SIGA
OT Solutions

ICS / OT Applications Brief

SIGA ICS/OT Solutions:

- Operational Reliability
- Process Optimization
- Risk Minimization
- ROI from Operational Optimization
- Critical Assets Intelligence
- Early Failure Detection
- Independent Real-Time Alerts
- Forensics & Recovery
- Machine Learning; actionable insights and "hidden" anomalies
- Enhanced Safety and Regulatory Compliance
- Provides Talent & Native Knowledge Retention

SIGA's patented technology provides a holistic solution for data analysis from the source with full resolution and advanced analytics.

SIGA, connects unidirectionally to the I/O components in the electrical board and copies data from the electrical signals from the analog and discrete contactors. This data is read and managed in a separate, out-of-band channel that is independent of the SCADA / ICS, providing a direct connection to the data without any data tampering. Most of the PLCs and smart I/Os presently marketed filter the reading data based on averaging or other derivative algorithm/s. SIGA is constantly recording the data without any filtering (as raw data) and processing the data to provide many features and insights that are the core of SIGA's offerings.

All the data is compressed and sent to the secured SigaPlatform™, with an independent ethernet connection that is not connected to the SCADA/ICS network. This method of data recording and reading; the SIGA "Data Reader and Forwarder" cannot change or issue any commands for system devices as its connected as "read only" in the system.

Using the SigaPlatform the client can analyze their data with cutting-edge web-based technology on a full feature portal including:

- View the current value of the I/O from the field, data points can be set as group for easy navigation and understanding of the process.
- Build multiple trends with single data point or with correlation to other data points for any time frame.
- View active alarms on the system and acknowledge them as needed.
- Configure alarms as rule based; correlations, prediction and anomaly detection.
- Using advanced analytics and Machine Learning algorithms that can provide an in-depth look at the critical elements of the process and identify very small variances that cannot be identified even with a "trained eye", these "overlooked" variances can develop into a system malfunction or cease production.

These strong capabilities also cover and provide alerts for all process deviations which were not anticipated in the design and therefore are not covered by previously set rule-based alarms.

The advanced analytics and Machine Learning model provide predictions and anomaly detection based on one or more data records enabling sophistication in the logic of the system, this can help shift the work process into a more prescriptive maintenance mode and provide a better, robust system as more resilience is added into the SCADA/ICS work process, enabling the owner to derive new insights into their processes.

At SIGA, we understand that every SCADA/ICS is different which is why our technology platform design is flexible to provide owner's the freedom to select their own setup at reading speeds up to 5000 samples/second for each analog, with resolution starting from **24Bit**, supporting any system on any scale.

SIGA's SigaPlatform™ provides several different owner selected storage profiles in which the owner can choose; indefinitely or for a specific period of time to save the data records based on their specific requirements.

Owners can utilize the SigaPlatform™ to better visualize the data for training and 3rd party demonstrations. The SIGA Technology will provide for consistency of operation even if the PLC or the SCADA system is disabled enabling a backup system in case of major disruptive event on the system.

Unique Features:

- Does not interfere with OT network- ICS Untouched, Completely Out-Of-Band
- Device visibility via monitoring untampered, unsmoothed electrical signals from source (Raw Data, Level 0)
- Independent verification and validation of PLC operation and function
- Machine Learning engine generates actionable insights, "hidden" anomalies & new rules
- ICS/OT- unhackable, cyber security anomaly detection solution; independent of data flow
- Equipment & protocol agnostic
- Legacy compatible
- Forensics, analysis & recovery through independent, out of band data archiving & secure data export

How Siga's Technology Works:

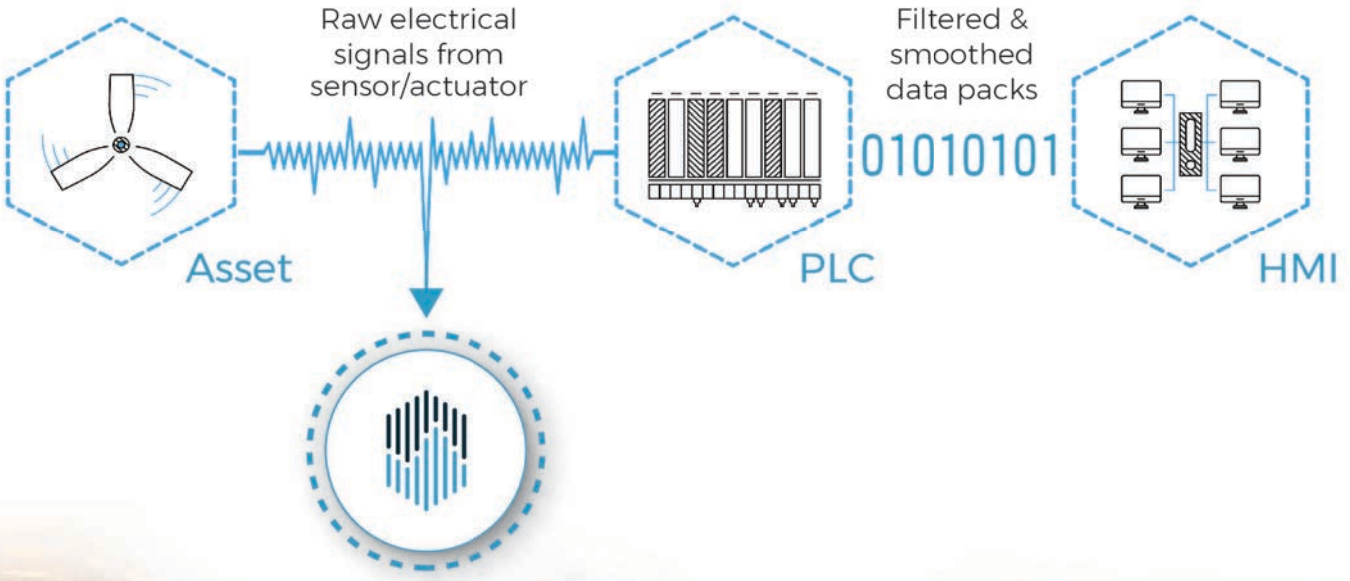
The SigaPlatform is completely out-of-band and works independently of the ICS/SCADA system, making it the most secure and reliable anomaly detection solution.

SIGA's core solution is a "next-generation" anomaly detection platform utilizing a copy of the raw electrical signals, based on fully "out-of-band" hardware and multi-layered analysis aims at identifying process abnormalities to generate new and valuable operational insights.

The SIGA solution is comprised of a hardware layer installed in the critical infrastructure to acquire low-level electric signals, and a software layer applying advanced analytics with optional reliable encrypted data delivery to other systems.

The electrical signals are acquired directly from the control loop between the PLC and the sensors/actuators, using unidirectional isolators, into a separate network. This raw data is analyzed by the SigaPlatform smart AI engine providing verification and validation of the real-time status of the critical end-devices in the OT network with alert and notification options.

SigaPlatform™



The Hardware Layer:

Isolated Transmitters: Utilization of this standard unidirectional automation control component provides non-invasive means to mirror selected electrical signals (current & voltage) utilized/emitted by the assets without affecting the ICS system or the signals themselves. The result is an identical copy of the signal that can be processed in the SigaPlatform, which can be benchmarked, analyzed, and compared across time periods and locations. The transmitter serves as a unidirectional gateway, preventing any possibility of a return signal reaching the I/O that is being monitored. The transmitter does not affect the signal or ICS in any way as its operation is completely "out-of-band" and in parallel to the input signal.

Multifunction Data Acquisition Unit (DAQ): This component acquires and converts the data received from transmitters to a digital representation and sends it to SIGA's main processing server/ computer over a TCP/IP network.

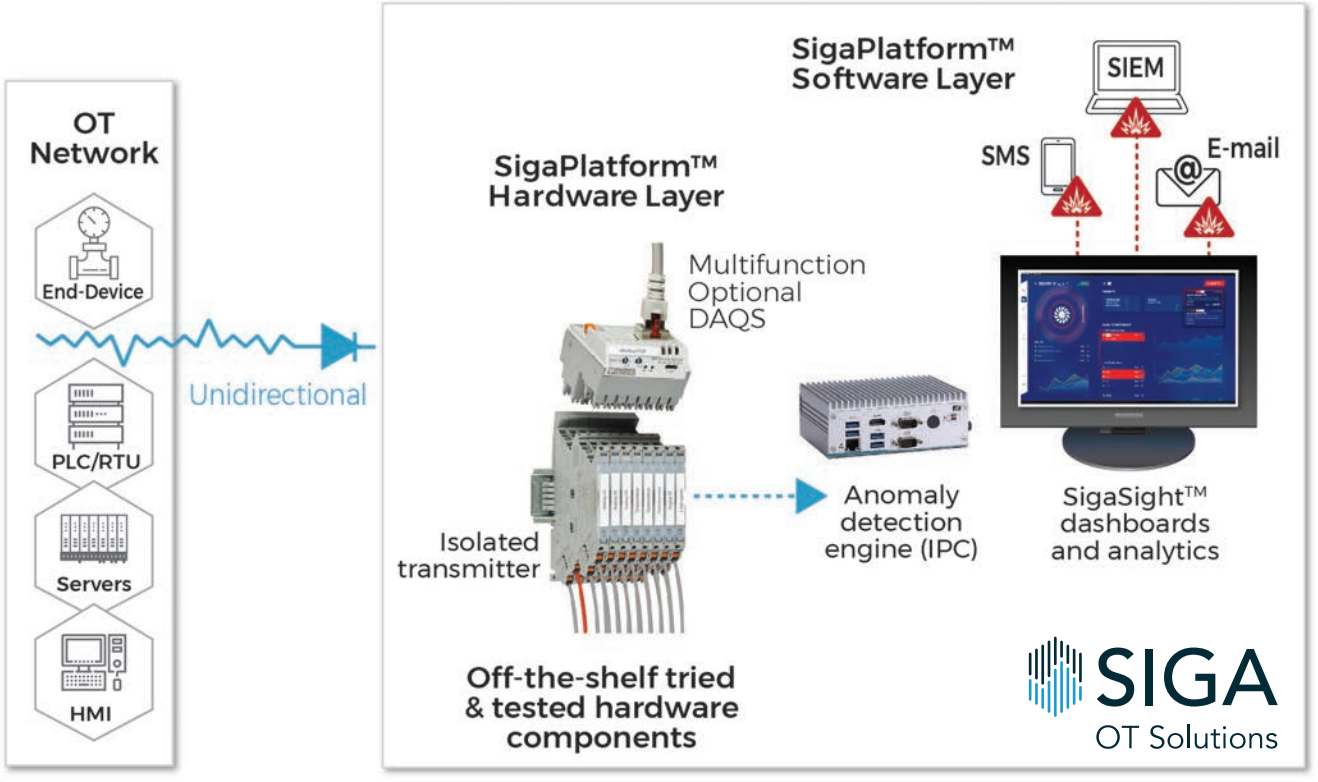
Industrial Computer: A compact rigid computer that is the host of the Anomaly Detection Engine (see Software Layer Components section below). This computer has a powerful processor and is suitable for operating in industrial conditions including high temperatures, dirt and heavy equipment vibrations.

The Software Layer:

Source Visualization: Is the core offering of the SigaPlatform which allows users to continuously monitor their sensors and operational process' health, with data that is normally unavailable in conventional, legacy systems. The information is displayed on a user-friendly and intuitive GUI dashboard named **SigaSight**. By default, the dashboard presents the overall system's state of health, as well as the state of every monitored I/O and a status assessment. Users can analyze trends and prepare reports of their equipment and process performance. In addition, the system logs all major events for future review.

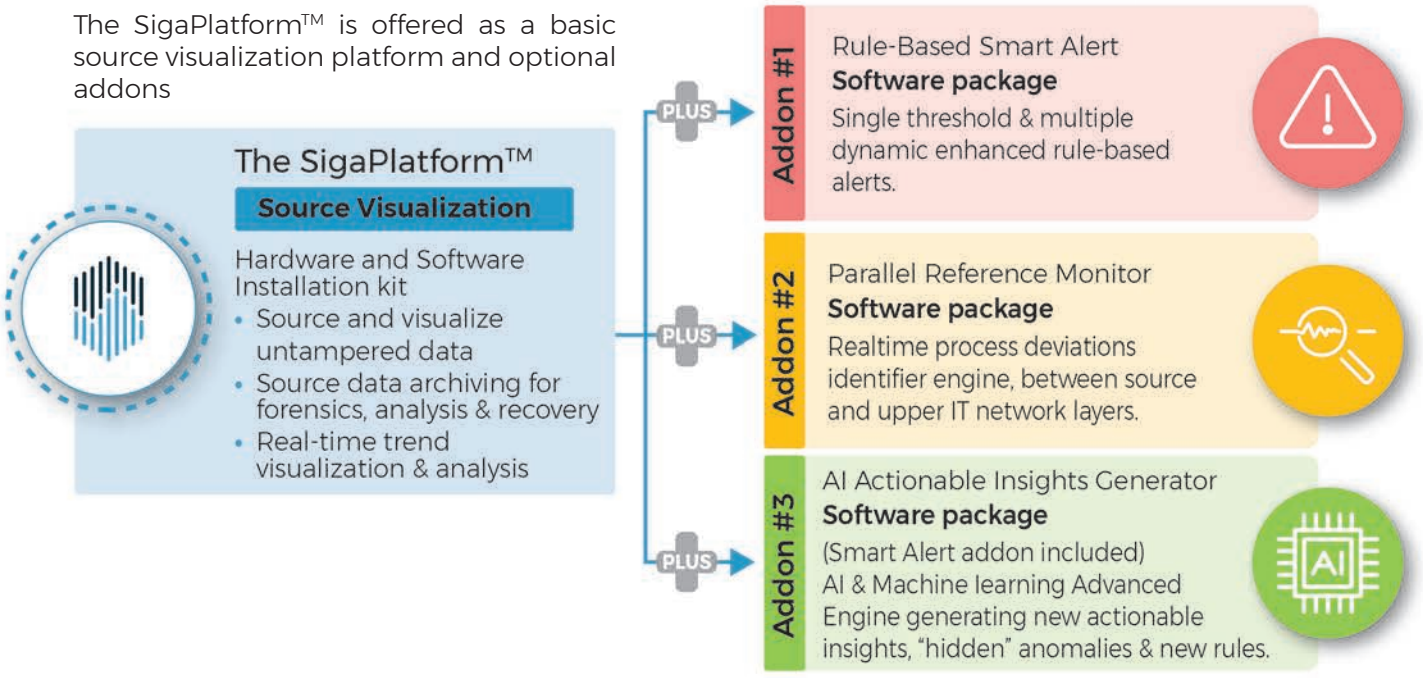
The SigaPlatform™ Architecture

Out-of-Band: Totally Separated, Isolated Network



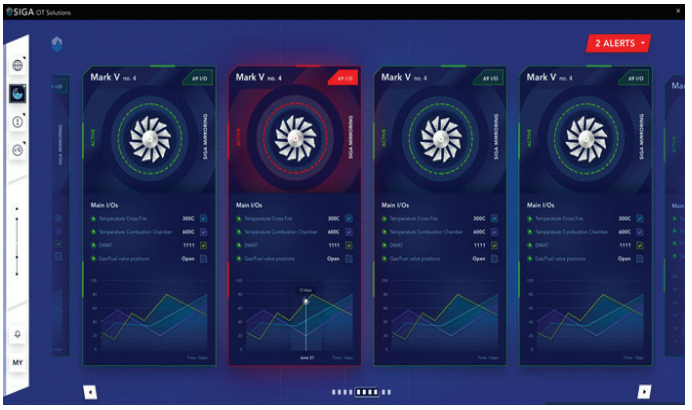
Product Offering:

The SigaPlatform™ is offered as a basic source visualization platform and optional addons



Machine Learning Engine:

The main ML engine's task is to detect anomalies and potential danger in the operational process which are not part of the expected fault cases and not included in pre-defined operational alarms or are unidentified for any reason (operational or cyber). This engine combines proprietary and advanced predictive analysis algorithms that employ machine learning to analyze all incoming signals and identify potential process related anomalies. Any possible threat is forwarded to the SigaSight™ dashboard where it is displayed to an operator or security professional who can investigate, shut-down the asset, flag the warning or determine as "not relevant".



When there is an anomaly in the I/O originating either from a compromised system or from an equipment problem it will create a visible notification with identification of the source of the anomaly.

Built-in ICS Cybersecurity Solution

The SigaPlatform safeguards industrial assets by directly monitoring raw electrical signals (Level 0 real-time monitoring) – as opposed to data packets which can be hacked. This makes the SigaPlatfrom™ a most reliable cyber-attack detection solution – detection which cannot be hacked remotely.

The detection engine is installed on a dedicated, off-the-shelf server (based on SIGA's detailed specifications) and is installed in the client's control room or any other secure location chosen by the client.

The SigaPlatform™ creates value to both operational needs and cyber security needs both under the same platform.

Examples of I/Os for Monitoring: Water Utilities, Building Management Systems (BMS), Power Plants, Chemical, Food, and Pharmaceuticals

Water Utilities

Water Purification facilities:

1. Water level sensors
2. Water turbidity
3. Chloride residues concertation
4. ALOM pumps
5. HCl pumps
6. ClO2 Systems
7. Fluoride pumps
8. Flow-meter
9. Slug mixers
10. Water Conductivity

Dams:

1. Water level sensors
2. Gates position
3. Filters pressure HVAC and Plumbing Systems

Power Plants

Gas-Turbines

1. DC Current
2. SRV POS - Pressure
3. DWAT LVDT
4. Magnetic Pick-up
5. Thermocouples TTXD/CTXF (Cross Fire Tube)
6. Spikes recognition connectors
7. Air valves & pressure
8. Gas valves & pressure

Steam Turbines

1. Heat Exchangers temperatures
2. Evaporator valves

Nuclear
(In addition to the above mentioned)

1. Heavy-water pumps, Chillers etc.
2. Reactor Temp, pressure etc.
3. Generator power supply, Electricity fluctuations, Air conditions
4. Electricity production: Gas/Hydro Turbines

Building Management Systems

HVAC and Plumbing Systems

1. Chiller:
   1.1. On/Off
   1.2. Temperature – In/Out
   1.3. Flow-rate
   1.4. Pressure
2. Pumps:
   2.1. On/Off
   2.2. Frequency (Hz)
   2.3. Pressure
3. AC Units
   3.1. On/Off
   3.2. Water Temperature – In/Out
   3.3. Air Temperature – In/Out
   3.4. Water Pressure
   3.5. Air Pressure
   3.6. Blower Frequency (Hz)
4. Power in (Voltage, Current, Frequency) for various systems
5. Electrical Valves (Actuators)
6. Flood Sensor - water leak detector

Fire Alarm System

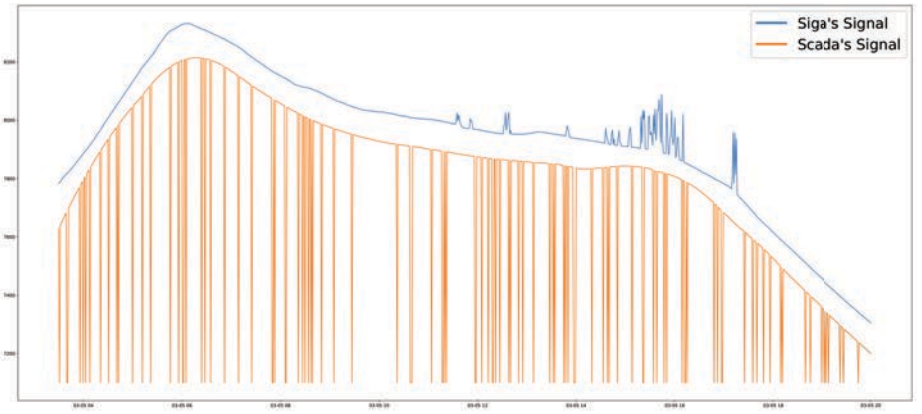
1. Smoke Detectors
2. Heat Detectors
3. Elevator Control

Chemicals Production, Food, Pharmaceutics

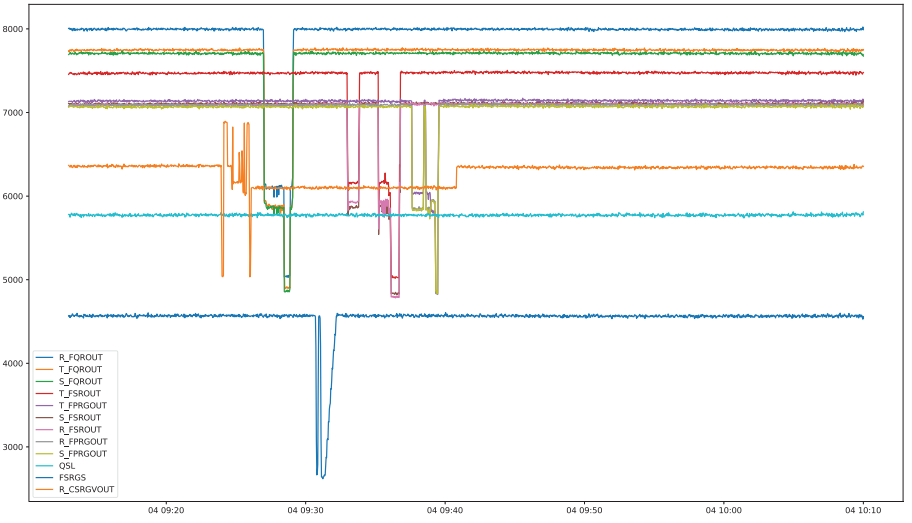
1. Process speed (conveyer belts, rotators)
2. Pressure and capacities
3. Process temperature
4. Counter of products
5. Composition of ingredients
6. Bulk goods
7. CCPs (Critical Control Points) limits
8. Weight of materials

Use case examples of “Hidden” anomaly detection by Siga’s ML Algorithm:

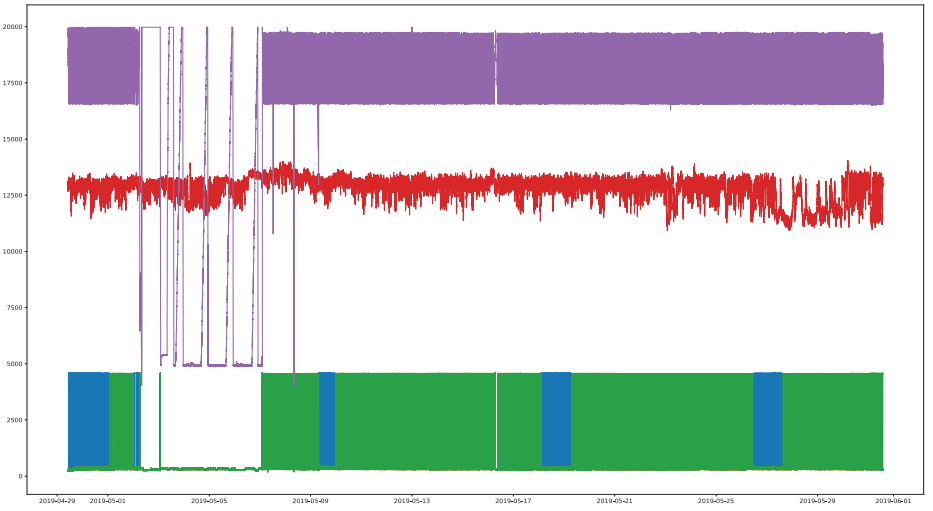
1. Electric spiking detected in a water treatment facility



2. Fault detected in a turbine ignition process



3. Anomaly detection in a water treatment facility



About Siga:

SIGA OT Solutions develops and markets unique OT & cyber security, protocol agnostic solutions based on raw electrical signals of level 0 – sensors and actuators monitoring.

The Siga technology is U.S. patented and ISO/IEC 27001:2013 certified providing OT monitoring, anomaly detection and cybersecurity solutions for commercial, industrial, critical infrastructure, ICS and SCADA systems.

Siga Data Security and Siga OT Solutions Inc., a Delaware corporation, boasts satisfied customers in the United States, Europe, Singapore, Japan, and Israel, and were named a Gartner "Cool Vendor" for Industrial IoT and OT Security in 2018, and are a recipient of the EU Research and Innovation program - Horizon 2020.

Why SIGA:

SigaPlatform™ represents a paradigm shift in how early warning OT process anomaly detection systems operate and is used not only for cyber security but also for predictive maintenance, performance optimization, safety management, regulatory reports – all within the same platform.

The uniqueness and robust SigaPlatform™ is synergetic to many state of the art and legacy solutions, either currently implemented, or already deployed, in the global industrial space.

Using SIGA's machine learning knowledge and algorithms, operators may now, not only gain process monitoring and anomaly detection, but also deeper operational insights of how these processes can be optimized.

Easy Implementation:

- The only generic solution that can be easily be implemented in industrial and critical infrastructure applications that currently have a (ANY) IT/network cyber security solution, weak security or no cyber security protection at all.
- Simple and Fast installation: Doesn't require special configurations or involved installation.
- SigaPlatform™ works with all SCADA equipment and is protocol agnostic.
- Each installation can immediately and securely export the information in any format to any platform.

Enablement:

- Device visibility via monitoring untampered, unsmoothed electrical signals from the source (Raw Data, Level 0).
- Independent verification and validation of PLC operation and function.
- Machine Learning engine detects "hidden" anomalies, generates new rules & actionable insights for process optimization.
- Cyber security, 100% out of band, cannot be circumvented, ensuring resilience & reliability.
- Forensics, analysis & recovery through independent, out of band data archiving & secure data export.

Gartner Cool Vendor 2018

European Commission | Horizon 2020 European Union funding for Research & Innovation

PATENTED PATENTED PATENTED

Information Security Management System ISO 27001 Certified