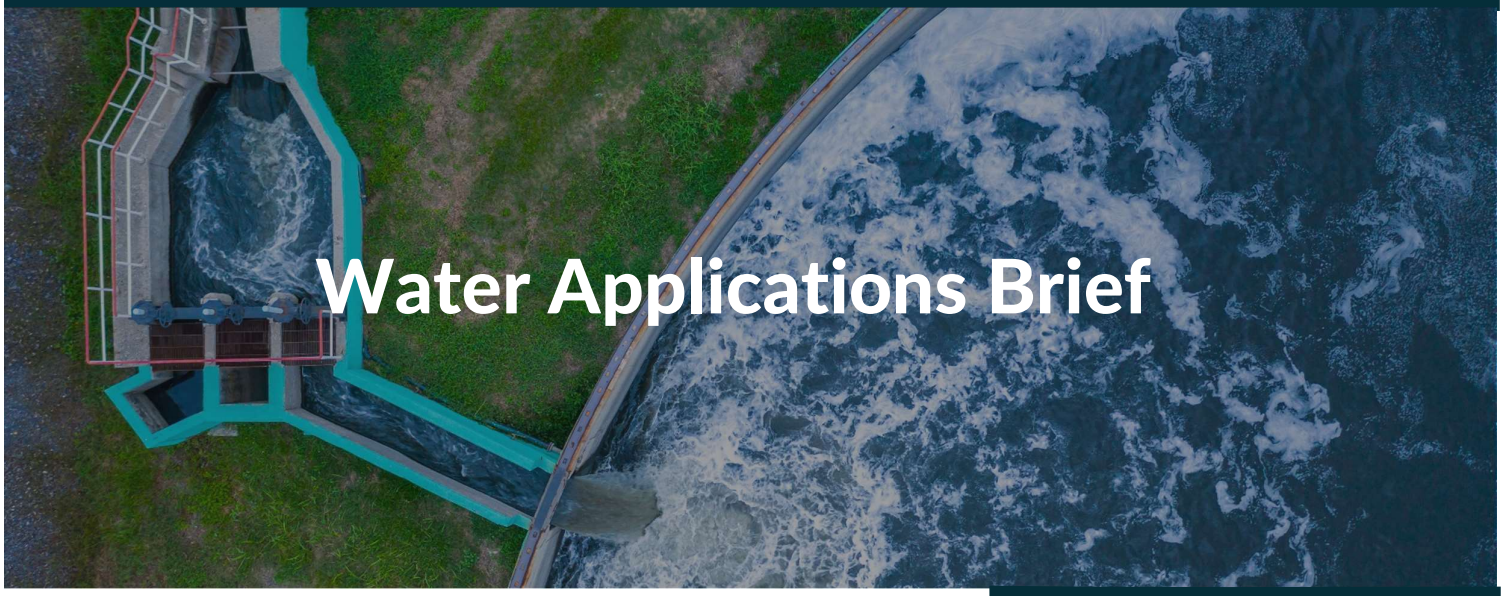
SIGA
Level Zero OT Resilience



# Water Applications Brief

## 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 cyber-attacks or operational failures.

### Siga solutions are ideal for:

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

## A History of Water Security Challenges

In 2016, hackers breached a regional US water utility, taking control of hundreds of programmable logic controllers (PLCs) that governed the flow of water treatments' 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) infrastructures, despite being automated and computerized, are highly vulnerable 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 downtimes.

## The Solution:

### Elevateing Operational Technology (OT) cybersecurity to Level 0

SIGA's flagship solution, SigaGuard 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 SigaGuard, operators can be confident that they know, anywhere and in real-time the exact status of every critical component.

SIGA capitalizes on machine learning-powered predictive analytics to protect critical water infrastructure assets by monitoring the electrical signals coming directly from Level 0. SIGA's cutting-edge technology directly monitors raw electrical signals – rather than data packets – to detect process anomalies faster, at far greater sampling rates to ensure your organization's cyber resilience.

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:

## SigaGuard's Value Proposition:

**Out-of-band monitoring**
Performs 24/7 detection without interrupting your physical processes.

**Feeling the machinery's pulse**
Provides operators with the most reliable source of data.

**Inaccessible insights**
Delivers precise granular visibility with cutting-edge AI insights.

**More data at higher resolution**
Reads the electrical signals up to one hundred times per second.

**Data archives**
Improved preparedness for future attacks.

**Dynamic hardware**
Integrates with your preferred provider's hardware.

**SigaGuard's unique positioning (Level - 0)**
Serves as a complementary solution to other OT solutions.

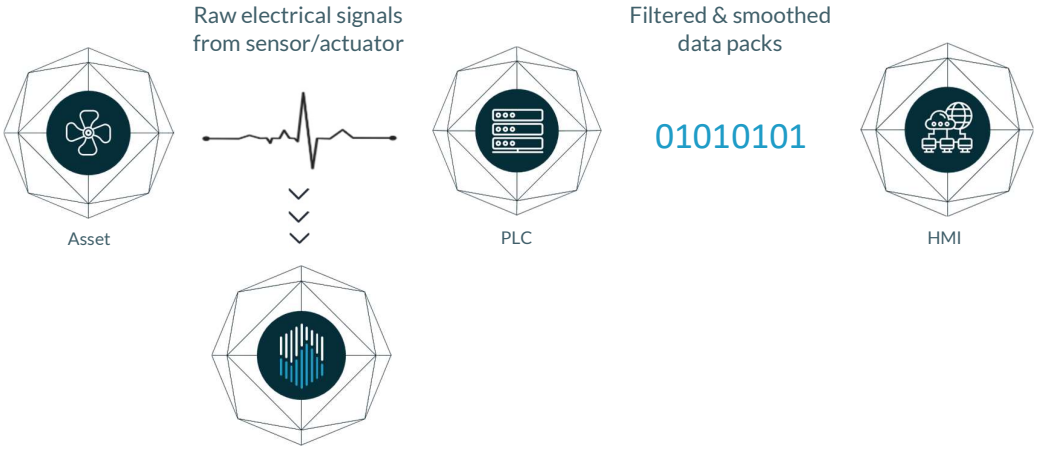
**Reduces downtime to a minimum**
Unmatched visibility ensures a quick and safe recovery from downtimes.

**Regulation compliant**
Complies with the most stringent regulations.

## How SIGA's technology works:

SIGA's core solution is a next generation anomaly detection platform which is based raw electrical signals. Based on a fully out-of-band hardware and multi-layered analysis, SIGA's solution is able to detect cyber-attacks that will otherwise go unnoticed. SIGA's solution comprises of both a hardware layer installed in the critical infrastructure, to measure low-level electric signals, and a software layer applying advanced analytics to detect the process anomalies.

The electrical signals are acquired directly from the control loop between the PLC and the sensors/ actuators, by using unidirectional isolators, into a separate network. This raw data is analyzed by the SigaGuard's smart AI engine which provides real-time and totally reliable status of the critical end-devices while sending smart notifications according to customer's specifications.




## SIGA's 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.

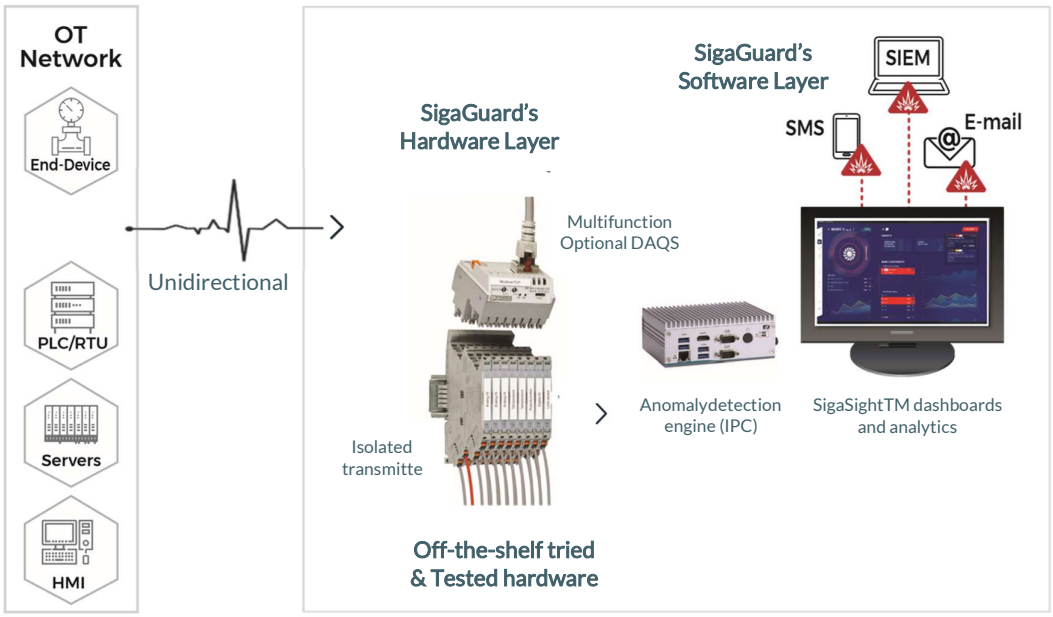
**Industrial Computer:** A compact rigid computer that is the host of the Anomaly Detection Engine (see Software Layer Components section below). This computer has a powerful processor and is suitable for operating in industrial conditions including high temperatures, dirt, and heavy equipment vibrations.

## SIGA's Software Layer:

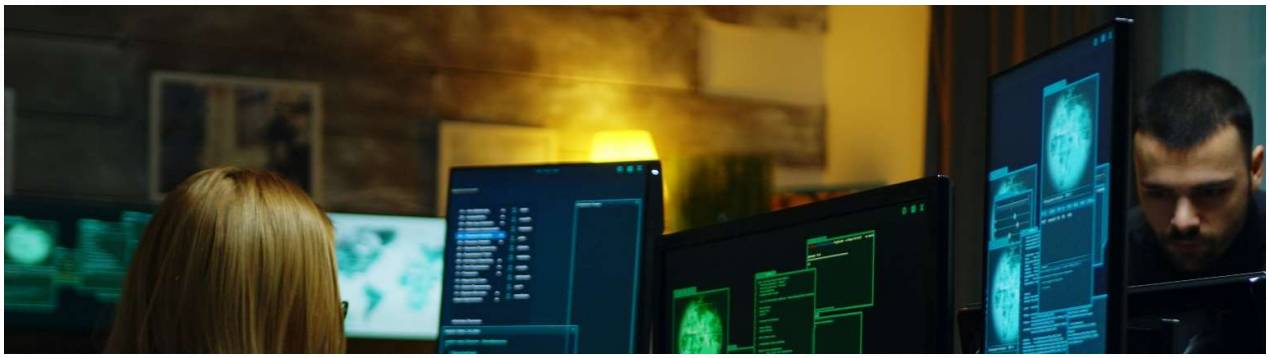
**Source Visualization:** SigaGuard ensures users can continuously monitor their sensors and operational process' health, with data that is normally unavailable in conventional network-based systems. The information is displayed on a user-friendly and intuitive GUI dashboard. By default, the dashboard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

## SigaGuard's Architecture:

Out-of-Band: Totally Separated, Isolated Network




The unidirectional transmitter is installed at the client location between the PLC and end-device equipment without interfering with or impeding ongoing operations and completely isolated from externally connected communications networks. Isolation from the enterprise network reduces the risk of potential manipulation of machine-learning algorithms, enabling optimal cyber resiliency.



## SigaGuard's Value Proposition:

### Out-of-band monitoring
Performs 24/7 detection without interrupting your physical processes.

### Dynamic hardware
Integrates with your preferred provider's hardware.

### Feeling the machinery's pulse
Provides operators with the most reliable source of data.

### SigaGuard's unique positioning (Level - 0)
Serves as a complementary solution to other OT solutions.

### Inaccessible insights
Delivers precise granular visibility with cutting-edge AI insights.

### Reduces downtime to a minimum
Unmatched visibility ensures a quick and safe recovery from downtimes.

### More data at higher resolution
Reads the electrical signals up to one hundred times per second.

### Regulation compliant
Complies with the most stringent regulations.

### Data archives
Improved preparedness for future attacks.

## 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 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.

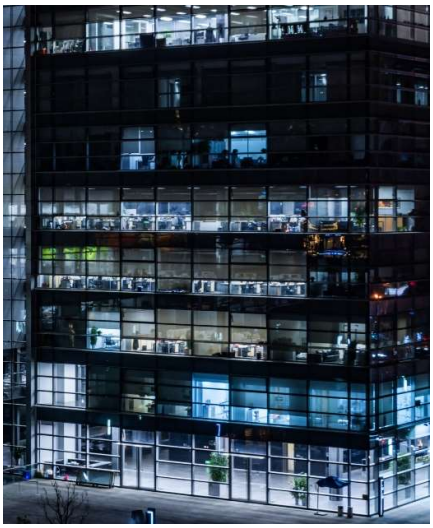
**SigaGuard is the ultimate cyber as well as operational solution elevating Operational Technology (OT) cybersecurity to Level 0**

## Use Case 1: Cybersecurity Protection for Commercial Office Building and Government CERT

SigaGuard was installed in a building housing a number of data centers and other sensitive systems requiring constant and uniform voltage, continuous, faultless cooling, temperature monitoring and emergency response capability for immediate generator operation. SigaGuard is connected to process sensors, located in the building ducts, and continuously monitors electrical signals obtained from chiller frequency, heat pumps, operating commands, etc.

SigaGuard employs unsupervised machine learning to learn the normal operational processes, enabling advanced identification of operational faults in early stages. The platform provides alerts and reports to the operation managers in order to promote cyber resilience, prevent system downtime, ensure operational efficiency, timely maintenance, safety and cyber protection.

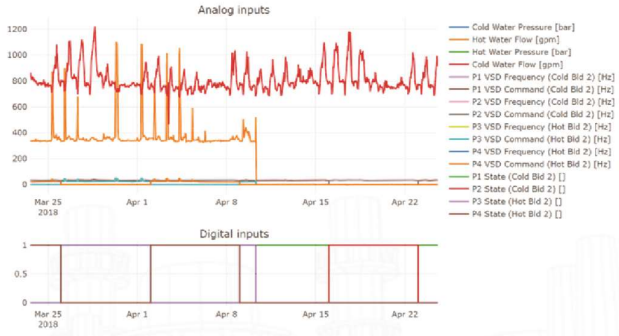
A normal process is one in which both chillers and heat pumps operate simultaneously. SigaGuard has the ability to distinguish between a normal process and any process deviation, providing process optimization and power conservation by maintaining ideal operating requirements. Malfunction/shutdown of pumps may result from voltage fluctuations in the electrical grid, malfunctioning PLC or a mechanical malfunction. SigaGuard detects the faults at the onset and provides real-time alerts immediately upon identification of any anomaly in the process. The system sends an accurate detailed SMS/screen notification (in addition to any required logs) describing the specific alert.



SigaGuard saves countless “human-hours” by producing automatic & continuous operational reports on demand, providing real-time data on each process, or pinpointing critical end-points for monitoring as a separate and independent system. Real-time fault detection is invaluable to critical asset management and operational reliability.

### Anomaly Detection in Pump 2 (Cold Water)

### Normal pattern of Cold/Hot Water Pumps



## 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 SigaGuard 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. "

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

Public Utilities Board (PUB), Singapore: SigaGuard was tested by the Singapore University of Technology and Design (SUTD) at the secure water treatment testbed in PUB's water reclamation plant, in February, 2019. "SigaGuard 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, PUB has deployed SigaGuard inside their operations network at the Ulu Pandan facility.

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 SigaGuard 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

## 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 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.