Cybersecurity of smart-grid control systems: Intrusion detection in IEC 61850 automation systems

Maëlle Kabir-Querrec, Stéphane Mocanu, Jean-Marc Thiriet, Eric Savary

Cybersecurity of smart-grid control systems: Intrusion detection in IEC 61850 automation systems

Maëlle KABIR-QUERREC[1,2], Stéphane MOCANU[1], JEAN-MARC THIRIET[1], ERIC SAVARY[2]

1 Univ. Grenoble Alpes, GIPSA-lab, F-38000 Grenoble, France
firstname.name@gipsa-lab.grenoble-inp.fr
2 Euro-System, F-38760 Varces, France
firstname.name@euro-system.fr

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

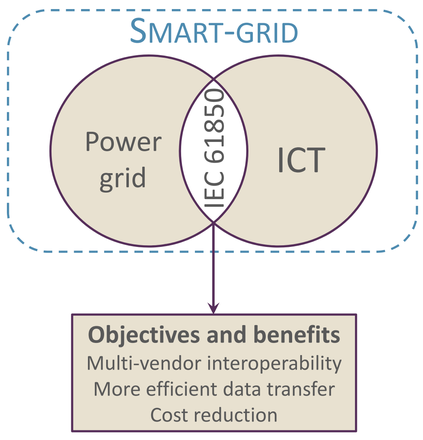

Fig. 1: IEC 61850, a smart-grid standard

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.

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.

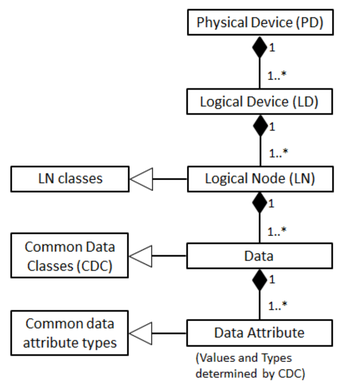

Fig. 2: IEC 61850 data object model

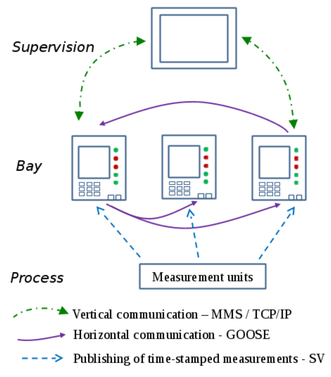

Fig. 3: IEC 61850 communication architecture

Information transfer

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.

Contributions

Cybersecurity extension to IEC 61850 standard: specification of an intrusion detection function

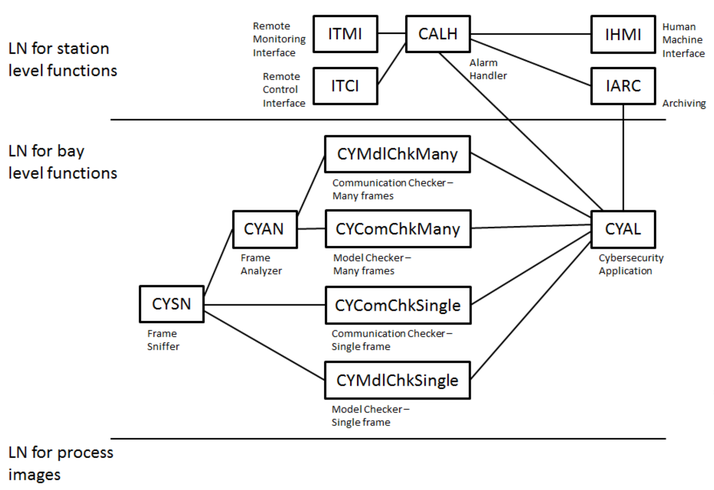

Fig. 4: IEC 61850 decomposition of a cybersecurity function into Logical Nodes (LN) on the different Substation Automation System (SAS) levels

- 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

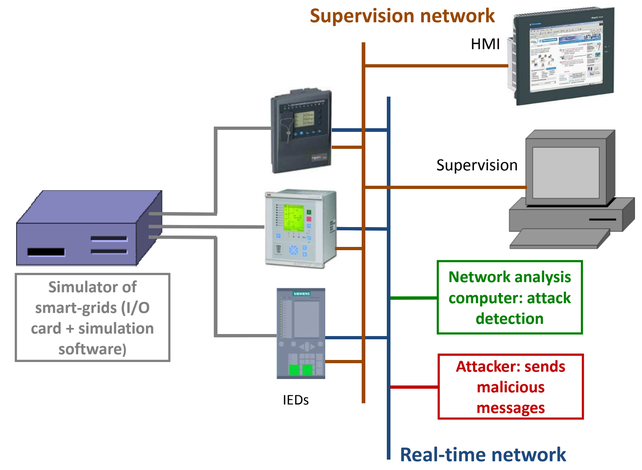

Fig. 5: Test bench for IEC 61850 systems cybersecurity

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.

An attacker exploits GOOSE transfer mechanism and publishes broadcast false GOOSE packets mistakenly interpreted as valid from subscriber devices. [2]

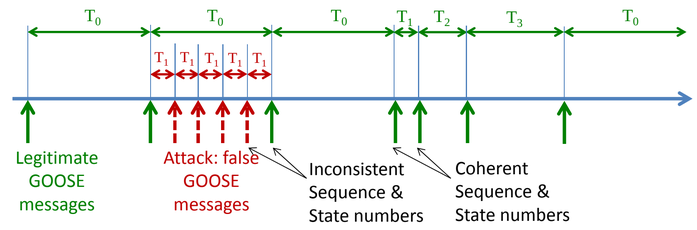

Fig. 6: Timeline of a legitimate GOOSE message transfer mechanism (green) and a spoofing attack

ts	src MAC addr	goID	stNum	sqNum	
88.181864	**:**:**:**:**:**	myIED/CB1/LLN0/Control_Dataset	1	1140	← Legitimate message
90.183886	**:**:**:**:**:**	myIED/CB1/LLN0/Control_Dataset	1	1141	← Legitimate message
90.207759	**:**:**:**:**:**	myIED/CB1/LLN0/Control_Dataset	2	0	← False message
92.185861	**:**:**:**:**:**	myIED/CB1/LLN0/Control_Dataset	1	1142	←

SqNum / StNum inconsistency

Fig. 7: Output of false GOOSE detection module

A network analyzer checks GOOSE messages integrity. Alarms are transferred to supervision where decision of entering a safe mode independent from GOOSE communication can be taken.
- Proof of concept with tcpdump, a linux packet analyzer.
- Final implementation in Bro, an open-source Network IDS. [3]

References

[1] G-ICS https://persyval-lab.org/en/platform/g-ics-sandbox-green-er-industrial-control-systems-sandbox

[2] Hoyos, J., Dehus, M., & Brown, T. X. (2012). Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure. 2012 IEEE Globecom Workshops.

[3] Lin, H., Slagell, A., Di Martino, C., Kalbarczyk, Z., & Iyer, R. K. (2013). Adapting Bro into SCADA: building a specification-based intrusion detection system for the DNP3 protocol. Proceedings of the 8th Annual Cyber Security and Information Intelligence Research Workshop.

Grenoble Images Parole Signal Automatique
UMR CNRS 5216 – Grenoble Campus
38400 Saint Martin d’Hères - FRANCE