EnergyShield pilot at Turin DSO

Whitepaper

2022

iren

IRETI

CSP
innovazione nelle ICT

Authored by:
Gianluca Serale, Giuseppe Carnevale, Stefania Sella, Alessandro Armellin, Emiliano Roggero

ENERGY SHIELD

EnergyShield pilot at the electrical energy distribution grid of Turin

> "
>
> *The increasing adoption of connected devices that drives cyber-security is to become a crucial asset of Distribution System Operators*
>
> *Sergio Manno,*
>
> *Head of IRETI's electrical network SCADA system*

IN A NUTSHELL

The Iren Group participated to the European project EnergyShield that aims at developing & testing an integrated cyber security toolkit for the energy sector.

Iren participated in the project by providing a case study where testing the tools developed in the project with a particular focus to anomaly detection and security behaviour analysis tools.

The case study is the electrical distribution grid of the city of Turin including the grid operators (employees of Ireti, a company controlled by Iren managing the grid) and a primary substation converting High Voltage to Medium Voltage.

Results were used to strengthen the cybersecurity approach of the company facing the problem in a holistic manner. Cybersecurity is expected to become more and more crucial in the very next years since the digitalization of the grids increases the sources of threats and risks.

CONTEXT

Cybersecurity is becoming more and more important in several industries and contexts. This aspect is particularly true in the Electrical Power and Energy System (EPES) sector since it represents a critical infrastructure for any other business.

Distribution System Operators (DSOs) are the entities and companies responsible for distributing and managing energy from the generation sources to the final consumers. The DSO operates and maintains Medium Voltage (MV) and Low Voltage (LV) grids, substations for the conversion of voltage (e.g., HV/MV or MV/LV), and the fiscal metering system.

Digitalisation is a key pillar for the evolution of the DSO business, which requires investments in automation, smart meters, real-time

systems, big data, and data analytics. Nevertheless, without a proper approach with cyber and asset security the huge amount of data that might be generated on the distributed assets of a grid might represent a threat. Indeed, smart and connected devices might represent a backdoor in the Information and Communication Technologies (ICT) of the DSO representing a potential access for malicious hacker attacks.

The IREN Group operates as a DSO the electrical grid of three important municipalities in the Northwest of Italy (Turin, Vercelli, and Parma) serving an area with a population of over 1.1 million inhabitants. For this reason, IREN is fully committed in the research and innovation regarding cybersecurity in the EPES sector.

The IREN Group participates as a partner of the Energy Shield project that has been funded within the Horizon2020 scheme. The aim of the project is capturing the needs of EPES operators and combining the latest technologies for vulnerability assessment, supervision, and protection to draft a defensive toolkit. In the project, IREN is one of the two operators providing real environment pilots to assess the technologies devised during the project including IRETI's assets and personnel as testbeds.

IREN is supported in the EnergyShield project by CSP a research and consulting centre specialized in the ICT sector.

TECHNICAL DETAILS

IREN and IRETI are in charge of the Italian Pilot of the EnergyShield project with the support of CSP for the informatic aspects. The Italian Pilot is divided in two primary Use Cases named IT_01 and IT_02. Moreover, support to partners developing EnergyShield tools is also provided.

The Use Case IT_01 is focused on testing the "Security Behaviour Analysis" (SBA) tool provided to SCADA AMI systems operators and people involved in sensitive roles within IRETI organizational structure. The test is provided to the over 250 people operating in the units of IREN and IRETI that cover relevant roles for DSO cyber-security (i.e. the entire cybersecurity and tele-control departments, the over 200 employees of the electrical distribution grid). Indeed, those people are the ones that are more relevant for the cybersecurity aspects of the company, especially in OT.

The Use Case IT_02 is focused on testing the Integration of the "Anomaly Detection" (AD) module on SCADA systems for attack or anomaly detection (e.g., on primary switches) even if SCADA system is bypassed or offline and using Artificial Intelligence predictive maintenance purposes. The tool is tested in the infrastructure of the municipality of Turin with a special focus on the Martinetto primary substation.

The Turin MV electricity network has ten HV/MV substations operated by IRETI that are the inter-changing points between the Transmission System Operator (TSO) and the DSO. One of those

substations, the Martinetto substation, was selected during the project to install the hardware necessary to test the EnergyShield AD tool, the so called SigaBox provided by SIGA. The Martinetto substation is divided in five MV lines (22kV according to Italian regulation). Each of them operates at a nominal current value of 400 A (typical operation values around 80-100 A and maximum applicable load 8000 A).

ENERGYSHIELD DEMONSTRATOR

The SBA tool was tested targeting a pool of Iren and Ireti employees covering roles significant for the cybersecurity in the EPES sector. Three questionnaires assessing competences, attitude and know-how were prepared and submitted to all the people involved in OT of the Electrical Distribution DSO and telecontrol units of the ICT department. The tests were submitted to approximately 260 employees and the response rate was very significant, reaching 48.7% (the target was overtaking 35% that was an internal benchmark of typical Iren's employee response rate to surveys). The results were evaluated by the EnergyShield partner National Technical University of Athens (NTUA) in an anonymized form. Employees were clustered over several verticals such as year of experience, assumption date, instruction level, seniority level, etc. The tests will be coupled with a simulation of phishing campaign to assess the ability of employee to apply theoretical concepts to ordinary working life.

The AD tool was tested into the Martinetto HV/MV primary substation. The test consisted in the installation of the AD tool designed by the Israelian EnergyShield partner Siga, an electrical cabinet named Siga Box. IRETI designed and devised the connectivity among the SigaBox and the grid. The SigaBox is supplied as a closed box with all the hardware components installed and pre-wired inside, with terminals ready to be connected to the electrical signals from the transducers. The installation included transducers and voltage/current converters to gather values from the field and transforming them into data that can be processed by the SigaBox. ICT and cybersecurity departments provided the cellular connectivity and the integration with IREN firewalls and security tools. The peculiarity of the Siga AD tool is the ability to gather direct measurements from the field monitoring the situation even in case of penetration of the IT system (e.g., SCADA telecontrol of the network). The system was installed in September 2021 and the following months were used to assess a baseline working condition of the IRETI's substation. Tests are planned for May 2022 to simulate the occurrence in field of faults and misfunctioning. The goal of those tests will be assessing the ability of the Siga Box to individuate problem and communicating to the OT operators the countermeasures to be performed.

BEST PRACTICES & LESSONS LEARNED

Many reports show that the losses to cybercrime are enormous, and it is necessary to invest in training [1] of company employees. Cybersecurity as praxis is by now a well-known idea in EU law and practice, established in a multitude of legal texts and formal policies that are almost a decade old [2]. The implemented model is described by scientific studies, defined and necessary in the EPES sector [3].

The results of the SBA campaign will be used to plan an educational campaign and to improve the company culture targeted to cybersecurity topics. Moreover, if area of critical weakness will be detected the efforts of the cybersecurity team will be spent to reduce any potential risk affecting those areas.

The AD detection tool test represented a great opportunity to IREN and IRETI to self-question about the cybersecurity level of its substations. Indeed, the great amount of data generated by the field might represent not only a great opportunity of smart grid development but also a potential risk of cyber penetration.

The EnergyShield project was the opportunity of an internal discussion about such topics and a comparison with other best practice undertaken by various companies in the European EPES sector.

AVAILABLE LITERATURE

[1] Edyta Karolina Szczepaniuk, Hubert Szczepaniuk, Analysis of cybersecurity competencies: Recommendations for telecommunications policy, Telecommunications Policy, Volume 46, Issue 3, 2022, 102282, ISSN 0308-5961

[2] Vagelis Papakonstantinou, Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?, Computer Law & Security Review, Volume 44, 2022, 105653, ISSN 0267-3649,

[3] Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures INNOVATION ACTION H2020 Grant Agreement Number: 83290, WP2 - VULNERABILITY ASSESSMENT & SECURITY BEHAVIOUR ANALYSIS, D2.2 UPDATED SECURITY CULTURE FRAMEWORK AND TOOL (https://energy-shield.eu/wp-content/uploads/2020/10/EnergyShield_D2.2_Updated_security_culture_framework_and_tool_v1.0.pdf)
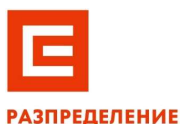
ABOUT THE COMPANIES

IREN is one of the largest Italian multi-utilities. IREN is active in several sectors such has electrical energy production, distribution, and commercialization, waste and water management, energy efficiency of buildings, district heating, gas trading and distribution.

IREN owns IRETI that is the DSO of three urban areas in Northwest Italy (Turin, Vercelli, and Parma). IRETI operates over 7.700 km of electricity grid in High (HV), Medium (MV), and Low (LV) voltage. The grid consists in 15 primary substations converting HV/MV and about 4.300 secondary substations converting MV/LV. IRETI dispatches over 4.100 GWh of electrical energy annually. The company, as a DSO, coordinates operational and maintenance activity on-field, the remote control of the network (e.g., SCADA system), the physical security of the assets and the emergency interventions in case of outages.

CSP is a non-profit research organization based in Piedmont – Italy with 20+ years of experience in working on IC, applied research & technology. CSP is an acknowledged laboratory by the Italian Ministry of University and Research. The mission of CSP is to transfer outputs to local communities, enterprises, SMEs, government offices. Main contact: innovazione@gruppoiren.it

SIMAVI
Software Imagination & Vision

PSI

SIGA
OT Solutions

foreseeti

L7DEFENSE

konnektable
TECHNOLOGIES

TechInspire
Inspire for innovation

KTH
VETENSKAP
OCH KONST

CITY
UNIVERSITY OF LONDON
EST 1894

iren

ESO EAD

РАЗПРЕДЕЛЕНИЕ

K3

SC Software Company Ltd
Developing quality software solutions since 1996

MIG23
turnkey engineering

GOLDLINE

HPP LENISHTA