA-lab, F-38000 Grenoble, France
2 Euro-System, F-38760 Varcers, France

Abstract

- Cybersecurity problem in IEC 61850 power utility automation systems
- IEC 61850 standard scarcely takes into account the cybersecurity problem

Two main contributions of this PhD:
- Study of the standard requirements to propose an extension of the IEC 61850 information model to make possible handling of intrusion detection
- Development of a test bench dedicated to the study of cyber vulnerabilities of IEC 61850 automation systems, including attack generation and intrusion detection

Keywords: critical infrastructure security, industrial control system security, intrusion detection, IEC 61850, test bench, hardware-in-the-loop

Objectives

- Propose an extension to IEC 61850 data model: specification of an intrusion detection function
- Develop an intrusion detection system (IDS) for IEC 61850 automation systems:
  - Intrusion detection for GOOSE communication, a time-critical protocol
  - An IEC 61850 Substation Automation System (SAS) architecture resilient to attacks

Contributions

- Cybersecurity extension to IEC 61850 standard: specification of an intrusion detection function
  - Definition of an intrusion detection function model: managing traffic flowing over the network, extracting relevant features and verifying them, one packet at a time but also sequences of multiple packets, and finally generating alarms and reports.
  - Specification of all data elements: LNs, Data, Data Attributes, including logical connections between LNs (PICOM – Piece of information for COMmunication).

- Development of a test bench for the study of IEC 61850 cybersecurity
  - An attacker exploits GOOSE transfer mechanism and publishes broadcast false GOOSE packets mistakenly interpreted as valid from subscriber devices. [2]

Keywords: critical infrastructure security, industrial control system security, intrusion detection, IEC 61850, test bench, hardware-in-the-loop

References

[1] G-ICS [GreEn-ER Industrial Control system Sandbox] [1] is a teaching and research platform for ICS interoperability and cybersecurity. As part of it we develop a IEC 61850 test bench including off-the-shelf IEDs (Intelligent Electronic Device), a process simulator, supervision and engineering workstations, an attacker computer and a network analysis computer.
