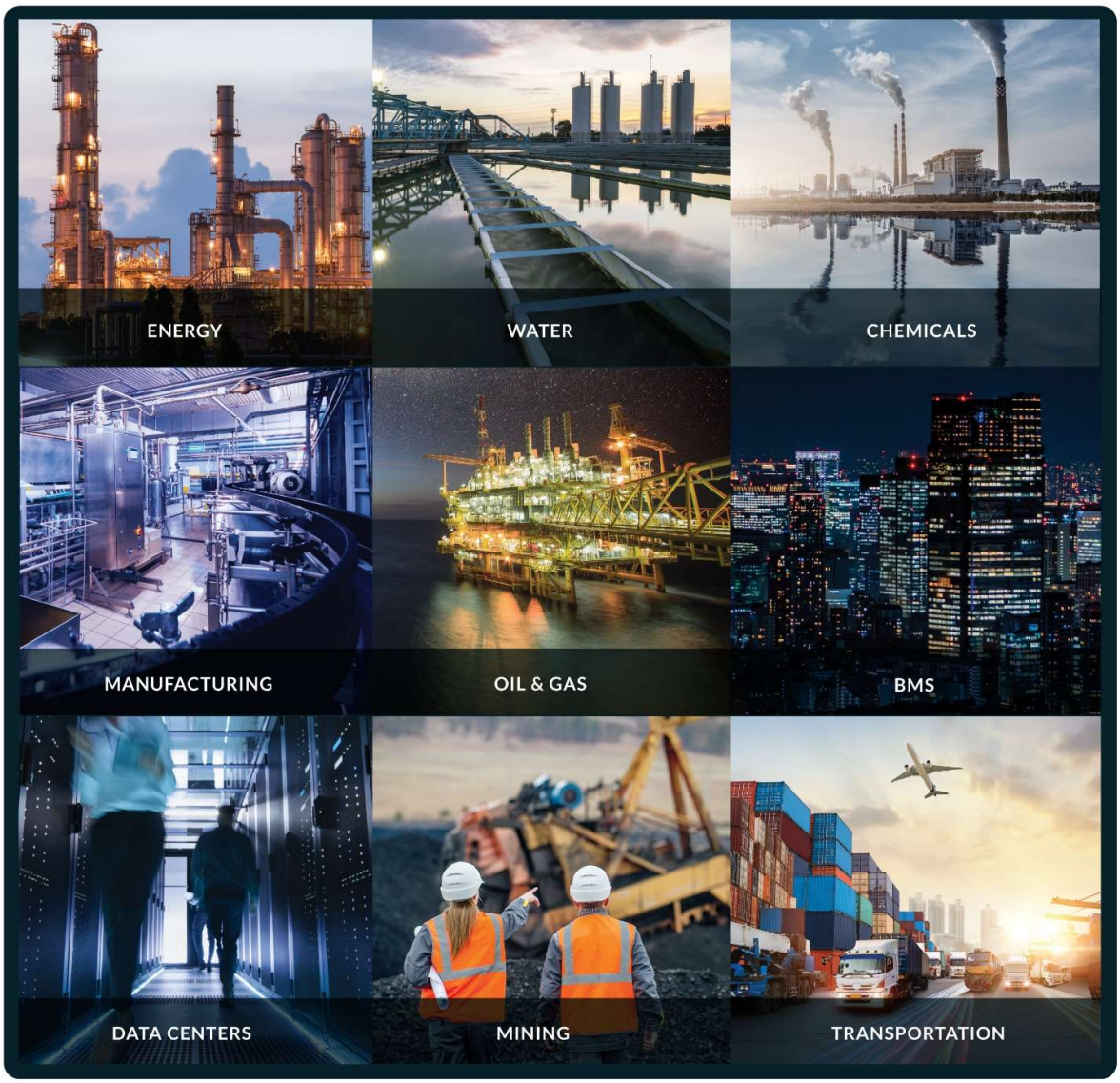
SIGA
Level Zero OT Resilience

Elevating Operational Technology (OT) to Level 0

Total Cyber Resilience for your Mission-Critical Operational Assets

SigaGuard, an out-of-band, cybersecurity solution for Operational Technology (OT) environments, offers the most advanced detection and analytics tool of cyber-attacks on mission-critical automated equipment, machinery & processes.



Total Cyber Resilience for your Mission-Critical Operational Assets

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 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.

The transition to Industry 4.0 requires IT/OT convergence and accelerated "connectivity", along with the ever growing frequency & magnitude of cyber-attacks, raise new concerns and potentially disastrous consequences: financial losses, regulatory breaches, reputational damage, law suits, management liability, high remedial costs & risk to health.

Notable High Profile Industrial Cyber Security 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

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 and business management. Although securing the data-network is crucial, relying solely on these protection layers proves to be insufficient, as many cyber threats to critical assets go unnoticed, leaving your operational processes at the mercy of the attackers.

Operational Technology (OT) environments are designed for protecting mission-critical machines, yet the solutions at-hand only focus on securing the network, hence data packets, while none "speaks" to the machines in a "language" they use and understand – electrical signals coming directly from the sensors and actuators located at the physical layer (Level 0).

SigaGuard – The only Level 0 cyber solution Crucial for any Critical OT Asset

By activating Machine Learning on rich and unfiltered electrical signals at Level 0, SigaGuard delivers an autonomous cyber inspection & analytics solution, offering bullet-proof detection of any cyber-attack, while delivering inaccessible insights, and operational resilience of industrial processes and automated machinery. Electrical signals at Level 0 are the most reliable source of data for OT environments. This source of data is rich & reliable and often unavailable to operators.

SigaGuard safeguards industrial assets by monitoring raw electrical signals (Level 0 real-time monitoring) – 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 support intelligent, real-time, business- critical decision making. SigaGuard delivers unique visibility into physical processes – enabling the system's operators to feel the machinery's pulse and act upon cyber or operational threats quickly and effectively. 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.

SigaGuard 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

Ensuring absolute Cyber Resilience for organizations with ZERO TOLERANCE for operational downtime or failure of their critical assets.

- ICS/OT cybersecurity solution based on the most reliable source- electrical signals at Level 0
- Out of Band: unidirectional secure data export
- Device visibility from untampered, unsmoothed raw data (Level 0)
- Enabler for continuous operation even when the ICS/SCADA system is compromised or shut down
- Operational reliability & risk minimization
- Situational awareness – 24/7 anywhere & anytime
- Smart alerts – rule-based, real-time alerts
- Forefront Machine Learning (ML) engine: monitoring, analysis, anomaly detection & alerts
- ICS cybersecurity solution delivering an operational ROI

SigaGuard for SOC and Managed Service Providers (MSSPs)

SigaGuard's unique, out-of-band architecture and unidirectional monitoring system, make it an ideal solution for a managed service. SigaGuard serves as 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 circumvented (unidirectional).

SigaGuard 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.

SigaGuard As-A-Service for SOC and managed service providers (MSSPs) is a cutting-edge anomaly detection solution, highly secured, reliable, and cost-effective.

How this Unique 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.

SIGA's solution comprises of both a hardware layer installed in the critical infrastructure, to measure low-level electrical signals, and a software layer applying advanced analytics by employing its pioneering Machine Learning algorithms. 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 SigaGuard's 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 specifications.

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 is processed by SigaGuard 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.

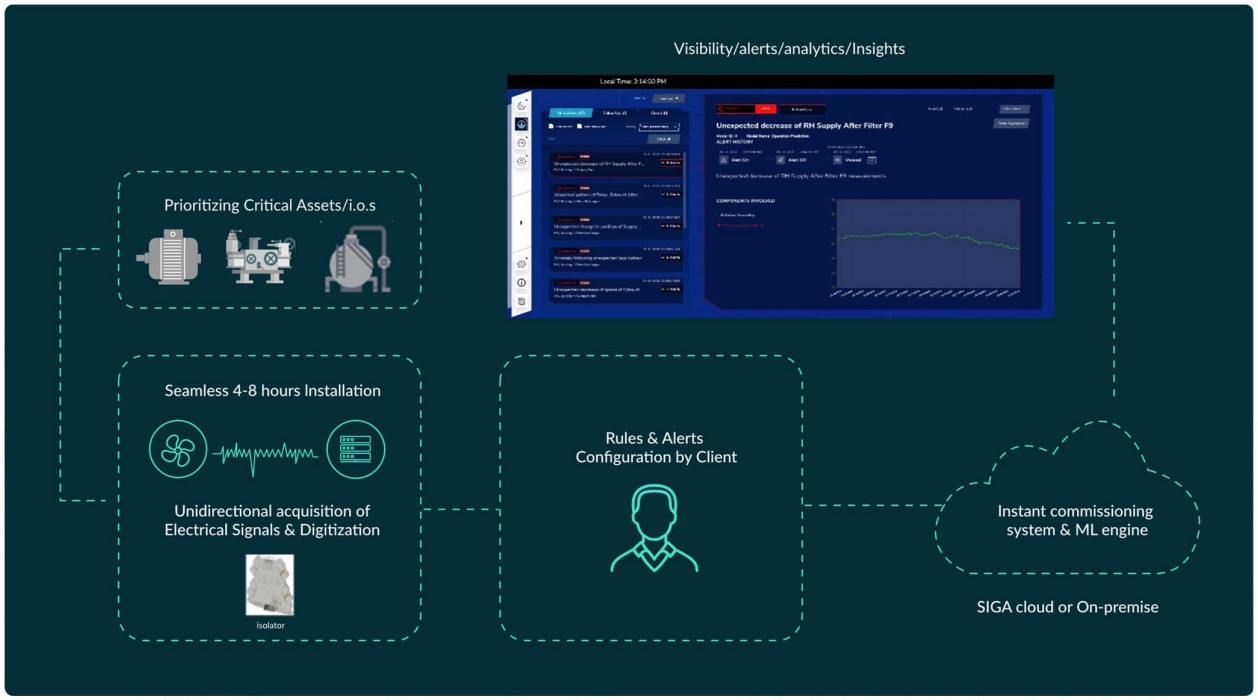
Multifunction Data Acquisition Unit (DAQ): This component acquires and converts the data received from transmitters to a digital representation and sends it to SIGA's main processing server/ computer over a TCP/IP network.

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: SigaGuard ensures users can continuously monitor their sensors and operational process' health, with data that is normally unavailable in conventional network-based systems. The information is displayed on a user-friendly and intuitive GUI dashboard. 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.

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 prepare analytical reports and prepare a trend analysis of their equipment's performance. In addition, the system logs all major events for future reviews and trainings.



Machine Learning Engine

The main ML engine's task is to detect anomalies and potential danger in the operational process which will not be detected otherwise whether cyber threats or operational faults. This engine combines proprietary and advanced predictive analysis algorithms that employ machine learning algorithms to analyze all incoming signals and identify potential process related anomalies.

Any possible threat is forwarded to the SigaGuard's dashboard where it is displayed to an operator or security professional who can investigate, shutdown the asset, flag the warning or determine it as "not relevant". Whenever SigaGuard's algorithms detect an anomaly whether caused by a cyber-attack or a mechanical malfunction it will create a visible notification with identification of the source of the anomaly.

SIGAGUARD

Indegy DRAGOS SCADAfence SECURITY MATTERS

NOZOMI NETWORKS INDUSTRIAL DEFENDER® CyberX Trusted. Industrial. Cybersecurity.

CLAROTY radiflow sentryo PAS VERACITY Industrial Network Security

NexDefense Integrity NextNine Industrial Strength Cyber Security

Level 0

PLC

OT Network

Our Verticals

SigaGuard 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 SigaGuard the 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.

SigaGuard is the ultimate cyber as well as operational solution elevating Operational Technology (OT) cybersecurity to Level 0

About SIGA

Founded in 2014, SIGA OT Solutions is an innovative cybersecurity company driving a paradigm shift within the world of OT cybersecurity.
The company strives to expand the boundaries of OT operations with deepened security and elevated process integrity, by delivering AI enhanced monitoring and deeper operational perception to operators of critical assets.