SIGA
OT Solutions

Water Applications Brief

Siga Solutions Are Ideal For:

- Drinking water
- Municipal water
- Desalination plants
- Industrial water
- Wastewater
- Storage and distribution networks

Securing the Future of Water Infrastructure

A safe water supply and effective wastewater management are crucial elements of modern economies. To better manage growing demand, water authorities worldwide invest heavily in automation and computerization for water purification, wastewater management, desalination, storage and delivery.

Water infrastructure ecosystems have zero tolerance for downtime, human risk and failure. Yet despite ever-tighter regulations and increasing public scrutiny, reliance on sensor data for decision-making leaves critical water infrastructure dangerously exposed to attack or failure.

A History of Water Security Challenges

In 2016, hackers breached a regional US water utility, taking control of hundreds of programmable logic controllers (PLC's) that governed the flow of water treatment chemicals and endangering thousands of lives. This incident, which in part led to the US Water Infrastructure Act of 2018, highlighted the inherent vulnerability of critical water infrastructure worldwide.

Most global water OT (Operations Technology) infrastructure, despite being automated and computerized, is still not resilient in the face of cyberthreats, natural disasters, and equipment malfunctions. Malicious manipulation of data or malfunction can leave operators blind to the actual state of critical assets and result in costly or even catastrophic downtime.

The Solution:
SIGA Incipient Failure Detection and Cyber Protection

Siga offers water infrastructure operators greater operational reliability and control over mission-critical systems – preventing service interruptions and enabling full compliance with strict regulatory regimes including the "Water Infrastructure Act". **With Siga, operators can be confident that they know, anywhere and in real-time the exact status of every critical component.**

Siga uses machine learning-powered predictive analytics to protect critical water infrastructure assets by monitoring the electrical signals that control them. SIGA's incipient failure detection technology directly monitors raw electrical signals – rather than data packets – to detect process anomalies faster, at far greater sampling rates.

Siga delivers unmatched visibility into physical processes - supporting more informed decision-making. The system provides customizable real-time alerts and enables water infrastructure operators to consolidate all critical sensor data into one platform for optimized situational awareness.

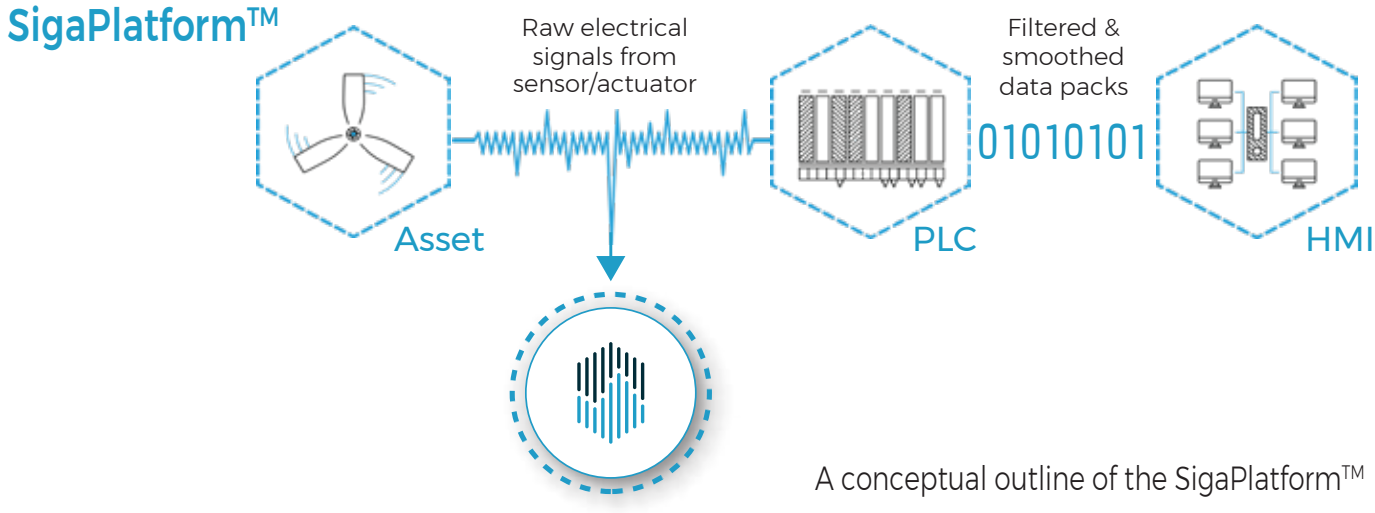
Our Value Proposition:

- Enabler for **Safety & Regulatory Compliance** (AWIA, EU and others)
- Enabler for **continuous operation** even when the SCADA system is compromised or shut down
- **Consolidation of data-critical points** into one usable interface
- **Accessible and reliable awareness** directly from the source, allowing you to know the actual status
- **Real-time alerts & notifications** sent safely to any platform of your choice (SMS, e-mail etc.)
- **Asset performance optimization** & early failure detection by ML providing actionable data

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.



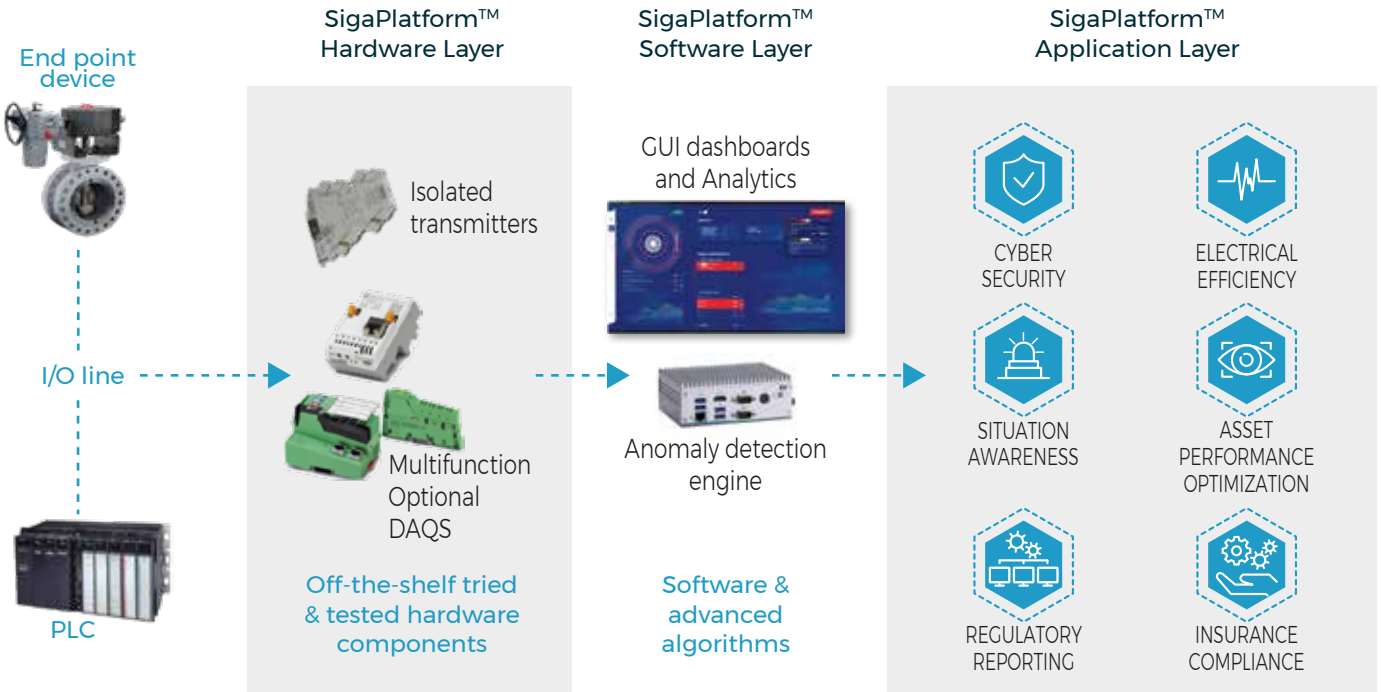
A conceptual outline of the SigaPlatform™

The Hardware Layer:

- **Isolated Transmitters:** 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.
- **Modem (optional):** for safe wireless connectivity.

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



The SigaPlatform™ Architecture

Product Offering:

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

The SigaPlatform™

Source Visualization

Hardware and Software Installation kit

- Source and visualize untampered data
- Source data archiving for forensics, analysis & recovery
- Real-time trend visualization & analysis

PLUS

Addon #1

Rule-Based Smart Alert
Software package
Single threshold & multiple dynamic enhanced rule-based alerts.

PLUS

Addon #2

Parallel Reference Monitor
Software package
Realtime process deviations identifier engine, between source and upper IT network layers.

PLUS

Addon #3

AI Actionable Insights Generator
Software package
(Smart Alert addon included)
AI & Machine learning Advanced Engine generating new actionable insights, "hidden" anomalies & new rules.

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.

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.

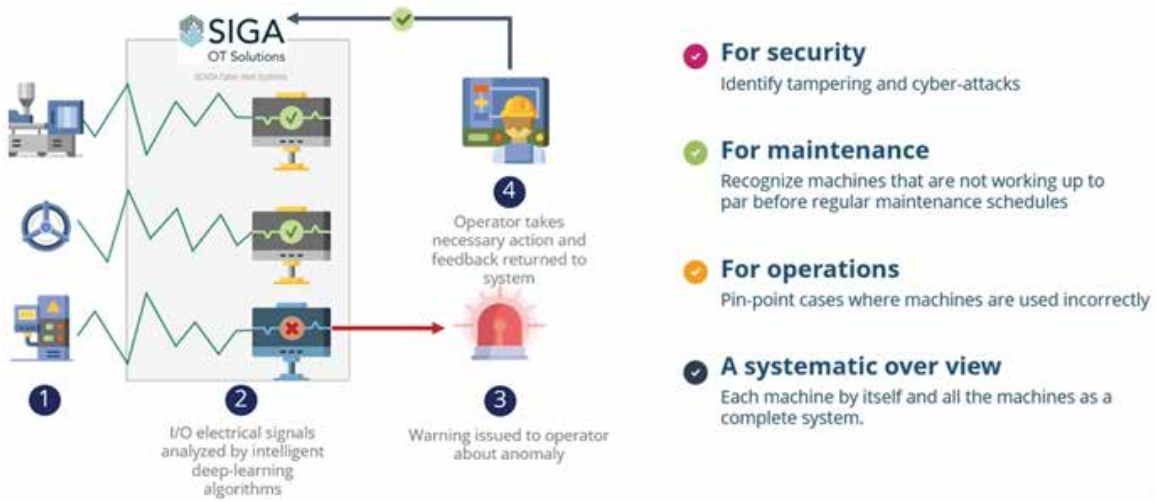
Using SIGA's machine learning knowledge and algorithms, operators may now, not only gain process monitoring and anomaly detection, but also deeper operational insights of how these processes can be optimized.

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.



Gartner Cool Vendor 2018

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

PATENTED PATENTED PATENTED

ISO 27001 Certified

Serving Major Water Authorities Worldwide

Metropolitan Water Reclamation District of Greater Chicago (MWRD) - MWRD's Lockport Powerhouse generates an average of 40 million kWh per year. Siga monitors water level equipment, helping regulate canal levels to prevent flooding, while allowing for navigation on area waterways.

MWRD Chicago: "SIGA installed in 2018 its innovative SigaPlatform™ technology at MWRD's Lockport Powerhouse on the Chicago Sanitary & Ship Canal. SIGA's main mission is to monitor the MWRD's water level equipment, detect any cyber related anomalies and provide further insights for the operators. SIGA's critical infrastructure monitoring solution successfully provided important early warnings & allowed regulatory compliance to any cyber related risks. "

National Water Agency in Asia - National Water Agency – Siga was chosen as a reliable, out-of-band, OT-based cybersecurity solution to monitor critical water infrastructure processes.

National Water Agency in Asia: SigaPlatform™ was tested by the Singapore University of Technology and Design (SUTD) at a secure water treatment testbed in a water reclamation plant, in February, 2019. "SigaPlatform™ has successfully detected 2 cyber-attacks which caused water level violations, including a time-sensitive alert of a sudden drop of water level." Further to this successful test, SigaPlatform™ was installed in a very large water operations network in Asia.

HAGIHON

Jerusalem Water Authority - Siga is connected to critical water management assets, including main valves and level meters, and monitors the behavior patterns of devices and sensors by continuously reading electrical signals and detecting faults and anomalies in real time.

Jerusalem Water Authority ("Hagihon Ltd.") "Starting at 2016, Siga Technology was deployed at Bayit Vagan Reservoir, the largest such facility in Israel, and has been delivering beneficial results. The SIGAPlatform™ is connected to critical water management processes, including our main valves and level meters.
SIGA's technology is a reliable and highly effective tool for detecting significant deviations in normal operations".

About Siga

SIGA OT Solutions develops and markets unique OT & Cyber Security, protocol agnostic solutions based on 0,1 zone direct electrical signal monitoring. The Siga technology is U.S. patented and ISO / IEC 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.

SIGA
OT Solutions

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