Overcoming Cybersecurity Gaps in the Energy Sector:

How to Address Stuxnet-Type Scenarios Using Level-0 Monitoring

White Paper Published by:

SIGA Level Zero OT Resilience | New York Power Authority

November 2021

Executive Summary

The New York Power Authority (NYPA) is America's largest state power organization, with 16 generating facilities and more than 1,400 circuit-miles of transmission lines.

NYPA identified cyberattacks as a major threat to its operations in the coming years. As a result, NYPA established the Advanced Grid Laboratory for Energy (AGILe) lab as a Cyber Security center that will "allow researchers to study the impacts and challenges of cyber incidents on the grid."1 The lab was largely designed to identify and mitigate threats as part of a long-range plan to minimize risk.

NYPA and SIGA OT Solution, a leading OT cybersecurity company, formed a collaboration in 2019 as part of a New York State economic development partnership. NYPA's cyber division—together with the AGILe team—aimed to reduce the risk of cyber-attacks on its production facilities. The main objective of the collaboration is to reveal otherwise undetectable cyber threats—such as Stuxnet-type scenarios—using advanced electrical signal

A three-phase plan was laid out to explore these scenarios:

- Phase 1- demonstrated the ability to detect various anomalies without interrupting the operations.
- Phase 2- demonstrated the ability to identify all tested attacks (including Stuxnet) on a substation controller. The success rate was 100% with a detection time of no more than a few seconds.
- Phase 3- is planned for 2021-2022 with field implementation at NYPA's operational facilities.

1 nypa.gov/innovation/digital-utility/agile-lab

Background

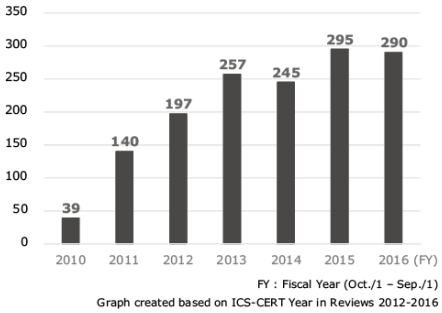
Current Climate

The industrial world is becoming more and more digital. An increasing number of companies' operations are automated: from field sensors to controllers, data & interface computers and networks, to executive-level decision-making and reporting tools. More and more industries and services have become so dependent on one another that a disruption in one could cause failure/disruption in another.

Infrastructure is defined as critical when disrupting its function could lead to a significant socio-economic crisis with the potential to undermine the stability of a society, causing political, strategic, and security consequences2.

This digital realm, due to its rapid development and growth, began with little protection. While locks and keys were once sufficient, today we need a new set of cutting-edge digital tools to safeguard assets, operations, and public safety.

Operation Technology (OT) Cyber Protection is all about protecting an organization's operations from malicious attacks.



The number of critical infrastructure cyber-attacks worldwide is increasing. 1

Operation Technology (OT) Cyber Protection is all about protecting an organization's operations from malicious attacks.

Cyber Threats to Industrial Facilities (OT) and Critical Infrastructure

The following list includes some of the recent high-profile industrial cybersecurity incidents

2010 Iran / Stuxnet

Malware attacked industrial control program in Iran's Natanz uranium enrichment base.

2017 A.P. Maersk

Shipping and Logistics Ransomware: NotPetya, 2 weeks operation disruptions. COST $300 million

2015 Blackenergy

Ukraine power grid attacked, by invading grid control center. 225K customers without power .

2018 Saudi Aramco

Oil and Gas, OT-Specific Malware: TRITON, Business and process disruption, revenue loss of $1B.

2016 Duke Energy

Electric Power Company Failure to Meet Regulated Cyber Security Standards. COST $10 million.

2019 Norsk Hydro

Metals and Mining, CYBER INCIDENT, reduced its output by 50%. Ransomware: LockerGoga. COST $70 million

1 https://www.nypa.gov/innovation/digital-utility/agile-lab
2 Critical Infrastructure Protection against Cyber Threats, Lior Tabansky, Military and Strategic Affairs, Vol. 3, No. 2, Nov 2011.

Current Research and Key Targets

As part of a long-term plan to minimize risk, NYPA and SIGA planned a three-phase operation to validate the SigaGuard solution for the detection and prevention of specific-related cyber-attack scenarios on NYPA's assets and facilities.
The key objectives were to identify attack vectors unaddressed to date in the OT cybersecurity solution market and demonstrate how Level-0 monitoring using the SigaGuard solution provides the capability to identify these attacks and display meaningful alerts to operators.

The Need to Address the Security Gap of Field-level Devices (Level 0)

Control systems in commercial, industrial, and critical infrastructures employ a combination of commercial off-the-shelf human-machine interfaces and communication networks with field devices, such as process sensors, actuators, and field-level network drives. The Purdue Model represents an organization's network divided into five levels: Level 5 is the internet DMZ. Level 4 is the organization's corporate network. Level 3 is the manufacturing zone or main control center that communicates with HMI control points at Level 2. These Level 2 HMIs interact with Level 1 controllers and Level 0 field devices.

From a cyber perspective, Levels 1 to 5 consist of traditional Information Technology (IT) cyber solutions, comprised of servers, workstations, switches, routers, and firewalls. However, at Level 0, the environment is considerably different. Controllers (PLCs) dictate the physical space, communicating with machinery via current and voltage signals. That is why cybersecurity at Level 0 must be regarded differently.
Traditionally, cybersecurity in OT environments has taken a top-down approach—achieved by first building digital walls around the digital assets and then identifying malware and network anomalies in the IP networks (network anomaly detection) to ensure that data has not been compromised. The IT approach has been expanded to address control systems by monitoring OT control system Ethernet networks.

Why Do Stuxnet Scenarios Remain an Unresolved Issue in OT Cybersecurity?

The network-monitoring approach is essential, but not sufficient for securing control systems and preventing severe damage to OT equipment and machinery. This is because network monitoring will never be able to fully cover the real assets of the OT architecture: the physical equipment and processes (aka, Level-0 devices). Network cybersecurity anomaly-detection systems assume that process sensors provide secure, authenticated input, however, no cyber security or authentication functionality exists in these devices or device networks. Legacy control system devices have no cybersecurity or authentication options, nor do they identify which control system devices (e.g., pumps, valves, motors, relays, etc.) are
vulnerable to network attacks.

Closing the Gap

Monitoring the electric signals transmitted directly from critical assets is a viable and reliable method for detecting malicious cyber-attacks on operational machinery and equipment. Unlike Intrusion Detection Solutions at the network levels—which are often "blind" to the actual process—monitoring and diagnosing the unfiltered and unhackable electric signals directly from Level 0 can deliver bulletproof protection to mission-critical operational assets.
Many cyber-attacks, such as Stuxnet, Irongate, and the most recent cyber-attacks on industrial control systems, highlight the vulnerability of global OT infrastructures. Monitoring at Level 0 ensures operational resiliency—even when cyber-attacks are successful in manipulating the logic of ICS controllers, or when malware blinds operator dashboards.

Testbed Environment

NYPA's AGILe Lab simulated an actual substation in the state of New York using a Real-Time Digital Simulator (RTDS) and a Real-Time Automation Controller (RTAC) set up as a controllable hardware-in-the-loop (CHIL) with RTDS served as the substation controller for the testbed.
The SigaGuard platform was connected in the lab to the simulated substation field devices and acquired the real-time process data. The simulated substation was operated using actual demand data to mimic real-world loading conditions and served as the training phase. During the test, actual attack scenarios on the system were performed.

The testbed set up included the following steps:

1) **Test setup** – SigaGuard was configured and connected according to the IOs of the substation, tested and verified.

2) **Simulating normal behavior** – The Testbed substation was controlled by the RTAC based on field data simulated in RTDS for a period of 2 weeks.

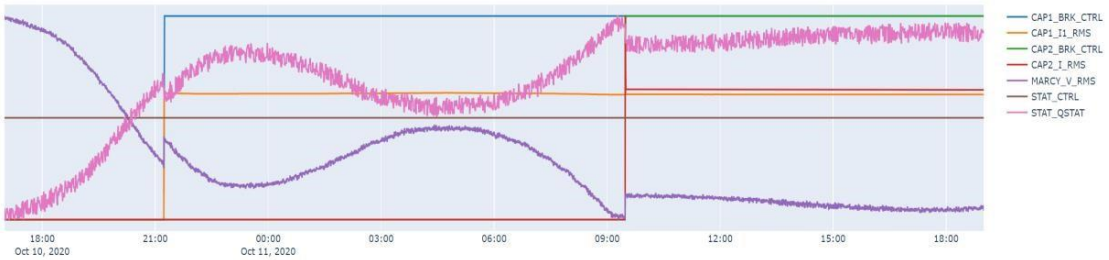
3**) Learning period** – SigaGuard learned this data as the normal behavior of the substation using its proprietary Machine Learning (ML) algorithm engine.

4**) Attack and detect** – NYPA AGILe lab and cyber team worked on one end and generated various Stuxnet-like attacks while SigaGuard identified all of these attacks and reported them to the operators.

Learning Period

Data Collection

SigaGuard, through its parallel connection in the field, collected real-time data from the field devices (as simulated by the RTDS) and controlled devices (as set by the RTAC).
The RTAC monitored voltage and current signals from RTDS and issued STATCOM setpoints as well as capacitor ON/OFF commands. The RTAC was programmed to simultaneously issue STATCOM setpoints at 60-second intervals and independently switch the capacitor banks to maintain the bus at its rated voltage when it experienced varying loading conditions.
The following figure illustrates an example of 24 hours of normal operation.



Data Processing

The SigaGuard ML algorithm engine aggregated the testbed data for a period of about two weeks and learned this data as the normal behavior of the sub-station.

Execution: Cyber-Attacks on RTAC

Four different cyber-attacks on the RTAC, simulated by the NYPA AGILe Lab team, were performed one after another. In real-time, the SigaGuard detected each attack and issued alerts on the SigaSight Dashboard and via e-mails to the NYPA AGILe team. Once SIGA detected the attack and a quick overview of the alerts in the dashboard, the AGILe team moved on to the next attack.

Attack #1: RTAC Reboot Attack

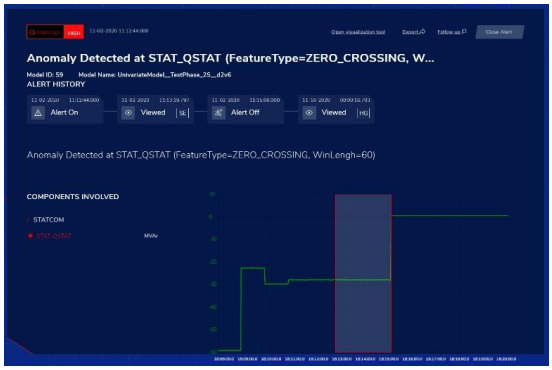
Attack Objective: To evaluate the effect of a compromised RTAC that has shut down while the RTAC is operational.

Attack vector: The attack involved a rogue agent gaining access to the RTAC and issuing a reboot command.

Detected at: The attack was detected around 1 minute after the RTAC reboot. (The value for the command from the RTAC is calculated every minute.)

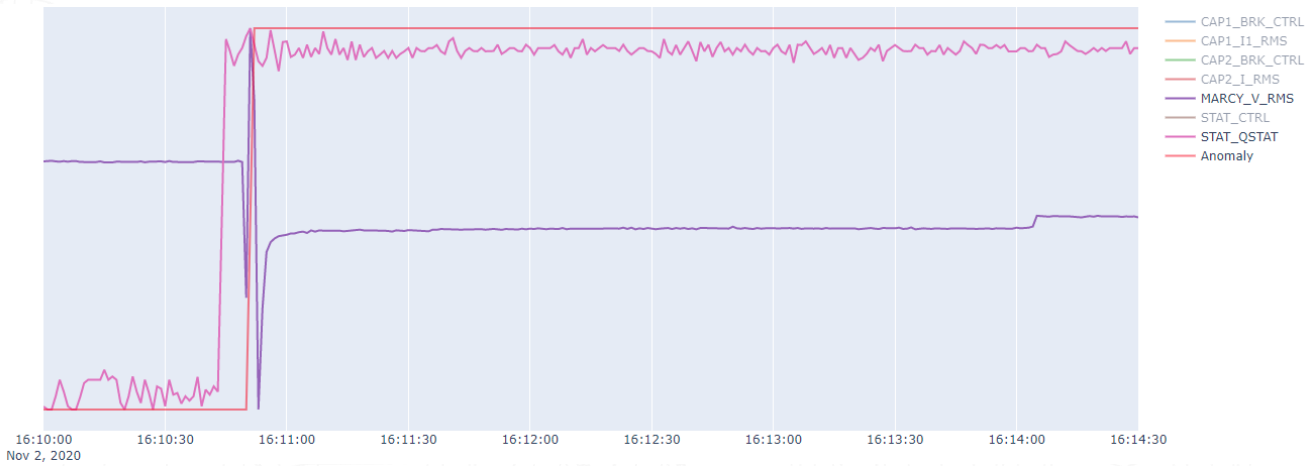
Detection: Siga alerted on two results from the attack. The operator alarms are displayed on the SigaGuard dashboard.

Rapid disturbance in RMS Voltage (V_RMS)



Frozen values in STATCOM Qref SIGNAL (STAT_QSTAT)

Attack Process Details: The graph below shows the process trend of the attack. The red line represents the detection time.



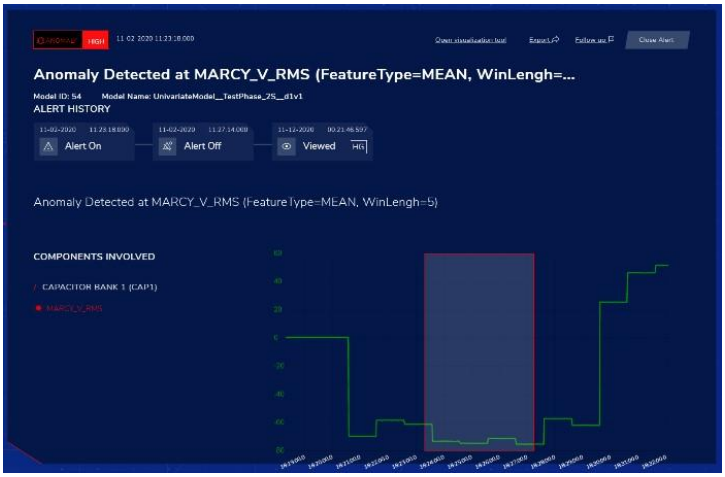
Attack #2: Invalid Input Attack 1 – Capacitor Banks

Attack Objective: To evaluate the effect of a compromised RTAC that its programming has been changed.

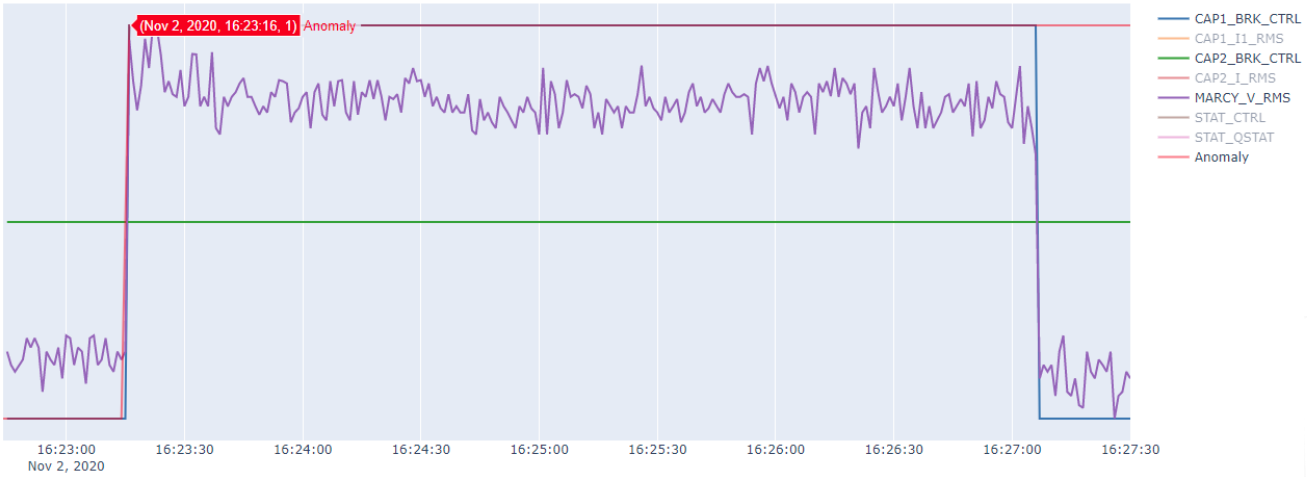
Attack vector: The attack involves a rogue agent gaining access to the RTAC and manipulating its operating logic to issue wrong CAPACITOR operation commands, thereby disturbing the bus voltage (V_RMS) from its stable operating point.

Detected: Immediately after the attack.

Detection: SIGA alerted on the anomalous behavior with multiple alerts from different areas of the process. The first anomaly is shown on the SigaGuard dashboardare displayed on the SigaGuard dashboard.



Attack Process Details: The graph below shows the process trend of the attack. The red line represents the detection time.



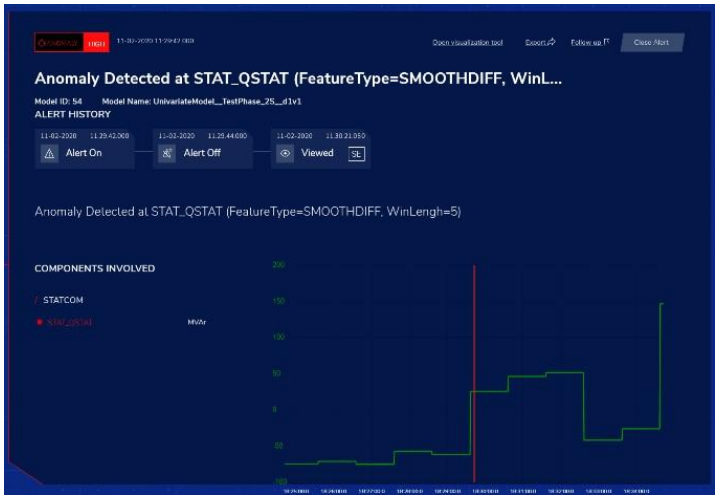
Attack #3: Invalid Input Attack 2.1 – 20% STATCOM Setpoints Increase

Attack Objective: To evaluate the effect of a compromised RTAC whose programming/parameters were changed.

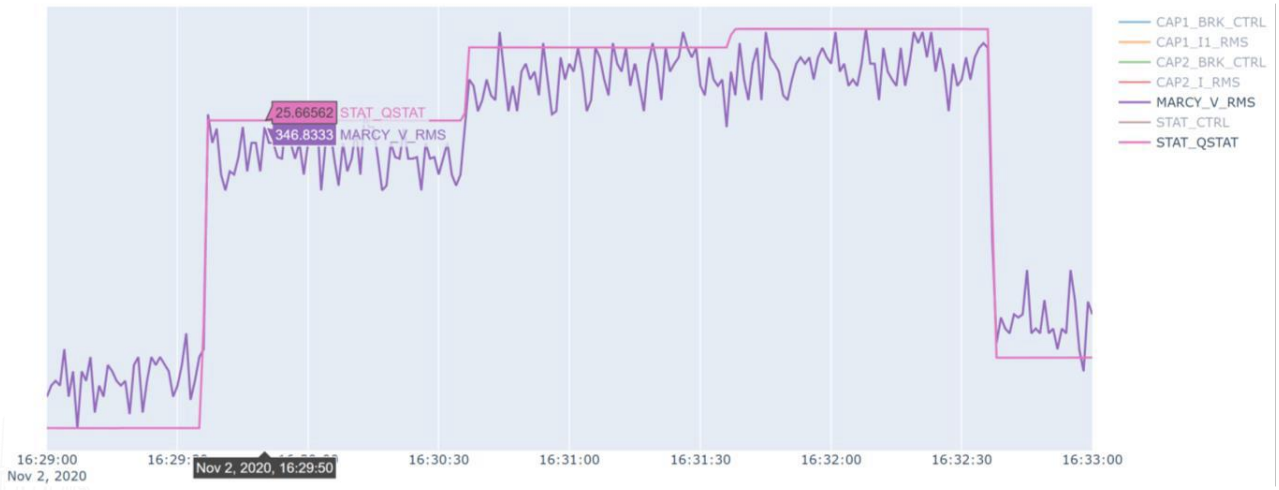
Attack vector: The scaling attack involves a rogue agent gaining access to the RTAC and manipulates its operating logic/parameters to issue STATCOM setpoints 20% more than its actual value during normal operations.

Detected: Immediately after the attack.

Detection: SIGA's first alert was issued right away for the anomalous behavior of STATCOM Qref SIGNAL (STAT_QSTAT) and appeared on the SigaGuard dashboard. Other related alerts followed.



Attack Process Details: The graph below show the process trend of the attack.



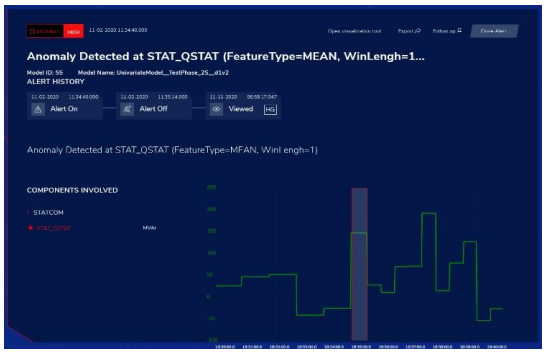
Attack #4: Invalid Input Attack 2.2 – Random STATCOM Setpoints

Attack Objective: To evaluate the effect of a compromised RTAC whose programming/parameters were changed.

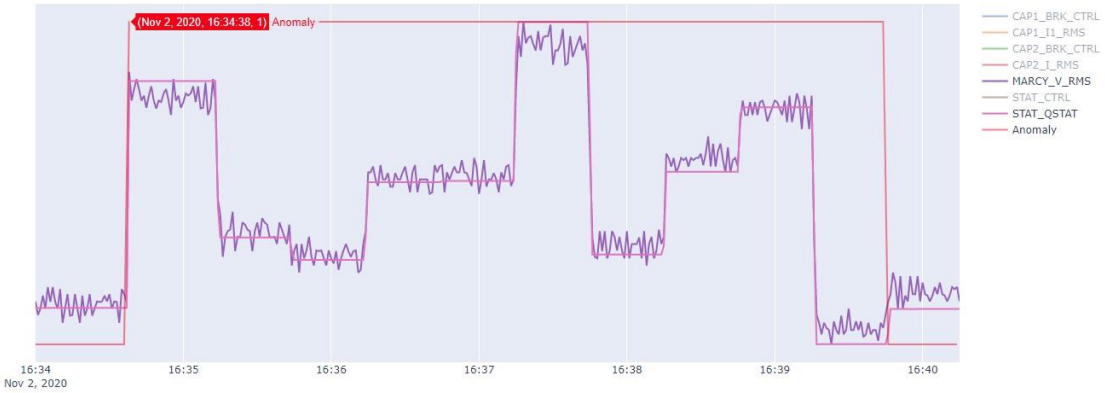
Attack vector: The scaling attack involves a rogue agent gaining access to the RTAC and manipulates its operating logic/parameters to issue randomized STATCOM setpoints at faster intervals.

Detected: Immediately after the attack.

Detection: SIGA's first alert is issues immediately for the anomalous behavior of STATCOM Qref SIGNAL (STAT_QSTAT). This alert and other related alerts that followed appeared on the SigaGuard dashboard.



Attack Process Details: The graph below shows the process trend of the attack. The red line represents the detection time.



Conclusions

Cybersecurity gaps in OT environments need to be addressed taking a multi-level approach, with ongoing threat analysis to minimize the attack surface of potential hackers. When considering adversary tactics and threat models, there is an apparent gap in the field level of the process and sensors, Level 0. This gap was exploited in several cases in recent years and can cause dangerous situations which can affect the OT process and endanger lives.

For this purpose, NYPA and SIGA collaborated in a simulated attack environment to test these scenarios. The sequence of attacks was carefully designed and executed by NYPA's AGILe lab team and cyber experts, focusing on the main cyber scenarios which affect the real operation of the sub-station with either false or no reporting to the control level.

These scenarios were carefully chosen to test SigaGuard as the only process-oriented detection (POD) solution based on Level 0 information which cannot be tampered with or masked. These types of attacks can be prevented by other IDS's only during the actual intrusion (in some cases), but once the perimeter (physical, electronic, or supply chain) is breached, the full process (i.e., the asset) is exposed to the attackers' manipulation while being masked from the control level.

The test outcome was defined to measure the percent of detection events, the time from attack to the first detection, and the assurance of the detection based on the number of internal detection mechanisms recognizing the attack. SigaGuard used only four sequences of a 24-hour substation's normal operation data for the ML engine's training, and all detections were based on deviations from the learned normal data.

Based on the learned data, SigaGuard detected all four attacks in less than 1 second. All attacks were identified by multiple detection mechanisms, setting a high probability of preventing false alerts.

This set of tests validates the significance of Level 0 monitoring as a holistic approach towards OT cybersecurity, clearly demonstrating the unique advantages of combining POD and Level 0 data. Focusing on electric signals—before they are converted into data packets and filtered by the PLC—is probably the most effective technique for accurately identifying an operation anomaly, regardless of the cause. It can bring the highest possible level of visibility into process equipment and sensor functioning, closing an intractable gap against determined adversaries.

Contact SIGA: info@sigasec.com www.sigasec.com