Cyber-Attack Detection at Turin's Primary Substation

Contents

Background

As part of the European Union (EU)'s Horizon 2020 program, SIGA has taken part in the Energy Shield project for the development of an integrated cybersecurity solution for the vulnerability assessment, monitoring, and protection of critical energy infrastructures. This project is conducted by a consortium of over 15 partners, including cyber-security service providers, academic institutions, and electrical utilities suppliers from all over Europe. In this project, SIGA was responsible for developing an Anomaly Detection (AD) tool for Electrical Power and Energy Systems (EPES), based on its level 0 SigaGuard technology.

Following the completion of the development phase, SigaGuard was installed and tested in two operational pilot sites, one is a substation owned by IRETI, a prominent electricity distribution organization in Italy. IRETI is a part of the IREN group, an Italian multiutility energy company, that was also a partner with SIGA in the Energy Shield project. The test outlined in this report was conducted in a dedicated testing area in one of IRETI's HV/MV sub-station, located in the city of Turin, Italy in June 2022.

The MV (Medium Voltage) electricity grid of Turin's metropolitan area was selected as this project's case study as it is a significant substation managed by IRETI. The grid consists of about 2000 km of MV lines, over 2500 km of LV (Low Voltage) lines and over 550,000 Points of Delivery in LV. Every year over 2700 GWh of energy are dispatched by IRETI. The Turin grid has 10 HV/MV (High Voltage/Medium Voltage) substations that are the interchanging points between the TSO (Transmission System Operator) and the DSO (Distribution System Operator).

The challenge

IRETI decided to focus the Italian pilot on the MV as it raises serious cybersecurity concerns. The aim of the pilot is to evaluate the most effective solutions (hardware and software options, organizational approaches, changes in the procedures and staff qualification) to face malicious cyber-attacks to DSOs and EPES sector in the most effective way. SigaGuard was implemented to monitor the operation of 5 different lines of the substation (circuit breaker and current measurement in each line) and the main bus bar (voltage measurements). Nine different attack scenarios were launched against IRETI's control sub-systems, all of which were detected and alerted by SigaGuard's Machine Learning (ML) algorithms.

This report outlines the environment in which the test was conducted along with various attacks launched on the tested control systems. Each attack scenario is thoroughly described together with an in-depth overview of SigaGuard's detection process.

Test set-up (part 1)

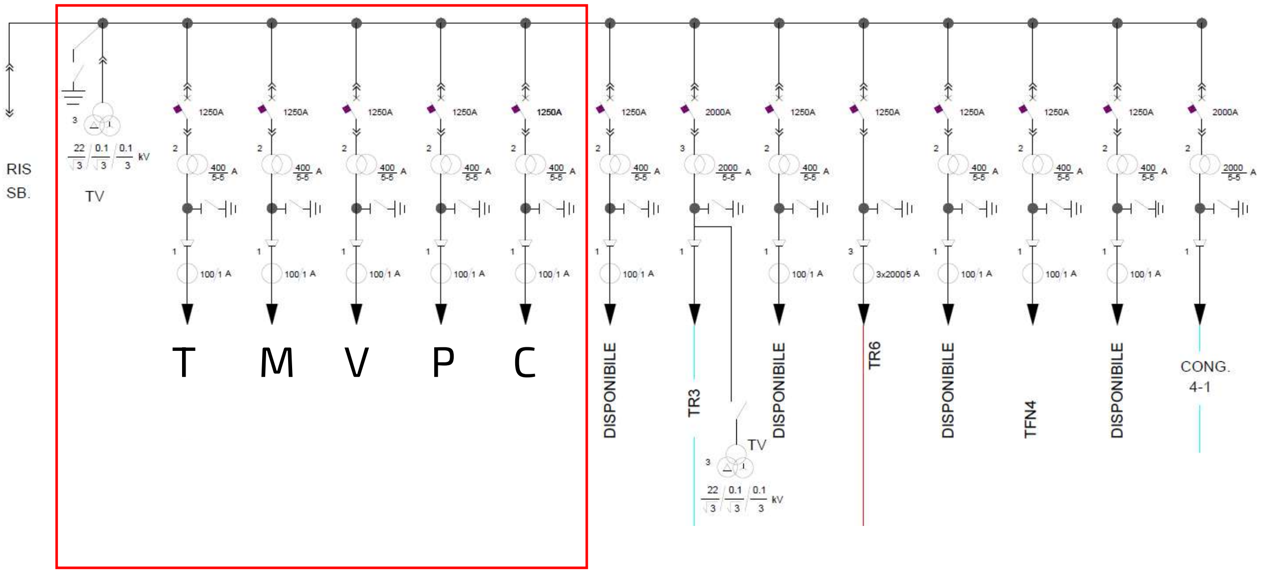
The tested substation is a HV/MV substation located in Turin (Italy) and is one of 10 HV/MV substation operated by IRETI as an inter-changing point between the Transmission System Operator (TSO) and the Distribution System Operator (DSO) in Turin. The substation is divided by 5 MV (220V according to the Italian regulation) lines listed as follows: line T, M, V, P, and C. Each line operates at a nominal current value of 400 A (typical operation values around 80-100 A and maximum applicable load 8000 A). Every line has a protection CB (Circuit Breaker) and a current measurement transmitter.

The connection between the HV and the MV grid in the substation is performed by large step-down transformers that reduce the voltage from high voltage (220 kV) to medium voltage (22 kV). On top of the measures mentioned above, the substation has capacitors for grid reliability installed. The substation is equipped with hardware components to control and monitor the on-field variables and auxiliary protections in-charge of transmitting data to the main SCADA system.

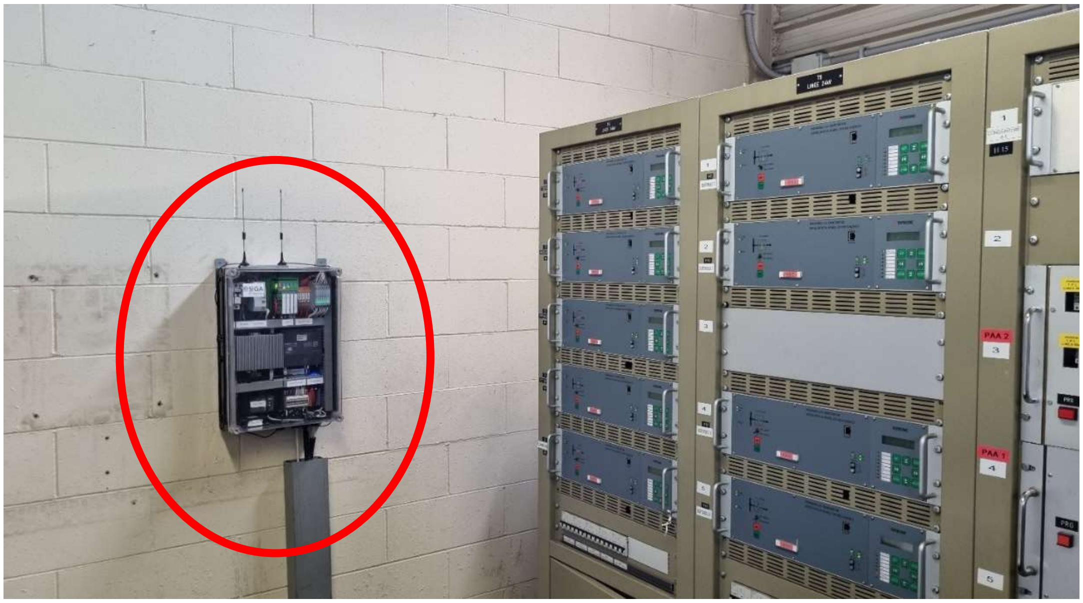
SigaGuard was installed in the tested substation to monitor the process operation of the 5 lines mentioned above - the most critical components of the asset. SigaGuard is connected to 13 IOs (Input/Output) in the substation, which are the electrical signals between the controller and the field devices (input signals from sensors, circuit breakers status etc. and output signals for commands to actuators, circuit breakers, etc.).

Test set-up (part 2)

The below diagram sketches the substation's parts monitored by SigaGuard (marked in a red frame):



SigaGuard was installed in the tested substation in August 2021, when IRETI's team installed the SigaBox (SigaGuard's hardware platform) and connected it to the substation's protection and control systems. The learning period started right afterwards. Once the learning period was completed the ML models of SigaGuard were activated, detecting anomalies caused by abnormal behavior of the substation's processes.



Test structure

In June 2022 a cyber test was conducted by IRETI's team to test SigaGuard's capabilities of alerting cyber-attacks on the physical processes. The test consisted of multiple manipulations to the physical processes of the substation to simulate cyber-attacks. Various attacks were launched (each with several variants) by IRETI's operators, some were conducted physically on the substation's systems and some other attacks were performed from the control room by using the main control system. The test consisted of 5 different cyber-attack scenarios, tested by 9 distinct cyber-attacks simulations:

Scenarios
1. "SolarWinds" Vulnerabilities / Supply Chain Attack – Malware inserted to legitimate SW update/patch or to the supplied equipment itself
2. "Aurora" Vulnerability – Changing process logic without crossing thresholds
3. HMI spoofing ("Stuxnet/ Irongate") – Spoofing the HMI to show a different situation than what is actually happening in the physical assets
4. Attacker is gaining access to the OT network via legitimate credentials
5. Direct access to OT assets

Test results

No.	Attack Scenario	Attack sequence	Source of Simulation	Start time	Alert Time	Result
1.1	A	Main busbar voltage increase (ascending by 275V each step)	Signal simulator	11:10	11:11	Alerted immediately after the second step change
1.2	A	Main busbar voltage increase (decending by 275V each step)	Signal simulator	11:48	11:48	Alerted immediately after the first step change
1.3	A	Main busbar voltage increase (ascending by 275V each step)	HMI	11:57	11:59	Alerted immediately after the second step change
1.4	A	Main busbar voltage increase (decending by 275V each step)	HMI	12:04	12:05	Alerted right before the second step change
2	B	Manipulating line's CB sequence of operation	Signal Simulator	13:37	13:37	Alerted immediately
3.1	C	Changing circuit breaker status without visibility in HMI (2 cases with different values)	Signal Simulator	14:09	14:09	Alerted immediately
				14:14	14:14	Alerted immediately
3.2	C	Changing circuit breaker status without visibility in HMI	Physical	14:26	14:29	Alerted immediately
4	D	Line current increase	HMI	15:25	15:28	Alerted immediately
5	E	Circuit breakers manipulation	Physical	15:26	15:26	Alerted immediately

Summary

The sequence of the attacks was carefully planned and executed by IRETI's engineering team, focusing on the main cyber scenarios which affect the real operation of substations with either false reports or no reports at all to the control level.

These scenarios were meticulously designed to test SigaGuard's capabilities considering its unique POAD (Process-Oriented-Anomaly-Detection) solution based on Level 0 data which cannot be tempered nor masked.

The tests' outcome was defined to measure the percentage of detection events, the time measured from the attack initiation to the first detection, and the assurance level of the detection based on the number of models detecting the attack.

Based on the learnt data, SigaGuard has detected all nine attacks - some were detected instantly while some were detected in a matter of seconds from the time the anomaly started to evolve. All attacks were identified by multiple models indicating the high probability of SigaGuard's efficient and quick detection of such attacks.

By detecting all the cyber-attacks scenarios launched, SigaGuard has demonstrated its outstanding abilities and enormous potential to alert on cyber-attacks on critical assets in the power and electricity sector, by using POAD based on Level 0.

About SIGA

SIGA's provides a Process-Oriented OT Cybersecurity for real-time decision-making capabilities for managing all Incident Response phases of an OT cyberattack – including Detection, Containment and Cyber Forensics. Unlike other solutions, SIGA detects all expressions of a cyber-attack based on its unfiltered view of all Levels of Cyber OT, including Level Zero visibility.

Founded in 2014, SIGA has global customers in multiple sectors including Oil & Gas, Power Utilities, Data Centers and Water.

For more information visit:
www.sigasec.com