SIGA
OT Solutions

ICS Cybersecurity Application Brief

SIGA Solutions are ideal for any ICS/ SCADA network:

- Oil & Gas
- Energy & Utilities
- Water facilities
- Critical Manufacturing
- Building Management Systems
- Data Centers
- SOC Operators & MSSPs

ICS/SCADA Cybersecurity – Huge Risk, Big Challenge

Industrial control systems (ICS) were considered to be safe from cyber-attacks because they are isolated, air-gapped networks. However, these critical systems are extremely vulnerable! The development of the Industrial Internet of things (IIoT) and the convergence of operational technology (OT) and IT networks are creating a perfect environment for hackers to attack highly attractive targets - ICS network operators.

Recent deliberate disruptions of critical automation systems (such as the BlackEnergy APT attacks targeting Ukraine's energy companies or the Kemuri Water Company attacks targeting a U.S. water utility's control system) prove that cyber-attacks can have disastrous consequences for citizens and nations. Malicious code can potentially be used to manipulate the controls of power plants, water infrastructure, manufacturing facilities, building management systems and even large ships. All of these are considered critical infrastructure with damage potential resulting in real-world catastrophic physical damage, such as blackouts, disruptions to an entire city's water supply and substantive threat to human lives.

Current ICS Cybersecurity Solutions are Crucial yet Insufficient

Increasing awareness of the ICS cybersecurity threats has led many software companies to develop and offer security solutions specifically designed for OT networks. These solutions are defined by 5 NIST framework functions – identify, detect, protect, respond and recover. Currently, ALL available ICS cybersecurity solutions are based on securing the IP-based network (Data packets), starting from the PLCs, Level 1 of the Purdue Model, and moving up the network to supervisory controls, operations management and business management.

Of course, securing the data-network is crucial, however, it can be hacked despite the layers of protection installed and the operators don't even know it. **Something is missing!**

The Solution:
Monitoring the un-hackable raw electrical signals of critical assets

Paradox: The role of an ICS is to preserve the integrity of physical processes yet current ICS security solutions, designed to protect them, are installed in the most vulnerable levels, the data-packets network! This paradox can be solve by monitoring the most reliable source of information, the physical source which cannot be hacked – the raw electrical signals of level 0 – sensors and actuators.

The SigaPlatform™ safeguards industrial assets by monitoring raw electrical signals (level 0 real-time monitoring) – as opposed to data packets which can be hacked. The SigaPlatform™ 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.

SIGA delivers unique visibility into physical processes - supporting more informed decision-making. The system provides customizable real-time alerts and enables ICS/SCADA operators to consolidate all critical sensor data into one platform for optimized situational awareness.

The SigaPlatform™ is an essential ICS security, level 0 solution, complementary to all other IP-based solutions in the ICS network, level 1 and up.

Our Value Proposition

- ICS/OT cybersecurity solution not depended on data flow and cannot be hacked
- Out of Band: unidirectional secure data export
- Device visibility from untampered, unsmoothed raw data (0 level)
- Enabler for continuous operation even when the ICS/SCADA system is compromised or shut down
- Operational reliability & risk minimization
- Situational awareness – 24/7 anywhere
- Smart alert – rule-based, real-time alerts
- Non rule-based Machine Learning engine: monitoring, analysis, anomaly detection & alerts
- **ICS cybersecurity solutions showing an operational ROI**

The SigaPlatform™ for SOC and managed service providers (MSSPs)

The SigaPlatform™ unique, out-of-band architecture and uni-directional monitoring system, allow this solution to be deployed as a managed service.

The system is the most reliable source of information of a SOC (Security Operations Center), as the information, in the form of electrical signals (physics) is coming directly from the device; and in a communication medium which cannot be hacked or circumvented.

The SigaPlatform™ enables a wide variety of notifications options e.g. email, SMS, and also allows direct integration to SIEM-SOC via Syslog, XML or REST API.

The SigaPlatform™ As-A-Service for SOC and managed service providers (MSSPs) is an ideal anomaly detection solution, highly secured, reliable, unhackable and very cost-effective.

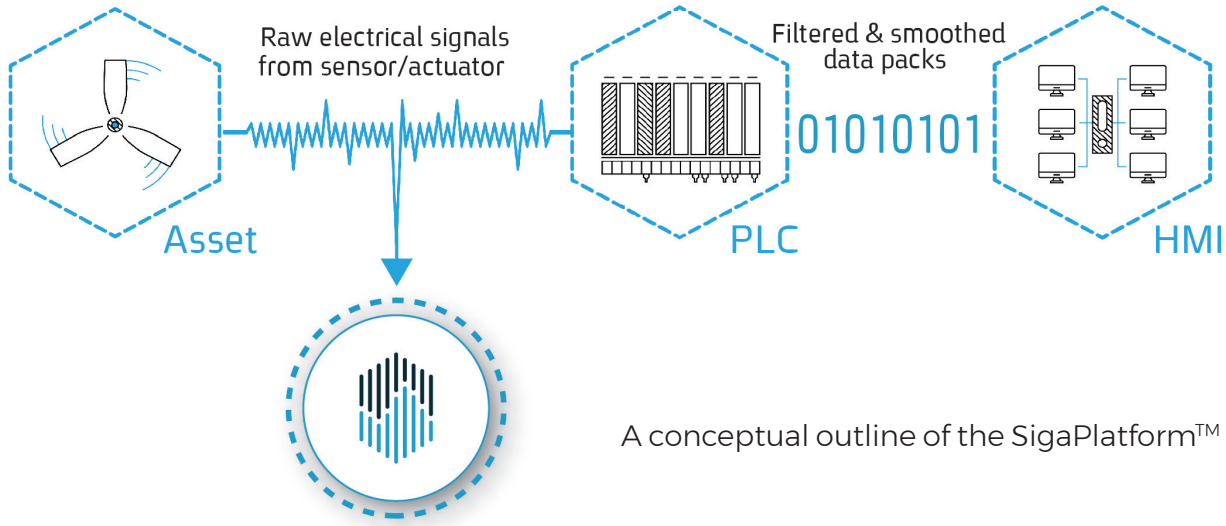
How Siga's technology works:

SIGA's core solution is a next generation anomaly detection platform which is based on securing raw data duplication, based on fully out-of-band hardware, reliable encrypted data delivery and multi layered analysis aiming to identify process abnormalities and generate new and valuable operational insights.

The SIGA solution is comprising both a hardware layer installed in the critical infrastructure, to measure low-level electric signals, and a software layer applying advanced analytics.

The electrical signals are acquired directly from the control loop between the PLC and the sensors/actuators, using uni-directional isolators, into a separate network. This raw data is analyzed by the SigaPlatform™ smart AI engine providing real-time, totally reliable status of the critical end-devices of the OT network, and send smart notifications according to customer specs.

SigaPlatform™



A conceptual outline of the SigaPlatform™

The hardware layer:

Isolated Transmitters: A standard automation control component, Utilization of non-invasive Isolated Transmitters to mirror selected electrical signals (current/ voltage) utilized by the assets without affecting the ICS system or the signals themselves. The result is an identical signal that can be processed in the SigaPlatform, which can be benchmarked, analyzed, and compared across time periods and locations. The transmitter also serves as a uni-directional 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 parallel to the input signal.

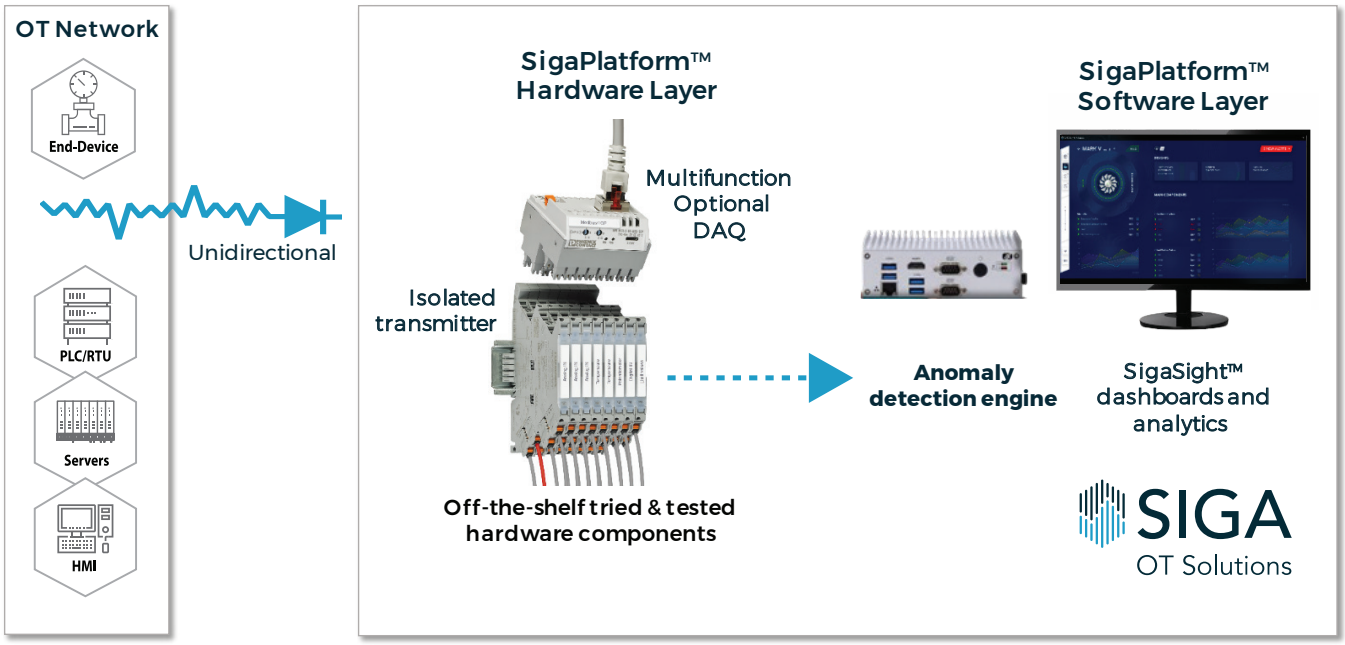
Multifunction Data Acquisition Unit (DAQ): This component acquires and converts the data received from transmitters to a digital representation and sends it to the main processing server/ computer over a TCP/IP network.

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 it is suitable for operating in industrial conditions of high temperatures, dirt and heavy equipment.

The Software Layer:

Source visualization: The basic SIGA Platform which allows users to continuously monitor their sensors and process health, with data that is missing in their 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 are able to prepare analytical reports and ת prepare a trend analysis of their equipment's performance. In addition, the system logs all major events for future reviews.

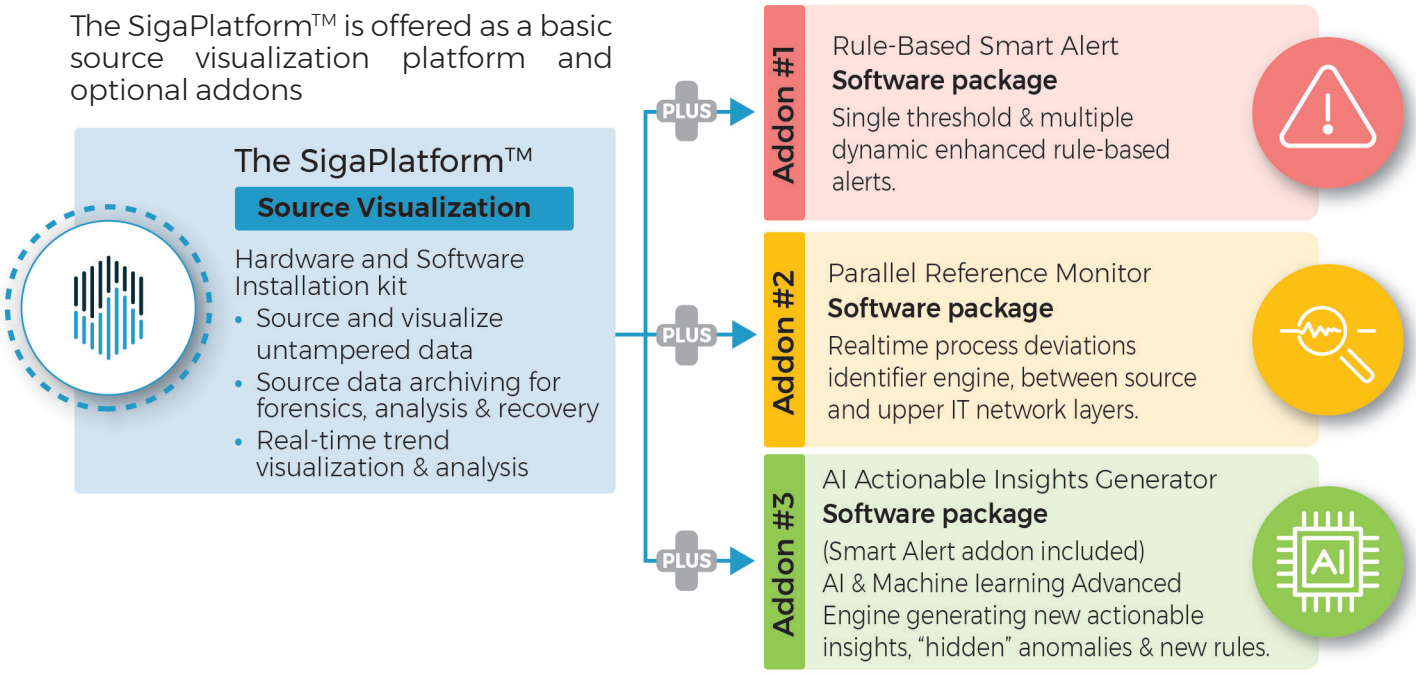
The SigaPlatform™ Architecture



Out-of-Band: Totally Separated, Isolated Network

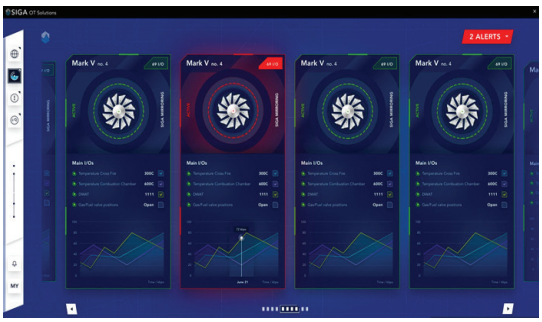
Product Offering:

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



Add-ons:

SIGA offers a set of different add-ons for each customer to choose according to their needs. These add-ons will integrate with the source visualization platform and will supply the users with specific operation insights that fit their needs.



1. **Rule based Smart Alert -** Single threshold & multiple dynamic enhanced rule-based alerts.

2. **Parallel reference monitor -** Realtime process deviations identifier engine, between source and upper IT network layers.

3. **AI actionable insights generator -** AI & Machine learning Advanced engine generating new actionable insights, "hidden" anomalies & new rules.

Machine Learning Engine:

The engine's main task is to detect anomalies and danger zones in the operational process which are either not identified for any reason (operational or cyber) by the operational system or not part of the expected fault cases hence not covered by the predefined operational alarms.

This engine combines proprietary and advanced predictive analysis algorithms that employ machine learning to analyze all incoming signals and identify potential cyber-attacks or process related anomalies. Any possible threat is forwarded to the SIGA Dashboard where it is presented to an operator or security professional who can investigate, shut-down the asset, or flag the warning as "not relevant". The actions of the security professional are re-introduced to the algorithm to improve its accuracy and reliability. The detection engine is installed on a dedicated, off-the-shelf server (based on SIGA's detailed specs) and is placed in the client's control room or any other secure location chosen by the client.

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 directions as to the source of the anomaly.

Cyber attack example: IronGate malware attack with SIGA Installed

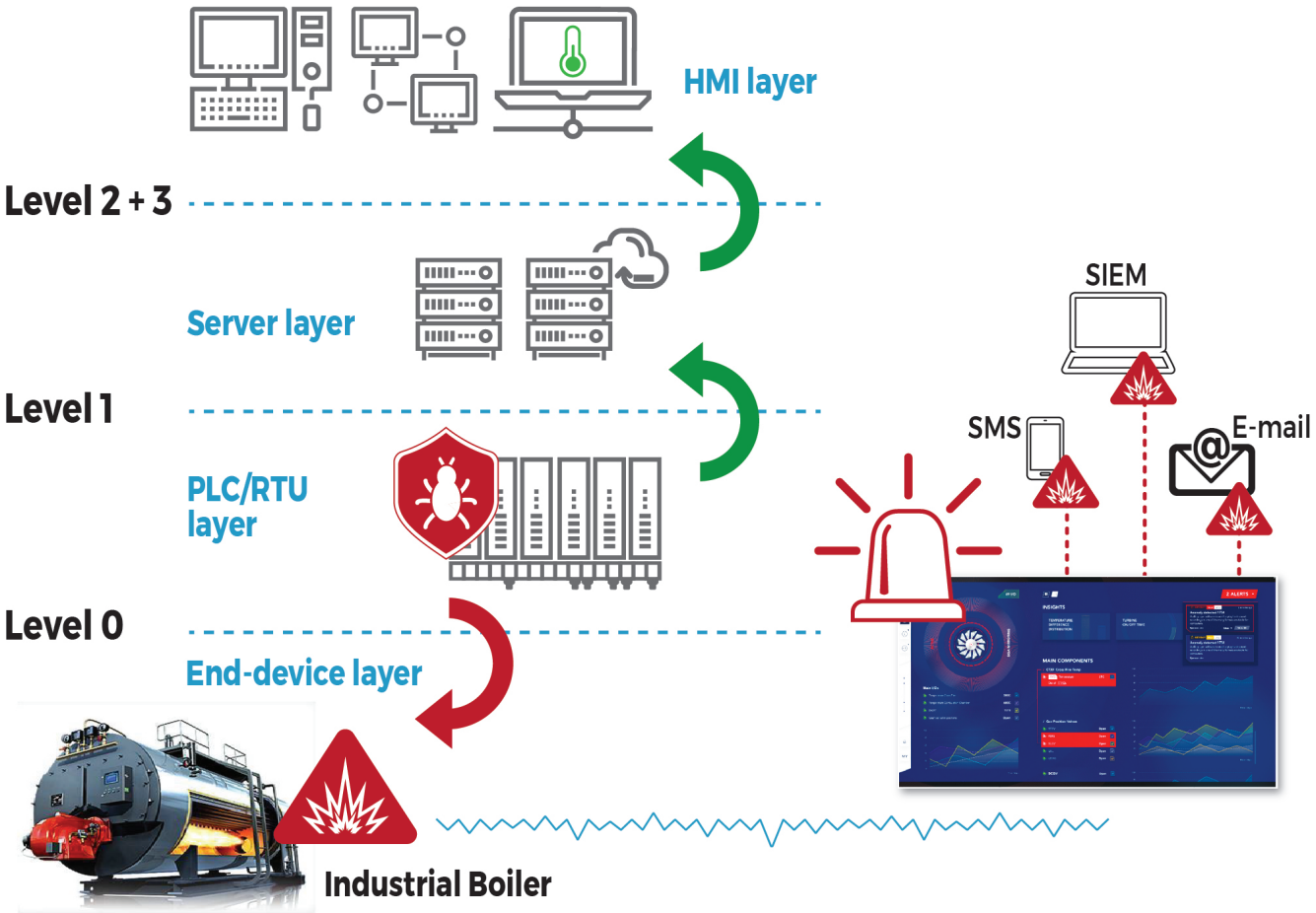
The IronGate Malware, first detected in 2015, targets a simulated control system environment and replicates the type of man-in-the-middle attack seen in Stuxnet. The man-in-the-middle attack allows it to record normal traffic to a PLC and play it back to an HMI.

The illustration below shows an example of an IronGate attack with a SigaPlatform™ installed:

Step 1 Malware sends command to boiler to raise temperature

Step 2 Malware reports back to HMI – **"Temp. is OK"**
Temperature is above normal – HMI is blind

Step 3 Electrical signals are intact and not hacked
SigaPlatform™ sends an immediate, real-time alert



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

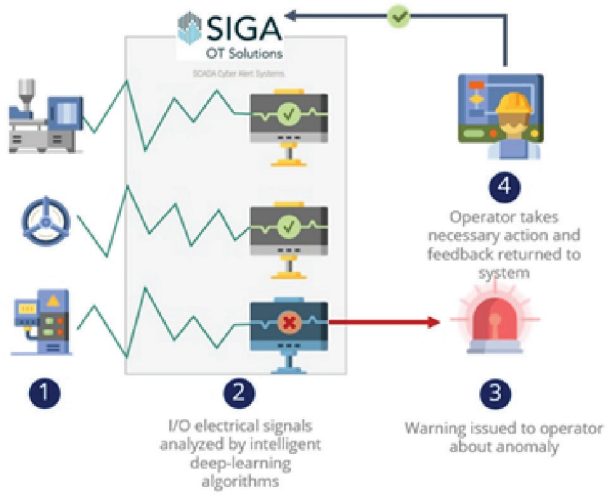
Using SIGA's machine learning knowledge and algorithms, operators may now, not only gain process monitoring and anomaly detection, but also deeper operational insights of how these processes can be optimized.

Benefits:

- Allows operators take concrete actions.
- Monitors the process for process anomalies which are not according to the standard operation.
- Monitors and produces pre-alerts on events that are defined as safety prohibited events.

Unique Features:

- **Applicability:** the only generic solution that can be easily implemented in industrial and critical infrastructure applications that currently have weak or no security at all.
- **Simple and Fast installation:** Doesn't require special configurations or special installation.
- **Flexibility:** SigaPlatform™ works with all SCADA equipment and is protocol agnostic.
- **Connectivity:** Each installation can immediately and securely export the information in any format to any platform.
- **High security level:** SigaPlatform™ provides cyber security, 100% out of band, cannot be circumvented, ensuring resilience & assurance.

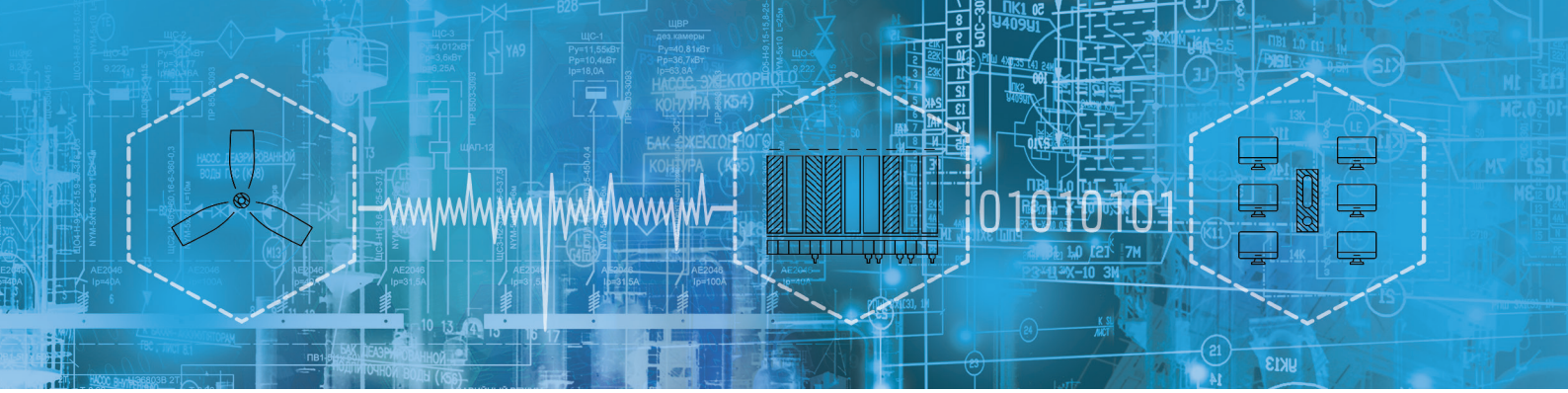


For security
Identify tampering and cyber-attacks

For maintenance
Recognize machines that are not working up to par before regular maintenance schedules

For operations
Pin-point cases where machines are used incorrectly

A systematic over view
Each machine by itself and all the machines as a complete system.



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 27001- 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.

Gartner Cool Vendor 2018

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

PATENTED PATENTED PATENTED

Information Security Management System ISO 27001 Certified

SIGA OT Solutions

SIGA OT Solutions | info@sigasec.com | www.sigasec.com