Anomaly Detection Tool

Whitepaper

2022

SIGA

OT Solutions

Authored by:
Hagai Galili

ENERGY SHIELD

Anomaly Detection Tool

IN A NUTSHELL

This paper is describing the work done in the Energy Shield project, as part of the Horizon 2020 program on the anomaly detection (AD) tool. This tool is a part of the complete solution developed in this project, which is aimed to answer all the cyber-security aspects and challenges in the EPES sector. This anomaly detection tool is based on the SigaGuard solution and technology developed by SIGA OT Solutions. SigaGuard safeguards industrial assets by monitoring raw electrical signals (using advanced ML on level 0 data) – as opposed to data packets which can be hacked. SigaGuard brings new and unmatched operational reliability into physical processes, to provide real-time anomaly detection and to support intelligent, real-time, business- critical decision making.

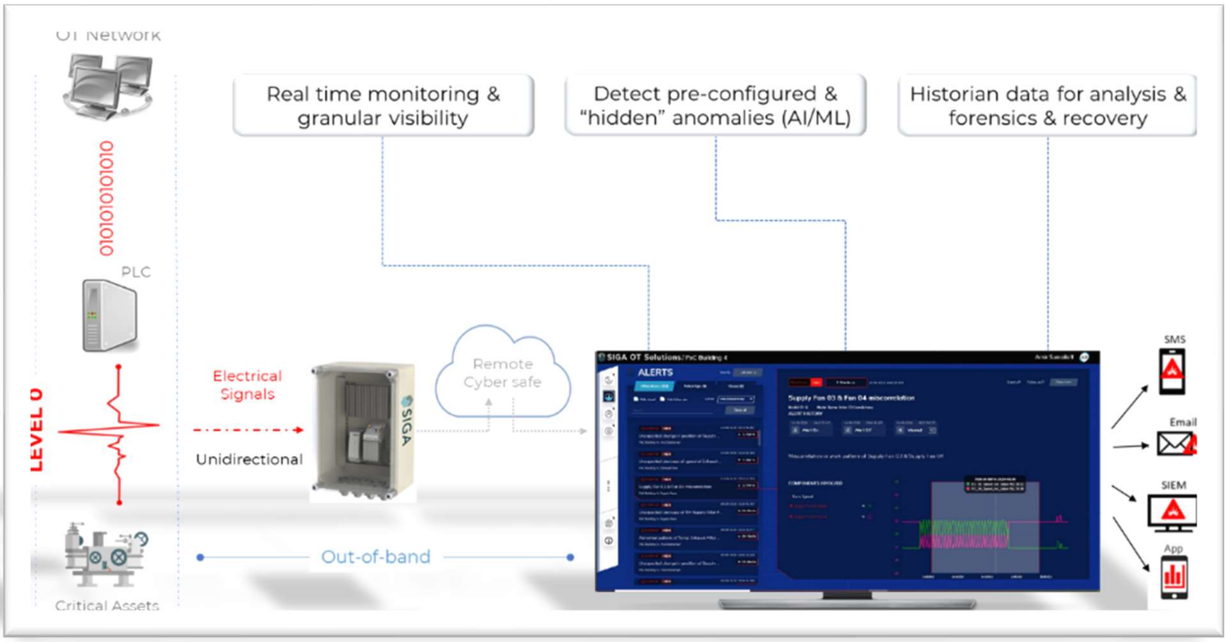
The AD tool was developed based on this approach and technology, adjusting the solution to the EPES. To do so, an existing ML model of SigaGuard was improved, a new ML model was developed, and new features were added to the application. Additionally, the AD tool was installed in two pilot sites to test and demonstrate the tool capabilities.

> “
>
> ***The adoption of machinery and devices monitoring will drive cyber-security to become a crucial asset of Distribution System Operators***
>
> *Sergio Manno,*
>
> *Head of IRETI’s Electrical Network SCADA Systems, IREN Group*

CONTEXT

This anomaly detection tool is based on the solution and technology developed by SIGA OT Solutions, a company which provides OT monitoring and anomaly detection for ICS and SCADA in industrial and critical infrastructure applications. SIGA offers a unique and innovative approach to monitor critical assets and process at level 0 – a bullet-proof, 100% detection rate of any cyber-attack that affects the operation, or causes malfunctions, system failures or deficiencies in the critical asset.

SIGA’s solution is a comprehensive process anomaly detection system that monitors critical infrastructures’ utilities and assets, indicating on a potential on-going cyber-attack on the asset machinery and process layer. The tool is duplicating unidirectionally the ICS/SCADA electrical signals, which run between sensors/actuators and the PLC, and performs real-time process-oriented anomaly detection by using ML models on this data. The tool is autonomously learning the normal behaviour of the asset's process for a limited time period and then detecting abnormal behaviour in real-time and alerts the operators.



The AD tool is customized especially for the EPES market. It can be installed on level 0 of OT systems of all EPES utilities (generation, distribution etc.). With its new developed ML models, the tool can provide the EPES critical assets with level 0 process anomaly detection, that will enhance the ability to detect cyber-attacks that are trying to compromise and intervene with the EPES machinery/process proper operation. The tool will detect the attack in its early stage and alert the operators

TECHNICAL DETAILS

The tool is applying real-time ML models on live process data, which is generated by the tool physical hardware platform, who is duplicating and acquiring the electrical signals. The tool architecture is composed out of four layers:

1. Data Acquisition – A hardware layer that combines off-the-shelf industrial standard electronic components that are assembled into a platform, which is designed for duplicating and acquiring the ICS/SCADA electrical signals and use these signals as data for the anomaly detection engine and for GUI visualization.
2. Software framework – On the hardware layer runs the tool's software framework, ML engine and GUI. From there it can be connected to the internet, allowing for remote access to the Graphical User Interface (GUI) and send alerts and

reports in multiple ways (e.g., e-mail, SMS etc.) and to interface with multiple platforms (e.g., SIEM, SOC etc.). The tool's software framework, ML engine and GUI can also run on a remote server.

The software framework layer is responsible for collection of real time raw handling it and utilize it to be used by the ML engine layer and the GUI Layer.

Another feature of this layer is clustering and aggregation of alerts, to reduce the number of alerts the system will send to the users and to frame specific process anomalies into one event.

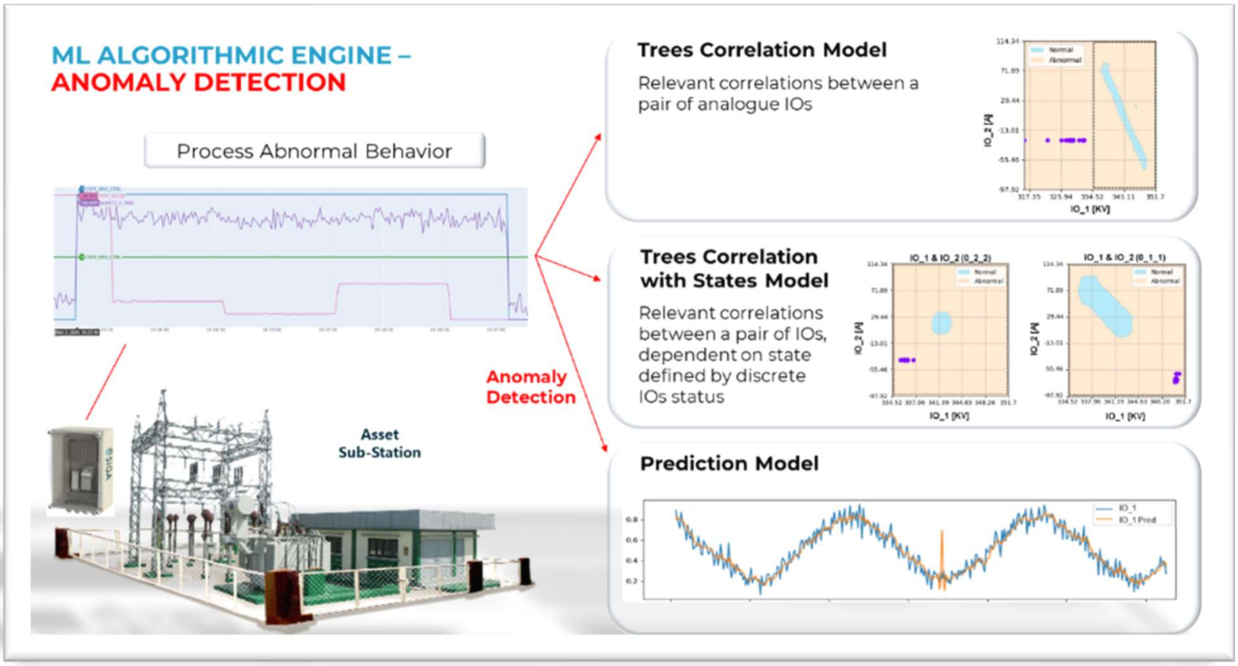
3. ML engine – This layer is pre-processing the data received from the database and then applies multiple ML models on the data for training (in the learning period) and to detect anomalies in real-time (while in operation).

   Once the anomaly has been detected, the ML algorithms engine sends the alert information to the database. It also provides the user with access to the Anomaly ML Analysis tool.

4. Graphical User Interface (GUI) - The tool's graphical user interface is called SigaSight, and it provides the user with asset visualization, alerts and analyses.

SIGA developed the AD tool, based on SIGA's technology, to have 3 new main capabilities for detecting abnormalities in EPES assets' operational process:

1. Improved anomaly detection capabilities and extended user's understanding of anomalies by developing new ML models:
   - Coupled Dependencies Boundary Analysis (CDBA) ML model for detection of abnormal behaviour of analogue IO pairs in multi-dimensional time-series data of the operational process
   - Coupled Dependencies Boundary Analysis (CDBA) with States ML model for detection of abnormal behaviour of analogue IO pairs combined with discrete IOs conditions in multi-dimensional time-series data of the operational process
   - Time Series Parallel Neural-Network Detection ML model for creating multiple parallel prediction, using a neural network (NN) architecture on time-series data of the operational process
2. Improved explainability of alerts, allowing the user more understanding and actionable insights from each alert
3. Added more sources of EPES operational process data for analytics



ML ALGORITHMIC ENGINE – ANOMALY DETECTION

Process Abnormal Behavior

Anomaly Detection

Asset Sub-Station

Trees Correlation Model

Relevant correlations between a pair of analogue IOs

Trees Correlation with States Model

Relevant correlations between a pair of IOs, dependent on state defined by discrete IOs status

Prediction Model

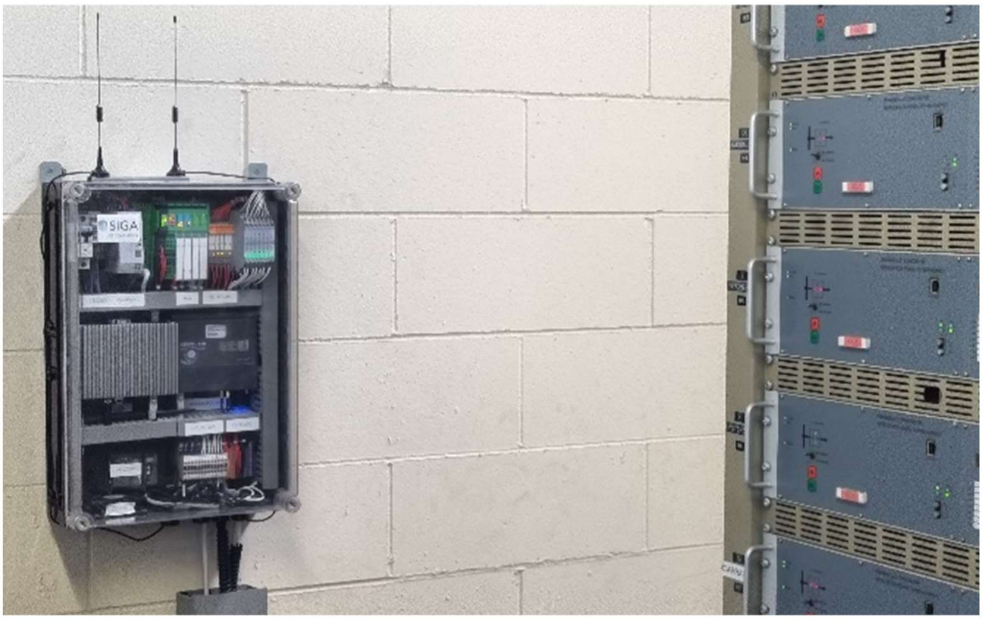
The new ML models were extensively tested for effectiveness, based on true tagged events and very importantly for their false alerts. All models were tested on actual collected data from EPES utilities and integrated into the framework, while each additional model is significantly strengthening the overall tool's performance.

ENERGYSHIELD DEMONSTRATOR

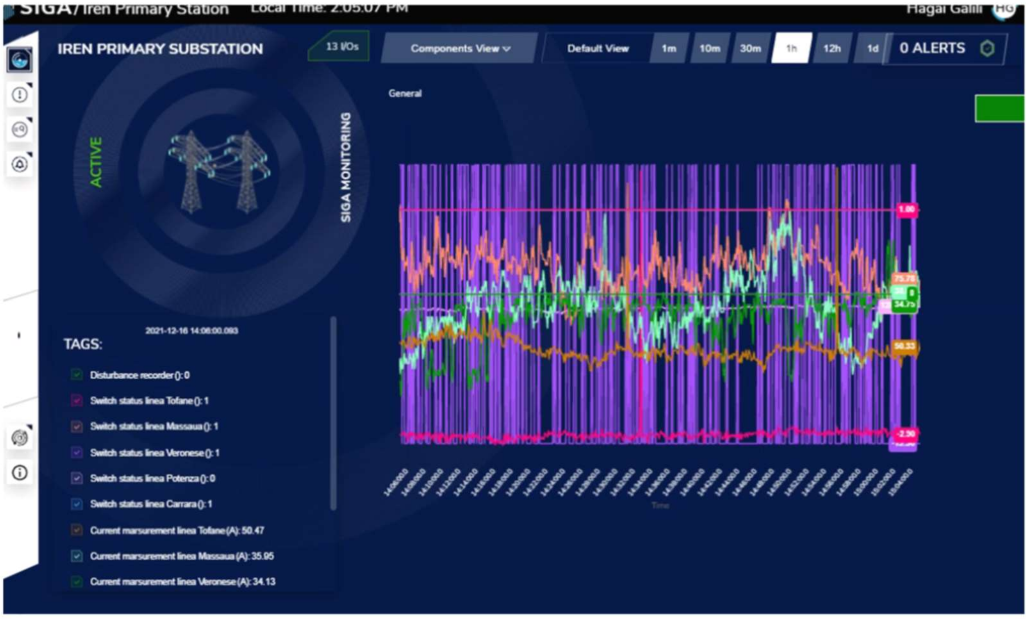
The AD tool was deployed in two pilot sites: in Iren's Martinetto HV/MV substation in Turin, Italy, and in HPP Lenishta hydro power plant in Bulgaria. The deployment included the installation of the SIGA hardware platform in the substation, with the SIGA software and ML engine running on the platform computing device.

The SIGA hardware platform is packaged in a small cabinet, called SigaBox, and was connected and wired to the sub-station and hydro power plant's sensors, circuit breakers and actuators. The hardware platform acquires the data to be used by the tool software and its ML engine is detecting anomalies. The users are provided with SIGA's GUI with secure remote access for visualization and analytics.

In the Italian pilot site, the AD tool is monitoring the operation of 5 different lines of the sub-station (circuit breaker and current measurement in each line) and the main bus bar (voltage measurements). In the Bulgarian pilot site, the AD tool is monitoring the operation of the hydro power (temp., power, flow and pressure sensors).



First, after the installation, the AD tool has learned the normal behavior of the sub-station/power plant process. Once the learning period was completed, the AD tool is now detecting anomalies in real-time. The anomalies the tool detects are caused by abnormal behavior of the substation/power plant operational process. These anomalies can potentially be caused by a cyber-attack performed on the SCADA, in which the attacker is trying to manipulate the substation process operation and harm the machinery, causing a breakdown of the substation/power plant. This can stop the electricity transfer out of the sub-station or the power generation of the power plant, and in some cases endanger the safety of the machinery and even risk human life.



2021-12-16 14:06:00.093

TAGS:

- ☑ Disturbance recorder (): 0
- ☑ Switch status linea Tofane (): 1
- ☑ Switch status linea Massaua (): 1
- ☑ Switch status linea Veronese (): 1
- ☑ Switch status linea Potenza (): 0
- ☑ Switch status linea Carrara (): 1
- ☑ Current marsurement linea Tofane (A): 50.47
- ☑ Current marsurement linea Massaua (A): 35.95
- ☑ Current marsurement linea Veronese (A): 34.13

The AD tool GUI in the pilots is enabling the users full visualization of the process, receive alerts on anomalies, perform analysis and forensics etc.

CYBER TEST IN A PILOT SITE – USE CASE

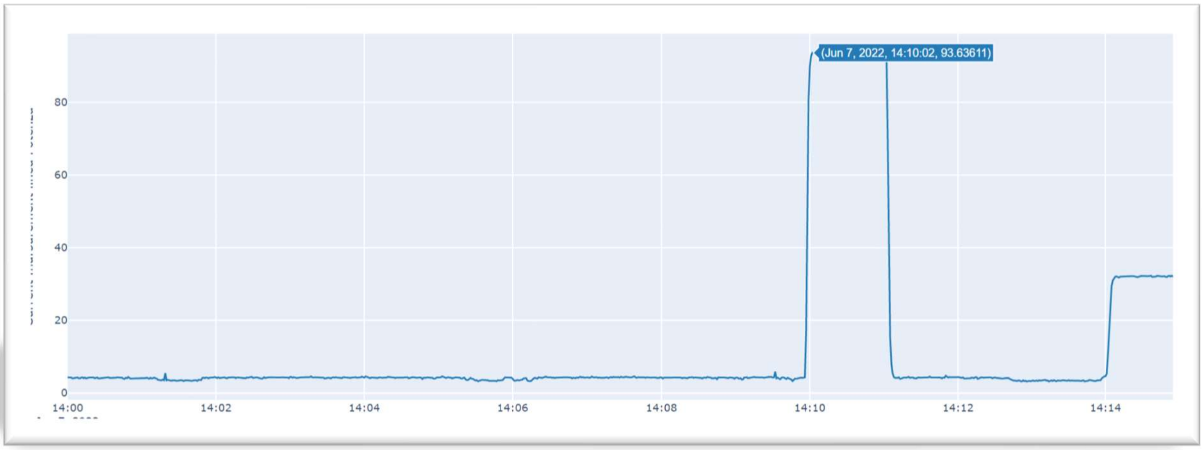
As part of the evaluation of the AD tool performance and functionalities, a cyber-attack simulation test was conducted in the Italian site. in June 2022 Iren's team performed physical manipulation of the physical process of the sub-station, to simulate cyber-attacks and test the tool's capabilities to detect anomalies and alert

Various attacks were simulated (each with several variants), some attacks were conducted physically in the substation systems and some attacks were performed from the control room by using the main control system. The main attack types are presented in the following table

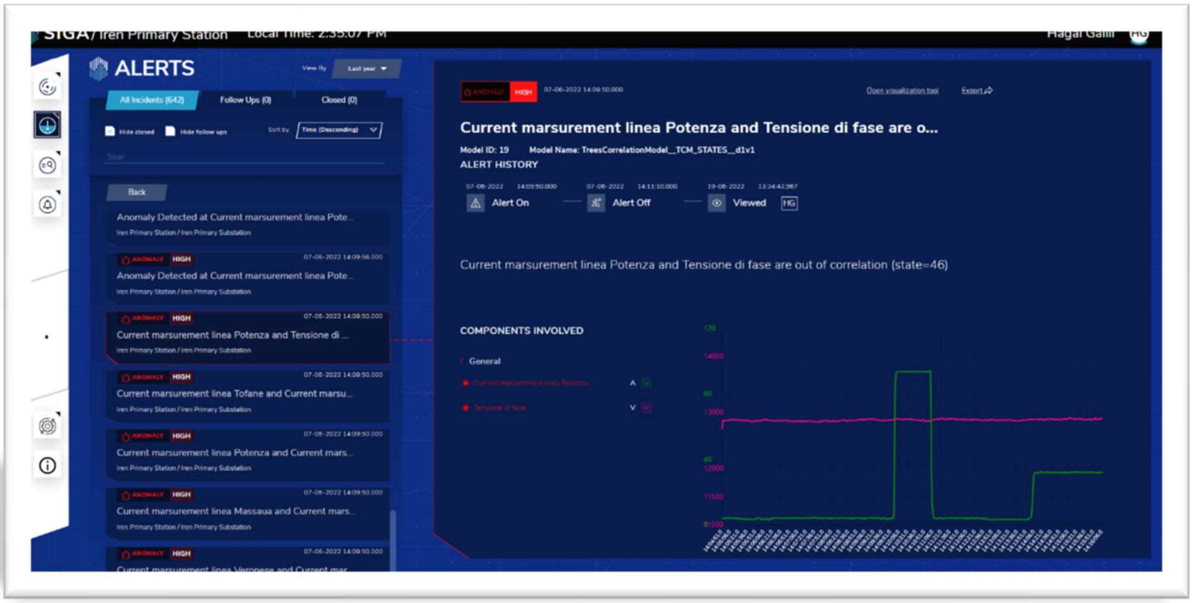
Attack Description	Attack Potential Damage	Test Result
Attacker changes the voltage on the main bus bar	Power outages in all lines	Anomaly detected immediately and alert was fired
Line circuit breaker protection mechanism is manipulated by attacker	Equipment damage and safety issues	Anomaly detected immediately and alert was fired
Attacker is Increasing the load on a line to abnormal values	Interruptions in the grid, damage to the equipment	Anomaly detected immediately and alert was fired
Circuit breakers sequence is changed by attacker	Power outages in some areas of the city	Anomaly detected immediately and alert was fired

To demonstrate the operation of the AD tool, here is an example of an anomaly detection of one of the variants of the attack in which the attacker is increasing the load on the Potenza line, reaching abnormal values:

1. The attacker is suddenly increasing the load on Potenza line, using the control system, from 4 A to 93 A, at 14:09:50



2. The AD tool detects this process anomaly at 14:09:50 (immediately) with various ML models (TCM and TCM with states models).Alert is fired in the GUI and sent by e-mail to Iren's team. The users can now see the alert details and visualization of the attack on the sub-station process.



SIGA/ Iren Primary Station   Local Time: 2:35:07 PM   Hagai Galili HG

ALERTS   View By: Last year

All Incidents (642)   Follow Ups (0)   Closed (0)

☑ Hide closed   □ Hide follow ups   Sort by: Time (Descending)

Back

Anomaly Detected at Current marsurement linea Pote...
Iren Primary Station / Iren Primary Substation

ANOMALY HIGH 07-06-2022 14:09:56.000
Anomaly Detected at Current marsurement linea Pote...
Iren Primary Station / Iren Primary Substation

ANOMALY HIGH 07-06-2022 14:09:50.000
Current marsurement linea Potenza and Tensione di ...
Iren Primary Station / Iren Primary Substation

ANOMALY HIGH 07-06-2022 14:09:50.000
Current marsurement linea Tofane and Current marsu...
Iren Primary Station / Iren Primary Substation

ANOMALY HIGH 07-06-2022 14:09:50.000
Current marsurement linea Potenza and Current mars...
Iren Primary Station / Iren Primary Substation

ANOMALY HIGH 07-06-2022 14:09:50.000
Current marsurement linea Massaua and Current mars...
Iren Primary Station / Iren Primary Substation

ANOMALY HIGH 07-06-2022 14:09:50.000
Current marsurement linea Veronese and Current mar...

ANOMALY HIGH 07-06-2022 14:09:50.000   Open visualization tool   Export

Current marsurement linea Potenza and Tensione di fase are o...

Model ID: 19   Model Name: TreesCorrelationModel__TCM_STATES__d1v1

ALERT HISTORY

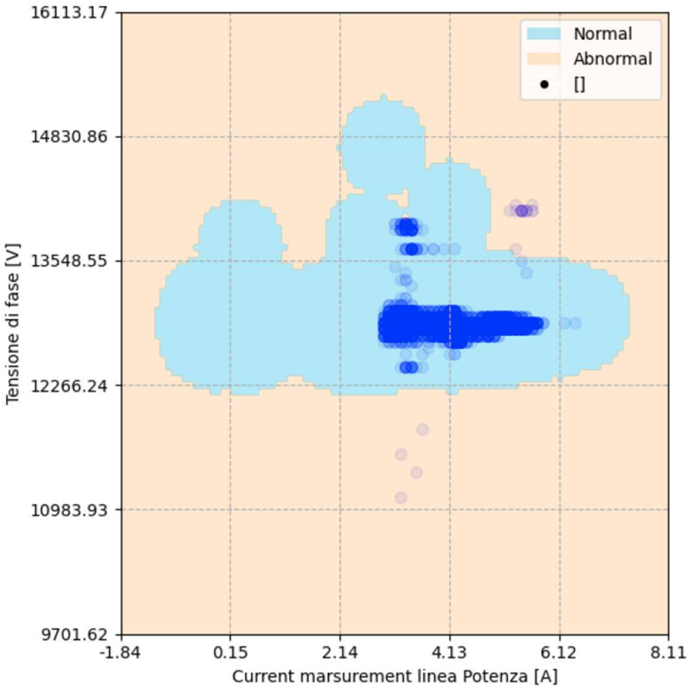
07-06-2022 14:09:50.000 Alert On — 07-06-2022 14:11:10.000 Alert Off — 19-06-2022 13:34:42.987 Viewed HG

Current marsurement linea Potenza and Tensione di fase are out of correlation (state=46)

COMPONENTS INVOLVED

General
- Current marsurement linea Potenza A ☑
- Tensione di fase V ☑

3. The user enters the ML visualization tool in the GUI to investigate the alert and understand where, how and when the attack took place on the process. The following graph is a the TCM correlation map, presenting the correlation between the Potenza line and the bus bar voltage. The blue area is the normal behavior correlations area and the dots outside of it are the abnormal correlations from the attack.



This example demonstrates the importance and advantages of detecting anomalies in the process from level 0. SIGA's AD tool is the only solution that provides the operator with complete visibility into its operations and machinery by performing the analysis of electrical signals directly from the OT/ICS Level 0. The process signals oriented ML models deliver the most elaborated insights to allow the operators to really feel their machinery pulse, and act upon potential threats quickly and effectively, so that downtime is avoided or reduced to the minimum.

ABOUT THE COMPANY

SIGA OT Solutions is securing the integrity of critical OT processes by delivering AI enhanced monitoring and in-depth operational perception. SIGA's Solution, SigaGuard, is a unique comprehensive OT cyber security solution for critical infrastructure and industrial assets using ICS/SCADA electrical signal-based Machine Learning. SIGA is providing out-of-band real-time OT sensors and processes monitoring and analytics for safeguarding the critical industrial assets.

SIGA OT Solutions has implemented SigaGuard in the US, Canada, Italy, Germany, Bulgaria, Singapore, Japan, Dubai and Israel. SIGA holds approved US & European patents and is also certified with the ISO/IEC 27001 information security standard. SIGA was named a "Cool Vendor" in Gartner's "Cool Vendors in Industrial IoT and OT Security" for 2018, awarded the European Union's "Seal of Excellence" in 2019. SIGA is a partner in two development project consortiums: the EU's H2020 DS-04 program and BIRD Foundation Energy Center program – both for developing cyber protection toolkits for the energy sector.

This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907

Website: www.energy-shield.eu Twitter: @EnergyShield_

LinkedIn Group: https://www.linkedin.com/groups/8831159/

Youtube channel: https://www.youtube.com/channel/UCtNRlf0uXvDsxVCSo1NfF_Q

E-mail: EnergyShield@siveco.ro