Substation-Aware. An intrusion detection system for the IEC 61850 protocol.

Jose Antonio López*
Fundación Tecnalia research & Innovation
josea.lopez@tecnalia.com

Iñaki Angulo
Fundación Tecnalia research & Innovation
inaki.angulo@tecnalia.com

Saturnino Martínez
Fundación Tecnalia research & Innovation
satur.martinez@tecnalia.com

ABSTRACT

The number of cyberattacks against the Smart Grid has increased in the last years. Considered as a critical infrastructure, power system operators must improve the cybersecurity countermeasures of their installations. Intrusion Detection Systems (IDS) appears as a promising solution to detect hidden activity of the hackers before launching the attack. Most detection tools are generalist, designed to find predefined patterns such as frequency of messages, well-known malware packets, source and destination of the messages or the content of each packet itself. These tools also allow plugging modules for different protocols, offering a better understanding of the analysed data, such as the protocol action (read, write, reset...) or data model/schema understanding. However, the semantics of the data transmitted cannot be inferred. The Substation-Aware (SBT-Aware) tool adds the latest feature for primary and secondary substations, taking into account not only the protocols defined in the IEC 61850 standard, but the substation topology as well. In this paper we present the SBT-Aware, an IDS that has been developed and tested in the course of the H2020 SDN-microSENSE project.

CCS CONCEPTS

• **Smart Grid**; • **Intrusion Detection System**; • **Network Protocol**;

KEYWORDS

IEC 61850, Substation protection, Cybersecurity

ACM Reference Format:
Jose Antonio López*, Iñaki Angulo, and Saturnino Martínez. 2022. Substation-Aware. An intrusion detection system for the IEC 61850 protocol.. In *The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3538969.3543818

1 INTRODUCTION

Until a few years ago, the Smart Grid has been considered a secure infrastructure. However, the digitalization and the last world conflicts have increased the interest of the hackers for this infrastructure and, consequently, the number of cyberattacks have multiplied in recent years.

Since the hacker gains access to the communication network until the attack is launched can last 2 or 3 months [1]. This time is used by the hacker to collect information about computer systems, communications, and the power grid. The more knowledge the hacker has, the more damage can make [2], selecting the weaker points to, not only opening and closing switches, but spoofing and injecting false data as well, in order to grid operators take wrong decisions. As a result, companies must consider, in its comprehensive cybersecurity plan[3][4] continuous surveillance to detect the early stages which precede to the real attack and the Intrusion Detection Systems (IDS) appears as a promising solution to it.

An IDS monitors and analyzes the packets transmitted among the control devices and application systems that are connected to the communication network using different technologies like rules, patterns or machine learning [5]. Most of IDS are generalist, designed to find predefined patterns such as frequency of messages, well-known malware packets, source and destination of the messages or the content of each packet itself. More advanced tools incorporate plugging modules for different protocols, offering a better understanding of the analysed data [6], such as the protocol action (read, write, reset...) or data model/schema understanding. However, the semantics of the data transmitted cannot be inferred.

The IEC 61850 is an international standard for electric substation automation which includes, apart from several communication protocols, a data model and a substation configuration language (SCL). These two last features provide information about the topology of the substation and the configuration of all control devices that are deployed. In the course of the H2020 project, SDN-microSENSE, Tecnalia has been working in the development of the SBT-Aware, an IDS that incorporates substation knowledge to enrich the detection rules. The SBT-Aware is a specifically designed for primary and secondary electric substations to detect attacks to substation systems, devices and applications which uses the IEC 61850 series standards.

2 INTRUSION DETECTION IN THE SMART GRID ENVIRONMENT

An intrusion detection system is a device or software application that detects malicious activity in a communication network, as well as policy or configuration violations. It monitors traffic and checks it against an up-to-date database of known attack signatures or defined rules. When the IDS detects a suspicious activity, it notifies it to a top-level system like a SIEM (Security Information and Event Management) system. Intrusion detection system can be classified in two categories: network IDS, that analyse the data traffic in a section of the communication network, and host IDS that analyse the message into an IED. In the last years intrusion

ARES 2022, August 23–26, 2022, Vienna, Austria

ACM ISBN 978-1-4503-9670-7/22/08.
https://doi.org/10.1145/3538969.3543818

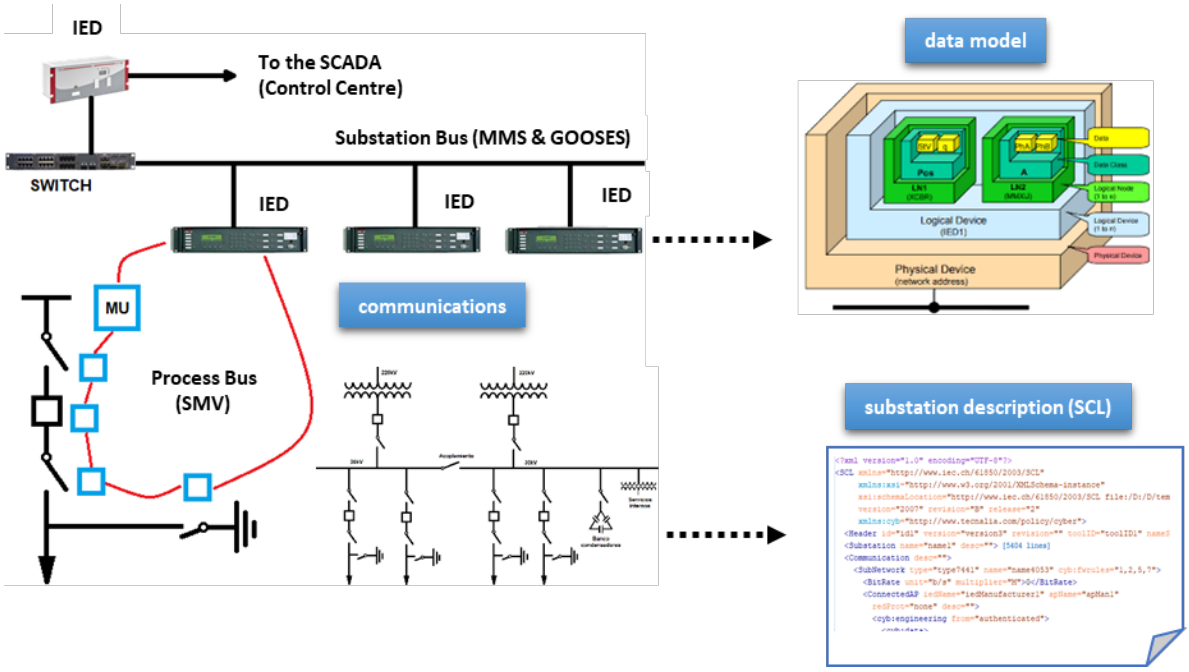

Figure 1: Elements of the IED 61850 standard.

detection systems have been used in the IT domain with relative success, on most of the cases oriented to the detection of malicious patterns in network traffic. The current threats against OT networks have motivated the use of these tools in industrial environments.

Among the most popular open source IDSs are SNORT, Suricata and Zeek. Suricata is a fork of Snort and has some improvements. It is currently the most widely used because it has good performance and a big community support generating new rules. It can act as an Intrusion Detection System (IDS) detecting only or as Intrusion Prevention System (IPS), detecting and dropping the anomalous traffic. Its functionality is also extendable through the creation of Lua scripts.

However, the main drawback of the Intrusion Detection Systems is that they are designed for IT protocols and, although most of them incorporate industrial protocols like Modbus or DNP3, their analysis focuses on the type of message being sent, the sequence of the messages or the source and destination addresses. A semantic analysis of the message content would provide more precision in the detection of hidden activity in a communication network. Fortunately, the IEC 61850 protocol does provide mechanisms to introduce semantic analysis into the detection rules used by these systems.

2.1 IEC 61850

IEC 61850 is the international standard for electric substation automation. It is oriented to facilitate the interoperability between application systems, like Supervisory Control And Data Acquisition (SCADA), and Intelligent Electronic Devices (IED), from different manufacturers. IEDs are electronical devices in charge of controlling and protecting the electrical assets installed in substations, such as switches, transformers, capacitor banks, etc. They have a high processing capacity which allows them to perform not only the functions related to the protection and control of the system, but also share information between them and the SCADA systems. In Figure 1 we can see the communication architecture of a primary substation, which is composed by a substation bus, that connects IEDs among them, and the process bus that connects the IEDs with the electrical assets. The figure also shows the three elements of the IEC 61850 standard that enables the interoperability of IEDs and SCADA: TCP/IP communication protocols [7], the data model and the SCL.

Three are the main **Communication Protocols** defined in IEC 61850: MMS, GOOSE and SMV:

The MMS (Manufacturing Message Specification) is a TCP based protocol used for client/server communications and buffered and unbuffered reports among IEDs and the SCADA.

The GOOSE (Generic Object Oriented Substation Event) is an Ethernet (layer 2) protocol used to exchange information between the IEDs about substation events. The objective of this protocol is to receive messages as soon as possible, with the lowest processing overload as possible.

The SMV (Sampled Measured Values) is also an Ethernet (layer 2) protocol designed to replace multiple analogic cables [8] by a single Ethernet cable to carry electric values, therefore it is used in the process bus. The data (I, V, phases) are linked to timestamps and transmission frequency depends on the samples per period (SPP). According to IEC 61850-9-2LE [9] recommendations for 50 Hz systems, 80 SPP must be used. It must publish a packet every (1/50)/80 seconds (250 microseconds). But for 60 Hz systems, 256

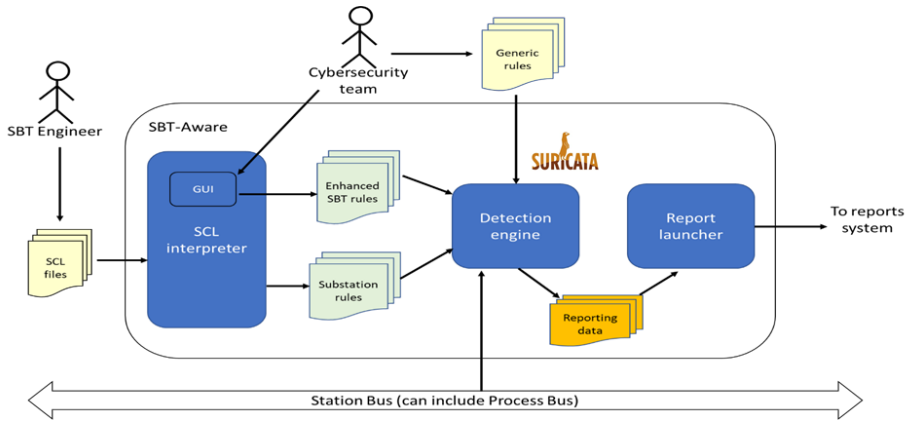

Figure 2: SBT-Aware tool, including modules, I/O data and relevant actors

SPP are needed, sending a packet every (1/60)/256 seconds (65 microseconds).

The second element of the IEC 61850 is the **Data Model**, which provides a unified vision of the objects and functions of any IED. The data model is very important for two reasons: it allows the auto-description of the substation components, and it enables the interoperability and the interchangeability of devices.

Finally, the **Substation Configuration Language** provides a mechanism for the description of the substation and its components. Described in XSD (XML Schema Definition) the standard defines several types of configuration files. The more interesting for the intrusion detection purpose are the IED Capability Description (**ICD**) file, containing the data templates, data types, and logical nodes implemented by each device, and the Substation Configuration Description (**SCD**), that contains the electrical topology of the substation, the connected IEDs and the information interchanged among them.

2.2 Improving the intrusion detection process with the IEC 61850. The SBT-Aware.

As previously mentioned, one of the main limitations of the intrusion detection systems is that they do not analyse the semantic content of the messages. One reason is because most of industrial protocols does not define a data model used in the communication messages. Unlike other protocols, the IEC 61850 does define a data model that, together with the configuration language, allows us to know which information is transmitted between the different components (IEDs and SCADA) of a substation. This feature introduces two clear advantages in the detection process. On the one hand, the IDS could incorporate this knowledge in the detection rules to detect those operations, and requested data, that does not comply with the data model. On the other hand, the IDS will be customized to a particular substation. This is the essence of STB-Aware, an IDS specifically designed to detect illegal activity in the IEF 61850 protocol.

As can be seen in Figure 2., the SBT-Aware extracts the semantic knowledge from the configuration files, and incorporates it into Suricata, an open-source intrusion detection system, improving the detection process. Any activity in the communication network of the substation that differs from what it is specified in the configuration files is considered by SBT-Aware as suspicious to be done by an intruder.

SCL-Interpreter reads the SCD and ICD files, to infer all data that can be encapsulated into the messages (reports, GOOSE and MMS) and transforms them into a set of rules that are included in the detection engine (Suricata). The Detection Engine analyses the messages that are transmitted in the communication networks (Substation Bus) to detect any discrepancy between the transmitted messages and the rules generated by the SCL interpreter. If a discrepancy is detected, the Report Launcher sends an alarm to a centralised SIEM (Security Information and Event Management).

Two actors have been included in the diagram: the SBT engineer and the Cybersecurity team. The SBT engineer is responsible for designing and configuring the substation; the person who composes the SCD file or generates one CID file for each IED. The cybersecurity team can add additional security information to be included in the detection rules following the security policies of the electric company.

In the Defense in Depth (DiD) strategy, where the security of a substation follows the onion model, we can locate the STB-Aware in the inner layer. In Figure 3., this approximation is translated to its corresponding IEC 61850 substation elements. The hacker will first try to connect to the communication network (substation bus) circumvented logical perimetral controls like firewalls or access control. Once there, it will try to access a device (IED), sending messages to an application (logical Device) to manipulate the data handled by that application (electrical measures or operational states).

3 GENERATING DETECTION RULES BASED ON IEC 61850

The first step in the configuration of the STB-Aware is the rules generation. This process is carried out by the SCL-Interpreter, an XML parser that processes the Substation SCL files (IEC61850-6, -7.2 [10], -7.3 [11] and -7.4 [12]), to extract the relevant information that will be included in the detection rules. Table 1 shows the information that is extracted from the SCL files.

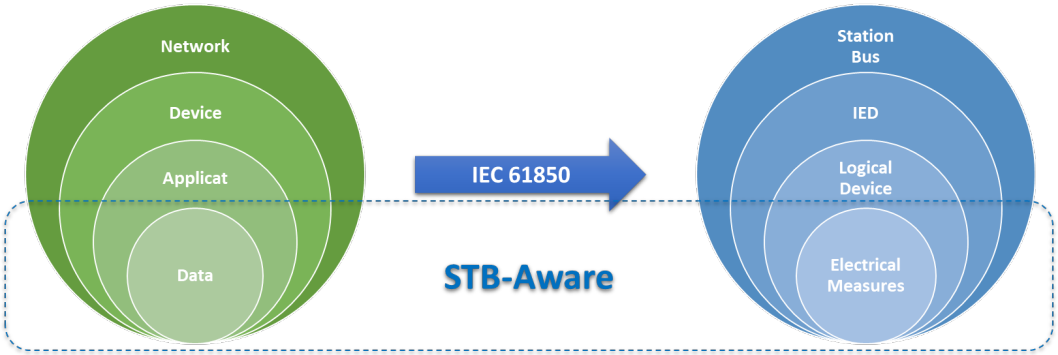

Figure 3: Defense in Depth for devices and for an IEC 61850 substation

Table 1: Information extracted from the SCL files

SCL Section	Content extracted
<Communication.Subnetwork.ConnectedAP>	All the devices connected to the different communication networks within the substation: IED IP address, IED identification, . . .
<IED.Services>	Services offered by each IED: data model, data sets, reports, . . .
<DataTypeTemplates.LNodeType>	Data types generated by each IED, and data type the IED is subscribed from other IEDs
<IED.AccessPoint.Server.LDevice.LN and LN0 nodes>	Elements that can appear as attributes in substation messages

An important weakness of Suricata is that it looks for malicious patterns within the traffic, having an internal database with those patterns. For conventional attacks, whenever a message complies with one pattern within the database, an alert is launched. However, in the case of the rules generated by the SCL-Interpreter we have to apply the inverse detection, which means that any message that complies with the generated patterns should be considered a valid message, and the alarm should be launched when the message from/to the IED, logical device, logical node, data object, data attribute and functional constraint is not found in the database.

To solve this limitation in Suricata, a rule in Lua has been implemented to raise alerts in inverse detection scenarios. Automatically, one rule and one script are generated for each IED containing the IP, the logical device, logical node, and the accessed object, including its functional constraint (FC). The script parses the captured MMS packet and compares the requested object or report with the approved list extracted from the SCL files.

Figure 4. shows an example of the mapping between a SCL file and Lua detection rules. On the left side of the figure, we can see the configuration information of an IED in the SCL file, which is parsed by SBT-Aware to create the detection rules automatically in Lua language, on the right side of the figure. These rules are used for checking origin/destination IP, for enabling the defined reports, and for reading/writing logical nodes (circuit breakers, disconnectors, I/O signals, analogical data, etc.). IP addresses are collected from the ***<Communication>*** element, where the IEDs serve data in their connected networks by means of their access points. Reports are collected from the LLN0 element and the data model for MMS messages are retrieved from each logical node.

In real time, if the object or report requested is not present in the configuration, Suricata writes an alert in its log system. This log is structured as JavaScript Object Notation (JSON) format which includes general information and the reason. The general information includes the timestamp, packet number, physical Ethernet interface, number of packets, and IP/port source and destination. The reason of the log entry contains the severity of the alert and a descriptive text, such as “Accessed object not included in the substation configuration”, “Unknown IP accessing data”, etc. This information will be useful for the cybersecurity team analysis.

4 SBT-AWARE VALIDATION

The validation of the SBT-Aware has been done in Tecnalia’s Cybersecurity Laboratory for the Smart Grid (Figure 5.), which contains two commercial IEDs, a Substation Control Unit (SCU), and a substation SCADA (HMI). All these components are connected to the substation bus together with an additional PC which emulates the hacking activity, and one server containing the SBT-Aware. The process bus is simulated with the help of an OMICROM 256 which provides substation electric measures. SBT-Aware is also connected to the substation bus through a TAP (Terminal Access Point), a hardware device that is placed between two points to monitor the network traffic that flows between those two points. Finally, the hacker activity is simulated by a KALI LINUX also connected to the substation bus.

Figure 4: Mapping between SCL files and Lua detection rules

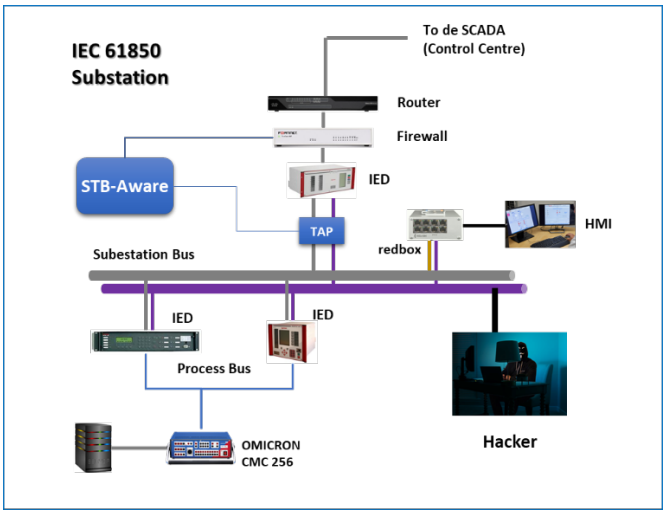

Figure 5: STB-Aware testing environment.

The test cases shown in Table 2 have been implemented to validate the SBT-Aware. In the first two test cases the hacker launches the attack from a Kali Lunix looking for information about other IEDs. In the third and fourth test cases the hacker has gained access to the HMI.

These four test cases have been sequentially executed in a scenario with a delay of 2 minutes among them. Figure 6 shows the packets sniffed from the substation and the packets detected by the SBT-Aware. By average, there are about 13 MMS packets per second, along with their corresponding TCP messages (SYN, ACK, etc.) in the normal communication, which are reports between the two IEDs and the clients (SCADA and SCU).

As we can see at the left of the Figure 6, the test cases 1a and 1b were detected by SBT-Aware because the origin of the MMS request came from a non-defined IP. As expected, test case 2a did not fire any event because the origin was requesting data defined in the substation (the same information which could be requested from, for example, the SCADA). However, the test case 2b requested the data object associated to one circuit breaker which is present in the IED data model, but it is not used in the substation. For this reason, the SBT-Aware detects and reports it.

5 BENEFITS OF THE SOLUTION

As we have mentioned before, most detection tools are generalist, designed to find predefined patterns. The solution presented in this paper incorporates substation domain knowledge in the detection rule creation process, which provides several advantages:

The detection rules are created automatically extracting the information from the SCL files.

Rules are specific to each individual substation.

The tool is in the deepest layer of the DiD strategy; if a hacker has managed to enter in the station bus, its actions still can be detected.

Any change in the configuration of an IED can be easily detected and the substation operator can be warned.

Connections of external devices or systems, for example during maintenance tasks, are also detected.

It can be used to configure, not only the detection rules of an IDS, but other protection tools like Firewalls.

Unlike machine learning approach, a training period is not necessary

It reduces false positives, avoiding alerts which are not attacks or IDS misconfigurations

6 CONCLUSIONS AND FUTURE WORK

In this paper we have presented SBT-Aware, an intrusion detection system focused on the IEC 61850 protocol that uses the substation configuration files to create automatically detection rules for hidden

Table 2: Test Cases implemented

No	Test case description	Obtained Result
1a	The hacker consults an IED element configured in the SCD from a device NOT included in the configuration file.	SBT-Aware detects the illegal connection of the hacker.
1b	The hacker consults an IED element NOT configured in the SCD from a device NOT included in the configuration file.	SBT-Aware detects both, the illegal connection of the hacker and the illegal request to an IED element not included in the SCL.
2a	The hacker consults an IED element configured in the SCD from a device included in the configuration file.	SBT-Aware considers that this action is correct as the action comes from a valid element and request information of an existing IED element.
2b	The hacker consults an IED element NOT configured in the SCD from a device included in the configuration file.	SBT-Aware detects the illegal request to an IED element not included in the SCL.

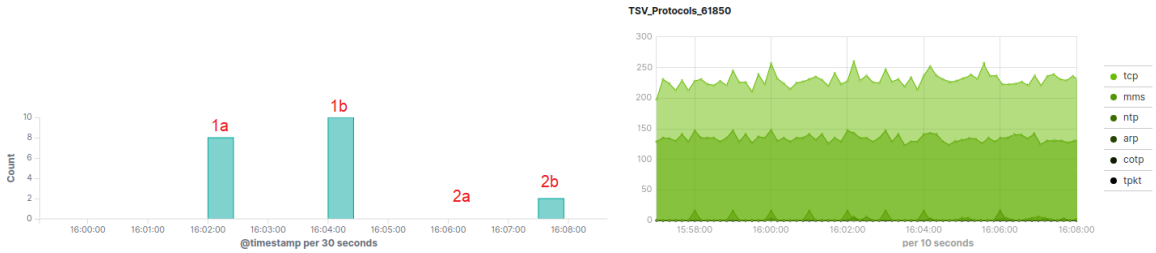

Figure 6: Test case results

hacker activity inside a substation. SBT-Aware extracts information about the topology and components of a substation from its SCL configuration files and uses this information to create intrusion detection rules specific for this substation. SBT-Aware incorporates Suricata as the Detection Engine. The solution has been validated in a lab environment demonstrating its effectivity in several test cases where a hacker tries to obtain information from the substation devices. The work presented in this paper can be extended in two directions: to extent the information contained in the SCL files and to extend the detection rules to the GOOSE and SMV protocols.

The IEC 61850 standard allows that any SCL can be extended by any other model. It is made by extending the tBaseElement to add any element (xsd:Any) or any attribute (xsd:AnyAttribute). This extension allows utilities to introduce into the SCL files cybersecurity policies to be applied in the applications and devices. For example, user roles, encryption key management, Disaster Recovery Plans for one IED, switch, network and even the whole substation, etc.

SBT-Aware uses Suricata, which is IT protocols oriented and it is not able to apply rules to layer 2 of the OSI model protocols. It is precisely in this layer where the GOOSE and SMV messages are transmitted, which means that it is not possible to detect any anomalies in these messages. Tecnalia is developing a detection engine which analyse layer 2 messages allowing us the extension of the functionality.

ACKNOWLEDGMENTS

The research presented has been done in the context of SDN-microSENSE project. SDN-microSENSE has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833955. The information contained in this publication reflects only the authors' view. EC is not responsible for any use that may be made of this information.

REFERENCES

[1] Marie Baezner, Patrice Robins. Cyber and Information warfare in the Ukrainian Conflict (version 2). 2018. Center for Security Studies (CSS), ETH Zürich.
[2] Yingmeng Xiang, Lingfeng Wang, and Nian Liu. Coordinated attacks on electric power systems in a cyber-physical environment. Electric Power Systems Research, Vol. 149, August 2017, pages 156-168.
[3] Wenye Wang, Zhuo Lu. Cyber security in the Smart Grid: Survey and challenges. 2013. Computer Networks. https://doi.org/10.1016/j.comnet.2012.12.017
[4] Tagarev, Todor; Sharkov, George. Computationally Intensive Functions in Designing and Operating Distributed Cyber Secure and Resilient Systems. 2019. International Conference - Ruse, Bulgaria. Proceedings of the 20th International Conference on Computer Systems and Technologies - CompSysTech '19 - Computationally Intensive Functions in Designing and Operating Distributed Cyber Secure and Resilient Systems. DOI:10.1145/3345252.3345255
[5] Shuva Paul, Zhen Ni, and Chaoxu Mu. A Learning-Based Solution for an Adversarial Repeated Game in Cyber–Physical Power Systems. 2020. IEEE Transactions on Neural Networks and Learning Systems. Volume: 31, Issue: 11, Pages: 4512 – 4523. Nov. 2020. DOI: 10.1109/TNNLS.2019.2955857
[6] Wei Huang, Tianyi Zhang, and Xinwei Yao. Optimization for sequential communication line attack in interdependent power-communication network. Physica A: Statistical Mechanics and its Applications. Vol. 592,15th April 2022
[7] Wei Huang. Learn IEC 61850 Configuration In 30 Minutes. 2018 71st Annual Conference for Protective Relay Engineers (CPRE). 26-29 March 2018. DOI: 10.1109/CPRE.2018.8349803
[8] David Dolezilek, David Whitehead, and Veselin Skendzic. 2011. Integration of IEC 61850 GSE and Sampled Value Services to Reduce Substation Wiring. Presented at the 47th Annual Minnesota Power Systems Conference Brooklyn Center, Minnesota. November 1–3, 2011
[9] IEC 61850-9-2. Communication networks and systems for power utility automation – Specific communication service mapping (SCSM) – Sampled Values over ISO/IEC 8802-3.
[10] IEC 61850-7-2. Communication networks and systems for power utility automation – Basic information and communication structure – Abstract communication service interface (ASCI), IEC International Standard, Edition 2.0, 2010-08

[11] IEC 61850-7-3. Communication networks and systems for power utility automation – Basic information and communication structure – Common data classes, IEC International Standard, Edition 2.0, 2010-08

[12] IEC 61850-7-4. Communication networks and systems for power utility automation – Basic communication structure – Compatible logical node classes and data object classes, IEC International Standard, Edition 2.0, 2010-03.