A Test bed dedicated to the Study of Vulnerabilities in IEC 61850 Power Utility Automation Networks

Maëlle KABIR-QUERREC, Stéphane MOCANU, Jean-Marc THIRIET
Control department
GIPSA-lab (Grenoble Images Speech Signal and Control laboratory)
F-38000 Grenoble, France
Firstname.name@gipsa-lab.grenoble-inp.fr

Eric SAVARY
Euro-System
F-38760 Varces, France
Firstname.name@euro-system.fr

***Abstract*—Industrial control systems rely more and more on digital technologies. Although the cyber risk such technologies induce is widely judged as serious, especially for critical infrastructures, these systems have generally not been designed to serve cybersecurity purposes. Instead they were thought first for serving operational efficiency. It thus becomes critical to study cyber threats in industrial environments and experimental test beds are needed to evaluate risks, physical consequences of cyber incidents, and performance of countermeasures. The test bed we present here focuses on studying cyber risks and their mitigation in IEC 61850 power utility automation systems. The operational part is composed of engineering computers, supervision software, off-the-shelf intelligent relays (Intelligent Electronic Device – IED), a hardware-in-the-loop process simulation, and the cybersecurity tools include an attack generation station and a network analyzer. In this paper, we present the operational part, giving details on the power grid hardware-in-the-loop simulation and its importance in the understanding of cyber consequences on the global system. The article concludes giving preliminary experimental results showing consequences of a false data injection attack on a simple electrical architecture.**

Keywords—cybersecurity; IDS; smart-grid; test bed; hardware-in-the-loop; IEC 61850; electrical protection; false data injection

I. INTRODUCTION

The two last decades have given examples of blackouts caused by both informatics bugs [1] and cyber-attacks [2]. They make it plain that there is an urgent need of developing and deploying cybersecurity means to secure the smart-grid. There exist a wide range of them: some to be included at design time of products (e.g. secure boot of devices) and others to be set up when conceiving automation systems (e.g. Network-based Intrusion Detection System – NIDS). As available today, automation system technologies (relays, communication protocols, supervision software…) offer very few cybersecurity mechanisms for two main reasons: first because the threat is rather recent and Industrial Control Systems (ICS) often have a many-decade lifetime, and second because transposing security technologies from business field to industrial field is widely considered as difficult and not always relevant. Research is a necessity to develop cybersecurity methods and tools for ICS, and particularly for smart-grid control environments.

Such research cannot be run in real facilities and dedicated test beds help to discover cyber vulnerabilities in industrial control applications, to understand their possible impacts on the facilities, to develop cybersecurity solutions, to test and validate them. The test bed we are setting up specifically concerns Substation Automation System (SAS), which is responsible for electrical protection, i.e. the mechanisms ensuring infrastructure resiliency to electrical faults. Its components use Ethernet-based communication protocols, such as Modbus/TCP or more recently IEC 61850. Using such standard technologies introduces vulnerabilities in SAS, which if exploited may lead to consequences out SAS boundaries, as critical as a blackout for instance. The objective of this test bench is thus the study of cybersecurity in IEC 61850 communication networks and systems for power utility automation.

Section II of this article explains the basics of IEC 61850 electrical protection. Section III presents similar initiatives. Section IV describes the proposed test bed. A concrete example of an attack scenario is given in section V with experimental results. To conclude the paper, section VI gives an insight of the global research project this test bed is part of.

II. ELECTRICAL PROTECTION

Electrical protection role is to stem breakdown, to contain it and prevent it from spreading and causing a cascading failure. Protection is realized by SAS whose protection relays continuously monitor the state of the supervised electrical components and isolate them when they are subjected to serious disturbances such as short circuits. Protection mechanisms cannot prevent disturbances from occurring, they aim at limiting their impact instead. Their main purpose is to protect people from electrical accidents and power assets from damages (a three-phase short-circuit on medium-voltage bus bars can melt up to 50 kg of copper in one second), and to provide service continuity [3].

A. *Selectivity*

Selectivity is key to electrical protection, it is essential for maintaining service continuity. It consists in localizing and disconnecting the fault part of the power grid, and no more, while maintaining under power the greatest part of the architecture [4]. This is done by opening the circuit breaker (CB) immediately upstream to the fault and that CB alone. There are many selectivity methods, among which the two main are time-based and logical or communication-based selectivity. In Figure 1, the fault on transmission line A is observed by both protecting relays A and B. The relay the closest to the fault, A, is supposed to open its associated CB A if the fault is persistent. If relay B still observes the fault after a configured time-delay, it means that CB A has failed to trip and relay B opens CB B. In a wider application there could be C and D relays/CBs with longer time delays. Logical selectivity ensures a quicker isolation of the affected power assets because it does not rely on programmed time-delays: relay A sends a command to its upstream relay B to prevent it from tripping CB B. If the CB A fails to open and the fault still exists, relay A stops sending its blocking command to relay B that opens CB B.

In conventional protection systems, such logical selectivity blocking commands are transmitted from relay to relay through copper wires. In IEC 61850 design, these hard wired command signal exchange is replaced by a high speed inter-relay communication, thus reducing cost. In Figure 1, IED stands for Intelligent Electronic Device and denotes intelligent relay, that is a relay with digital capacities, especially an IEC 61850 relay.

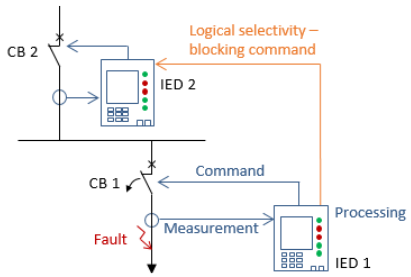

Fig. 1. Protection and selectivity systems.

B. *IEC 61850 high speed inter-relay communication*

Among the three IEC 61850 protocols, one is devoted to inter-IED high-speed information exchange: GOOSE (Generic Object Oriented Substation Event). To meet IEC 61850 standard requirements its end-to-end transfer time must be less than 4ms. This time-critical specification explains GOOSE implementation as an Ethernet Link layer-based protocol (mapped on ISO/IEC 8802-3): GOOSE messages are broadcasted over the Ethernet network, IEDs that need a specific-GOOSE message content must have been subscribed to it at configuration time of the substation. To ensure reliability of such communications, message publication follows a periodical mechanism: in stable conditions, the same information is published with a T0 period. When a data item changes, its new value is sent at a higher frequency, then publication rhythm progressively slows down back to stable conditions. Details about GOOSE protocol are given in the standard [5] and in [6].

III. Related Works

Literature is full of examples of test beds developed for cybersecurity of the smart-grid. Power grid simulation software with hardware-in-the-loop often serves the purpose of evaluating the performance of a developed tool. This is the objective of the experimental framework depicted in [7]-[8]: its end is to test the presented IDS (Intrusion Detection System). Simulink is used to run the virtual physical model of a transmission line. A communication module then manages Modbus communication with a PLC (Programmable Logic Controller) emulating a protection relay and performing the overcurrent protection algorithm. Similarly, the test bed set up for testing the IDS of [9] uses a Real-Time Digital Simulator (RTS), that is a commercial software for power grid simulation running on-the-fly to ensure a behavior as close to a real network as possible. Such real-time capabilities may be useful when evaluating time performance of the designed IDS. RTS simulation is hardwired to real relays and measurement units to avoid time delay induced by communication between process simulation and real devices. This solution is costly, though. Communication protocol in control network is Modbus/TCP too.

This second test bench is actually part of a platform developed at Mississippi State University (MSU) [10], which is very comparable to Idaho National Laboratory initiative [11] or the G-ICS lab (see next section) with its double objective, teaching and research in cybersecurity of many critical industries.

Test beds dedicated to cybersecurity in IEC 61850 systems exist but are not well documented. We can mention two initiatives from British Columbia Institute of Technology [12] and Freiburg Intelligent and Secured Systems Institute iSIS [13].

IV. Test Bed

Ense3 Grenoble Institute of Technology, together with GIPSA-lab (Grenoble Images Speech Signal and Control laboratory), has developed an experimental platform dedicated to ICS interoperability and cybersecurity, G-ICS (GreEn-ER[1] Industrial Control Systems Sandbox) [14]. The presented test bed comes as a part of G-ICS. Its objective is the study of cybersecurity in IEC 61850 communication networks and systems for power utility automation. It includes all typical components of a SAS:

- Ethernet network for supervision-to-IEDs and inter-IEDs communications.
- Off-the-shelf IEDs from diverse vendors: Current experiments use a bay controller, an overcurrent protection relay, a transformer protection relay and a feeder protection relay from two vendors. Other IEDs are available but have not been operated yet.
- Engineering workstations with configuration tools.
- Supervision applications (such as PCVue) and Human-Machine Interfaces (HMI).

1. *Grenoble Energy - Enseignement Recherche (Grenoble Energy - Teaching Research): a center of innovation for Energy field*

Regarding the process, that is the power grid, we do not have access to any real infrastructure (neither real-world one nor small-size laboratory one). But the process must be part of such a test bench dedicated to cybersecurity of the automation systems controlling it to comprehend possible impacts of cyber risks on the physical infrastructure. We thus made the choice of a feasible and affordable solution: hardware-in-the-loop simulation where electrical architectures are simulated by a software platform but still controlled and monitored by real off-the-shelf IEDs. Of course, such a solution helps understanding the system behavior but cannot give a complete representation of components interactions. A STM32-based I/O (Input/Output) card was developed by GIPSA-lab to ensure signal conversion between simulation and IEDs. Simulation software communicates with the I/O card over UDP for sending and receiving both analog and binary values to and from the IED physical connections. The card is wired to the IED binary I/O and to its measurement modules.

Regarding cybersecurity tools, an attacking computer is connected to the high-speed real-time network and launches false data injection and spoofing GOOSE attacks, and another computer runs our anomaly detection tool.

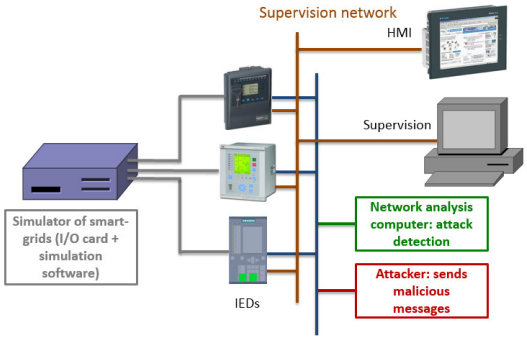

Fig. 2. IEC 61850 cybersecurity test bed.

V. Attack Scenario Example

A. Protection scenario

Let us consider a simple distribution substation from the typical substation topologies used as reference in the IEC 61850 standard [5]. These are classified by types (transformation or distribution) and size (small, medium, large) to be representative of worldwide substations. Figure 3 shows the considered distribution single-line diagram with an overcurrent protection and a backup protection. Logical selectivity as explained in section II is implemented here.

When an overload or a phase-to-phase short-circuit occurs downstream line 1, the associated protection relay IED 1 measures an overcurrent. It simultaneously sends a trip signal to CB 1, the CB directly upstream to the fault, and publishes a GOOSE message with the faulty current value and a Boolean variable to prevent CB 2 from opening. When CB 1 operating time has elapsed and fault is still present, meaning CB 1 has failed to open, or if CB 1 has an internal failure, IED 1 changes blocking Boolean variable to false. When IED 2 receives the corresponding GOOSE message, it sends a trip signal to CB 2.

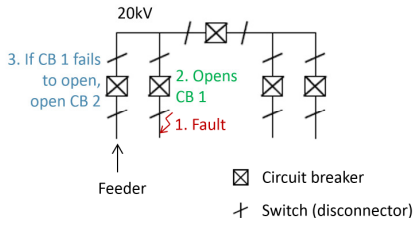

Fig. 3. Example of a distribution substation with overcurrent protection.

B. Risk analysis

The IEC 62351 [15] standard provides requirements about data and communication security in power systems. It points out the importance of risk assessment in the process of understanding cybersecurity risk and deploying countermeasures to target only pertinent assets and to the right level of security. No risk assessment methods or threat modeling has been developed specifically for substation communication, though. Attempts of assessing cyber risk in the smart-grid can be found in literature [16] and help to run such an analysis at the scale of a substation, first step of a global cyber risk analysis covering the distribution grid.

Cyber threats in IEC 61850 power utility automation systems include: malware insertion to modify IED programs or erase them, theft of credentials and passwords to launch malicious operations from work and supervision stations, communication integrity violation such as spoofing and false data injection…

Considering the simple distribution substation described in previous paragraph, we focus our risk analysis onto false data injection in the high-speed Ethernet network. Such an attack can cause CB 2 to trip inappropriately or conversely to not trip when it should. In case of an inappropriate trip, the whole substation is de-energized since CB 2 protects the incoming feeder line. If there is an electrical fault on line 1 and neither CB 1 nor CB 2 trips, fault is not isolated and possible consequences are physical damages to substation components (worst possible case being destruction) and/or substation breakdown.

Of course, we consider a single protection mechanism in this case study but a single IED may implement many and a substation has multiple layers of protection like concentric barriers so if an inner barrier fails next one takes over. All the electrical protection layers should be examined when assessing cyber risk with both success and failure outcomes of protection mechanisms.

C. Attack model

A fictive attacker wants to disturb the production of a factory. His/her target is then the substation responsible for powering the factory facilities, which topology is shown in Figure 3. We assume that the attacker can connect to the substation Ethernet network and sniff or send packets. We also assume he/she knows the substation GOOSE messages configuration. The attacker is thus able to read GOOSE

messages, forge new ones and inject them on the network for targeted IEDs to read them and use their malicious content. Attacker's objective is to de-energize the facility. He/she sniffs GOOSE packets of the substation until the situation of an overcurrent on line 1. He/she then injects GOOSE messages with the genuine current value (greater than configured overcurrent threshold) and Boolean variable "CB 1 Failure" as TRUE while its genuine value is FALSE. Attack timeline is depicted in Figure 4. Once IED 2 has read an attack GOOSE message it denies following genuine GOOSE flow because of mismatching message counters [5]-[6].

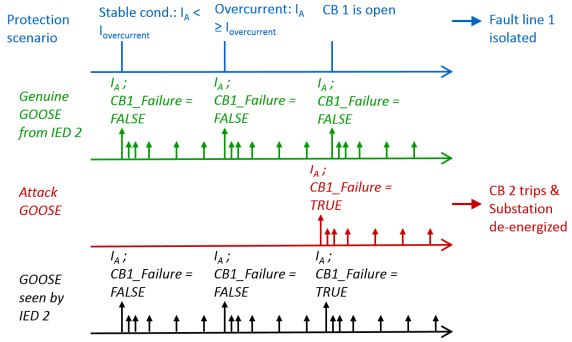

Fig. 4. Protection scenario, its associated genuine GOOSE communication published by IED 1 and GOOSE messages injected by the attacker.

D. Preliminary experimental results

Time	Source	Protocol
04.590774	:1c	GOOSE
05.003989	:1a	GOOSE
05.232881	:1c	GOOSE
06.285668	:1a	GOOSE
06.515010	:1c	GOOSE
07.640722	:1a	GOOSE
07.938807	:1c	GOOSE
07.950246	:1c	GOOSE
07.962112	:1c	GOOSE
07.983909	:1c	GOOSE
08.025609	:1c	GOOSE
08.107058	:1c	GOOSE
08.268311	:1c	GOOSE
08.589623	:1c	GOOSE
09.036434	:1c	GOOSE
09.042467	:1a	GOOSE
09.055043	:1a	GOOSE
09.067054	:1a	GOOSE
09.089230	:1a	GOOSE
09.130961	:1a	GOOSE
09.212629	:1a	GOOSE
09.231743	:1c	GOOSE

Fig. 5. GOOSE traffic during attack scenario.

Our protection scenario is simulated on Matlab, current values and CBs states are sent to IEDs over UDP initially and then when changing. IED commands to CBs are also transferred to the simulation in UDP packets. The described protection and attack scenarios are run. Figure 5 shows the resulting GOOSE communication captured with Wireshark protocol analyzer. First column is capture time. Source column gives the MAC address of publisher IED: the "1c" address is IED 1's and "1a" is IED 2's. Green messages from IED 1 corresponds to stable conditions with no fault and pale blue messages from IED 2 asserts CB 2 state is closed. Orange messages from t=7.938807s to t=8.589623s evidences an overcurrent with operating delay for CB 1 still going on. Attack message is highlighted by the red rectangle. It consequences is that IED 2 opens CB 2 and sends this new CB 2 state in the blue GOOSE messages. The orange message with capture time t=9.231743s is the next genuine message from IED 1. But it is too late, CB 2 has already been open and the substation is not powered any longer.

VI. Conclusion

Test beds are clearly needed for supporting research on cybersecurity in industrial environments such as power utility automation systems. The test bed presented here includes real IEDs for a hardware-in-the-loop simulation. It is part of a research project on intrusion detection in IEC 61850 networks. An experimental set up was required to validate tools and methods we developed (main one being an IEC 61850 NIDS) but further use is also possible for research and industrial purpose: penetration testing, vulnerabilities discovery, risk assessment, Factory Acceptance Testing, etc. Further development of the test bed includes more protection and attack scenarios with other protection functions and more complex systems, development of attacks exploiting the other IEC 61850 protocols, use of the other vendor IEDs available on G-ICS platform.

References

[1] G. Andersson et al., "Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance," in IEEE Trans. on Power Systems, 20(4), pp. 1922-1928, Nov. 2005.

[2] ICS-CERT, Alert (IR-ALERT-H-16-056-01), "Cyber-Attack Against Ukrainian Critical Infrastructure".

[3] Schneider, "Protection guide", 2006.

[4] Alstom, "Network Protection and Automation Guide", 2011.

[5] IEC 61850-2013, "Communication networks and systems for power utility automation"

[6] M. Kabir-Querrec, S. Mocanu, P. Bellemain, J.-M. Thiriet, and E. Savary, "Corrupted GOOSE Detectors: Anomaly Detection in Power Utility Real-Time Ethernet Communications," GreHack, 2015.

[7] M. Parvania, G. Koutsandria, V. Muthukumary, S. Peisert, C. McParland, and A. Scaglione, "Hybrid control network intrusion detection systems for automated power distribution systems," 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp. 774–779, 2014.

[8] G. Koutsandria, V. Muthukumar, M. Parvania, and Peisert, "A hybrid network IDS for protective digital relays in the power transmission grid," IEEE Smart Grid Communications (SmartGridComm), pp. 914–919, 2014.

[9] S. Pan, T. Morris, S. Member, U. Adhikari, and S. Member, "Developing a hybrid intrusion detection system using data mining for power systems," in IEEE Trans. on Smart Grid, 6(6), pp. 3104–3113, 2015.

[10] T. Morris, R. Vaughn, and Y.S. Dandass, "A testbed for SCADA control system cybersecurity research and pedagogy," Workshop on Cyber Security and Information Intelligence Research, 2011.

[11] Idaho National Laboratory "Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program," November 2008.

[12] H. Farhangi, "W4: Smart Grid Cyber Security," IEEE Smart Grid Communications (SmartGridComm), 2013.

[13] iSIS Available: http://isis.heia-fr.ch/EN/presentation/Pages/core-competences.aspx

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

[15] IEC 62351-2007 "Power systems management and associated information exchange - Data and communications security"

[16] L. Langer, P. Smith, and M. Hutle, "Smart grid cybersecurity risk assessment," International Symposium on Smart Electric Distribution Systems and Technologies (EDST), pp. 475-482, 2015.