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.archives-ouvertes.fr/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.
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

Context

IEC 61850 standard (Ed.1 2003, Ed.2 2013) “Communication networks and systems for power utility automation”:
• Preponderant for smart-grid deployment
• Dealing with digital management of control operations and electrical protection functions
• Information handling and transfer in the power grid automation system.

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

Info 61850 data objects are hierarchized following an object oriented structure. Catalogs of common objects for main Substation Automation System (SAS) functionalities are defined in the standard.

Information modeling

IEC 61850 data objects are hierarchized following an object oriented structure. Catalogs of common objects for main Substation Automation System (SAS) functionalities are defined in the standard.

Information modelng

IEC 61850 standard defines three protocols to be used in the Substation Automation System (SAS) according to the communicating entities and the real-time requirements.
1. MMS (Manufacturing Message Specification) is TCP/IP based and dedicated to communication between supervision and IEDs (Intelligent Electronic Device), Multicast protocol.
2. GOOSE (Generic Object Oriented Substation Event) is for inter-IEDs information transfer.
3. SV (Sampled Values) is used by sensors to publish measurements. Multicast protocol.

References